
بسم الله الرحمن الرحیم

تقدیم به بزرگ بانوی دو عالم حضرت فاطمه الزهرا(سلام الله علیه)

آموزش امنیت سایبری

ممیزان

مولف

مهندس ناصر نامخواه

سرشناسه: نامخواه، ناصر، ۱۳٤۰

عنوان و نام پدیدآور: آموزش امنیت سایبری – ممیزان

مشخصات نشر:

مشخصات ظاهری: ۳۸۳ص. ، مصور، جدول، نمودار

شابک:

وضعیت فهرست نویسی: فیپا

یادداشت: واژه‌نامه

یادداشت:

کتابنامه: ص. ۳۸۳

موضوع:

موضوع:

نام کتاب: آموزش امنیت سایبری – ممیزان

تألیف: مهندس ناصر نامخواه

نوبت چاپ: اول، بهار ۱۳۹۰

ناشر:

صفحه آرایی : مجید بهمنی

طراح جلد : مجید بهمنی

شابک:

تیراژ:

قیمت: ریال

مقدمه

در طول تاریخ توسعه و امنیت همیشه مانند دو بال پرندگان در کنار یک‌دیگر نبوده‌اند. قبل از اختراع برق که شاید بتوان از آن به عنوان شروع عصر جدید انسان‌ها نام‌برده عصری که امروزه از آن با عنوان دوره نوین و در برخی موارد عصر دیجیتال نام بردند، امنیت همپای توسعه دارای رشد مناسبی بوده است. هر میزان دسترسی انسان‌ها به علم و فن‌آوری تا این زمان منجر به افزایش امنیت می‌گردید. ابزار تولیدی در مسیر توسعه همراه با خود امنیت فکری و اجتماعی انسان‌ها را افزایش می‌داد. با ورود بشریت به دوره جدید که برخی شروع آن را هم زمان با اختراع برق نامیده و اختراع ابزاری مانندترانزیستور و مدار مجتمع و تجهیزات الکترونیکی تهدیدات جدیدی فراروی انسان‌ها گشوده شد.

سرعت رشد تکنولوژی در اعصار جدید از سرعت بسیار بالاتری برخوردار بوده است، لکن به نظر می‌رسد که هر توسعه جدیدی همراه با خود ناامنی‌های جدید را به ارمغان می‌آورد. این مطلب باعث شده است پژوهش‌های مختلف ارتباط بین امنیت و توسعه را رابطه‌ای معکوس بنامند لذا به نظر می‌رسد یکی از راه‌های وصول به امنیت در دنیای دیجیتال شناخت واقعی این عرصه ابزار مرتبط با آن می‌باشد.

با گسترش فعالیت مباحث پدافندی غیر عامل در کشور و حرکت تخصصی این فعالیت‌ها به مرور شاهد نشر دانش تخصصی در عرصه پدافند غیر عامل فاوا با رویکردهای علمی و عملی در زمینه تهدیدات موجود و راه‌های شناخت آسیب‌پذیری‌ها و مقابله با آن‌ها توسط سازمان‌ها، نهادها و کاربران و مدیران در این عرصه می‌باشیم.

کتابی که در پیش روی دارید که یکی از چهار جلد کتابی است که با هدف آشنایی افراد مرتبط با این گونه ابزار و به منظور حفاظت از منابع و سرمایه‌های ملی نظام جمهوری اسلامی، ایجاد ثبات در کاربرد

سیستم‌ها و اطمینان از استمرار و سلامت اجرای فرآیند فعالیت‌های کاربران مختلف جمع‌آوری و تألیف گردیده است.

تمام دستورالعمل‌ها و اسناد عملیاتی تنظیمی در لایه‌های مختلف سازمان و هر جامعه‌ای می‌بایست به روش‌های علمی و عملیاتی و در برهه‌های مختلف از زمان می‌بایست ممیزی گردد و میزان

کارآیی آن‌ها و قابلیت اعتماد به روش‌های اجرایی آن سنجیده شود. در این کتاب که به نام ممیزان تقدیم می‌گردد کوشش گردیده است روش‌های ممیزی و امنیت در دنیای دیجیتال و راه‌های عملیاتی نمودن این گونه ارزیابی از اجرای عملیاتی دستورالعمل‌ها سنجیده شود. در کتاب ممیزان تلاش گردیده است بیش‌تر روش ممیزی ارائه شود تا دستورالعمل‌های بی‌روح ممیزی.

د کتاب کاربران تلاش گردیده است کاربرانی که به نوعی از رایانه‌ها و ابزار دیجیتال به صورت کاربردی در زندگی شخصی و اجتماعی و کاری بهره می‌برند، از زاویه دفاع سایبری با این ابزار آشنا شده و ضمن آشنایی با عرصه‌های امنیتی این ابزار بتوانند به‌ترین روش امنیت، پایداری و ایمنی این گونه وسائل را انتخاب و به کار بگیرند.

در کتاب متخصصان که با هدف آشنایی متخصصین و اهل فن با امنیت ابزار دیجیتال به رشته تحریر درآمده است تلاش گردیده است با عمق بخشی به مطالب زمینه استنباط علمی این گروه از عزیزان در حد بضاعت فراهم گردیده و نیازمندی‌های علمی و امنیتی آنان در کتاب مربوط به ایشان جمع آوری و ارائه گردد.

با توجه به این که مدیران، یکی از حساس‌ترین لایه‌های درگیر با استفاده از ابزار رایانه‌ای و دیجیتال و ارتباطی می‌باشند و منابع هر سازمان با گرایش مدیر مربوطه در این زمینه‌ها مصروف می‌گردد. در کتاب سوم که ویژه مدیران محترم در سطوح عملیاتی استراتژیک تنظیم گردیده است، مطالب سمت و سوی کاربردی مدیریتی پیدا نموده و مطالب مرتبط و مورد نیاز این قشر از جامعه جمع‌بندی و تقدیم گردیده است.

امید است این تحفه‌های ناقابل که قطعاً با نقادی صاحب‌نظران در اقصی نقاط کشور و مجامع علمی و دانشگاهی سیر رشد و تعالی خود را طی خواهد نمود زمینه‌های گسترش حرکت علمی در زمینه‌های پدافند غیر عامل فاوا را در کشور (ولو هر چنداندک) بتواند ایجاد نموده و از نظرات و پیشنهادات صاحب‌نظران علمی استقبال نموده و با تکمیل آن‌ها در کتب آتی بتوانیم در هرچه پربارتر نمودن این گونه کتاب‌ها کوشا باشیم.

کتاب حاضر در ۶ فصل تقدیم می‌گردد. در انتهای هر فصل اهداف هر فصل برشمرده شده و پس از بررسی مطالب فصل، در انتهای فصل سؤالاتی با انگیزه کمک به هر چه به‌تر یادگیری مطالب کتاب به صورت خود آموز طراحی گردیده تا خوانندگان محترم بتوانند با مرور بر پاسخ آن‌ها یک بار دیگر فصل را بررسی و به ماندگاری مطالب در ذهن کمک بیش‌تری داشته باشد.

در فصل اول مباحث مربوط به مقدمات و مبانی مورد نیاز برای ورود به بحث اصلی پرداخته شده و ضمن آشنایی با اطلاعات و اسناد و انواع تهدیدات و فرصت‌های کلی در امنیت دیجیتال با قاعده اصلی پدافند غیر عامل در حوزه فاوا که همان قابلیت اتکا به سازندگان این گونه ابزار است آشنا شده و با انواع آسیب‌های دیجیتال آشنا می‌شویم.

فصل دوم به آشنایی با پدافند غیر عامل در حوزه فاوا پرداخته و ضمن ارائه مفاهیم امنیت، ایمنی و پایداری در این حوزه با انواع سرمایه‌ها و تهدیدات از این منظر آشنا می‌گردیم.

در فصل سوم که اختصاص به اصول ممیزی و ارزیابی دارد به اهمیت روند ممیزی و ارزیابی پرداخته و انواع ممیزی داخلی و خارجی را بحث نموده و سپس به کلیات یک برنامه ممیزی می‌پردازد. در این فصل ضمنا مباحث مربوط به مدیریت کلان یک برنامه ممیزی و اهداف ممیزی نیز مطرح می‌گردد.

در فصل چهارم که اختصاص به ممیزی و ارزیابی امنیتی سیستم‌های فن‌آوری اطلاعات دارد در رابطه با شناخت مدیریت ریسک و مباحث مربوطه و همچنین دسته بندی عوامل تهدید مطالبی مطرح می‌گردد.

در فصل پنجم که اختصاص به روش‌ها و راه کارهای ارزابی دارد مسائلی مانند انواع روش‌های فنی ارزیابی شبکه‌ها و سیستم‌های کامپیوتری و دیواره‌های اتش و تشخیص نفوذ و آزمون کلمات عبور

پرداخته شده و انواع تکنیک‌های پویش فنی و تست سلامت شبکه نیز مورد بحث و بررسی قرار می‌گیرد.

در فصل ششم نمونه چک لیست‌های مورد نیاز برای ممیزی سیستم‌های فن آوری اطلاعات ارائه شده است که ممیزان قادر خواهند بود ضمن استفاده از آن‌ها ، از آن‌ها الگو گرفته و چک لیست‌های مورد نیاز خود را طراحی نمایند.

امیدواریم بهره‌گیری این کتب بتواند نقشی ولو اندک در حفظ امانات شهدای گران‌قدر انقلاب اسلامی که همانا اطلاعات و اسناد نظام جمهوری اسلامی می‌باشد داشته باشد و با توصیف واقعیت‌های موجود در امنیت و ایمنی و پایداری این ابزار توانسته باشیم دریچهٔ نگاه جدیدی را به روی کاربران گرامی باز کرده باشیم.

مؤلف

فهرست مطالب

فهرست چک لیست‌ها

فصل اول – تعاریف

آن چه در این فصل خواهید آموخت:

تعریف اطلاعات

تعریف اسناد

تعریف امنیت

تقسیم بندی سرمایه‌ها و مناطق قابل حفاظت

تعریف پدافند عامل

تعریف پدافند غیر عامل

تعریف تهدید نرم

تعریف مدیریت تهدید

امنیت در دنیای سنتی و نوین

۱-تعاریف

۱-۱- تعاریف

با توجه به این که امروزه مفاهیم معانی مختلفی پیدا کرده‌اند و برد استفاده از آن‌ها گسترگی فراوانی پیدا نموده است در این فصل ابتدا با تعاریف مورد نیاز برای ادامه کار آشنا شده و تعاریف عملیاتی و اختصاصی خاصی را که در ادامه کتاب به آن نیاز داریم بررسی می‌نماییم.

۱-۲- تعریف اطلاعات

با توجه به این که اطلاعات جمع اطلاع بوده و اطلاع به معنی آگاهی یافتن و واقف شدن بر کاری می‌باشد می‌توان اطلاعات را به هرگونه اقدام یا روشی که منجر به آگاه شدن از هر مطلب و مسئله‌ای می‌باشد تلقی نمود . هرگونه ابزار و یا حرکت یا نوشته و ایما و اشاره‌ای که منجر به آگاهی رسانی شود را می‌توان در حیطه اطلاعات تعریف نمود . با توجه به این که امروزه برای اطلاعات تقسیم بندی‌های مختلف انجام می‌دهند رایج‌ترین نوع اطلاعات را اطلاعات خام[۱] نامیده و شامل کلیه آگاهی رسانی‌های بدون ارزیابی شده و تمام انواع اطلاعات را در بر می‌گیرد.

با توجه به این که رایج‌ترین نوع اطلاعات را امروزه از اسناد استنتاج می‌نمایند ذیلا به صورت تفصیلی به این مطلب می‌پردازیم.

۱-۳-تعریف اسناد

---

۱ data

به موجب ماده ۱۲۸۴ قانون مدنی ایران سند عبارت است از «هر نوشته که در مقام اثبات دعوا یا دفاع قابل استناد باشد».

۱-۴- تعریف امنیت

در تعریفی عام امنیت عبارت است از مکانیزم‌های پیش‌گیری یا کاهش احتمال وقوع رخدادهای خطرناک و جلوگیری از تمرکز قدرت در هر نقطه از شبکه و احیای شبکه در حین وقوع رخدادهای ناخوشایند (وقتی که رخدادهای خطرناک حادث می‌شوند) هر عاملی که به‌طور بالقوه بتواند منجر به وقوع رخدادی خطرناک شود یک تهدید امنیتی به شمار می‌آید.

امروز برای امنیت تعاریف مختلفی ارایه شده است و برخی امنیت را در بعد فیزیکی آن مورد بررسی قرار داده و برخی در ابعاد روانی آن را مورد بررسی قرار داده‌اند. امروزه برخی امنیت را مترادف با کلمه حفاظت دانسته و از این زاویه به آن نگاه می‌کنند. واژه security در فرهنگ فارسی معادل واژه‌هایی همچون امن ، محفوظ، مطمئن، محفوظ داشتن ، تامین کردن آمده است. امنیت عمدتاً به نوعی احساس روانی اطلاق می‌گردد که به‌خاطر نداشتن‌ترس ، وضعیت آرامش و اطمینان خاطر حاصل می‌گردد. امنیت به حداقل رساندن خطر یا تهدید است که این خطرها نه فقط از نوع سنتی و نظامی هستند بلکه تهدیدات جدید غیر نظامی را نیز در بر می‌گیرند. فقدان تهدید ، عنصر اساسی تعریف امنیت است گرچه عده‌ای فقدان تهدید را امری ناممکن و دست نیافتنی دانسته و از این‌رو به حداقل رساندن تهدید را مفهوم اصلی امنیت می‌دانند. طبق نظر "ولفرز" « امنیت در معنای عینی فقدان تهدید در برابر ارزش‌های کسب شده را مشخص می‌کند و در معنای ذهنی ، فقدان‌ترس و وحشت از حمله علیه ارزش‌ها را. . . یک ملت زمانی امنیت دارد که بتواند بدون خطر از ارزش‌های اساسی خود حفاظت کند، از جنگ اجتناب نماید و بتواند در هنگام چالش ارزش‌های خود را با موفقیت حفظ نماید».

۱-۵- تقسیم بندی سرمایه‌ها و مناطق قابل حفاظت:

امروزه با توجه به اهمیت سرمایه‌ها و مناطق قابل حفاظت آن‌ها را به دسته بندی‌های مختلفی تقسیم می‌نمایند.

۱-۵-۱- عادی

تقریبا کلیه سرمایه‌ها و مراکز عام را که انسان‌ها با آن مراوده دارند در این گروه قرار می‌گیرد . گروه عادی گروهی است که انسان‌ها به صورت عادی تلاش خاصی برای حفظ و نگهداری آن انجام نمی‌دهند و صرفاً با مالکیت قانونی یا عرفی و شرعی آن را به تصرف درآورده و در تمام دنیا برای حفظ آن قوانین مدون و غیر مدونی وجود دارد و با احترام به این قوانین و رعایت آن عملاً حفاظت از این گروه از سرمایه‌ها ، مناطق انجام می‌پذیرد.

۱-۵-۲- مهم

مراکز مهم مراکزی هستند که در صورت انهدام یا بروز آسیب در کل یا قسمتی از آن‌ها، آسیب و صدمات محدودی در نظام سیاسی، اجتماعی و دفاعی با سطح تاثیر گذاری محلی و موضعی وارد می‌گردد.

۱-۵-۳- حساس

مراکز حساس مراکزی هستند که انهدام یا ایجاد اختلال در کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات جدی و مخاطره آمیز در نظام‌های سیاسی، هدایت، کنترل و مدیریت، تولیدی و اقتصادی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی، دفاعی با سطح تأثیرگذاری منطقه‌ای یا بخشی در کشور می‌گردد.

۱-۵-۴- حیاتی

مراکز حیاتی عبارتند از مراکزی که انهدام یا ایجاد اختلال در کل یا قسمتی از آن‌ها، موجب بروز بحران، آسیب و صدمات قابل توجه در نظام سیاسی، هدایت، کنترل و مدیریت، اقتصادی و تولیدی، پشتیبانی، ارتباطی و مواصلاتی، اجتماعی و دفاعی با سطح تاثیرگذاری فرابخشی یا در سراسر کشور می‌گردد.

۱-۶- تعریف پدافند عامل

پدافند عامل عبارت از رویارویی و مقابله مستقیم و به کارگیری جنگ افزارهای مناسب و موجود توسط نیروه‌های نظامی به منظور دفع حمله و خنثی کردن اقدامات آفندی و در واقع شامل عملیاتی در برگیرنده حمله ، مقابله و دفاع نظامی با ابزارها و سلاح‌های جنگی ، می‌باشد.

۱-۷- تعریف پدافند غیر عامل

پدافند غیرعامل مجموعه‌ای از اقدامات، طرح‌ها و تمهیداتی است که توان دفاعی سیستم را افزایش داده، پیامدهای حوادث و بحران‌ها را کاهش دهد و هم‌چنین امکان بازیابی سیستم‌های آسیب‌دیده را با حداقل هزینه‌ی ممکن فراهم سازد.

۱-۷-۱- امنیت

امنیت اطلاعات از سه جنبه مختلف مدنظر قرار می‌گیرد: محرمانگی۱، یکپارچگی۲ و دسترس‌پذیری۳.

محرمانگی به معنای اطمینان از این موضوع است که تنها افراد مجاز به اطلاعات دسترسی دارند.

یک‌پارچگی به معنای اطمینان از دقیق و کامل بودن اطلاعات و روش‌های پردازش آن است.

دسترس‌پذیری به معنای اطمینان از دسترسی افراد مجاز به اطلاعات در صورت لزوم است.

۱-۷-۲-ایمنی

ایمنی به مفهوم امن بودن در مقابل تهدیدات و حملات سخت و نیمه سخت می‌باشد. هر سیستمی به منظور تداوم بقا و توان ارائه تولیدات و خدمات باید ایمن باشد.

---

۱ Confidentiality

۲ Integrity

۳ Availability

۱-۷-۳- پایداری

هرچند امنیت و ایمنی سیستم‌ها از منظر پدافند غیر عامل بسیار مهم و ضروری است اما به مفهوم تامین سیستم دفاعی کامل نمی‌باشد . یکی از نکات مهم، وجود پایداری در تولید و ارائه خدمات در مراکز حیاتی، حساس و مهم است. پایداری به این معنی است که یک مرکز در شرایط عادی و یا در صورت بروز حمله و خدشه‌دار شدن هر دو یا یکی از دو جزء ذکر شده، یعنی امنیت و ایمنی، باید امکان تداوم ارائه تولیدات و خدمات خود را داشته باشد.

۱-۸- تعریف تهدید نرم

برای تعریف تهدید نرم تعاریف مختلفی ذکر شده است. تهدید نرم عبارت از «نوعی تلاش برنامه‌ریزی شده برای بهره‌گیری از ابزارها و روش‌های تبلیغی رسانه‌ای، سیاسی و روان شناختی برای تاثیر نهادن بر حکومت‌ها و مردم کشورهای خارجی به منظور تغییر نگرش‌ها، ارزش‌ها و رفتارهای آنان است. » (الیاسی ۴۶:۱۳۸۸) همچنین تهدیدهای نرم آن دسته از تهدیداتی است که اهداف متفاوتی را موضوع خود قرار داده و به جای تمامیت ارضی، هویت ، هنجار، فرهنگ و . . . را هدف قرار می‌دهند. (فصلنامه میثاق،گفتگوی علمی۱۳۸۶: ۱۴۵)

۱-۹- تعریف مدیریت تهدید

مدیریت تهدید یا جنگ نرم از چه منظری یا با چه نگاه تئوریکی به مقوله تهدید و جنگ نرم نگریسته شود، متفاوت خواهد بود؛ از این لحاظ اگر با منظر گفتمان سلبی، در حوزه نظریات به مقوله تهدید نگریسته شود، مدیریت خاص خودش را می‌طلبد. زیرا از بعد سلبی، امنیت عبارت است از عدم وجود تهدید ، در این گفتمان امنیت ماهیت برون‌گرایی و سخت‌افزاری دارد. مکاتب رئالیسم و نئورئالیسم چنین تعریفی را ارائه می‌دهند. اساسا واقع‌گرایان از منظر قدرت به امنیت می‌نگرند و امنیت را از مشتقات قدرت تلقی می‌کنند. آن‌ها ضمن آن که امنیت را واقعیتی «عینی» می‌دانند. تنها بر بعد «عینی» امنیت نیز تأکید دارند و آسیب‌های داخلی در این نگاه اساساً مورد عنایت نیست.

اگر گفتمان ایجابی مبنای نگرش به تهدید باشد، مدیریت تهدید بیش از این که نگاه برون‌گرایی داشته باشد، به داخل و سرمایه اجتماعی تکیه دارد. زیرا از این منظر، از بُعد ایجابی امنیت به معنای رضایت و تناسب بین داشته‌ها و خواسته‌ها است. (فصلنامه میثاق،افتخاری ۱۳۸۳) در این دیدگاه امنیت دارای بستر و مجموعه متکثری است که اگر شاخص‌های آن آماده باشد ،برای انسان نوعی آرامش و اطمینان به وجود می‌آورد در غیر این صورت ناامنی محل ظهور پیدا خواهد کرد. به عبارت دیگر، این رویکرد برای امنیت و تهدید، ماهیت تأسیسی قائل است و بر این باور است که تهدید، تنها در وضعیتی وجود دارد که آن جامعه در سطح قابل قبولی از اطمینان برای تحصیل و پاسداری از منافع ملی و ارزش‌های حیاتی‌اش نباشد. (همان، افتخاری، ۱۳۸۴، ص ۱۶) اگر این گفتمان را ملاک قرار دهیم قبل از ظهور "تهدید عینی" یا جنگ نرم، دوره تکوین و شکل گیری راه را برای طراحی و اجرای مدیریت‌های پیش‌گیرانه هموار می‌سازد. این تلقی که تحت "نظریه فضایی" در کتاب کالبد شکافی تهدید مطرح شده است، بدان معنی است که سیکل حیات تهدید در سه فضای اجتماعی، سیاسی و امنیتی معنا پیدا می‌کند و در هر فضایی الزامات و شرایط خاص خودش را دارد. در این میان حیات تهدید در فضای اجتماعی بسیار قابل توجه است. و مدیریت پیش‌گیری بیش‌تر در این مرحله معنا و مفهوم پیدا می‌کند. در این فضا تلقی این است که تهدیدات در یک شبکه روابط اجتماعی شکل می‌گیرند؛ در فضای سیاسی پدیده مورد نظر با قدرت رسمی به‌صورت ایجابی و سلبی ارتباط پیدا می‌کند. فضای امنیتی عبارت است از قلمروی از بحث که در آن پدیده مورد نظر به‌صورت ایجابی و سلبی با ثبات نظام ملی ارتباط برقرار می‌کند.

بر این مبنا، مدیریت پیش‌گیری مبتنی بر این نظریه است که تهدیدات قبل از ورود به مقطع ظهور عینی‌شان، حضور دارند. از این رو، پدیده‌ها قبل از آن که در فضای خارجی، هویتی عینی بیابند، دارای هویتی اجتماعی درون ساختار جامعه می‌باشند. (همان ، افتخاری، ۱۳۸۵: ۷)

۱-۱۰- امنیت در دنیای سنتی و نوین

تحولات جوامع بشری را می‌توان به اعتبار شیوه و متد مدیریتی حاکم بر آن، به چهار عصر تقسیم نمود که هر یک از آن‌ها برای ادامه حیات خود نیازمند به ابزار و لوازم خاص خود بودند و از این جهت هر یک از این تحولات شرایط و ویژگی‌های خود را دارا می‌باشند، این چهار عصر عبارتند از:

۱) عصر شکار

در این عصر که اولین مدل مدیریتی بشر می‌باشد، هدف همه ابنا بشر جمع آوری شکار بود. گروه‌های کوچک مردم که همواره در حال حرکت و مهاجرت و تحرک بودند همه مشغول تهیه مایحتاج زندگی و غذای خود بودند. در این عصر هر کس که کار می‌کرد سهم غذا داشت در غیر این صورت امکان ادامه حیات نداشت. سبک مدیریت در این عصر قدرت زور و چماق بود.

۲) عصر کشاورزی

در این عصر توانائی بشر به حدی رسیده بود که بتواند برای خود غذا تولید نماید تا افرادی که توانائی انجام کار را ندارند نیز از غذا بهره‌مند شوند. در عصر کشاورزی انسان یاد گرفت که می‌تواند در یک منطقه سکنی گزیند و نیازی به مهاجرت دائم از یک منطقه به منطقه دیگر ندارد.

۳) عصر صنعتی

در این عصر انسان و بشر با استفاده از ماشین آلات و ابزار تولید توانست افزایش فوق‌العاده‌ای را در تولیدات مصرفی و محصولات کشاورزی ایجاد نماید.

۴) عصر فراصنعتی (اطلاعات)

در این عصر اکثر افراد در خدمت تولید فرآورده‌ای به نام اطلاعات هستند و پیش‌بینی می‌شود که این روند روزبه‌روز نیز افزایش یابد و عده‌ی قلیلی در امر تولید محصولات کشاورزی و مواد غذایی باقی بمانند و در عوض عده‌ی بیش‌تری در امر تولید و پردازش اطلاعات قرار گیرند.

عنصر با ارزش این عصر اطلاعات است و فن‌آوری‌های اطلاعات و ارتباطات کشورها را به سوی جامعه اطلاعاتی سوق می‌دهد. ظهور شبکه‌ای رایانه‌ای جهانی به مدد فن‌آوری‌های پیشرفته مخابراتی دنیای جدیدی به وجود آورد که عده‌ای آنرا دنیای مجازی یا دیجیتال نامیدند. انقلاب دیجیتال و مجازی شدن همه چیز از کار و آموزش و مدیریت گرفته تا مناسبات اجتماعی و حتی جنگ از نشانه‌های شروع عصر جدیدی در جهان است.

توسعه شگفت انگیز تکنولوژی اطلاع رسانی در عصر انفجار اطلاعات نوید زمان بی‌نظیری را می‌دهد که همه ابعاد تمدن بشری از آن تاثیر پذیرفته است. در عصر اطلاعات و جامعه اطلاعات محور اقتصاد، سیاست، فرهنگ، هنر و اصولا تمامیت دانش بشری با ابزارها و شیوه‌های تبادل الکترونیکی اطلاعات پیوند دارد.

فشرده شدن کار در واحد زمان از مشخصه‌های بارز دنیای جدید است. رشد و توسعه تکنولوژی هر روز بر این فشردگی می‌افزاید. از طرفی فشردگی کار در واحد زمان موجب می‌شود که رشد تکنولوژی با نسبتی چند برابر ادامه یابد. حافظه‌های الکترونیکی و ابر رایانه‌های موجود بر فشردگی مزبور می‌افزایند و هر لحظه شرایط جدیدی را برای دستیابی سریع‌تر به نیازمندی‌های بشر فراهم می‌آورند.

۱-۱۰-۱- تهدیدات و فرصت‌ها در دنیای سنتی

در دنیای حقیقی انسان‌ها باید در گروه‌ها جمع شوند تا بتوانند تاثیر گذاری در گروه‌ها داشته باشند ولی در دنیای مجازی انسان‌ها به‌صورت انفرادی می‌توانند تاثیر گذار باشند.

در دنیای حقیقی سیاست جغرافیایی مفهوم دارد ولی در دنیای مجازی سیاست مبتنی بر جغرافیا نداریم و به‌جای آن سیاست مبتنی بر زمان و تندی داریم.

در دنیای حقیقی مرزهای فیزیکی وجود دارد ولی در دنیای مجازی مرزی وجود ندارد.

۱-۱۰-۲- تهدیدات و فرصت‌ها در دنیای نوین

در دنیای حقیقی ما حوزه‌های همپوشان منافغ نداریم (یا بسیار کم داریم) ولی در دنیای مجازی مرزهای همپوشان و حوزه‌های هم پوشان داریم .

در دنیای حقیقی با تضاد تضادها سروکار داریم – مانند امنیت و عدم امنیت – ولی در دنیای مجازی می‌توان تضادها را با هم جمع کرد .

در دنیای مجازی امنیت و ناامنی مطلق نداریم بلکه مخلوطی از آن را داریم .

در دنیای حقیقی حذف تهدیدات داریم ولی در دنیای مجازی حذف تهدیدات نداریم بلکه قابلیت همزیستی با تهدیدات داریم. یعنی قابلیت تهدید پذیری و تهدید زدایی افزایش پیدا می‌کند.

۱-۱۰-۲-۱- انواع تهدیدات:

تهدیدات انواع و اقسام مختلفی داشته و از زوایای مختلفی می‌توان آن‌ها را تقسیم بندی نمود . در این کتاب تلاش بر این شده است تا از زاویه منشا این تهدیدات تقسیم بندی صورت پذیرد.

۱-۱۰-۲-۱-۱- تهدیدات فنی

در عصر فن‌آوری اطلاعات یکی از مهم‌ترین و رایج‌ترین تهدیدات این نوع از تهدید می‌باشد. در بسیاری از مواقع خطراتی که جوامع را تهدید می‌کند به علت گستردگی ضریب نفوذ ابزار فنی ، این نوع از تهدید می‌باشد . در قرن اخیر به علت دست‌یابی انسان به ابزار پیش‌رفته فنی و نقش این ابزار در زندگی بشر استفاده از این ابزار جزوی از زندگی آدمی شده است و بدون آن‌ها در بسیاری از مواقع ادامه حیات بسیار سخت خواهد شد و به این خاطر گرایش به سمت استفاده هر چه بیش‌تر از این ابزار می‌باشد.

۱-۱۰-۲-۱-۱-۱- تهدیدات سخت‌افزاری

این گونه تهدیدات از جانب سخت‌افزارهایی است که استفاده می‌شود . به طور مثال استفاده از انواع ابزار نوین مانند رایانه‌ها و خودروها و هواپیماها و لوازم اداری و صنعتی که استفاده می‌شود در این تقسیم بندی قرار می‌گیرد. قبل از استفاده از ابزار صنعتی ، تهدیدات مربوطه نمی‌توانست یک کشور را از راه دور تهدید نماید لیکن در عصر حاضر کشورهایی که استراتژی خود را بر مبنای صنعت قرار داده‌اند به مجرد این که صنعت آنان به هر علتی با رکود مواجه شود باعث خواهد شد تا امنیت ملی آن کشور نیز به خطر افتد و به همین خاطر تلاش دارند تا به هر شکل ممکن این ابزار را از خطرات دور نگه دارند و دشمنان آنان نیز تلاش دارند از این ناحیه خطر را متوجه آن کشور نمایند.

۱-۱۰-۲-۱-۱-۲- تهدیدات نرم‌افزاری

تهدیدات نرم‌افزاری تهدیداتی را تشکیل می‌دهند که بیش‌تر مغز افزار می‌باشند تا سخت‌افزار . این گونه تهدیدات در مواقعی خطمشی‌ها و روش‌های زندگی و نوع نگرش و نوع رفتار و الگوی رفتاری و این گونه موارد را در بر می‌گیرد و در برخی موارد نرم‌افزارهای رایانه‌ای که وظیفه مدیریت بر سخت‌افزارهای به کار گرفته را بر عهده دارد در بر می‌گیرد. در صورت ایجاد تهدیدات بالقوه در نرم‌افزارهای رایانه‌ای و به مجرد بالفعل تبدیل شدن این تهدیدات، متخاصمین خواهند توانست از راه دور و در زمان مورد نیاز اشرافیت اطلاعاتی خود را بر کشور دیگری مسلط نموده و به نوعی فکر و فرهنگ و فیزیک آن کشور را به دست بگیرند.

۱-۱۰-۲-۱-۱-۳- تهدیدات سیستم‌های ارتباطی

با توجه به این که امروزه کلیه کشورهای دنیا از طریق سیستم‌های ارتباطی ملی و بین‌المللی به یک‌دیگر پیوند خورده و بدون این ارتباطات عملاً هیچ کشوری قادر به ادامه حیات نخواهد بود و کلیه تحرکات خود را در ابعاد مختلف سیاسی ، اقتصادی ، اجتماعی ، فنی ، ارتباطی و دیگر مسائل از این طریق با داخل و خارج خود پیوند می‌دهد ، در صورت دسترسی هر ساختاری به این ابزار ارتباطی عملاً اشرافیت بر اطلاعات تبادلی نیز صورت خواهد پذیرفت. اشرافیت بر ارتباطات به علت سهل‌الوصول بودن و استفاده از تکنولوژی‌های کنترل از راه دور معمولاً کم هزینه و پرفایده می‌باشد و بسیاری از سلطه گران به علت این که این ابزار تولید آن‌ها می‌باشد به راحتی امکان تسلط بر این ابزار را از راه دور داشته و بدون حضور فیزیکی امکان اشرافیت بر اطلاعات را برای خود مهیا می‌کنند.

۱-۱۰-۲-۱-۱-۴- تهدیدات الکترومغناطیسی

با پیشرفت علم و فن‌آوری در حوزه نیمه‌هادی‌های الکترونیکی ، استفاده از تجهیزات رایانه‌ای ، مخابراتی و الکترونیکی کاربردهای فراوانی پیدا کرده است . امروزه تمام ابزار اداری ، صنعتی و نظامی از تجهیزات الکترونیکی استفاده می‌کنند و این مسئله آن‌ها را در مقابل لطمات الکترومغناطیسی آسیب‌پذیر نموده است.

مدارات بردهای الکترونیکی که از ابتدا لامپی بوده‌اند و با ولتاژهای بالایی کار می‌کردند با پیدایش‌ترانزیستور تبدیل به قطعات بسیار کوچک‌تری شدند که با ولتاژهای پایین‌تری کار می‌کنند . با کاهش حجم و مصرف انرژی ، استفاده از نیمه‌هادی‌های الکترونیکی رواج بیش‌تری پیدا کردند.

با توجه به این که ادامه حیات سرمایه‌های زندگی انسان‌ها که همان ابزار کاربردی می‌باشند به قطعات و سیستم‌های الکترونیکی، رایانه‌ای و مخابراتی وابسته است به همین دلیل یکی از جدّی‌ترین مخاطرات موجود تهدیدات الکترومغناطیسی می‌باشد. که هم به صورت طبیعی و هم ساخت دست بشر وجود دارد. از این تهدیدات می‌توان به رعد و برق ، سویچینگ خطوط انتقال برق، دستگاه جوش ژنراتور الکتریکی ، تسلیحات الکترومغناطیسی و انفجارات اتمی اشاره نمود.

۱-۱۰-۲-۱-۲- تهدیدات مصنوعی (انسان ساخت):

تهدیدات عمدی (که بیش‌ترین خسارت و دشوارترین راه مقابله را دارند) عبارت است از « هر گونه اقدام برنامه‌ریزی شده جهت افشا، نابودی یا تغییر در داده‌های حیاتی شبکه یا ایجاد اختلال در خدمات معمول سرویس دهنده‌ها». به‌طور عامّ هرگونه اقدام برنامه‌ریزی شده برای تحقق یک « رخداد خطرناک » ، یک « تهدید امنیتی عمدی » تلقّی می‌شود.

۱-۱۰-۲-۱-۲-۱- تهدیدات برنامه ریزی شده

سازندگان سخت‌افزار و نرم‌افزار بنا بر سیاست‌های استراتژیک خود در زمان تولید این ابزار با اهداف مختلفی امکاناتی را بر روی آن‌ها تعبیه می‌نمایند تا در زمان مورد نیاز بتوانند به صورت آشکار و پنهان از راه دور و نزدیک به این ابزار دسترسی داشته و مدیریت آن‌ها را به دست بگیرند. ساده انگارانه‌ترین این اقدام برای تعمیر این ابزار از راه دور می‌باشد و بدبینانه‌ترین آن اشرافیت پنهانی بر اطلاعاتی که توسط این ابزار در مبدا به کارگیری تولید می‌شود و همچنین مدیریت استراتژیک این ابزار در زمان جنگ می‌باشد.

در کشورهای مختلف همچون امریکا برای این کار تدابیر قانونی نیز اندیشیده شده است تا تولید کنندگان بدون رعایت این مطلب این ابزار را به دیگر کشورها صادر ننمایند.

۱-۱۰-۲-۱-۲-۲- تهدیدات با منشا خطای انسانی

تهدیدات غیر عمد از اشتباهات سهوی و نا خودآگاه عوامل انسانی (همانند مدیران شبکه، کارکنان و کاربران) ناشی می‌شود و می‌تواند منجر به افشا یا نابودی اطلاعات یا اختلال در خدمات معمول شبکه و گاه تحمیل خسارت‌های کلان به جمیع کاربران شود. از این تهدیدات غیر عمد، می‌توان به موارد ذیل اشاره کرد:

طراحی نا صحیح زیر ساخت شبکه یا عدم وجود افزونگی در تجهیزات شبکه

عدم تهیه‌ی نسخه‌های پشتیبان از داده‌های حیاتی

سهل‌انگاری در وظایف روزمره (مثل بررسی مستمر سیستم‌ها از لحاظ آلودگی به ویروس)

نا آگاهی کاربران از ماهیت عملیات خطرناک

بروز اشکالات پیش بینی نشده[۱] در سطح سخت‌افزار، نرم‌افزار یا سیستم عامل

عدم اعمال صحیح سیاست‌های انتخاب و تعویض مداوم کلمات عبور توسط عوامل درگیر در شبکه

۱-۱۰-۲-۱-۳- تهدیدات طبیعی

این تهدیدها از عواملی مانند زلزله، سیل، گردباد، رعد و برق، آتش سوزی، آتشفشان و نظایر آن از قوّه به فعل می‌رسند و نسل بشر چنین تهدیدهایی را به عنوان حقایق زندگی پذیرفته است. این تهدیدها همان گونه که زندگی را هدف گرفته‌اند می‌توانند در درجات خفیف‌تر منجر به نابود شدن یا افشای اطلاعات محرمانه و اختلال در سرویس‌های مؤلفه‌های اساسی شبکه شوند. از آنجا که خدمات شبکه‌های رایانه‌ای مرزهای جغرافیایی را در نوردیده است لذا تهدیدهای طبیعی می‌توانند در خارج از محدودهٔ بَلا دیده نیز منجر به اختلال در عملیات روزمرهٔ افراد و انتشار بحران در سطح وسیع شوند. لذا اگرچه تهدیدهای طبیعی خارج از قدرت بشرند ولی برای بازگرداندن خدمات شبکه از وضعیت بحران به

---

۱ BUG

وضعیت عادی، از همان ابتدای طراحی شبکه، تمهیداتی برای جلوگیری از گسترش دامنهٔ بحران به مناطق دیگر پیش بینی و اجرا می‌شود. به عنوان مثال ایجادتراز پشتیبان در دیگر مناطق جغرافیایی و بهره‌گیری از خطوط ماهواره‌ای در کنار خطوط فیبر نوری در این رده از تمهیدات قرار می‌گیرد.

۱-۱۰-۳- شناخت اطلاعات دیجیتال

اسناد دیجیتال(رایانه‌ای): شامل داده‌های رایانه‌ای ، دیسکت‌های رایانه‌ای ، سی دی‌های رایانه‌ای ، امواج مخابراتی . یعنی تمام اطلاعات رایانه‌ای از هر نوع که باشد به‌عنوان "اسناد دیجیتال" تلقی می‌شود. آن چه که در این جا مهم می‌باشد آن است که بدانیم اطلاعات دیجیتال به مجرد تولید شدن ، قابل از بین بردن نمی‌باشند و در صورت امحا می‌توان آن‌ها را به روش‌های مختلفی بازیابی کرد یا نمی‌توان با استفاده از رمزگذاری این اطمینان را حاصل نمود که کسی به اطلاعات ما دستبرد نزند. رابطه رشد علم و فن‌آوری تولید سند با امنیت سند رابطه‌ای معکوس است. یعنی هر چه علم و فن‌آوری پیش‌رفته‌تر می‌شود امنیت آن به همان میزان پائین‌تر می‌آید. پس امروز باید نگاهمان را به امنیت اسناد تغییر دهیم و ضمن شناخت ابزار تولید سند(سخت‌افزار ، نرم‌افزار ، شبکه‌های مربوطه ،) دیدگاهِمان را نسبت به مقوله امنیت اسناد عوض کنیم.

۱-۱۰-۳-۱- انواع اطلاعات دیجیتال

اطلاعات دیجیتال در ابزار ذخیره ساز انواع و اقسام مختلفی دارند و بر مبنای آن مورد استفاده‌های خاصی قرار می‌گیرند.

۱-۱۰-۳-۱-۱- اطلاعات ذخیره شده

این گونه اطلاعات کلیه اطلاعاتی است که در ابزار ذخیره ساز به شکل‌های مختلف ذخیره شده و حفظ و نگهداری می‌شود و در صورتی که فردی به صورت مجاز و یا غیر مجاز به این ابزار دسترسی پیدا نماید می‌تواند به این اطلاعات دسترسی پیدا کرده و آن‌ها را در اختیار بگیرد. به‌طور مثال در صورت مفقود شدن و یا به سرقت رفتن ابزار ذخیره‌سازی کلیه اطلاعاتی که در آن زمان بر روی این ابزار وجود دارد از

نوع اطلاعات ذخیره شده می‌باشد و افراد بدون این که تلاش خاصی داشته باشند می‌توانند به این اطلاعات دسترسی و آن‌ها را مورد استفاده قرار بدهند.

۱-۱۰-۳-۱-۲- اطلاعات پشتیبان

به منظور اطمینان از این که همیشه اطلاعات تولید شده قابل استفاده می‌باشد در زمان‌های مختلف از اطلاعات پشتیبان تهیه شده و در صورتی خرابی اطلاعات موجود می‌توان از این اطلاعات بهره‌برداری نمود اطلاعات پشتیبان در ابزار ذخیره‌سازی جانبی کپی برداری شده و در محل‌های امن نگهداری می‌گردد درصورتی‌که فردی به صورت مجاز و یا غیر مجاز به این ابزار دسترسی پیدا نماید می‌تواند اطلاعات آن را مورد بهره‌برداری قرار بدهد.

۱-۱۰-۳-۱-۳- اطلاعات در حال عبور

اطلاعات در حال عبور همان اطلاعات تعاملی می‌باشند . در شبکه موجودیت‌ها در فاصله‌های دور از هم قرار دارند برای این که کلیه کاربران بتوانند از اطلاعات شبکه استفاده نمایند می‌بایست از طریق امکانات مخابراتی به یک‌دیگر وصل گردند اطلاعاتی که در بستر شبکه‌های مخابراتی در حال حرکت می‌باشند از موجودیتی به موجودیت دیگر منتقل می‌شوند و اطلاعات در درون سیستم‌های ارتباطی در حال حرکت می‌باشد چنان چه فرد غیر مجازی در مسیر عبور داده‌های اطلاعاتی که از طریق یک سیستم مخابراتی و در یک بستر شبکه‌ایی در حال تبادل و عبور هستند قرار گیرد؛ خواهد توانست از اطلاعات در حال عبور بهره‌برداری نماید .

۱-۱۰-۳-۲- سابقه امنیت دیجیتال

سابقه امنیت دیجیتال به قدمت دسترسی انسان‌ها به ابزار دیجیتال می‌باشد. از همان روزی که انسان‌ها توان این را پیدا کردند تا در عصر حاضر از ابزار دیجیتال در زندگی خود استفاده نمایند اولین مطلبی که ذهن آن‌ها را مشغول نمود مسئله امنیت اطلاعات دیجیتال می‌باشد. بدون امنیت دیجیتال عملاً اطلاعات تولید شده توسط دشمنان به راحتی قابل دسترسی می‌باشد.

۱-۱۰-۳-۲-۱- اصول امنیت دیجیتال:

در امنیت دیجیتال اصول مختلفی حاکم می‌باشد و با توجه به رعایت این اصول افراد تلاش می‌کنند تا امنیت اطلاعات خود را تأمین نمایند. بدون رعایت این اصول عملاً تأمین امنیت قابل اتکا نخواهد بود. امنیت دیجیتال مانند زنجیره‌ای به هم پیوسته می‌باشد و در صورت عدم رعایت امنیت در یکی از زنجیره‌ها عملاً امنیت در کل آن مخدوش خواهد شد .

۱-۱۰-۳-۲-۱-۱- اصل کلی- قابلیت اعتماد و اتکاپذیری

این اصل به مفهوم آن می‌باشد که قبل از این که هر ابزار دیجیتالی را مورد استفاده قرار داد ابتدا باید بررسی نمود تولیدکنندگان این ابزار با چه هدف و با چه نیتی این ابزار را تولید و در اختیار دیگران قرار داده‌اند. آیا در چرخه دسترسی به اطلاعات دیگران از مبدا تولید و با هدف دسترسی به این اطلاعات این ابزار تولید شده است. آیا این ابزار توسط دوست و یا دشمن تهیه شده است . آیا تولیدکننده این ابزار برای صدور آن به دیگر کشورها دارای دستورالعمل یا آیین‌نامه خاصی می‌باشد یا خیر. به‌طور مثال یکی از قوانین آمریکا برای صدور سخت‌افزار و نرم‌افزار به دیگر کشورها وجود نقاط آسیب‌پذیر در آن که به تایید اف‌بی‌آی رسیده باشد می‌باشد و فقط در صورت تأیید این ابزار قابلیت صدور به دیگر کشورها را پیدا می‌کند. در این گواهی اف‌بی‌آی تأیید می‌نماید که ابزار لازم برای دسترسی از راه دور و به دست گرفتن مدیریت ابزار از راه دور دراین سخت‌افزار و نرم‌افزار تأمین شده و به راحتی از راه دور می‌توان آن را به دست گرفت و بر مبنای نیاز تغییراتی در آن در زمان جنگ ایجاد نمود .

۱-۱۰-۳-۲-۱-۲- اصول فرعی (مبانی نقد پذیر ISMS):

علاوه بر اصل ذکر شده که با عنوان پایه اصلی امنیت اطلاعات می‌باشد و در تامین امنیت اطلاعات دارای نقش اساسی می‌باشد و بدون در نظر گرفتن اصل کلی و صرفاً رعایت اصول فرعی امنیت اطلاعات در درون سیستم تأمین شده و از خارج از سیستم به راحتی امکان اشرافیت بر اطلاعات به شکل آشکار و پنهان قابل تامین می‌باشد این مسئله باعث خواهد شد در زمان جنگ و صلح به راحتی تولیدکنندگان ابزار سخت‌افزاری و نویسندگان نرم‌افزاری به صورت آشکار و پنهان عملاً قادر به دست گرفتن مدیریت از راه دور اطلاعات باشند.

۱-۱۰-۳-۲-۱-۲-۱- محرمانگی

به مجموعه مکانیزم‌هایی که تضمین می‌کند داده‌ها و اطلاعات مهم کاربران از دسترس افراد بیگانه و غیر مجاز دور نگاه داشته شود، «سرویس محرمانگی»اطلاق می‌شود. این سرویس‌ها عموماً با روش‌های رمزنگاری تحقق می‌یابند . روش‌های مختلف رمزنگاری اطلاعات، زیربنای مابقی سرویس‌های امنیتی است.

۱-۱۰-۳-۲-۱-۲-۲- در دسترس بودن

مکانیزم‌هایی که دسترسی به کوچک‌ترین منابع اشتراکی شبکه را تحت کنترل درآورده و هر منبع را بر اساس سطح مجوز کاربران و پروسه‌ها در اختیار آن‌ها قرار می‌دهد، «کنترل دسترسی» خوانده می‌شود.

۱-۱۰-۳-۲-۱-۲-۳- صحت و یکپارچگی اطلاعات

مجموعۀ مکانیزم‌هایی که از هرگونه تحریف، دستکاری، تکرار[۱] ، حذف یا آلوده سازی داده‌ها پیش‌گیری می‌کنند یا حداقل باعث کشف چنین اقداماتی می‌شوند، «سرویس تضمین صحت اطلاعات» نامیده می‌شود.

۱-۱۱- رابطه بین رشد علم و فن‌آوری و امنیت

در دنیای فیزیکی رابطه بین رشد علم و فن‌آوری و تأمین امنیت رابطه‌ای مستقیم می‌باشد یعنی هرچه علم و فن‌آوری پیش‌رفته‌تر می‌شود امنیت به‌تر قابل تمدید خواهد بود. اما این مسئله در دنیای نوین کاملاً بالعکس می‌باشد یعنی هر چه حد علم و فن‌آوری پیش‌رفته می‌کند امنیت به همان میزان کاهش پیدا می‌کند دلیل آن ابداع روش‌های دسترسی پنهان در ابزار دیجیتال می‌باشد. هر وسیله‌ای دیجیتال که ساخته می‌شود همراه با خود ناامنی‌های جدیدی به همراه دارد. با قرار گرفتن این ابزار در کنار ابزار دیگر ناتوانی‌های جدید به شکل تصاعدی بیش‌تر شده و زمینه را برای دسترسی غیرمجاز عناصر بیگانه فراهم می‌آورند.

۱-۱۲- تحقیقات اجمالی انجام شده در رابطه با کلیات امنیت در دنیای دیجیتال

---

۱ Reply

در جهان سنتی و فیزیکی اندیشمندان امنیتی همیشه بر این باور بودند که با افزایش علم و فن‌آوری امنیت نیز حداقل به همان میزان افزایش پیدا می‌کند . اگر به دنبال حفظ و حراست از کالای گران قیمیت بودند ، در تلاش برای استفاده از فن‌آوری‌های نوین برای حفظ آن بودند . دیوارها را بلندتر می‌ساختند تا هر چه می‌توانند فاصله بین نا امن گرایان را با متاع گران قیمت خود بیش‌تر سازند . اگر طلای خود را می‌خواستند هر چه بیش‌تر از دست سارقان دورتر نگهدارند از ابزار نوین آنالوگ مانند انواع دزدگیر و . . . استفاده می‌نمودند. و همیشه این‌اندیشه در ذهن آنان غالب بود که با افزایش علم و فن‌آوری و ابداعات در دنیای فیزیکی امنیت را می‌توان بالاتر برد.

اما در سال ۲۰۰۰ میلادی نتیجه پژوهشی که توسط دانشگاه برکلی[۱] (berkley. com) امریکا منتشر شد این نظریه را کاملا منسوخ ساخت.

این تحقیق که به مدت بیست و پنج سال از سال ۱۹۷۵ الی ۲۰۰۰ میلادی انجام شد نشان می‌داد که هر چقدر که از سال ۱۹۷۵ به سمت جلوتر حرکت می‌کنیم علم و فن‌آوری و نوآوری و میزان دسترسی انسان‌ها به ابداعات و ابتکارات جدید و کشفیات بیش‌تر می‌شود . اگر در سال ۱۹۷۵ برای دسترسی غیر مجاز به اطلاعات دیجیتال می‌بایست چندین مهندس کار کشته و باتجربه باید در کنار هم و با کار گروهی تلاش می‌کردند تا بتوانند به یک دسترسی کوچک به این اطلاعات دسترسی پیدا نمایند ، این کار در سال ۲۰۰۰ بسیار راحت‌تر شده بود و یک نوجوان ۱۷ ساله ، بدون تحصیلات دانشگاهی و به تنهایی می‌توانست یک دسترسی نسبتاً بزرگی به صورت غیر مجاز به اطلاعات مهم داشته باشد.

نتیجه بیست سال از تحقیقات بیست و پنج ساله منتشر شده است ابتدا دسترسی غیر مجاز مشکل‌تر بوده است اما هر چه جلوتر می‌رویم این کار راحت‌تر می‌شود .

دانشگاه برکلی آمریکا به دو علت عمده به این نتیجه رسیده است:

دسترسی ارزان‌تر و آسانتر به ابزار دسترسی غیر مجاز به اطلاعات دیجیتال

---

۱ berkley

همان گونه که ملاحظه می‌نمایید هر چه به سمت سال ۲۰۰۰ حرکت می‌کنیم در طی سالیان مختلف ابزار نفوذ غیر مجاز بیش‌تری نوشته شده و به صورت ارزان و همه گیر از طریق اینترنت در اختیار همگان قرار گرفته است و هر کس می‌تواند با دسترسی به اینترنت و سی دی‌های ارزان قیمت که در همه جای دنیا قابل تهیه است به این ابزار دسترسی پیدا نموده و با استفاده از آن‌ها شانس خود را برای دسترسی غیر مجاز به اطلاعات به آزمون بگذارد.

افزایش فراوانی آسیب‌پذیری با افزایش تولید ابزار نوین جدید

هرچقدر ابزار جدید تولید می‌شود همراه با خود آسیب‌پذیری‌های جدید را به ارمغان می‌آورد . اگر زمانی که فقط پول کاغذی وجود داشت یک دغدغه خاطر وجود داشت و آن حفظ پول از دست سارقان بوده است ، اما به مجرد دسترسی به پول الکترونیکی باید این پول در مکان‌های مختلف که سارقان به شکل‌های مختلف به آن دسترس داشتند مورد حفاظت قرار گیرد تا با هک[۱] شدن رمز ورود و کارت بانکی و شبکه بانکی و شبکه مخابراتی و . . . . به دست دیگران نیفتد.

۱-۱۳- آسیب‌های امنیتی (سلطه اطلاعاتی):

در دنیا تمام سلطه‌گران به دنبال اهدافی هستند . آن‌ها با توجه به این اهداف به دنبال گسترش ابزار خود در تمام دنیا بود و با استراتژی از قبل تعیین شده نسبت به تولید و توسعه این ابزاراقدام می‌نمایند.

۱-۱۳-۱- اشرافیت بر ارتباطات

یکی از اهداف سلطه گران اشرافیت در ابزار ارتباطی به کل ارتباطات در دنیا می‌باشد. امروز سیستم‌های مخابراتی ملی به بین‌المللی وظیفه ارتباط بین کلیه آحاد مختلف در دنیا را به عهده دارند . اگر چنان‌چه ساختاری بتواند به این ابزار دسترسی پیدا کند عملاً قادر خواهد بود در مسیر چرخش اطلاعات بین

---

۱ Hack

کلیه ابزار دیجیتالی که توسط کاربران مورد استفاده قرار می‌گیرد قرار بگیرد و بر آن اشرافیت داشته باشد.

۱-۱۳-۲- اشرافیت بر اطلاعات

هدف اصلی سلطه‌گران اشرافیت بر اطلاعات می‌باشدکلیه اقداماتی که به منظور اشرافیت بر ارتباطات انجام می‌دهند با هدف اشرافیت بر اطلاعات بوده و تمام سرمایه‌گذاری‌ها برای تولید ابزار اطلاعاتی و ارتباطی از ابتدا با استراتژی اشرافیت بر اطلاعات تولید شده در مبدأ توسط کاربران بوده و این یک نوع سرمایه‌گذاری اقتصادی محسوب می‌شود.

۱-۱۴- آسیب‌های دنیای دیجیتال:

از بین رفتن کیان و کارکرد خانواده

در جوامع سنتی، خانواده نهادی اجتماعی با مرکزیت و محوریت مشخص است و هویت افراد، با توجه به خانواده‌هایشان شناخته می‌شود. اعضای خانواده سنتی را پدر و مادر، فرزندان، پدر بزرگ‌ها و مادر بزرگ‌ها تشکیل می‌دهند و جایگاه و احترام هر کدام مشخص و حفظ می‌شود.

سرپرست خانواده، رفتار و منش اعضای خود را کنترل می‌کند و اگر زمانی فرزندان با ازدواج یا ادامه تحصیل، از خانواده جدا بشوند، باز هم از کنترل و نظارت خارج نیستند و در مواقع لزوم نیز خانواده به یاری آنان همت می‌گمارد.

دین، باورها و آداب و رسوم مذهبی، در خانواده‌های سنتی جایگاه ویژه‌ای دارد و ارتباط مستقیمی میان دین و سلامت اخلاقی و رفتاری افراد خانواده وجود دارد. از این رو، در خانواده‌های سنتی ناهنجاری‌های کم‌تری دیده می‌شود. معمولاً سرلوحه همه رفتارهای خانواده سنتی، محبت و فداکاری و از ویژگی‌های آشکار این خانواده‌ها، رسیدن اعضای آن به احساس آرامش و سلامت روانی است. در مقابل، تاثیری که تمدن، تکنولوژی، ماهواره و اینترنت بر خانواده‌های به اصطلاح مدرن امروزی گذاشته، آن‌ها را با نوعی کاستی و سردی در روابط و مناسبات روبه رو کرده است. در نتیجه، دوام و پایداری آن‌ها دست خوش تهدیدهای جدی قرار گرفته است.

آسیب‌های خانواده، به دو دسته بیرونی و درونی تقسیم می‌شوند. نادیده گرفتن مسائل اخلاقی و حقوقی و رعایت نکردن امور مربوط به روابط انسان‌ها، از آسیب‌های درونی هستند که متوجه اعضای خانواده می‌شود.

عوامل آسیب‌زای بیرونی را نیز باید در خارج از محیط خانواده یافت. در عصر حاضر با ورود وسایل ارتباط جمعی مانند روزنامه، کتاب، رادیو، تلویزیون، ماهواره و شبکه‌های اینترنتی، نوع زندگی خانوادگی تغییر کرده و پی‌آمدهای گوناگون و دشواری را به همراه داشته است. مدرن و به روز بودن، اصل هویت خانواده را با درگیری‌های جدی روبه‌رو ساخته است و تکنولوژی‌ها و اختراعات مختلف که برای رفاه بخشیدن به زندگی جوامع امروزی پدید آمده‌اند، خانواده را دچار سردرگمی کرده و مصرف گرایی راترویج کرده‌اند. فعالیت‌های بیش از حد والدین نیز آسیب‌های عاطفی بسیاری را متوجه فرزندان کرده و خانواده را در به انجام رساندن مسئولیت‌هایش با مشکل روبه رو ساخته است.

ناهماهنگی و نبود تعادل در خانواده، شادابی و پویایی را نیز از جامعه می‌گیرد و بی‌توجهی به بهداشت روانی خانواده، از مشکلات مهم زندگی‌های امروزی است. پژوهشگران، بالا رفتن آمار افسردگی در مردم را از پی‌آمدهای نوع زندگی قرن بیستم می‌دانند؛ که در آن، خانواده‌ها از هم گسسته‌اند و بیشتر مردم در کنار خانواده و باترتیب درست و اصولی آنان رشد نمی‌کنند. در این شرایط، والدین وقت کافی برای همراهی موثر فرزندان خود ندارند و در نتیجه، استرس‌های گوناگون، افراد را در معرض افسردگی و بیماری‌های روانی قرار می‌دهد.

افزایش زمینه‌های تحریک جنسی نیز در پی گسترش و تنوع وسایل جدید تکنولوژی، خانواده‌ها را با گرفتاری‌های نگران کننده‌ای روبه‌رو کرده است. دنیای مدرن، عصر تنوع و هیجان و نوآوری است. تعدد مشاغل مردان و فشار بیش از حد ناشی از فعالیت زنان خانه و مشاغل رسمی آنان در جامعه، همراه با افزایش استرس‌ها و ضعف مهارت زوجین در برقراری ارتباط سالم جنسی نیز کارکردتربیت جنسی خانواده را ضعیف می‌کند.

امروزه مسئولیت خانواده‌ها درتربیت فرزندان بیش از گذشته است و پرورش فرزندانی که ثبات شخصیت و هویت اجتماعی داشته باشند، دشوارتر شده است. فرزندان نیز با وظایف سنگین حاضر و بحران‌های

پیش آمده، بسیار ضعیف و شکننده عمل می‌کنند و فرزند سالاری، در بسیاری از خانواده‌ها، اقتدار و نظارت والدین را بر هم زده است. بر این اساس، هر کدام از کارکردهای خانواده، نقش مهمی در استحکام و تقویت بنیان خانواده ایفا می‌کند. با این حال، مسئله ناخوشایند این است که در بسیاری از خانواده‌های مدرن، وظایف خانواده، به درستی انجام نمی‌شود.

از آفت‌هایی که خانواده امروزی را تهدید می‌کند، بی اعتباری تدریجی هنجارها، اخلاق، باورهای دینی و ارزش‌های مذهبی و سنتی و در کنار آن، گسترش انواع انحراف‌ها و رفتارهای ناپسند در جامعه است.

کم توجهی به ارزش‌ها در جوامع مدرن که با کنار گذاشتن خدا، دین و اخلاق همراه است، به انسان امروزی، جرات دست زدن به هر کاری را می‌دهد. اخلاق مدرن، ریشه خود را در عقل گرایی جست‌وجو می‌کند و به همین سبب، با اخلاق سنتی و دینی فاصله گرفته است. آسیب‌پذیری خانواده امروزی، ناشی از نادیده گرفتن بایدها و نبایدهای دینی و اخلاقی است. بشر امروزی، هنوز به این نتیجه نرسیده است که زندگی بدون ایمان و معنویت، رنج و عذاب روانی و همیشگی را همراه او خواهد کرد.

از بین رفتن حریم‌های خصوصی

در دنیای سنتی، ارتباطات هم سنتی بود، که شامل ارتباطات انسانی، شفاهی، چهره به چهره و بی واسطه فردی و گروهی بود که به رغم ظاهر ساده و ابتدایی می‌تواند کارکردی پیچیده و متنوعی داشته باشد. این نوع ارتباطات گرچه به دلیل گسترده و پیچیده شدن جوامع انسانی کارکرد گذشته خود را از دست داد. اما هنوز هم از نفوذ و اعتبار خاصی برخوردارند زیرا بر طبیعت انسانی و نیازهای عاطفی او نزدیک‌ترند. در فرهنگ اسلامی ایرانی ما در دنیای سنتی مراسماتی چون نقالی، شاهنامه خوانی، حضور در میادین روستا و شهرها و ... حاکم بوده است که کارکردهای مثبت فراوانی داشته که در گستره زمان جای خود را به رادیو، تلویزیون و امروز به اینترنت و ماهواره داده است و دیگر از آن کارهای مثبت و سازنده خبری نیست و بر عکس آثار زیان بار و مخربی همچون نفوذ به حریم خصوصی افراد سوغات فن‌آوری جدید بشر یعنی اینترنت می‌باشد.

اینترنت به عرصه تبدیل و انتقال آزاد و افکار گردیده و حد کنار سرعت دادن به ارتباطات بشری خود معضلی جدی گردید.

اینترنت به عرصه فعالیت متصدیان جمع آوری اطلاعات در سراسر جهان تبدیل شده است. عملیات نفوذ به سیستم با نرخی هشدار دهنده افزایش یافته است، زیرا اینترنت به محلی کاملاً راحت و جالب برای هکرها تبدیل شده است. اینترنت را با رعایت مسایل حفاظتی طراحی نکرده‌اند. اینترنت شبکه‌ای عظیم و ظریف بوده و حاوی بسیاری کاستی‌های نرم‌افزاری است. به راحتی می‌توان در شبکه بدون ذکر نام خویش فعالیت کرد. چون همه چیز به هم مرتبط است، هر چیزی قابل نفوذ بوده و متجاوزی حرفه‌ای می‌تواند با ایجاد ردپایی در میان ده‌ها سیستم در چندین کشور مختلف ردپای خود را گم کند. بسیاری از ابزار مورد استفاده هکرها که در سال‌های قبل نیاز به دانشی عمیق داشت، اکنون خودکار شده و به راحتی قابل استفاده می‌باشد.

شکسته شدن حریم خصوصی افراد از هر قشر و رده‌ای، باعث ناامنی روانی و اجتماعی می‌شود و می‌تواند پیامدهای جبران ناپذیری به همراه داشته باشد.

همزمان افراد تلاش وافری در حفظ اطلاعات شخصی خود به هر شکل ممکن می‌کنند و این تلاش همیشگی دو طرفه برای کشف و حفظ اسرار شخصی افراد موجب ایجاد چالشی جدی در جوامع بشری است.

در این میان میثاق‌ها، بیانیه‌ها و قطعنامه‌های متعددی که منتشر می‌شود دست و پا زدن‌های انسان عصر مدرن را می‌ماند که سعی می‌کند خفگی‌اش را اندکی به تاخیر بیندازد.

۱-۳) دنیای دیجیتال

بر اساس تحقیقات انجام شده ۵۱٪ از نفوذ وتخریب سیستم‌های دیجیتال توسط ویروس‌ها و۲۷ ٪ توسط کارکنان ناراضی ، ۱۵٪ خرابکاری از بیرون ، ۷٪ توسط جاسوسان صنعتی انجام می‌شود .

الف: ویروس‌ها و سایر امراض نرم‌افزاری

ویروس قطعه‌ای کوچک از کد رایانه‌ای است که درون برنامه رایانه‌ای دیگری پنهان می‌شود . مثل ویروس واقعی ، ویروس رایانه‌ای می‌تواند خود را تکثیر کرده و سایر رایانه‌ها را بیمار کند و سپس بدون

حرکت طی ماه‌ها یا سال‌ها باقی مانده و دوباره حمله کند . ویروس تنها یکی از چندین نوع رشته منطقی است که می‌تواند رایانه‌یا کل شبکه را صدمه بزند .

کرم‌ها ، بمب‌های منطقی ، و اسب‌های تروا امراضی مشابه هستند که معمولاً با ویروس‌های رایانه‌ای گروه بندی می‌شوند . کرم رایانه‌ای مثل ویروس پراکنده می‌شود اما به جای آن که درون برنامه دیگری پنهان شود ، خود برنامه‌ای مستقل است . بمب منطقی برنامه‌ای است که معمولاً در اعماق رایانه اصلی پنهان شده و منتظر می‌ماند تا در مرحله‌ای خاص در آینده فعال شده و داده‌ها را خراب کند . اسب‌تروا را در قالب برنامه‌ای نرم‌افزاری و مشروع پنهان می‌سازد و منتظر می‌ماند تا آن که نوعی رویداد از قبل تعیین شده یا تاریخی مقرر سر برسد و آن گه بار خود را تحویل می‌دهد و بدین‌ترتیب فایل‌ها یا دیسک‌ها را منهدم می‌کند .

ب: هکرها

نکته: وقتی به اینترنت وصل می‌شوید ،به رایانه‌های سراسر جهان متصل می‌شوید و مهم‌تراینکه آنان نیز به کامپیوتر شما وصل می‌شوند . کاربر رایانه از ارتباط دیگران خبری ندارد ، اما هر ارتباطی با سایت روی اینترنت ، در واقع مثل خیابانی دو طرفه می‌ماند !

هکرهای متخصص ، ابزار نرم‌افزاری پیچیده‌ای را ایجاد کرده و برای دیگران می‌فرستند ، تا آنان بتوانند از نقاط ضعف انسانی و فنی موجود در حفاظت از سیستم‌های رایانه‌ای دیگران استفاده کنند . این ابزار مشتمل است بر استفاده از ابزار کشف کلمات عبور، شماره گیرهای جنگی ، اسکنرهای نقاط آسیب پذیر ، بویشگرها ، رباینده‌گان ای . پی و از این قبیل ، چون بسیاری از این ابزار روی اینترنت موجود است ، تازه واردها چه بسا از آن‌ها استفاده کرده و اقدام به دانلود آن‌ها نمایند ، و سطح پیچیدگی همه انواع هکرها را افزایش دهند .

اکنون با توسعه شبکه‌های بی سیم ، هکرها فرصت‌های تازه‌ای برای کسب دسترسی به رایانه شما یافته و از طریق شما به کل کشور دسترسی می‌یابند .

نکته: هدف نخست هکر عبارت است از نیل دسترسی به تمامی شبکه شما به منظور خواندن فایل‌ها . در اغلب موارد ، کلمات عبور بی اثر ، مودم‌های نا امن ، و به گفته هکرها ، مهندسی اجتماعی، نخستین روزنه را به سوی سیستم می‌گشایند .

- مهندسی اجتماعی

مهندسی اجتماعی در اصطلاح هکرها عبارت است: از فریب کاربران مشروع رایانه برای تامین اطلاعات مفید برای هکرها به منظور دسترسی غیر مجاز به سیستم‌های رایانه ی .

هکری که از مهندسی اجتماعی استفاده می‌کند ، اغلب خود را شخصی مشروع در یک سازمان معرفی کرده و از داستان ساختگی قابل باوری استفاده می‌کند تا کاربر رایانه را با نیرنگ مجبور به ارایه اطلاعات مفید کند . این امر معمولاً با تلفن انجام می‌شود ، اما شاید با پیام‌های جعلی ایمیل یا ملاقات رو در رو نیز صورت پذیرد .

نکته: اکثر افراد تصورات نادرستی از سرقت‌های رایانه ی دارند و فکر می‌کنند این سرقت‌ها کاملا فنی بوده و در نتیجه نقص‌های فنی سیستم‌های رایانه ی متجاوزان امکان توفیق در کار خود را می‌یابند . حقیقت این است که به هر حال ، مهندسی اجتماعی معمولاً نقش بزرگی را در کمک به هکرها برای رد شدن از موانع امنیتی بر عهده دارد . چنان چه هکر هیچ گونه مجوز دسترسی به سیستمی را نداشته باشد ، فقدان آگاهی امنیتی و زودباروی کاربران رایانه معمولاً موجب رخنه آسان وی به درون سیستم حفاظت شده می‌شود .

« کوین میتنیک» ، بدنام‌ترین هکر رایانه‌ای در کشور آمریکا بعد از آزاد شدن از زندان در جلسه شهادت خود در مقابل کنگره گفت ، ضعیف‌ترین عنصر در حفاظت از رایانه عنصر انسانی است . میتینک گفت: «در مهندسی اجتماعی چندان پر قدرت بودم که بندرت پیش می‌آمد نیازی به حمله فنی داشته باشم »

ج: تهدید نیروهای داخلی (کارمندان ناراضی)

عموما معتقد هستند حفاظت از رایانه‌یعنی مقابه با تهدید گروه کثیری از هکرهای بداندیش که در حال حاضر وجود دارند و بر همین اساس تمرکز بسیاری از اقدامات حفاظت رایانه به روی دور نگهداشتن افراد بیرونی از دسترس به رایانه‌ها می‌باشد و این کار را از طریق اقدامات فیزیکی و فنی مثل دروازه‌های ورود، نگهبانان، قفل‌ها، دیوارهای آتش، کلمات عبور، و غیره انجام می‌دهند. با همه این‌ها اگر چه تهدید از ناحیه افراد بیرونی در واقع در همان حد تصور موجود، گسترده است، اما نیروهای داخلی بد طینت نیز با دسترسی مجاز به سیستم تهدید حتی بزرگ‌تر از تهدید نیروهای بیرونی محسوب می‌شوند!

تحقیقات پیاپی حکایت از آن دارد که اغلب خسارات را نیروهای داخلی یعنی افراد دارای دسترسی به شبکه رایانه‌ای وارد کرده‌اند. بسیاری از نیروهای داخلی از دسترسی و دانش لازم برای نفوذ و ایجاد اختلال در سیستم‌ها و شبکه‌های رایانه‌ای برخورد هستند.

افزون بر رخنه نیروهای اطلاعات خارجی حریف به سیستم، شبکه رایانه‌ای که در اختیار دارید در معرض خطراتی از جانب انواع نیروهای بیرونی نیز قرار دارد.

د: نیروهای بیرونی

از نمونه نیروهای بیرونی به موارد زیر می‌توان اشاره کرد:

- دلالان آزاد اطلاعات.
- رقبای خارجی یا داخلی.
- سرویس‌های نظامی کشورهای متخاصم که سرگرم توسعه قابلیت خود برای استفاده از اینترنت به عنوان سلاح نظامی هستند.
- سازمان‌های تروریستی که برای آن‌ها هک کردن سازمان یافته، عاملی بالقوه و کم هزینه، کم خطر و در عین حال همراه با منافع بالا به حساب می‌آید.
- سندیکاهای جرم و جنایت و کارتل‌های مواد مخدر.

- هکرهای ماجراجو که برای سرگرمی یا انجام خراب کاری‌های تفریحی وارد سیستم شما می‌شوند.
- سارقان عادی که متخصص در سرقت و فروش مجدد رایانه‌ها و لپ‌تاپ هستند.

۱-۱۴-۱- ایجاد شکست در فرآیند مدیریت

با توجه به این که مدیریت در هر سیستمی اصلی‌ترین عامل به کارگیری منابع و سازمانی بوده و راهبرد اصلی سازمان توسط مدیران طراحی و اجرا می‌گردد. بسیاری از صاحب نظران مدیریت را علم همراه با هنر مدیر تعریف کرده‌اند . مدیریت اقدامی نیست که در یک مرحله شروع و در همان مرحله نیز به اتمام برسد ، بلکه مدیریت فرآیندی است که ازیک مدیر در سازمان شروع شده و به آخرین لایه‌های ساختاری رسوخ پیدا می‌نماید. به همین دلیل هرگونه تاثیری در مدیریت می‌تواند در کلیه امور یک سازمان و یا یک کشور اثر گذار باشد و به همین دلیل سلطه‌گران به این نتیجه رسیده‌اند که با اثر گذاری در فرآیند مدیریت می‌توانند در دیگر لایه‌های سازمانی نیز اثر گذار باشند. هر گونه شکستی در این لایه برابر است با شکست در اهداف سازمان .

۱-۱۴-۲- هدایت مدیریت به سمت مسیر خود خواسته

سلطه‌گران در رابطه با اعمال نقطه نظرات خود به‌صورت پنهان و آشکار سرمایه گذاری‌های فراوانی انجام می‌دهند. به دنبال آن می‌باشند تا با کم‌ترین سرمایه گذاری مادی و معنوی به بیش‌ترین اثرات نائل شوند. به دنبال اجرای عملیات خود با کم‌ترین آثار و تبعات ملی و بین‌المللی می‌باشند. به دنبال این مطلب می‌باشند تا در مقابل واژه‌های خودساخته‌ای مانند حقوق بشر که امروزه تبدیل به ابزار سلطه‌گری شده است کم‌تر پاسخ‌گو باشند. به همین دلیل تلاش دارند تا فرآیند مدیریت را به سمت استفاده از ابزار مدیریت قابل هدایت از راه دور به صورت پنهان و آشکار سوق دهند تا در زمان مورد نیاز ابتکار عمل را خود به دست گرفته و در شرائط خاص بهره‌برداری خاص خود را داشته باشند.

۱-۱۴-۳- سرقت اطلاعات

سرقت اطلاعات در دنیای آنالوگ کاملاً آشکار بود و پس از سرقت می‌توان سریعاً متوجه این مطلب شد که کالایی به سرقت رفته است اما سرقت اطلاعات در دنیای دیجیتال به صورت کاملاً پنهان انجام

می‌گیرد سرقت کننده به دنبال این می‌باشد که به صورت پنهانی این سرقت را انجام دهد تا مسیر برای سرقت‌های بعدی بسته نشود چنان‌چه سرقت اطلاعات در ابزار دیجیتالی صورت بگیرد ممکن است تا زمان زیادی مالکت اطلاعات متوجه این کار نشود .

۱-۱۴-۴- حملات ویروس

ویروس‌ها برنامه‌های اجرایی کوچکی می‌باشند که به مجرد اجرا شدن بر روی رایانه قربانی می‌تواند تغییرات مورد نظر را به صورت پنهان و یا آشکار بر روی رایانه ایجاد نماید.

۱-۱۴-۵- آسیب‌های اتفاقی

منظور از آسیب‌های اتفاقی آسیب‌هایی است که بدون داشتن هیچ هدفی و با استفاده کردن از ابزار به وقوع می‌پیوندد این گونه آسیب‌ها دارای هدف اولیه نبوده و با در کنار هم قرار گرفتن سخت‌افزارها و نرم‌افزارها به وجود می‌آید.

۱-۱۴-۶- خرابکاری و دستکاری

هرگاه داده‌های در حال جریان بین مبدأ و مقصد توسط شخص غیر مجاز به هر نحو دستکاری یا تحریف شود، حملهٔ «دستکاری داده‌ها» رخ داده است.

۱-۱۴-۷- شکستگی اطلاعات

در بانک‌های اطلاعاتی از کنار هم قرار گرفتن فیلدهای اطلاعاتی رکوردها تشکیل می‌شود این فیلدها با نظم خاصی در کنار هم قرار دارند به طور مثال در کنار هر نام یک فیلد نام خانوادگی وجود دارد و درهر حال نام به نام خانوادگی مربوطه متصل می‌شود. در صورت ایجاد شکستگی در اطلاعات عملاً کل اطلاعات به هم ریخته و مخدوش خواهند شد این کار ممکن است با ارتقا یا تنزل یک فیلد ایجاد شود.

۱-۱۴-۸- خطای در سیستم‌های ارتباطی

با توجه به این که سیستم‌های یک شبکه از طریق سیستم‌های ارتباطی با هم متصل می‌باشند هر گونه خطایی در سیستم‌های ارتباطی قادر خواهد بود در شبکه اثرگذار باشد . این اثرگذاری ممکن است عمدی و یا غیرعمدی صورت بگیرد .

۱-۱۴-۹- استراق سمع

هرگاه یک شخص غیر مجاز به هر نحو بتواند نسخه‌ای از داده‌های در حال جریان بین مبدأ و مقصد را به نفع خود شنود کند، حملهٔ «استراق سمع» به وقوع پیوسته است.

۱-۱۴-۱۰- افزایش اطلاعات ناخواسته

هرگونه افزایش و کاهش اطلاعات به صورت ناخواسته می‌تواند اطلاعات را مخدوش نماید. به‌طور مثال افزایش ۱۰ و یا کاهش آن در یک حساب بانکی می‌تواند آن را به ۱۰٪ کاهش و یا ۱۰ برابر افزایش دهد.

۱-۱۴-۱۱- اقدامات مداخله گرایانه

هرگونه اقدامی که نتیجه آن به هم ریختن منطق موجود سیستم باشد اقدامات مداخله گرایانه نام دارد . اقدامات با هدف اولیه مخدوش سازی سیستم و در نتیجه به دست گرفتن مدیریت سیستم و یا به هم ریختن اطلاعات صورت می‌پذیرد

۱-۱۴-۱۲- آسیب‌های سیستم عامل

نرم‌افزارها انواع و اقسام مختلفی دارند یکی از بارزترین نرم‌افزارها سیستم عامل می‌باشد. وظیفه سیستم عامل مدیریت بر سخت‌افزار و نرم‌افزار رایانه می‌باشد. با توجه به نقش مهم این نرم‌افزار در مدیریت رایانه آسیب‌های آن نیز شکل ویژه‌ای به خود می‌گیرد به همین دلیل نفوذگران تلاش می‌کنند تا از آسیب‌پذیری‌های سیستم عامل برای مدیریت بر سیستم استفاده نمایند.

۱-۱۴-۱۳- آسیب‌های سخت‌افزاری

تمام سخت‌افزارها می‌توانند دارای نقاط آسیب‌پذیر از قبل تعریف شده و یا پس از استفاده باشند این گونه نقاط آسیب‌پذیر در صورت شناسایی می‌تواند باعث دسترسی به اطلاعات از راه دور باشد . هرگونه آسیب سخت‌افزاری عملاً باعث آسیب رسانی به اطلاعات خواهد شد.

۱-۱۴-۱۴- آسیب‌های نرم‌افزاری

با توجه به این که نرم‌افزارها از کدهای به هم پیوسته تشکیل شده است عملاً می‌توان با نوشتن کدهای خاص ، نرم‌افزار را به سمت خاصی هدایت نمود. چنان‌چه نویسنده نرم‌افزار در نرم‌افزار خود از کدهای پنهان استفاده نماید می‌تواند باعث آسیب‌های نرم‌افزاری گردد و آسیب‌های نرم‌افزاری به صورت عمدی و یا غیرعمدی در نرم‌افزارها قرار داده شود.

۱-۱۴-۱۵- آسیب به اطلاعات خصوصی

هر کاربر زمانی که با رایانه کار می‌کند هم‌زمان تولید اطلاعات خصوصی می‌نماید. به‌طور مثال درصورتی‌که در نظر داشته باشد بر روی اینترنت از آدرس ایمیل استفاده نماید باید از قبل با ارائه اطلاعات خصوصی آن را ایجاد نماید و یا چنان‌چه در نظر داشته باشد برای استعلام قبولی و یا عدم قبولی در کنکور استعلامی انجام دهد باید اطلاعات خصوصی را در رایانه وارد نماید و یا اگر در نظر داشته باشد اطلاعات بانکی خود را کنترل نمایند باید اطلاعات خصوصی را در رایانه وارد نماید تجمیع این اطلاعات در رایانه می‌تواند باعث آسیب رسانی به اطلاعات خصوصی گردد.

۱-۱۴-۱۶- کلاهبرداری در اطلاعات

سواستفاده کنندگان از اطلاعات به دنبال دسترسی به اطلاعات می‌باشند تا بتوانند بر اساس آن از افراد کلاهبرداری نمایند یکی از خطراتی که رایانه و اطلاعات آن را تهدید می‌کند دسترسی افراد کلاهبردار به اطلاعات و سواستفاده از آن می‌باشد .

۱-۱۵- امنیت چالش اصلی جهان نوین

با توجه به این که در کلیه کشورهای جهان مسائل زیر به عنوان یکی از اولین اولویت‌های استفاده از ابزار نوین می‌باشد، مسئله امنیت آن نیز اولویت اول را در بر می‌گیرد. تمام کشورهای دنیا به خاطر حفظ امنیت ملی خود تلاش بر این دارند تا امنیت ابزار نوین دیجیتال خود را حفظ نمایند و این مسئله به چالشی جهانی تبدیل شده است .

در تمام دنیا:

افزایش اطلاعات

تبدیل اطلاعات آنالوگ به دیجیتال

استفاده از اطلاعات در مبدا تولید

افزایش توان بهره‌برداری از اطلاعات

سرعت بخشی به تبدیل اطلاعات به تصمیم

جزو دغدغه‌های اصلی تمام کشورها می‌باشد.

۱-۱۶- سئوالات خودآزمایی

ضمن تعریف اطلاعات، نقش اسناد در امنیت اطلاعات را بیان نمایید.

پدافند غیر عامل را تعریف کرده و اختلاف آن را با پدافند عامل بیان نمایید.

اختلاف بین تهدیدات و فرصت‌ها در دنیای سنتی و نوین را بیان نمایید.

انواع تهدیدات را نوشته و تهدیدات انسان ساخت را توضیح دهید.

انواع اطلاعات دیجیتال را نام برده و توضیح دهید.

پنج نوع از آسیب‌های دنیای دیجیتال را نام برده و توضیح دهید .

اصل کلی و اصول فرعی امنیت دیجیتال را نام برده و توضیح دهید.

فصل دوم - آشنایی با پدافند غیر عامل فاوا

آن چه در این فصل خواهید آموخت:

تعریف فاوا

تعریف پدافند غیر عامل

تعریف پدافند غیر عامل فاوا

سابقه پدافند غیر عامل فاوا

مفاهیم امنیت در فاوا

۲- آشنایی با پدافند غیر عامل فاوا

پدافند غیر عامل از ابتدا تاکنون در حوزه‌های تخصصی مختلفی نمود داشته و عرصه اقدامات پیشگیرانه را به روی کاربران گشوده است . یکی از عرصه‌های آسیب‌پذیر دنیای ارتباطات و فن‌آوری اطلاعات می‌باشد که در این فصل اختصاصاً به آشنایی با پدافند غیر عامل در حوزه فاوا۱ خواهیم پرداخت.

۲-۱- تعریف فاوا

هر چند به نظر می‌رسد مفهوم فن‌آوری اطلاعات ، و فن‌آوری اطلاعات و ارتباطات (فاوا) روشن باشد اما در واقع چنین نیست . تعاریف مختلفی از فن‌آوری اطلاعات توسط افراد مختلف ارائه شده است . از جمله می‌توان به تعاریف زیر اشاره نمود:

مطالعه ، طراحی ، توسعه و مدیریت کلیه نرم‌افزارها و سخت‌افزارهایی که در یک شبکه و یک محیط ارتباطی با هم کار می‌کنند .

منظور از فن‌آوری اطلاعات همه شکل‌های فن‌آوری است که به وسیله آن‌ها عملیات دستیابی ، ذخیره سازی و مبادله اطلاعات به شکل‌های گوناگون مثل متن ، تصویر ، صدا و نمایش چند رسانه‌ای انجام می‌شود .

فن‌آوری اطلاعات دانشی است که به بررسی ویژگی‌ها و چگونگی اطلاعات نیروهای حاکم بر جریان اطلاعات و ابزار آماده سازی آن‌ها برای به حداکثر رساندن دستیابی به اطلاعات و قابل استفاده کردن آن

۱فن‌آوری اطلاعات و ارتباطات

می‌پردازد . آماده سازی اطلاعات شامل تفکیک اطلاعات دقیق ، علمی و مستند ، جمع آوری، سازمان دهی ، ذخیره ، بازیابی ، تفسیر ، اشاعه و استفاده از آن می‌شود . (مؤسسه فن‌آوری جورجیا ، ۱۹۶۲ – نقل از اترتون ،۱۹۹۷).

اصطلاح فن‌آوری اطلاعات برای توصیف فن‌آوری‌هایی به کار می‌رود که ما را در ضبط ، ذخیره سازی ، پردازش ، بازیابی ، انتقال و دریافت اطلاعات یاری می‌کند . این اصطلاح ، فن‌آوری‌هایی مانند رایانه ، انتقال از طریق دورنگار ، ارتباط از راه دور ، تلفن ، ماشین حساب ، چاپ و حکاکی را نیز در بر می‌گیرد (کیت بهان و دیانا هولمز ، ۱۹۹۸) .

فن‌آوری اطلاعات به مجموعه به هم پیوسته‌ای از روش‌ها ، سخت‌افزارها ، نرم‌افزارها ، و تجهیزات ارتباطی که اطلاعاتی را در اشکال گوناگون (صدا ، تصویر و متن) جمع آوری ، ذخیره سازی ، بازیابی ، پردازش ، انتقال و یا عرضه می‌کند ، اطلاق می‌شود (دبیرخانه شورای عالی انفورماتیک ، ۱۳۷۸) .

فن‌آوری اطلاعات متشکل از سخت‌افزار ، نرم‌افزار ، نیروی انسانی ، اطلاعات ، مدیریت ، تولید و نگهداری است که در ارتباط متقابل با یک‌دیگرند و فضایی مملو از اطلاعات ذخیره شده به صورت نظام‌دار و با قابلیت دسترسی آسان پدید می‌آورند . این فضا در خدمت نیازهای اقتصادی ، اجتماعی و فرهنگی جامعه قرار می‌گیرد و سبب بهره‌وری و افزایش کیفیت و محصولات سازمان‌های متبوع می‌شود (اسکاپ ESCAP) .

فن‌آوری اطلاعات همانند محور و مرکز مجموعه‌ای از فعالیت‌های هدایت شده است که کنترل مدیریت ، بهره‌وری ، تولید ، آموزش و ارتقای یک سیستم (اعم از سازمان یا پایگاه اطلاعاتی و . . .) را با یک مرکزیت بر عهده دارد . همه سازمان‌ها ، ارگان‌ها ، نهادها و وزارتخانه‌ها ناگزیر از برقراری ارتباط با یک‌دیگر و انتقال اطلاعات هستند . سازمان فن‌آوری اطلاعات مسؤول برقراری این ارتباطات در اشکال پیشرفته الکترونیکی است و به طور کلی مسؤلیت کلی تولید ، حفظ ، ذخیره ، بازیابی و انتقال اطلاعات در یک شبکه پیچیده را بر عهده دارد (محمدی ، ۸۲).

فن‌آوری اطلاعات ، نقطه همگرایی الکترونیک ، پردازش داده‌ها و ارتباطات دور که شامل تعدادی رایانه قوی ، فن‌آوری‌های ارتباطی و هم‌چنین نرم‌افزار است ، که نیاز به آن بر اثر سه عامل ایجاد می‌شود. اول آنکه فن‌آوری اطلاعات خود صنعتی راهبردی (استراتژیک) و بسیار سودآور در جهان است . دوم آن که فن‌آوری کلیدی است و در همه صنایع و خدمات کاربرد دارد . سوم آن که زیر بنای اساسی است که به همه مؤسسات و واحدهای اقتصادی امکان می‌دهد تا در استفاده از دانش بشری و انتقال آن سهیم شوند ؛ سبب کاهش هزینه‌ها می‌شود و در نتیجه به افزایش بهره‌وری و کیفیت محصول می‌انجامد (سازمان راهبردهای فن‌آوری اطلاعات آمریکاNSIT) .

فن‌آوری اطلاعات تنها در ارتباط با رایانه‌ها ، نرم‌افزار و یا خدمات وابسته به آن‌ها نیست . فن‌آوری اطلاعات‌ترکیبی از همه این موارد است با این نگرش که چگونه این فن‌آوری می‌تواند کمکی به سازمان و رسیدن به اهداف آن کند . . . . فن‌آوری اطلاعات باعث می‌شود انجام کارهای زیاد و طولانی با عملیات کمی انجام گیرد (Sutter ۲۰۰۳) .

فن‌آوری اطلاعات نوعی از فن‌آوری است که در آن انتقال داده ، اطلاعات و دانش انجام می‌گیرد . این مفهوم ضرورتاً وابسته به رایانه‌ها نیست ، هر چند که امروزه رایانه‌ها به عنوان ابزاری در گسترش و ایجاد راه‌هایی بسیار قدرتمند در انجام امور هستند . نقشه‌کشی ، هندسه تحلیلی ، دستگاه‌های کپی ، تلگراف ، تلفن ، فاکس و غیره به خوبی نمونه‌هایی از فن‌آوری اطلاعات هستند (Fischiner ۲۰۰۰) .

برای بسیاری از مردم این واژه مترادف است با « فن‌آوری جدید» که از ماشین‌هایی که بر مبنای ریز پردازنده‌ها کار می‌کنند ، استفاده می‌کند . به عبارت دیگر گفته می‌شود که « فن‌آوری اطلاعات » به طور ساده ، بیانگر کوششی است برای ممکن نمودن توسعه و پیشرفت محرک‌های تجارتی به طور الکترونیکی و هم‌چنین ایجاد حرکتی سیاست گونه برای کنترل دسترسی به اطلاعات (Zorkoczy and Nicholas ۱۹۹۵) .

در سال‌های اخیر ، کتاب‌ها ، مجلات ، مقالات و کنفرانس‌ها ، راه‌هایی را برای ارتباط پژوهشی و علمی ایجاد نموده‌اند . امروزه فن‌آوری به ویژه فن‌آوری اطلاعات ، در حال تاثیر گذاری بر روی هر یک از این

سیستم‌های ارتباطی است . نشر الکترونیکی ، متن الکترونیکی ، پیام مبتنی بر صدا و کنفرانس‌های تصویری ، چند نمونه از اثر فن‌آوری اطلاعات هستند . فن‌آوری اطلاعات به ما راه‌های جدیدی برای ارتباط می‌دهد و اساساً این امکان را به وجود می‌آورد تا سیستم‌های ارتباطی موجود نیز مورد تصحیح و بهبود قرار گیرند . این کار آسان به نظر می‌رسد که تغییر و تحول از سیستم‌هایی که از تنظیمات دستی استفاده می‌کنند به سیستم‌های الکترونیکی انجام گیرد (Karamouzis ۱۹۹۹) .

فن‌آوری اطلاعات‌ترکیبی از دو مفهوم فن‌آوری و اطلاعات است . اطلاعات مفهوم گسترده‌ای را در بر دارد و به یک سری محتویات اشاره می‌شود ، در حالی که فن‌آوری به ابزارهایی که برای دستکاری این محتویات به کار می‌رود ، گفته می‌شود . فن‌آوری یک عنصر ضروری درتراکنش‌های پردازش اطلاعات است که مشاهده ، آگاهی و تجربه از یک رابطه سلسله مراتبی در آن برخوردار هستند . اطلاعات منجر به پیدایش آگاهی شده ، و از به وجود آمدن آگاهی زیاد ، تجربه حاصل می‌گردد . اطلاعات از داده‌هایی که ضرورتاً قابل احساس و ادراک هستند نشأت می‌گیرد . هنگامی که داده‌ها برای استفاده در برخی امور سودمند به دسته‌ها و طبقه‌هایی دسته بندی و سازمان دهی می‌شوند ، تبدیل به اطلاعات می‌گردند (Chaurasia ۲۰۰۳) .

فن‌آوری اطلاعات هر مجموعه‌ای از ابزارها ، روش‌ها و رسانه‌ها است که برای ثبت ، ذخیره ، و انتقال اطلاعات به کار گرفته می‌شود . معمولاً امروزه هنگامی که این اصطلاح را به کار می‌بریم ، در حقیقت در مورد زیر مجموعه خاصی از فن‌آوری اطلاعات صحبت می‌کنیم: فن‌آوری اطلاعات دیجیتالی شبکه‌ای (Willis ۲۰۰۲) .

فن‌آوری اطلاعات عبارت است از سخت‌افزار ، نرم‌افزار ، ارتباط مخابراتی و سرویس‌ها و خدماتی از کارمندان فن‌آوری اطلاعات (Effy Oz ۲۰۰۲) .

فن‌آوری اطلاعات ، حوزه‌ای نسبتاً جوان در مقابله با اکثر نظام‌های علمی دیگر است . با این وجود ، در حدود ۵۰ سال ، این فن‌آوری به عنوان بخشی از علم و دانش در آمده که به خوبی قابل استدلال بوده و تقریباً پیچیده‌تر از نظام‌های علمی سنتی از قبیل ادبیات یا روانشناسی ،و یا پچیده‌تر از حوزه‌های

حرفه‌ای از قبیل کسب و کار یا قانون است . در هر صورت ، فن‌آوری اطلاعات ، اساساً متفاوت از این نظام‌ها در برخی از نسبت‌های مهم بوده ، و بنابراین سواد فن‌آوری اطلاعات ، ضرورتاً متفاوت از سواد در حوزه‌های دیگر است(Ralph ۱۹۹۷) .

اما به نظر می‌رسد هیچ‌یک از تعاریف ، نتواند ابعاد حقیقی مفهوم فاوا را به درستی تبیین نماید . این‌ها واژه یکسانی را برای مفاهیم مختلف به کار می‌برند . لازم به تذکر است که مفهومی که مستقل از یک واژه ، با توجه به معنای لغات و صرف نظر از موارد کاربردی و استدلالات به کار برندگان آن ، استنباط می‌شود ، ممکن است با مفهومی که این واژه در تبیین آن مفهوم رواج دارد ، متفاوت باشد . هدف ما در این جا ، شناسایی آن مفهوم است . به نظر می‌رسد سه دیدگاه مختلف ، و سه دسته مختلف از تعاریف – مفاهیم برای فاوا وجود داشته باشد:

دسته اول: این دسته ، مفهوم فن‌آوری اطلاعات (و ارتباطات) را به نوعی همان فن‌آوری رایانه و سیستم‌های رایانه ی اطلاعاتی و ارتباطی ، در وجود نرم‌افزار و سخت‌افزار و شبکه و نظایر آن و مسائل مدیریتی مربوط به آن می‌دانند . اغلب تعاریف از این دسته‌اند

دسته دوم:این دسته فن‌آوری اطلاعات را از بُعد اطلاعات محض آن که حتی شامل مواردی نظیر مستند سازی و کتاب‌داری نیز می‌شود ، مورد توجه قرار می‌دهند . در این دسته تمرکز بر خود اطلاعات است و فن‌آوری اطلاعات ، هرگونه استفاده از ابزارها و روش‌ها و تکنیک‌هایی است که مدیریت و سازماندهی این اطلاعات را فراهم می‌کند . تعریف‌های اولیه و با سابقه بیش‌تر از این دسته‌اند . البته این مفهوم شاید نزدیک‌ترین مفهوم به معنای مستقیم واژه فاوا باشد . از جمله تعریف مؤسسه فن‌آوری جورجیا از این دسته است .

دسته سوم: این دسته ، برای فاوا نقشی کلیدی و محوری نسبت به سایر فن‌آوری‌ها و کاربردها قائل می‌شود . این دسته با زاویه‌ای فراتر از زاویه‌های دو دسته قبلی به فاوا نگاه می‌کند . اما مشکل این دسته آن است که به درستی نمی‌تواند ابعادی را که برای فاوا از این زاویه مشاهده می‌کند ، توضیح دهد و در

یک عبارت و تعریف مشخص ، بیان کند . از جمله تعریف سازمان راهبردهای فن‌آوری آمریکا (NSIT) و تعریف آخر از این دسته‌اند . (erfan۲۰۰۰. persiangig. ir)

۲-۲- تعریف پدافند غیر عامل

علاقه به حیات و حفظ بقاء به صورت غریزی در هر انسانی وجود دارد. لذا در طول تاریخ، بشر برای دستیابی به ملزومات حیاتی خود از جمله غذا و انرژی به گسترش و توسعه مراتع و زمین‌های کشاورزی و معادن پرداخته یا به جهت دفع تجاوز دشمنان خود جنگ‌ها و منازعات بسیاری را پشت سر نهاده است. سلاح‌هایی که جوامع بشری قبل از دوران صنعتی در جنگ‌ها به کار می‌بردند دست ساز و بسیار ساده بود. بین روند رشد دانش و فن‌آوری با نوع سلاح‌هایی که جوامع بشری برای بهره گیری از آن‌ها در جنگ ابداع و اختراع می‌کرده‌اند، ارتباط نزدیکی وجود داشته است.

در دوران معاصر، این پیوستگی در اثر تحولات و پیشرفت‌های عظیم در فن‌آوری رو به فزونی نهاده است. پس از وقوع انقلاب صنعتی که توسعه‌ی همه‌جانبه‌ای را در همه‌ی سطوح فن‌آوری پدید آورد، تحولات گسترده‌ای در نوع و کیفیت استفاده از تجهیزات تسلیحاتی نیز ایجاد شد.

اساساً جنگ‌ها و منازعات در طول تاریخ به دلیل تعارض منافع و تمایل ذاتی انسان‌ها به برتری جویی روی داده است. در درگیری‌ها، طرفین درگیری تمایل دارند خواسته‌های خود را در حوزه‌های مختلف بر گروه مقابل تحمیل کنند و این کار در صورت عدم موفقیت در عرصه‌ی دیپلماسی منجر به جنگ می‌گردد.

ماهیت جنگ‌ها و تخاصمات بشری در دوره‌های مختلف تاریخ دستخوش تغییرهای زیادی گردیده است. در عصر حاضر پس از پشت سر گذاشتن سه نسل از جنگ‌ها، در چهارمین دوره از منازعاتی قرار داریم که از ابتدای تاریخ بین افراد و جوامع مختلف در گرفته است. در ادامه به بررسی نسل‌های مختلف جنگ می‌پردازیم.

نسل اول جنگ

از زمان پیدایش پدیده جنگ بین گروه‌های جمعیتی (قبایل و . . .) و با تشکیل حکومت‌ها توسط انسان بین ملت‌ها یا کشورها تا ورود سلاح‌های آتشین به میدان جنگ در این نسل از جنگ‌ها قرار می‌گیرند که عموماً متکی به تعداد نفرات و زور و بازو یا توان برخی افراد و مهارت آن‌ها در بکارگیری سلاح‌های سرد بوده است. گرچه نبوغ فرماندهان و طراحان جنگ همیشه نقش اساسی داشته است.

نسل دوم جنگ

با ورود سلاح‌های آتشین به عرصه جنگ‌ها، بسیاری از اصول و مبانی طرح ریزی و فرماندهی جنگ تغییر کرد. اهمیت زور و نیروی بدنی و تعداد نفرات تا حدودی کاسته شد. میدان درگیری و مانورها و حرکات تغییر کرد، برج و باروها و . . . آسیب پذیر شدند و بدین‌ترتیب انسان نسل دوم جنگ‌ها را تجربه کرد.

نسل سوم جنگ

انقلاب صنعتی موجب تحول و شکوفایی بشر در عرصه اختراعات و تولید فن‌آوری‌ها و ماشین‌های مختلف گردید. ورود فن‌آوری‌ها و ماشین‌ها (خودروها، تانک، نفربر، هواپیما، زیردریایی و تجهیزات پیشرفته) به عرصه جنگ‌ها، یک‌بار دیگر حوزه‌های طرح ریزی و فرماندهی جنگ را به شدت تحت تأثیر قرار داده و متحول ساخت. تعاریف و مفاهیم (قوی و ضعیف و . . .) تغییر کرد. عرصه‌های درگیری و نبرد به طرز حیرت آوری توسعه یافت و بشر یک دوره نسبتاً طولانی و بسیار خسارت‌بار با تلفات انسانی غیرقابل تصور از جمله دو جنگ جهانی و صدها جنگ منطقه‌ای و محدود را از این نسل جنگ‌ها تجربه کرده و در حال تجربه کردن می‌باشد.

نسل چهارم جنگ

تدوام رشد علوم و فن‌آوری‌ها موجب شد که قدرت‌های سلطه گر تحمیل منافع و نظرات خود بر رقبا و کشورهای ضعیف را بدون جنگ فیزیکی و نظامی و با بکارگیری ابزارهای قدرت اقتصادی، سیاسی، تبلیغاتی، فرهنگی و . . . طرح ریزی و تعقیب نمایند و ضربه و جنگ نظامی را به عنوان آخرین حربه در

اولویت آخر قرار دهند تا ضمن ارائه ریاکارانه چهره‌ی مسالمت‌جو، خود را از عوارض (هزینه‌ها، تلفات و . .) جنگ نظامی دور نگه دارند و بدین‌ترتیب بشر سال‌های نخست نسل جدید جنگ یعنی جنگ‌های نسل چهارم را آغاز کرده است.

این تغییرات که از آن به نسل چهارم جنگ‌ها تعبیر می‌شود، منجر به بروز جنگ‌های اقتصادی و اجتماعی گردیده است. در این نسل نوپا از درگیری‌ها، دشمنان با استفاده از حربه‌های اقتصادی، فرهنگی و اجتماعی و با به کارگیری همه‌ی مؤلفه‌های قدرت به زورآزمایی می‌پردازند. منازعات نسل چهارم در قدیمی‌ترین شیوه‌ی خود در تحریم‌های اقتصادی نمود یافت. اما استفاده از ابزارهای نوین اطلاع‌رسانی، گسترش شبکه‌ی جهانی اینترنت و به وجود آمدن شبکه‌های اجتماعی در بستر آن و نیز خدمات پردازش سیار به گسترش این دسته از منازعات در عرصه‌ی اجتماعی کمک شایانی نموده است. در واقع مهاجمان در این نوع درگیری‌ها با اجرای انواع توطئه‌های اقتصادی و سیاسی و نیز با گسترش فضای نارضایتی اجتماعی از طریق شبکه‌های ارتباطی و اطلاع‌رسانی، حریف خود را درگیر مشکلات داخلی و بین‌المللی نموده و از این طریق وی را به پذیرش اغراض سیاسی خود در میدان زورآزمایی‌های داخلی یا فرامنطقه‌ای مجبور می‌سازند.

در قبال این نوع منازعه تجهیز به ابزارهای دفاعی یا پدافندی تنها منحصر به نظامیان و لشکریان نیست. بلکه لازم است کلیه‌ی افراد، سازمان‌ها و مجموعه‌ها را با فرآیندها و روش‌هایی غیرنظامی برای مقابله آماده ساخت.

پدافند غیرعامل به مجموعه اقداماتی اطلاق می‌گردد که مستلزم به کارگیری جنگ افزار نبوده و با اجرای آن می‌توان از وارد شدن خسارت به تجهیزات و تاسیسات حیاتی و حساس نظامی و غیرنظامی و تلفات انسانی جلوگیری نموده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد.

در ادبیات موضوع، علاوه بر پدافند غیرعامل، به مفهومی به نام دفاع غیرنظامی برمی‌خوریم که عبارت است از تقلیل خسارات مالی و صدمات جانی وارده بر غیرنظامیان در جنگ یا در اثر حوادث طبیعی نظیر سیل، زلزله، طوفان، آتش‌فشان، آتش‌سوزی و خشکسالی.

در منابع تخصصی سایر کشورها، وظایف دفاع غیرمسلحانه شامل چهار عنوان می‌باشد:

اقدامات پیشگیرانه و کاهش دهنده۱

آماده سازی و امداد رسانی۲

هشدار و اخطار۳

باز سازی مجدد۴

اقدامات دفاع غیرعامل شامل اصول اساسی و ملاحظاتی است که در اغلب کشورهای جهان، با کمی اختلاف پذیرفته شده‌اند ولی شیوه به کارگیری آن‌ها ابتکاری، هنرمندانه و خردمندانه است. به همین دلیل وسعت این اقدامات به خلاقیت‌های فکری بشر و شرایط زمان و مکان بستگی دارد و بعضاً نمی‌توان حد و مرزی برای آن تعیین کرد.

در تعریف دیگری پدافند غیرعامل به کلیه‌ی اقدامات و تدابیری گفته می‌شود که بدون استفاده از سلاح موجب کاهش آسیب‌پذیری، تلفات و خسارات و افزایش پایداری شود.

به طور خلاصه می‌توان گفت پدافند غیرعامل یعنی دفاع در مقابل تهدید، بدون استفاده از سلاح. به عبارتی دفاع غیرعامل، مکمل دفاع عامل است و در حوزه‌ی امنیت ملی مفهوم دفاع، تلفیقی از دفاع عامل و دفاع غیرعامل است.

---

۱ Mitigation

۲ Preparation

۳ Response

٤ Recovery

اقدامات پدافند غیرعامل در سطوح مختلفی طراحی و اجرا می‌گردند. این سطوح شامل موارد زیر است:

سطح استراتژیک: اقداماتی است که در سیاست‌های کلی کشور و تأمین مبانی و پشتوانه‌های قانونی، حقوقی و سیاست‌های برنامه بلندمدت توسعه کشور تأثیرگذار است.

سطح عملیاتی: اقداماتی است که در برنامه‌های ۵ ساله‌ی توسعه‌ی سازمان‌ها تأثیرگذار است.

سطح تاکتیکی: اقداماتی است که در برنامه‌های سالانه‌ی سازمان مؤثر است.

سطح اقدامات ویژه: که شامل اقداماتی است که تأثیر آن در اولویت‌های خاص و نقاط مهم می‌باشد.

اگر بخواهیم به صورت فهرست‌وار به برخی از اقدامات پدافند غیرعامل در حوزه‌های غیر از فن‌آوری اطلاعات اشاره کنیم، موارد زیر قابل ذکر است:

مکان یابی مناسب

انتخاب مقیاس بهینه

پراکندگی در سایت

استفاده از عمق زمین

توزیع عمل‌کرد

فریب در نمای عمل‌کردها

داشتن طرح پوشش وفریب

مدیریت بحران ناشی از جنگ

موازی سازی اقدامات

کاهش وابستگی

پوشش اطلاعاتی

چند منظوره کردن عمل‌کردها

کاهش امکان تهدید

استفاده از فن‌آوری بومی

توسعه شبکه پایش و هشدار امنیتی

ایجاد اهداف مجازی وکاذب

ایمن سازی سیستم فرماندهی وکنترل

نامرئی سازی در برابر دشمن

تولید موانع دومنظوره و چند منظوره

از منظر امنیت ملی، پدافند غیرعامل بستر مناسبی برای توسعه‌ی پایدار اقتدار ملی کشور در حوزه‌ی دفاعی است. هم‌چنین پدافند غیرعامل با سیاست‌های تنش‌زدایی همراستا است. چراکه کشورهایی که توسعه پدافند غیر عامل را به عنوان یک سیاست دفاعی مستمر در دستور کار خود قرار می‌دهند هیچگاه در مظان اتهام تهدید بر علیه کشورهای دیگر قرار نمی‌گیرند.

اقدامات پدافند غیرعامل به دلیل غیرنظامی بودن، پایدارترین و ارزان‌ترین روش دفاع و هم‌چنین مناسب‌ترین راهکار افزایش آستانه‌ی مقاومت می‌باشد. این دسته از اقدامات مناسب‌ترین شیوه‌ی کاهش مخاطرات و آسیب‌پذیری‌ها و از طرفی مهم‌ترین ابزار بازدارندگی هستند. به عبارت دیگر کشورهایی که

پدافند غیر عامل را به عنوان یک راه کار اصلی بر می‌گزینند به شرایطی از نظر کاهش آسیب‌پذیری دست می‌یابند که مطامع کشورهای تهدید کننده بر علیه آن‌ها کاهش می‌یابد.

در جهان امروز کشورهایی که نقاط آسیب‌پذیری آن‌ها فراوان است و دشمن می‌تواند با ضربات سریع، حیاتی‌ترین منابع آنان را منهدم نماید، عوامل تهدید بیرونی را تحریک و دشمنان را تحریص می‌نمایند. از این رو برای دست‌یابی به یک توسعه‌ی پایدار با سطح قابل قبولی از امنیت، پدافند غیرعامل در سطح کشور باید به یک فرهنگ عمومی تبدیل شود. (پدافند غیرعامل کشور – پورابراهیمی و بنابی -۱۳۸۹)

اقدامات پدافند غیرعامل باید در سه حوزه امنیت، ایمنی و پایداری طرح‌ریزی و اجرا شود. مجموعه این اقدامات در کنار یک‌دیگر و به عنوان سه جزء اساسی و غیر قابل تفکیک می‌باشند.ترکیب این سه جزء در کنار یک‌دیگر می‌تواند درتأمین دفاع غیرعامل و کاهش آسیب‌پذیری زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم کشور در مقابل تهدیدات از طریق فرهنگ‌سازی، سیاست‌گذاری، طرح‌ریزی و برنامه‌ریزی راهبردی و تدوین ضوابط و دستورالعمل‌های تخصصی با قابلیت هدایت بخش‌های کشوری و لشکری موفق باشد.

به بیان ساده‌تر می‌توان گفت ایجاد بازدارندگی دفاعی کشور از طریق اقدامات پدافند غیرعامل مستلزم:

حفظ اسرار و اطلاعات کشور و ممانعت از دسترسی دشمنان به اطلاعات ارزشمند ملی و بخشی کشور

ایمن‌سازی زیر ساخت‌های ملی و مراکز حیاتی، حساس و مهم.

پایدار سازی زیرساخت‌های ملی و مراکز حیاتی،حساس و مهم کشور.

می‌باشد

در نگرش سیستمی این عوامل سه جزء یک سیستم می‌باشند که در تعامل با یک‌دیگر مفهومی تحت عنوان توسعه‌ی دفاع غیرعامل و افزایش قدرت بازدارندگی را شکل می‌دهند.

۲-۲-۱- امنیت

امنیت اطلاعات از جنبه‌های مختلف حائز اهمیت می‌باشد که محرمانگی و در دسترس بودن و حفظ تمامیت از جمله آنها می‌باشد . امروزه بدون بومی سازی نمی‌توان انتظار ایجاد امنیت مطلوب را داشت. امنیت از جمله مواردی می‌باشد که معمولا در تضاد با برون سپاری بوده و می‌بایست توسط نیازمند به امنیت و به صورت بومی تولید و ایجاد گردد.

۲-۲-۲- ایمنی

ایمنی به مفهوم امن بودن در مقابل تهدیدات و حملات سخت و نیمه سخت می‌باشد. هر سیستمی به منظور تداوم بقا و توان ارائه تولیدات و خدمات باید ایمن باشد. به منظور تامین ایمنی باید در خصوص هر یک از مراکز حیاتی،حساس و مهم طرح‌های لازم تهیه گردد. برای این منظور باید نسبت به تعریف و درجه بندی میزان حفاظت برای هر طرح در برابر تهدید اقدام شود.

هر چند در هر برنامه ریزی، تحلیل هزینه-فایده باید مد نظر قرار گیرد، در مواردی که تأمین ایمنی مراکز حیاتی،حساس مورد نظر است این اقدامات باید با اولویت بالا تامین هزینه شود. چرا که باید در مقابل منافع ظاهری، منافع مؤثر در امنیت ملی در این حوزه نیز مورد توجه باشد.

برخی از اقداماتی که در این حوزه می‌توان انجام داد عبارتند از:

سطح بندی (تعیین میزان اهمیت تأسیسات، مرکز یا تشکیلات)

تعیین اهمیت واولویت طرح‌ها

تعیین سطح ایمنی مورد نیاز

مکان یابی

طراحی

تعیین شاخص‌ها واستانداردهای پدافند غیرعامل در استقرار عمل‌کردها

تعیین شاخص‌های عمل‌کردی هر سیستم در استقرار

تعیین مجموعه ضوابط واستانداردها برای استقرار

بررسی نقاط امن در پهنه‌ی جغرافیای مورد نظر

انتخاب گزینه‌های نقاط امن برای استقرار عمل‌کردها

تعیین شاخص‌های مناسب مکان گزینی پدافند غیرعامل

امتیاز دهی و وزن دهی به شاخص‌ها بر اساس اهمیت و وزن

انتخاب جایگزین بهینه در مکان‌گزینی مناسب برای استقرار طرح‌ها

۲-۲-۳- پایداری

هرچند امنیت و ایمنی سیستم‌ها از منظر پدافند غیر عامل بسیار مهم و ضروری است اما به مفهوم تامین سیستم دفاعی کامل نمی‌باشد . یکی از نکات مهم، وجود پایداری در تولید و ارائه خدمات در مراکز حیاتی، حساس و مهم است. پایداری به این معنی است که یک مرکز در شرایط عادی و یا در صورت بروز حمله و خدشه دار شدن هر دو یا یکی از دو جزء ذکر شده، یعنی امنیت و ایمنی، باید امکان تداوم ارائه تولیدات و خدمات خود را داشته باشد. برای این تداوم و پایداری سیستم‌ها راه کارها و شیوه‌های مختلفی وجود دارد. برخی از این راه کارها عبارتند از:

موازی سازی

تأمین ظرفیت‌های موازی

پیش بینی روش‌های موازی

تأمین احتیاط (پشتیبانی۱)

کاهش وابستگی

وابستگی فن‌آورانه، علمی و . . . به خارج از کشور

وابستگی خدمات و پشتیبانی به سایر بخش‌ها (داخلی یا خارجی)

تنوع منابع پشتیبانی

توسعه اشتراک منافع

توسعه و ارتقاء موقعیت بین‌المللی (به‌دست آوردن فرصت‌های منطقه‌ای و بین‌المللی)

۲-۳- تعریف پدافند غیر عامل فاوا

هر اقدام غیر مسلحانه‌ای که موجب کاهش آسیب‌پذیری نیروی انسانی، ساختمان‌ها، تاسیسات، تجهیزات، اسناد و شریان‌های کشور در مقابل عملیات خصمانه و مخرب دشمن گردد، پدافند غیرعامل خوانده می‌شود.

به بیان ساده‌تر پدافند غیرعامل، مجموعه اقداماتی است که انجام می‌شود تا در صورت بروز جنگ و حتی در زمان صلح ، خسارات احتمالی به حداقل میزان خود برسد.

هدف از اجرای طرح‌های پدافند غیرعامل کاستن از آسیب‌پذیری نیروی انسانی ، تجهیزات حیاتی و حساس و مهم کشور علیرغم حملات خصمانه و مخرب دشمن و استمرار فعالیت‌ها و خدمات زیر بنایی و تامین نیازهای حیاتی و تداوم اداره کشور در شرایط بحرانی ناشی از جنگ است.

---

۱ Back up

به عنوان مثالی ساده، از پدافند غیرعامل می‌توان به استتار، اختفا و ایجاد سرپناه برای تاسیسات مهم و استراتژیک اشاره کرد.

در پدافند عامل مثل سیستم‌های ضد هوایی و هواپیماهای رهگیر، فقط نیروهای مسلح مسئولیت دارند. در حالی که در پدافند غیرعامل تمام نهادها، نیروها، سازمان‌ها، صنایع و حتی مردم عادی می‌توانند نقش مؤثری بر عهده گیرند

دفاع غیرعامل در واقع مجموعه تمهیدات ،اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد . چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب‌دیده را با کم‌ترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد، ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارآیی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

با پیچیده‌تر شدن جنگ‌ها و به کارگیری تکنولوژی و فن‌آوری در جنگ‌های نوین، پدافند غیر عامل نیز چهره‌های متفاوتی را به خود گرفته است. امروزه مردم برای ادامه زندگی نیازمند خدمات متفاوتی هستند و احتیاج به محیط آرام و قابل سکونت درون شهرها دارند و بایستی ایمنی و آسایش کافی داشته باشند.

درحال حاضر عمده‌ترین هدف پدافند غیرعامل، ایمن سازی و کاهش آسیب‌پذیری زیرساخت‌های مورد نیاز مردم است تا به تدریج شرایطی را برای امنیت ایجاد نماید. این گونه اقدامات مهم در اکثر کشورهای دنیا انجام شده و یا در حال اقدام است. این اقدامات اگر به صورت یک برنامه ریزی و با طراحی در توسعه کشور(توسعه پایدار) نهادینه شود، خودبه‌خود بسیاری از زیر ساخت‌هایی که ایجاد

می‌شود، در ذات خود ایمنی خواهند داشت . برای اصلاح زیرساخت‌های فعلی هم می‌توان با ارائه راهکارهایی مثل مهندسی مجدد، آن‌ها را مستحکم کرد.

اهداف پدافند غیرعامل:

- کاهش قابلیت و توانایی سامانه‌های شناسایی، هدف یابی و دقت هدف‌گیری تسلیحات آفندی دشمن.

- بالا بردن قابلیت بقا، استمرار عملیات و فعالیت‌های حیاتی و خدمات رسانی مراکز حیاتی، حساس و مهم نظامی و غیر نظامی کشور در شرایط وقوع تهدید، بحران و جنگ.

- تقلیل آسیب‌پذیری و کاهش خسارت و صدمات تاسیسات، تجهیزات و نیروی انسانی مراکز حیاتی، حساس و مهم نظامی و غیر نظامی کشور در برابر تهدیدات و عملیات دشمن.

- سلب آزادی و ابتکار عمل از دشمن.

- صرفه جوئی در هزینه‌های تسلیحاتی و نیروی انسانی.

- فریب و تحمیل هزینه بیش‌تر به دشمن و تقویت بازدارندگی.

- افزایش آستانه مقاومت مردم و نیروی خودی در برابر تهاجمات دشمن.

-حفظ روحیه و انسجام وحدت ملی و حفظ سرمایه‌های ملی کشور.

- حفظ تمامیت ارضی، امنیت ملی و استقلال کشور. (padafand-gh-amel. persianblog. ir)

۲-۳-۱- امنیت دیجیتال

امنیت دیجیتال عبارت است از قابلیت اعتماد به تولید کنندگان ابزار دیجیتال که برای حفظ محرمانگی و یکپارچگی و دسترس پذیر بودن این ابزار اقداماتی را انجام داده‌اند تا در عین این که افراد مجاز به آن بتوانند دسترسی داشته باشد افراد غیر مجاز قادر به دست‌یابی و استفاده سو از آن‌ها نباشند.

۲-۳-۲- ایمنی سرمایه‌های دیجیتال

ایمنی سرمایه‌های دیجیتال به امن نگهداشتن این سرمایه‌ها در مقابل انواع تهدیدات سخت و نیمه سخت و نرم‌افزاری می‌پردازد . با توجه به این که هر سیستمی برای ادامه بقا خود نیازمند به ایمن بودن دارد می‌بایست با تحلیل هزینه – فایده موارد تامین ایمنی هرکدام از سرمایه‌های دیجیتال مورد تجزیه و تحلیل و بررسی قرار گرفته و به‌ترین و سودمندترین روش را که با به صرفه بودن همراه است انتخاب و به کارگیری گردد.

۲-۳-۳- پایداری سامانه‌های دیجیتال

در تامین سیستم دفاعی کامل علاوه بر مد نظر داشتن امنیت و ایمنی باید به استمرار قابلیت ادامه حیات این سرمایه‌ها نیز عنایت نمود. یکی از این نکات مهم قابلیت ارائه خدمات دیجیتال در مراکز مهم ، حساس و حیاتی می‌باشد. این قابلیت زمانی می‌تواند وجود داشته باشد که در صورت حمله به این مراکز و به خطر افتادن امنیت و یا ایمنی سرمایه‌های دیجیتال همچنان بتوانند به حیات خود ادامه دهند و در این زمینه پایداری لازم را داشته باشند. بدون پایداری به مجرد به خطر افتادن امنیت و ایمنی کل سرمایه دیجیتال با خطر از بین رفتن روبرو خواهد شد.

۲-۴- سابقه پدافند غیر عامل فاوا

می‌توان ادعا نمود که قدمت پدافند غیر عامل به قدمت تمدن بشری باز می‌گردد. لیکن این موضوع برای نسل‌های بشر به صورت تلاش آن‌ها برای حراست و مراقبت در برابر دشمنان طبیعی و انسانی نمایان شده است و در طول تاریخ همواره تمهیداتی را برای در امان ماندن از این حوادث مد نظر داشته است . برج و باروهای حفاظتی شهرها ، قلعه‌ها و حصارها نمونه‌های بارزی در این خصوص می‌باشند.

در عصر جدید با توجه به مقتضیات عالم جدید و ایجاد دولت‌ها، این موضوع از حیطه شهری به گستره ملی انتقال پیدا نمود. با بروز جنگ جهانی اول و دوم و کشیده شدن پای جنگ به شهرها این موضوع اهمیت بیشتری یافت و شکل علنی به خود گرفت. پس از آن جنگ سرد و چالش‌های جهانی مرتبط با

سلاح‌های کشتار جمعی اهمیت این بحث را بیشتر نمود. در نهایت با وقوع حادثه ۱۱ سپتامبر و جنگ‌های دهه اخیر بین کشورها، این مبحث وارد فاز جدیدی از مطالعات و برنامه‌های اجرایی شد.

جایگاه پدافند غیر عامل در قانون برنامه چهارم توسعه:

هیات وزیران در سال ۱۳۸۴آئین نامه اجرائی بند پ تبصره ۱۷ قانون بودجه سال ۸۴ کل کشور را به تصویب رسانده و در فصل ۱۰ این قانون که قوانین مرتبط با امنیت ملی مطرح شده است و در بند ۱۱ ماده ۱۲۱ به موضوع پدافند غیر عامل اشاره دارد و مطابق متن زیر مواردی را در این خصوص برای خود لازم الاجرا نموده است.

رعایت اصول پدافند غیر عامل درطراحی و اجرای طرح‌های حساس و مهم و در دست مطالعه و نیز تأسیسات زیربنایی و ساختمان‌های حساس و شریان‌های اصلی و حیاتی کشور و آموزش عمومی مردم توسط دستگاه‌های اجرایی و تخصصی موضوع ماده (۱۶۰) قانون برنامه چهارم توسعه، به منظور پیش‌گیری و کاهش مخاطرات ناشی از سوانح غیرطبیعی مد نظر بوده و این دستگاه‌ها موظف‌اند بر اساس سیاست‌ها ،الویت‌هاو دستورالعمل‌های کارگروه دائمی پدافند غیر عامل کشور درصدی از اعتبارات تملک دارائی‌های سرمایه‌ای خود راجهت اجرای طرح‌های مصوب کارگروه اختصاص دهند. بر اساس این قانون کمیته‌های دائمی پدافند غیر عامل در دستگاه‌های اجرائی و تخصصی کشور به منظور اجرائی کردن اهداف پدافند غیر عامل تشکیل و فعالیت خواهند داشت.

هم‌چنین در مهر ماه سال ۸۶ سندی را با عنوان سند راهبردی پدافند غیرعامل کشورتوسط مجمع تشخیص مصلحت نظام تهیه و به تصویب رسانده شده، که بخش عمده‌ای از طرح جامع پدافند غیر عامل کشور در آن پیش‌بینی شده است که شامل چشم‌انداز و همسو با چشم‌انداز ۲۰ ساله، اهداف کلان و بلند مدت، اهداف کوتاه مدت، سیاست‌های اجرایی و راهبردی می‌باشد.

تلاش برای توسعه پایدار کشور و تحقق اهداف چشم‌انداز ۲۰ ساله توسعه‌ای کشور ایجاب می‌کند، که عنصر پدافند غیر عامل که به معنی ارزیابی آسیب‌پذیرها و تهدیدهای احتمالی و برنامه ریزی برای

حذف این موارد در اجرای طرح‌های اقتصادی ،اجتماعی و توسعه‌ای کشور است، مورد توجه ویژه قرار گیرد.

موارد زیر اشاره به برخی موارد در خصوص تامین بودجه در سال ۸۶ در بخش پدافند غیر عامل با توجه به اهمیت موضوع دارد که در سال (۸۷)نیز این اعتبارات به صورت تکمیلی‌تر در قانون بودجه کشور لحاظ شده است:

۱) تبصره ۲۰ بند ر، بخش ششم از قانون بودجه سال ۸۶

بند "ر" ـ در اجرا طرح‌های پدافند غیرعامل و انسداد مرزها با اولویت مرز شرقی اجازه داده می‌شود ،حداکثر مبلغ دو هزار و هشتصد و هفتاد و چهار میلیارد ریال اعتبار ردیف ۵۰۳۹۱۸ قسمت چهارم و ۲۰۲۰۱۰۲۴ پیوست شماره یک این قانون براساس پیش‌نهاد دستگاه‌های اجرایی و تصویب کمیته دائمی پدافند غیرعامل کل کشور در خصوص اعتبار ردیف ۵۰۳۹۱۸ پدافند غیرعامل در اختیار دستگاه‌های اجرائی ذی‌ربط قرارگیرد تا براساس شرح عملیات موافقتنامه مبادله شده با سازمان مدیریت و برنامه‌ریزی کشور به مصرف برسد. این اعتبارات از شمول قانون محاسبات عمومی و سایر مقررات کشور مستثنی می‌باشد.

۲) تبصره ۱۷ بند د، بخش ششم از قانون بودجه ۸۶

بند"د" ـ در اجرای طرح‌های پدافند غیر عامل موضوع آئین‌نامه اجرایی بند (۱۱) ماده (۱۲۱) قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران اجازه داده می‌شود حداکثر مبلغ چهارصد و چهل میلیارد ریال اعتبار ردیف ۵۰۳۹۱۸ قسمت چهارم این قانون، براساس پیش‌نهاد دستگاه‌های اجرایی و تصویب کمیته دائمی پدافند غیرعامل کل کشور در اختیار دستگاه‌های اجرایی ذی‌ربط قرار گیرد تا براساس شرح عملیات موافقتنامه مبادله شده با سازمان مدیریت و برنامه‌ریزی کشور (معاونت برنامه ریزی و نظارت راهبردی ریاست جمهوری) به مصرف برسد.

جایگاه فنی پدافند غیر عامل:

ریشه بحث‌های پدافند غیر عامل به نیازهای انسان برای زندگی بر می‌گردد ، با مروری بر هرم نیازهای انسانی، نقش بسیار مهم خواسته ایمنی و امنیت آشکار است. پدافند غیر عامل به منظور تامین ایمنی و امنیت انسان در برابر پتانسیل‌های بروز خطر، می‌باشد. از طرفی دیگر پدافند غیر عامل را می‌توان از زاویه مدیریت بحران مورد تحلیل قرار داد، در این صورت شناسایی پتانسیل‌های بحران خیزی ، نحوه مدیریت و کنترل بحران به عنوان ورودی‌های سیستم‌های پدافند غیر عامل شناخته می‌شوند.

هم‌چنین پدافند غیر عامل را از زاویه دید آسیب‌پذیری نیز مورد بررسی قرار می‌دهند، که در این صورت شناخت جایگاه‌هایی که به عنوان نقطه ضعف سیستم می‌باشند، به عنوان ورودی‌های سیستم بوده. ضلع دیگر مباحث پدافند غیر عامل بحث‌های ایجاد ایمنی و امنیت عمومی می‌باشد که به صورت آموزش و همکاری همگانی تبلور می‌یابد.

اهمیت،ضرورت و اهداف پدافند غیرعامل

برابر آمار سرشماری سال ۱۳۷۸، تعداد شهرهای کشور ۶۰۰ و تعداد روستاهای آن ۶۵۰۰ روستا بوده است، پدافند هوائی مراکز حیاتی و حساس موجود کشور در شهرها صرفاً با توپ ضد هوائی ۲۳ میلیمتری، نیازمند ۲۴۰۰۰۰ قبضه توپ، یک میلیون و دویست هزار نفر نیروی انسانی (خدمه)، ۳۰۰۰۰ آتشبار و ۷۵۰ گردان ویژ پدافند هوایی خواهد بود که امکان تامین، تشکیل، سازماندهی و پشتیبانی آن دور از دسترس می‌باشد.

دفاع غیرعامل در واقع مجموعه تمهیدات ،اقدامات و طرح‌هایی است که با استفاده از ابزار، شرایط و حتی‌المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت‌گیرد . چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب‌دیده را با کم‌ترین هزینه فراهم می‌سازد. در حقیقت طرح‌های پدافند غیرعامل قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیه چنین طرح‌هایی فراهم می‌گردد،ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ

گردند. به‌کارگیری تمهیدات و ملاحظات پدافند غیرعامل علاوه برکاهش شدید هزینه‌ها، کارآیی دفاعی طرح‌ها، اهداف و پروژه‌ها را در زمان تهاجم دشمن بسیار افزایش خواهد داد.

امروزه با توجه به توسعه فاوا در کلیه امور زندگی انسان‌ها باید به این نکته توجه داشت که وارد عصر جدیدی از زندگی شده و می‌بایست با نگاه جدیدی به پدافند غیر عامل نگریست. باید باز تعریف جدیدی از امنیت و ایمنی و پایداری در عرصه فاوا ارائه نمود. این مطلب در برنامه چهارم توسعه به خوبی خود را نشان داده است . با توجه به این که بسیاری از ارکان زندگی در عصر حاضر با فاوا گره خورده است بدون در نظر گرفتن این مسئله عملاً بسیاری از اقدامات در زمینه پدافند غیر عامل می‌تواند به هدر رفته و هدف اصلی از دیده‌ها پنهان گردد.

۲-۵- مفاهیم امنیت در فاوا

با توجه به روند جنگ‌ها و شرایط حال حاضر دنیا(چه از لحاظ تکنولوژیکی و چه از لحاظ سیاست‌های راهبردی) رویکردهای زیر برطرح پدافند غیرعامل حاکم است:

۱- به عنوان یک فرض مسلم و قطعی، پرداختن و توجه ویژه به مقوله پدافند غیرعامل از لحاظ کمی و کیفی و بررسی سامانه‌هایی که می‌بایست مورد توجه پدافند غیرعامل قرارگیرند، نقش مهم و ارزشمندی را در تعیین سرنوشت جنگ بر عهده خواهد داشت.

۲- نظر به اهمیت در خور توجه و بایسته پدافند غیرعامل و سامانه‌های آن، وحدت فرماندهی و هماهنگی در خصوص نحوه و چگونگی اجرا، هدایت و راهبرد عملیات استتاری در سطوح عمودی و افقی نیروهای مسلح کشور و سایر منابع ملی، لازمه موفقیت در عملیات‌های پدافند غیرعامل و کارآمدی مدیریت راهبردی این نوع پدافند مبتنی برشیوه‌های نوین است .

۳- بدون شک پیشرفت‌های روز افزون در حوزه‌های ارتباطات، مخابرات و سیستم‌های شناسایی و جمع‌آوری اطلاعات، تغییرات قابل توجهی را در مکانیسم‌ها و ساز و کارهای حاکم بر فعالیت‌ها و

چالش‌های نظامی و دفاعی به وجود آورده‌است. هم‌چنین شرایط حاضر جهانی بسیار متغییر بوده و روند رو به رشد سیستم‌های مزبور بسیار شتاب‌آلود و سریع است.

۴- از آنجا که روش‌های طراحی، مراقبت و نگهداری، برنامه‌ریزی و توسعه میدانی در پدافند غیرعامل نوین با توجه شرایط و نحوه رویارویی و تقابل با دشمن از نظر سیاسی و جغرافیایی متفاوت است، تنوع شرایط و راهکارها، انعطاف و پویایی مفهوم فرماندهی وکنترل عملیات پدافند غیرعامل را در پی دارد.

۲-۵-۱- تهدیدات سیستم‌های ارتباطی از منظر پدافند

همان گونه که در مغز انسان ارتباطات عصبی و انتقال اطلاعات از طریق تارهای عصبی و نرون‌ها برقرار می‌شود و به مجرد آسیب رسانی به هر کدام از این تارها ، تار دیگری این وظیفه را بر عهده می‌گیرد. در دنیای فاوا نیز سیستم‌های ارتباطی مختلفی برای تعامل و انتقال اطلاعات به کار گرفته می‌شوند. در صورت آسیب رسانی به هر کدام از این سیستم‌های ارتباطی در صورت عدم وجود سیستم ارتباطی جایگزین ادامه حیات ابزار دیجیتال و انتقال اطلاعات میسر نخواهد بود. آسیب‌پذیری‌های که سیستم‌های ارتباطی را تهدید می‌نمایند به دنبال هدف از بین بردن تعاملات اطلاعاتی بوده و اصل اشرافیت بر اطلاعات را منظور نظر خود قرار می‌دهند.

۲-۵-۲- تهدیدات سیستم‌های رایانه‌ای با نگاه پدافندی

سیستم‌های رایانه‌ای از جمله سیستم‌های می‌باشند که از راه دور و نزدیک و با استفاده از ابزار دیجیتال و آنالوگ قابلیت تهدید پذیری دارند. در صورت تبدیل هر کدام از این تهدیدات از بالقوه به بالفعل عملاً ادامه عمل‌کرد سیستم‌های رایانه‌ای امکان پذیر نبوده و با اختلال مواجه خواهد شد. با توجه به این که در عصر حاضر بسیاری از روش‌های زندگی بر مبنای به کار گیری این ابزار پایه گذاری شده است ، آسیب‌پذیری ابزار دیجیتال منجر به آسیب رسانی به امنیت و ایمنی و پایداری بقا انسان‌ها خواهد شد.

۲-۵-۳- تهدیدات سیستم‌های اطلاعاتی مبتنی بر رایانه در پدافند غیر عامل

سیستم‌های اطلاعاتی مبتنی بر رایانه[۱] از انواع مختلفی تشکیل شده است . کوچک‌ترین این سیستم‌ها بانک اطلاعات می‌باشد که در ابعاد بزرگ و کوچک توسط سازمان‌ها و شرکت‌ها و موسسات و حتی افراد به صورت خصوصی به کار گرفته می‌شوند. هر چه سیستم گسترده می‌شود سیستم‌های تصمیم گیری[۲] به آن اضافه شده و برخی از تصمیم‌گیری‌ها روشمند شده و توسط سیستم‌ها انجام و اعمال می‌گردد. عملاً کنترل بسیاری از ابزار دیجیتال به صورت روزمره به این گونه از سیستم‌ها واگذار می‌شود و هر کس که بتواند آگاهانه یا نا آگاهانه به این سیستم‌ها دسترسی داشته و بر آن اثر گذار باشد این قابلیت را خواهد داشت تا بر خروجی سیستم نیز اثر گذار باشد. به همین دلیل امن نگه داشتن این سیستم‌ها به منزله امن نگه داشتن کل فرآیند می‌باشد.

---

۱) CBIS) computer based information system

۲ (DSS) decision support system

۲-۶- سئوالات خودآزمایی

فاوا مخفف چیست ؟ توضیح دهید.

اصول کلی پدافند غیرعامل را نام برده و توضیح دهید.

پدافند غیر عامل در حوزه فاوا را توضیح دهید.

سابقه پدافند غیرعامل فاوا در ایران را بنویسید.

تهدیدات سیستم‌های ارتباطی از منظر فاوا کدامند؟ توضیح دهید.

تهدیدات سیستم‌های رایانه‌ای از منظر فاوا کدامند؟ توضیح دهید.

تهدیدات سیستم‌های اطلاعاتی مبتنی بر رایانه از منظر فاوا کدامند؟ توضیح دهید.

فصل سوم - اصول ممیزی و ارزیابی

۳-۱- هدف این فصل

در این فصل در بخش اول اهمیت روند ارزیابی و ممیزی امنیتی و جایگاه روند ممیزی در چرخه امنیتی سازمان تشریح می‌گردد. در ادامه در بخش دوم اصول کلی فرایند ممیزی و ارزیابی و مراحل موجود در آن از نقطه نظر مدیریتی تشریح می‌گردد. جهت انجام این کار باید اقدامات مختلفی از قبیل فعالیت‌های مقدماتی ممیزی، آماده سازی برای انجام فعالیت‌های ممیزی در محل، انجام فعالیت‌های ممیزی در محل و تهیه و تصویب و توزیع گزارش ممیزی انجام گیرد.

انتظار می‌رود در پایان این فصل خواننده بتواند مفاهیم زیر را درک نموده و قادر به تشریح نکات فنی مرتبط با آن‌ها باشد:

- علل و ضرورت انجام روند ممیزی و ارزیابی
- کلیات روند ممیزی و ارزیابی و مراحل موجود در آن
- نحوه مدیریت یک برنامه ممیزی

۳-۲-مقدمه

اطلاعات به سرمایه‌هائی اطلاق می‌شود که برای سازمان مربوطه دارای ارزش می‌باشند. بنابراین باید به‌طور مناسب محافظت شوند. در حقیقت می‌توان گفت که اطلاعات به‌عنوان مبنائی است که سازمان بر اساس آن فعالیت‌های تجاری خود را انجام می‌دهد.

هدف از امنیت اطلاعات، محافظت مناسب از مجموعه اطلاعات سازمان و رونده‌ای تجاری‌ای که سازمان مربوطه آن‌ها را پشتیبانی می‌کند در موارد زیر می‌باشد:

محرمانگی: اطلاعات تنها برای افرادی که مجاز به دسترسی به آن‌ها می‌باشند، قابل دسترسی باشد.

تمامیت: اطمینان داشتن از صحیح و کامل بودن اطلاعات و روش‌های پردازش آن‌ها.

در دسترس بودن: اطلاعات و مجموعه وابسته به آن در هنگام نیاز کاربران مجاز، در دسترس آن‌ها قرار داشته باشد.

برای رسیدن به این هدف، استانداردهای امنیتی مختلفی به‌وجود آمده است که اغلب بر اساس آن‌ها، روندها و روال‌های امنیتی برای سازمان مربوطه تهیه شده و پیاده سازی می‌شوند. یکی از مهم‌ترین رونده‌ای استفاده شده برای این منظور استفاده از چرخه بهبود (PDCA) می‌باشد که در ادامه به‌طور مختصر شرح داده می‌شود.

در این چرخه، چهار مرحله اصلی وجود دارد که عبارتند از:

- مرحله برنامه ریزی (Plan)

این فاز در واقع مرحله طراحی و مشخص شدن تعاریف اولیه پیاده‌سازی مدیریت امنیت اطلاعات سازمان است. سیاست‌های امنیتی، مقاصد، پردازش‌های مختلف درون سازمانی و روتین‌های عملیاتی، و . . . در این مرحله تعریف می‌شوند .

- مرحله پیاده سازی (DO)

پیاده‌سازی و اجرای سیاست‌های امنیتی، کنترل‌ها و پردازش‌ها در این مرحله انجام می‌شوند. در واقع در این مرحله کلیه تعاریف فاز اول اجرا می‌شوند.

- مرحله ارزیابی (CHECK)

این مرحله را می‌توان فاز ارزیابی نیز نامید. در این مرحله ارزیابی موفقیت پیاده‌سازی سیاست‌های مختلف امنیتی، تجربه‌های عملی و گزارش‌های مدیریتی گردآوری خواهند شد. مرور نتایج ما را در جهت پیدا کردن دیدی به‌تر رهنمون می‌سازد.

- مرحله ترمیم و بازنگری (ACT)

اجرای موارد ترمیمی و بازنگری در نحوه مدیریت اطلاعات، هم‌چنین تصحیح موارد مختلف در این فاز انجام می‌شود.

پس از پایان عملیات فاز چهار دوباره به فاز اول یعنی مرحله برنامه ریزی بازگشته و با تعریف سیاست‌های جدید مورد نیاز، مراحل بعدی پی گرفته می‌شود. با توجه به تعاریف ارائه شده در بالا، عملیات فوق فرآیندی چرخشی و پویا است که با تغییرات درون سازمانی امکان تصحیح در مدیریت اطلاعات همواره وجود دارد.

همان‌طور که در این فرآیند نیز مشخص است، روند ارزیابی و ممیزی امنیتی به‌عنوان یکی از مراحل مهم موجود در چرخه بهبود امنیت اطلاعات سازمان در نظر گرفته شده و باید بر طبق یک برنامه منظم و مداوم انجام شود. در حقیقت اجرای دقیق و مداوم روند ارزیابی و ممیزی باعث می‌شود این اطمینان برای مدیران ارشد سازمان ایجاد گردد که روندها و کنترل‌های امنیتی پیاده سازی شده در سازمان بر طبق برنامه در حال اجرا بوده و آسیب‌پذیری‌ها و نقاط ضعف امنیتی احتمالی نیز توسط این روند استخراج گشته و به‌طور مناسبی کنترل می‌شوند.

نکته‌ای که باید در اینجا یادآوری شود این است که با توجه به این که روند طراحی و پیاده سازی صورت گرفته به منظور ایجاد امنیت مناسب، بر اساس استانداردهای امنیتی بوده، در نتیجه برای اجرای روند ارزیابی و ممیزی امنیتی سازمان نیز باید بر اساس استانداردهای امنیتی مناسب عمل نمود.

۳-۳-اهمیت روند ممیزی و ارزیابی امنیتی

هدف از انجام ممیزی، مشخص نمودن عیب‌هایی است که از چشم سازمان به دور مانده و هدف، کمک به سازمان در جهت یافتن عیوب مذکور است؛

ممیزی باید برای سازمان‌ها ارزش افزوده داشته باشد. در حقیقت پس از این که برنامه مشخصی جهت امن سازی سازمان تعیین گردید و روند پیاده سازی و امن سازی تجهیزات و سامانه‌های موجود در سازمان بر اساس آن روند اجرا گردید، باید جهت اطمینان از اجرای مناسب روند امن سازی و تعیین و

استخراج نقاط ضعف و آسیب‌پذیری‌های امنیتی که احتمالاً در طول روند امن سازی مخفی مانده‌اند، روند ممیزی و ارزیابی امنیتی اجرا گردد.

از فواید دیگر اجرای روند ممیزی و ارزیابی امنیتی، حصول اطمینان از پیاده سازی صحیح و کامل کنترل‌ها و راه کارهای امنیتی پیش‌نهاد شده در طرح امنیتی سازمان می‌باشد. به این معنی که امکان دارد جهت برطرف نمودن نقاط ضعف و آسیب‌پذیری‌های امنیتی استخراج شده در فاز طراحی کنترل‌های مناسبی تعیین شده باشند اما در هنگام پیاده سازی آن کنترل‌ها به دلایل مختلف از جمله سهل انگاری مجریان، عدم آشنایی کافی با مسایل تکنیکی و فنی و مسایل عملیاتی و مدیریتی، به نحو مطلوبی پیاده سازی نشده باشند که خود این مسئله می‌تواند باعث ایجاد مشکلات امنیتی گردد.

بدیهی است ممیزی به عنوان یک ابزار قوی و مهم در فراهم آوری اطلاعات نسبت به عمل‌کرد اثربخشی و میزان کارایی فرآیندها در سیستم مدیریت مورد توجه قرار می‌گیرد و از آن جا که ممیزی فرآیندی است که به دنبال یافتن انطباق‌های موجود در یک سازمان، با استانداردهای مورد نظر می‌باشد، باید در کمال صحت و دقت و به دور از هرگونه خطا و اشتباه صورت گیرد. فرآیند ممیزی از یک سو اعتبار سازمان ممیزی کننده را حفظ می‌کند و از دیگر سو به سازمان ممیزی شونده نیز در جهت رسیدن به اهدافش یاری می‌رساند.

۳-۳-۱-چرا باید امن سازی مورد ممیزی قرار گیرد؟

هدف از ممیزی امنیتی مقایسه اقدامات جاری با بهترین روش انجام اقدامات موجود است. به‌واسطه این مقایسه، یک ممیزی خوب می‌تواند به دنبال شکاف‌ها و رخنه‌ها (که در خطمشی، روال یا فن‌آوری رخ داده) در فعالیت‌های فعلی شما بگردد و سپس آن‌ها را به منظور ارائه توصیه‌های پایه‌ای و زیر بنایی برای بهبود بخشیدن سطوح امنیتی سوق دهد.

به طور خلاصه ممیزی یکی از معدود راه‌های جستجوی تمام و کمال و تعریف چگونگی امن سازی یک دارایی خاص می‌باشد.

به‌طور کلی اجرای روند ممیزی به دو صورت قابل انجام می‌باشد:

- اجرای ممیزی با استفاده از کارشناسان داخل سازمان (ممیزی داخلی)
- استفاده از کارشناسان خارج سازمان (ممیزی خارجی)

البته ممیزی کردن به صورت داخلی و به صورت خارجی دارای نکات مثبت و منفی خود هستند. که در جدول زیر به برخی از آن‌ها اشاره شده است.

جدول (۱) نکات مثبت و منفی انجام ممیزی به صورت داخلی و خارجی

نکات مثبت

- مقرون به صرفه
- دارای موانع سیاسی و فرهنگی محدود
- دانش روال‌های موجود
- مستقل و هدفمند
- سال‌ها تجربه عملی در ممیزی
- دارای گواهی‌نامه (برای سازگاری با قوانین)

نکات منفی

- اتلاف منابع و وقت سازمان
- عدم آگاهی کارکنان از به‌ترین روش‌های ممیزی
- بسیار هزینه بر است

- فقط خطاهایی که از قبل در خصوص آن‌ها توافق شده است را گزارش می‌کند
- مقاومت و عدم همکاری کارکنان

درباره اهداف ممیزی می‌توان گفت که ممیزی باعث هوشیاری افرادی می‌شود که مستمر اشتباه مرتکب شده‌اند. مهم‌تر این که مشکلات پنهان سازمان نیز آشکار می‌گردد.

مواردی که موجب کاهش ارزش ممیزی می‌شوند عبارتند از:

- نبود تعهد مدیریت ممیزی شونده؛

- نبود آگاهی مدیریت از ممیزی؛

- مشغول بودن بیش از حد پرسنل ممیزی شونده؛

- ممیزانی که آموزش‌های لازم را ندیده‌اند.

چنان چه ممیزی روی اصول مناسب اجرا نشود، باعث می‌شود تا مشکلات افزایش یابد در حالی که هیچ‌کس متوجه این افزایش نیست از طرفی افراد ایمان خود به کیفیت را از دست می‌دهند.

اما آن‌چه که باعث افزایش ارزش ممیزی در یک سازمان می‌شود عبارتند از:

مستقل بودن ممیزین، کنجکاوی، سرسختی، نگرش کلی به سیستم تا تمرکز بر روی فرآیندها و ارتباط میان فرآیندها.

به طور کلی کم‌تجربگی ممیزان می‌تواند فرآیند را آسیب برساند این در حالی است که در بسیاری از موارد برای حل مشکلات باید دلایل مشکلات ریشه‌ای نه سطحی بررسی شود. در بسیاری مواقع اقدامات اصلاحی در یک سازمان به طور محدود صورت می‌گیرد به همین علت است که در برخی اوقات یافته‌های ممیزی توسط ممیزی شونده پذیرفته نمی‌شود.

نتایج مطلوب حاصل از اجرای روند ممیزی می‌تواند شامل موارد زیر باشد:

- استفاده از تحلیل علل ریشه‌ای و ارتقای آن

- توجه بیش‌تر به نتایج ممیزی و اقدامات صورت گرفته

- یاری رساندن به سازمان در فراهم آوردن منابع

مسلماً اجرای ممیزی داخلی مناسب در هر سازمان، باعث تقویت سیستم مدیریت کیفیت شده و اجرای پرقدرت ممیزی داخلی نقاط ضعف سیستم فعلی را مشخص می‌سازد. در این راستا متأسفانه در بسیاری از سازمان‌ها شاهد بوده‌ایم که ممیزی داخلی به روش درستی صورت نگرفته و اثربخشی لازمه را ندارد. بنابراین سیستم مدیریت کیفیت سازمان به درستی تجزیه و تحلیل نشده و نقاط بهبود زا و نیز مشکل‌دار مشخص نمی‌گردد. مسلماً در این حالت پس از مدتی سیستم کرخت شده و نسبت به ممیزی داخلی بی‌انگیزه می‌گردد و از طرف دیگر مجموعه این عوامل باعث شده تا در ممیزی مراقبتی مشکلات زیادی به وجود آید.

۳-۳-۲تجزیه و تحلیل ممیزی داخلی با استفاده از نگرش فرآیندی

از دیدگاه سیستمی می‌توان گفت که هر فرآیند، بخش اساسی یک نظام (سیستم) را تشکیل می‌دهد که وظیفه و مأموریت اساسی آن نظام، یعنی تبدیل ورودی یا ورودی‌هایی خاص را به خروجی یا خروجی‌هایی خاص، به انجام می‌رساند. به هر فرآیند می‌توان از زاویه یک «زنجیره ارزش» نگاه کرد. در هر فرآیند، هر مرحله کار یا هر گامی که در جهت تولید محصول یا ارائه خدمت برداشت می‌شود باید بتوانند با ایجاد ارزش افزوده جدید، ارزش مراحل یا گام‌های قبل از خود را افزون کند. بنابراین توجه به فرآیند عملیات سازمان می‌تواند بسیار مفید باشد. عمل‌کرد اثربخش سازمان‌ها درگرو این است که فرآیندهای مرتبط و موثر بر هم متعددی را شناسایی و اداره کنند. در این راستا می‌توان ممیزی داخلی را نیز به صورت یک فرآیند با ورودی‌ها و خروجی‌های مشخص، در نظر گرفت. طبق شکل شماره ۱ پس از بررسی، مشخص می‌شود که اجزای فرآیند ممیزی داخلی عبارتند از:

- ورودی‌های پروسه برنامه‌ریزی: وضعیت و اهمیت فرآیندها، برنامه کلان ممیزی، نتایج ممیزی‌های قبلی، لیست میزان داخلی واحدهای مختلف، برنامه کاری واحدهای مختلف، نتایج شاخص‌های پایش فرآیندها، نتایج اقدامات اصلاحی و شکایات

- ورودی‌های پروسه انجام ممیزی: چک لیست ممیزی، ممیزی شونده، برنامه نهایی ممیزی، استاندارد مرجع

- خروجی‌ها: اجرای ممیزی داخلی اثربخش، گزارشات ممیزی و تعیین اقدامات اصلاحی

حال با توجه به مشخص شدن ورودی‌های فرآیند، می‌توان ممیزی داخلی را تجزیه و تحلیل کرد. در واقع ورودی‌های فرآیند در خروجی تأثیر مستقیم داشته و در صورت با کیفیت بودن و مناسب بودن ورودی‌ها، حتماً خروجی مناسب با ممیزی داخلی قابل قبولی خواهیم داشت. در این راستا با تجزیه و تحلیل ورودی‌ها، نقاط ضعف ممیزی داخلی نیز مشخص می‌گردد.

موارد زیر نقاط ضعف و شکست در ممیزی داخلی تلقی می‌شوند:

۱- عدم داشتن مهارت و دانش کافی برای ممیزی داخلی

۲- نبود انگیزه کافی برای ممیزین در ممیزی داخلی

راهکار: اجرای سیستم تشویقی و پاداش دهی که باید متناسب با موقعیت و شغل ممیز، متناسب با تعداد جلسات ممیزی و نیز متناسب با اثربخشی و کارآمدی جلسه ممیزی باشد.

۳- نبود چک لیست‌های مناسب ممیزی

این باعث می‌شود تا ممیزی با سرعت و بدون عمق لازم انجام شود.

راهکار: تهیه یک چک لیست جامع، قبل از انجام ممیزی تا به الزامات سازمانی، مشتری و الزامات دولتی توجه لازم شود.

۴- ثابت بودن پرسش‌های ممیزی و تکراری شدن آن‌ها برای واحدها

راهکار: تدوین پرسش‌های جدید.

۵- مناسب نبودن گزارش‌های ممیزی

راهکار: برای رفع این ضعف باید دامنه ممیزی، کارفرمای ممیزی، رهبر تیم ممیزی، معیارها، یافته‌ها و تمام نقاط ضعف واحدها مشخص شود تا بتوان نتیجه گیری کاملی ارائه کرد.

۶- ثابت بودن برنامه کلان ممیزی بدون توجه به مشکلات واحدها

راهکار: نماینده مدیریت در سیستم مدیریت کیفیت باید به مواردی چون، تعداد مغایرت‌های واحد در ممیزی قبلی داخلی و ممیزی قبلی مراقبتی و نیز تعویض مدیریت یک واحد، تعداد شکایت‌ها و تعداد اقدامات اصلاحی و پیش‌گیرانه توجه کند.

۳-۴-کلیات یک برنامه ممیزی

در ادامه ابتدا کلیات یک برنامه ممیزی از نقطه نظر مدیریتی تشریح می‌گردد. همانند کلیه روندها و روال‌های موجود در زمینه مدیریت، انجام روند ممیزی و ارزیابی امنیتی نیز نیاز به برنامه‌ریزی و تهیه ملزومات و نیازمندی‌های مختلف جهت اجرای مناسب و مفید روند ممیزی دارد. در نتیجه در ادامه ضمن تعریف مراحل مختلف موجود در این روند، فعالیت‌های مدیریتی مورد نیاز در هر مرحله تشریح می‌گردد.

۳-۴-۱-اصول ممیزی

یک برنامه ممیزی با لحاظ نمودن ملاحظاتی نظیر وضعیت و اهمیت فرآیندها و نواحی که بایستی ممیزی شوند، لازم است طراحی گردد. یعنی نتایج بازبینی‌های قبلی (در صورت انجام)، معیار ممیزی‌ها، محدوده ممیزی، تأثیر و روش‌های ممیزی بایستی تعریف شوند. گزینش و انتخاب ممیزان و انجام ممیزها بایستی تضمین کننده اهداف و بی‌طرفی فرآیند ممیزی باشد. ممیزان نبایست کارهای خودشان را ممیزی نمایند. در یک روش اجرایی مدون، بایستی مسئولیت‌ها و الزامات برنامه‌ریزی و هدایت ممیزی‌ها و گزارش نتایج و نگهداری سوابق تعریف شوند.

ممیزی بر اساس چند اصل بنا نهاده می‌شود. این اصول با فراهم آوردن اطلاعاتی که بر اساس آن‌ها یک سازمان قادر به بهبود عمل‌کرد خود می‌شود، ممیزی را تبدیل به ابزاری مؤثر و قابل اطمینان در پشتیبانی خط مشی‌ها و کنترل‌های مدیریت می‌کنند. پیروی از این اصول، پیش‌نیازی برای رسیدن به نتایج مرتبط و مناسب ممیزی، و هم‌چنین توانمند ساختن ممیزانی که به صورت مستقل از یک‌دیگر کار می‌کنند در دست‌یابی به نتایج مشابه در شرایط یکسان می‌باشد.

ممیزان باید بر مبنای اصول زیر عمل نمایند:

الف) رفتار بر پایه‌ی اصول اخلاقی: اساس یک رفتار حرفه‌ای؛ اعتماد، درستی، رازداری و خردمندی لازمه ممیزی می‌باشند.

ب) ارائه منصفانه: التزام به گزارش‌دهی مبتنی بر واقعیات و به طور دقیق یافته‌ها، نتایج و گزارش‌های ممیزی به طور دقیق و مبتنی بر واقعیات فعالیت‌های ممیزی را منعکس می‌کنند. موانع عمده‌ای که ممکن است در طول ممیزی به وجود آیند و هم‌چنین وجود هرگونه اختلاف نظر برطرف نشده بین اعضای تیم ممیزی و ممیزی شونده، گزارش می‌شوند.

ج) توجه و مراقبت متناسب با شغل: داشتن پشتکار و توانایی قضاوت مناسب در ممیزی.

ممیزان با توجه به اهمیت وظیفه‌ای که بر عهده دارند و اطمینانی که کارفرمایان ممیزی و دیگر طرف‌های ذی‌نفع به آن‌ها داشتند، توجه زیادی در انجام وظایف خود اعمال می‌کنند. داشتن صلاحیت لازم، عامل بسیار مهمی می‌باشد.

اصول دیگری با انجام ممیزی مرتبط می‌باشند، که بر پایه‌ی وجه مستقل و سیستماتیک بودن تعریف ممیزی مورد توجه قرار می‌گیرد.

د) استقلال: پایه‌ای برای بی‌طرف بودن ممیزی و موضوع‌گرا بودن نتایج ممیزی.

ممیزان از فعالیتی که ممیزی می‌شود مستقل بوده و هم‌چنین از جانب‌داری و تضاد منافع به دور می‌باشند. ممیزان در طول فرآیند ممیزی از اعمال نظر شخصی خودداری می‌کنند تا اطمینان حاصل نمایند که یافته‌ها و نتایج ممیزی صرفاً بر اساس شواهد ممیزی بنا شده‌اند.

هـ) رویکرد مبتنی بر شواهد: روشی مستدل تا بتوان به نتایج قابل اطمینان، تکرار پذیر و قابل استناد در یک فرآیند سیستماتیک ممیزی دست یافت.

شواهد ممیزی قابل تصدیق می‌باشند. با توجه به محدود بودن زمان و منابع ممیزی، این شواهد بر مبنای نمونه‌هایی از اطلاعات در دسترس بنا نهاده می‌شوند. استفاده صحیح از نمونه‌گیری ارتباط نزدیکی با سطح اطمینان نتایج ممیزی دارد.

۳-۴-۲-مدیریت یک برنامه ممیزی

۳-۴-۲-۱-کلیات

یک برنامه ممیزی بسته به اندازه، ماهیت و پیچیدگی سازمانی که قرار است ممیزی شود، ممکن است از یک یا چند ممیزی تشکیل شود. این ممیزی‌ها ممکن است اهداف متفاوتی داشته و هم‌چنین شامل ممیزی‌های مشترک یا ترکیبی شوند. علاوه بر این یک برنامه ممیزی شامل کلیه فعالیت‌های لازم برای طرح‌ریزی و سازماندهی انواع و تعداد ممیزی‌ها و هم‌چنین فراهم آوردن منابع لازم برای ممیزی‌ها به صورت کارآ و اثربخش در مدت زمان تعیین شده می‌باشد.

یک سازمان ممکن است بیش از یک برنامه ممیزی را تهیه نماید.

مدیریت ارشد سازمان بایستی وظیفه مدیریت برنامه ممیزی را به شخص واجد صلاحیت تفویض نماید.

افرادی که مسئولیت مدیریت برنامه ممیزی را بر عهده می‌گیرند، بایستی:

الف) برنامه ممیزی را تهیه، مستقر، پایش و بازنگری کرده و آن را بهبود دهند.

ب) منابع لازم را شناسایی نموده و از فراهم شدن آن‌ها اطمینان حاصل نمایند.

ممکن است دو یا چند سازمان ممیزی کننده به عنوان بخشی از برنامه‌های ممیزی‌شان، برای انجام یک ممیزی مشترک با یک‌دیگر همکاری نمایند. در چنین شرایطی بایستی توجه خاصی به تقسیم وظایف، فراهم‌سازی هرگونه منبع اضافی، صلاحیت تیم ممیزی و هم‌چنین روش‌های اجرایی مناسب معطوف شود. هرگونه توافق در مورد این مسائل بایستی پیش از شروع ممیزی حاصل گردد.

۳-۴-۳-فعالیت‌های مقدماتی ممیزی

۳-۴-۳-۱-انتصاب سرممیز

کسانی که مسئولیت مدیریت برنامه ممیزی را بر عهده دارند، بایستی فردی را به عنوان سرممیز برای ممیزی مورد نظر انتخاب کنند.

در صورتی که ممیزی به صورت مشترک انجام شود، حصول سازمان‌های ممیزی کننده به توافق در مورد مسئولیت‌های خاص هر سازمان، به خصوص در مورد اختیارات سرممیز انتخاب شده برای انجام ممیزی، پیش از آغاز ممیزی حائز اهمیت می‌باشد.

تعریف اهداف، دامنه کاربرد و معیارهای ممیزی

هر ممیزی در داخل محدوده اهداف کلی یک برنامه ممیزی، بایستی بر مبنای اهداف، دامنه کاربرد و معیارهای مدوّن بنا شده باشد.

اهداف ممیزی مشخص می‌کند که چه چیزی قرار است توسط ممیزی صورت پذیرد، و ممکن است شامل موارد زیر شوند:

الف) تعیین میزان انطباق سیستم مدیریت ممیزی شونده یا بخش‌هایی از آن با معیارهای ممیزی امنیتی از قبیل میزان محرمانگی، تمامیت و در دسترس بودن اطلاعات و سیستم‌های موجود

ب) ارزیابی قابلیت سیستم مدیریت به منظور حصول اطمینان از انطباق با الزامات قانونی، دولتی و قراردادی و استانداردهای امنیتی موجود که در سازمان مربوطه پیاده سازی شده‌اند.

ج) ارزیابی اثربخشی سیستم مدیریت در دست‌یابی به اهداف مقرر شده آن

د) شناسایی نواحی بالقوه بهبود سیستم مدیریت.

دامنه کاربرد ممیزی، محدوده و مرزهای ممیزی را از قبیل مکان‌ها، واحدهای سازمانی، فعالیت‌ها و فرآیندهایی که بایستی ممیزی شوند، و هم‌چنین بازه زمانی ممیزی را تشریح می‌کنند.

معیارهای ممیزی به عنوان مرجعی که انطباق با آن مورد بررسی قرار می‌گیرد به کار می‌روند و ممکن است شامل خط مشی‌ها، روش‌های اجرایی، استانداردها، قوانین و دستورالعمل‌ها، الزامات سیستم مدیریت، الزامات قراردادی یا مجموعه دستورالعمل‌های خاص هر بخش از صنعت / کسب و کار باشند.

اهداف ممیزی بایستی توسط کارفرمای ممیزی تعیین شوند. دامنه کاربرد و معیارهای ممیزی بایستی توسط کارفرمای ممیزی و سرممیز مطابق با روش‌های اجرایی برنامه ممیزی مشخص شوند. هرگونه تغییری در اهداف، دامنه کاربرد یا معیارهای ممیزی بایستی مورد موافقت این افراد قرار گیرد.

در صورتی که ممیزی به صورت ترکیبی انجام شود، حصول اطمینان سرممیز از تناسب اهداف، دامنه کاربرد و معیارهای ممیزی با ماهیت ممیزی ترکیبی، دارای اهمیت می‌باشد.

۳-۴-۳-۲-تعیین امکان‌پذیری انجام ممیزی

امکان‌پذیری ممیزی بایستی با در نظر گرفتن عواملی نظیر در دسترس بودن موارد زیر تعیین شود:

- اطلاعات کافی و مناسب برای طرح‌ریزی ممیزی
- همکاری مناسب از طرف ممیزی شونده
- زمان و منابع کافی.

در صورتی که انجام ممیزی امکان‌پذیر نباشد، پس از مشورت با ممیزی شونده بایستی ممیزی جای‌گزینی به کارفرمای ممیزی پیش‌نهاد شود.

۳-۴-۳-۳-انتخاب تیم ممیزی

پس از این که امکان‌پذیری انجام ممیزی به اثبات رسید، بایستی یک تیم ممیزی با در نظر گرفتن صلاحیت‌های لازم برای تحقق اهداف ممیزی تشکیل شود. در صورتی که فقط یک ممیز وجود داشته باشد، شخص ممیز بایستی کلیه وظایف یک سرممیز را انجام دهد. نکات زیر بایستی در تعیین اندازه و ترکیب تیم ممیزی مورد توجه قرار گیرند:

الف) اهداف، دامنه کاربرد، معیارها و زمان تخمین زده شده برای انجام ممیزی.

ب) این که ممیزی به صورت ترکیبی یا مشترک انجام می‌شود.

ج) صلاحیت مورد نیاز تیم ممیزی برای تحقق اهداف ممیزی.

د) الزامات قانونی، دولتی، قراردادی و تأیید اعتبار/ دریافت گواهی‌نامه، در مورد مقتضی.

ه) نیاز به حصول اطمینان از مستقل بودن تیم ممیزی از فعالیت‌هایی که قرار است ممیزی شوند و جلوگیری از تضاد منافع.

و) توانایی اعضای تیم ممیزی در برخورد مؤثر با ممیزی شونده و در همکاری با یک‌دیگر.

ز) زبان ممیزی، و درک ویژگی‌های خاص اجتماعی و فرهنگی ممیزی شونده

این موضوعات ممکن است توسط مهارت‌های شخص ممیز برآورده شده یا این که با استفاده از یک کارشناس فنی محقق شود.

فرآیند تضمین صلاحیت تیم ممیزی به استی شامل مراحل زیر باشد:

- شناسایی دانش و مهارت‌های لازم برای تحقق اهداف ممیزی
- انتخاب اعضای تیم ممیزی به گونه‌ای که کلیه دانش و مهارت‌های لازم در تیم ممیزی وجود داشته باشد.

در صورتی که دانش و مهارت‌های لازم، به طور کامل توسط ممیزان تیم ممیزی پوشش داده نشود، نیاز به استفاده از کارشناسان فنی به وجود می‌آید. این کارشناسان بایستی تحت نظارت یک ممیزی فعالیت کنند.

می‌توان از ممیزان در حال آموزش، در تیم ممیزی استفاده نمود، ولی این افراد نباید بدون نظارت یا راهنمایی به ممیزی بپردازند.

کارفرمای ممیزی و ممیزی شونده می‌توانند بر مبنای دلایل مستدل بر پایه اصول ممیزی تشریح شده، خواستار تغییر برخی از اعضای تیم ممیزی شوند. برخی از این دلایل مستدل شامل موقعیت‌هایی که در آن تضاد منافع وجود دارد (مثلاً حالتی که یکی از اعضای تیم ممیزی قبلاً از کارکنان ممیزی شونده بوده یا خدمات مشاوره‌ای برای ممیزی شونده انجام داده باشد) و رفتار غیراخلاقی ممیز در گذشته می‌باشد. این‌گونه دلایل بایستی به اطلاع سرممیز و کسانی که مسئولیت مدیریت برنامه ممیزی را بر عهده دارند رسانده شود و ایشان بایستی پیش از اتخاذ هرگونه تصمیمی در زمینه جای‌گزین نمودن اعضای تیم ممیزی، با کارفرمای ممیزی و ممیزی شونده به حل و فصل موضوع بپردازند.

۳-۴-۳-۴-برقراری تماس اولیه با ممیزی شونده

تماس اولیه با ممیزی شونده می‌تواند به صورت رسمی یا غیررسمی حاصل شود، ولی در هر حال این تماس بایستی توسط کسانی که مسئولیت مدیریت برنامه ممیزی را بر عهده دارند یا سرممیز صورت پذیرد. هدف از این تماس اولیه عبارت است از:

الف) ایجاد کانال‌های ارتباطی با نماینده ممیزی شونده

ب) تأیید اختیارات انجام ممیزی

ج) فراهم آوردن اطلاعاتی در خصوص تنظیم زمان و ترکیب تیم ممیزی پیش‌نهادی

د) درخواست دسترسی به مستندات مورد نیاز، شامل سوابق

ه) تعیین قوانین مقتضی ایمنی محل ممیزی

و) انجام هماهنگی‌های لازم برای ممیزی

ز) حصول توافق در مورد حضور شاهدان و نیاز به وجود راهنماهایی برای تیم ممیزی.

۳-۴-۳-۵-انجام بازنگری مستندات

پیش از انجام فعالیت‌های ممیزی در محل، مستندسازی ممیزی شونده بایستی به منظور تعیین انطباق سیستم مدون با معیارهای ممیزی، مورد بازنگری قرار گیرد. این مستندسازی ممکن است شامل مستندات و سوابق مربوط به سیستم مدیریت، و گزارش ممیزی‌های قبلی شود. در انجام این بازنگری نکاتی نظیر اندازه، ماهیت و پیچیدگی سازمان، و اهداف و دامنه کاربرد ممیزی بایستی مورد توجه قرار گیرند. در برخی از موقعیت‌ها، این بازنگری اگر به اثربخشی انجام ممیزی آسیبی نرساند، می‌تواند تا آغاز فعالیت‌های در محل به تعویق بیفتد. در شرایط دیگر، ممکن است یک بازدید مقدماتی از محل به منظور بررسی وضعیت اطلاعات در دسترس انجام شود.

در صورتی که نحوه مستندسازی نامناسب تشخیص داده شود، سرممیز بایستی این موضوع را به اطلاع کارفرمای ممیزی، افرادی که مسئولیت مدیریت برنامه ممیزی را بر عهده دارند، و هم‌چنین ممیزی شونده برساند. در این حالت بایستی در مورد ادامه ممیزی یا تعویق آن تا زمان برطرف شدن مشکلات مستندسازی تصمیم‌گیری شود.

۳-۴-۴-آماده سازی برای انجام فعالیت‌های ممیزی در محل

۳-۴-۴-۱-تهیه طرح ممیزی

سرممیز بایستی طرح ممیزی را به منظور به وجود آوردن مبنایی برای ایجاد توافق بین کارفرمای ممیزی، تیم ممیزی و ممیزی شونده در مورد نحوه انجام ممیزی تهیه کند. این طرح بایستی زمان‌بندی و هماهنگی فعالیت‌های ممیزی را تسهیل کنند.

میزان جزئیات ارائه شده در طرح ممیزی بایستی منعکس کننده دامنه کاربرد و پیچیدگی ممیزی باشد. میزان جزئیات ممکن است برای ممیزی‌های اولیه و متعاقب و هم‌چنین برای ممیزی‌های داخلی و

خارجی متفاوت باشد. طرح ممیزی بایستی از انعطاف‌پذیری لازم برای در نظر گرفتن تغییراتی مانند تغییرات به وجود آمده در دامنه کاربرد، که با پیشرفت فعالیت‌های ممیزی در محل ضرورت می‌یابند، برخوردار باشد.

طرح ممیزی بایستی موارد زیر را پوشش دهد:

الف) اهداف ممیزی

ب) معیارهای ممیزی و هر نوع مستندات مرجع

ج) دامنه کاربرد ممیزی، شامل شناسایی واحدهای سازمانی و عملیاتی و فرآیندهایی که قرار است ممیزی شوند

د) زمان‌ها و مکان‌های انجام فعالیت‌های ممیزی در محل

ه) زمان شروع و مدت زمان پیش‌بینی شده برای انجام فعالیت‌های ممیزی در محل، شامل جلسات تشکیل شده با مدیریت سازمان ممیزی شونده و جلسات تیم ممیزی

و) وظایف و مسئولیت‌های اعضای تیم ممیزی و افراد همراه

ز) تخصیص منابع مناسب به نواحی بحرانی ممیزی

در موارد مقتضی، برنامه ممیزی بایستی موارد زیر را نیز در برگیرد:

ح) شناسایی نماینده ممیزی شونده برای ممیزی

ط) زبان کاری و گزارش‌دهی ممیزی در صورتی که با زبان ممیز یا ممیزی شونده متفاوت باشد

ی) عناوین گزارش ممیزی

ک) تمهیدات لجستیک (مسافرت، تسهیلات در محل و امثال آن)

ل) موضوعات مرتبط با محرمانه بودن

م) هر گونه اقدامات پیگیری ممیزی

طرح ممیزی بایستی پیش از آغاز فعالیت‌های ممیزی در محل، توسط کارفرمای ممیزی مورد بازنگری قرار گرفته و پس از پذیرش وی به ممیزی شونده ارائه شود.

هرگونه اعتراض ممیزی شونده بایستی بین سرممیز، ممیزی شونده و کارفرمای ممیزی حل و فصل شود. طرح ممیزی اصلاح شده بایستی پیش از ادامه ممیزی مورد توافق طرف‌های مربوطه قرار گیرد.

۳-۴-۴-۲-تخصیص کار به تیم ممیزی

سرممیز با مشورت تیم ممیزی، بایستی مسئولیت ممیزی فرآیندها، حیطه‌های سازمانی، محل‌ها، نواحی یا فعالیت‌های مشخصی را به هر یک از اعضای تیم تخصیص دهد. در انجام این امر بایستی نیاز به استقلال و صلاحیت ممیزان و استفاده مؤثر از منابع و هم‌چنین وظایف و مسئولیت‌های متفاوت ممیزان، ممیزان در حال آموزش و کارشناسان فنی را در نظر گرفت. ممکن است با پیشرفت ممیزی، کارهای تخصیص داده شده به افراد به منظور اطمینان از تحقق اهداف ممیزی تغییر کنند.

۳-۴-۴-۳-تهیه مستندات کاری

اعضای تیم ممیزی بایستی اطلاعات مرتبط با قسمت‌هایی از ممیزی که به آن‌ها واگذار شده را مورد بازنگری قرار داده و مستندات کاری لازم به عنوان مرجع و برای ثبت روند ممیزی را تهیه کنند. این مستندات کاری می‌توانند شامل موارد زیر باشند:

چک لیست‌ها و طرح‌های نمونه‌گیری ممیزی

فرم‌هایی برای ثبت اطلاعات، از قبیل شواهد پشتیبان، یافته‌های ممیزی و سوابق جلسات.

استفاده از چک لیست‌ها و فرم‌ها نباید باعث محدود شدن دامنه فعالیت‌های ممیزی که می‌توانند در نتیجه اطلاعات جمع‌آوری شده در طول ممیزی تغییر کنند، شود.

مستندات کاری، شامل سوابق به وجود آمده در نتیجه استفاده از این مستندات، بایستی حداقل تا پایان ممیزی گردآوری شوند. مستنداتی که حاوی اطلاعات محرمانه یا خاص باشند بایستی همواره توسط اعضای تیم ممیزی حفظ و نگهداری شوند.

۳-۴-۵-انجام فعالیت‌های ممیزی در محل

۳-۴-۵-۱-برگزاری جلسه افتتاحیه

جلسه افتتاحیه ممیزی بایستی با حضور مدیریت سازمان ممیزی شونده یا در موارد مقتضی افراد مسئول حیطه‌ها یا فرآیندهایی که قرار است ممیزی شوند، برگزار شود. هدف از برگزاری جلسه افتتاحیه عبارت است از:

الف) تأیید طرح ممیزی،

ب) ارائه خلاصه‌ای از این که فعالیت‌های ممیزی چگونه انجام خواهند شد

ج) تأیید کانال‌های ارتباطی

د) فراهم آوردن فرصتی برای ممیزی شونده برای مطرح کردن سؤالات.

۳-۴-۵-۲-راهنمای کاربردی-جلسه افتتاحیه

در بسیاری از موارد، به عنوان مثال در ممیزی‌های داخلی در سازمان‌های کوچک، جلسه افتتاحیه ممکن است صرفاً به منظور مطلع ساختن ممیزی شونده از انجام ممیزی و توضیحی درباره ماهیت ممیزی برگزار شود.

در سایر موقعیت‌ها، جلسه بایستی رسمی بوده و سوابق حضور افراد باید نگهداری شود. جلسه بایستی توسط سرممیز هدایت شده و موضوعات زیر در موارد مقتضی در نظر گرفته شوند:

الف) معرفی شرکت‌کنندگان، شامل شرح مختصری در مورد وظایف ایشان،

ب) تأیید اهداف، دامنه کاربرد و معیارهای ممیزی،

ج) تأیید جدول ساعات کار ممیزی و دیگر هماهنگی‌های مرتبط با ممیزی شونده، از قبیل تاریخ و زمان جلسه اختتامیه، جلسات دیگر بین تیم ممیزی و مدیریت سازمان ممیزی شونده، و هرگونه تغییرات آتی،

د) روش‌های اجرایی که برای انجام ممیزی مورد استفاده قرار می‌گیرند، شامل مطلع ساختن ممیزی شونده از این امر که شواهد ممیزی صرفاً بر مبنای نمونه‌ای از اطلاعات در دسترس خواهند بود؛ می‌باشند و بنابراین همواره عدم قطعیت در ممیزی وجود خواهد داشت،

ه) تأیید کانال‌های ارتباط رسمی بین تیم ممیزی و ممیزی شونده،

و) تأیید زبانی که در طول مدت ممیزی مورد استفاده قرار خواهد گرفت،

ز) تأیید این امر که در طول مدت ممیزی، ممیزی شونده از میزان پیشرفت ممیزی مطلع خواهد شد،

ح) تأیید این که منابع و تسهیلات لازم برای تیم ممیزی در دسترس می‌باشند.

۳-۴-۵-۳-راهنمای کاربردی-انجام مصاحبه‌ها

مصاحبه یکی از روش‌های مهم جمع‌آوری اطلاعات بوده و بایستی با در نظر گرفتن موقعیت و وضعیت شخص مصاحبه شونده انجام شود. با این حال، یک ممیز بایستی موارد زیر را نیز در نظر داشته باشد:

الف) مصاحبه بایستی با افرادی از سطوح و حیطه‌های سازمانی مناسب که فعالیت‌هایشان در چارچوب دامنه کاربرد ممیزی باشد، انجام پذیرد،

ب) مصاحبه بایستی در ساعات متداول کاری و تا حد امکان در محل کار شخص مصاحبه شونده انجام شود،

ج) همه تلاش‌های لازم بایستی صورت پذیرد تا شخص مصاحبه شونده پیش از انجام مصاحبه و در حین مصاحبه احساس آرامش داشته باشد،

د) هدف از انجام مصاحبه و هرگونه یادداشت برداشتن بایستی توضیح داده شود،

ه) مصاحبه را می‌توان با درخواست از افراد برای تشریح کارشان آغاز کرد،

و) از پرسیدن سؤالاتی که بر نحوه‌ی پاسخ دادن فرد اثر می‌گذارند (از قبیل سؤالات هدایت کننده) بایستی خودداری کرد،

ز) خلاصه نتایج حاصل از انجام مصاحبه بایستی با فرد مصاحبه شونده مورد بازنگری قرار گیرد،

ح) در خاتمه بایستی از افراد مصاحبه شونده برای شرکت در مصاحبه و همکاری‌شان تشکر نمود.

۳-۴-۵-۴-ایجاد یافته‌های ممیزی

به منظور دست‌یابی به یافته‌های ممیزی، بایستی مشاهدات ممیزی را با معیارهای ممیزی سنجید. یافته‌های ممیزی می‌توانند انطباق یا عدم انطباق با معیارهای ممیزی را نشان دهند. در صورتی که در اهداف ممیزی ذکر شده باشد، می‌توان از یافته‌های ممیزی برای شناسایی فرصت‌های بهبود استفاده کرد.

در صورت لزوم، تیم ممیزی بایستی در مراحل مناسبی در طول مدت ممیزی، برای بازنگری یافته‌های ممیزی با یک‌دیگر تشکیل جلسه دهند.

خلاصه‌ای از انطباق با معیارهای ممیزی تهیه شود که نشان دهنده مکان‌ها، حیطه‌های سازمانی یا فرآیندهایی که ممیزی شده‌اند، باشند. هم‌چنین در صورتی‌که در طرح ممیزی ذکر شده باشد، یافته‌های ممیزی هر یک از ممیزان در مورد انطباق و شواهد پشتیبان آن‌ها نیز بایستی ثبت شود. عدم انطباق‌ها و شواهد ممیزی پشتیبان آن‌ها بایستی ثبت شوند. عدم انطباق‌ها را می‌توان رتبه‌بندی کرد. ممیزی شونده بایستی عدم انطباق‌ها را مورد بازنگری قرار داده و دقت شواهد ممیزی و درک کامل عدم انطباق‌ها را تصدیق نماید. کلیه تلاش‌های لازم بایستی برای از میان بردن اختلاف نظرات موجود در مورد شواهد یا یافته‌های ممیزی صورت پذیرفته و اختلاف نظرات باقی‌مانده بایستی ثبت گردند.

۳-۴-۵-۵-آماده کردن نتایج ممیزی

تیم ممیزی بایستی پیش از جلسه اختتامیه ممیزی با یک‌دیگر تشکیل جلسه دهند:

الف) به منظور بازنگری یافته‌های ممیزی، و دیگر اطلاعات مناسبی که در طول ممیزی جمع‌آوری شده‌اند، با توجه به اهداف ممیزی،

ب) به توافق رسیدن در مورد نتایج ممیزی، با در نظر داشتن عدم قطعیت ذاتی موجود در فرآیند ممیزی،

ج) تهیه پیش‌نهادها، در صورتی که در اهداف ممیزی تعیین شده باشد،

د) تبادل نظر در مورد پیگیری ممیزی در صورتی که در طرح ممیزی ذکر شده باشد.

۳-۴-۵-۶-برگزاری جلسه اختتامیه

جلسه اختتامیه ممیزی که توسط سرممیز هدایت می‌شود، بایستی به منظور ارائه یافته‌ها و نتایج ممیزی به نحوی که توسط ممیزی شونده به طور کامل درک و تصدیق شوند، و در موارد مقتضی حصول توافق با ممیزی شونده در مورد بازه زمانی ارائه برنامه اجرایی اقدامات اصلاحی و پیش‌گیرانه، تشکیل گردد. ممیزی شونده بایستی در جلسه اختتامیه شرکت داشته و هم‌چنین کارفرمای ممیزی و دیگر طرف‌ها نیز می‌توانند در این جلسه حضور داشته باشند. در موارد مقتضی سرممیز بایستی ممیزی شونده را از موقعیت‌هایی که در طول ممیزی با آن مواجه شده‌اند و ممکن است میزان اطمینان از نتایج ممیزی را کاهش دهند، مطلع نمایند. در بسیاری از مواقع، مثلاً در ممیزی‌های داخلی انجام شده در یک سازمان کوچک، جلسه اختتامیه می‌تواند صرفاً انتقال یافته‌ها و نتایج ممیزی باشد.

در سایر شرایط، جلسه بایستی رسمی بوده و صورت جلسات، شامل سوابق مربوط به حاضرین در جلسه، بایستی نگهداری شوند.

هرگونه اختلاف نظری بین تیم ممیزی و ممیزی شونده در مورد یافته‌ها یا نتایج ممیزی بایستی مورد بحث قرار گرفته و در صورت امکان حل و فصل شود. در غیر این صورت، کلیه نقطه نظرات بایستی ثبت شوند.

در صورتی که در اهداف ممیزی تعیین شده باشد، پیش‌نهادهای بهبود بایستی ارائه شوند. هم‌چنین بایستی تأکید شود که این پیش‌نهادها الزامی نیستند.

۳-۴-۶-تهیه، تصویب و توزیع گزارش ممیزی

۳-۴-۶-۱-تهیه گزارش ممیزی

سرممیز بایستی مسئولیت تهیه و محتوای گزارش ممیزی را بر عهده بگیرد.

گزارش ممیزی بایستی ثبت کامل، دقیق، موجز و شفافی از ممیزی بوده و بایستی شامل موارد زیر یا ارجاع به آن‌ها باشد:

الف) اهداف ممیزی،

ب) دامنه کاربرد ممیزی، به خصوص شناسایی فرآیندها یا واحدهای سازمانی و عملیاتی ممیزی شده و دوره زمانی پوشش داده شده،

ج) شناسایی کارفرمای ممیزی،

د) شناسایی سرممیز و اعضای تیم ممیزی،

ه) تاریخ‌ها و مکان‌های انجام فعالیت‌های ممیزی در محل

و) معیارهای ممیزی،

ز) یافته‌های ممیزی،

ح) نتایج ممیزی.

گزارش ممیزی در موارد مقتضی می‌تواند شامل موارد زیر یا ارجاع به آن‌ها نیز باشد:

ط) طرح ممیزی،

ی) لیستی از نمایندگان ممیزی شونده. ،

ک) خلاصه‌ای از فرآیند ممیزی، شامل عدم قطعیت یا موانع موجود که می‌توانستند باعث کاهش اطمینان نتایج ممیزی شوند،

ل) تأیید این که اهداف ممیزی در چارچوب دامنه کاربرد ممیزی و مطابق با طرح ممیزی محقق شده‌اند،

م) هر حوزه‌ای که با وجود این که در دامنه کاربرد ممیزی بوده، با این حال پوشش داده نشده است،

ن) هرگونه اختلاف نظر حل و فصل نشده بین تیم ممیزی و ممیزی شونده،

ص) پیش‌نهادهایی برای بهبود، در صورتی که در اهداف ممیزی مشخص شده باشد،

ع) برنامه‌های اجرایی پیگیری توافق شده در صورت وجود،

ف) بیانیه‌ای در مورد ماهیت محرمانه بودن محتویات گزارش،

س) لیست توزیع گزارش ممیزی.

۳-۴-۶-۲-تصویب و توزیع گزارش ممیزی

گزارش ممیزی بایستی در دوره زمانی مورد توافق تهیه شود. در صورتی‌که تهیه گزارش در این زمان امکان‌پذیر نباشد، دلایل تأخیر بایستی به اطلاع کارفرمای ممیزی رسانده شده و زمان جدید بایستی مورد توافق طرفین قرار گیرد.

گزارش ممیزی بایستی مطابق با روش‌های اجرایی برنامه ممیزی تاریخ‌گذاری، بازنگری و تصویب شود.

گزارش ممیزی تصویب شده بایستی بین کسانی که توسط کارفرمای ممیزی تعیین شده‌اند، توزیع شود.

گزارش ممیزی متعلق به کارفرمای ممیزی است. اعضای تیم ممیزی و کلیه دریافت‌کنندگان گزارش ممیزی بایستی در حفظ و محرمانه نگه داشتن گزارش دقت داشته باشند.

۳-۴-۶-۳-تکمیل ممیزی

ممیزی پس از انجام کلیه فعالیت‌های تشریح شده در طرح ممیزی و توزیع گزارش تصویب شده ممیزی، پایان می‌یابد.

مستندات مربوط به ممیزی بایستی بر اساس توافق بین طرف‌های مشارکت کننده در ممیزی و مطابق روش‌های اجرایی برنامه ممیزی و الزامات قانونی، دولتی و قراردادی نگاه داشته شده یا از بین بروند.

تیم ممیزی و افرادی که مسئولیت مدیریت برنامه ممیزی را بر عهده دارند، مگر در مواقعی که قانون تصریح کند، اجازه فاش کردن محتویات مستندات، دیگر اطلاعات به دست آمده در طول ممیزی، یا گزارش ممیزی را برای افراد دیگر بدون تصویب صریح کارفرمای ممیزی و در موارد مقتضی تصویب ممیزی شونده ندارند. در صورت ضرورت فاش کردن محتویات یکی از مستندات ممیزی، کارفرمای ممیزی و ممیزی شونده در اسرع وقت از این امر مطلع شوند.

۳-۵-خلاصه و نتیجه گیری

روند ارزیابی و ممیزی امنیتی به‌عنوان یکی از مراحل مهم موجود در چرخه بهبود امنیت اطلاعات سازمان در نظر گرفته شده و باید بر طبق یک برنامه منظم و مداوم انجام شود. در حقیقت اجرای دقیق و مداوم روند ارزیابی و ممیزی باعث می‌شود این اطمینان برای مدیران ارشد سازمان ایجاد گردد که روندها و کنترل‌های امنیتی پیاده سازی شده در سازمان بر طبق برنامه در حال اجرا بوده و آسیب‌پذیری‌ها و نقاط ضعف امنیتی احتمالی نیز توسط این روند استخراج گشته و به‌طور مناسبی کنترل می‌شوند.

در این فصل کلیات برنامه ممیزی امنیتی و مراحل موجود در آن از نقطه نظر مدیریتی تشریح گردید. همانند سایر اقدامات مدیریتی، برای اجرای مناسب روند ممیزی و حصول نتایج مطلوب از اجرای ممیزی ضروری است ابتدا کلیه مراحل موجود در روند ممیزی توسط مدیران سازمان و کارشناسان مجری مورد بررسی قرار گرفته و ملزومات و نیازمندی‌های هر مرحله و رونده‌ای اجرایی و عملیاتی آن مورد تایید مدیریت قرار گیرند.

همان طور که در این فصل شرح داده شد، جهت اجرای روند ممیزی امنیتی، باید رونده‌ای تکنیکی و فنی خاصی طراحی گردیده و بر اساس آن‌ها تجهیزات و رونده‌ای مورد استفاده در سازمان مورد ممیزی و ارزیابی امنیتی قرار گیرد .

۳-۶-سوالات تشریحی

۱- چهار مرحله اصلی موجود در چرخه بهبود فرآیند امن سازی مدیریت اطلاعات سازمان را شرح داده و جایگاه روند ارزیابی و ممیزی امنیتی را در این چرخه توضیح دهید.

۲- جهت انجام فعالیت‌های ممیزی در محل، چه اقدامات کلی باید توسط سرممیز و تیم ممیزی انجام گیرند؟

۳- مراحل کلی مدیریتی موجود در اجرای یک برنامه ممیزی را تشریح نمایید.

۴- برخی از مواردی که در فرآیند طراحی و اجرای ممیزی باید در نظر گرفت را شرح دهید.

۵- مهم‌ترین وظایف سر ممیز در هنگام اجرای روند ممیزی را نام ببرید؟

فصل چهار - ممیزی و ارزیابی امنیتی سیستم‌های فن‌آوری اطلاعات

ارزیابی و ممیزی، فرآیندی است که نیازمند تجربه، تخصص و دقت بالا بوده و می‌بایست در قالب کار گروهی و با بهره گیری از توان مسئولین و کارشناسان ذی‌ربط انجام پذیرد. این فعالیت تیمی نیز زمانی به نتیجه مطلوب دست خواهد یافت که تیم ارزیاب، علاوه بر برخورداری از تجربه و تخصص لازم، از زبان مشترکی نیز در درک مفاهیم و روش‌های مورد استفاده برخوردار باشند. در این راهنما سعی شده است تا ضمن ارائه تعاریف و تشریح مفاهیم مورد استفاده در ارزیابی ریسک، نمونه‌ها و لیست‌های مرجعی نیز جهت استفاده کارشناسان ارائه شود.

۴-۱- تعاریف

تهدید: حادثه‌ای که به‌طور بالقوه امکان دارد سبب ایجاد یک واقعه ناگوار (از قبیل دسترسی غیر مجاز، دست‌کاری، افشاء یا خراب‌کاری) بر روی دارایی‌های اطلاعاتی موجود در سازمان گردد.

آسیب‌پذیری: ضعف موجود در یک سیستم، برنامه کاربردی، زیر ساختار، کنترل یا طراحی است که می‌تواند در جهت مختل کردن تمامیت سیستم‌های موجود و روال‌های کاری و سازمانی و مأموریت‌ها و فعالیت‌های سازمان، از سوی تهدید مورد استفاده و بهره برداری قرار گیرد.

ریسک: احتمال این که یک تهدید مشخص بتواند از یک آسیب پذیری (نقطه ضعف) خاص موجود در سیستم‌های سازمان استفاده نماید.

ارزیابی ریسک: مراحل مورد نیاز برای شناسایی حوزه و دارایی‌های موجود در آن، تهدیدهای موجود علیه دارایی‌ها، اولویت بندی نقاط ضعف مربوط به تهدیدها و مشخص نمودن سطح ریسک‌ها و کنترل‌های مناسب را گویند.

۴-۲- روش اجرا

نخستین گام اجرای فرآیند ارزیابی و ممیزی، شناسایی تمامی دارایی‌های اطلاعاتی موجود در حوزه مورد بررسی است تا پس از آن بتوان ریسک‌های متوجه هر یک از آن‌ها را به‌طور کامل مشخص نمود. برای شناسایی و دسته‌بندی دارایی‌ها می‌توان از ضمیمه (الف) استفاده نمود. در این ضمیمه، دارایی‌ها به چهار دسته دارایی‌های اطلاعاتی، نرم افزاری، سخت افزاری و انسانی تقسیم شده و برای هر یک، نمونه‌هایی ذکر شده است.

پس از تعیین و شناسایی دارایی‌ها، تیم ارزیابی اقدام به شناسایی ریسک‌های مربوط به هر یک از دارایی‌ها می‌نماید. همان‌طور که از تعریف ارائه شده برای ریسک استنباط می‌شود، هر ریسک از سه عنصر یا جزء تشکیل شده است. لذا تعریف ریسک به معنی تعیین دقیق این سه عنصر است. این سه عنصر عبارتند از عامل تهدید، سرمایه و اثر تهدید. به عبارت دیگر:

ریسک = عامل تهدید + سرمایه + اثر تهدید.

همان گونه که از رابطه فوق بر می‌آید، با تغییر هر یک از اجزاء موجود در طرف چپ تساوی، ریسک جدیدی حاصل می‌شود. در نتیجه در اغلب موارد امکان دارد که برای یک دارایی مشخص، چندین ریسک مختلف را با توجه به نوع عامل تهدید و انواع اثرات آن، بتوان شناسایی نمود. در این صورت، برای هر مورد، یک شناسنامه ریسک به طور مجزا تهیه خواهد شد. برای مشخص کردن انواع عوامل تهدید قابل اعمال بر روی دارایی‌های اطلاعاتی و نیز اثرات ناشی از آن‌ها، می‌توان به ترتیب از ضمیمه (ب) و (ج) این راهنما استفاده کرد.

در پایان این مرحله، باید برای تمامی دارایی‌های موجود در حوزه بررسی، ریسک‌های مربوطه مطابق فرمول فوق‌الذکر شناسایی شده و در بخش اول شناسنامه ثبت شوند. به‌عنوان مثال، برخی از ریسک‌های شناسایی شده ممکن است به صورت زیر ثبت شوند:

کاربران به دلیل بی توجهی (سهل انگاری) باعث خراب شدن هارد کامپیوتر سرور دبیرخانه شوند.

به دلیل ویروسی شدن، هارد کامپیوتر سرور اینترنت قابل استفاده و دسترسی نباشد.

تعداد بیش‌تری از ریسک‌ها ممکن در ضمیمه (د) این راهنما ارائه شده است.

۴-۳- حوزه ریسک:

منظور از حوزه ریسک، تعیین گروه دارایی مورد بررسی است. همان گونه که پیش از این نیز ذکر شد، حوزه ریسک می‌تواند یکی از حوزه‌های کلی سخت افزار، نرم افزار، نیروی انسانی و اطلاعات باشد.

۴-۳-۱- تعیین طبیعت ریسک:

ریسک‌ها را می‌توان با توجه به ماهیت وجودی خود و با توجه به ابعاد، حوزه و گستره اثرگذاری، دسته بندی نمود. این دسته بندی که به تعیین «طبیعت ریسک» موسوم است، به ارزیاب کمک می‌کند تا با توجه به حوزه‌های اثرگذاری ریسک، قادر باشد با دقت بیش‌تری به شناسایی اثرات و عواقب تهدید اقدام نماید. به‌طور کلی، ریسک‌ها را می‌توان به حوزه‌های زیر تقسیم نمود:

استراتژیک: ریسک‌هایی که تمامیت، موجودیت و بقای سازمان را با خطر مواجه می‌کنند مانند فقدان اطلاعات کلیدی و استراتژیک

مالی: اثرات و عواقب مالی به دنبال دارند نظیر غیر قابل استفاده شدن سخت افزارها و تجهیزات

عملیاتی: در انجام فعالیت‌ها و فرآیندهای سازمان خلل ایجاد می‌کنند مانند قطع سرویس سرور

تکنولوژیکی: اطلاعات فنی یا سخت افزارهای کلیدی را مورد هجوم قرار می‌دهند

محیطی: بر نیروی انسانی یا شرایط زیست محیطی سازمان تأثیرگذار هستند نظیر آتش سوزی

از آنجایی که اغلب، هر تهدید (ریسک) بیش از یک اثر به دنبال خواهد داشت، لذا با توجه به تنوع اثرات، ممکن است طبیعت یک ریسک در بیش از یک حوزه یا حتی تمامی حوزه‌ها قرار گیرد.

۴-۳-۲- زیان دیدگان (ذینفعان) ریسک:

منظور از زیان دیده، تمامی افراد یا واحدهایی از سازمان است که به طور مستقیم یا غیر مستقیم تحت تأثیر نتایج تهدید قرار می‌گیرند. این ذینفعان ممکن است یک یا تمامی موارد ذیل باشند:

کاربر

مسئول واحد

مدیریت ارشد سازمان

کارکنان واحد

تمامی کارکنان سازمان

سهامداران

جامعه

. . .

۴-۳-۳- تعیین آثار ریسک:

کلیه نتایج و عواقب بروز ریسک که می‌تواند هر یک از ذینفعان اطلاعات یا ویژگی‌های آن‌را تحت تأثیر قرار دهد، در این بخش در نظر گرفته می‌شود. به‌تر است در این بند، بیش‌تر به اثرات مستقیم ریسک اشاره شود و در صورت وجود ابهام یا کلی گویی، به توالی تبعات و اثرات آن اشاره نمود. این اثرات را می‌توان در یک یا چند مورد از انواع ذکر شده در ضمیمه (ج) این راهنما، جستجو نمود.

۴-۳-۴- تعیین مشخصه‌های کمی ریسک:

۴-۳-۴-۱- ریسک سخت افزار:

برای تعیین مشخصه‌های کمی ریسک (احتمال و اثر) دارایی‌های سخت افزاری، باید از جداول مربوطه در ضمیمه (ه) استفاده نمود. در این جداول، هر دو مشخصه احتمال و اثر، با توجه به تعاریف و مثال‌های ارائه شده، در گستره ۱ تا ۱۰ طبقه بندی شده‌اند. لازم به ذکر است که جداول مذکور، استاندارد بوده و بر اساس روش ارزیابی ریسک FMEA، بومی سازی شده‌اند.

۴-۳-۴-۲- ریسک نرم افزار:

مشابه تعیین مشخصه‌های کمی ریسک دارایی‌های سخت افزاری انجام خواهد شد.

۴-۳-۴-۳- ریسک اطلاعات:

همانند دو دارایی قبل انجام می‌شود.

۴-۳-۴-۴- ریسک نیروی انسانی:

در مورد دارایی‌های انسانی، با توجه به تفاوت ماهیت این نوع دارایی با دارایی‌های قبلی، از روش جداگانه‌ای استفاده خواهد شد. در این روش، هفت مؤلفه به عنوان مؤلفه‌های ارزش نیروی انسانی تعیین می‌شوید که عبارتند از: تخصص، سابقه، رتبه، سختی کار، مدرک تحصیلی، وجود جای‌گزین و سطح دسترسی. هر یک از کارکنان سازمان، مطابق راهنمای ارائه شده در ضمیمه (و) این راهنما، در هر یک از موارد مذکور، امتیازی بین ۱ تا ۱۰ دریافت خواهند کرد. در نتیجه، ارزش کل هر یک از کارکنان، عددی بین ۷ تا ۷۰ خواهد بود.

برای محاسبه شدت اثر ریسک نیروی انسانی، امتیاز اکتسابی هر فرد، بر حداکثر امتیاز قابل کسب (عدد ۷۰) تقسیم می‌شود و عدد حاصل در ضریب ۱۰ ضرب می‌شود تا امتیاز اثر، در گستره ۱ تا ۱۰ محاسبه شود.

برای تعیین احتمال نیز، یکی از اعداد جدول ذیل انتخاب می‌گردد.

معیار	شرح	مقدار
بالا	در اغلب مواقع، ریسک به وقوع می‌پیوندد. (یک‌بار یا بیش‌تر در سال)	۱۰-۵. ۷
متوسط	در اغلب موارد، احتمال وقوع ریسک وجود دارد. (یک‌بار در ۲ سال)	۴ .۷-۳
محتمل	ریسک گاهی اوقات به وقوع می‌پیوندد. (یک‌بار در ۵ سال)	۹ .۲-۲
غیر محتمل	ریسک گاهی اوقات ممکن است به وقوع بپیوندد. (یک‌بار در ۱۰ سال)	کمتر از ۲

همانند سایر دارایی‌ها، سطح ریسک از حاصل‌ضرب دو عدد انتخاب شده برای اثر و احتمال بدست می‌آید.

ضمیمه (الف): دسته بندی دارایی‌ها

تعریف سرمایه:

عبارتست از دارایی فیزیکی یا اطلاعاتی که برای سازمان دارای ارزش و اهمیت بوده و باید به طور خاص مورد محافظت قرار گیرد.

دارایی‌های سخت افزاری

شامل سرورها، کامپیوترهای شخصی، انواع CD، فلاپی، پرینتر، اسکنر، نوت بوک، فلش مموری، درایورهای قابل حمل، اجزا شبکه ارتباطی از قبیل روترها، مودم، سوئیچ، . . .

دارایی‌های نرم افزاری

نرم افزارهایی که در داخل سازمان تولید شده و در راستای مأموریت و فعالیت‌های سازمان مورد استفاده قرار می‌گیرند.

نرم افزارهایی که در خارج از سازمان تهیه شده و در راستای مأموریت و فعالیت‌های سازمان مورد استفاده قرار می‌گیرند مانند سیستم‌های اتوماسیون اداری، نرم افزارهای مالی، انبارداری و . . . .

نرم افزارهای معمول و موجود در بازار که برای انجام امور عادی و روزمره مورد استفاده قرار می‌گیرند مانند نرم افزارهای تایپ و صفحه گسترده، نقشه کشی و . . . .

سایر موارد.

سرمایه‌های اطلاعاتی

شامل هر نوع اطلاعات (چه فیزیکی از قبیل کاغذ و نامه و . . .) و چه غیر فیزیکی (داده‌ها) که برای سازمان دارای ارزش باشند.

اطلاعات کاری و سازمانی از قبیل سوابق پروژه‌ها و فعالیت‌های انجام شده، مأموریت و گزارشات سازمانی موجود، روندها و طرح‌های سازمانی و . . .

اطلاعات پرسنلی از قبیل اطلاعات حقوقی، اطلاعات شخصی، سوابق کاری و خدمتی، شماره حساب‌های بانکی و . . .

اطلاعات امنیتی از قبیل کلمات عبور، اطلاعات مربوط به رمزنگاری و احراز صلاحیت و احراز هویت کاربران و . . .

بانک‌های اطلاعاتی موجود بر روی سرورها، فایل‌های اطلاعاتی ذخیره شده بر روی سرورها یا کامپیوترهای کاربران

سایر موارد

سرمایه‌های انسانی

سرمایه‌های انسانی شامل تمامی کارکنانی می‌شود که در سازمان مشغول بکار بوده و در صورت از دست دادن آن‌ها، به روند اجرایی سازمان و روال‌های کاری و سازمانی لطمه وارد خواهد شد. نظِیر:

مدیران ارشد قسمت‌های مختلف سازمان و جانشینان و معاونین آن‌ها

رؤسای بخش‌ها و دوایر

پرسنل متخصص و با سابقه

مدیران و کارشناسان بخش فن‌آوری اطلاعات و امنیت اطلاعات

پرسنل متخصص و تکنیکی موجود در دوایر و بخش‌ها

سایر

ضمیمه (ب)- دسته بندی عوامل تهدید

تهدیدات طبیعی: طوفان، زمین لرزه، گردباد، رانش زمین، بهمن، طوفان‌های الکتریکی و رویدادهای مشابه.

تهدیدات انسانی:

الف) رویدادها و اتفاقاتی که منشاء انسانی غیر عمدی دارند (اشتباهات و غفلت‌ها) مانند عدم به‌کارگیری صحیح تجهیزها، عدم نصب صحیح نرم‌افزارها و برنامه‌های کاربردی، آلوده نمودن غیر عمدی شبکه به ویروس، دسترسی ناخواسته به اطلاعات محرمانه و . . .

ب) رویدادها و اتفاقاتی که منشا انسانی عمدی دارند چه از داخل سازمان و چه از خارج از آن (سوءاستفاده، نرم افزار مخرب، دسترسی غیرمجاز، کدهای مخرب، ویروس، بمب‌ها، اخلال‌گری الکترونیکی، آتش سوزی عمدی، قطع برق عمدی و . . .). بر طبق آمار، تهدیداتی که موجب وارد شدن بیش‌ترین آسیب به منابع اطلاعاتی می‌شوند، دارای منشا انسانی هستند.

تهدیدات محیطی: قطع طولانی مدت برق، آلودگی، مواد شیمیایی، نشت مایعات، آتش سوزی غیر عمدی، استهلاک تجهیزات و لوازم و . . .

ضمیمه (ج)- انواع اثرات تهدیدات

تعریف اثر تهدید: به نتایج و پیامدهای منفی حاصل از وقوع تهدید گفته می‌شود که می‌توانند بر روی سرمایه‌های اطلاعاتی سازمان، تأثیر منفی در پی داشته باشند.

سؤ استفاده از دارایی اطلاعاتی

دست‌کاری غیر مجاز

افشاء غیر مجاز

سرقت

عدم سرویس دهی یا قطع مقطعی آن

کپی و تکثیر غیر مجاز

تخطی از قواعد و قوانین سازمانی

کاهش کارایی سازمان

کاهش ایمنی افراد

از دست رفتن جامعیت اطلاعات

از دست رفتن دسترس پذیری اطلاعات (در زمان لزوم، در مکان مورد نیاز نباشد)

فعالیت‌های بیهوده مالی (زیان مالی)

تهدیدهای مربوط به محیط زیست

اختلال در فرآیندهای سازمانی

از بین رفتن دارایی

ضمیمه (د)- نمونه‌ای از ریسک‌ها قابل شناسایی در سازمان

اعضای تیم ارزیابی ریسک می‌توانند از این فهرست نمونه‌ای ریسک‌ها، به‌عنوان نقطه شروعی جهت شناسایی انواع ریسک‌های قابل اعمال بر دارایی‌های اطلاعاتی سازمان مطبوع خود استفاده نمایند. نکته‌ای که در این جا ذکر آن ضروری است این است که این فهرست تنها به‌عنوان نمونه و نه یک لیست جامع و کامل از تمامی ریسک‌ها موجود و محتمل می‌باشد و اعضای تیم می‌بایست بر اساس تجربه و تخصص خود و با استفاده از سوابق مربوط به حوادث گذشته، تمامی ریسک‌ها محتمل قابل اعمال بر مجموعه تحت بررسی خود را شناسایی نمایند. در هنگام مشخص نمودن ریسک‌ها، توجه به این نکته نیز ضروری است که تنها از ریسک‌هایی می‌توان چشم پوشی نمود که احتمال آن‌ها صفر (غیر ممکن و محال) باشد. در غیر این صورت حتی کم احتمال‌ترین ریسک‌ها نیز می‌بایست ثبت شوند. نکته دیگر این است که برخی از ریسک‌ها ممکن است از سوی عوامل مختلف اعمال شوند که همان گونه که پیش از این نیز گفته شد، برای هر یک از آن‌ها می‌بایست شناسنامه جداگانه‌ای تهیه شود.

فهرست نمونه‌ای انواع ریسک‌های قابل اعمال بر سازمان مبتنی بر فن‌آوری اطلاعات

خرابی هارد کامپیوتر سرور/ شخصی به دلیل سهل انگاری مسئول/ کاربر مربوطه

خرابی هارد کامپیوتر سرور/ شخصی به دلیل نفوذ ویروس از طریق اینترنت

خرابی هارد کامپیوتر سرور/ شخصی به دلیل نفوذ ویروس از طریق کاربران

دسترسی غیر مجاز به اطلاعات موجود در کامپیوتر سرور/ شخصی توسط کاربران داخلی

دسترسی غیر مجاز به اطلاعات موجود در کامپیوتر سرور/ شخصی از طریق اینترنت

افشا غیر مجاز اطلاعات موجود در کامپیوتر سرور/ شخصی به دلیل سهل انگاری کاربر مجاز

افشا غیر مجاز اطلاعات موجود در کامپیوتر سرور/ شخصی از طریق اینترنت

سرقت اطلاعات موجود در کامپیوتر سرور/ شخصی از طریق اینترنت

سرقت اطلاعات موجود در کامپیوتر سرور/ شخصی به دلیل سهل انگاری کاربر مجاز

عدم سرویس دهی کامپیوتر سرور/ شخصی به علت نفوذ ویروس از طریق اینترنت

عدم سرویس دهی کامپیوتر سرور/ شخصی به علت نفوذ ویروس از طریق کاربر مجاز

عدم سرویس دهی کامپیوتر سرور/ شخصی به علت قطع برق و نبود UPS

شرح ریسک‌های مرتبط با محرمانگی سرمایه‌های اطلاعاتی سازمان:

داده / اطلاعات به طور نادرستی توسط مسئول مربوطه یا کاربر برچسب گذاری شود.

داده / اطلاعات به‌طور نادرستی توسط مسئول مربوطه یا کاربر دسته بندی شود.

داده / اطلاعات قبل از این که از طریق کانال‌های مناسب انتشار یابد به اشتراک گذاشته شود.

استفاده از سیستم‌های غیر امن برای انتقال داده / اطلاعات حساس

افشای اطلاعات و نقض قوانین حریم شخصی و مالکیت

عدم وجود توضیحات شفاف در مورد قوانین محرمانگی

محافظت نامناسب از فهرست کلمات عبور

وجود در پشتی[۱] در نرم افزارها داده‌ها و برنامه‌های کاربردی

مدیر اجرایی عصبانی و ناراضی که دارای امتیازات و توانایی‌های امنیتی بالایی باشد.

---

۱ backdoor

عدم بررسی کامل اثرات نهفته و مخفی قبل از اعمال نمودن تغییرات مورد نیاز بر روی سیستم‌ها و برنامه‌های مورد استفاده سازمان

توانایی حدس زدن مشخصات فردی دیگر توسط کاربران سازمان یا هکرها

کارمندان و افراد از طریقه نحوه صحیح انتشار یا ذخیره کردن اطلاعات موجود بر روی وب ناآگاه باشند.

دست‌پاچه و گیج شدن مسئولین امنیتی شبکه در مورد جایی که اطلاعات حساس در آن جا ذخیره شده است.

دادن قابلیت دسترسی به افرادی که از نظر شغلی نیازی به داشتن این امتیاز نداشته باشند.

اطلاعات مربوط به سیستم‌های داخلی به طور سهوی انتشار یابند که ممکن است در آینده برای حمله به سیستم مورد استفاده قرار گیرند.

استفاده از IDهای مشترک توسط کاربران سازمان

دسترسی به فایل‌های پشتیبانی کننده توسط مدیر اجرایی سیستم به طور مناسبی کنترل نشود.

تکنولوژی‌های جدید باعث نفوذ در مسایل محرمانگی شوند.

تلاش‌ها و تصمیماتی برای تغییر دادن مدل امنیتی صورت گیرد.

عدم تشریح مسایل محرمانگی برای افراد غیر کارمند موجود در سازمان

ردیابی بسته‌ها توسط افراد غیر مجاز از خارج سایت اینترنتی سازمان

جریمه‌های در نظر گرفته شده برای تخطی کردن از مقررات امنیتی آنقدر کافی نباشد که باعث جلوگیری کردن از فعالیت‌های نامناسب افراد گردد.

امکان وجود تجهیزات استراق سمع الکترونیکی در محل‌های مختلف مجموعه مورد نظر

شرح ریسک‌های مرتبط با تمامیت سرمایه‌های اطلاعاتی سازمان:

پایگاه داده توسط خطای سخت افزاری، نرم افزاری بد یا نادرست، خراب شود.

عدم گزارش کردن نکات و موارد مربوط به تمامیت توسط کاربران سازمان

اجرای ناقص یک روند یا عدم توانایی در اجرای صحیح روند توسط افراد باعث خراب شدن داده شود.

نبود پردازش‌های داخلی برای ایجاد کنترل و مدیریت داده در حین انجام فعالیت‌های مختلف

عدم تشخیص و اعلام مشکلات تمامیت به‌وجود آمده توسط کاربران و مسئولین امنیتی شبکه سازمان

امکان دسترسی اشخاص ثالث به اطلاعات محرمانه موجود در سازمان

عدم تعیین صلاحیت منشأ تقاضا کننده درخواست در روال‌ها و سیاست‌های موجود در سازمان

عدم قابلیت دسترسی به اطلاعاتی که مجاز به دسترسی به آن‌ها می‌باشید.

کارمندان مربوطه آموزش‌های لازم برای انجام تغییرات مورد نیاز را دریافت نکرده باشند.

عدم پاسخ دهی مناسب به تقاضاهای انجام شده در مدت زمان مورد نظر

تغییرات انجام شده در داده / نرم افزارهای سیستم یا برنامه‌های کاربردی ذخیره نشده باشند.

استفاده کاربران از کپی‌هایی از داده که از رده خارج شده باشند.

وجود مشکلات همسان سازی و یک‌نواخت کردن در هنگام استفاده از وسیله‌های جبران ساز و بازگرداننده توسط کاربران

تغییر داده‌ها به علت وجود ویروس

عدم گزارش کردن به موقع وضعیت کاربران توسعه دهندگان، پشتیبانی کنندگان و غیره توسط مسئولین مربوطه

شرح ریسک‌های مرتبط با در دسترس بودن سرمایه‌های اطلاعاتی سازمان:

هکرها سایت مجموعه مورد نظر را تعطیل نمایند.

نفوذکنندگان قادر به دسترسی فیزیکی به تجهیزات و امکانات مجموعه مورد نظر شوند.

وجود خطای سخت افزاری در مورد سرور اینترنت

ارتباطات موجود با تهیه کننده سرویس قطع شود.

سایت میزبان محافظ‌های فیزیکی مناسبی برای اطلاعات نداشته باشد.

ارتباط با سیستم‌های پشتیبان اداره قطع شود.

طراحی کلی سیستم پیچیده باشد.

ایجاد تغییرات نادرست نرم افزار یا سخت افزار سیستم توسط کاربران مجاز

مقادیر و پیش‌بینی‌های مورد استفاده و معمول غیر قابل انتظار باشند.

رونده‌ای برنامه استمرار پذیری سازمان آزمایش نشده باشند.

هیچ تضمینی برای آماده بودن سرور توسط تهیه کننده سرویس داده نشده باشد.

اقدامات و اعتصاب‌هایی در سازمان تهیه کننده سرویس به وقوع بپیوندد.

تعمیر و نگهداری برنامه ریزی شده معمولی باعث آماده و در دسترس نبودن سرویس شود.

طراحی توپولوژی مانع کارایی / قابل قبول بودن میزان در دسترس بودن سرویس‌های عمومی شود.

سرمایه گذاری‌های نامناسب سازمان برای قابلیت‌های پشتیبانی

حملات برنامه ریزی شده توسط معترضان و مخالفین سازمان

ساختار بندی سیستم برای در دسترس بودن زیاد مناسب نباشد.

منابع و افراد تکنیکی سازمان آموزش‌های مناسب ندیده باشند.

تراکم موجود در اینترنت باعث عدم رضایت کاربران شود.

به علت وجود ویروس ممکن است داده / اطلاعات در دسترس نباشند.

به علت عدم نظارت کافی بر سایت وب سازمان ممکن است آماده نبودن سیستم گزارش نشود.

به علت نقص در روتر یا دیواره آتش ممکن است دسترسی به سرویس‌ها امکان پذیر نباشد.

پشتیبان‌های موجود در سازمان کافی نباشند.

سوءاستفاده کاربران از امکانات شبکه و کلمات عبور سایر افراد

۴-۴- سوالات خود آزمایی:

روش اجرای ریسک را بنویسید.

چگونه می توان مشخصه های کمی ریسک را تعیین نمود.

موارد سواستفاده از دارایی اطلاعاتی سازمان را نوشته و توضیح دهید.

ده نوع از ریسک های قابل اعمال در سازمان های مبتنی بر فن اوری اطلاعات را بنویسید.

پنج نوع از ریسک های مرتبط با در دسترس بودن سرمایه های اطلاعاتی سازمان را نوشته و توضیح دهید.

فصل پنجم - ارزیابی ،روش‌ها و راه‌کارها

در این فصل که مجموعه مطالب بیش‌تری را در خود جای داده سعی می‌شود مباحث مربوط به ارزیابی‌های امنیتی، روش‌های مطرح ارزیابی، نقطه‌های هدف در یک ارزیابی، روش‌های درونی و بیرونی ارزیابی و نکاتی از این قبیل مورد توجه قرار گیرد. آزمون نفوذ این امکان را برای مدیران شبکه فراهم می‌آورد که تمامی نقاط آسیب‌پذیر و حفره‌های امنیتی شبکه سازمان خود را پیش از آنکه این حفره‌ها توسط هکرها و افراد فرصت‌طلب جهت فروپاشی و تسخیر شبکه به کار گرفته شوند؛ بشناسند.

آزمون نفوذ جهت کشف کلیه حفره‌ها در تمامی اجزای زیرساخت‌های اطلاعاتی طراحی شده است. در آزمون نفوذ با توجه به سیستم‌های اطلاعاتی، برای هر بخش گزینه‌ای در نظر گرفته شده است، که عبارتند از:

اکتشافات و شناسایی شبکه

پویش پورت‌ها

شناسایی سرویس‌ها

شناسایی سیستم

جست‌جو و آزمون حفره‌های امنیتی

آزمون برنامه‌های کاربردی تحت وب

آزمون مسیریاب

آزمون سیستم‌های طبقه بندی شده

آزمون دیواره آتش

آزمون سیستم تشخیص نفوذ

دور زدن و اغفال مکانیزم‌های امنیتی

آزمون کلمان عبور

آزمون استعداد فروپاشی در برابر حمله انکار سرویس

متدولژی آزمون نفوذ با استفاده از روش‌های نوین و راهکارهای جدید تدوین شده است. سپس این متدولژی با توجه به تجربیات بدست آمده توسط تیم آزمون نفوذ، توسعه پیدا کرده و تقویت شده است. در ضمن این متدولژی با استفاده از استانداردها و برترین روش‌های موجود آزمون نفوذ، طراحی گردیده است. استانداردهایی که کارآمدی خود را در طول سالیان به اثبات رسانیده است. از جمله استانداردهای به کار رفته در تدوین متدولژی آزمون نفوذ می‌توان به موارد زیر اشاره کرد:

The Open Source Security Testing Mathodology

The Open Web Application Security Project (OWASP)

هدف این فصل ایجاد یک راهنما برای نظام‌بندی، برنامه‌ریزی و تعریف ارزیابی‌های فنی امنیت اطلاعات، آنالیز و استراتژی کاهش خطرات و تهدیدات احتمالی می‌باشد. در این فصل پیشنهاداتی عملی برای طراحی و ایجاد یک آموزش اولیه برای ارزیابی و تست امنیت، ارائه می‌گردد. هم‌چنین می‌تواند برای اهداف مختلف از جمله یافتن نقاط آسیب‌پذیری در یک سیستم و اصلاحات مطلوب بر اساس نیاز، مورد استفاده قرار گیرد. این راهنما به معنای یک راهنمای کامل و جامع ارزیابی و تست سیستم‌های امنیتی نبوده و یک دید کلی از عناصر اصلی و کلیدی، برای ارزیابی و تست ارائه نموده و با تاکید بیش‌تر بر مشخصات و پارامترهای فنی، مزایا و محدودیت‌های آن‌ها، در نهایت پیش‌نهادهایی در این زمینه ارائه می‌نماید.

این بخش برای استفاده کسانی است که در بخش امنیت کامپیوتر، مدیران برنامه، مدیران شبکه و سیستم و سایر کسانی که مسئول آماده سازی اطلاعات فنی می‌باشند، اپراتورها، پدید آورندگان شبکه و سیستم‌ها ایجاد شده است. مدیران هم‌چنین می‌توانند از اطلاعات جمع آوری شده برای تصمیم گیری و داوری استفاده نمایند. محور اصلی مطالب این بخش، بر اساس مطالب فنی می‌باشد. فرض بر آن است که خوانندگان حداقل اطلاعات کلی در مورد امنیت سیستم‌ها و شبکه‌ها را دارا می‌باشند.

۵-۱- کلیات تست‌ها و آزمایشات امنیتی

سیستم ارزیابی امنیتی میزان تأثیر ارزیابی موجود را بیان می‌کند. به‌طور کلی سه روش برای ارزیابی وجود دارد: ۱- تست ۲- آزمایش ۳- مصاحبه و مشاهده. نتایج ارزیابی برای پشتیبانی و کنترل موثر امنیت به کار برده می‌شوند.

تهیه نتایج تست‌های فنی و انتشار آن و انجام آزمایش‌های فنی، در تعریف و تایید صحت و ارزیابی نقاط آسیب‌پذیر کاربرد داشته و برای درک و توسعه وضعیت امنیتی شبکه‌ها و سیستم‌ها به کار برده می‌شوند. این فرآیندها به معنای جای‌گزین کردن کنترل امنیت و مراقبت از امنیت سیستم نیست ولی به تایید سازماندهی سیستم و این که احتمالاً امن بوده و تعریف یک نظام امنیتی که نقاط ضعف کم‌تری نسبت به سایر سیستم‌ها داشته باشد،کمک می‌کند.

این فصل یک دید کلی از روش‌های ارزیابی امنیت اطلاعات و تکنیک‌های تست‌ها و آزمایش‌ها ارائه می‌دهد.

۵-۱-۱- روش ارزیابی و امنیت اطلاعات

یک روش مستند و تکرارپذیر ارزیابی امنیت دارای فواید زیر است:

ایجاد ثبات و ساختار برای تست‌های امنیتی که می‌تواند ریسک‌های تست را حداقل نماید.

تسریع در عبور از دوره گذار کارکنان جدید ارزیابی.

از آن جا که ارزیابی امنیت اطلاعات به منابعی از قبیل زمان، نیروی انسانی، سخت‌افزار و نرم‌افزار نیاز دارد، میزان محدودیت دسترسی به این منابع، دوره تکرار ارزیابی امنیتی را مشخص می‌کند. سنجش

انواع تست‌های امنیتی و آزمایش‌های ساختار موجود، تکمیل یک روش مناسب، تعریف منابع مورد نیاز و ساختار دادن به فرآیند ارزیابی برای پشتیبانی ملزومات می‌تواند مشکل کمبود منابع را به حداقل برساند.

این امر به ساختار اجازه می‌دهد تا از منابع (افراد آموزش دیده) دوباره استفاده نماید. هم‌چنین کاهش زمان مورد نیاز و نیاز به تجهیزات و نرم‌افزار و در نهایت کاهش هزینه‌های ارزیابی را به دنبال خواهد آورد.

برنامه ریزی

اصلی‌ترین مطلب برای موفقیت یک برنامه ارزیابی امنیتی، فاز برنامه‌ریزی برای جمع‌آوری اطلاعات مورد نیاز ارزیابی از جمله مواردی که باید مورد ارزیابی قرار گیرد، تهدیدهایی که وجود دارند کنترل‌هایی که تهدیدهای موجود را کاهش می‌دهد، می‌باشد. یک برنامه ارزیابی امنیتی باید به سایر اهداف پروژه که برنامه مدیریت پروژه به عنوان اهداف پروژه مشخص نموده است، هم‌چنین محدوده پروژه، محدودیت‌ها، مسئولیت‌ها، موفقیت‌ها، مفروضات، منابع، زمان بندی‌ها و تحویل شدنی‌های پروژه را در نظر بگیرد.

اجرا

اهداف اولیه در این فاز تعریف نقاط آسیب‌پذیری و تعیین میزان اهمیت آن‌ها است. در این مرحله می‌بایست تکنیک‌ها و روش‌های ارزیابی را مشخص نمود. گرچه فعالیت‌های خاص این فاز با نوع ارزیابی متفاوت می‌باشد، پس از پایان این مرحله ارزیاب می‌تواند به تعریف سیستم، شبکه و آسیب‌ها، دست پیدا کند.

بعد از اجرا

در این فاز تمرکز بیش‌تر بر روی آنالیز نقاط آسیب شناسایی شده می‌باشد که در نهایت به شناسایی ریشه‌های اصلی و دادن سفارش لازم برای حداقل کردن خطرات و تهیه گزارش نهایی منجر خواهد شد.

۵-۱-۲- تکنیک‌های ارزیابی فنی

تکنیک‌های بسیار زیادی در زمینه آزمایش‌ها و تست‌های امنیت اطلاعات وجود دارد که وضعیت سیستم یا شبکه را مشخص می‌نمایند. رایج‌ترین این تکنیک‌ها از دیدگاه این فصل که در آینده بیش‌تر به آن خواهیم پرداخت در سه دسته زیر تقسیم شده‌اند:

۵-۱-۳- تکنیک‌های مروری:

این تکنیک‌ها در واقع تکنیک‌های آزمایش هستند که برای ارزیابی سیستم، کاربردها، شبکه، سیاست گذاری‌ها فرآیند پوشش آسیب‌ها، و دستورالعمل‌های عمومی بکار می‌روند. هم‌چنین شامل مستندات، وقایع، نتایج، مرور ساختار سیستم بررسی شبکه و چک‌های مربوط به فایل‌ها می‌شود. بخش سه به این تکنیک پرداخته خواهد شد.

۵-۱-۴- تکنیک‌های آنالیز و شناسایی اهداف

این تکنیک‌های تست می‌تواند سیستم، خروجی‌ها، سرویس‌ها، پتانسیل آسیب‌ها، را شناسایی و تعریف نمایید. این کار می‌تواند به‌طور دستی انجام شود ولی معمولاً به صورت اتوماتیک انجام می‌شود و شناسایی شبکه و سرویس‌ها و خروجی‌های آن را شامل می‌شود.

۵-۱-۵- تکنیک ارزیابی آسیب‌پذیری هدف

این تکنیک‌های آزمایش وجود آسیب‌پذیری را تائید می‌کنند و شاید بسته به تکنیک‌های خاص استفاده شده و مهارت تیم تست آن‌را به صورت دستی یا با استفاده از ابزارهای اتوماتیک انجام می‌دهند. تکنیک ارزیابی آسیب‌پذیری هدف شامل تجزیه رمزها، تست‌های نفوذ کردن، مهندسی اجتماعی و تست‌های ایمنی کاربردی می‌شود. اطلاعات بیش‌تر در زمینه این تکنیک‌ها را می‌توان در بخش ۵ پیدا کرد.

از زمانی که هیچ‌کدام از تکنیک‌ها نتوانست یک تصویر از ایمنی سیستم یا شبکه را آماده نماید، سازمان‌ها می‌بایست تکنیک‌های مناسب را برای تامین نمودن ارزیابی‌های ایمنی محکم با یک‌دیگر ترکیب نمایند. به‌طور مثال، تست نفوذ معمولاً بر انجام دادن پورت شبکه و مشخصات سرویس و تست آسیب‌پذیری بر مشخصات‌هاست‌ها و سرویس‌ها و شاید هدف‌ها برای نفوذ آینده تکیه می‌کند.

۵-۱-۶- مقایسه تست‌ها و آزمایش‌ها

آزمایشات اصولاً شامل بازخوانی مستندات مانند خطمشی‌ها، فرآیندها، هدف‌های ایمنی، نیازمندی‌های ایمنی، فرآیندهای عملیات استاندارد، دیاگرام‌های ساختاری، مستندات مهندسی، موجودی دارایی‌ها، پیکر بندی سیستم، قواعد، شاخه‌های سیستم می‌باشد. آن‌ها برای مشخص نمودن این که آیا سیستم به‌طور صحیح مستند گردیده است و برای بدست آوردن شناخت ظاهر ایمنی که تنها از طریق مستندات موجود می‌باشد، رهبری می‌شوند. این مستندات طراحی با برنامه، نصب، پیکر بندی، عمل‌کرد، و نگهداری سیستم‌ها و شبکه، و هم‌چنین بازخوانی و ارجاع جهت متقاعد نمودن پیروی و سازگاری را تعیین می‌کنند. برای مثال، نیازمندی‌های ایمنی محیطی بایستی مستنداتی شامل هدف‌های ایمنی سیستم و فرآیندهای عمل‌کرد استاندارد را پیش ببرد. بنابراین ارزیاب‌ها بایستی مطمئن باشند که تمامی هدف‌ها، فرآیندها، ساختارها، و پیکربندی‌ها با نیازمندی‌های ایمنی ثابت و خطمشی‌های قابل اجرا در یک راستا هستند. یک مثال دیگر، بازخوانی قوانین دیوارهای آتش است برای اطمینان از این که آن‌ها با خطمشی‌های ایمنی سازمان‌ها با توجه به استفاده اینترنت، مانند استفاده از پیغام‌های فوری، به اشتراک گذاشتن فایل‌های دو به دو، و دیگر قابلیت‌های اعمال محدودیت شده منطبق هستند.

۵-۱-۷- دیدگاه‌های استفاده از تست

۵-۱-۷-۱- داخلی و خارجی

تست امنیتی خارجی از خارج محیط امنیتی سازمان اجرا می‌شود. معمولاً از اینترنت یا هر ارتباط ورودی بیرون از سازمان اتفاق افتاده و با هدف معلوم کردن آسیب‌پذیری می‌تواند توسط حمله کننده خارجی استفاده شود.

استفاده از تست خارجی اغلب با تکنیک‌های شناسایی که داده‌های ذخیره شده عمومی را جست‌جو می‌کند، اطلاعات سرور، ثبت نمودن اطلاعات گروهی افرادی که در اینترنت فعالیت دارند، و دیگر اطلاعات عمومی در دسترس برای انتخاب اطلاعات. (به‌طور مثال، نام سیستم‌ها، آدرس‌های پروتکل اینترنتی، سیستم‌های عملیاتی، نشانه‌های تکنیکی از ارتباط)، آغاز می‌شود که می‌تواند به ارزیاب برای شناسایی آسیب‌پذیری، کمک نماید. سپس، شماره گذاری با استفاده از کشفیات شبکه و تکنیک‌های

استفاده از کاوش برای مشخص نمودن مهمان‌های خارجی و سرویس‌های شنود آغاز می‌شود. تا زمانی که محیط دفاعی مانند دیوار آتش، روترها، و لیست‌های کنترل دسترسی اغلب شکل ترافیکی اجازه داده شده به سوی شبکه داخلی را محدود می‌کنند، ارزیاب‌ها اغلب از تکنیک‌هایی که این تجهیزات دفاعی را شبیه سازی می‌کنند - درست همان طور که حمله کننده‌های خارجی می‌خواهند - استفاده می‌کنند. سرورهایی که به صورت خارجی قابل دسترسی‌اند برای آسیب پذیر بودن مورد تست قرار می‌گیرند زیرا ممکن است مورد دسترسی سرورهای داخلی قرار گیرند.

تست‌های داخلی به اندازه تست‌های خارجی محدودیت ندارند زیرا در جلو فایروال قرار می‌گیرند. اگر تست‌های داخلی و خارجی هم‌زمان اجرا شوند معمولاً تست‌های خارجی در اولویت قرار می‌گیرند این مسئله مخصوصاً وقتی بیش‌تر ین فایده را نشان می‌دهد که ارزیاب‌ها بخواهند هردو نوع تست را انجام دهند زیرا ممکن است با ارزیابی‌های بیرونی خطر صدمه خوردن از ناحیه تست‌های داخلی را به حداقل برسانند.

۵-۱-۸- تکنیک‌های پویش

تکنیک‌های پویش غیر فعال، سیستم‌ها برنامه‌های کاربردی شبکه‌ها، سیاست‌ها و رویه‌های کشف آسیب‌پذیری را، مورد بررسی قرار می‌دهند. آن‌ها هم‌چنین اطلاعات را به منظور تسهیل و بهینه سازی و سایر تکنیک‌های ارزیابی جمع آوری می‌نمایند. از آن جا که تکنیک‌های پویش در دسته حملات غیر فعال هستند، حداقل ریسک را برای سیستم‌ها و شبکه‌ها ایجاد می‌کنند این بخش چندین تکنیک بازنگری متداول را پوشش می‌دهد که عبارتند از: بازنگری مستند سازی، ثبت وقایع، مجموعه قوانین و پیکربندی سیستم، آزمایش مداوم شبکه و بررسی یک پارچی انجام فایل‌ها.

۵-۱-۹- بازنگری در مستند سازی

بازنگری مستند سازی تعیین می‌کند آیا جنبه‌های تکنیکی و فنی سیاست‌ها و رویه جاری عملی و جامع هستند. این مستندات مبنایی را برای وضع امنیتی سازمان فراهم می‌نمایند که البته غالباً در طول ارزیابی های فنی نادیده گرفته می‌شوند. گروه‌های امنیتی درون سازمان بایستی ارزیابی‌هایی را با قدرت مستندسازی مناسب جهت اطمینان از یک بازنگری جامع تدارک ببینند. مستندات فنی شامل:

سیاست‌ها، معماری‌ها و الزامات امنیتی، رویه‌ها و استانداردهای عملیاتی، برنامه‌های امنیتی سیستم و توافقنامه‌های درک و توافق پیوندهای سیستم و برنامه‌های ثبت رویداد می‌شوند.

مستند سازی می‌تواند ضعف‌ها و شکاف‌ها را که ممکن است منجر به فقدان با اجرای نامناسب کنترل‌های امنیتی شوند را کشف نماید. ارزیابی‌ها نوعاً تحقیق (بررسی) می‌کنند که مستندات سازمان تابع استانداردها و مقرراتی مثل FISMA هستند و در جست‌جوی سیاست‌های خطمشی‌های هستند که ناکارا و منسوخ می‌باشند. ضعف‌ها متداول مستند سازی شامل رویه‌ها یا پروتکل‌های امنیتی سیستم عامل هستند که دیگر مورد استفاده قرار نمی‌گیرد و شکست‌هایی (عدم موفقیت‌هایی) که شامل یک سیستم عامل جدید و پروتکل‌ها می‌شوند. بازنگری مستند سازی اطمینان نمی‌دهد که کنترل‌ها امنیتی به درستی اجرا شده‌اند. فقط از این اطمینان حاصل می‌نماید که هدایت و راهنمایی برای حمایت از زیر ساخته‌های امنیتی وجود دارد یا خیر.

ثبت بازنگری مستند سازی می‌تواند برای تنظیم دقیق سایر تکنیک‌های بررسی و آزمون مورد استفاده قرار گیرد برای مثال اگر یک سیاست مدیریت اسم رمز الزامات خاص برای حداقل کردن طول و پیچیدگی اسم رمز دارد، این اطلاعات می‌تواند از ابزارهای شکاف کلمه رمز جهت عمل‌کرد کاراکتر مورد استفاده قرار گیرد.

۵-۱-۱۰- بازنگری ثبت وقایع:

بازنگری ثبت وقایع مشخص می‌کند آیا کنترل‌های امنیتی ثبت اطلاعات درست هستند و آیا سازمان به سیاست‌های مدیریت ثبت وقایع وفادار است. به عنوان یک منبع اطلاعات تاریخی، ممیزی ثبت وقایع می‌تواند به تأیید سیستم در حال عمل کردن طبق سیاست‌های مقرر کمک نماید. به‌عنوان مثال، اگر سیاست ثبت وقایع بیان می‌کند که تمام تلاش‌ها می‌بایست ثبت شوند، بازنگری ثبت وقایع تعیین خواهد کرد آیا اطلاعات جمع آوری شده و سطح مناسبی از جزئیات را نشان می‌دهند. بازنگری ثبت وقایع هم‌چنین ممکن است مشکلاتی مثل خدمات پیکربندی نامناسب و کنترل‌های امنیتی، دسترسی‌های غیر مجاز و ورودی‌های غیر مجاز انجام شده را آشکار سازد به‌عنوان مثال، اگر یک سنسور سیستم کشف ورود بدون اجازه پشت یک دیوار آتش قرار بگیرید ثبت‌های انجام شده توسط آن می‌تواند جهت ارزیابی ارتباطی که دیوار آتش آن‌ها داده است. مورد استفاده قرار گیرد. اگر سنسور فعالیت‌هایی

که می‌بایست مسدود می‌شدند را ثبت نماید، نشان دهنده آن است که دیوار آتش به صورت ایمن پیکر بندی نشده است.

مثال‌هایی از اطلاعات ثبت وقایع که ممکن است هنگامی که ارزیابی‌های امنیتی فنی اجرا می‌شوند سودمند باشند عبارتند از:

ثبت‌های سیستم یا سرور تایید کردن ممکن است شامل تلاش‌های تایید موفق یا نا موفق باشد.

ثبت‌های سیستم شامل اطلاعات راه اندازی یا خاموش کردن سیستم و سرویس، نصب نرم افزار غیر مجاز، دسترسی به فایل تغییرات سیاست امنیتی، تغییر اکانت (به عنوان مثال، ایجاد و حذف اکانت، واگذاری حق انحصاری اکانت و به‌کارگیری امتیاز می‌باشد.)

ثبت سیستم شناسایی و ممانعت از ورود غیر مجاز ممکن است شامل فعالیت مغرضانه و استفاده نادرست باشد.

ثبت‌های دیوار آتش و مسیر یاب ممکن است شامل تماس‌های مربوط به خارج که ابزارهای به خط افتاده داخلی را مشخص می‌نماید، باشد.

ثبت های دیوار ممکن است شامل تلاش‌های برقراری تماس غیر مجاز و استفاده نا مناسب باشد.

ثبت‌های مربوط به استفاده ممکن است در برگیرنده تلاش‌های تماس غیر مجاز و تغییرات اکانت استفاده از امتیاز و اطلاع نحوه استفاده و به‌کارگیری پایگاه داده باشد.

ثبت‌های مربوط به ویروس کش ممکن است شامل به روز رسانی عدم موفقیت یا دیگر نشانه‌های امضا و نرم افزاهای منسوخ شده باشد.

ثبت‌های مربوط به ایمنی خصوصاً مدیریت وصله امنیتی و بعضی IDS و محصولات سیستم جلوگیری از ورود بدون اجاره، ممکن است اطلاعات را روی برنامه‌ای کاربردی و سرویس‌های آسیب پذیر شناخته شده ثبت نماید.

بازنگری ثبت وقایع به صورت دستی می‌تواند بسیار وقت گیر و خسته کننده باشد. ابزارهای ممیزی خودکار موجود به طور قابل ملاحظه‌ای می‌توانند زمان بازنگری را کاهش داده و گزارش‌های سفارش و از پیش تعریف شده‌ای را پدید آورند که محتوای ثبت را حذف کرده و رد آن‌ها را تا مجموعه‌ای از فعالیت‌های مشخص دنبال نمایند. ارزیاب‌ها هم‌چنین می‌توانند از این ابزارها جهت تسهیل تجزیه و تحلیل ثبت با تبدیل از فرمت‌های مختلف به فرمت ساده و استاندارد برای تجزیه و تحلیل استفاده نمایند. علاوه بر این، اگر ارزیاب‌ها در حال بازنگری یک فعالیت مشخص – مثل تعداد تلاش‌های ورود به سیستم ناموفق در یک سازمان باشند. آن‌ها می‌توانند از این ابزارها به منظور فیل‌تر کردن ثبت‌ها بر اساس فعالیت‌های بررسی شده استفاده نمایند.

۵-۱-۱۱- بازنگری تنظیمات

یک تنظیمات مجموعه‌ای از مقررات یا امضاهایی است که ترافیک شبکه یا فعالیت سیستم مورد مقایسه قرار می‌گیرند. تا مشخص گردد چه اقدامی انجام شود به عنوان مثال، ارسال یا رد کردن یک بسته، ایجاد یک علامت هشدار دهنده، یا اجازه دادن به یک رویداد سیستم بازنگری این تنظیمات به منظور حصول اطمینان از جامعیت و شناسایی (تشخیص) شکاف‌ها و ضعف‌های وسایل امنیتی و به طور کلی سیستم دفاعی لایه لایه مثل آسیب‌پذیری شبکه خطای شکستن سیاست و مسیرهای ارتباطی ناخواسته یا آسیب پذیر، انجام می‌شود. یک بازنگری هم‌چنین می‌تواند از ناکارآمدی‌هایی که اثر منفی بر روی عمل‌کرد تنظیمات دارد پرده برداری کند.

تنظیمات برای بازنگری شامل شبکه و دیوار آتش IDS/IPS و لیست‌های کنترل دسترسی مسیر یاب‌ها می‌باشد فهرست زیر مثال‌هایی از انواع بررسی‌هایی است که غالباً در بازنگری‌های تنظیمات انجام می‌پذیرد.

۵-۱-۱۲- برای دسترسی به سویچ‌ها

هر قانون همچنان مورد نیاز است (برای مثال قوانینی که برای اهداف موقت افزوده شده بودند به محض این که دیگر مورد نیاز نباشند، حذف می‌گردند.

تنها ترافیکی که رد هر سایت اجازه داده شده مجاز می‌باشد و همه ترافیک‌های دیگر با تصور غفلت تکذیب رد می‌گردند.

۵-۱-۱۳- تنظیمات دیواره آتش

تمام قوانین همیشه ضروری هستند. قوانین تاکید می‌کنند که کم‌ترین حق دسترسی وجود داشته باشد، مانند مشخص کردن فقط آدرس‌های IP و پورت‌هایی که مورد نیاز است.

برای قوانین مربوط به دیوار آتش میزبان محور، قوانین وجود نرم افزاری جاسوسی را نشان نمی‌دهند (مانند قوانین IDS/IPS)

مجموعه‌های غیر ضروری فعال می‌شوند یا از بین می‌روند تا تاییدیه‌های نابه‌جا از بین برداشته و عمل‌کرد بهبود یابد.

مجوزهای ضروری فعال شده و به صورت دقیق تنظیم شده و کاملاً نگهداری و مراقبت می‌شوند

۵-۱-۱۴- بازبینی و پیکر بندی سیستم

بازبینی و پیکر بندی سیستم یک فرآیند شناسایی نقاط ضعف کنترل کننده‌های پیکر بندی حفاظتی می‌باشد، مانند سیستم‌هایی که محکم نشده است یا طبق سیاست‌های امنیتی تنظیم نشده است. برای مثال این نوع بازبینی سرویس و فعالیت‌های غیر ضروری، تنظیمات نام کاربری و کلمه عبور نابه‌جا یا ورود تنظیمات پشتیبانی نابه‌جا را مشخص می‌کند.

مثال‌های پیکر بندی امنیتی که ممکن است مورد بازبینی واقع شوند تنظیمات سیاست‌های امنیتی ویندوز و فایل‌های پیکربندی امنیتی یونیکس و از این قبیل می‌باشند. ارزیاب‌ها از دستورالعمل‌های تکنیک بازبینی استفاده کرده به راهنما و چک لیست‌های پیکربندی امنیتی مشخص می‌کند تا تنظیمات سیستم جهت به حداقل رساندن ریسک‌های امنیتی تنظیم شود به منظور بازبینی دستی پیکربندی سیستم ارزیاب‌ها به تنظیمات متنوع امنیتی دسترسی پیدا می‌کند که بر روی دستگاه‌هایی قرار دارد که مورد سنجش واقع شده‌اند و آن‌ها را با تنظیمات پیش‌نهادی که در چک لیست‌ها آمده‌اند مقایسه کنند. تنظیماتی که حداقل استانداردهای امنیتی را اضافه نمی‌کنند، علامت گذاری شده و

گزارش می‌شوند. پروتکل خودکار کردن محتوای امنیتی (SCAP) یک روش برای استانداردهای ویژه است که مدیریت و اندازه گیری آسیب گذاری خودکار و سنجش خطمشی را قادر می‌سازد.

ابزارهای دیگر می‌توانند به منظور بازاریابی و گزارش تنظیمات امنیتی بکار گرفته شوند و راهنمای جبران (درمان) را فراهم می‌آورند.

ابزارهای خودکار اغلب به صورت مستقیم بر روی دستگاه‌های که مورد ارزیابی واقع می‌شوند بکار می‌روند ولی می‌توانند بر روی سیستم‌های با دسترسی شبکه‌ای نیز بکار گرفته شوند.

این در حالی است که بازبینی پیکر بندی سیستم اتوماتیک خودکار سریع‌تر از روش‌های دستی هستند. البته تنظیماتی که می‌بایست به صورت دستی چک شوند هر دو روش دستی و اتوماتیک به دسترسی به سر شاخه فایل‌های مدیر اداره کننده احتیاج دارند. به صورت کلی به‌تر که چک اتوماتیک به جای چک دستی انجام شود. تست اتوماتیک می‌توانند خیلی سریع‌تر انجام شود و نتیجه جداگانه و تکرار پذیر بدست آورد. هرچند که تست کردن دستی صدها هزاران تنظیمات بسیار خسته کننده و خطا پذیر است.

۵-۱-۱۵- شنود شبکه

شنود شبکه یک تکنیک غیر فعال آشکار ساز ارتباط شبکه، پروتکل‌های رمز کننده و آزمایش بر چسب و.. می‌باشد که اطلاعات مهم را علامت گذاری می‌کند گذشته از این به عنوان یک تکنیک بازبینی استفاده می‌شود. شنود شبکه می‌تواند به عنوان یک تکنیک شناسایی و تجهیزیه تحلیل مقصد نیز بکار رود. ، دلایل استفاده از شنود شبکه به قرار زیر است.

- ضبط کردن پاسخ‌گویی نقل انتقالات شبکه.

- انجام جست‌جوی غیر فعال شبکه (به عنوان مثال شناسایی دستگاه‌های فعال موجود در شبکه)

- شناسایی سیستم عامل، فعالیت‌های غیر مجاز و نابه‌جا مانند نقل و انتقالات رمز نشده اطلاعات حساس

- جمع آوری اطلاعات مانند نام کاربری و کلمات عبور رمز گذاری نشده

- شنود شبکه، اثر کمی در سیستم دارد ولی اثرات قابل توجیهی بر پهنای باند دارد.

شنودگر وسیله‌ای که شنود شبکه را میسر می‌سازد احتیاج به یک وسیله دارد که به شبکه متصل باشد مانند یک هاب گذرگاه اتصال یا یک سوئیچ متصل به گستره پورت‌ها.

محدودگر پورت‌ها فرآیندی است که از ترافیک ارسالی به پورتی که این دستگاه به آن متصل است کپی تهیه می‌کند. سازمان‌ها می‌توانند شنودگرهای شبکه را به جاهای مختلف شبکه بکار گیرند مراکز معمول بکارگیری آن‌ها به قرار زیر است.

در یک محدوده محیط، به منظور بازرسی ترافیک ورودی و خروجی شبکه.

پشت دیوار آتش، به منظور بازرسی قوانین فیلترینگ ترافیک.

یکی از محدودیت‌های بکارگیری شنود شبکه، استفاده از رمز گذاری می‌باشد، خیلی از حمله کنندگان از مزایای رمزگذاری جهت مخفی کردن فعالیت‌هایشان بهره می‌برند. در این صورت ارزیابی ارتباطات انجام شده را مشاهده می‌کنند ولی قادر به دیدن محتوای آن‌ها نیستند دیگر از محدودیت‌های شنود شبکه این است که فقط قادر به کنترل قسمت کوچکی از شبکه در آن جا نصب شده‌اند می‌باشند. این عامل سبب می‌شود ارزیاب مجبور باشد بین قسمت‌های مختلف در حرکت باشد. ارزیابی‌ها ممکن است برای پیدا کردن یک پورت فیزیکی باز به چالش بر خورد کند به علاوه شنود شبکه یک فعالیت پرزحمت بوده که نیازمند حضور افراد با درجه بالای تخصص می‌باشند که ترافیک شبکه را به خوبی تقسیم نماید.

۵-۱-۱۶- تست کردن سلامت فایل

آزمایش کردن سلامت فایل یک روش شناسایی فایل‌ها را مهیا می‌کند که تغییر کرده‌اند و یک نمونه از فایل‌های محافظت شده را ذخیره کرده و یک پایگاه داده پایدار را فراهم می‌کند. نمونه ذخیره شده بعداً مورد پردازش مجدد قرار گرفته تا مقادیر ذخیره شده مقایسه و فایل‌های تغییر کرده شناسایی می‌کند.

یک قابلیت آزمایش‌گر سلامت فایل معمولاً همراه یک IDS میزبان محور است.

اگر چه آزمایش‌گر سلامت فایل نیاز به وجود افراد تخصص بالا ندارد ولی باید به صورت دقیق بکار گرفته شود تا از اثر بخشی آن اطمینان حاصل شود. آزمایش سلامت فایل به بیش‌تر ین اثر زمانی دارد تا فایل‌ها سیستم با پایگاه داده مرجع چک شوند که از یک سیستم ایمنی تهیه شده‌اند این کار باعث می‌شود که از سلامت فایل‌های پایگاه داده اطمینان حاصل نمود پایگاه داده مرجع باید به صورت آن لاین تهیه شود تا از حملات حمله کننده‌ها درامان باشد و ردپای آن‌ها با تصحیح پایگاه داده پوشش داده شود به علاوه به دلیل اعمال پچ (Patch)های مختلف فرآیند فایل‌های تغییر یافته، پایگاه داده می‌بایست مدام به روزی رسانی شود.

به منظور استفاده از آزمایش‌های سلامت فایل می‌بایست از یک رمزگذاری بومی استفاده کرد تا از سلامت پایگاه داده تهیه شده اطمینان حاصل نمود.

۵-۱-۱۷- خلاصه

جدول ۱-۳ خلاصه قابلیت‌ها مهم تکنیک‌های بازبینی مشروح در بخش ۳ می‌باشد.

قابلیت‌ها	تکنیک
*سنجش خط‌مشی‌ها و روال‌ها برای دقت فنی و تکامل	بازبینی مدارک
*فراهم آورنده تاریخچه اطلاعات در مورد استفاده هم پیکر بندی و تصحیح *آشکار کننده خطاهای سیاست‌ها و مشکل‌های بالقوه می‌باشد.	بازبینی ثبت وقایع
*آشکار کننده روزنه‌های موجود و مجموعه قوانین کنترل امنیتی می‌باشد.	بازبینی مجموعه قوانین
*قدرت پیکر بندی سیستم را سنجش می‌کند. *بررسی می‌کند که آیا سیستم‌ها بر اساس سیاست مقاوم سازی پیکر بندی شده‌اند.	بازبینی پیکر بندی سیستم

*ترافیک شبکه را در یک قسمت محدود آشکار کرده تا اطلاعاتی نظیر سیستم‌های فعال، سیستم‌های عامل، پروتکل ارتباط، سرویس‌ها و عمل‌کردها را ضبط نماید. *بررسی رمز گذاری ارتباط.	شنود شبکه
*تغییر فایل‌های مهم را بررسی و می‌تواند شکل مخصوص از فایل‌های ناخواسته مانند ابزارهای معروف حمله کنندگان را شناسایی کرده.	آزمایش سلامت فایل

جدول ۱-۳

میزان خطر پذیری به هر تکنیک و ترکیب آن وابسته است، به منظور اطمینان از اجرای سالم و دقیق تمامی روش‌های فوق، هر ارزیاب باید مهارت‌های پایه‌ای مشخصی را داشته باشد.

جدول ۲-۳ خطوط راهنماهایی را فراهم آورد که بیان گر حداقل مهارت‌های لازم هر یک از تکنیک‌ها می‌باشد که در بخش ۳ ارائه شده است.

مجموعه مهارت‌های پایه‌ای	تکنیک
دانش عمومی امنیتی از یک دورنمای خط‌مشی	بازبینی مدارک
دانش قالب‌های ثبت وقایع و توانایی تغییر داده‌های ثبت وقایع، توانایی استفاده از تجزیه و تحلیل اتوماتیک ثبت وقایع و اجزا وابسته	بازبینی نسبت وقایع
دانش قالب‌های مجموعه قوانین و ساختار آن‌ها توانایی تجزیه و تحلیل مجموعه قوانین دستگاه‌های متنوع	بازبینی قوانین
دانش پیکر بندی امنیتی سیستم، شامل مستحکم سازی سیستم تحلیل و پیکربندی خط‌مشی امنیتی برای سیستم‌های عامل متنوع، توانایی استفاده از	بازبینی پیکر بعدی سیستم

ابزار آزمایش اتوماتیک پیکر بندی امنیتی	
مجموعه مهارت‌های پایه‌ای	تکنیک
دانش عمومی کنترل پروتکل‌ها (TCP/IP)و دانش شبکه ،توانایی تفسیر و تحلیل ترافیک شبکه، توانایی به‌کارگیری و استفاده ابزارهای شنود	شنود شبکه
دانش عمومی فایل‌های سیستم، توانایی استفاده از ابزارهای آزمایش سلامت فایل اتوماتیک و تغییر نتایج.	آزمایش سلامت فایل

جدول۲-۳ مجموعه مهارت‌های پایه‌ای برای ارزیابی تکنیک‌ها

۵-۲- تکنیک‌های تجزیه و تحلیل و تعیین هدف:

در این بخش روش‌های تجزیه و تحلیل هدف بررسی می‌شود که به تشخیص اجزای فعال و بخش‌های جانبی آن‌ها و آنالیز خطرات بالقوه متمرکز شده‌اند. ارزیاب با استفاده از این اطلاعات به جست‌جوی اجزای در معرض خطر می‌پردازد. سازمان‌ها اغلب از روش‌های غیر تکنیکی اضافه یا روش‌های تکنیکی برای تعیین و آنالیز این موارد استفاده می‌کنند. مثلاً ممکن است فهرست دارائی‌ها یا لیست‌های دیگر مد نظر قرار گیرد، مثال دیگری تشخیص ارزیاب از دارایی‌های مشهود است که با روش‌های تکنیکی پیدا نمی‌شوند، نظیر میزبان‌هایی که وقتی روش‌های تکنیکی انجام می‌شدند از شبکه قطع بودند.

۵-۲-۱- کشف شبکه:

در کشف شبکه از چند روش برای تعیین میزبان‌های فعال، ضعف تشخیص و فهم نحوه کار شبکه استفاده می‌شود. هر دو روش غیر فعال (آزمایش) و فعال (تست) برای کشف اجزاء در یک شبکه قابل استفاده است. روش‌های غیر فعال با استفاده از یک دریچه شبکه ترافیک، شبکه را نظارت کرده و آدرس‌های IP میزبان‌های فعال را ثبت می‌کنند و می‌توانند گزارش کنند که کدام بخش در حال استفاده و کدام سیستم عامل در شبکه کشف شده است. کشف غیر فعال هم‌چنین می‌تواند روابط بین میزبان‌ها شامل ارتباطات هر میزبان با دیگران، تعداد ارتباط برقرار شده و نوع ترافیکی که داشته‌اند را معین نماید و معمولاً به عنوان یک میزبان در شبکه داخلی عمل می‌نماید که بر ارتباطات آن‌ها نظارت

می‌کند. این فرآیند بدون ارسال یک سیگنال انجام می‌شود. کشف غیر فعال زمان بیش‌تری برای جمع آوری در مقایسه با کشف فعال صرف می‌نماید و میزبان‌هایی که در دوره بررسی ترافیک ارسال یا دریافت ندارند، ثبت نمی‌شوند.

روش‌های فعال انواع مختلفی از بسته‌های شبکه را می‌فرستند نظیر پروتکل پیام کنترل اینترنت[۱] که برای درخواست پاسخ از میزبان‌های شبکه عموماً با استفاده از یک ابزار اتوماتیک بکار می‌روند. فعالیت موسوم به تعیین سیستم عامل، ارزیاب را برای تعیین سیستم عامل با ارسال ترکیبی از ترافیک شبکه نرمال، غیر نرمال و مجاز معین می‌نماید. فعالیت دیگر شامل ارسال بسته‌ها به تعدادی پورت مشترک برای تولید پاسخ است که پورت‌های فعال را معین می‌کند. ابزار پاسخ‌ها را تجزیه و تحلیل کرده و آن‌ها را با نتایج یک سیستم عامل و سرویس‌های شبکه‌ی استاندارد مقایسه می‌کند و آن را قادر می‌سازد تا میزبان‌ها، سیستم عامل‌هایی که وجود دارند را، پورت‌های آن‌ها و وضعیت این پورت‌ها را تعیین نماید.

از این اطلاعات برای اهدافی نظیر جمع آوری اطلاعات هدف برای آزمایش، تولید نقشه مسیر، تعیین دیواره‌های آتش و ترکیب IDS و کشف خطرات در سیستم‌ها و ترکیب شبکه استفاده می‌شود. ابزار کشف شبکه از روش‌های مختلفی برای جمع آوری اطلاعات استفاده می‌کند. دیوارهای آتش و سیستم‌های کشف مقدماتی می‌تواند از اسکن‌های اولیه به ویژه آن‌هایی که از اغلب بسته‌های تأییدیه استفاده می‌نمایند. (نظیر اسکن SYN/FIN و اسکن NULL) بهره‌برداری نمایند. ارزیابی‌هایی که کشف از طریق دیوار آتش و سیستم‌های آشکار سازی را طراحی می‌کنند باید نوع اسکن‌هایی را مد نظر داشته باشند که نتایج را بدون متوجه شدن سیستم مورد ارزیابی حاصل نماید و این که با یک روش آرام و آهسته برای افزایش شانس موفقیت عمل نمایند. ارزیاب‌ها باید موقع انتخاب انواع اسکن که باعث از کار افتادن سیستم می‌شود، مراقب باشند. معمولاً بهترین اسکن نزدیک فعالیت عادی است که تشابه کم‌تری برای مسایل عملیاتی ایجاد نماید.

در کشف شبکه می‌توان اجزای تأیید نشده در حال کار در شبکه را هم تعیین کرد. به عنوان مثال، در سازمانی که فقط از سیستم عامل‌های محدودی استفاده می‌کند می‌توان سریعاً اجزای تأیید نشده را که

۱ICMP

با دیگری متفاوتند معین کرد وقتی یک جزء خطرناک مشخص شده در نقشه شبکه موجود آن در جانمایی کرده و مشخص می‌کند که به کدام قسمت شبکه وصل است.

چند ابزار برای کشف شبکه وجود دارد و باید توجه شود که ابزارهای بسیار زیادی هم برای اسکن و روش‌های غیر فعال وجود دارند. اغلب یک واسطه‌ی گرافیکی مصرف کننده (GUI) پیش‌نهاد می‌شود و هم‌چنین واسطه‌ی خطی دستور هم مناسب است.

یادگیری واسطه‌های خط دستور طولانی تراز GUIS است چرا که تعداد دستورات و سوئیچ‌های مشخص کننده تست‌هایی که باید انجام شود بیش‌تر است و ارزیاب باید آموزش بیش‌تری ببیند. هم‌چنین ماژول‌هایی برای ابزارهای سرورهای باز نوشته شده است که به ارزیاب اجازه می‌دهد تا به راحتی خروجی ابزار را بفهمد. مثلاً ترکیب قابلیت‌های خروجی ابزارهای XML و یک دیتابیسی ایجاد شده می‌تواند ابزار قوی ایجاد نماید که شبکه را برای تشخیص سرویس غیرمجاز بررسی نماید. آموزش این که دستورات زیاد چه می‌کنند و چگونگی ترکیب آن‌ها به‌ترین روش کمک به یک مهندس امنیتی مجرب است. بسیاری از متخصصین مجرب فن‌آوری اطلاعات از جمله نگهدارنده‌ی شبکه و سایر مهندسین شبکه باید بتوانند نتایج را بررسی نمایند، اما کار با ابزار کشف بیش‌تر توسط یک مهندس امنیت انجام می‌شود.

چند مزیت کشف فعال در مقایسه با کشف غیر فعال این است که دسترسی از شبکه‌ی مختلف قابل انجام است و معمولاً به زمان کم‌تری برای جمع آوری اطلاعات مورد نیاز است. در کشف غیر فعال باید اطمینان از این که همه‌ی میزبان‌ها دارای ترافیک معمولی هستند تا بررسی آن‌ها ممکن گردد. ممکن است زمان زیادی را صرف گردد به ویژه وقتی با شبکه‌های بزرگی کار می‌کنیم. یک عیب کشف فعال این است که نویز شبکه تولید می‌کند. از آن جا که کشف فعال درخواست‌هایی را برای دریافت پاسخ ارسال می‌نماید، این فعالیت اضافی شبکه می‌تواند ترافیک را پایین آورده و بسته را در قسمت ضعیف شبکه بنشاند، کشف فعال می‌تواند هشدارهای IDS را فعال نماید، چرا که بر خلاف کشف غیر فعال به نقطه‌ی اصلی ارجاع می‌شود. توانایی کشف موفقیت آمیز همه‌ی سیستم‌های شبکه می‌تواند تحت تأثیر محیطی که اجزای شبکه محافظت می‌شوند و روش‌ها و امنیت اولیه‌ی اجزا قرار گیرد. مثلاً در محیطی که از ترجمه‌ی آدرس شبکه (NAT) استفاده می‌شود که به سازمان‌ها اجازه می‌دهد آدرس‌های IP داخلی غیر عمومی داشته باشند که به آدرس‌های عمومی برای ترافیک‌های خروجی ترجمه می‌شوند را

نمی‌توان خارج از شبکه به‌طور صحیح کشف کرد. دیوارهای آتش تشخیص ممکن است کشف جزء هدف را مسدود نماید. اطلاعات ناصحیح حاصل از سعی در فعالیت شناسایی اجزا ممکن است بدست آید. اطلاعات حاصله از نتایج کشف فعال باید به نوع چیدمان شبکه‌ی هدف ارتباط داده شود.

در هر دو کشف فعال و غیر فعال اطلاعات دریافتی به ندرت کاملاً صحیح هستند. فقط میزبان‌هایی که موقع کشف روشن و وصل هستند تشخیص داده می‌شوند. اگر سیستم‌ها یا بخشی از شبکه در زمان ارزیابی خاموش باشند فاصله‌ی بالقوه زیادی در کشف وجود دارد. هم‌چنین کشف غیر فعال فقط اجزائی را که در زمان کشف اطلاعات را ارسال یا دریافت می‌کنند، پیدا می‌کند، از تولیداتی نظیر نرم افزارهای مدیریت شبکه برای قابلیت کشف مداوم و تولید اتوماتیک هشدار وقتی یک جزء در شبکه حاضر باشد می‌توان استفاده کرد. در کشف مداوم می‌توان محدوده‌های آدرس‌های IP برای آدرس‌های جدید یا بررسی درخواست‌های آدرس جدید IP را انجام داد. هم‌چنین ابزارهای کشف بسیاری را می‌توان به‌طور برنامه‌ریزی شده و نظیر یک زمان خاص در هر چند روز فعال کرد. این کار نسبت به استفاده موقتی از ابزار نتایج صحیح‌تری خواهد داد.

۵-۲-۲- تعیین سرویس و پورت شبکه:

تعیین سرویس و پورت شبکه با استفاده از یک اسکنر پورت برای تشخیص پورت‌های شبکه و خدمات عملیاتی میزبان‌های فعال نظیر FTP و HTTP و کاربردهایی که از اجرای هر سرویس مشخص حاصل می‌شود نظیر سرور اطلاعاتی اینترنتی مایکروسافت (IIS) یا خدمات HTTP انجام می‌شود سازمان‌ها باید مدیریت پورت‌های شبکه و تعیین سرویس را برای تشخیص میزبان‌ها اگر قبلاً به روش دیگری انجام نشده است (نظیر کشف شبکه) انجام دهند و خدمات خطرناک بالقوه را علامت بزنند. از این اطلاعات برای تعیین اهداف آزمایش‌های بالقوه استفاده می‌شود.

اسکنرهای پایه می‌توانند پورت‌های باز و میزبان‌های فعال را تشخیص دهند، اما چند اسکنر هم قادر به تولید اطلاعات اضافی در میزبان اسکن شده هستند. برای جمع آوری اطلاعات یک پورت باز حین اسکن برای تشخیص سیستم عامل هدف از فرآیند تشخیص سیستم عامل استفاده می‌شود.

از چند نوع اسکنر می‌توان در تشخیص یک پورت خاص با فرآیند موسوم به تعیین سرویس استفاده کرد. اسکنرها از یک فایل سرویس استفاده می‌نمایند که شماره‌های پورت‌های عمومی و نوع سرویس

آن را لیست کرده است. مثلاً اسکنری که تشخیص می‌دهد TCP پورت ۸۰ یک میزبان باز است گزارش می‌دهد که یک سرور Web در آن پورت وجود دارد اما مراحل دیگری مورد نیاز است تا این شناسایی نهایی گردد.

اسکنرهایی برای تشخیص ارتباطات مشاهده شده از یک پورت و آنالیز آن برای تعیین نوع سرویس با مقایسه فعالیت کشف شده با اطلاعات جمع شده قبلی استفاده می‌شوند. از این روش‌ها هم‌چنین می‌توان برای تعیین کاربرد سرویس و ورژن آن و حتی نوع سیستم عامل استفاده کرد. روش اسکن بی عیب هم نیست چرا که یک سیستم ایمنی می‌تواند سدهای عبور را تغییر دهد یا سایر مشخصات را با هدف حفظ ماهیت سرور عوض نماید. به هر حال روش اسکن از روش‌های ساده اسکن فایل سرور مناسب‌تر است.

مدل‌های اسکنر از روش‌های مختلف اسکن با نقاط قوت و ضعف که در مستندات آن‌ها آمده حمایت می‌کنند. مثلاً چند نوع از اسکنرها از طریق دیوارهای آتش به‌تر عمل می‌کنند در حالی که بقیه برای داخل دیوار آتش به‌تر کار می‌کنند. نتایج بسته به پورت استفاده شده متفاوت خواهند بود. پاسخ بعضی اسکنرها با یک جواب ساده برای هر پورت باز یا بسته می‌باشد در حالی که بقیه‌ی جزئیات بیش‌تری را شامل می‌شوند (نظیر فیل‌تر شده یا فیل‌تر نشده) که می‌تواند به ارزیاب در تعیین سایر اسکن‌ها برای جمع آوری اطلاعات بیش‌تر کمک کند.

برای تعیین سرویس و پورت شبکه از آدرس‌های IP حاصل از کشف شبکه اسکن قطعات استفاده می‌شود. اسکن‌های پورت را می‌توان به‌طور مستقل در داخل بسته‌های آدرس‌های IP اجرا کرد. در این جا اسکن پورت با حالت پیش فرض از طریق تشخیص میزبان‌های فعال داخل شبکه انجام می‌شود. نتیجه‌ی کشف شبکه و پورت شبکه و تعیین سرویس لیستی شامل همه‌ی اجزای فعال در فضای آدرس که به ابزار اسکن پاسخ داده‌اند را تشکیل می‌دهد. سایر اجزای فعال هم می‌تواند موجود باشد که به اسکن پاسخ نداده‌اند، نظیر آن‌هایی که خاموش بودند یا با دیواره‌ی آتش محافظت شده‌اند.

برای کشف این اجزا اسکن آن‌ها با قرار دادن اسکنر در قسمتی که به این اجزا دسترسی دارد یا غلبه بر دیواره‌ی آتش با اسکن نوع دیگر استفاده نماید (نظیر اسکن Xmas یا SYN/FIN).

توصیه شده است که اگر هر دو اسکن خارجی و داخلی استفاده می‌شود ارزیاب آزمایش‌ها را بدون اولویت انجام دهد. اسکن‌های خارجی باید اول انجام شود. با این روش می‌توان بررسی و مقایسه را قبل و در حین انجام آزمایش‌های داخلی انجام داد. در حال انجام اسکن‌های خارجی ارزیاب می‌تواند از هر روش بهینه‌ای استفاده نماید تا بسته‌ها را از طریق دیواره‌ی آتش از کشف IDS یا IPS دریافت نماید. ابزار برای جداسازی، دو برابر شدن، ادغام خارج از محدوده و روش‌های زمانی برای عوض کردن بسته‌ها استفاده می‌شوند تا آن‌ها را وارد سیستم نموده و شباهت بیش‌تری به ترافیک پیش‌نهادی داشته باشند.

در تست‌های داخلی تمایل به استفاده از روش‌های اسکن کم‌تر پیشرفته است چرا که این اسکن‌ها پیچیدگی کم‌تری نسبت به اسکن‌های خارجی دارند. استفاده از اسکن‌های پیشرفته‌تر داخلی احتمال موفقیت عمل‌کرد مناسب بدون نیاز به بهبود نتایج اسکن را افزایش می‌دهد. ایجاد توانایی اسکن شبکه با بسته‌های سفارشی هم برای تست‌های داخلی ممکن است، چرا که تست برای خطرات ویژه نیاز به بسته‌های سفارش زیادی دارد. ابزار با توانایی ساخت بسته برای این فرآیند مفید هستند. وقتی بسته تولید می‌شود می‌توان آن‌ها را از طریق برنامه‌ی اسکن دوم که نتایج را جمع می‌کند ارسال کند. از آن جایی که بسته‌های سفارشی می‌تواند یک سرویس خطر (DOS) را تحریک کند، این نوع از آزمایش‌ها باید در طول دوره ترافیک شبکه پایین نظیر شب یا در تعطیلات انجام شود.

اگرچه اسکنرهای پورت، میزبان‌های فعال را شناسایی می‌کنند، سیستم‌های عامل، پورت‌ها، خدمات و کاربردها، اما آن‌ها نمی‌توانند خطرات را تشخیص دهند. بررسی‌های بیش‌تری نیاز است تا حضور پروتکل‌های نا امن را تأیید کنند (نظیر پروتکل انتقال فایل [TFTP]، کارکردهای تأیید نشده و خدمات خطرناک و... ، برای تشخیص خدمات خطرناک، ارزیاب تعداد و نوع خدمات را با لیستی از ورژن‌های خطرناک مقایسه می‌کند یا اسکن اتوماتیک را مطابق شرح بخش (۳-۴) انجام می‌دهد. با اسکنرهای پورت، فرآیند اسکن در سطح زیادی اتوماتیک است اما اولویت بندی اطلاعات اسکن شده انجام نمی‌شود.

اگرچه اسکن پورت با مصرف باند شبکه و کاهش زمان پاسخ عمل‌کرد شبکه را مختل می‌کند، اما سازمان را قادر می‌سازد تا مطمئن شود میزبان‌های تأیید شده‌ای برای خدمات شبکه در اختیار دارد. انتخاب نرم افزار اسکن باید با دقت کافی انجام شود تا اختلال حاصل از اسکن پورت را حداقل کند.

۵-۲-۳- اسکن تهدید:

مشابه تشخیص سرویس و پورت شبکه، اسکن تهدید میزبان‌ها و جزئیات آن‌ها (نظیر سیستم عامل کاربردها، پورت‌های باز) را تشخیص می‌دهد، و سعی دارد تهدیدات را بیش از نقش دخالت انسان نتایج اسکن معین نماید. اسکنرهای تهدید زیادی مجهز به تجهیزات پذیرش نتایج از کشف شبکه و تشخیص خدمات و پورت شده‌اند که حجم کار مورد نیاز برای اسکن تهدید را کاهش می‌دهند. هم‌چنین اسکنرهایی هستند که می‌توانند کشف شبکه‌ی و پورت شبکه و بررسی را انجام دهند. اسکن تهدید می‌تواند به تعیین ورژن نرم افزار تاریخ گذشته، مسیرهای فراموش شده و ترکیب نادرست و مقایسه‌ی معتبر منتج از سیاست ایمنی سازمان کمک کند. این فعالیت‌ها با تعیین سیستم عامل و اجرای نرم افزار اصلی بر روی میزبان و تطبیق با اطلاعات تهدیدات شناخته شده. شبکه سورت شده در پایگاه اطلاعاتی تهدیدات انجام شود.

اسکن تهدید می‌تواند:

- قابلیت‌ها را با کارکرد میزبان و سیاست‌های ایمنی چک کند.
- اطلاعات اهداف برای آزمایش خطرات را تهیه کند.
- اطلاعات چگونگی کاهش تهدیدات را تهیه کند.

اسکنرهای تهدید را می‌توان بر علیه میزبان محلی یا شبکه اجرا کرد. چند اسکنر پایه شبکه‌ی دارای سنجش پایه کاربر بر روی میزبان‌های جدا قابل اجراست و می‌تواند اطلاعات میزبان‌ها را توزیع کند. سایر اسکنرهای شبکه پایه چنین ویژگی ندارند و باید در اسکن شبکه هدایت شوند تا میزبان‌ها را مشخص و سپس این میزبان‌ها را برای تهدیدات اسکن کنند. در چنین حالت‌هایی اسکن شبکه پایه ابتدا استفاده می‌شود. تا کشف شبکه انجام و پورت باز را معین و تهدیدات مربوطه در بیش‌تر حالت‌ها را آشکار نماید، این فرآیند با سیستم عامل هدف محدود نمی‌شود. اسکن شبکه‌ی پایه را می‌توان هم داخلی و هم خارجی انجام داد و البته اسکن داخلی معمولاً بیش‌تر تهدیدات را نمی‌پوشاند اما آزمایش از هر دو روش مهم‌تر است. اسکن خارجی باید با اجزای ایمنی که ترافیک را مسدود می‌نماید محاسبه شود، محدود کردن ارزیابان به اسکن فقط پورت به عبور از ترافیک کمک می‌کند.

ارزیابانی که اسکن خارجی را انجام می‌دهند ممکن است مواردی شبیه کشف شبکه نظیر NAT یا دیوارهای آتش میزبان را پیدا کنند. برای غلبه بر مسایل NAT و هدایت اسکن شبکه پایه ارزیابان می‌تواند از مسئول دیوار آتش سؤال کند تا پورت را به آدرس IP یا گروهی از آدرس‌ها هدایت کند. ارزیاب هم‌چنین می‌تواند دیوارهای آتش میزبان پایه را مجهز به آدرس‌های IP در طول دوره‌ی ارزیابی نماید. این مراحل ارزیاب را در ورود به شبکه کمک می‌کند، اما به‌طور کامل نمی‌تواند قابلیت حجم خارجی را منعکس نماید، اگرچه ممکن است شاخص بهتری از توانایی‌های مهاجم داخلی یا خارجی را برای ارزیاب به میزبان دیگر شبکه وجود داشته باشد. ارزیاب‌ها هم‌چنین می‌توانند هر میزبان را جداگانه اسکن نمایند. برای اسکن تهدید محلی، یک اسکنر در هر میزبان مورد نظر برای اسکن نصب می‌شود. این کار ابتدا با تعیین سیستم عامل میزبان و عدم تطابق کارکرد و تهدیدات انجام می‌شود. اسکن محلی قادر به آشکار سازی تهدیدات در سطح بالاتری از جزئیات در مقایسه با اسکن شبکه پایه است چرا که اسکن محلی معمولاً شرایط هر دو میزبان (محلی) و مجذور آن را ارزیابی می‌کند. بعضی اسکنرها قابلیت اعمال عدم تطبیق محلی را هم دارند.

یک اسکنر تهدید نسبتاً سریع عمل کرده و برای کمّی کردن خطرات سازمان راه آسانی است. یک تهدید سطحی ضعف در تفکیک مستقل از سایر تهدیدات است. رفتارهای سیستم و خروجی‌های پاسخ به تهدید ارسالی توسط اسکنر با تهدیدات مشخص مقایسه می‌شوند و ابزار هر تطبیق مشاهده شده‌ای را گزارش می‌نماید. غیر از اسکن پایه، چند اسکنر تهدید می‌توانند الگوی حمله را تشخیص و نمونه سازی تهدیدات شبیه سازی کننده تهدیدات پیدا شده را با این روش گزارش کنند که خیلی مفید است.

یک مشکل در تعیین سطح ریسک تهدیدات این است که آن‌ها واقعاً جدا هستند. مثلاً چند تهدید ریسک پایین می‌تواند وجود داشته باشند که ممکن است با ترکیب آن‌ها ریسک بالایی ظاهر شود. اسکنرها قادر به آشکار سازی تهدیدهایی که منتج از ترکیب الگوهای حمله هستند، نیستند. ابزار می‌تواند یک ریسک پایین به هر تهدید تخصیص دهد و ارزیاب را در تعیین امنیت به اشتباه بیاندازد. یک روش مطمئن‌تر برای تعیین ریسک تهدید مسیر آزمایش است که در بخش (۲-۵) توضیح داده شده است.

مسئله‌ی دیگر در تعیین سطح ریسک تهدیدات این است که اسکنرها اغلب از روش اولویت بندی خودشان برای تعیین سطوح استفاده می‌کنند. مثلاً یک اسکنر ممکن است از سطح پایین، متوسط و بالا

استفاده کند در حالی که اسکنر دیگری ممکن است از اطلاعات سطح، پایین متوسط و بالا و بحرانی استفاده نماید. این مسأله مقایسه نتایج اسکنرهای متفاوت را مشکل می‌کند. البته سطوح ریسک تخصیص داده شده با یک اسکنر ریسک واقعی را نمی‌توان منعکس نمود.

به عنوان مثال یک اسکنر یک سرور FTP را با دیسک متوسط مشخص می‌کند چرا که پسورد را به صورت یک متن منتقل می‌کند، اما در سازمان از سرور FTP به عنوان یک سرور عمومی که از پسورد استفاده نمی‌کند بهره‌برداری می‌شود. لذا ریسک واقعی ممکن است نشان داده نشود ارزیاب باید سطح ریسک مناسب را برای هر تهدید معین نماید و به سادگی سطح تهدید تخصیصی توسط اسکنرهای تهدیدات را نپذیرد.

اسکن تهدید شبکه- پایه چند نقطه ضعف بزرگ دارد. وقتی شبکه کشف می‌شود این نوع از اسکن تهدیدات را فقط برای سیستم‌های فعال پوشش نمی‌دهد. معمولاً تهدیدات سطحی را پوشش می‌دهد و قادر به آدرس دهی سطح ریسک کلی شبکه اسکن شده نیستند. اگرچه فرآیند به تنهایی در سطح بالایی خودکار است، اسکنرهای تهدید می‌توانند یک نسبت خطای اشتباهی بالایی داشته باشند (بدین معنی که تهدیداتی گزارش شوند که وجود ندارند).

یک تیم مجهز با سیستم ایمنی sdsjl uhlg باید نتایج را ارزیابی کند و به دلیل این که اسکن شبکه پایه نیاز به اطلاعات بیش‌تری در مقایسه با اسکن پورت دارد تا تشخیص مطمئنی از تهدیدات بر روی یک میزبان حاصل شود. لذا ترافیک شبکه بیش‌تری ایجاد می‌شود. این مسأله یک اثر منفی روی میزبان‌های با شبکه‌های اسکن شده می‌تواند ایجاد کند، یا در قسمتی از شبکه ترافیک زیادی ایجاد نماید. هم‌چنین اسکنرهای تهدید زیادی شامل تست‌های شبکه پایه برای حملات DOS وجود دارند که برای ارزیاب غیر ماهر مؤثر است می‌تواند یک اثر منفی روی میزبان اسکن شده بگذارد. اسکنرها اغلب به تست‌های حمله DOS اجازه انجام می‌دهد تا ریسک اثر میزبان طی آزمایش را کاهش دهد.

محدودیت بزرگ دیگر اسکنرهای تهدید شبیه اسکنرهای ویروس و IDS این است که آن‌ها نقشی از خود به جا می‌گذارند. این ویژگی به ارزیاب قابلیت تکرار اسکنر برای شناسایی آخرین تهدیدات را ایجاد می‌نماید. قبل از اجرای هر اسکنی، ارزیاب باید آخرین به روز رسانی دیتابیس تهدیدات را نصب نماید. تناوب به روز رسانی یک نکته اساسی در انتخاب اسکنر تهدید است. اغلب اسکنرهای تهدید به ارزیاب

اجازه اسکن در سطوح مختلف را می‌دهد که قابلیت بالاتری می‌دهد. از آن جا که اغلب اسکن پیشرفته ممکن است تهدیدات بیش‌تری آشکار کرده باعث کند شدن فرآیند اسکن کلی می‌گردد. غیر از این در اسکن تهدید بسیار مهم است که تهدیدات کاهش یابد قبل از این که آن‌ها کشف گردند.

همانند سایر ابزار تطبیق الگو، اسکنرهای تهدید معمولاً نسبت‌های مثبت خطای بالایی دارند. ارزیابان باید اسکنرها را کالیبره کنند تا هر دوی خطاهای مثبت و منفی را حداقل کنند و نتایج را برای ارزیابی تهدید واقعی بهینه نمایند. اسکنرها هم‌چنین نسبت‌های بالاتری از خطای منفی را ارائه می‌دهند که سایر ابزار را بهینه می‌نماید. اما تهدیدات آشکار نشده با اسکنرهای اتوماتیک به طور بالقوه توسط اسکنرهای تهدید دیگر با شکل‌های دیگری از تست آشکار می‌شوند. یک الگوی عمومی، استفاده از اسکنر چندگانه است که ارزیاب را برای مقایسه‌ی نتایج کمک می‌کند.

۵-۲-۴- اسکن بدون سیم:

تکنولوژی‌های بدون سیم در ساده‌ترین حالت آن یک یا چند وسیله را قادر به برقراری ارتباط بدون نیاز به اتصال فیزیکی نظیر شبکه یا کابل‌های جانبی می‌نماید. محدوده‌ی آن‌ها از تکنولوژی‌های ساده نظیر کیبوردها و موس‌های بدون سیم تا شبکه‌های پیچیده‌ی تلفن همراه و شبکه‌های محلی بدون سیم (WLAN) را می‌پوشاند.

هم‌زمان با افزایش تعداد و قابلیت‌های اجزای بی‌سیم برای سازمان‌ها مهم است تا محیط بدون سیم را به طور ایمن بتوانند تست کنند. اسکن‌های بدون سیم به سازمان‌ها کمک می‌کنند تا اقدامات اصلاحی برای کاهش ریسک حاصل از تکنولوژی‌های بدون سیم را انجام دهند.

عوامل زیر در محیط سازمان‌ها وقتی سیستم‌های ایمنی تکنیکی طراحی می‌شوند باید مد نظر قرار گیرند:

- موقعیت تجهیزات مورد اسکن، با توجه به محدوده‌ی فیزیکی یک ساختمان تا یک محیط عمومی (نظیر خیابان‌ها و محیط‌های مشترک عمومی) یا موقعیت آن در یک محیط خیلی شلوغ ممکن است خطرات ریسک را افزایش دهد.
- سطح ایمنی اطلاعات مورد انتقال با تکنولوژی بدون سیستم.

⌑ وسیله هر چند مرتبه یک‌بار از محیط وصل و قطع می‌شوند و سطح ترافیک عمومی برای قطعه بدون سیم چقدر است؟ (یعنی فعالیت مقطعی یا فعالیت ثابت)- این به این علت است که فقط قطعات بدون سیم فعال در طول دوره اسکن قابل کشف هستند.

⌑ وضعیت جاری آشکار سازی و سیستم‌های محدود کننده (WIDPS)، که ممکن است قبلاً اطلاعات لازم برای تست جمع آوری شده‌اند.

اسکن بدون سیستم باید با کمک یک وسیله موبایل با نرم افزارهای آنالایزر نصب شده نظیر یک کامپیوتر قابل حمل، وسایل دستی یا وسایل خاص انجام گردد. نرم افزار اسکن یا ابزار باید اجازه‌ی تنظیم سیستم برای اسکن را به اپراتور بدهد و تا تغییرات مورد نیاز شرایط ایمنی سازمان را بتواند اعمال نماید.

در بعضی موارد، قطعه باید به یک آنتن خارجی وصل شود تا یک سطح بالاتری از فرکانس رادیو (RF) ایجاد شود. تکنولوژی‌های پشتیبان بدون سیم نظیر بلوتوث به ارزیابی حضور سایر خطرات بدون سیم کمک می‌کند.

توجه شود که قطعاتی که از تکنولوژی‌های غیر استاندارد یا فرکانس‌های خارج از محدوده‌ی فرکانس RF اسکن آشکار نمی‌شود یا توسط ابزار اسکن به‌طور کامل تشخیص داده نمی‌شوند. ابزاری نظیر آنالیزر طبق RF به سازمان در تعیین انتقال بین محدوده‌ی فرکانسی طیف کمک می‌کند. اسپکتروم آنالیزها معمولاً در محدوده‌ی وسیع فرکانس (حدود ۳ تا ۱۸ گیگاهرتز) را می‌پوشاند و هم‌چنین این قطعات آنالیز ترافیک را انجام نمی‌دهند، آن‌ها ارزیاب را قادر می‌سازند تا فعالیت بدون سیم را در محدوده‌ی فرکانس مشخصی معین نماید و تست‌های اضافی و آزمایشات را انجام دهد.

چند قطعه هم‌چنین نقشه‌ی جانمایی قطعات را با کمک یک ابزار نقشه کش انجام می‌دهند و در بعضی مواقع از سیستم موقعیت یاب جهانی (GPS) بر اساس نقشه حمایت می‌کنند. ابزار اسکن بی‌سیم پیشرفته این اجازه را به مصرف کننده می‌دهند تا بتواند با ورود یک نقشه با طرح در ترسیم موقعیت فیزیکی قطعه‌ی کشف شده کمک کند. (این مهم است که توجه شود که GPS محدودیت ظرفیت ورودی را دارد.)

افراد با یک درک قوی از شبکه‌ی بی سیم- به ویژه فن‌آوری IEEE ۸۰۲. ۱۱ a/b/g/n- با ابزار اسکن بی سیم می‌تواند کار کنند.

این اپراتورها باید روی قابلیت و ظرفیت ابزار اسکن بی سیم و نرم افزار آموزش ببینند تا فهم بهتری از جمع آوری اطلاعات حاصل نمایند و آمادگی لازم برای پیدا کردن فعالیت‌های خطرناک بالقوه را پیدا کنند.

افراد با چنین مهارت‌هایی برای آنالیز اطلاعات و نتایج اسکن بی سیم باید در اختیار باشند. اپراتور ابزار اسکن باید از مضرات سیگنال‌های RF برای استفاده در محیطی که باید اسکن شود، آگاه شد.

۵-۲-۵- اسکن بدون سیم غیرفعال:

روش اسکن غیرفعال برای اندازه گیری ایمنی بی سیم قبلاً مدون شده است، نظیر WIDPCS- از ابزار اسکن بی سیم برای اسکن کاملاً غیرفعالی که اطلاعاتی را منتشر نمی‌کنند، استفاده می‌شود و این ابزار به هیچ وجه اثری روی عمل‌کرد شبکه‌ی بی سیم ندارد. با عدم انتقال اطلاعات، یک ابزار اسکن غیرفعال توسط سایر استفاده کنندگان و سایر اجزاء مخفی می‌ماند. این مسأله احتمال کشف افراد در آشکار سازی و قطع اجزای شبکه‌ی بی سیم را کاهش می‌دهد. ترافیک بی سیم حاصل از ابزار اسکن غیر فعال توسط طیفی از آنتن‌های ابزار منتقل می‌شود. بیش‌تر ابزار شامل چند کلید مربوط به ابزار بی سیم کشف شده هستند از جمله تعیین کننده‌ی نوع سرویس (SSID)، نوع قطعه، کانال، آدرس کنترل دسترسی به وسیله‌ی (MAC)، قدرت سیگنال و تعداد بسته‌هایی که می‌توانند منتقل شوند. از این اطلاعات در ارزیابی امنیت محیط بدون سیم استفاده می‌شود و برای تشخیص قطعات بالقوه خطرناک در محدوده‌ی قطعات اسکن شده استفاده می‌شود. ابزار اسکن بی سیم باید بتواند بسته‌ها را برای تشخیص احتمال اختلال عمل‌کردی بررسی نماید.

ابزارهای اسکن بی سیم نظیر IEEE ۸۰۲. ۱۱ a/b/g/n کانال فرکانس به‌طور مجزا اغلب برای چند صد میلی ثانیه در زمان بکار می‌روند. ابزار اسکن غیر فعال نمی‌توانند همه‌ی انتقالات روی یک کانال مشخص را دریافت کنند. مثلاً ابزار ممکن است در حال اسکن کانال ۱ در لحظه‌ی به خصوصی باشد وقتی یک قطعه بی سیم یک بسته را در کانال ۵ انتقال می‌دهد. این مسأله نشان دهنده‌ی اهمیت تنظیم زمان فعالیت ابزار به اندازه‌ای طولانی است تا همه‌ی بسته‌ها را دریافت کند و به اندازه‌ای کوتاه

باشد تا هر کانال را به‌طور مؤثر اسکن نماید. ترکیب زمان فعالیت به قطعه یا ابزار مورد استفاده در اسکن بی سیم را دارد. به علاوه افراد امنیتی متصدی ابزار اسکن باید به آرامی از محیط اسکن شده بروند تا تعداد قطعات آشکار نشده کاهش یابد.

اجزای معیوب به چند طریق در اسکن غیر فعال مشخص می‌شوند:

- آدرس‌های MAC یک قطعه بی سیم کشف شده نشان می‌دهد که واسطه‌ی بی سیم چگونه است. اگر یک سازمان فقط نقش واسط بی سیم در قسمت‌های A و B را ایفا کند، حضور واسطه در سایر قسمت‌ها نشاندهنده‌ی قطعات معیوب است.

- اگر یک سازمان ثبت قطعات بی سیم را به طور صحیح انجام دهد ارزیاب می‌تواند آدرس‌های MAC قطعات کشف شده را با آدرس‌های MAC قطعات صحیح مقایسه کند. بیش‌تر ابزار به ارزیاب اجازه می‌دهند تا لیستی از قطعات بازرسی شده را وارد کند. از آن جا که آدرس‌های MAC می‌تواند محدود کننده داشته باشند، ارزیاب نباید فرض کند که آدرس‌های MAC قطعات کشف شده صحیح هستند. اما چک کردن آدرس‌های MAC می‌تواند قطعات زیادی را که از محدود کننده‌ها استفاده نکرده‌اند آشکار کند.

- قطعات خطرناک ممکن است از SSIDS استفاده کنند که به وسیله‌ی سازمان شناسایی نمی‌شوند.

- بعضی قطعات ممکن است از SSIDS استفاده کنند که به وسیله‌ی سازمان تشخیص داده شوند اما در شرایط ترکیب ایمنی بی سیم مد نظر قرار نگیرند.

قدرت سیگنال اجزای معیوب بالقوه باید بررسی شوند تا محل استقرار قطعات مشخص گردد که در کجای محل اسکن شده قرار دارند.

قطعاتی که در خارج یک مجموعه‌ی سازمانی کار می‌کنند ممکن است ریسک بالایی داشته باشند چرا که اجزای سازمان ممکن است به‌طور ناصحیح به آن‌ها نسبت داده شوند.

۵-۲-۶- اسکن بی سیم فعال:

سازمان‌ها می‌توانند از اسکن بی سیم غیر فعال به اسکن بی سیم فعال حرکت کنند. این ترکیب روی اطلاعات جمع شده در طی اسکن غیر فعال و سعی در پیدا کردن قطعات و آزمایش خطرناک مربوطه انجام می‌شود. مثلاً سازمان‌ها می‌توانند از اسکن بی‌سیم فعال در تعیین قطعات بدون سیم برای اطمینان از این که شرایط بدنه‌ی ایمنی بی سیم رعایت می‌شود، استفاده کنند- شامل روش‌های تشخیص، جمع آوری اطلاعات و سطوح دسترسی اگر این اطلاعات از سایر روش‌های قبلی قابل جمع آوری نبودند.

سازمان‌ها باید در اسکن فعال مراقبت نمایند تا قطعات و اجزای سازمان مجاور را در محدوده خودشان در نظر بگیرند. این مهم است که زمان تغییر فیزیکی قبل از اسکن فعال آن‌ها محاسبه گردد. سازمان‌ها هم‌چنین در انجام اسکن فعال قطعات معیوب دقت نمایند تا قطعات موجود در تجهیزات سازمانی را ارزیابی نمایند.

چنین قطعاتی می‌توانند متعلق به یک بازدید کننده باشند که به‌طور مستقل دسترسی بی سیم دارد یا یک سازمان مجاور با قطعه‌ای که از نظر مشخصات مشابهت دارد اما در داخل مجموعه نیست. معمولاً سازمان‌ها باید روی تعیین اجزای معیوب و موقعیت مکانی آن‌ها بیش‌تر از انجام اسکن فعال روی آن‌ها متمرکز شوند. سازمان‌ها می‌توانند از اسکن فعال در زمان انجام آزمایش‌های عیب یابی اجزای بی سیم خود استفاده کنند.

از ابزار برای حملات و عمل‌کرد، اندازه‌گیری سطح ایمنی بکار رفته و محاسبه‌ی سطوح ایمنی اجزا استفاده می‌شود. مثلاً ابزار برای آزمایش‌های عیب یابی بی سیم سعی می‌کنند تا به نقطه‌ی دسترسی (AP) از طریق روش‌های مختلف به ترکیبات ایمنی راه یابند. اگر ابزار بتواند به AP دسترسی داشته باشد می‌تواند اطلاعات را اخذ و شبکه با سیم را تشخیص داده و اجزای بی سیم را که به AP وصلند، مشخص نماید. چند ابزار فعال هم‌چنین می‌توانند خطرات کشف شده در اجزا را گزارش یا آزمایش‌های عیب یابی را مطابق شرح بخش ۴ انجام دهند.

مادامی که اسکن فعال انجام می‌شود، WIDPS، سازمان می‌تواند آن را نظارت کرده تا عمل‌کرد و قابلیت‌های خود را ارزیابی نمایند. بسته به اهداف ارزیابی، ارزیاب مسئول این اسکن‌ها ممکن است نیاز داشته باشد تا به مسئولین WIDPS و شبکه‌ی بی سیم اطلاع دهد تا آن‌ها برای آلارم‌ها و هشدارهای

احتمالی آماده باشند. به علاوه از ترکیب چند WIDPS برای صرف نظر از هشدار و آلارم تحریک شده توسط یک قطعه خاص نظیر آن که اسکن روی آن انجام می‌شود، استفاده کنند.

همچنین ابزار و فرآیندهایی برای تعیین اجزای معیوب و خطرات روی شبکه‌های بی سیم را می‌توان برای مشخص کردن قطعات با سیم مشکل دار استفاده کرد. اسکن قسمت سیم دار فرآیند دیگری است که برای کشف موقعیت احتمالی اجزای معیوب استفاده می‌شود. بخش ۵-۳ و ۱-۴ اسکن سیم دار را بررسی کرده‌اند.

جست‌جوی موقعیت اجزای بی سیم:

افراد امنیتی که ابزار اسکن بی سیم را بکار می‌برند باید بتواند موقعیت اجزا را پیدا کنند. سیگنال RF به طریقی نسبت به محیط پخش می‌شود که اهمیت آن‌را برای اپراتور جهت فهم نحوه‌ی پشتیبانی تکنولوژی بی سیم از این فرآیند نشان می‌دهد. نقشه‌ی توانمندی در اینجا مفید است اما فاکتور اصلی مورد نیاز برای حمایت از این قابلیت یک اپراتور ماهر و یک آنتن بی سیم می‌باشد.

اگر قطعه‌ی معیوب و موقعیت فیزیکی آن در طی فرآیند اسکن بی سیم کشف شود، اپراتور باید مطمئن شود که سیاست مشخص و فرآیند لازم برای قطعه‌ی کشف شده را می‌داند.

نظیر خاموش کردن آن، تطابق مجدد آن با سیاست سازمان یا حذف کامل جزء معیوب. اگر قطعه باید برداشته شود، پرسنل امنیتی باید عمل‌کرد قطعه‌ی معیوب را قبل از جابه‌جایی ارزیابی کنید. این کار با نظارت انتقالات و دسترسی به قطعه انجام می‌شود.

اگر قطعات بی‌سیم کشف شده را نتوان در زمان اسکن مستقر کرد، پرسنل امنیتی باید با استفاده از WIDPS برای استقرار قطعه‌ی کشف شده تلاش کنند. لازمه‌ی این کار استقرار آدرس‌های MAC در WIDPS است که در زمان اسکن کشف شده است. احتمالاً استفاده از WIDPS قابلیت کمک به پرسنل امنیتی در استقرار این قطعات را ایجاد می‌کند و معمولاً استفاده‌ی چند گانه از سنسورهای WIDPS در احتمال استقرار قطعات مفید است. از آن جا که WIDPS تنها قادر به استقرار یک قطعه در چند جا است، یک ابزار اسکن بی سیم جهت استقرار قطعات مورد نیاز است.

۵-۲-۷- اسکن بلوتوث:

برای سازمان‌هایی که می‌خواهند شرایط ایمنی بلوتوث خود را برآورد کنند اسکن غیر فعال برای قطعات بی سیم دارای بلوتوث باید انجام شود تا فعالیت‌ها چک گردند. از آن جا که بلوتوث برد محدودی دارد، به‌طور متوسط ۹ متر (۳۰ فوت) چنین قطعاتی برد کمی حدود یک متر (۳ فوت) دارند. لذا اسکن آن‌ها سخت و زمان بر می‌تواند باشد. ارزیاب‌ها باید محدودیت برد را در زمان انجام این نوع اسکن مد نظر داشته باشند.

ممکن است سازمان بخواهد فقط در محیطی که تجهیزات آن برای عموم قابل دسترسی است اسکن انجام دهد. برای دیدن این که اگر مهاجمان بخواهند از طریق بلوتوث حمله کنند، یا این که اسکن را در یک نمونه‌ای از مکان فیزیکی به جای اجرا در کل محیط انجام دهد. از آن جا که بسیاری از قطعات دارای بلوتوث (نظیر تلفن‌های همراه، تجهیزات تخصصی دیجیتال (PDA)) قابل حمل هستند انجام چند بار، اسکن غیر فعال در یک دوره‌ی زمانی مورد نیاز است. سازمان‌ها هم‌چنین تجهیزات زیر بنایی نظیر نقاط دسترسی را اسکن نمایند. اگر نقاط دسترسی مشکل‌دار کشف شوند، سازمان باید مطابق فرآیند و سیاست جاری آن را حل نماید.

چند نوع ابزار برای آزمایش فعالیت امنیتی و عمل‌کردی قطعات بلوتوث در دسترس است. این ابزار سعی در ارتباط با قطعات کشف شده و انجام حملات برنامه‌ریزی رشده به قطعات بلوتوث دار دارند. ارزیابان باید خیلی مراقب انجام اسکن فعال باشند چراکه قطعات بلوتوث دار مختلف در محیط حضور داشته که در بسیاری از مکان‌ها آن را می‌بینیم. به عنوان یک قاعده‌ی کلی ارزیاب باید فقط زمانی از اسکن فعال استفاده کند، که مطمئن باشد قطعه‌ی مورد نظر متعلق به سازمان است. از اسکن فعال می‌توان در ارزیابان مد ایمنی در جایی که یک قطعه بلوتوث دار کار می‌کند، استفاده کرد و قدرت اعداد مشخصه کلمه عبور را چک کرد (PIN). از اسکن فعال هم‌چنین می‌توان برای صحه گذاری این که این قطعات دارای حداقل قدرت مورد نیاز برای محدود کردن برد آن‌ها هستند، استفاده کرد.

مطابق قاعده IEEE ۸۰۲. ۱۱ a/b/g/n قطعات بلوتوث دار معیوب باید وفق قانون و سیاست سازمان بررسی شوند.

۵-۳- خلاصـــه:

جدول ۱-۴- مهم‌ترین قابلیت‌های تکنیک‌های آنالیز و تعیین هدف در بخش ۴ را خلاصه کرده است:

تکنیـــک	قابلیت‌هـــا
کشف شبکه	- کشف قطعات فعال - تعیین مسیرهای ارتباطی و امکانات تعیین ساختمان شبکه
پورت شبکه و تعیین سرویس	- کشف قطعات فعال - کشف پورت‌های باز و کاربردهای خدمات مربوطه
اسکن خطرات	- تعیین پورت‌های باز و میزبان‌ها - شناسایی خطرات شناخته شده (توجه: دارای نسبت مثبت خطاهای بالا) - اغلب برای کاهش خطرات کشف شده‌ی قطعات بکار می‌رود
اسکن بی‌سیم	- تعیین قطعات بی‌سیم غیر مجاز در محدوده‌ی اسکن‌ها - کشف سیگنال‌های خارج از محدوده‌ی سازمان‌ها - آشکار سازی خطرات بالقوه و تهدیدات امنیتی

جدول ۴-۱- روش‌های آنالیز و تعیین هدف

برای هر روش و ترکیب آن‌ها ریسک مخصوص به خود وجود دارد. برای اطمینان از این که همه به طور ایمن و صحیح اجرا می‌شوند، هر ارزیاب باید حداقل مهارت‌هایی را داشته باشد.

جدول ۴-۲- راهنمایی برای حداقل مهارت‌های مورد نیاز برای هر روش ارائه شده در بخش ۴ داده شده است.

روش	مهارت‌های مورد نیاز
کشف شبکه	دانش عمومی شبکه و ICP/IP: توانایی استفاده از هر دوی ابزار کشف شبکه‌ی فعال و غیر فعال
پورت شبکه و تعیین سرویس	دانش عمومی شبکه و TCP/IP: دانش پورت و مقررات برای سیستم‌های عامل: توانایی استفاده از ابزار اسکن پورت، توانایی استخراج نتایج از ابزار
اسکن خطرات	دانش عمومی شبکه و TCP/IP: شناسایی پورت‌ها و مقررات- خدمات و خطرات برای سیستم‌های عامل- توانایی استفاده از ابزار اسکن اتوماتیک و تحلیل نتایج
اسکن بی‌سیم	دانش عمومی محاسبه و انتقال امواج رادیویی به علاوه دانش تخصصی مقررات بی سیم- خدمات و پیکر بندی‌ها- توانایی استفاده از اسکن بی‌سیم اتوماتیک و ابزار مربوطه

جدول۴-۲- مهارت‌های مورد نیاز برای روش‌های آنالیز و تعیین هدف

۵-۴- روش‌های اعتبار سنجی آشکار سازی تهدیدات هدف:

در این بخش روش‌های اعتبار سنجی آشکار سازی تهدیدات اهداف که از اطلاعات تولیدی تشخیص هدف استفاده و برای آنالیزهای آن‌ها در تهدیدات بالقوه بکار می‌رود. مقصد اثبات وجود تهدید و ارائه‌ی راهکار به بخش امنیتی برای اقدام در زمان واقعه است. اعتبار سنجی آشکار سازی تهدیدات سطح تحمل ریسک در ارزیابی را بالا می‌برد، چراکه این روش‌ها قابلیت بیش‌تری در اثر روی سیستم‌های هدف یا شبکه بیش از سایر روش‌ها دارند.

۵-۴-۱- قفل شکن کلمه عبور:

وقتی یک مصرف کننده یک کلمه عبور را وارد می‌کند، یک الگو از رمز وارد شده تولید و با یک الگوی ذخیره شده از کلمه عبور واقعی مقایسه می‌شود. اگر الگوها تطابق داشته باشند، مصرف کننده تأیید می‌شود. قفل شکنی کلمه عبور فرآیند کشف کلمه عبور از الگوی ذخیره شده‌ی رمز در سیستم کامپیوتر یا خط انتقال شبکه است. این کار معمولاً در دوره‌ی ارزیابی برای کشف ضعف کلمه عبور انجام می‌شود. قفل شکن کلمه عبور روی الگوی رمز که در یک شبکه تشکیل شده یا از سیستم هدف حاصل شده است که برای سطح دسترسی مسئول شبکه نیاز است یا دسترسی فیزیکی به سیستم هدف انجام می‌شود. وقتی که الگو به دست آمد، یک قفل شکن کلمه عبور اتوماتیک خیلی سریع الگوهای اضافی را تولید می‌کند تا یک تطبیق حاصل شود، یا این که ارزیاب نتواند قفل شکنی را با موفقیت انجام دهد.

یک روش برای تولید الگو حمله دیکشنری است که از همه‌ی کلمات دیکشنری یک فایل متن استفاده می‌کند. دیکشنری‌های زیادی روی اینترنت در دسترس است که زبان‌های مهم و عادی، نام‌ها، شوهای تلویزیونی عمومی و... را می‌پوشاند. یک روش دیگر قفل شکن هجوم هایبریدی است که از روش دیکشنری حروف و اعداد را به کلمات دیکشنری اضافه می‌کند. بسته به قفل شکن کلمه عبور مورد استفاده در این نوع از هجوم می‌توان ترکیبات مختلفی از حروف و اعداد قابل استفاده است (نظیر P@ssword و H۴chml). امکان اضافه مشخصات و اعداد در شروع و خاتمه‌ی کلمات دیکشنری (نظیر Password & % و Password۹۹) نیز وجود دارد.

هم‌چنین روش دیگر قفل شکن کلمه عبور به نام روش کلیه حالات[۱] وجود دارد. در این روش همه‌ی رمزهای عبور تا یک طول مشخص و الگوهای مربوطه تولید می‌شود.

اگرچه کلیه حالات می‌تواند زمان زیادی ببرد اما نسبت به اغلب روش‌های تغییر کلمه عبور کمتر طول می‌کشد. در نتیجه کلمه عبورهای کشف شده هنوز خیلی ضعیف هستند. به طور تئوری همه‌ی رمزهای عبور توسط هجوم به روش کلیه حالات قابل رمز گشایی است اگر زمان و نیروی انسانی کافی صرف شود، اگرچه ممکن است سال‌ها طول بکشد، و نیروی محاسباتی خیلی قوی مورد نیاز باشد. ارزیابان و مهاجمان ماشین‌های چند منظوره‌ای دارند که وظیفه‌ی کشف رمز را تقسیم و زمان واقعی خیلی کمتر از مقادیر پیش بینی شده است.

رمز گشایی را با میز تطبیق هم می‌توان انجام داد که با الگوهای پیش فرض مقایسه می‌کند. مثلاً یک میز تطبیق را می‌توان ایجاد کرد که هر رمز ممکن با حروف داده شده با طول مشخص را تولید کند. ارزیاب‌ها سپس میز را جست‌جو می‌کند. الگوی رمز مورد نظر را پیدا کند. میزهای تطبیق مقادیر متنابهی از فضای ذخیره در اختیار دارند و زمان زیادی برای تولید صرف می‌کند اما توجیه اولیه‌ی آن این است که الگوی رمز با استفاده از غیر مؤثر نماید. ترکیب کلی یک جزء تصادفی از اطلاعات در فرآیند الگوی رمز است که جای‌گزین یک کلمه عبور مشابه یک الگوی رمز است. میزهای تطبیق بدون اعمال ترکیب در محاسبات نتایج صحیحی نمی‌دهند. اما به طور وحشتناکی فضای حافظه‌ی مورد نیاز میز را زیاد می‌کند.

سیستم‌های عامل مختلفی از مکانیزم الگوی رمز ترکیبی برای کاهش ضعف میزهای تطبیق و رمز گشاهای دیگر استفاده می‌کنند.

رمز گشایی را می‌توان در طول ارزیابی برای مقایسه سیاست امنیتی با مقایسه‌ی کلمه عبور اصلی اجرا کرد. مثلاً اگر سازمان یک سیاست رمز دوره‌ای داشته باشد رمز گشایی را می‌توان در مقطع تعویض رمز انجام داد. اجرای رمز گشایی به طور offline اثر خیلی کمی روی سیستم یا شبکه دارد یا بی اثر است و این نقطه قوت در سیاست رمز سازمان و صحه گذاری بر آن مؤثر است.

---

۱ Bruth force

۵-۴-۲- آزمایش‌های کشف:

آزمایش‌های کشف تست‌های امنیتی است که ارزیاب هجوم واقعی برای تشخیص روش‌های صدمه به سیستم یا شبکه را انجام می‌دهد. این کار شامل حمله‌ی واقعی به سیستم واقعی و اطلاعاتی است مهاجم از ابزار و روش‌ها توأمان استفاده می‌کند. اغلب تست‌های کشف از ترکیب تهدیدات روی یک یا چند سیستم است که دسترسی بیش‌تری به تهدیدات مجزا را می‌دهد. آزمایش‌های کشف را هم‌چنین می‌توان برای تعیین موارد زیر انجام داد:

- چگونگی توزیع واقعی سیستم الگوی مهاجم.

- سطح مشابهت پیچیدگی یک مهاجم نیاز به تجمیع سیستم دارد.

- سایر مواردی که خطرات سیستم را کاهش می‌دهد.

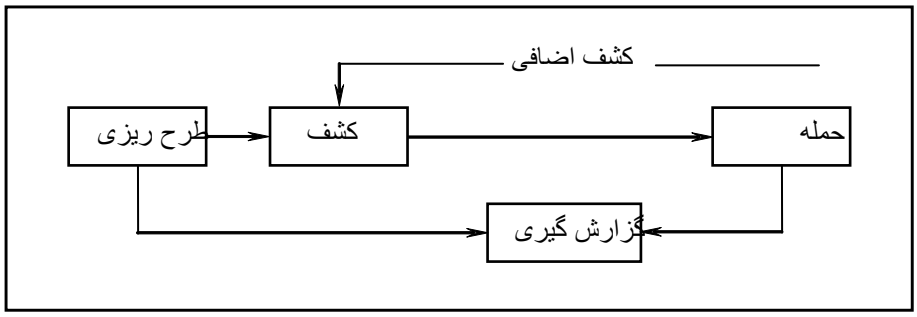
- توانایی مدافعان برای آشکار سازی اهداف و پاسخ مناسب.

تست‌های کشف می‌تواند ارزشمند باشد اما تجهیزات سرمایه‌ای زیادی نیاز دارد تا ریسک سیستم‌های هدف را کاهش دهد. سیستم‌ها ممکن است خراب شود. در طول تست غیر فعال گردد، اگر چه تست‌های تهدید پیشرفته ریسک را کاهش می‌دهد، اما به طور کامل قابل حذف نیست. تست‌های کشف را فقط بعد از بررسی کامل، برنامه‌ریزی و طرح ریزی باید انجام داد.

تست‌های کشف اغلب شامل روش‌های غیر تکنیکی حمله می‌شود. مثلاً یک آزمایشگر کشف می‌تواند کنترل ایمنی فیزیکی را تحت تأثیر قرار دهد اما ارتباط به شبکه، اخذ اطلاعات حساس (احتمالاً با نصب قطعات کلیدی) و سایر موارد یا منجر به قطع ارتباط شود. وقتی تست‌های امنیتی فیزیکی انجام می‌شود نکات لازم باید مد نظر قرار گیرد. نگهبانان امنیتی باید در مورد ارزش فعالیت آموزشگرها آموزش ببینند نظیر یک نقطه ارتباط برای اتصال یا مستند سازی را فرا بگیرند. معنی دیگر روش‌های غیر تکنیکی استفاده از مهندسی اجتماعی، نظیر میز تست و... می‌باشد. اطلاعات اضافی تست‌های امنیتی فیزیکی، روش‌های مهندسی اجتماعی و سایر معانی روش‌های غیر تکنیکی موارد مربوط به این محدوده هستند.

۵-۴-۳- مراحل تست:

شکل ۵-۱- چهار فاز تست‌های کشف را نشان می‌دهد. در فاز طرح ریزی قواعد مشخص می‌شود، تأیید مدیریت نهایی و مستند شده و اهداف تست مشخص می‌گردد. فاز طراحی کارهای زیر بنایی را برای تست موفق کشف را انجام می‌دهد. هیچ آزمایش واقعی در این تست انجام نمی‌شود.



شکل ۵-۱ چهار فاز تست‌های کشف

فاز کشف تست تهدید شامل دو قسمت است. قسمت اول شروع تست‌های واقعی و پوشش اطلاعات جمع آوری شده و اسکن شده است. تشخیص پورت شبکه و سرویس مطابق شرح بخش ۲-۴- برای تشخیص هدف بالقوه انجام می‌شود. به علاوه برای تشخیص سرویس و پورت، از سایر روش‌ها برای جمع آوری اطلاعات برای شبکه‌ی هدف استفاده می‌شود:

اطلاعات نام و آدرس IP را می‌توان از روش‌های متعددی جمع آوری کرد نظیر NIC (WHOIS) و کشف شبکه (معمولاً فقط در تست‌های داخلی).

اطلاعات نام و آدرس پرسنل را می‌توان با جست‌جو در سرور Web سازمان بدست آورد.

طلاعات سیستم شبیه نام‌ها و مشترکین را از روش‌هایی نظیرNet BIOS(معمولاً فقط در تست‌های داخلی) و سیستم‌های اطلاعاتی شبکه(NIS) (معمولاً فقط در تست‌های داخلی)

اطلاعات سرویس و کاربردها، نظیر اعداد تنوع را می‌توان از طریق سدها ثبت کرد.

در بعضی حالت‌ها کاربرد روش‌هایی نظیر امکان عبور فیزیکی استفاده شود تا اطلاعات اضافی را روی شبکه‌ی هدف جمع کنند و هم‌چنین ممکن است اطلاعات اضافی را در طول تست‌ها نظیر نوشتن کلمه عبور روی کاغذ را شامل شوند.

بخش دوم فاز کشف آنالیز تهدیدات است که شامل مقایسه‌ی سرویس‌ها، کاربردها و سیستم‌های عامل میزبان اسکن شده می‌باشد (یک فرآیند که برای اسکن‌های تهدید اتوماتیک است) از تسترهای دستی یا دیتابیس عمومی برای تشخیص تهدید به صورت دستی در این دیتابیس می‌توان استفاده کرد.

فرآیندهای دستی می‌توانند تهدیدات جدید را کشف کنند که اسکنرهای اتوماتیک ممکن است از دست بدهند اما خیلی از اسکنرهای اتوماتیک کندتر هستند.

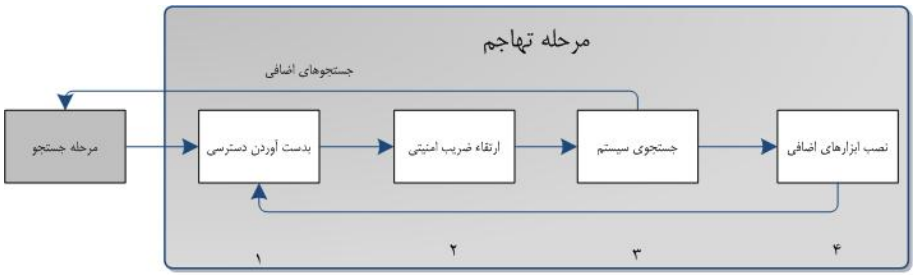
اجرای یک حمله قلب هر تست تهدید است. شکل ۲-۵- مراحل جداگانه‌ی فازهای حمله را نشان می‌دهد. (فرآیندهای تشخیص قبلی تهدیدات بالقوه با گسترش آن‌ها) اگر یک حمله‌ی موفق باشد تهدید تأیید و فرآیند ایمنی انجام می‌شود.

آن‌ها ممکن است در عوض از نتایج حاصل از تسترها چیزهای بیش‌تری درباره شبکه‌های مورد هدف و پتانسیل آسیب‌پذیری آن‌ها یا وادار کردن تغییرات به سطح امنیتی شبکه‌های مورد هدف فرا بگیرند.

برخی از عمل‌کردها تسترها را قادر می‌سازد که ویژگی و قابلیت‌شان را بر روی سیستم‌ها و شبکه‌ها برای بدست آوردن منابع بیش‌تر ارتقاء بخشند. اگر این مهم اتفاق بیافتد تجزیه تحلیل‌ها و تست‌های بیش‌تری مورد نیاز است تا سطح واقعی ریسک را برای شبکه‌ها مشخص نماید مانند مشخص کردن نوع داده‌هایی که در سیستم می‌تواند جمع آوری، تغییر یا پاک گردد.

اگر تسترها امکان رفتار به صورت یک آسیب‌پذیری را داشته باشند می‌توان روی سیستم هدف یا شبکه ابزار آلات بیش‌تری نصب نمود تا فرآیند تست را تسهیل نمایند. این ابزار آلات به منظور افزایش دسترسی به سیستم‌ها یا شبکه‌ها یا منابع بیش‌تر و هم‌چنین بدست آوردن دسترسی به اطلاعات سازمان یا شبکه مورد استفاده قرار می‌گیرند. تست و تحلیل بر روی سیستم‌های چندگانه می‌بایستی در خلال یک تست نفوذ که مشخص کننده سطح دسترسی دشمن می‌باشد مورد مدیریت قرار بگیرد. این

فرآیند در شکل شماره ۱-۵ که در آن حلقه بازخورد بین مرحله حمله و کشف تست نفوذ قرار دارد به نمایش درآمده است.



۱) در مرحله جست‌جو داده‌های کافی برای تلاش‌های آگاهانه جهت دسترسی به هدف صورت می‌گیرد.

۲) اگر در آخرین مرحله صرفاً سطح دسترسی به کاربر به دست آید تستر دسترسی کامل‌تری را به سیستم بدست خواهد آورد.

۳) فرآیند استخراج داده‌ها جهت مشخص کردن مکانیزم دسترسی به سیستم‌های اضافی آغاز می‌گردد.

۴) ابزارهای اضافی تست نفوذ برای بدست آوردن داده‌های اضافی و یا دسترسی یا هر دو آن‌ها نصب می‌گردد.

هنگامی که جست‌جوگر آسیب‌پذیری صرفاً امکان وجود آسیب‌پذیری را چک می‌نماید فاز حمله تست نفوذ به‌عنوان یک آسیب‌پذیری رفتار می‌کند تا وجود آن را تایید کند. بیش‌تر آسیب‌پذیری‌هایی که به وسیله تست نفوذ صورت می‌پذیرند در قالب دسته بندی‌های زیر قرار می‌گیرند:

- ترکیب بندی غلط: تنظیم غلط ترکیب بندی امنیتی و بالاخص تنظیمات ناامن پیش فرض در بسیاری از موارد به سادگی مورد سوءاستفاده قرار می‌گیرد.

- سوراخ کرنل: که کرنل هسته یک سیستم عامل است مدل امنیتی کلی را برای یک سیستم تنظیم می‌کند لذا هر سوراخ امنیتی در کرنل سیستم را در معرض خطر قرار می‌دهد.

- سرریز بافر: سرریز بافر هنگامی اتفاق می‌افتد که برنامه ورودی‌ها را به صورت مناسب از نظر طول چک نمی‌کند. در این صورت هرکد دلخواهی می‌تواند به سیستم معرفی گشته و توسط برنامه اجرایی با امتیاز حتی در سطح مدیریت[۱] اجرا گردد.

- اعتبار ناکافی ورودی‌ها: بسیاری از برنامه‌ها به علت عدم دریافت ورودی‌های معتبر کافی fail می‌کنند. به‌عنوان مثال می‌توان به برنامه web اشاره نمود که یک مقداری را از کاربرد در بانک اطلاعاتی خود[۲] وارد می‌کند. چنان‌چه کاربر از دستورات SQL به جایی یا علاوه بر مقادیر درخواستی استفاده کند برنامه‌های تحت web دستورات SQL را فیل‌تر نمی‌کنند و این دستورات sql ممکن است با توجه به دستورات sql باعث اعمال یک حمله گردد.

-لینک‌های صوری[۳]: فایل‌هایی هستند که اشاره به فایل‌های دیگری می‌کنند سیستم عامل شامل برنامه‌هایی است که می‌تواند مجوز اعطایی به یک فایل را تغییر دهد. اگر این برنامه‌ها با مجوز اعطایی اجرا گردند یک کاربر می‌تواند یک Symlink ایجاد نموده تا به این برنامه‌ها برای تعیین یا لیست کردن فایل‌هایی حیاتی سیستم حقه بزند.

-حملات[۴] (توصیف‌گر فایل): توصیف‌گر فایل ارقامی هستند که توسط سیستم برای نگهداری ترک (track) فایل‌ها به‌جای نام آن‌ها صورت می‌گیرد. انواع مشخصی از این توصیف گرها موارد استفاده دیگری نیز دارند. هنگامی که برنامه‌های مصون به صورت نامناسب مورد استفاده قرار می‌گیرند این باعث انشاء شدن و تخریب آن فایل‌ها می‌گردد.

---

۱ administrative

۲ Database query

۳ Symbolic Links

٤ File Descriptor

- شرایط مسابقه: شرایط مسابقه‌ای می‌تواند در هنگامی که برنامه یا فرآیند به مدمصون رفته دست رخ دهد. یک کاربر می‌تواند در زمان حمله برای بالا بردن درجه مصونیت برنامه در هنگامی که برنامه در مدمصون می‌باشد بیش‌ترین بهره را ببرد.

- مجوزهای فایل یا دایرکتوری ناصحیح: مجوزهای فایل و دایرکتوری دسترسی و استفاده کاربر از آن‌ها را کنترل می‌نماید مجوزهای ضعیف می‌تواند امکان اعمال انواع حمله‌ها از جمله نوشتن و خواندن کلمه عبور فایل یا اضافه نمودن به میزبان قابل اعتماد دوردست۱ را به‌وجود می‌آورد.

فاز گردش دهی با سه مرحله دیگر تست نفوذ به صورت هم‌زمان انجام می‌شود. (شکل ۱-۵ را ملاحظه کنید) در مرحله برنامه ریزی، برنامه‌ریزی دارایی‌ها یا ROE توسعه می‌یابد. در فاز جست‌جو و حمله گزارش‌های مکتوب نگهداری شده و همواره گزارش‌های متناوب برای مدیریت سیستم یا مدیران تولید می‌شود.

در اختتام تست نیز یک گزارش نهایی تدوین می‌گردد تا بیانگر آسیب‌پذیری‌های شناخته شده، نمایشگر نرخ ریسک بوده و راهنمایی‌هایی را در مورد کاهش و شناسایی نقاط ضعف ارائه می‌نماید.

۵-۵- پشتیبانی تست نفوذ

سناریو تست نفوذ می‌بایستی بر روی جانمایی و هدف‌گذاری عیوب موجود در طراحی و پیاده سازی نرم افزار، سیستم یا شبکه متمرکز گردد. تست می‌بایستی به صورت هم‌زمان در برگیرنده بیش‌ترین شباهت و بیش‌ترین تخریب حملات دیگر باشد و به عبارت دیگر می‌بایستی بدترین نمونه‌های سناریو را مانند حملات معاندانه به وسیله administrator را نیز شامل گردد. از آنجایی که سناریوهای تست می‌تواند به نحوی طراحی شود که به صورت هم‌زمان حملات داخلی و هم حملات بیرونی را شبیه سازی کند لذا می‌بایستی روش‌های تست امنیتی درونی و برونی می‌بایستی مورد توجه قرار گیرد. اگر هر تست درونی و بیرونی انجام گردد، معمولاً تست‌های بیرونی ابتدا صورت می‌گیرد.

---

۱ Trust remote host

سناریوهای بیرونی، مهاجمان بیرونی را که ممکن است کمی یا اصلاً آگاهی درباره اهداف خود یا فرضیات افرادی که در آن جا کار می‌کنند نداشته باشند. در شبیه سازی حملات بیرونی تسترها بر اساس اطلاعات غیرواقعی در مورد محیط هدف به جزء در مورد آدرس IPهای مورد تهاجم یا محدوده آدرس‌ها عمل می‌کنند و تحقیقاتی را با جمع آوری اطلاعات از صفحات اینترنت عمومی، اخبار گروه‌ها و سایت‌های مشابه انجام می‌دهند. جست‌جوگرهای محل‌های نفوذ و آسیب‌پذیری‌ها برای تعیین میزبان‌های مورد تهاجم مورد استفاده قرار می‌گیرند. پس از این که میزبان‌هایی که در شبکه امکان دسترسی به آن‌ها از خارج مورد شناسایی قرار گرفتند تسترها تلاش می‌کنند که یکی از میزبان‌ها را مورد حمله و تسویه قرار دهند اگر این حمله موفقیت آمیز بود در آن صورت ممکن است به سراغ سایر میزبان‌هایی که به صورت عمومی از خارج از شبکه در دسترس نیستند بروند. تست نفوذ یک فرآیند تکراری است که از کم‌ترین دسترسی برای رسیدن به دسترسی‌های بیش‌تر استفاده می‌کند. سناریو درونی، فعالیت‌های خصمانه درونی را شبیه سازی می‌کند یک تست نفوذ داخلی مانند یک تست نفوذ بیرونی است با این تفاوت که تسترها بر روی شبکه داخلی (پشت firewall) قرار دارند و امکان دسترسی به برخی از سطوح شبکه یا سیستم‌های خاصی از شبکه برای آن مقدور است. با این دسترسی تسترهای نفوذ سعی در بدست آوردن سطوح بیش‌تری از دسترسی به شبکه یا سیستم به وسیله ضریب مصونیت هستند. تسترها بر اساس اطلاعات شبکه‌ای که هر فرد با سطح مجاز دسترسی به صورت عمومی و بر اساس استاندارد واحد آن است طراحی گردیده و آن‌ها می‌توانند بسته به هدف تنها اطلاعات جای‌گزینی که مدیر شبکه یا سیستم لازم دارد را به آن‌ها ارائه نماید.

تست نفوذ اهمیت زیادی برای تعیین آسیب‌پذیری شبکه یک سازمان و سطح تخریبی که ممکن است در اثر نفوذ به آن اتفاق بیافتد دارد. این بسیار مهم است که بدانیم بسته به سیاست سازمان تسترها ممکن است مجاز به استفاده از برخی از ابزار آلات یا تکنیک‌هایی که صرفاً در برخی از ساعات یا روزهای مشخصی از هفته امکان استفاده از آن‌ها باشد، نباشند. هم‌چنین تست نفوذ ممکن است ریسک‌های جدی را در قبال شبکه یا سیستم سازمان همراه داشته باشد زیرا به صورت واقعی تولیدات سیستم و تولیدات داده‌ها را مورد تهاجم قرار می‌دهد. به علت هزینه بالا و تأثیر گذاری فراوان تست‌های نفوذ سالیانه ممکن است کافی باشد. هم‌چنین طراحی تست نفوذ می‌تواند به نحوی طراحی گردد که زمان متوقف هنگامی است که تستر به نقطه برسد که اقدامات اضافی دیگر باعث تخریب شود. نتایج تست نفوذ می‌بایستی بسیار جدی انگاشته شده و کشفیات آن بایستی سبب کاهش آسیب‌پذیری گردد.

نتایج پس از بدست آمدن می‌بایستی به مدیریت سازمان ارائه گردد سازمان می‌بایستی با استفاده از یک روش منظم از توانمندی کارکنان برای نگهداری سیستم جهت حفظ وضعیت امنیتی مطلوب اطمینان حاصل کند. یک برنامه منظم زمان بندی شده اسکن آسیب‌پذیری‌ها که به صورت پراکنده و متناوب اقدام به تست نفوذ می‌نماید از انجام انواع حمله‌ها جلوگیری نموده و از آثار تخریبی آن‌ها می‌کاهد.

۵-۵-۱- مهندسی اجتماعی

مهندسی اجتماعی کوششی است برای نیرنگ زدن به یک فرد تا اطلاعات مخفی خود مانند کلمه عبور را آشکار نماید که این روش می‌تواند در حمله به شبکه مورد استفاده قرار بگیرد. این جهت تست عناصر انسانی و آگاهی کاربر از امنیت و هم‌چنین برای آشکار ساز نمودن نقاط ضعف در رفتار کاربر مانند تبعیت از فرآیندهای استاندارد مورد استفاده قرار می‌گیرد. مهندسی اجتماعی هم‌چنین می‌تواند به وسیله ابزارهای مختلفی صورت پذیرد که شامل روش‌های آنالوگ مانند مکالمه هدایت شده از طریق تلفن و تخلیه تلفنی و روش‌های دیجیتال مانند ایمیل، پیام نگاری‌های جای‌گزین. یک نحوه مهندسی اجتماعی دیجیتال که بنام phishing شناخته می‌شود هنگامی است مهاجم سعی در دیدن اطلاعاتی مانند شماره کارت‌های اعتباری، شماره امنیتی، ID کاربر و کلمه عبور می‌کند.

Phishingها با استفاده از ایمیل‌های به ظاهر قابل اعتماد درخواست اطلاعاتی برای جمع آوری در یک وب جعلی می‌کنند از مثال‌های دیگر مهندسی اجتماعی دیجیتالی می‌توان ایمیل‌های جعلی و ارسال آن‌ها همراه پیوست‌هایی که می‌توانند فعالیت‌های کرم[۱] گونه خزنده داشته باشند اشاره کرد. مهندسی اجتماعی می‌تواند برای مورد حمله قراردادن افراد یا گروه‌های ویژه بسیار ارزشمند مانند مدیران اجرایی یا مجموعه اهداف گسترده مورد استفاده قرار گیرد. اهداف ویژه ممکن است هنگامی مشخص گردند که سازمان می‌داند یک تهدید وجود داشته یا حس می‌کند درز اطلاعات توسط فرد یا گروه ویژه‌ای می‌تواند اثرات زیانباری در پی داشته باشد.

به عنوان مثال حملات phishing می‌تواند از طریق اطلاعات عمومی در دسترس راجع به افراد ویژه اقدام نماید. ممکن است چنان‌چه تستر بتواند از این افراد اطلاعات لازم را استخراج نماید (در هنگام

---

۱ worm

تست) باعث خجالت آنان گردد. این بسیار مهم است که نتایج تست‌های مهندسی اجتماعی باعث ارتقاء امنیت سازمان می‌گردد.

تسترها می‌بایستی یک گزارش نهایی مشروحه که تاکتیک‌های موفق و ناموفق در آن مشخص گردیده‌اند ارائه نمایند.

این سطح از جزییات به سازمان کمک می‌کند که برنامه‌های آموزشی در زمینه آگاهی‌های امنیتی خود را مدون نمایند.

۵-۶- خلاصه

هر تکنیک تست امنیت اطلاعات نقاط قوت و ضعف خود را دارا می‌باشد. جدول شماره ۱-۵ انواع تکنیک‌های تست را مورد مقایسه قرار داده است.

قابلیت‌ها	تکنیک
رمزهای عبور ضعیف و هم‌چنین تدابیر مربوط به کلمه عبور را مشخص می‌کند.	رخنه در کلمه عبور
تست‌های امنیتی که روش‌ها و ابزارهای مشابه مهاجمان استفاده می‌کند. آسیب‌پذیری‌ها را تعیین می‌کند. نشان می‌دهد که آسیب‌پذیری‌هایی چگونه می‌توانند با استفاده از نفوذهای مکرر به دستاوردهای بزرگ‌تر نایل گردند.	تست نفوذ
امکان تست دستورالعمل‌ها و عناصر انسانی (آگاهی کاربر) را فراهم می‌سازد.	مهندسی اجتماعی

جدول ۵-۱ تکنیک های تست

ریسک‌ها وابسته به تکنیک‌ها و ترکیب آن‌ها می‌باشد. برای اطمینان از این که تکنیک‌ها به صورت بی خط و دقیق اجرا می‌گردند تسترها می‌بایستی دارای مجموعه‌ای از مهارت‌های ویژه باشند. جدول ۲-۵ مجموعه‌ای از حداقل مجموعه مهارتی که تکنیک‌های ارائه شده در این فصل به آن نیاز دارند ارائه گردیده است.

قابلیت‌ها	تکنیک
دانش ترکیب کلمه عبور امن و ذخیره سازی کلمه عبور برای سیستم عامل قابلیت استفاده از ابزارهای رخنه (crack) اتوماتیک	رخنه در کلمه عبور
TCP/IP گسترده، کار با شبکه و دانش سیستم عامل، دانش پیشرفته شبکه و دانش پیشرفته آسیب‌پذیری، دانش تکنیک‌ها برای گریز از آشکار سازهای امنیتی	تست نفوذ
قابلیت برای نفوذ و ترغیب افراد، قابلیت خونسرد بودن در فشار	مهندسی اجتماعی

جدول ۵-۲ مهارت های تست

۵-۷- برنامه ارزیابی امنیتی

برنامه ریزی مناسب برای یک ارزیابی امنیتی موفق بسیار حیاتی است این بخش راهنمایی است برای ایجاد یک نظام ارزیابی، اولویت بندی، برنامه ریزی ارزیابی که رویکردهای مناسب ارزیابی را انتخاب و

ملاحظات مربوط به پشتیبانی را نشان می‌دهد. این بخش هم‌چنین توصیه‌هایی برای توسعه یک برنامه ارزیابی و زمینه ملاحظات قانونی ارزیابی که سازمان به آن‌ها نیازمند است را نشان می‌دهد.

۵-۷-۱- توسعه نظام ارزیابی امنیتی

سازمان‌ها می‌بایستی نظام ارزیابی امنیتی اطلاعات خود را برای بدست آوردن راهنما و جهت ارزیابی امنیتی توسعه بخشند. این نظام می‌بایستی نیازمندی‌های ارزیابی امنیتی را مشخص کرده و افراد مسئول را آماده پاسخ‌گویی در قبال برآوردن نیازمندی‌های ارزیابی نگهدارد.

این نظام می‌بایستی موارد ذیل را مشخص نماید:

- نیازمندی‌های سازمانی به همراه این که کدام ارزیابی باید صورت پذیرد.

- نقش‌ها و مسئولیت‌های مناسب

- تبعیت از یک روش وضع شده

- تناوب ارزیابی

- نیازمندی‌های مستندسازی مانند نتایج ارزیابی و برنامه ارزیابی

هنگامی که بحث یک سناریو مناسب رسمی است، این سناریو می‌بایستی توسط مدیران ارشد مانند رئیس بخش اطلاعات، رئیس امنیت اطلاعات و رئیس بخش تکنولوژی مورد تایید قرار گیرد. مسئول ارشد می‌بایستی با سیاست و هرطرف سومی که ارزیابی را هدایت می‌کند در ارتباط باشد. توصیه می‌گردد که سازمان‌ها نظام ارزیابی خود را به صورت سالیانه یا هر هنگام که نیازهای مرتبط با ارزیابی جدیدی مطرح می‌گردد، مرور کنند. این مرور باعث امکان ادامه کاربرد نظام ارزیابی و هرگونه تغییرات لازم را مشخص می‌نماید و هم‌چنین فرصتی را برای جمع آوری تجاربی که کسب گردیده فراهم می‌سازد.

۵-۷-۲- اولویت بندی و برنامه ریزی ارزیابی

یک بخش از برنامه ریزی این است که سازمان تصمیم بگیرد که کدام سیستم‌ها باید متحمل ارزیابی امنیتی فنی شده و هر از چندی این ارزیابی می‌بایستی صورت پذیرد. این اولویت بندی برپایه دسته بندی سیستم‌ها، منافع مورد انتظار، نیازمندی‌های برنامه‌ای صورت می‌گیرد.

در این جا میزان اثر گذاری سیسم به عنوان مثال پایین، متوسط و بالا و هم‌چنین وضعتی ارزیابی (مثلاً اگر آخرین مورد باشد) نحوه حرکت به جلو را مشخص می‌کند به عنوان نمونه سازمان می‌بایستی عموماً سیستم با اثرگذاری بالا را قبل از سیستم با اثرگذاری متوسط ارزیابی کند ولی چنان‌چه سیستم با اثرگذاری متوسط تازه سر رسیده می‌بایستی قبل از سیستم با اثرگذاری بالا ارزیابی شود.

تناوب ارزیابی اغلب به وسیله نیازمندی‌هایی سازمانی برای اثبات نظام‌ها و قوانین خاص دیکته می‌شوند F/SM وابسته به ریسک و حداقل در سال یک‌بار نیاز به انجام تست دوره‌ای دارد.

از آن جا که یک تست صرفاً اقدام به ارزیابی امنیتی سازمان در یک لحظه خاص می‌کند لذا ممکن است سازمان‌ها نیاز به دفعات بیش‌تری از ارزیابی داشته باشند هم‌چنین ملاحظات مهم فنی می‌تواند به مشخص کردن دفعات تست کمک کند. به‌عنوان مثال اگر اعتقاد بر این است که یک سیستم دارای چندین نقطه ضعف است تست ممکن زودتر صورت بگیرد برای تشخیص وجود ضعف در آن یا ممکن با تاخیر صورت بگیرد تا این که نقاط ضعف کاهش یابد. زمان اعمال تست بسته به موضوع مورد تست است. ملاحظه دیگر این است که آیا هیچ‌گونه از فعالیت‌های مربوط به تست سیستم یا شبکه ممکن است به صورت عملی یا امنیتی بر محیط اثر بگذارد به‌عنوان مثال اگر یک upgrading بزرگ و مهم در حال پیاده سازی باشد عملیات تست باید به تاخیر بیافتد تا این upgrading به صورت کامل اتفاق بیافتد. مثال دیگری از ملاحظات فنی هنگامی است که یک سازمان بخواهد بر روی شبکه کابلی خود قطعات نامعتبر را مشخص نماید. این می‌تواند توسط یک یا چند تکنیک انجام پذیرد مانند جست‌جوی شبکه به وسیله جست‌جوی فعال و غیرفعال یا مرور مجموعه داده‌ها به وسیله نرم افزار مدیریت داده، سنسورهای کشف بدون مجوز در شبکه یا سایر ابزارهای دیگر که به صورت معمول فعالیت‌های شبکه را نظارت می‌کنند.

چنان‌چه این ابزارهای نظارت شبکه بتوانند به محض این که قطعات نامعتبر وارد شبکه می‌گردند، اقدام به اعلام خطر کنند در این صورت به مقدار کم یا اصلاً نیازی به تست‌های متناوب نیست زیرا تست موثر همواره در حال اجرا می‌باشد.

سازمان هم‌چنین به بررسی دسترسی به منابع نیازمند است. منابع می‌بایستی در ابتدا برای سیستم‌های با اولویت بالا تعریف گردد و پس از آن سیستم‌های با اولویت پایین‌تر نیز با تناوب کمتر مورد تست قرار می‌گیرند. چنان‌چه فاصله‌ای بین منابع مورد نیاز و منابع در دسترس باشد در این صورت سازمان می‌بایستی یا منابع بیش‌تری برای این کار اختصاص دهد یا محدوده ارزیابی برنامه ریزی شده را کاهش دهد.

مثالی از عناصر محدوده که باید مشخص گردد شامل:

- اندازه آن چه که می‌بایستی مورد ارزیابی قرار گیرد به ترتیب تعداد قطعات و اندازه شبکه

-پیچیدگی آن چه که می‌بایستی مورد ارزیابی قرار گیرد محیط‌های ناهمگن‌تر عموماً به حجم بیش‌تری از منابع احتیاج دارند زیرا مهارت و ابزارهای بیش‌تری مورد نیاز است.

- امکان سنجی استفاده از نمونه در ارزیابی به‌عنوان مثال این ممکن است بسیار کارآتر و موثرتر باشد که part scan یک میزبان[۱] صورت بگیرد تا این که هزاران میزبان صورت بگیرد بالاخص اگر که این میزبان‌ها و مدیریت آن‌ها شبیه هم باشند. منابع نیاز دارند که به تست‌های ویژه و تکنیک‌های تست هدایت گردند.

به عنوان مثال ساعت‌ها طول خواهد کشید که یک ارزیاب ماهر به صورت کامل مستندات امنیتی سیستم را مرور کند.

- به سطحی از تعاملات انسانی نیاز است. به‌عنوان نمونه اگر ارزیاب‌ها به صورت همکاری با کارمندان فن‌آوری اطلاعات کار می‌کند این ممکن است به صورت یک آموزش برای کارمندان فن‌آوری اطلاعات

---

۱ host

محسوب شود ولی در مقایسه با زمانی که ارزیاب‌ها و کارمندان فن‌آوری اطلاعات به صورت جداگانه کار می‌کردند زمان بیش‌تری را مصرف می‌نماید.

۵-۸- انتخاب و مطلوب سازی ابزارها

فاکتورهای بسیاری برای مشخص نمودن این که در یک ارزیابی ویژه از چه تکنیک‌ها و ابزارهایی می‌بایست استفاده نمود وجود دارد. در ابتدا سازمان می‌بایستی هدف خود را از ارزیابی مشخص کند مانند تمرکز بر روی قبول رسیدگی به یک تعهد خاص، رسیدگی به امنیت یک سیستم جهت فعالیت‌های گواهی‌نامه، تشخیص آسیب‌پذیری‌های موجود در یک سیستم.

در مرحله بعد سازمان باید سطح تکنیک‌های مورد استفاده در بدست آوردن اطلاعاتی که در رسیدن به اهداف کمک می‌کند را تعیین کند. برای برخی از تکنیک‌های تست سازمان باید دیدگاه ارزیاب را مشخص کند. از آن جایی که در بسیاری از موارد بیش از یک تکنیک برای رسیدن به اهداف ارزیابی مورد استفاده قرار می‌گیرد، سازمان باید مشخص کند کدام ابزار برای هر مورد مناسب‌تر است. همان طور که بحث شد یک ملاحظه بسیار مهم در منابع این است که برخی از منابع ممکن است ذاتاً به دلیل انواع ابزارهای مورد نیاز و ساعات کار کارمندان برای آن ارزشمندتر از بقیه منابع باشد. هم‌چنین برخی از تکنیک‌ها ممکن است برای انجام بسیار طولانی باشند. مهارت فیزیک فاکتور مهم دیگری است که در انتخاب تکنیک نقش دارد. به عنوان مثال سازمان ممکن است در میان کارمندان ارزیابی‌هایی با مجموعه مهارت‌های مناسب برای کار با یک تکنیک خاص نداشته باشد.

سازمان‌ها هم‌چنین می‌بایستی با دقت به ریسک‌ها در هنگام انتخاب تکنیک‌ها توجه داشته باشند. برخی تکنیک‌ها مانند تست نفوذ ممکن است منجر به از دست دادن برخی داده‌ها منجر گردد. در برخی موارد سازمان‌ها می‌بایستی توجه کنند که آیا تست‌ها بر روی محصولات واقعی باید صورت پذیرد یا می‌تواند به صورت مشابه بر روی تولیدات غیر واقعی سازمان نیز انجام شود. اگر سیستم جای‌گزین دیگری در دسترس باشند یا محدودیت وجود نداشته باشد می‌بایستی سعی گردد که این عملیات کم‌ترین تأثیر و اختلال را بر روی سیستم وارد آورد. فاکتورهایی که در هنگام تصمیم گیری باید به آن‌ها توجه داشت عبارتند از:

- تاثیرات ممکن بر روی تولیدات سیستم

- حضور داده‌های قابل تشخیص فردی حساس. اگر یک تست باعث افشاء شدن داده‌های قابل تشخیص فردی گردند یا داده‌های کارت اعتباری هر فردی که اختیارات دسترسی به آن‌ها را ندارد در این صورت سازمان می‌بایستی این تست‌ها را بر روی یک کارت غیرواقعی و بی استفاده انجام دهد.

- چه مقدار می‌توان سیستم‌های تولیدی با سیستم‌های غیرعملیاتی و غیرتولیدی شبیه سازی نمود. در عمل برخی مورد ناسازگاری بین شرایط عملی و شرایط تست وجود دارد و این بسیار مهم است که تا چه حد به نتایج حاصل از شرایط تست در شرایط واقعی نیز اعتماد کرد.

سازمان‌ها اغلب از ترکیبی از تکنیک‌ها برای بدست آوردن یک ارزیابی امنیتی عمیق استفاده می‌کنند همان طور که قبلاً ذکر شد تکنیک‌های غیرفنی ممکن است به جای یا همراه روش‌های فنی استفاده گردند. بسیاری از ارزیابی‌های ترکیبی از روش‌های فنی و غیرفنی را مورد استفاده قرار می‌دهند.

مثال زیر نشان می‌دهد که چگونه چند تکنیک فنی چگونه می‌تواند هم‌دیگر را تکمیل نموده و چگونه انتخاب تکنیک می‌تواند به مقوله ریسک مرتبط باشد. این مثال قصد دارد تکنیک‌های ترکیبی ارزیابی سازمان‌ها را به نمایش درآورد. هر مورد نسبت به مورد دیگری تفاوت داشته و سازمان‌ها می‌بایستی بر اساس نیازمندی‌ها و اهداف خود از ارزیابی نسبت به انتخاب تکنیک‌های مناسب اقدام نمایند.

در راستای کاهش ریسک در ساختار امنیتی سیستم و ترکیب امنیتی نقاط ضعف فنی را مشخص کنید.

قدم اول - مرور مستندات: نقاط ضعف دستورالعمل‌ها و سیاست‌ها و رخنه‌های ساختار امنیتی را تعیین کنید.

قدم دوم - مرور پیکره بندی و مجموعه قوانین امنیتی: انحراف از نظام امنیتی سازمان که ساختار امنیتی شبکه و رخنه‌های امنیتی سیستم تعیین کنید.

قدم سوم - اسکن بدون سیم: قطعات غیرمعتبر بدون سیم را در مجاورت سیستم تشخیص داده و نقاط ضعف مرتبط با شبکه بودن بدون سیم را پیدا نماید.

قدم چهارم - اسکن آسیب‌پذیری و جست‌جوی شبکه: فعالیت میزبان‌های سیستم را مشخص و آسیب‌پذیری آن‌ها را شناسایی کنید.

-نقاط ضعف فنی ساختار امنیتی را شناسایی و اعتبار آن‌ها را تایید کنید. معتبرسازی شامل فعالیت‌هایی است که منجر به فعال سازی آسیب‌پذیری‌ها می‌شود.

قدم اول - مرور پیکربندی و مجموعه قوانین امنیتی: انحراف از نظام امنیتی سازمان در ساختار امنیتی شبکه و رخنه‌های امنیتی سیستم را تعیین کنید.

قدم دوم – اسکن آسیب‌پذیری و جست‌جوی شبکه: فعالیت میزبان‌های سیستم را مشخص و آسیب‌پذیری آن‌ها را شناسایی کنید.

قدم سوم – تست نفوذ به همراه مهندسی اجتماعی.

از دیدگاه یک مهاجم بیرونی نقاط ضعف پیکره بندی امنیتی و ساختار سیستم را شناسایی کنید.

کارایی قابلیت‌های بازرسی سازمان را در مقابل مهاجم علیه سیستم ارزیابی کنید.

قدم اول - تست نفوذ بیرونی: جست‌جوی شبکه بیرونی، اسکن پرت، اسکن آسیب‌پذیری و حمله به آسیب‌پذیری‌های شناسایی شد.

قدم دوم – مرور گزارش: گزارش بازرسی کنترل امنیتی را برای مشخص کردن کارایی آن‌ها در ارایه گزارش مرتبط با فعالیت‌های مربوط به تست نفوذ بیرونی مرور کنید.

۵-۹- پشتیبانی ارزیابی

پشتیبانی ارزیابی فنی شامل تعیین کلیه منابع برای هدایت ارزیابی، محیطی که در آن تست انجام می‌شود و ابزار آلات سخت افزاری و نرم افزاری تست می‌باشد. در زیر به این موارد اشاره گردیده است.

علاوه بر نیازمندی‌های پشتیبانی استاندارد که در زیر درباره آن بحث می‌شود این بسیار مهم است که در خلال مرحله برنامه ریزی نیازمندی‌های پشتیبانی برای هر تست مشخص گردد. بسته به محدوده و محیط هر تستی ممکن است به تجهیزات تست اضافی مانند ارائه پیش‌نهاد برای ملاقات با یک تیم

تست خارجی، حمل تجهیزات برای تسهیل در انجام تست و برنامه ریزی برای سفرهای کوتاه یا بلند. این نیازها باید مورد به مورد در فرآیند برنامه ریزی مشخص گردد.

۵-۱۰- انتخاب ارزیاب و مهارت‌ها:

ارزیاب با استفاده از متدهای فنی و تکنیک‌ها تست‌ها را هدایت می‌کند.

سازمان‌ها می‌بایستی در انتخاب ارزیاب‌ها دقت کافی به خرج دهند زیرا مهارت مناسب و تجربه ارزیاب باعث پایین آمدن ریسک تست‌های امنیتی می‌گردد. به دلیل این که ارزیاب ممکن است نیاز به دسترسی به اطلاعات حساس بر روی معماری شبکه، وضعیت امنیتی و نقاط ضعف لذا لازم است سازمان سابقه امنیتی ارزیاب را به صورت شفاف بررسی نماید.

بسیاری از سازمان‌ها تیم‌های ارزیابی داخلی مشخص شده‌ای را دارند. بسته به ساختار سازمانی، ابعاد، موقعیت و منابع در دسترسی این تیم‌ها ممکن است بر اساس موقعیت جغرافیایی تقسیم شده یا متمرکز شده یا به وسیله مراکز مختلف و متعدد گسترده ارزیاب‌های خود را هدایت کنند. برخی از این تیم‌ها در زمینه‌های مختلف به صورت عمیق کار می‌کنند به‌عنوان نمونه ممکن است یک تیم در میان اعضا خود افرادی را داشته باشد در پیکره بندی سیستم‌ها یا برخی در زمینه ابزارهای ارزیابی اتوماتیک برای تشخیص آسیب‌پذیری‌ها و برخی دیگر نیز در زمینه فعالیت‌های شناسایی آسیب‌پذیری برای نشان دادن اندازه ناکارآمدی امنیتی سیستم مهارت داشته باشند.

ارزیاب‌ها می‌بایستی دانش شبکه و امنیت پیشرفته را که شامل تخصص در امنیت شبکه، دیوار آتش (firewall)، شناسایی ورود بی مجوز به سیستم، سیستم عامل، پروتکل‌های برنامه ریزی و شبکه مانند TCP/IP می‌باشد داشته باشند. محدوده گسترده‌ای از مهارت‌های فنی برای هدایت تست‌های موثر و کارا با حداقل ریسک مورد نیاز می‌باشد.

ارزیاب‌ها هم‌چنین باید در برخی انواع تکنیک‌های اجرایی مانند شناسایی آسیب‌پذیری‌ها و ممیزی کردن آن‌ها، پیکره بندی امنیتی، مدیریت آسیب‌پذیری و تست نفوذ تبحر داشته باشند. تجربه عملیاتی از آموزش آزمایشگاهی ترجیح دارد. اجازه به کارکنان بی تجربه با آموزش ندیده برای هدایت تست‌ها می‌تواند اثرات منفی را بر روی سیستم‌ها و شبکه‌های شبکه داشته و اعتبار ارزیاب‌ها و بخش مدیریت

برنامه امنیتی را خدچه دار نماید. هم‌چنین بسیار مفید خواهد بود که در تیم ارزیاب فردی با مهارت نویسندگی فنی داشته باشیم. این کمک می‌کند که نتایج ارزیابی به صورت موثر نائل شده و بالاخص خوانندگان غیرفنی نیز مشکلی نداشته باشند.

هنگامی که ارزیابی توسط تیم صورت گرفت رهبر تیم فرآیند ارزیابی را که عبارتند از ارائه درک صحیح از محیط سازمانی و نیازمندی‌ها و ارتباط نزدیک بین ارزیاب‌ها و گروه امنیت سازمان تسهیل می‌نماید رهبر تیم باید بر اساس دانش فنی کلی و تجربه تکنیک‌هایی که باید اجرا گردد آگاهی از اموالی که باید مورد ارزیابی قرار گیرد انتخاب گردد. رهبر تیم هم‌چنین باید دارای ارتباطات، سازماندهی، برنامه ریزی و مهارت حل اختلافات داشته باشد. تخصص‌های موجود در تیم بازرسی باید به نحوی بالانس باشد که یک نمای صحیح از وضعیت امنیتی سازمان ارائه دهد. مثلاً اگر یک متخصص در پدافند محیطی داشته باشیم مفید می‌باشد ولی اگر کل تیم در این زمینه متخصص باشند زائد خواهد بود مگر این که تست‌ها صرفاً بر روی وضعیت امنیتی محیطی متمرکز باشد. به صورت ایده‌آل یک تیم باید بر اساس نیازمندی‌های تست‌ها ایجاد شده باشد. مولفه‌های سیستم نیز هم‌چنین بسیار مهم است. به‌عنوان مثال سرپرستی کنترل و کسب داده سیستم تعدادی مولفه ویژه دارند که چنان‌چه ارزیاب امنیتی تجاری با آن‌ها آشنا نباشد باعث کاهش توانمندی ارزیاب برای انجام تست‌های رقیق و بی خطر می‌گردد.

در این مورد، یک یا چند کارشناس مواد موضوعه[۱] ممکن است برای تکمیل ارزیابی لازم باشد. کارشناسان ممکن است در زمینه تسترهای امنیتی تجربیاتی داشته و کارشناس سیستم باشد یا ممکن است صرفاً در زمینه سیستم مورد تست تخصص داشته باشد. درهر صورت کارشناسان می‌بایستی در زمینه اهداف، رویکردها و فرآیندهای ارزیابی آموزش دیده باشد هم‌چنین در صورت امکان در زمینه فرآیند برنامه ریزی فرآیند نیز آموزش دیده باشد.

مسئولیت‌های ارزیاب شامل موارد زیر است:

-آگاه سازی گروه‌های مناسب مانند مامور امنیتی، رئیس سیستم و کاربران از فعالیت‌های مربوط به ارزیابی امنیتی

---

۱ SME

-توسعه برنامه ارزیابی با مدیران سیستم، مدیران امنیتی سیستم

-اجرای تست‌ها و جمع آوری کلیه داده‌ها

-آنالیز داده‌های جمع آوری شده و توسعه توصیه‌های کاهش آسیب‌پذیری

-هدایت تست‌های کمکی در هنگام لزوم تایید فعالیت‌های مربوط به کاهش آسیب‌پذیری

علاوه بر موارد فوق مسئولیت ارزیاب‌های خارجی شامل موارد زیر می‌شود:

- هماهنگی و ارتباط با سازمانی که مورد ارزیابی قرار می‌گیرد.

- اطمینان از تفویض اختیارات مناسب و نگه‌داشتن یک برنامه ارزیابی امضا شده برای اطمینان از این که کلیه مستندات به روز گردیده‌اند.

-امضاء و پایبندی بر کلیه توافقات سری

- محافظت مناسب از اطلاعات بر اساس قواعد سازمان که شامل بررسی، انتقال ذخیره سازی و حذف گزارش‌های نتایج و اطلاعات جمع آوری شده می‌باشد.

۵-۱۱- انتخاب مکان

طبق تکنیک‌هایی که باید تست انجام گردد محیطی که ارزیاب‌ها در آن کار می‌کنند مختلف است. در بسیاری از انواع تنها ارزیاب‌ها می‌توانند هم در داخل مرکز و هم در خارج از آن تست را انجام دهند. به هر ترتیب انجام تست در بیرون از مرکز ممکن است تست را بیش‌تر غیرواقعی نماید.

برای تست‌ها ارزیاب‌ها می‌توانند عموماً درون مرکز قرار گرفته تا با سهولت بیش‌تری به مستندات امنیتی، گزارش‌ها و سایر اطلاعات سازمان دسترسی داشته باشند ارزیابی‌هایی که می‌بایستی توسط ۳ گروه صورت پذیرد لازم است سازمان سطوح دسترسی فیزیکی هریک را مشخص نماید. برای ارزیابی‌های فنی مانند اسکن آسیب‌پذیری و مرور پیکر بندی امنیتی ارزیاب‌ها می‌بایستی باید امکان

دسترسی به داخل مرکز از طریق شبکه خصوصی مجازی رمز شده (VPN) یا از طریق یک ارتباط پیش بینی شده از طریق فضای مطمئن را داشته باشد.

ارزیاب‌ها ممکن است بسته به ابزارهایی که مورد استفاده قرار می‌دهند به سطوح متفاوتی از دسترسی به شبکه نیاز داشته باشند برخی از ابزارها نیاز به امتیاز ویژه رییس شبکه نیازمند می‌باشند در این صورت سازمان می‌بایستی یک account جدید در خلال زمان ارزیابی برای آن‌ها ایجاد کند. هر ارزیابی می‌بایستی یک account خاص خود را داشته و نباید بهر دلیلی آن را به شراکت گذارد.

این به سازمان امکان نظارت بر accountها را داده و این accountها در خاتمه ارزیابی پاک شده یا غیرفعال می‌گردد.

ارزیابی فنی که از خارج از شبکه هدایت می‌گردد می‌توانند چندین سناریو را دنبال کنند.

ارزیاب سیستم می‌تواند مستقیماً به قطعات محیطی متصل گردند که این قطعات ارزیاب را در مرز فیزیکی و منطقی سازمان قرار می‌دهد. به هرترتیب استفاده از این مکان یک ارزیابی واقعی از وضعیت امنیتی سازمان را از دیدگاه دشمن ایجاد نمی‌کند.

تست بیرونی هم‌چنین می‌تواند از طریق ارتباط اینترنتی از شبکه سازمانی مورد تست صورت می‌گیرد. سازمان‌هایی که تست‌های خارجی را انجام می‌دهند هم‌چنین یک Server را با اینترنت مستقل کرایه می‌کنند. این سرویس توسط فروشندگان مختلفی ارایه می‌شود و به طور معمول به صورت ماهیانه اجاره می‌گردند. اگر سرور اجاره‌ای مورد استفاده قرار گیرد ارزیاب حتماً می‌بایستی داده‌های روی سرور را کاملاً پاک کرده و سرور را به حالت قبل از تست در بیاورد. وقتی که تست‌ها کامل گردید تیم تست می‌بایستی برای بررسی داده‌ها از راهنمایی‌ها بحث شده در بخش ۴-۷ تبعیت کنند.

در زمان انتخاب مکان ارزیابی سازمان باید ملاحظات مربوط به ریسک ذاتی ناشی از استفاده از مکان بیرونی را در نظر بگیرند. به صورت عمومی کنترل کم‌تری بر روی محل‌های ارزیابی بیرون نسبت به درونی وجود دارد و این ممکن است ریسکی را برای محل ارزیابی ایجاد کند. ترافیک شبکه بیرونی که می‌تواند توسط یک طرف سوم بدون مجوز کنترل شده و از طریق آن به شبکه نفوذ نماید و این خود یک ریسک برای مکان‌های بیرونی می‌باشد. همان طور که در گذشته بحث نمودیم مکان سیستم

ارزیابی بر روی نتایج برخی از تست‌ها ممکن است اثر بگذارد. به عنوان مثال چنان‌چه تست آسیب‌پذیری ترافیک شبکه از طریق firewall صورت می‌گیرد این firewall ممکن است به صورت غیرعمدی جلوی ترافیک شبکه (انتقال داده‌ها) را گرفته و از ایجاد آسیب‌پذیری تعیین شده جلوگیری می‌کند. هم‌چنین تشخیص نفوذ و سیستم‌های اجتناب و سایر کنترل‌های امنیتی ممکن است مشاهده ترافیک شبکه را مسدود کرده و آن‌را به صورت یک خراب‌کاری عمدی به نظر برساند. این مشکلات هنگامی که در مکان خارجی و توسط سه گروه که در هر گروه ارزیاب‌ها آگاهی از سازمان نداشته تشدید می‌شود.

۵-۱۲- انتخاب منابع و ابزارهای فنی

ساختارهای سیستم‌های اطلاعاتی برای اجرای ارزیابی امنیتی باید نیازهای ابزارهای خاص و مورد نیاز ارزیابی را تامین کنند به‌عنوان مثال سیستم‌های مرور مستندات باید دارای نرم افزارهای خواندن مستندات، تعقیب آسیب‌پذیری‌ها و گزارش ترکیب و ساخت باشد. سیستم‌های طراحی شده برای تست اجرا مانند ارزیابی آسیب‌پذیری و تست نفوذ در موارد نیازمندی‌های سیستم و ابزارهای نرم افزاری از پیچیدگی بیش‌تری برخوردارند. سیستم‌ها برای ارزیابی فنی می‌توانند شامل سرورها، workstationها و لپ‌تاپ‌ها گردند. لپ‌تاپ‌ها به صورت عمومی توسط ارزیاب‌های در حال مسافرت هستند و سرورها و workstationها هنگامی که ارزیاب‌ها در آزمایشگاه تست در موقعیت داخل مرکز قرار دارند مورد استفاده قرار می‌گیرند. ارزیاب‌ها هم‌چنین ممکن است یک شبکه برای اجرای تکنیک‌ها که یک محیطی برای پشتیبانی متمرکز سازی گزارش فعالیت‌ها و سرورهای شخصی که احتیاج به بالابردن توان پردازش دارند را ایجاد کنند نیازمندی‌های سیستم‌های تست مختلف است. سیستم‌هایی که عمل پردازش را انجام می‌دهند و حافظه مورد نیاز تمام ابزارها، سیستم عامل و ماشین‌های مجازی (VM) با در نظر گرفتن احتمال crash شدن سیستم در خلال تست می‌بایستی مدنظر قرار بگیرد. یک crash باعث می‌شود قطعات تست از کار افتاده، داده‌ها از دست رفته و سیستم‌های تست خراب شود. توان پردازش و نیازمندی حافظه بر اساس ابزارهای مورد استفاده و سرعت مورد نیاز تیم برای پردازش مشخص می‌شود. به‌عنوان مثال crack کردن کلمه عبور عموماً به توان پردازشی و حافظه بالا نیاز دارد. بر همین اساس تیم تست امیدوار هستند که یک سرور crack کلمه عبور مشخص و تعیین شده در اختیار داشته باشند.

یک سیستم مشخص به تیم امکان اجرای تست‌های دیگری را در خلال تست crack کلمه عبور را می‌دهد. نیاز Hard Drive به حجم داده جمع آوری شده برای ذخیره بستگی دارد. در مواقعی که حجم زیادی از ذخیره داده مورد نیاز است روش ذخیره سازی می‌بایستی مشخص گردیده و تدارکات مورد نیاز آن به صورت مناسب انجام گردد.

ابزارآلات مورد نیاز برای تست بسیار وابسته به محدوده تست می‌باشد ولی تیم تست می‌بایستی یک مجموعه اصلی از تجهیزات تست را داشته و آن‌را همیشه به روز کند. بسته به سازمان تیم تست ممکن است از ترکیبی از آبزار آلات خانگی (در خانه توسعه یافته)، ابزارهای Open Source یا ابزارهای تجاری استفاده کند. ابزارها می‌بایستی از منابع شناخته شده تهیه شده باشد. برخی سازمان‌ها دستگاه‌هایی دارند که تیم‌های تست را تشویق به استفاده از آن می‌کنند بسیاری از ابزارهای دیگری نیز در دسترس می‌باشند.

سازمان‌ها باید قبل از استفاده از تجهیزات هرکدام از این ابزارها را ارزیابی و بررسی کنند این فرآیند می‌تواند شامل دانلود ابزارها از سایت‌های مطمئن تا مرور عمیق کدها برای اطمینان از مخرب نبودن کدها شود. اغلب ابزارها، سیستم عامل را برای اجرای تست مشخص می‌کنند سیستم‌ها ممکن است به وسیله راه‌های مختلفی پیکربندی گردند که شامل یک سیستم عامل، یک سیستم عامل به همراه تصویر حافظه مجازی Vintual Memory Image و سیستم‌های بوت دوگانه است. یک مثال برای سیستم‌های بوت دوگانه سیستمی است که هم با Windows و هم با ورژن‌های Linux مانند Redhat، Mandrake یا Suse بوت می‌شود است. یک سیستم با بوت دوگانه به تستر اجازه می‌دهد که از دو سیستم عامل با یک دستگاه کامپیوتر استفاده کند ولی این ممکن است باعث دردسر شود زیرا تستر نیاز دارد برای سوئیچ کردن از یک سیستم عامل به دیگری سیستم را خاموش و روشن کند. گزینه دیگر استفاده از VM می‌باشد. بسیاری از ابزارهای تست به یک سیستم عامل مشخص نیاز دارند و VMها به تسترها اجازه می‌دهند که از گستره وسیعی از ابزارها با ساده‌گی بیش‌تر استفاده کنند زیرا آن‌ها به تستر اجازه می‌دهند بدون نیاز به روشن و خاموش کردن سیستم بین سیستم‌های عامل سوئیچ کنند و آن‌ها را قادر به استفاده همزمان از چند سیستم‌های عامل می‌سازند. این چندین مزایایی از جمله گزارش دهی قابلیت مستندسازی و اجرای همزمان چند تست را در بر دارد.

از آن جایی که سیستم‌های دارای VM باید قابلیت اجرای همزمان چند سیستم عامل را داشته باشند لذا احتیاج به حجم حافظه و توان پردازش بالاتری را دارند. تسترها باید مجرب، آگاه و انعطاف پذیر برای کار با چند سیستم عامل زیرا برای اجرای ابزارهای خاص یا قابلیت‌های موفق سیستم نیاز به بهبود متناوب ضروری است به‌عنوان مثال اگر تیم تست از لینوکس Redhat برای اجرای تست امنیتی بی سیم استفاده می‌کند تیم باید با نصب و پیکره بندی کارت‌های شبکه آشنا باشد زیرا ممکن است این

مرحله در Redhat مبتدی روشن و واضح نباشد. تصویر حافظه مجازی (VM) باید به صورت متناوب به روز گردد برای اطمینان از این که آخرین ابزارها و ورژن‌ها مورد استفاده قرار می‌گیرند. در خلال زمان Update تیم باید عمل‌کرد ابزارها از طریق مستندات تایید کرده و هر تغییر در عمل‌کرد آن‌ها را مشخص نماید. به روز کردن ابزارهای اسکن قبل از هر تست به ما کمک می‌کند که اطمینان حاصل کنیم که آخرین پوشش از آسیب‌پذیری‌ها در تست پیاده می‌گردد. علاوه بر آن برای نگهداری این ابزارها تیم باید به صورت متناوب به toolkit آن‌ها دسترسی داشته تا ابزارهای از رده خارج شده را حذف و ابزارهای جدید را اضافه کند. قبل از استفاده از سیستم‌های تست در تست امنیتی تیم تست باید آخرین Patch امنیتی را مورد استفاده قرار داده و صرفاً آن سرویس‌هایی که برای تست و اتصال لازم است را فعال کند.

این توصیه برای کلیه سیستم‌های عامل که در تست استفاده می‌شود نیز باید اجرا گردد. این شامل VMها نیز می‌باشد. گروه امنیت سازمان ممکن است سیستم‌های تست را از نظر تطبیق با نیازمندی‌های امنیتی سازمان مورد تایید قرار داده و قبل از اتصال به شبکه آن‌ها را تایید می‌کند.

این تایید می‌تواند از طریق سیستم‌های مشابه که برای تست فنی استفاده می‌شوند مانند اسکن آسیب‌پذیری صورت پذیرد. سیستم‌های تست ممکن است نیازمندی‌های امنیتی سازمان را کاملاً پوشش ندهد زیرا نیازمندی ابزارها برای تست صورت می‌گیرد به‌عنوان مثال تعدادی از کنترل‌های امنیتی ممکن است با عملیات ابزارها در تداخل باشد زیرا آن‌ها سعی در توقف اسکن یا حمله را انجام می‌دهند در این موارد ارزیاب ممکن است در هنگام کار با این ابزارها این کنترل‌های امنیتی را غیرفعال کند.

تیم‌های در حال سفر بایستی کلیه قطعات که شامل سیستم‌ها، تصاویر، ابزارهای کمکی، کابل‌ها، پروژکتورها و سایر ادوات که تیم برای اجرای تست در یک مکان دیگر به آن‌ها نیاز دارد را همراه داشته باشد. اگر یک سازمان از یک تیم تست خارجی استفاده می‌کند این تیم نمی‌تواند از منابع سازمان استفاده کند مگر آن که نیاز به آن باشد اگر یک سازمان اختیار اتصال به شبکه را به تیم تست نداده باشد، تیم خارجی باید کلیه ابزارهای مورد نیاز خود را بر روی یک سیستم Client تایید شده نصب کند یا یک سیستم فایل بوت شدن emulation مانند CD همراه خود بیاورد.

اگر ابزارها مستقیماً بر روی سیستم client نصب گردد تیم تست باید از پاک شدن کلیه فایل‌ها از روی سیستم پس از پایان تست اطمینان حاصل کند.

۵-۱۳- توسعه برنامه ارزیابی

یک برنامه ارزیابی یک ساختار ایجاد نموده و پاسخ‌گوی مستندسازی فعالیت‌های برای ارزیابی در خلال اطلاعات مرتبط دیگر می‌باشد.

این مراحل عبارتند از:

۱) مشخص کردن نوع ارزیابی کنترل امنیتی برنامه ریزی شده

۲) مشخص کردن کنترل‌های امنیتی و کنترل‌های پیشرفته‌ای که شامل ارزیابی می‌شوند.

۳) انتخاب دستورالعمل‌های مناسب ارزیابی که در ارزیابی مورد استفاده قرار می‌گیرد بر اساس کنترل‌های امنیتی و کنترل‌های پیشرفته برنامه امنیتی

۴) تدوین دستورالعمل‌های ارزیابی انتخاب شده برای سطح اثر سیستم اطلاعاتی و محیط اجرایی سازمان

۵) توسعه دستورالعمل‌های کمکی ارزیابی و در صورت نیاز ارجاع به کنترل‌های امنیتی و کنترل‌ها پیشرفته دیگر

۶) توسعه استراتژی استفاده از دستورالعمل‌های ارزیابی گسترده

۷) بهینه سازی دستورالعمل‌های ارزیابی برای کاهش دوباره کاری‌ها و تهیه یک روش ارزیابی مقرون به صرفه

۸) نهایی سازی برنامه ارزیابی و اخذ تاییدیه‌های لازم برای اجرای آن

هر ارزیابی می‌بایستی طبق یک برنامه ارزیابی با توجه به محدوده، سطح ورود غیرمجاز یا گروه‌هایی مجری تست انجام گردد. این برنامه شامل قوانین و مرزهایی است که هر ارزیاب باید به آن توجه داشته

باشد این برنامه سازمان را با کاهش ریسک حادثه مانند قطع تصادفی سیستم یا افشاء غیرعمدی اطلاعات حساس حفاظت می‌کند.

برنامه ارزیابی هم‌چنین به وسیله اطمینان از این که مدیریت سازمان از محدوده ارزیابی، فعالیت‌ها و محدودیت‌ها آگاه و موافق هستند از تیم تست حفاظت می‌کند. توسعه برنامه ارزیابی می‌بایستی یک فرآیند مشارکتی بین ارزیاب‌ها و اعضا کلیدی گروه امنیتی سازمان باشد.

برنامه ارزیابی می‌بایستی این سئوال‌های اساسی را پاسخ دهد:

- محدوده ارزیابی چیست ؟

- چه کسی اختیار هدایت ارزیابی را دارد ؟

- پشتیبانی ارزیابی شامل چه چیزهایی است ؟

- اطلاعات حساس چگونه بررسی می‌شود ؟

- در حوادث چه اتفاقاتی باید رخ دهد ؟

برنامه ارزیابی باید مشخص کند چه سیستم‌ها و شبکه‌هایی باید تست گردند. این می‌تواند با مشخص کردن شماره سیستم‌ها و آدرس IP یا محدوده آدرس سیستم‌های مورد استفاده اتفاق بیافتد. این برنامه هم‌چنین باید سیستم‌های خاص را حداقل با ذکر آدرس IP آن‌ها و ترجیحاً با ذکر نام سیستم که نباید بر روی آن‌ها تست انجام شود لیست نماید. به‌عنوان مثال اگر بانک اطلاعاتی لیست حقوق یک سازمان به‌عنوان یک مأموریت حیاتی برای انجام تست‌های ویژه فرض گردد می‌بایستی نام سیستم و آدرس IP آن شامل لیست استثناهای برنامه ارزیابی شود. اگر سازمان بخشی از شبکه را کنترل نمی‌کند مثلاً اگر بخشی از شبکه سازمان درشبکه یک طرف سوم مقیم است در هنگام نوشتن برنامه ارزیابی باید رضایت صاحب آن شبکه خارجی نیز جلب گردد.

یک وضعیت مشابه شامل سیستم‌هایی است که توسط سازمان‌ها به اشتراک گذاشته شده است، مثل سیستمی که از تکنولوژی دستگاه مجازی برای خدمات به سازمان‌های مختلف استفاده می‌نماید. به وسیله امضا طرح ارزیابی، همه طرفین قرارداد، ارزیابی را تصدیق و قبول می‌کنند. علاوه برتعیین

نظام‌هایی که برای ارزیابی مجاز شده‌اند، طرح ارزیابی بایستی هم‌چنین جزئیات، نوع و سطح آزمایش مجاز را مشخص کند.

برای مثال، اگر سازمانی خواستار ارزیابی میزان آسیب‌پذیری باشد، طرح ارزیابی باید اطلاعاتش را از روی فعالیت‌های مجازی که روی شبکه هدف مانند پورت و سرویس شناسایی، جست‌جوی آسیب‌پذیری، مرور ساختار امنیتی، کشف پسورد با جزئیات کافی برای شرح نوع آزمایش، نحوه عمل و دیگر وسایلی که وجود دارد، تهیه نماید. برای مثال، اگر قرار است از کشف رمز استفاده شود، آن روش باید از طریقی که پسوردها به دست می‌آیند (برای مثال، خارج شدن از شبکه یا نسخه برداری از فایل پسورد سیستم) درطرح ارزیابی بدست آید.

آن طرح نیز باید با صراحت اظهار دارد که هر نوع فعالیتی از این قبیل ممنوع می‌باشد برای مثال، ایجاد و اصلاح فایل در این صورت است که فضایی برای برداشتی دیگر باقی نمی‌ماند. اگر سئوالات در دوره ارزیابی راجع به دامنه و سطح دسترسی است، ارزیاب‌ها و نقطه تماس شناخته شده سازمان (نماینده سازمان)، باید با هم ملاقات و بحث نمایند.

طرح هم‌چنین باید جزئیات منطقی تعهد شامل تعداد ساعت‌های کار ارزیاب‌ها، حدود و سطح زمینه‌های آزمایش، یک روش تلفنی با اطلاعات تماس جاری، شبکه و مراکز امنیت عملیات، و نقطه اصلی تماس برای ارزیابی به مرکز، موقعیت فیزیکی که فعالیت‌های ارزیابی در آن جا آغازخواهد شد و تجهیزات و ابزاری که برای هدایت ارزیاب استفاده خواهد شد را مشخص کند. همه ملزومات برای دادن اطلاعات به سازمان‌های مادر، اجرای قانون، و یک تیم خبره کامپیوتر درطرح ارزیابی، باید مشخص شوند.

علاوه بر این ، فردی مسئول برای مطلع ساختن سازمان‌ها از مراحل ارزیابی امنیت باید مشخص گردد.

راجع به حالت مخفی یا آزمایش اعلام نشده دیگر، طرح ارزیابی باید هم‌چنین چگونگی آزمایش آشکار سازی و گزارش به وسیله کارکنان امنیت سازمان، گروه CIRT، و دیگرانی که باید از روند کارها مطلع شوند را مشخص کند. مقصود اولیه برای اطمینان از این است که فعالیت ارزیابی به حریم طرفین قرارداد و تیم خبره تجاوز نمی‌کند. برای توانمند سازی مدیر شبکه، نشانی پروتکل دستگاه‌ها از هر کدام از فعالیت‌های ارزیابی درطرح ارزیابی مشخص خواهد شد تا فعالیت‌های ارزیابی مثل تست حمله‌های نفوذی را از حمله‌های هکرهای واقعی متمایز نمایند.

اگر اهداف ارزیابی به ثمر برسد، اداره کننده‌های امنیت می‌توانند سیستم‌های کشف نفوذ و دیگر وسایل دیده‌بانی امنیت را سازماندهی کرده و از فعالیت تولید شده توسط این آدرس‌ها در طول تست چشم پوشی کنند.

ملزومات داده گردانی که باید در طرح ارزیابی مشخص شوند شامل:

ذخیره سازی داده‌های سازمان در طول ارزیابی روی سیستم‌های ارزیاب، شامل حفاظت فیزیکی از سیستم‌ها، پسوردها، و رمزگذاری داده‌ها

ذخیره سازی داده‌ها بلافاصله بعد از خاتمه ارزیابی، برای دست‌یابی به ذخیره سازی ملزومات در بلندمدت یا پیگیری آسیب‌پذیری

انتقال داده‌ها درطی یا بعداز ارزیابی در داخل یا خارج شبکه

پاک کردن اطلاعات از سیستم‌ها بعد از پایان ارزیابی خصوصاً، برای ارزیاب‌های ثالثی که شامل منابعی برای ملزومات ویژه‌ای است که به وسیله رویه‌ها و شیوه‌های سازمان اصلی مشخص می‌شوند.

بالاخره، طرح ارزیابی باید دستورالعمل ویژه‌ای را بر اساس جابه‌جایی حادثه فراهم کند که در هر صورت ارزیاب‌ها سبب شوند تا یک حادثه در طول دوره ارزیابی آشکار گردد.

این بخش از طرح باید زمان حادثه و رهنمودهایی را مشخص کند تا معلوم شود که آیا حادثه‌ای اتفاق افتاده است یا نه. طرح بایستی خصوصیات اولیه را شناسایی کرده و نقاط فرعی تماس را برای ارزیاب‌ها، عموما رهبر تیم و رهبر تیم دستیاران ارزیابی، و گروه امنیت سازمان، ایجاد نماید. رهنمودها باید به گونه‌ای باشند که هم ارزیاب‌ها و هم گروه‌های امنیت سازمان با یک تصمیم و با وضوح اظهار دارند که یک حادثه رخ داده است. برای مثال، اگر ارزیاب‌ها یک هکر واقعی یا رد پایی از یک هکر را در شبکه پیدا کردند، آیا آزمایش بایستی متوقف شود؟ هم‌چنین ، چه موقع و با مسئولیت چه کسی آزمایش می‌تواند مجددا آغاز شود؟ طرح ارزیابی باید دستورالعمل‌های صریحی را بر اساس آنچه ارزیاب‌ها در این مواقع انجام می‌دهند، فراهم نماید. به علاوه بعضی از ارزیاب‌ها از ROE (قوانین درگیری) برای یا به جای یک طرح ارزیابی استفاده می‌کنند.

ROE شامل همان اطلاعات در طرح ارزیابی است و نیز فعالیت‌های آزمایشی را که معمولاً توسط سازمان ممنوع شده را مشخص می‌کند. برای مثال، برخی فعالیت‌هایی که اغلب در طول آزمایش نفوذ انجام می‌شود، مانند اقدام برای کشف رمز سیستم‌ها، معمولاً به خاطر سیاست‌های سازمان ممنوع شده است. ROE به ارزیاب‌ها برای انجام چنین فعالیت‌هایی به‌عنوان بخشی از فرآیند ارزیابی، مجوز می‌دهد. هر سازمان بایستی مشخص کند که چه موقع از طرح‌های ارزیابی و یا ROEs استفاده شود. سازمان‌ها هم‌چنین باید توسعه طرح‌های ارزیابی مرکزی یا قالب‌های ROE یا پیش‌نویس‌های مختصر، و ملزومات مورد استفاده برای توسعه پایدار را در نظر داشته باشند.

۵-۱۴- رعایت قانون

یک برآورد از عوامل بالقوه نگرانی‌های قانونی قبل از شروع به کار ارزیابی باید صورت پذیرد. تا موقعی که مشاوران حقوقی سازمان درگیر مسائل سازمان هستند ، توصیه می‌شود که همیشه به تست‌های مزاحم یابی مثل تست نفوذ پرداخته شود. اگر یک سازمان بخواهد به یک موجودیت خارجی برای هدایت ارزیابی مجوز دهد، بخش‌های حقوقی آن سازمان ممکن است درگیر مسئله شوند. این قسمت‌ها ممکن است در بررسی طرح ارزیابی و مشخص کردن غرامت یا محدود کردن مسئولیت موارد موجود در قرارداد که ارزیابان ناظر امنیت مخصوصاً برای انواع آزمایشاتی که تجاوزکارانه تلقی می‌شوند بکار می‌برند، کمک کنند. هم‌چنین بخش حقوقی ممکن است نهادهای خارجی را ملزم کند که موافقت‌های عدم افشایی را که ارزیاب‌ها در آن از آشکار کردن هرآن چه حساس، اختصاصی یا به عبارت دیگر اطلاعات محرمانه است که برای نهادهای غیر مجاز منع شده است را امضا کند. بخش حقوقی هم‌چنین بایستی هر گونه حریم خصوصی که ممکن است سازمان داشته باشد را معلوم نماید. اغلب سازمان‌ها علامت‌های اخطار یا توافقنامه‌هایی دارند که مونیتورینگ توسط سیستم‌ها را مشخص می‌کند علامتی که اجازه می‌دهد افراد به واسطه استفاده از سیستم‌هایشان مراقبت شوند. اما، همه سازمان‌ها این علامت‌ها را در محل خود ندارند و بخش حقوقی بایستی حریم‌های قابل تجاوز را قبل از شروع ارزیابی مشخص کند.

به علاوه، اطلاعات به دست آمده ممکن است شامل داده‌های حساسی باشد که متعلق به سازمان یا اطلاعات شخصی یک کارمند نیست و ممکن است حریم خصوصی تلقی شود. ارزیاب‌ها باید از این خطرها آگاه باشند و از همه دستورات و ملزوماتی که به وسیله بخش حقوقی بیان می‌شود پیروی کنند.

بخش حقوقی هم ممکن است شرایط لازم برای داده گردانی را برای اطمینان از عدم افشای آن‌ها، مشخص کند (مثال: آسیب‌پذیری‌ها)

۵-۱۵- خلاصه

ارزیابی امنیت اطلاعات یک فعالیت پیچیده به دلیل ملزومات سازمانی، عدد و نوع سیستم‌ها در یک سازمان، تکنیک‌های فنی و مبحث همکاری، توسط ارزیاب‌ها انجام می‌شود. ارزیابی‌های امنیتی می‌توانند از طریق یک طرح ثابت با فرآیندهای تکرار پذیر ساده شوند و ریسک‌های ارتباطی کاهش یابند. هم‌چنین طرح ریزی درست و به موقع یک ارزیابی امنیت می‌تواند این اطمینان را بدهد که تمامی عوامل لازم برای موفقیت ارزیابی مورد توجه قرار گرفته‌اند.

فعالیت‌های اصلی در طرح ریزی برای یک ارزیابی شامل:

ایجاد سیاست ارزیابی امنیت:

سازمان‌ها باید یک سیاست ارزیابی امنیت اطلاعات ایجاد کنند تا جهت گیری و راهنمایی لازم را برای ارزیابی امنیت آن‌ها فراهم آورد. این سیاست باید نیازمندی‌های ارزیابی امنیت را شناسایی کرده و آن‌هایی که در جهت برآوردن این نیازها هستند، را نگه دارد. سیاست مصوب باید به پرسنل مربوطه و شرکت‌ها و سازمان‌هایی که در ارتباط با این سازمان هستند ابلاغ شود. این سیاست حداقل به صورت سالیانه یا موقع به‌وجود آمدن نیازهای جدید ارزیابی باید مورد بازنگری قرار بگیرد.

۵-۱۴-۱- اولویت بندی و زمانبندی ارزیابی‌ها:

سازمان‌ها باید تصمیم بگیرند که چه سیستم‌هایی باید مورد ارزیابی قرار بگیرد و این ارزیابی‌ها در چه زمان‌هایی باید انجام بگیرد. این اولویت بندی بر اساس طبقه بندی سیستم، منافع مورد انتظار، نیازهای زمانبندی، قوانین اجرایی جایی که ارزیابی مورد نیاز است و وجود منابع انجام می‌گیرد. هم‌چنین ملاحظات فنی نظیر صبر کردن تا زمان اصلاح ضعف‌های شناخته شده یا به‌روز رسانی برنامه ریزی شده قبل از آزمایش، می‌تواند فواصل زمانی ارزیابی را مشخص کند.

۵-۱۴-۲- انتخاب و سفارشی کردن تست‌های فنی وتکنیک‌های آزمایش

برای این که سازمان‌ها تعیین کنند که چه تکنیک‌هایی را برای یک ارزیابی ویژه استفاده کنند، باید عوامل زیادی را مورد توجه قرار دهند. عواملی نظیر اهداف ارزیابی، دسته‌ای از تکنیک‌هایی که می‌تواند اطلاعاتی را برای پشتیبانی این اهداف بدست آورد وتکنیک‌های مناسب در هر دسته. هم‌چنین سازمان تکنیک‌هایی را برای مشخص کردن دیدگاه ارزیاب (مثلاً داخلی در مقایسه با خارجی) لازم دارد به طوری که تکنیک‌های مربوطه بتوانند انتخاب شوند.

۵-۱۴-۳- مشخص کردن تدارکات لازم برای ارزیابی

این بخش شامل شناسایی کلیه منابع لازم شامل تیم ارزیابی؛ انتخاب محیط‌ها و مکان‌هایی که ارزیابی در آن‌ها انجام می‌گیرد؛ و گردآوری و پیکربندی تمامی ابزارهای تکنیکی لازم، می‌شود.

۵-۱۴-۴- ایجاد طرح ارزیابی

طرح ارزیابی فعالیت‌های طراحی شده برای یک ارزیابی و اطلاعات دیگر مربوط به آن را مستند می‌کند. برای هر ارزیابی یک طرح باید ایجاد شود تا قوانین و حدودی که ارزیاب باید به آن‌ها پایبند باشد، را تعیین کند. این طرح باید سیستم‌ها و شبکه‌های مورد ارزیابی، نوع و سطح تست‌های مجاز، جزئیات تدارکاتی ارزیابی، نیازمندی‌های داده‌گردانی و راهنمای برخورد با حوادث را شناسایی کند.

۵-۱۴-۵- مراجعه به ملاحظات قانونی

سازمان‌ها قبل از شروع به ارزیابی باید بنگاه‌های قانونی بالقوه‌ای را مورد شناسایی و ارزیابی قرار دهند، به ویژه اگر ارزیابی شامل تست‌های سرزده باشد (مثلا تست نفوذپذیری)یا توسط واحدهای خارجی انجام گیرد. دپارتمان‌های قانونی می‌توانند طرح ارزیابی را بازخوانی کرده، ملاحظات پنهان آن را استخراج کرده و کارهای دیگری را در پشتیبانی از طرح ارزیابی انجام دهند.

۵-۱۵- اجرای ارزیابی امنیت

در طول اجرای ارزیابی امنیت،آسیب‌پذیری‌ها به وسیله روش‌ها و تکنیک‌هایی که در فاز طراحی تعیین شده یا در طرح ارزیابی یا ROE مشخص شده‌اند، شناسایی می‌شوند. این مسئله که ارزیابی مطابق با طرح یا ROE اجرا شود خیلی مهم و حیاتی است و هدف این بخش پر رنگ کردن و بیان نکات کلیدی

است که ارزیاب‌ها آن‌ها را در فاز اجرایی مورد توجه قرار می‌دهند. برای مثال، هماهنگی مناسب در طی اجرای ارزیابی را آسان می‌کند و امکان وقوع ریسک‌های مرتبط را کاهش می‌دهد. ملاحظات کلیدی نظیر، نحوه برخورد با حوادث و ساختار چالش‌هایی که هنگام ارزیابی،آن‌ها مواجه می‌شویم نیز بحث می‌شود. این بخش هم‌چنین در مورد فرآیند تحلیل بحث می‌کند و پیش‌نهادهایی را در مورد جمع آوری،ذخیره سازی،انتقال و تخریب داده‌های وابسته به ارزیابی ارائه می‌کند.

۵-۱۵-۱- هماهنگی

در طی انجام ارزیابی این نکته خیلی مهم و حیاتی است که ارزیابی با واحدهای مختلف سازمان هماهنگ باشند. ملزومات این هماهنگی توسط طرح ارزیابی یاROE مشخص می‌شود و باید مطابق آن عمل شود.

هماهنگ شدن مناسب تضمین می‌کند:

افراد ذی‌نفع از زمان بندی ارزیابی، فعالیت‌ها و ضرباتی که ممکن است ارزیابی داشته باشد،آگاه می‌شوند

ارزیابی در هنگام به روز رسانی‌ها،اعمال فن‌آوری جدید یا سایر مواردی که امنیت سیستم تغییر می‌یابد، انجام نمی‌گیرد. (مثلاً تست به هنگام تعمیرات ویندوز یا دوره‌ای که بهره سیستم کم است)

امکان دسترسی لازم به امکانات و سیستم‌ها برای ارزیابی به شکل مناسبی فراهم می‌شود.

افراد مناسب (مانند ارزیاب‌ها، تیم پاسخ‌گو به حوادث، مدیریت ارشد) به هنگام وقوع حادثه آگاه می‌شوند. وقتی حادثه‌ای اتفاق می‌افتد، توصیه می‌شود که فعالیت‌های ارزیابی تا زمان شناسایی و گزارش حادثه متوقف شوند و هنگامی این فعالیت‌ها از سر گرفته می‌شود که مجوز لازم مطابق با طرح ارزیابی یا ROE به ارزیاب‌ها داده شده باشد. محدوده فعالیت‌هایی که باید به حالت تعلیق در آید، بر اساس سازمان و نوع حادثه تغییر پیدا می‌کند اما در بسیاری از موارد تنها فعالیت‌هایی که سیستم‌ها در آن به‌طور مستقیم با حادثه در گیر می‌شوند، معلق می‌گردند.

سطح هماهنگی بین ارزیاب‌ها و سازمان ابتدا توسط سیستم و نوع ارزیابی که انجام می‌شود، معین می‌گردد. سیستم‌های حساس عمدتاً نیاز به هماهنگی بیش‌تری دارند تا دسترس پذیری سیستم به

هنگام مشغول بودن سیستم تضمین گردد و تکنیک‌های ارزیابی سطوح مختلف از مخاطرات را به سیستم هدف در هنگام اجرا معرفی می‌کنند. تکنیک‌هایی که گروه بازبینی هستند دارای حداقل ریسک می‌باشند. گروه شناسایی هدف و تحلیل دارای ریسک متوسط هستند و گروه تایید آسیب‌پذیری هدف دارای بالاترین ریسک است. به عنوان مثال، سیستم حساسی که می‌خواهد تحت تست نفوذپذیری قرار بگیرد، عمدتاً نیاز بیش‌تری به هماهنگی دارد تا بازبینی سند یک سیستم حساس یا تست نفوذپذیری یک سیستم غیر حساس. با این وجود سازمان‌ها ممکن است با شرایط معکوس با این شرایط ذکر شده مواجه شوند که در این موارد سطح هماهنگی‌ها باید با نیازمندی‌ها و توجهات سازمانی متناسب باشند. ارزیاب‌ها و افراد ذی‌نفع- همانند صاحبان سیستم- باید در طول انجام ارزیابی‌ها هوشیار باشند. سطح دسترسی لازم برای ارزیاب‌ها هم‌چنین، هماهنگی لازم برای تضمین دسترسی فیزیکی و سیستمی مناسب را تعیین می‌کند. (به عنوان مثال هنگام تست تهدید خودی)

۵-۱۵-۲- ارزیابی کردن

هم‌چنان که بحث شد، طرح ارزیابی یا ROE رهنمودهایی را برای هدایت کردن ارزیابی،فراهم می‌کند. طرح یا ROE باید به طور کامل دنبال شود مگر این که اجازه خاصی در این مورد صادر شده باشد که این اجازه می‌تواند به صورت کتبی توسط امضا کننده اصلی یا دستوری از طرف یک مقام باشد این مسئله که ارزیاب‌ها طرح یا ROE را بخوانند و مفهوم آن را درک کنند خیلی مهم و حساس است. به ارزیاب‌ها توصیه می‌شود که طرح یا ROE را به‌طور متناوب در طول دوره ارزیابی بازخوانی کنند، به ویژه در مورد فعالیت‌هایی که در گروه تایید نفوذپذیری هدف قرار می‌گیرد.

در طول یک ارزیابی، تیم پاسخ‌گو به حوادث ممکن است یک حادثه را آشکار کنند. این حادثه می‌تواند ناشی از عمل ارزیاب‌ها باشد یا توسط یک مهاجم واقعی برای حمله به سیستم به هنگام ارزیابی به‌وجود آمده باشد. صرف نظر از این‌ها، تیم پاسخ‌گو به حوادث یا افرادی که حادثه را کشف می‌کنند باید رویه رشد طبیعی سازمان را دنبال کنند و ارزیاب‌ها باید رهنمودهایی که پیشاپیش توسط طرح ارزیابی یا ROE تعیین شده است پیروی کنند مگر این که طوری دیگر دستور داده شده باشد. اگر یک مهاجم در طول ارزیابی شناسایی شود، این مورد باید بلافاصله به فرد مناسب گزارش شود و ارزیاب باید بر اساس قرارداد مشخص شده در طرح ارزیابی یا ROE عمل کند. توصیه می‌شود، ارزیاب‌ها ارزیابی سیستمی که دچار حادثه شده است را متوقف کنند در حالی که سازمان در حال پاسخ‌گویی به آن است.

علاوه بر رویایی با حوادث یا آشکار کردن حوادث موجود، ارزیاب‌ها ممکن است با سایر چالش‌های تکنیکی، عملیاتی و سیاسی در طول ارزیابی مواجه شوند. این مواجه شدن می‌تواند شامل موارد زیر باشد:

۵-۱۵-۲-۱- مخالفت:

مخالفت با ارزیابی می‌تواند ناشی از منابع مختلفی در سازمان شامل مدیران سیستم و شبکه و کاربران نهایی باشد. دلایل این مخالفت می‌تواند شامل ترس از دست دادن، در دسترس بودن سیستم یا شبکه، ترس از مجازات شدن، اذیت رسانی و مقاومت در برابر تغییرات باشد. به دست آوردن مجوزهای لازم از مدیران رده بالا و پشتیبانی شدن از طرف آن‌ها به حل شدن مسائل مرتبط با مخالفت کمک می‌کند و ترکیب کردن و هماهنگ کردن ارزیابی‌های امنیت با سیاست‌های امنیتی کلی سازمان به برقراری فرآیندی کمک می‌کند که مدیران و کاربران را دچار شگفتی نمی‌کند.

۵-۱۵-۲-۲-کمبود واقع بینی:

هنگام آماده شدن برای ارزیابی، کاربران و مدیران بعضی وقت‌ها تنظیمات سیستم خود را تغییر می‌دهند تا سیستم خود را امن‌تر، مقاوم در برابر حملات یا هماهنگ با سیاست‌ها و سایر نیازها کنند. در حالی که این مسئله مثبت به نظر می‌رسد، ولی این تغییرات انجام شده فقط در طول ارزیابی اعمال می‌شوند و بعد از آن سیستم به تنظیمات اولیه خود باز گردانده می‌شوند. عدم ایجاد جلب توجه خاص برای ارزیابی به کاربران و مدیران به حل این چالش کمک می‌کند. بسیاری از سازمان‌ها بعضی وقت‌ها ارزیابی‌های اعلام نشده را انجام می‌دهند به عنوان متمم ارزیابی‌های اعلام شده.

۵-۱۵-۲-۳- کاهش سریع:

هنگامی که یک ضعف امنیتی در طول انجام ارزیابی شناسایی می‌شود، ممکن است مدیران بخواهند قدم‌هایی را در جهت کاهش این ضعف‌ها بردارند و از ارزیاب‌ها انتظار دارند آن‌ها را مورد ارزیابی مجدد قرار دهند تا مشخص شود که مشکل مربوط به سیستم آن‌ها مرتفع گشته است. گرچه چنین رفتاری برای کاهش سریع ضعف‌ها قابل تحسین است، ارزیاب‌ها باید توجه کنند به دنبال روی از رویه‌ها و سیاست‌های مدیریت تغییر سازمانی داشته باشند.

۵-۱۵-۲-۴- زمان:

ارزیابی امنیت اغلب مواقع با توسعه بخشی‌ها یا درجه توجه کم و زمان محدود ترکیب می‌شود . مسئله زمان نیز می‌تواند چالش به وجود آورد. موقعی که تکنیک‌های تست توانایی ایجاد عدم در دسترس بودن سیستم‌ها و شبکه‌ها را موقع تست داشته باشند. اغلب مواقع ارزیاب‌ها موقع تست کردن مجبور به محدود شدن به زمان خاص می‌شوند، در حالی که مهاجمان واقعی چنین محدودیتی را ندارند.

۵-۱۵-۲-۵- منابع:

ارزیابی امنیت به طور پیوسته با چالش به دست آوردن و نگهداری کردن منابع مناسب رو به رو است(به عنوان مثال تیم تست ماهر و سخت افزار و نرم افزار به روز). توصیه می‌شود که سازمان‌ها ابزار ارزیابی امنیت مانند لپ‌تاپ‌ها و کارت‌های بی سیم را منحصراً برای کار ارزیابی تخصیص دهند. اگر از نرم افزارهای تجاری استفاده می‌شود، نسبت به خریداری Licenceهای پیوسته و قراردادهای پشتیبانی باید توجه شود. ارزیاب‌ها باید طوری زمان بندی کنند که قبل از شروع ارزیابی از انجام تعمیر و به روز رسانی نرم افزارها مطمئن شوند. اگر ارزیاب‌های داخلی موجود نباشند یا نیازمندی‌های ارزیابی را برآورده نمی‌کنند، پیدا کردن ارزیاب‌های خارجی قابل اعتماد یک چالش خواهد بود. سازمان‌ها باید به دنبال شرکت‌هایی با روش‌های معلوم شده، فرآیندهای اثبات نشده، عمل‌کرد قبلی کافی و قابل مقایسه و پرسنل مجرب باشند. اگر سازمانی از ارزیاب‌های داخلی استفاده می‌کند، باید نسبت به استخدام و آموزش ارزیاب‌های ماهر اقدام کند.

۵-۱۵-۲-۶- رشد فن‌آوری:

ارزیاب‌ها باید از نظر ابزار و تکنیک‌های تست به روز باشند. بودجه باید طوری باشد که اجازه شرکت در کلاس‌ها و کنفرانس‌های دوره‌ای را به ارزیاب‌ها بدهد تا مهارت‌های خود را به روز و تازه کنند.

-ضربه‌های عملیاتی- گر چه ارزیابی‌ها به منظور جلوگیری از ضربه‌های عملیاتی طراحی شده‌اند، اما همیشه شانس عوارض تصادفی و غیر منتظره وجود دارد. هر تستی که انجام می‌شود باید اطلاعات مربوط به زمان‌ها، نوع تست، ابزار استفاده شده، لیست و دستورات و آدرس IP تجهیزات تست و غیره باید ثبت شوند. توصیه می‌شود که از کدهای ثبت کننده برای ثبت تمامی دستورات و کلیدهای فشار

داده شده در طول فرآیند تست استفاده شود. ابزارهای Terminal و GUI وجود دارند که می‌توانند فعالیت‌های تست کننده را ثبت کنند و این روش ثبت هم‌چنین کمک می‌کند به شمارش مواردی که تست به طور منفی روی عمل‌کرد سیستم تأثیر می‌گذارد. به علت خطر ضربه عملیاتی توصیه می‌شود که در طول تست یک طرح معتبر پاسخ گو به حوادث وجود داشته باشد.

۵-۱۶- تحلیل‌ها

گرچه برخی از تحلیل‌ها ممکن است بعد از کامل شدن ارزیابی شود، اغلب تحلیل‌ها در طول دوره ارزیابی انجام می‌گیرند. اهداف اصلی از تحلیل ارزیابی شناسایی نکات منفی، دسته بندی آسیب‌پذیری‌ها و پیداکردن علل آسیب‌پذیری‌ها می‌باشد. ابزارهای خودکار می‌توانند یافته‌های قابل توجهی را تولید کنند، اما این یافته‌ها در اغلب موارد نیاز به بررسی و تایید دارند تا یافته‌های نادرست مجزا گردند. ممکن است ارزیاب‌ها آسیب‌پذیری‌ها را با آزمایش دستی سیستم آسیب پذیر، تایید کنند یا این که ابزار خودکار دومی را نیز استفاده کرده و نتایج این دو را با هم مقایسه کنند. با وجود این که این کار سریع انجام می‌شود، این ابزارهای مقایسه‌گر اغلب نتایج مشابهی را تولید می‌کنند - که شامل همان یافته‌های نادرست است. آزمایش دستی معمولاً نتایج دقیق‌تری را نسبت به مقایسه نتایج ابزارهای گوناگون تولید می‌کند، اما این پتانسیل را نیز دارد که وقت گیر باشد.

اگر شناسایی و برطرف کردن آسیب‌پذیری‌های مختلف مهم می‌باشد، شناسایی علت اصلی آسیب‌پذیری‌ها کلید پیشرفت فرآیند امنیتی سازمان می‌باشد زیرا علت اصلی، اغلب ناشی از ضعف در سطح برنامه می‌باشد. بعضی از علت‌های اصلی معمول عبارتند از:

مدیریت ناکافی در اعمال پچ‌ها، شامل عدم اعمال به موقع پچ و اعمال نکردن پچ به همه سیستم‌های آسیب پذیر

مدیریت تهدید ناکافی، شامل ویروس کش‌های به روز نشده، فیل‌تر ناموثر هرزنامه‌ها و مجموعه قوانین Firewall که سیاست‌های امنیتی سازمان را تامین نمی‌کنند.

کمبود خطوط مبنای امنیتی مانند پیکره بندی امنیتی متناقض برای سیستم‌های مشابه

اعمال ضعیف مسائل امنیتی به چرخه حیات توسعه سیستم، شامل فقدان یا ناکافی بودن نیازمندی‌های امنیتی، و آسیب‌پذیری‌ها در کد اجرایی تولید شده توسط سازمان.

ضعف ساختار امنیتی مانند، فن‌آوری‌های امنیتی به‌طور صحیح در زیر ساخت‌ها در نظر گرفته نشده‌اند(مثلا قرارگیری ضعیف، پوشش ناکافی یا فن‌آوری‌های تاریخ گذشته) یا این که قرارگیری ضعیف سیستم‌ها که باعث افزایش ریسک سازش آن‌ها می‌شود.

فرآیندهای پاسخ به حادثه ناکافی مانند پاسخ‌های دیر به فعالیت‌های تست نفوذ پذیری.

آموزش‌های ناکافی هم برای کاربران نهایی(مثلا ناموفق بودن در شناسایی حملات مهندسی یا توسعه نقاط دسترسی بدون سیم)و برای مدیران شبکه و سیستم(مثلا توسعه سیستم‌ها با امنیت پایین)

ناکافی بودن سیاست‌های امنیتی یا اجبارهای امنیتی(مثلا درگاه‌های باز، سرویس‌های فعال،پررتکل‌های ناامن و پسوردهای ضعیف)

هدف دیگر تحلیل ارزیابی، شناسایی آسیب‌پذیری‌های حساسی است که سازمان باید بلافاصله از آن آگاه شود. به عنوان مثال، اگر تست نفوذ پذیری باعث آسیب‌پذیری گردد، ارزیاب‌ها بتوانند از حقوق مدیران سیستم در یک سیستم حساس برخوردار گردند، ارزیاب‌ها باید بلافاصله به شخص اشاره شده در طرح ارزیابی یا ROE معرفی گردند.

۵-۱۷- داده گردانی

روشی که به وسیله آن داده‌های یک سازمان از طریق ارزیاب بررسی شده تا اطمینان حاصل شود که از موارد مهمی مانند اطلاعات حساس که شامل چیدمان سیستم، ساختار حفاظتی، و آسیب‌پذیری سیستم‌ها، محافظت می‌شود. سازمان‌ها بایستی از صحت اسناد مورد نیاز برای داده گردانی در طرح ارزیابی یا ROE، و در خصوص وفاداری در سیاست‌ها و آسیب‌پذیری‌های سازمان‌هایشان اطمینان حاصل کنند. این بخش روش‌های توصیه شده‌ای را برای جمع آوری، ذخیره سازی، و انتقال داده درطی انجام کار ارزیابی، به به‌ترین نحو ممکن برای ذخیره سازی و انهدام داده‌ها پیش‌نهاد می‌کند.

۵-۱۸- جمع آوری اطلاعات

اطلاعات مناسب باید به وسیله یک تیم و از طریق ارزیابی جمع آوری شود. این موارد شامل اطلاعات ساختاری و چیدمانی شبکه‌های مورد بحث و هم‌چنین اطلاعات فعالیت‌های ارزیاب می‌باشد. زیرا این داده‌ها حساس است و مهم است که به نحوی شایسته ارزیابی شود. انواع اطلاعات ارزیاب‌ها ممکن است شامل موارد زیر باشد:

۵-۱۸-۱- ساختار و داده‌ها پیکربندی

نوع ارزیابی و نتیجه مطلوب باعث جمع آوری اطلاعات به وسیله تیم شده، که ممکن است شامل، نشانی پروتکل‌های اینترنت، سیستم عامل، موقعیت‌های فیزیکی و منطقی شبکه، پیکربندی‌های حفاظتی و آسیب‌پذیری‌ها باشد.

فعالیت‌های ارزیاب

ارزیاب‌ها بایستی یک ثبت روزانه که شامل اطلاعات ارزیابی سیستم و یک ثبت گام به گام از فعالیت‌هایشان داشته باشند. این پیگیری مستمر باعث می‌شود تا سازمان فرصت یابد بین فعالیت‌های ارزیاب‌ها و دشمنان واقعی فرق بگذارد. هم‌چنین ثبت فعالیت می‌تواند در توسعه گزارش نتایج ارزیابی، سودمند باشد.

با استفاده از ثبت کننده‌ی ضربه کلید روی سیستم ارزیاب، قدم به قدم می‌توان بسیاری از فعالیت‌های آزمایشگر را البته بدون ثبت کلیک موس، و نیز فعالیت‌های قطعی شده را ثبت نمود. برای وسائل خودکار، ارزیاب‌ها می‌توانند از هر وسیله مورد استفاده، اطلاعات ثبت شده را دریافت نمایند.

در صورتی که ممکن است ارزیاب‌ها ثبت کننده ضربه کلید یا دستگاه وقایع نگار را انتخاب کرده و کپی خروجی را از آن برای یک سیستم جداگانه به منظور ایجاد یک انبار متمرکز داده بگیرند، یک شیوه دیگر به صورت دستی، ثبت فعالیت‌هایی است که هر دستور اجرا شده به وسیله ارزیاب‌ها روی شبکه را مشخص می‌کند. این شیوه برای ارزیاب‌ها زمان‌بر است، و به خاطر این مشکل استفاده نمی‌شود. اگر از ثبت کننده فعالیت‌ها استفاده می‌شود، باید حداقل شامل اطلاعات تاریخ و زمان، اسم ارزیاب‌ها، شناسه سیستم ارزیاب، شناسه سیستم هدف وسیله استفاده شده، فرمان اجرا شده و توضیحات باشد.

۵-۱۸-۲- ذخیره سازی داده‌ها

ذخیره سازی ایمن داده‌های جمع آوری شده در طول ارزیابی، به انضمام آسیب‌پذیری‌ها، تجزیه و تحلیل نتایج، و توصیه‌های کاهش ریسک، از جمله مسوولیت ارزیاب‌ها می‌باشد. انتشار نامناسب این اطلاعات می‌تواند به شهرت سازمان آسیب رسانده و احتمال بهره کشی را افزایش دهد. در حداقل ممکن، ارزیاب‌ها بایستی اطلاعات ذیل را برای شناسایی، تجزیه و تحلیل، و گزارش دهی روی برگه‌ی حفاظت شده سازمان، و انجام پیگیری از فعالیت‌های آزمایش ذخیره کنند:

طرح‌های ارزیابی و ROE ها

مستندسازی بر روی پیکربندی حفاظتی سیستم و ساختار شبکه

نتایج به دست آمده از ابزار خودکار و یافته‌های دیگر

گزارش نتایج ارزیابی

طرح اقدامات اصلاحی یا طرح عمل و مایلستون‌ها

انتخاب‌های زیادی برای ذخیره سازی اطلاعات آسیب‌پذیری‌های کشف شده وجود دارد از جمله نگهداری یافته‌ها به فرمت خروجی به وسیله ابزار مورد استفاده، یا وارد کردن یافته‌ها در یک پایگاه داده.

بیش‌تر وسائل جست‌جوگر آسیب‌پذیری فرمت‌های لیست سیستم، آسیب‌پذیری‌ها، و راهکارها تکنیک‌های کاهش ریسک را گزارش می‌کنند.

اگر ارزیابی محدوده کوچکی داشته باشد این ممکن است یک شیوه قابل قبولی باشد (مثلا فقط از یک ابزار استفاده شود). برای دقت بالاتر، ارزیاب‌ها، سازمان‌های بزرگ‌تر یا ارزیاب‌هایی که از ابزارها و شیوه‌های گوناگون استفاده می‌کنند، از یک روش ذخیره سازی قوی‌تر مانند صفحه گسترده یا پایگاه داده‌ها می‌توانند استفاده کنند. هرگاه امکانات محدود باشد، یک صفحه گسترده ممکن است برای تست‌ها و آزمایشات فرد مناسب باشد زیرا توسعه سریعی داشته و استفاده از آن آسان است و نتایج خروجی آن با یک فرمت سازگار، قابلیت اصلاح دارند. برای تست‌های پیچیده یا تست‌هایی با روش‌های تکنیکی گوناگون، فعالیت‌های ارزیاب‌ها به طور مکرر تکرار می‌شود یا زمان‌هایی که نیاز به ارتباط داده‌های آسان وجود دارد، ایجاد یک پایگاه اطلاعات ممکن است مفید باشد.

سازمان‌ها باید از ذخیره سازی ایمن داده‌های حساس ارزیابی از قبیل طرح ارزیابی یا ROE، داده‌های خام آسیب پذیر و گزارشات ارزیاب، مطمئن شوند. مطلوب دشمن مانند اطلاعات راجع به ساختار شبکه، چیدمان سیستم، کنترل‌های حفاظتی، و آسیب‌پذیری‌های خاص سیستم، باعث می‌شود تا طرح و نقشه‌ای برای استفاده سیستم‌های اطلاعاتی سازمان تهیه شود. سازمان‌ها ممکن است اطلاعات را روی حافظه‌های جدا شدنی یا سیستم اطلاعاتی که در مواقع نیاز در دسترس قرار می‌گیرند ذخیره کنند. حافظه‌های جدا شدنی یا سیستم طراحی شده برای ذخیره سازی این اطلاعات باید به صورت فیزیکی و به طور منطقی و به صورت روزانه از سیستم جدا شوند. دسترسی به این سیستم و اطلاعات آن باید به افرادی که به واسطه کارشان و مسئولیتشان به آن‌ها نیاز دارند، محدود شود. هم‌چنین پیش‌نهاد می‌شود این داده‌ها برای اطمینان از این که ایمن باقی می‌ماند.

ملزومات حفاظتی برای ارزیابی‌های ایمن داده‌ها متنوع است و ممکن است وضعیت مشخصی در سازمان نداشته باشد اما این ملزومات حفاظتی برای ارزیابی، باید در طرح ارزیابی یا ROE مشخص گردد. پشتیبانی صحیح از داده‌ها برای یک ارزیابی سازمانی با پیگیری آسیب‌پذیری‌ها و بهینه سازی عمل‌کردها باعث کاهش ریسک‌های شناخته شده خواهد شد. یک پشتیبانی پیگیر همیشگی ممکن است باعث شود که اثر بخشی برنامه‌های حفاظت اطلاعات سازمان‌ها توسط نظام‌های راهبردی و از نظر نوع آسیب‌پذیری، فرکانس اتفاقات و متوسط زمان بازسازی، و غیره ارزیابی شود.

سیستم‌های ارزیابی مثل سرورها، لپ‌تاپ‌ها، یا وسیله‌های پرتابل دیگر هنگام ضبط داده‌های حساس در جا و مکان نامناسب و بدون محافظ نباید رها شوند. به عنوان مثال سیستم‌های پرتابل نباید بدون قفل باشند یا قفل غیر ایمن شوند و سیستم‌های پرتابل در اتاق‌ها باید توسط کابل‌های مخصوص قفل شوند و در اتاق‌های مطمئنی نگهداری شوند یا با وسائل فیزیکی دیگر محافظت شوند. علاوه بر این حفاظت‌ها، ارزیاب‌ها باید مطمئن شوند که سیستم به صورتی پیکربندی شده است که هکرها را از دستبرد زدن به آن مأیوس می‌کند. ارزیاب‌ها باید تست‌های مناسب برای اطمینان از صحت و قابل اعتماد بودن داده‌های یک سیستم انجام دهند و این که سیستم در کم‌ترین حالت ممکن، با یک پسورد قوی محافظت می‌شود و پیش‌نهاد می‌گردد که سازمان‌ها از دو فاکتور قانونی استفاده کنند. به علاوه، همه داده‌های حساس روی سیستم باید رمزدار شده باشد و باید یک مکانیزم اثبات صحت، جدا از اثبات صحت خود سیستم، برای محدود کردن دسترسی به اطلاعات رمزدار شده، استفاده شود.

۵-۱۸-۳- انتقال داده‌ها

ممکن است لازم شود که داده‌های ارزیابی از قبیل پیکربندی سیستم و آسیب‌پذیری‌ها بر روی شبکه یا اینترنت جابه‌جا شود و این مهم است که از ایمنی اطلاعات فرستاده شده در مقابل خطر، اطمینان حاصل شود. طرح ارزیابی یا ROE، بایستی ملزومات فرآیند انتقال اطلاعات حساس را درعرض شبکه یا اینترنت مشخص کند. روش‌های انتقال داده‌های ایمن شامل رمزدار نمودن فایل‌های شخصی محتوی اطلاعات حساس، رمزدار نمودن کانال‌های ارتباطی که از FIPS استفاده می‌کنند (مثل VPNها، پروتکل‌های SSL) و تهیه اطلاعات از طریق تحویل دادن کپی‌های سخت یا نرم می‌باشد

۵-۱۸-۴-انهدام داده‌ها

زمانی که داده‌های ارزیابی به مدت طولانی مورد نیاز نباشد، سیستم‌های ارزیابی، سندهای چاپ شده، و سندهای صوتی تصویری باید به طور صحیحی پاک شوند.

این کار ممکن است به یکی از چهار روش ذیل صورت پذیرد:

۵-۱۸-۴-۱- دورریختن:

عمل دور ریزی مدیا بدون هیچ‌گونه ملاحظات پاکسازی. این بیش‌تر اوقات شامل کاغذهای مخصوص که حاوی اطلاعات غیر محرمانه است می‌باشد اما ممکن است روی دیگر مدیاها انجام گیرد.

۵-۱۸-۴-۲- پاک کردن:

یک سطح از پاک‌سازی مدیا که از اطلاعات سری در مقابل حمله قوی توسط صفحه کلید محافظت می‌کند. حذف ساده آیتم برای پاک کردن کافی نیست. پاک کردن باید از اطلاعات در مقابل بازیابی داده‌ها، دیسکت، یا نرم افزارهای بازیابی اطلاعات، محافظت کند و باید در مقابل تلاش‌های بازیابی که به وسیله‌های مختلف اجرا می‌شود مقاومت کند. بازنویسی(روی اطلاعات قبلی) یک مثال از یک روش قابل قبول برای پاک کردن مدیا می‌باشد.

۵-۱۸-۴-۳- خالی کردن:

یک فرآیند پاک‌سازی مدیا که از اطلاعات سری در برابر حمله‌های آزمایشگاهی محافظت می‌کند. برای برخی مدیاها، پاک کردن تنها برای محافظت کافی نیست. به‌عنوان مثالی دیگر پاک کردن مدیا، اجرای دستور پاک کردن حافظه ROM و کاهش اثر الکترومغناطیس می‌باشد.

۵-۱۸-۴-۴- خراب کردن:

تخریب فیزیکی برای رسیدن به این هدف که اطلاعات هرگز قابل بازیافت نباشند. تخریب فیزیکی از روش‌های گوناگونی از قبیل تفکیک ،سوزاندن، کوبیدن، تکه تکه کردن و ذوب کردن، امکان‌پذیر می‌باشد.

سازمان‌ها باید یک سیاست بر اساس ملزومات پاکسازی سیستم‌های ارزیابی خود داشته باشد.

ارزیاب‌های ثالث باید این اطمینان را بدهند که نیازهای سازمان را برای پاکسازی را درک می‌کنند، هم‌چنین روش‌ها ممکن است در سازمان‌های مختلف و حتی بخش‌های مختلف همان سازمان متفاوت باشد. برای مثال، در برخی سازمان‌ها ارزیاب‌ها به‌عنوان شخص ثالث از داشتن هرگونه دسترسی به داده‌های ارزیابی غیر از زمانی که گزارشات پایانی‌شان را ارائه می‌دهد منع شده‌اند در چنین مواقعی یک شخص واجد شرایط از سازمان باید ارزیابی کند که عمل پاک‌سازی به میزان کافی انجام شده باشد.

۵-۱۹- فعالیت‌های پس از آزمون

به دنبال فاز اجرایی- که علت به‌وجود آمدن به موضوع آسیب‌پذیری بر می‌گردد – سازمان‌ها باید در جهت مشخص کردن آسیب‌هایی که برای آن‌ها وجود دارد و تعریف شد قدم‌هایی بردارند. در این بخش راهکارهایی که سازمان می‌تواند یافته‌های خود را در کنش و کردار خود تعبیر نماید ارائه می‌کند و میزان حفاظت را ارتقا می‌دهد. ابتدا آنالیزها و متدها باید شکل بگیرد و سپس عمل‌کردهای تسکینی و کاهشی توسعه داده شود. در مرحله دوم توصیه‌ای اجرایی باید به صورت گزارش ارائه شود. نهایتاً از میان عوامل فوق فعالیت‌های تخفیفی استخراج خواهد شد – بسیاری از فعالیت‌های ارائه شده در این بخش ممکن است در خارج از فرآیند و روال سنجش اتفاق بیفتد- برای مثال به صورت بخشی از یک ریسک مالیاتی که از نتایج آزمون بهره می‌برد.

۵-۱۹-۱- توصیه‌های کاهش

همان طوری که تشریح شد بسیاری از آنالیزها و بررسی‌ها در طی دوره تست اتفاق می‌افتد. تجزیه و تحلیل نهایی نظیر بسط نتایج نهایی معمولاً بعد از اتمام کامل فعالیت‌های آزمونی شکل می‌گیرد و بعد از آن توصیه‌های کاهش گسترش یافته، درگیر خواهد شد. با توجه به این که تعریف و دسته بندی آسیب‌ها مهم می‌باشد، آزمون‌های امنیتی بسیار با ارزش‌تر و مفیدتر خواهد بود چنان‌چه برای استراتژی کاهش اجرا شده در سازمان بسط داده شده بتواند تأثیر گذار باشد. توصیه‌های کاهش که پی آمد تجزیه و تحلیل ریشه‌های انگیزه‌ای است باید برای هر یافته‌ای توسعه یابد علاوه بر آن شاید توصیه‌های فنی (برای مثال بکار بستن بخشی از یک پچ) و توصیه‌های غیر فنی که فرآیندهای سازمان را هدایت می‌کنند (برای مثال فرآیند بروز کردن مدیریت پچ) نیز استفاده شود. مثال یک فعالیت کاهش شامل سیاست، فرآیند، روش بهینه سازی، تغییرات در معماری امنیتی، آرایش تکنولوژی‌های جدید امنیتی و آرایش OS و کاربری پچ‌ها می‌باشد.

۵-۱۹-۲- گزارش دهی

به محض اتمام یک فعالیت تجزیه و تحلیل گزارش باید ارائه شود به طوری که در آن تعریف کامل سیستم، شبکه، آسیب‌های سازمانی و هم‌چنین فعالیت‌های توصیه‌ای کاهش را در بر داشته باشد. از نتایج آزمون‌های امنیتی می‌توان در موارد ذیل استفاده نمود:

به عنوان یک نقطه مرجع برای فعالیت‌های اصلاحی

در تعریف فعالیت‌های کاهش برای مشخص کردن تعاریف آسیب‌ها

به عنوان یک مبنا برای رهگیری میزان پیشرفت سازمان در حصول نیازهای امنیتی

برای دست‌یابی به وضعیت پیاده سازی نیازهای یک سیستم امنیتی

برای هدایت تجزیه و تحلیل نسبت هزینه/ سود به منظور توسعه سیستم‌های امنیتی

برای بالا بردن میزان سایر فعالیت‌های چرخه حیات نظیر تشخیص ریسک، C&A و تلاش برای توسعه فرآیندها

برای رسیدن به نیازهای گزارشی سازمان

نتایج آزمون امنیتی باید مستندسازی شود و فقط برای کارشناسان خاص قابل دسترسی باشد. این کارشناسان ممکن است شامل مدیران برنامه‌های خاص و صاحبان سیستم باشند. به دلیل این که گزارش ممکن است برای ارائه به چندین مخاطب باشد، لذا شاید نیاز به چنین قالب گزارش باشد تا مطمئن شویم که تمام موارد لحاظ شده باشد.

گزارش‌هایی که در سازمان باقی می‌ماند می‌تواند برای مخاطبین خاص نظیر مدیران برنامه، مدیران اطلاعات، مهندسین امنیت، مدیران ساختار یا گروه تکنسین‌ها مناسب باشد. گزارشات داخلی باید شامل روش آزمون، نتایج آزمون، تجزیه و تحلیل باشد. POA & M شما را مطمئن می‌سازد که آسیب‌های خاص با مشخصات‌شان به طور کامل معین شده‌اند. این مشخصات شامل میزان سنجش پذیری، در دسترس بودن، واقعیت گرا و قابل لمس بودن و محسوس بودن فعالیت‌ها می‌باشد.

۵-۱۹-۳- کاهش /اصلاحات

اولین قدم در این فرآیند آزمون توصیه‌های اصلاحی است. قبل از پیاده سازی یک فرآیند بهینه سازی فنی در محصولات تولیدی، باید ابتدا آزمون انجام شود. این آزمون در یک محیطی که نمونه کاملاً مشابه شبکه مورد نظر است در یک سیستم تستی اجرا خواهد شد و کلیه فعالیت‌های کاهشی در آن پیاده سازی خواهد شد برای مثال قبل از اقدام به انجام سرمایه گذاری، پچها باید در یک سیستم مشابه در محیط تست نصب شود و مورد ارزیابی قرار گیرد که در صورت بروز مشکل در آن‌ها مشخص شوند. این گونه تست‌ها ریسک این که سیستم در عمل به طور وارونه از آن چه که مورد نظر بوده کار نماید را، به‌طور جدی کاهش می‌دهند اما حذف نمی‌کند.

مرحله دوم باید با شکل و ساختار کنترلی سازمان یا ساختار مدیریت ارشد آن هماهنگ شود زیرا تمایل به ایجاد تغییرات در سیستم، شبکه، سیاست‌ها و روش‌های موجود دارد. بسط تغییرات هم قبل از گزارش و هم در زمان تکمیل فرآیندها ما را مطمئن می‌سازد که آگاهی لازم و مناسب انحصاراً در طول تغییرات و در محیطی فشرده با ماموریت‌ها و نحوه اجرا وجود دارد. حداقل مدیر برنامه یا صاحب سیستم، قبل از اجرای هر فعالیت باید آگاهی یابد و یک موافقت نامه برای اجرای طرح فعالیت‌های کاهشی قبل از پیاده سازی آن‌ها فراهم نماید. به دست آوردن مجوز مدیریتی می‌تواند با چالش همراه شود. تعریف این که چرا مجوز مورد نیاز است ممکن است سودمند باشد (به عبارت دیگر آیا فعالیت با

سیاست یا تکنولوژی جلو برده می‌شود) و به عنوان یک نکته مثبت در فعالیت‌های کاهشی ایده آل خواهد بود (به عبارت دیگر میزان امنیت را در وضعیت موجود و مطلوب افزایش می‌دهد).

تجزیه و تحلیل نسبت سود / هزینه با تجزیه و تحلیل کمیت افزایش میزان ذخایر ممکن است واقعی‌تر باشد. فاز بعدی که ممکن است دنبال شود و مورد نظر مدیریت ارشد سازمان نیز هست شامل کاهش افشای اطلاعات، کنترل پیشرفته سرمایه، کاهش آسیب‌پذیری، گرایش دست‌یابی به امنیت و نگهداری در سطح مطلوب می‌باشد.

مرحله سوم، فعالیت‌های کاهشی که پیاده سازی می‌شوند باید مرتب بازنگری شوند تا اطمینان یابیم که آن‌ها مناسب و دقیق پیاده سازی شده‌اند. بازنگری می‌تواند توسط ادامه ارزیابی سیستم، باز آزمون سیستم و اجزای آن و استفاده از کارمندان حساب‌رسی بخش دارایی در مستند سازی صورت پذیرد. ارزیابی سیستم یک بازنگری فنی از تغییرات ایجاد شده در سیستم را فراهم می‌کند و می‌تواند به کمک کارمندان بخش امنیت داخلی یا استفاده از یک سیستم امنیت در خارج از سازمان دنبال شود. تیم ارزیابی ممکن است از استراتژی کاهش به عنوان چک لیست استفاده کند برای این که مطمئن شود هر فعالیت به طور کامل انجام شده است. هم‌چنین بازآزمون سیستم تضمینی است جهت اجرای کامل فعالیت‌های کاهشی. نکته بسیار مهم این است که همواره به خاطر داشته باشیم که تیم آزمون‌گر فقط در صورتی قادر است پیاده سازی‌هایش را بازنگری کند که یک کپی کامل از سیستم مورد آزمون اصلی در اختیار داشته باشد.

آنچه از این روند استنتاج می‌شود این است که ممکن است آسیب‌پذیری‌های دیگری در طی آزمون‌های امنیتی سرپوشیده بماند. سازمان ممکن است بازنگری در پیاده سازی استراتژی‌های کاهشی را بدون معانی فنی نظیر مستند سازی انتخاب نماید. برای مثال ممکن است مقرون به صرفه باشد که کارمندان امنیتی برای پیاده سازی استراتژی کاهش، پاسخ‌گو بمانند که در این صورت باید سندی را که کل فعالیت‌های تکمیلی را شرح می‌دهد امضا نمایند. در کوتاه مدت این روش برای سازمان بسیار مقرون به صرفه است اما ریسک‌هایی که به دلیل عدم بازنگری فنی تغییرات انجام شده ممکن است به وجود آید، از بین نخواهد رفت.

در آخرین قدم، به عنوان پیاده سازی بخشی از استراتژی بسیار مهم است که اقدامات پیوسته به روز شود مخصوصاً برای تعریف فعالیت‌هایی که به طور کامل، نیمه تمام و فعالیت‌های معلق شده توسط شخص یا سیستم باقی مانده است. باید اطمینان یافت که اقدامات در روش‌های ساختار مدیریت سازمان تجمیع شده و یک پیگیری مرکزی و مدیریت در تغییرات سیستم، سیاست‌ها، مراحل، روش‌ها هم‌چنین یک مکانیزم فوق محلی که نیازهای مطلوب را روشن خواهد کرد را دنبال می‌کند.

۵-۲۰- سوالات فصل

ارزیابی امنیتی به چه منظور انجام می‌شود؟

دو نمونه از متدهای ارزیابی را نام ببرید؟

چرخه آزمون نفوذ را توضیح دهید؟

فعالیت‌های مستند سازی در آزمون نفوذ شامل چه بخش‌هایی می‌شود؟

عوامل پس از آزمون را توضیح دهید؟

آزمون شبکه‌های بی‌سیم از چند بخش تشکیل می‌شود؟

آزمون‌های بیرونی با آزمون‌های درونی چه تفاوتی با یک‌دیگر دارند.

فصل ششم - آزمون نفوذ پذیری

فصل ششم - آزمون نفوذ پذیری[1]

۶-۱- مقدمه:

امروز بسیاری از سازمان‌ها هزینه‌های گزافی را جهت برقراری سیستم‌های امن در شبکه‌های خود صرف می‌کنند.

در مقابل برخی سازمان‌های دیگر هنوز به اهمیت این امر پی نبرده‌اند.

انجام آزمون‌های نفوذ پذیری نه تنها برای سازمان‌های دسته دوم بلکه برای سازمان‌هایی که اقـدام به برقـراری سیستم‌های امن نموده‌اند نیز توصیه می‌شود. چرا که حتی در صورت پرداخت هزینه و استقرار چنین سیستم‌هایی نیاز به کنترل دائمی سیستم از لحاظ امنیتی امری اجتناب ناپذیر تلقی می‌گردد.

آزمون نفوذ پذیری به شبیه سازی آنچه نفوذ گران واقعی انجام می‌دهند می‌پردازد، اما در قالبی قانونمند و اخلاقی وبه منظور کشف ورفع آسیب‌پذیری‌های امنیتی سیستم‌ها.

لذا در این فصل ابتدا به معرفی این نوع آزمون‌ها وروش‌های اجرایی آن‌ها می‌پردازیم وسپس یک قالب نمونه از گزارشات نتایج آزمون را مورد بررسی قرار می‌دهد.

۶-۲- تعریف:

---

[1] Penetration Test

آزمون نفوذ پذیری به عنوان روشی جهت ارزیابی امنیت سیستم‌ها یا شبکه‌های کامپیوتری محسوب می‌گردد که در آن با شبیه سازی حمله‌های نفوذی افراد موسوم به crackerها میزان امنیت سیستم مورد بررسی قرار می‌گیرد.

۶-۳- روش‌های اجرایی:

۶-۳-۱- الف –روش جعبه سیاه[۱]

در این روش سیستم به شکل یک جعبه سیاه ناشناخته در نظر گرفته شده و آزمون گیرنده با فرض عدم

شناخت ساختار سیستم وفقدان دانش کافی، به تست آن می‌پردازد.

۶-۳-۲- ب-روش جعبه سفید[۲]

در این روش بر خلاف روش پیشین آزمون گیرنده از ساختار سیستم اعم از دیاگرام‌های شبکه، کدها

و آدرس‌های IP اطلاع کافی داشته و با این پیش فرض به تست سیستم می‌پردازد.

۶-۳-۳- ج-روش جعبه خاکستری[۳]

بدیهی است که این روش تلفیقی از دو روش فوق می‌باشد و در عین این که آزمون گیرنده به یک تست

---

۱ Black Box

۲ white Box

۳ Gray Box

صرفاً «کور کورانه (blind)نمی‌پردازد اما ممکن است به تمام ساختار سیستم نیز اشراف نداشته باشد.».

نکته:

آزمون نفوذ پذیری می‌بایست بر روی تمام سیستم‌ها، تمام سایت‌ها و زیر سایت‌ها انجام شود تا احتمال نفوذ کلیه کاربران عادی واستثنایی را به حداقل برساند.

۶-۴- متد لوژیهای نفوذ پذیری:

۶-۴-۱- متدلوژی OSSTM:۱

متد لوژی OSSTM روشی است که نحوه اجرای آزمون‌های امنیت واستفاده از معیارها واستانداردهای موجود را بیان می‌کند. مباحثی که در آزمون‌های OSSTM مورد بررسی قرار می‌گیرند به پنج دسته کلی ذیل تقسیم می‌شوند:

۱-کنترل‌های مربوط به اطلاعات وداده‌ها.

۲- سطوح آگاهی امنیتی کارکنان.

۳- سطوح کنترلی در خصوص جرائم کامپیوتری و مهندسی اجتماعی۲.

۴- شبکه‌های کامپیوتری و ارتباطی (مثل دستگاه‌های بی سیم –موبایل‌ها و ...).

۵-کنترل‌های مربوط به سطوح فیزیکی و محیطی امنیت (ساختمان‌ها، انواع محیط‌های فیزیکی).

---

۱ (the Open Source Security Testing Methodology Manual)

۲ Social Engineering

متدلوژی فوق با تمرکز بر روی جزئیات فنی به بررسی اقدامات پیش گیرنده، نگهدارنده و مقابله کننده پرداخته و در این راستا به معرفی روش‌های اندازه گیری بر روی نتایج بدست آمده نیز می‌پردازد.

۶-۴-۲- متدلوژی ISSAF[۱]:

متدلوژی ISSAF روشی است ساخت یافته و جدید که در بررسی و ارزیابی امنیت سیستم‌های اطلاعاتی، آن‌ها را به حوزه‌های مختلف تقسیم نموده و به بررسی و ارزیابی جزئیات در حیطه هریک از حوزه‌های مذکور می‌پردازد.

هدف روش مذکور ایجاد ورودی‌های خاص سیستمی به گونه‌ای است که امنیت را در یک سناریوی واقعی مورد بررسی قرار دهد.

در حقیقت ISSAF به عنوان روشی اولیه جهت تکمیل ارزیابی امنیتی یک سازمان به کار می‌رود. البته این روش همچنان در مراحل اولیه اجرایی خود قرار دارد.

۶-۴-۳- متدلوژی آزمون نفوذ پذیری[۲]:

این متد لوژی به بخش‌های کلی ذیل تقسیم می‌گردد:

۱-اسکن پورت‌ها.

۲-کاری که هم‌زمان با اسکن پورت‌ها جهت بررسی امنیت انجام می‌شود.

۳- انجام عمل Fingerprint بر روی سیستم.

۴-بررسی وکاوش سرویس‌ها.

۶-۵- آزمون نفوذ پذیری برنامه‌های تحت وب:

---

۱ Information Systems Security Assessment Framework

۲ Penetration Test

این نوع آزمون مجموعه‌ای از سرویس‌هایی است که جهت بررسی امنیت برنامه‌های تحت وب بکار می‌روند.

این سرویس‌ها عموما «به تشخیص موارد مربوط به موضوعات ذیل می‌پردازند:».

۱-تشخیص نقاط نفوذ پذیر وریسک‌های موجود در برنامه‌های تحت وب به صورت عمومی.

۲- تشخیص نقاط نفوذ پذیر شناخته شده یا ناشناخته جهت مبارزه با تهدیدها در فاصله زمانی یافتن راه حل مناسب جهت رفع مشکل امنیتی.

۳-تشخیص نفوذ پذیری‌های فنی (اسکیرپت‌های سایت‌ها، تشخیص هویت کاربران توسط برنامه، کلمات رمز موجود در حافظه، سر ریز بافرها، مدیریت اختیارات کاربران، دست‌کاری آدرس‌های URL و ...).

۴-تشخیص ریسک‌های تجاری (از دست دادن اعتماد مشتری، انتقال غیر مجاز وجوه و سرمایه، ورودهای غیر مجاز به سیستم، استخراج اطلاعات شخصی و ...).

با بیان توضیحات فوق و جهت تکمیل موضوع ارائه یک مثال عملی از نحوه ارائه نتیجه اقدامات یک آزمون نفوذ پذیری خالی از لطف نمی‌باشد.

۶-۶- قالب نمونه گزارش آزمون نفوذ پذیری.

- قالب گزارش.

- معرفی.

-جزئیات مربوط به تیم آزمون.

- تاریخ وموقعیت آزمون.

- جزئیات شبکه.

- یک به یک، کلاینت – سرور، مدل Domain ومدل Active Directory

- جزئیات سیستم‌های عامل.

- تعداد سرورها وایستگاه‌های کاری.

- برنامه‌های نرم افزاری اصلی.

- تنظیمات مربوط به سخت افزارها.

- ارتباطات (T۱، ماهواره، WAN، leased line و ...).

- رمز گزاری‌ها.

- نقش‌های اصلی شبکه وسیستم‌ها.

- حیطه آزمون.

- محدودیت‌های تحمیلی به تیم آزمون (آیتم‌های خارج از محدوده).

- هدف از تست.

- گسترش نسخ جدید نرم افزار.

- اطمینان از امنیت.

- نوع آزمون.

- ارزیابی نقاط نفوذ پذیر۱.

- آزمون نفوذ پذیری۱ .

---

۱ Vulnerability Assessment

-روش اجرایی.

- جعبه سفید.

تیم آزمون آگاهی و دسترسی کامل برای تست شبکه، سخت افزار، سیستم عامل وبرنامه‌ها را

دارد.

- جعبه سیاه.

نیازی به دانش خاصی از شبکه ارگان مورد بررسی نیست. (حمله بیرونی برون دانش).

- جعبه خاکستری.

تیم آزمون همانند یک کاربر درون سازمانی با اطلاعات معمول اقدام به حمله می‌نماید.

- جمع بندی (خلاصه وغیر فنی).

- موارد امنیتی سیستم عامل با سطوح بحرانی متفاوتی مورد بررسی قرار گرفت.

- موارد استخراج شده.

- ضعف سخت افزاری.

- ضعف نرم افزاری.

- اشتباهات ناشی از اعمال کاربران.

- مواردی که به دلیل محدودیت‌های محیطی قابل استخراج نیستند.

---

[1] Penetration test

- موارد امنیتی برنامه کاربردی.

- موارد استخراج شده ...

- موارد استخراج نشده ...

- موارد امنیتی فیزیکی.

- موارد استخراج شده ...

- موارد استخراج نشده ...

- موارد امنیتی کاربران.

- موارد استخراج شده ...

- موارد استخراج نشده ...

- موارد امنیتی عمومی.

- موارد استخراج شده ...

- موارد استخراج نشده ...

- گزارش فنی.

- موارد امنیتی سیستم عامل.

- امنیت فایل سیستم‌ها.

- جزئیات.

- پارتیشن بندی از نوع FAT در سیستم موجود می‌باشد که اجازه کنترل و تریسها را نمی‌دهد.

- پیش‌نهاد.

- پارتیشن مذکور می‌بایست به صورت NTFS فرمت گردد.

- کلمات رمز.

- جزئیات.

- رمز گذاری LM hash در شبکه مشاهده گردید.

- پیش‌نهاد.

- از نصب واستفاده از NTLM۲ در شبکه وتنظیمات مربوط به گروه‌ها اطمینان حاصل گردد.

- Patchها.

- جزئیات.

- چندین Patch ها از آخرین Patch های مایکرو سافت موجود نیستند.

- پیش‌نهاد.

- استفاده از Policy Patching و تست اولیه آن بر روی یک LAN آزمایشی و تست سرور WSUS واطمینان از بروز رسانی آن.

- آنتی ویروس.

- جزئیات.

- چندین ایستگاه کاری با آنتی ویروس بروز رسانی نشده یافت شد.

- پیش‌نهاد.

- نصب آنتی ویروس تحت سرور و تست بروز رسانی آن بر روی کلیه ایستگاه‌های کاری.

- Trust

- جزئیات.

- کاربران یک دامین قادر به دسترسی به منابع درختی نیستند.

- پیش‌نهاد.

- کلیه Trust های مستقیم وغیر مستقیم مورد بررسی قرار گرفته واز وجود کلیه Trustهای مرتبط ومناسب اطمینان حاصل گردد.

- امنیت سرور وب.

- امنیت فایل سیستم‌ها.

- جزئیات.

- دسترسی غیر صحیح بر روی شاخه www وجود دارد.

- پیش‌نهاد.

- تدابیر محکم‌تری بر روی شاخه فوق در نظر گرفته شود یا گروه‌ها وکاربران مختلفی که به این شاخه دسترسی دارند حذف گردند.

- کلمات رمز.

- جزئیات.

- فضاهایی که باید در سایت وب مورد دسترسی قرار نگیرند دارای کلمات رمز نمی‌باشند.

- پیش‌نهاد.

- فضاهای مذکور شناسایی و با کلمه رمز مورد محافظت قرار گیرند.

- ابزار قفل.

- جزئیات.

- ابزار قفل IIS بر روی سرور وب نصب نمی‌باشد.

- پیش‌نهاد.

- ابزار فوق بر روی یک سرور آزمایشی نصب و پس از اطمینان از سازگاری آن با برنامه‌های کاربردی بر روی سرور وب نصب گردد.

- امنیت سرور پایگاه.

- مانند موارد قبل.

- امنیت برنامه‌های عمومی.

- مانند موارد قبل.

- امنیت تجاری.

- موارد مورد بررسی.

- تهیه نسخ پشتیبانی.

- دسترسی‌ها.

- تامین کاربران.

- تامین نرم افزاری.

- تامین سخت افزاری.

- تامین مستندات.

- سایر موارد.

- بررسی سر ریز بافرها.

- بررسی سرویس‌ها و خروجی‌های ناخواسته آن‌ها

- بررسی مشکلات ناشی از پیمایش دایر کتوری‌های سیستمی.

-بررسی سازمان به روش مهندسی اجتماعی.

- بررسی دیاگرام شبکه.

- روش‌های حمله در آزمون نفوذ پذیری.

- روش شناسایی[۱].

- در این روش آزمون گیرنده به جمع آوری تمامی اطلاعـات شبکه در حد امکان می‌پـردازد.

روش شناسایی می‌تواند به دو صورت حمله فعال و غیر فعال مورد استفاده قرار گیرد که روش حمله غیر فعال از آن جا که به طور نامحسوس عمل می‌کند مناسب‌تر به نظر می‌رسد. استفاده از مهندسی اجتماعی یکی از راه‌های روش حمله فـعال است که موجب ثبت احتمالـی حمله در سیستم‌های دارای log می‌گردد.

---

۱ Reconnaissance

- روش پویش.

- در این روش آزمون گیرنده از ابزارهای Fingerprint سیستم عامل به صورت متعدد بهره گرفته وبه کاوش در خصوص تعداد وانواع سرورها وسرویس‌های اجرایی در شبکه می‌پردازد.

- روش اسکن.

- در این روش و با استفاده از اسکنرهای نفوذ پذیری سرورهای یافت شده مورد بررسی قرار گرفته و از نتایج این بررسی‌ها، نقاط نفوذ پذیر سرور یا شبکه مورد نظر مشخص می‌گردد.

- دسترسی یافتن.

- در این روش با استفاده از نقاط ضعف برنامه‌های کاربردی، سرویس‌ها یا سیستم‌های عامل می‌توان به آن‌ها دسترسی پیدا نمود. به عنوان مثال می‌توان با استفاده از exploit engine هایی از قبیل "Metasploit" یا ابزارهای password cracking اقدام به این حمله نمود.

- حفظ دسترسی‌ها.

- در این روش با نصب یک backdoor در شبکه مورد نظر امکان بازگشت آزمون گیرنده ودسترسی همیشگی وی به منابع مورد نظر وجود خواهد داشت. این کار با یکی از روش‌های back door Trojan ، rootkit یا تعریف یک کار بر جعلی امکان پذیر می‌باشد.

- پاک کردن شواهد.

- این روش عبارتست از پاک نمودن logهای سیستمی که رد پای حمله کننده را نشان می‌دهد. در صورت دسترسی جهت حذف یا تغییر این log ها امکان رد یابی حمله کننده بسیار پایین است که در این خصوص باید بسیار دقت گردد.

بدیهی است موارد دیگری نیز به فراخور نوع شبکه و اطلاعات هر سازمان می‌توانند در آزمون نفوذ پذیری مربوطه لحاظ گردند.

۶-۷- جمع بندی:

امروزه آزمون نفوذپذیری چه برای سازمان‌هایی که از تجهیزات امن استفاده می‌کنند و چه برای آن دسته از سازمان‌هایی که در استقرار تجهیزات نرم افزاری، سخت افزاری و شبکه‌ای قوی، نو پا محسوب می‌گردند، به عنوان یک روش نفوذی قانونمند در جهت شناسایی آسیب‌پذیری‌های سیستم کاربرد وسیعی یافته است. به طور کلی مقدمات استفاده از این نوع آزمون عبارتند از:

- شناخت روش‌های اجرایی.
- شناخت و بستر سازی جهت استفاده از متدلوژی‌های استاندارد.
- تدوین قوانین استفاده از آزمون در سازمان.
- تهیه فرمت‌های مورد استفاده در گزارشات عمل‌کرد.
- تجهیز و به روز رسانی نرم افزار، سخت افزار و شبکه.

۶-۸- کار عملی این فصل.

تهیه یک گزارش از تست انجام شده در محیط تحت نظر استاد راهنما.

۷

فصل هفتم - چک لیست‌ها

فصل هفتم - چک لیست چیست؟

چک لیست روشی برای کمک به انجام ممیزی است که گر چه استفاده از آن اجباری نیست ولی در مجموع فواید زیادی دارد. در واقع چک لیست سئوالاتی از پیش طراحی شده برای انجام ممیزی است که به وسیله این سئوالات مسئول ممیزی روند ممیزی را به سمت جلو می‌برد.

کمک به حافظه و یادآوری به مسئول ممیزی، اطمینان از این که تمامی موارد پوشش داده می‌شود، اجرای آسان‌تر ممیزی، کمک در هنگام نوشتن گزارش ممیزی، یک‌نواختی در اطلاعات جمع آوری شده توسط گروه از مسئولان ممیزی، نظام بندی در شواهد عینی ممیزی، امکان ثبت مشاهدات و شواهد عینی روبروی هر سئوال و کمک به مستند سازی مصاحبه و جلوگیری از انحراف از اصل موضوع از جمله مزایای استفاده از چک لیست است.

چک لیست می‌تواند از نوع کلان یا خرد تهیه شود .

چک لیست کلان معمولاً با آیا آغاز شده و خواسته‌های کلی استاندارد را مورد بررسی قرار می‌دهد.

چک لیست خرد معمولاً جزئیات بیش‌تری را برای هر یک از سئوالات کلان فراهم می‌نماید و چگونگی کار را با کلماتی از قبیل چه چیزی، چه کسی، چه موقع و با چه وسیله‌ای مورد پرسش قرار می‌دهد.

در این بخش نمونه‌هایی از چک لیست‌های مورد نیاز در امر ممیزی فن‌آوری اطلاعات که می‌توان از تلفیق آن‌ها چک لیست‌های مورد نیاز را تهیه نمود آورده شده است. ممیزان قادر خواهند بود با استفاده از چک لیست‌های پیش‌نهادی، چک لیست‌های مورد نیاز خود را تهیه نمایند. ذکر جداول چک لیست‌ها به منزله تکمیل بودن آن‌ها نمی‌باشد و صرفاً به عنوان الگو و راهنمایی برای تهیه لیست‌های مورد نیاز آورده شده است.

چک لیست شماره یک: نقاط ضعف و آسیب‌پذیری حوزه IIS ۴ و IIS ۵

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه IIS ۴ و IIS ۵	بله	خیر
۱	آیا خاصیت سرویس ایستگاه کاری سرور را غیرفعال کرده‌اید؟		
۲	آیا خاصیت سیستم فایل توزیع شده سرور را غیرفعال کرده‌اید؟		
۳	آیا خاصیت سیستم‌های مسیریابی لینک توزیع شده کاربر را غیرفعال کرده‌اید ؟		
۴	آیا خاصیت عامل مونیتور شبکه سرور را غیرفعال کرده‌اید؟		
۵	آیا خاصیت مرورگر رایانه سرور را غیرفعال کرده‌اید؟		
۶	آیا سرویس رجیستری راه دور سرور را غیرفعال کرده‌اید؟		
۷	آیا سرویس مدیریت دیسک منطقی سرور را غیرفعال کرده‌اید؟		
۸	آیا سرویس ورود به سیستم با استفاده از گواهی نامه سرور را غیر فعال کرده‌اید؟		
۹	آیا عامل سیاست امنیت IP سرور را غیرفعال کرده‌اید؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه IIS ۴ و IIS ۵	بله	خیر
۱۰	آیا قابلیت اجرا به عنوان یک سرویس سرور را غیرفعال کرده‌اید؟		
۱۱	آیا قابلیت برنامه ریزی فعالیت‌های سرور را غیرفعال کرده‌اید؟		
۱۲	آیا قابلیت ذخیره سازی بر روی حافظه‌های جدا شدنی را غیر فعال کرده‌اید؟		
۱۳	آیا قابلیت زمان دهی ویندوز را غیرفعال کرده‌اید؟		
۱۴	آیا قابلیت سرویس تلفنی سرور را غیر فعال کرده‌اید؟		
۱۵	آیا قابلیت مدیریت سرور را غیرفعال کرده‌اید؟		
۱۶	آیا قابلیت نصب از طریق ویندوز سرور را غیرفعال کرده‌اید؟		
۱۷	آیا کلاینتWINS سرور را غیرفعال کرده‌اید؟		

چک لیست شماره دو: نقاط ضعف و آسیب‌پذیری حوزه اجرا

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه اجرا	بله	خیر
۱	آیا بازرسی‌های دوره‌ای برای کسب اطمینان از رعایت خط‌مشی‌های مربوط به نرم‌افزارها رعایت می‌شود؟		
۲	آیا کارکنان مسئول نقض خط مشی‌ها و حقوق کپی‌رایت می‌باشند؟		
۳	آیا کلیه مقررات مربوط به موافقت با لیسانس نرم‌افزارها اجرا می‌شوند؟		

چک لیست شماره سه: نقاط ضعف و آسیب‌پذیری حوزه ارزیابی پیشرفت و نگهداری سوابق

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه ارزیابی پیشرفت و نگهداری سوابق	بله	خیر
۱	آیا تست دوره‌ای بر روی کنترل‌ها و حفاظ‌های فیزیکی انجام می‌شود؟		
۲	آیا محیط امنیتی بر اساس روند مبتنی بر بهبود، نظارت و پایش می‌شود؟		
۳	آیا مستند سازی و خط‌مشی امنیتی بر اساس روند مبتنی بر بهبود، به روز می‌شود؟		
۴	آیا وسایلی برای نگهداری وضعیت جاری مرتبط با راه حل‌ها و الزامات امنیت فیزیکی وجود دارد؟		

چک لیست شماره چهار: نقاط ضعف و آسیب‌پذیری حوزه آزمایش

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه آزمایش	بله	خیر
۱	آیا امنیت دیواره آتش پس از اعمال کردن هر محافظ تکنولوژیکی جدید تست می‌شود؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه آزمایش	بله	خیر
۲	آیا امنیت دیواره آتش پس از هر تغییر در پروفایل تهدید سازمان تست می‌شود؟		
۳	آیا به طور مرتب دیواره آتش جهت تعیین آسیب‌پذیری‌های شناخته شده تست می‌شود؟		
۴	آیا تمامی قوانین دیواره آتش اسکن و آزمایش می‌شود تا معلوم شود که چه بسته‌هایی وارد و خارج می‌شوند؟		
۵	آیا سرویس‌های طرف ثالث (یعنی نرم‌افزارهای فیلترینگ محتوی یا اسکن کننده‌های پست الکترونیک) که از میان دیواره آتش رد می‌شوند تست می‌شوند؟		

چک لیست شماره پنج: نقاط ضعف و آسیب‌پذیری حوزه اقدامات پیش‌گیرانه

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه اقدامات پیش‌گیرانه	بله	خیر
۱	آیا تفکیک وظایف وجود دارد؟		
۲	آیا سطح بررسی‌های سوابق کارکنان قابل قبول است؟		
۳	آیا نظارت بر عمل‌کرد کارکنان یک فرآیند مداوم است؟		
۴	قبل از استخدام کارکنان سازمان، سوابق مربوط به آن‌ها مورد بررسی و		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه اقدامات پیش‌گیرانه	بله	خیر
	تحقیق قرار می‌گیرد؟		

چک لیست شماره شش: نقاط ضعف و آسیب‌پذیری حوزه اکتیو دایرکتوری WIN ۲ K

ردیف	نقاط ضعف و آسیب‌پذیری حوزه اکتیو دایرکتوری WIN ۲ K	بله	خیر
۱	اگر برخی از کاربران از نسخه‌های پایین‌تر ویندوز استفاده می‌کنند، اطمینان حاصل نمایید آیا سطح احزار هویت مدیر LAN حداقل به اندازه" NTLMv۲ ۲" قرارداده شده است یا خیر؟		
۲	اگر همه‌ی کاربران از ویندوز ۲۰۰۰ استفاده می‌کنند آیا کنترل کننده‌های حوزه طوری تنظیم شده‌اند که هر نوع دیگر روند احراز هویت را نپذیرند ؟		
۳	آیا از استفاده غیر مجاز از فلاپی درایو بر روی سرورها جلوگیری به عمل آمده است؟		
۴	آیا بازبینی از اعضای گروه مدیریت شبکه انجام شده است تا اطمینان حاصل شود تغییرات غیرمجاز در طرح اکتیو دایرکتوری انجام نشده است؟		
۵	آیا بازبینی واحدهای سازمانی و خط‌مشی‌های ممیزی انجام شده است؟		
۶	آیا پروتکل مدیریت شبکه ساده در کنترل کننده‌های حوزه نصب نشده		

ردیف	نقاط ضعف و آسیب‌پذیری حوزه اکتیو دایرکتوری WIN ۲ K	بله	خیر
	است؟		
۷	آیا خط‌مشی برنامه‌های کاربردی بازبینی شده است؟		
۸	آیا خط‌مشی تعیین محل (موقعیت) بازبینی شده است؟		
۹	آیا خط‌مشی طبقه‌بندی یا دسته بندی کاربران بازبینی شده است؟		
۱۰	آیا زیر سیستم‌های ۲/os و posix از سیستم‌هایی که به طور مستقیم به اینترنت وصل می‌شوند، حذف شده‌اند؟		
۱۱	آیا سرویس‌های اطلاعاتی اینترنت ۵. ۰ (IIS۵) از سرورهای win ۲k غیر وب حذف شده است. در صورتی که در همه‌ی سرورهای win ۲k به صورت پیش‌فرض فعال شده است؟		
۱۲	آیا قابلیت اپراتور سرور برای زمانبندی کارها غیرفعال شده است؟		
۱۳	آیا قابلیت خاموش کردن سیستم بدون نیاز به ورود به سیستم غیرفعال شده است؟		
۱۴	آیا گزینه " ارسال کلمه عبور غیر رمزی برای اتصال به سرورهای SMB طرف دیگر" غیرفعال شده است؟		
۱۵	آیا گزینه " به صورت دیجیتالی داده‌های کانال امن را امضا نمایید" فعال است ؟		
۱۶	آیا گزینه " به صورت دیجیتالی داده‌های کانال امن را رمزنگاری نمایید" فعال است؟		

ردیف	نقاط ضعف و آسیب‌پذیری حوزه اکتیو دایرکتوری WIN ۲ K	بله	خیر
۱۷	آیا گزینه " تقویت مجوزهای پیش فرض دسترسی به موضوعات سیستم عمومی " فعال است؟ و برای حساب‌های غیر از مدیر شبکه در حالت دسترسی فقط خواندنی قرار داده شده است؟		
۱۸	آیا گزینه " کنسول بازیافت: اجازه دادن ورود اتوماتیک به سیستم برای مدیرشبکه" غیرفعال شده است؟		
۱۹	آیا گزینه "باز داشتن سیستم از نگهداری کلمه عبور حساب رایانه" برای رایانه‌ها و سرورهایی که عضوی از حوزه هستند غیرفعال شده‌اند؟		
۲۰	آیا گزینه "صفحه فایل حافظه جانبی را هنگامی که سیستم خاموش شده پاک کنید" فعال شده است؟		
۲۱	آیا گزینه "کنسول بازیافت: اجازه دادن کپی فلاپی و دسترسی به کلیه درایورها و پوشه‌ها"غیرفعال شده است؟		
۲۲	آیا گزینه بازداشتن کاربران از نصب درایورهای چاپ فعال شده است؟		
۲۳	آیا گزینه" عدم نصب درایور تایید نشده " به طور مناسب تنظیم شده است؟		
۲۴	آیا گزینه‌ی "خاموش کردن سریع سیستم در صورتی که ثبت ممیزی‌های امنیتی ممکن نباشد" فعال شده است؟		
۲۵	آیا گزینه‌ی "نشان دادن پیغام برای کاربرانی که سعی دارند وارد سیستم شوند" مورد استفاده قرار می‌گیرد؟		
۲۶	آیا مجوز بیرون کشیدن رسانه‌های NTFS به طور مناسبی به گروه‌های مربوطه مثلا مدیران سیستم، اپراتورهای پشتیبان‌گیری و غیره واگذار		

ردیف	نقاط ضعف و آسیب‌پذیری حوزه اکتیو دایرکتوری WIN ۲ K	بله	خیر
	شده است؟		
۲۷	آیا محدودیت‌های اضافی برای ارتباطات بی‌نام به صورت پیش فرض بر روی حالت خیر قرارداده شده است؟		
۲۸	آیا مدت زمان تنظیم شده برای خروج اتوماتیک کاربران از سیستم هنگامی که زمان ورود به سیستم آن‌ها به پایان رسیده باشد، مناسب است؟		
۲۹	آیا مقدار زمان وقفه مورد نیاز قبل از قطع جلسه مناسب تنظیم شده است؟		
۳۰	آیا نرم‌افزاری برای پشتیبانی داده‌های مربوط به رجیستری و امنیت که دیسکت های تعمیر اضطراری از آن‌ها پشتیبانی نمی‌کنند، خریداری شده است ؟		
۳۱	آیا نقشه کلی امتیازات کاربران برای کلیه کاربران، گروه‌ها و واحدهای سازمانی ارائه شده است؟		
۳۲	آیا نقشه کلی امتیازات کاربران برای کلیه کاربران، گروه‌ها و واحدهای سازمانی به صورت دوره‌ای و منظم به روز شده است؟		

چک لیست شماره هفت: نقاط ضعف و آسیب‌پذیری حوزه امحا

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امحا	بله	خیر

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امحا	بله	خیر
۱	آیا جدول زمانی برای استحکام داده‌ها/ اسناد امن و نیز امحا آن‌ها دارید؟		
۲	آیا خروجی اسنادی که برای امحا در نظر گرفته شده‌اند به‌قدر کافی بزرگ می‌باشد که بهره‌بری از خدمات امحا را توجیه کند؟		
۳	آیا سازمان از اسنادی که چرخه حیات آن‌ها به‌پایان رسیده است خلاص می‌شود؟		
۴	آیا سازمان می‌داند که طبق قانون بایستی برخی از اسناد به صورت امن امحا شوند؟		
۵	آیا فهرستی از اسنادی که باید امحا شوند دارید؟		
۶	آیا نگهداری اسناد در خانه قابل اجرا است؟		
۷	آیا همه کارکنان از آن‌چه که اطلاعات شخصی مشتری محسوب می‌شود و پس از گذشت چرخه حیات آن‌ها بایستی نابود شوند آگاهی دارند؟		
۸	آیا همه کارکنان از این که چگونه و کجا بایستی اطلاعات شخصی مشتری که قرار است نابود شوند نگهداری شوند، آگاهی دارند ؟		

چک لیست شماره هشت: نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور IIS ویندوز / سرورهای وب XP

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور IIS ویندوز / سرورهای وب XP	بله	خیر
۱	آیا آسیب پذیری دسترسی به پوسته ODBC سرور را غیرفعال کرده‌اید؟		
۲	آیا انشعاب‌های Front Page سرور را برداشته‌اید؟		
۳	آیا به طور مرتب مرورگر رخداد به منظور چک کردن اقدام‌های غیر مجاز صورت گرفته برای دسترسی به فایل‌ها و فولدرهای ممنوعه بررسی می‌شود؟		
۴	آیا به‌حساب کاربری پیش فرض با نام کامپیوترهای پیش فرض حداقل میزان امتیاز داده شده است؟		
۵	آیا خاصیت ایندکس کردن مراجع بر روی کلیه وب‌سایت‌ها را غیر فعال کرده‌اید؟		
۶	آیا خاصیت در نظر گرفتن حساب‌ها و فایل‌های مشترک SAM (توسط کاربران ناشناس) را غیرفعال کرده‌اید؟		
۷	آیا خاصیت سرویس‌های داده راه دور سرور را غیرفعال کرده‌اید؟		
۸	آیا خاصیت مرورکردن دایرکتوری بر روی کلیه وب‌سایت‌ها و دایرکتوری‌های مجازی را غیر فعال کرده‌اید ؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور IIS ویندوز / سرورهای وب XP	بله	خیر
۹	آیا دایرکتوری‌های: Admin Scripts، IIS Samples،و 'Scripts' پاک شده‌اند؟		
۱۰	آیا سایت وب پیش فرض سرور را غیر فعال نموده و تمام فایل‌های آن‌را حذف نموده‌اید؟		
۱۱	آیا سایرشاخه‌ها وفایل‌های حساس روی وب سرور نیز به صورت غیر فعال بوده و نظارت مناسبی بر روی آن‌ها صورت می‌گیرد؟		
۱۲	آیا سرویس Net Logon سرور را غیر فعال نموده‌اید؟		
۱۳	آیا سرویس Locator RPC سرور را غیر فعال کرده‌اید؟		
۱۴	آیا سرویس ایندکس سرور در حالت غیرفعال قرار دارد؟		
۱۵	آیا سرویس درایور مونیتور شبکه سرور در حالت غیرفعال قرار دارد؟		
۱۶	آیا سرویس مسنجر سرور را غیر فعال نموده‌اید؟		
۱۷	آیا سرویسClip Book سرور در حالت غیرفعال قرار دارد؟		
۱۸	آیا سرویسSpooler سرور را غیر فعال نموده‌اید؟		
۱۹	آیا سرویس‌های IP/TCP ساده سرور در حالت غیرفعال قرار دارد؟		
۲۰	آیا فایل‌های ذیل را به صورت غیرفعال وتحت ممیزی‌های امنیتی قرار داده‌اید؟ ftp . Exe،t ftp . exe، cmd، command. Com،exe tel net. exe		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور IIS ویندوز / سرورهای وب XP	بله	خیر
۲۱	آیا کلیه برنامه‌های مرتبط کننده بدون استفاده را از وب سرور برداشته‌اید؟		
۲۲	آیا کلیه دایرکتورهای باقی‌مانده Front Page سرور را برداشته‌اید؟		
۲۳	آیا کلاینتDHCP سرور را غیر فعال نموده‌اید؟		
۲۴	آیا همه وب‌سایت‌ها را در مورد این که مجوز 'نوشتن' را فعال نکرده باشند چک کرده‌اید؟		

چک لیست شماره نهم: نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور SQLمایکرو سافت

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور SQLمایکرو سافت	بله	خیر
۱	آیا ابزارهای بهره برداری از نقاط ضعف امنیتی و اسکنرهای امنیتی در یک محیط شبیه‌سازی به‌منظور شناسایی دور زدن امتیازات دسترسی یا آسیب‌پذیری‌های دیگر مورد استفاده قرار گرفته‌اند؟		
۲	آیا به‌منظور کسب اطمینان از این که دسترسی به کسانی که کم‌تر مورد وثوق می‌باشند داده نشده است رونده‌ای ذخیره شده مورد تجدید نظر قرار گرفته‌اند؟		
۳	آیا روندهایی موجود است که از ایجاد یک جدول موقتی در Tempdb جلوگیری نماید زیرا که ممکن است موجب حمله عدم سرویس دهی با		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور SQLمایکرو سافت	بله	خیر
	استفاده اتصالات گم نام شوند؟		
۴	آیا همه مکان‌هایی‌که فایل گذرواژه در آن‌ها ذخیره شده شناسایی شده و امنیت دسترسی مناسب برای آن‌ها فراهم شده است؟		

چک لیست شماره دهم: نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور اوراکل

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور اوراکل	بله	خیر
۱	آیا از نشتی‌های داده‌های سرویس فراخوان با استفاده از وصله‌های امنیتی مناسب ارسال شده توسط سرور اوراکل جلوگیری شده است؟		
۲	آیا امنیت سرویس فراخوان از نظر روند احزار هویت مورد بررسی قرار گرفته است؟		
۳	آیا بلوکی برای مجبور کردن به فرستادن گذرواژه از طریق سرویس فراخوان به‌کارگرفته شده است؟		
۴	آیا مشکل سرریز شدن بافر به‌وسیله اجرای رونده‌ای امنیتی شرح داده شده در وب سایت اوراکل برطرف شده است؟		

چک لیست شماره یازدهم: نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور وب

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور وب	بله	خیر
۱	آیا اقدامات امنیتی مناسب جهت دیواره‌های آتش میان وب سرور و سرور(های) سازمان وروترها انجام شده است؟		
۲	آیا خط‌مشی‌ای درباره مجوز ندادن به بارگذار / آپ‌لودکردن فایل‌های حساس به / از وب‌سرورها در دست دارید؟		
۳	آیا زیرشاخه‌هایی که از خارج شبکه قادر به دریافت فایل هستند به‌عنوان فقط دسترسی "نوشتن" فهرست می‌شوند؟		
۴	آیا زیرشاخه‌هایی که به خارج شبکه قادر به ارسال فایل هستند به‌عنوان فقط دسترسی خواندن فهرست می‌شوند؟		
۵	آیا فایل‌های مناسب در زیرشاخه‌های روی وب‌سرور به طور مرتب به‌منظور مجوز دادن / ممنوع کردن دسترسی جابه‌جا می‌شوند؟		
۶	آیا کلیه ابزارهای کاربردی و توسعه‌ای از وب سرورها برداشته شده‌اند؟		
۷	آیا کلیه سرویس‌های غیرلازم ازقبیل FTP یا SNMP غیر فعال شده‌اند؟		
۸	آیا مجوزدهی URL به‌منظور محدودسازی دسترسی به وب سرور مورد بررسی قرار گرفته است؟		
۹	آیا میان وب سرور و سرور(های)اصلی سازمان یک دیواره آتش قرار دارد؟		
۱۰	آیا وب سرور در مکانی قرار دارد که به لحاظ فیزیکی مجزا شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت سرور وب	بله	خیر
۱۱	آیا وب‌سرور فقط یک سرور یک منظوره است و برای انواع دیگر سرور همچون سرور نامه‌های الکترونیکی به‌کار نمی‌رود؟		
۱۲	آیا یک گروه محلی برای کاربران وب ایجاد شده است که مشتمل بر کاربران خیلی خاص باشد؟		
۱۳	برای هر کاربری وبی که با اطلاعات حساس سر و کار داشته باشد، آیا از SSL جهت برقراری ارتباط میان مشتری‌ها و سرور وب استفاده می‌شود؟		
۱۴	به‌هنگام نصب نرم‌افزار بر روی وب سرور آیا دایرکتوری پیش‌فرض نصب برگزیده نمی‌شود؟		

چک لیست شماره دوازدهم: نقاط ضعف و آسیب‌پذیری حوزه امنیت فیزیکی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت فیزیکی	بله	خیر
۱	اگر محل، در یک ساختمان چند طبقه واقع شده آیا محتوای آن‌چه که در بالای امکانات و تجهیزات قرار دارد، به منظور ارزیابی ریسک خسارت احتمالی ناشی از خرابی لوله‌کشی، امکانات و تجهیزات یا ساکنان طبقه فوقانی، مورد شناسایی قرار گرفته است؟		
۲	آیا اتاق تجهیزات صندوق صوتی سازمان به وسیله دیوارها و درهای ضد آتش (ضد حریق) محافظت می‌شود؟		
۳	آیا اتاق تجهیزات صندوق صوتی سازمان در برابر افزایش حرارت (حرارت بسیار بالا) و رطوبت زیاد حفاظت شده است؟		
۴	آیا اتاق صندوق صوتی سازمان دارای یک واحد اطفا حریق است؟		
۵	آیا از کلیدها / کارت‌های هوشمند برای ورود به اتاق صندوق صوتی سازمان استفاده می‌شود؟		
۶	آیا امکانات و تجهیزات مهم مأموریتی در یک ناحیه قرار داده شده تا هزینه حفاظت از یک محل تقلیل یابد؟		
۷	آیا ایستگاه‌های مدیریتی اصلی که قادرند حقوق دسترسی دیگر رایانه‌ها را تغییر دهند در محل‌های امن قرار داده شده‌اند؟		
۸	آیا خطوط اصلی تلفن که وارد ساختمان شده ایمن شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت فیزیکی	بله	خیر
۹	آیا دسترسی به دیواره آتش محدود به پرسنل مناسب می‌باشد؟		
۱۰	آیا دسترسی به صندوق صوتی سازمان صرفا به کارمندان خاص و مناسب محدود شده است؟		
۱۱	آیا دیواره آتش به یک پریز USP یا برق اضطراری دیگر وصل می‌باشد؟		
۱۲	آیا دیواره آتش دارای یک محافظ افزایش برق می‌باشد؟		
۱۳	آیا سخت‌افزار دیواره آتش در مقابل حرارت و رطوبت خیلی زیاد به طور مناسب محافظت می‌شود؟		
۱۴	آیا سخت‌افزار/نرم‌افزار دیواره آتش در درون اتاق مرکز داده / سروردادە قرار دارند؟		
۱۵	آیا صندوق صوتی سازمان دارای یک UPS یا منبع تغذیه جای‌گزین است؟		
۱۶	آیا صندوق صوتی سازمان دارای یک محافظ نوسانات جریان برق می‌باشد؟		
۱۷	آیا کلیه امکانات و تجهیزات در یک اتاق امن قفل شده که دسترسی به آن محدود به افراد مجاز باشد نصب شده‌اند؟		
۱۸	آیا کلیه خطوطی که به سخت‌افزار منتهی می‌شوند از لحاظ فیزیکی امن می‌باشند؟		
۱۹	آیا کلیه سخت‌افزارها و نرم‌افزارهای دیواره آتش دارای قفل و کلید می‌باشند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت فیزیکی	بله	خیر
۲۰	آیا کلیه سخت‌افزارهای مربوط به دیواره آتش به لحاظ فیزیکی امن می‌باشند؟		
۲۱	آیا کلیه کدهای دسترسی به اتاق دیواره آتش از دسترس افراد غیرمجاز خارج است؟		
۲۲	آیا کلیه سیم‌ها و کابل‌هایی که به اتاق تجهیزات صندوق صوتی سازمان وارد شده و از آن خارج می‌شوند (ورودی و خروجی) از بین یک ماده نسوز یا دیرسوز عبور کرده‌اند؟		
۲۳	آیا محل امکانات وتجهیزات در منطقه‌ای واقع شده است که میزان جرم و جنایت پائین است و آیا دور از فرودگاه یا ساختمان‌هایی که در معرض تهدیدات امنیتی قرار دارند می‌باشد؟		
۲۴	آیا محل و امکانات و تأسیسات بر اساس اصول حفاظت از امکانات و تجهیزات پردازشگر الکترونیکی /داده‌ها در برابر آتش سوزی ساخته شده است؟		
۲۵	آیا مرکز داده‌ها دور از مراکزی با ترافیک سنگین می‌باشد؟		
۲۶	آیا مرکز داده‌ها عاری از هرگونه تابلوی علامت و اعلانات است؟		
۲۷	آیا منابع IT در ناحیه‌ای قرار داده شده که فقط رفت و آمده‌ای مجاز در آن نواحی صورت می‌گیرد		
۲۸	آیا همه بازدیدکنندگان، ارباب رجوع، پیمانکاران و سایر قشرها تا زمانی که در ناحیه صندوق صوتی سازمان هستند همراهی می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه امنیت فیزیکی	بله	خیر
۲۹	آیا همه پنل‌های تلفن‌ها به طور فیزیکی ایمن شده‌اند؟		
۳۰	آیا همه تجهیزات صندوق صوتی سازمان قفل و بست دارند؟		
۳۱	آیا همه کانال‌های کابل‌های داده به همراه خطوط تلفن داخلشان ایمن شده‌اند؟		

چک لیست شماره سیزدهم: نقاط ضعف و آسیب‌پذیری حوزه آموزش و تربیت

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه آموزش و تربیت	بله	خیر
۱	آیا ابزاهای پیگیری و ثبت وقایع به صورت دوره‌ای آزمایش می‌شوند؟		
۲	آیا اخذ گواهی‌نامه مجدد بر اساس سطح ریسک و اهمیت خسارت وارده بالقوه مورد نیاز است؟		
۳	آیا آموزش در چند مرحله ارائه شده است؟ (مثلا آموزش امنیتی اضافی یا پیشرفته برای آن‌هایی که مرحله مقدماتی را گذرانده‌اند)		
۴	آیا آموزش کافی در زمینه دیواره آتش برای کارکنان IT و امنیت تدارک دیده‌اید؟		
۵	آیا آموزش کافی در رابطه با صندوق صوتی سازمان و ارتباطات از راه دور وجود دارد که به کاربران نهایی ارائه شود؟		
۶	آیا آموزش‌ها بر اساس نیازمندی‌های آگاه سازی امنیتی کاربران، تهیه و		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه آموزش و تربیت	بله	خیر
	تدوین شده است؟		
۷	آیا برای پیمانکاران نیز آموزش موارد امنیتی در نظر گرفته شده است؟		
۸	آیا برخی از کارمندان برای راه‌اندازی یا کار با بخش‌هایی از سیستم‌های رایانه‌ی سازمان، باید گواهی‌نامه یا اعتبارنامه لازم را داشته باشند؟		
۹	آیا بودجه مربوط به آموزش کافی و مناسب است؟		
۱۰	آیا ترکیب بندی و ذات دستور العمل های آموزشی انتخاب شده بر اساس نیازمندی‌های ریسک می‌باشد؟		
۱۱	آیا تمرینات اطفا حریق به‌طور آزمایشی برای کسب آمادگی در مواقعی که حادثه‌ای روی می‌دهد انجام می‌شوند؟		
۱۲	آیا تنظیم زمان جلسات آموزشی و مراعات فواصل جلسات مورد توجه و رسیدگی قرار گرفته است؟		
۱۳	آیا جلسات آگاهی دهنده در رابطه با صندوق صوتی سازمان حداقل به صورت سالیانه برگزار می‌شود؟		
۱۴	آیا جلسات آموزشی و اطلاع‌رسانی رسمی به منظور آشنایی کارمندان جدید ترتیب یافته است؟		
۱۵	آیا در روند آموزشی، کارمندان از چگونگی درخواست کمک در هنگام پیش آمدن مشکلات مرتبط با موارد امنیتی آگاه می‌شوند؟		
۱۶	آیا دوره‌های آموزش مجدد و مرور مفاهیم قبلی ارائه می‌شود و امتحان‌های امنیتی دوره‌ای برگزار می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه آموزش و تربیت	بله	خیر
۱۷	آیا روند آموزش به عنوان یک فرایند اجباری برای کارمندان می‌باشد؟		
۱۸	آیا روندی به منظور اطمینان از درک موارد آموخته شده توسط کارمندان ایجادشده است؟		
۱۹	آیا صندوق صوتی سازمان برای شناخت شکاف‌ها یا آسیب‌پذیری‌ها به طور منظم مورد آزمایش قرار می‌گیرد؟		
۲۰	آیا طرح‌های محدود شده یا ممنوعه به طور منظم آزمایش می‌شوند؟		
۲۱	آیا طرح‌هایی برای ارائه برنامه‌های آموزشی دارای گواهی‌نامه درباره دیواره آتش به کارکنان صلاحیت‌دار IT وجود دارد؟		
۲۲	آیا فرد شایسته و آموزش یافته‌ای برای سروکار داشتن با مباحث و موضوعات مربوط به صندوق صوتی سازمان در دسترس می‌باشد یا خیر؟		
۲۳	آیا فروشنده آموزش‌های امنیتی خاص مربوط به صندوق صوتی سازمان را تهیه کرده است؟		
۲۴	آیا فروشنده آموزش‌های امنیتی ویژه دیواره آتش ارائه می‌نماید؟		
۲۵	آیا کاربران آگاهی کامل از رابطه میان دیواره آتش و پردازش‌های داده دارند؟		
۲۶	آیا کاربران نهایی قدرشناسی و درکی از دیواره آتش به‌عنوان جنبه اساسی امنیت داده و شبکه نشان می‌دهند؟		
۲۷	آیا کارکنان متوجه اقدامات، نحوه عمل و رونده‌ای دیواره آتش می‌باشند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه آموزش و تربیت	بله	خیر
۲۸	آیا کاربران جدید قبل از این که بتوانند به سیستم دسترسی داشته باشند آموزش مناسبی دیده‌اند؟		
۲۹	آیا گواهی نامه و مدارک به صورت دوره‌ای بازبینی می‌شود؟		
۳۰	آیا منبع تغذیه جای‌گزین / UPS به صورت دوره‌ای آزمایش می‌شود؟		
۳۱	آیا مهم‌ترین نواحی در آموزش پوشش داده شده‌اند؟		
۳۲	آیا موارد آموزشی به صورت کتابچه در اختیار کارمندان، گذاشته می‌شود؟		
۳۳	آیا موضوعات ویژه خاص پوشش داده شده‌اند؟		
۳۴	آیا موقعیت‌های متفاوتی مثل امنیت لب‌تاپ در مسافرت نیز پوشش داده شده است؟		
۳۵	آیا همه کارمندان آموزش امنیت را به‌طور مناسب فرا گرفته‌اند؟		
۳۶	آیا وقفه‌های موجود در آموزش شناسایی شده و مد نظر قرار دارند؟		
۳۷	آیا یک فرد آموزش دیده با صلاحیت برای حل مسائل مربوط به دیواره آتش در اختیار دارید؟		
۳۸	آیا یک طرح آموزشی امنیت وجود دارد؟		

چک لیست شماره چهاردهم: نقاط ضعف و آسیب‌پذیری حوزه انتخاب سرویس دهنده

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه انتخاب سرویس دهنده	بله	خیر
۱	آیا ارزیابی در خصوص توانایی و قابلیت کنترل ریسک‌ها با توجه به وجود کاربران مختلف و تغییرات مداوم محیط سازمان انجام گرفته است؟		
۲	آیا برای تحقیق و انتخاب تهیه کننده سرویس مناسب، تلاش وکوشش مستمر امنیتی صورت می‌گیرد؟		
۳	آیا در قراردادهای بیمه، موارد مرتبط با مسئولیت‌های امنیتی، کنترل‌ها و گزارش دهی به اندازه کافی و مناسب می‌باشند؟		
۴	آیا در هنگام انتخاب تهیه کننده سرویس مناسب، تاکید اصلی بر روی مدیریت امنیت است؟		
۵	آیا سرویس دهنده‌ها از نظر کیفی واجد شرایط هستند و توانایی کنترل ریسک‌ها و موارد امنیتی را دارند؟		
۶	آیا کارمندان امنیتی سرویس‌دهنده واجد شرایط مناسب می‌باشند؟		
۷	آیا مستندات و مدارک امنیتی سرویس‌دهنده مورد بازبینی قرار گرفته است؟		

چک لیست شماره پانزدهم: نقاط ضعف و آسیب‌پذیری حوزه اینترانت

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه اینترانت	بله	خیر

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه اینترانت	بله	خیر
۱	آیا امتیازهای دسترسی از راه دور به اینترانت بر اساس نیاز کاری به هر فرد خاص نسبت داده شده است؟		
۲	آیا برنامه جست‌جوگر استفاده شده به وسیله کارمندان برای دسترسی به اینترانت، استاندارد سازی شده و سایر نرم‌افزارهای جست‌جوگر دیگر ممنوع شده است ؟		
۳	آیا برنامه جست‌جوگرهای وب که برای کاربردهای سازمان استفاده می‌شوند، قابلیت محتوای فعال دارند؟		
۴	آیا حساب‌های کاربران به صورت دوره‌ای چک می‌شود تا کارمندانی که دیگر کار نمی‌کنند یا رفته‌اند مشخص شوند؟		
۵	آیا روش‌های رمزنگاری و احراز هویت ورود به سیستم برای کاربران اینترانت پیاده‌سازی شده است؟		
۶	آیا قبل از ایجاد تغییرات یا تعمیر، به طور کامل و کلی از اینترانت پشتیبان گیری تهیه می‌شود؟		
۷	آیا گذرواژه‌های کاربران بر اساس خط‌مشی تنظیم شده است؟		
۸	آیا مجوز اضافه کردن، حذف کردن یا تغییر دادن محتوای اینترانت برای کاربران اینترانت محدودشده است؟		
۹	آیا همه کارمندان موافق هستند که استفاده از اینترانت ممکن است به صورت غیر منتظره تحت نظر قرار بگیرد؟		

چک لیست شماره شانزدهم: نقاط ضعف و آسیب‌پذیری حوزه بازبینی قرارداد سرویس دهنده

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه بازبینی قرارداد سرویس دهنده	بله	خیر
۱	آیا در قراردادها بخش‌های مختلف مدیریت ریسک روال‌های امنیتی تعیین شده است؟		
۲	آیا در قراردادها موارد امنیتی که باید بر اساس ضوابط و مقررات بازرسی انجام شوند، قید شده است؟		
۳	آیا در قراردادها، مساله عدم افشای اطلاعات مرتبط با سیستم‌ها و داده‌های سازمان عنوان شده است؟		
۴	آیا قراردادها به طور خلاصه بیان می‌کند که چه کسی مسئول چه بخشی از مدیریت امنیتی، داده‌ها و غیره می‌باشند؟		
۵	آیا قراردادهای تهیه کننده سرویس یا توافقات مرتبط با موارد امنیتی به صورت دوره‌ای موردبازبینی قرار می‌گیرند؟		
۶	آیا همه قراردادها بر است سطوح صحیح موجود در سازمان امضا شده و تایید صلاحیت شده‌اند؟		

چک لیست شماره هیفدهم: نقاط ضعف و آسیب‌پذیری حوزه برچسب‌زنی و سر جمع‌داری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه برچسب‌زنی و سر جمع‌داری	بله	خیر

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه برچسب‌زنی و سر جمع‌داری	بله	خیر
۱	آیا آخرین دیاگرام‌های شبکه‌ای و سر جمع داری از دسترسی غیرمجاز محافظت می‌شوند؟		
۲	آیا از دیاگرام‌های شبکه برای مستند کردن اتصالات فیزیکی میان امکانات و تجهیزات و پردازش اطلاعات استفاده می‌شود؟		
۳	آیا امکانات وتجهیزات و نواحی مهم شناسایی و ثبت شده‌اند؟		
۴	آیا بر روی اقلام و کابل‌های حساس به جای توصیف فیزیکی از کد استفاده می‌شود؟		
۵	آیا برچسب اموال و شماره سریال بر روی کلیه امکانات وتجهیزات کامپیوتری به‌کار می‌روند؟		
۶	آیا به طور دوره‌ای چک می‌شود که فقط امکانات وتجهیزات مجاز به شبکه وصل باشند؟		
۷	آیا به طور دوره‌ای شرایط امکانات وتجهیزات قدیمی‌تر را چک می‌نمایید؟		
۸	آیا به طور سالیانه لیست دارایی‌های ثابت با خود اقلام مقایسه می‌شوند؟		
۹	آیا روندی در دست دارید که با آن به طور دوره‌ای امکانات و تجهیزات را در سوابق انبار و دیاگرام‌ها دنبال کنید تا صحت و دقت سوابق را تأیید نمایید؟		
۱۰	آیا فهرستی از اموال در یک محل امن نگهداری می‌شود؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه برچسب‌زنی و سر جمع‌داری	بله	خیر
۱۱	آیا ممیزی مرتب اموال اجرا می‌شود؟		
۱۲	آیا یک روند رسمی تست دارید تا تجهیزات را پس از جابه‌جایی اضافه و تعویض، تست کنید؟		

چک لیست شماره هیجدهم: نقاط ضعف و آسیب‌پذیری حوزه برخورد با خلاف‌ها و شرایط اضطراری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه برخورد با خلاف‌ها و شرایط اضطراری	بله	خیر
۱	آیا برای جلوگیری از رخ دادن مجدد حوادث، آن‌ها را بررسی می‌نمایید؟		
۲	آیا رونده‌ای برخورد با شرایط اضطراری مثل بستن درها، خاموش کردن امکانات وتجهیزات و محافظت از دارایی‌ها در محل‌های مناسب نصب شده‌اند؟		
۳	آیا زمان‌های لازم برای نشان دادن عکس‌العمل تعیین شده و نظارت می‌شود؟		
۴	آیا سوابق مربوط به خلاف‌ها و موارد اضطراری را نگهداری می‌کنید؟		
۵	آیا کارکنان آموزش لازم جهت برخورد با طوفان‌ها و شرایط بد هوا دیده‌اند؟		
۶	آیا کارهای بعد از حوادث را برنامه‌ریزی کرده‌اید؟		
۷	آیا کلیه امکانات وتجهیزات و اماکن، ریسک‌های احتمالی، وفاداری کارکنان، از دست رفتن کسب و کار به دلیل تعطیلی‌ها و گسیختگی‌ها تحت پوشش بیمه می‌باشند؟		
۸	آیا یک طرح مواقع اضطراری برای از سرگیری کارهای سازمان که مبتنی بر کار سخت‌افزارها و نرم‌افزارها است در دست دارید؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه برخورد با خلاف‌ها و شرایط اضطراری	بله	خیر
۹	در صورت وقوع یک جنایت، آیا اطلاعات جهت تماس با واحد جنایی محلی موجود می‌باشد؟		

چک لیست شماره نوزدهم: نقاط ضعف و آسیب‌پذیری حوزه برنامه امنیتی پست الکترونیکی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه برنامه امنیتی پست الکترونیکی	بله	خیر
۱	آیا از سوی کاربران نهایی پشتیبانی لازم از قواعد کاربری پست الکترونیک شده است؟		
۲	آیا از سوی مدیریت ارشد پشتیبانی لازم از قواعد کاربری پست الکترونیک شده است ؟		
۳	آیا بخش نیروی انسانی و حقوقی برای تعیین مجازات نقض خطمشی با هم کمک کرده‌اند؟		
۴	آیا جهت تنظیم قواعد کاربری پست الکترونیک با بخش حقوقی درباره مسائل خاص صنعت رایزنی شده است؟		
۵	آیا جهت تنظیم قواعد کاربری پست الکترونیک با بخش حقوقی رایزنی شده است؟		
۶	آیا جهت تنظیم قواعد کاربری پست الکترونیک با بخش نیروی انسانی		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه برنامه امنیتی پست الکترونیکی	بله	خیر
	رایزنی شده است؟		
۷	آیا متصدی پست الکترونیک به طور دوره‌ای گزارش وضعیت ارائه می‌کند؟		
۸	آیا مدیر پست الکترونیک به طور دوره‌ای مسائل پست الکترونیک را با کاربران مورد بحث قرار می‌دهد؟		
۹	آیا یک برنامه امنیتی پست الکترونیک به‌کار گرفته شده است؟		
۱۰	آیا یک فرد را متصدی فرستادن پست الکترونیک‌ها از طریق سیستم پیام‌رسانی کرده‌اید؟		

چک لیست شماره بیستم: نقاط ضعف و آسیب‌پذیری حوزه بعد از تست نفوذ پذیری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه بعد از تست نفوذ پذیری	بله	خیر
۱	آیا بارگزاری‌ها و اسناد تست پس از اجرای تست نفوذ از سیستم حذف شده‌اند؟		
۲	آیا کارهای لازم و راه حل‌ها بر اساس سطح ریسک و آسیب‌پذیری اولویت‌بندی شده‌اند؟		
۳	آیا کارهای لازم و راه حل‌ها هر چه زودتر تکمیل می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه بعد از تست نفوذ پذیری	بله	خیر
۴	آیا گزارش و ارائه نتایج به وسیله نرم‌افزار/ مجری تست نفوذ برای مدیریت IT تهیه شده است؟		
۵	آیا همه مجوزها، آدرس‌های IP و غیره در ترکیب بندی اصلی دومرتبه تنظیم شده‌اند، به جز آن‌هایی که به‌عنوان نتیجه تست نیاز به تغییر دارند؟		
۶	آیا یک زمانبندی مناسب برای تست‌های نفوذ بعدی (سه ماه یک‌بار، سالیانه و غیر) انجام گرفته است؟		
۷	بعد از اتمام تست، آیا یک بازرسی انجام شده است؟		

چک لیست شماره بیست یک: نقاط ضعف و آسیب‌پذیری حوزه پاسخ‌گوئی کارکنان

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه پاسخ‌گوئی کارکنان	بله	خیر
۱	آیا افراد مسئول و پاسخ‌گوی اعمال خود می‌باشند؟		
۲	آیا افرادی که باید بتوانند در شرایط خاص برخی از کنترل‌های فنی و روال‌های عملیاتی مهمی را کنار گذاشته و دور بزنند، مورد آزمایش و گزینش قرار گرفته‌اند؟		
۳	آیا اقدامی در مورد اعطای دسترسی حداقل به منظور انجام وظایف روزانه کارمندان انجام شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه پاسخ‌گوئی کارکنان	بله	خیر
۴	آیا بازبینی عمل‌کردها اجرا می‌شود؟		
۵	آیا فرایند پاسخ‌گویی کاربران با شناسائی و احراز هویت کاربرانی که از سیستم‌های سازمان استفاده می‌کنند، تکمیل شده است؟		
۶	آیا مسئولیت امنیت هر نرم‌افزار کاربردی به یک فرد مناسب واگذار شده است؟		
۷	آیا همه اعمال و کارهایی که هر کاربر در سیستم انجام می‌دهد، قابل ردیابی است؟		
۸	به منظور جلوگیری از این که یک فرد بتوانند یک فرآیند حساس و حیاتی را خراب کند، آیا وظایف مرتبط با آن فرایند تفکیک شده و به افراد مختلف واگذار شده است؟		

چک لیست شماره بیست دو: نقاط ضعف و آسیب‌پذیری حوزه پس از خرید

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه پس از خرید	بله	خیر
۱	آیا اسناد مربوط به نرم‌افزارها در یک محل امن ذخیره می‌شوند؟		
۲	آیا اقلام حساس و مهم با دسترسی کنترل شده در جای امن حفظ می‌شوند؟		
۳	آیا کپی‌های جاری از نرم‌افزار کاربردی نگهداری و محافظت می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه پس از خرید	بله	خیر
۴	آیا مجوز یا سند اثباتی مالکیت برای هر نرم‌افزار دارید؟		

چک لیست شماره بیست سه: نقاط ضعف و آسیب‌پذیری حوزه پیکربندی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه پیکربندی	بله	خیر
۱	اگر لازم است آیا برنامه تفسیر آدرس‌های پورت‌ها/ شبکه (PAT/NAT) طوری پیکیربندی می‌گردد که فقط IP آدرس‌هایی را ترجمه نماید که بر روی بخش‌های شبکه محلی وجود دارند؟		
۲	آیا برای کاربران داخلی به جای اجازه دادن ایجاد تماس مستقیم از طریق دیواره آتش از پروکسی‌های کاربردی استفاده می‌کنید؟		
۳	آیا برنامه‌ها و سرویس‌های غیر ضروری روی دیواره آتش اجرا می‌شود؟		
۴	آیا پورت‌های خدمات ویژه همچون خدمات مدیریت راه دور، قواعدی دارند که آن‌چه را که IP آدرس‌های منبع که به آن‌ها وصل شوند، را محدود نمایند (مثلاً SSH)؟		
۵	آیا پورت‌های خدمات ویژه همچون خدمات مدیریت راه دور، وقتی مورد استفاده نیستند از کار انداخته می‌شوند؟		
۶	آیا خط‌مشی پیش‌فرض برای دیواره آتش جلوگیری از ورود انواع ترافیک مشکوک می‌باشد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه پیکربندی	بله	خیر
۷	آیا دیواره آتش به طور مرتب اسکن می‌شود تا پورت‌های باز را فیل‌تر نماید؟		
۸	آیا دیواره آتش طوری پیکربندی گردیده است که از داده‌های نابه‌جا هم‌چون بسته‌های تکه‌تکه شده، آدرس‌های IP جعلی، انواع ICMP بی‌اعتبار و داده‌های TCP بی‌اعتبار و . . . جلوگیری نماید؟		
۹	آیا رایانه‌های تازه خریداری شده قبل‌از اتصال به شبکه برای کارکرد امن پیکربندی شده‌اند ازجمله آیا همه سیستم عامل و نرم‌افزارهای تکمیلی آن برای کارکرد امن قبل از اتصال به شبکه آیا پیکربندی شده‌اند؟		
۱۰	آیا رایانه‌های سازمان استانداردهای ضد ویروس دسک‌تاپ سازمان جهت حداقل امنیت را از طریق اسکن کردن پسیو رعایت می‌کنند؟		
۱۱	آیا ردگیری تماس برای تسهیل و بهسازی معیارهای مطابقت پذیری ترافیک و هم‌چنین برای بررسی صحت تماس به‌کار می‌رود ؟		
۱۲	آیا روند خاصی برای نصب نرم‌افزار ضد ویروس بر روی وسایل خصوصی افراد که در امور تجاری به‌کار می‌برند دارید؟		
۱۳	آیا سرور پست الکترونیک برای کمک به راه‌حل ضد ویروس پیکربندی گردیده است؟		
۱۴	آیا سرورهای سازمان جهت پذیرش، به‌هنگام‌سازی و توزیع فایل‌های تعریف ویروس به صورت به موقع و به نحو مناسبی پیکربندی شده‌اند؟		
۱۵	آیا سرورهایی که با بیرون در ارتباط می‌باشند درمقابل حمله ویروسی و آلوده شدن محافظت می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه پیکربندی	بله	خیر
۱۶	آیا سیستم عامل تحت دیواره آتش کاملاً امن و به‌روز می‌باشد؟		
۱۷	آیا سیستم عاملی که نرم‌افزار ضد ویروس بر روی آن اجرا می‌شود، به طور کامل امن شده و وصله‌های امنیتی بر روی آن کاملا اعمال شده‌است؟		
۱۸	آیا شبکه سازمان در مقابل تجهیزاتی که از راه دور به آن متصل می‌شوند به‌نحو مناسبی محافظت شده است؟		
۱۹	آیا کلیه خدمات شبکه‌ای که توسط سرور میزبانی می‌گردند، به بخشی از شبکه که مجزا از سایر بخش‌های حساس شبکه می‌باشد، وصل می‌باشند؟		
۲۰	آیا نرم‌افزار ضد ویروس بر روی همه رایانه‌ها، لب‌تاپ‌ها و دیگر لوازم نصب گردیده است؟		
۲۱	آیا وضعیت نرم‌افزار ضد ویروس ضد ویروس (مثلاً نصب، نگارش‌های نو و غیره)درمیان همه رایانه‌های سازمان ردگیری شده است؟		

چک لیست شماره بیست چهار: نقاط ضعف و آسیب‌پذیری حوزه پیگیری خدمات سرویس دهنده

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه بازبینی قرارداد سرویس دهنده	بله	خیر
۱	آیا در قراردادها بخش‌های مختلف مدیریت ریسک روال‌های امنیتی		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه بازبینی قرارداد سرویس دهنده	بله	خیر
	تعیین شده است؟		
۲	آیا در قراردادها موارد امنیتی که باید بر اساس ضوابط و مقررات بازرسی انجام شوند، قید شده است؟		
۳	آیا در قراردادها، مساله عدم افشای اطلاعات مرتبط با سیستم‌ها و داده‌های سازمان عنوان شده است؟		
۴	آیا قراردادها به طور خلاصه بیان می‌کند که چه کسی مسئول چه بخشی از مدیریت امنیتی، داده‌ها و غیره می‌باشند؟		
۵	آیا قراردادهای تهیه کننده سرویس یا توافقات مرتبط با موارد امنیتی به صورت دوره‌ای موردبازبینی قرار می‌گیرند؟		
۶	آیا همه قراردادها بر است سطوح صحیح موجود در سازمان امضا شده و تایید صلاحیت شده‌اند؟		

چک لیست شماره بیست پنج: نقاط ضعف و آسیب‌پذیری حوزه تأییدات و مشورت

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تأییدات و مشورت	بله	خیر
۱	آیا بخش IT سازمان، آخرین تعاریف ویروس را به طور مرتب دریافت می‌کند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تأییدات و مشورت	بله	خیر
۲	آیا بخش مشاوره و هشدار فروشنده، فایل‌های معرف تهدیدهای ویروسی جدید شناخته شده در ۲۴ ساعت گذشته را ارائه می‌نماید؟		
۳	آیا تعاریف ویروس‌ها به طور خودکار برای همه رایانه‌های مشتری توزیع می‌شود؟		
۴	آیا مدیرIT به طور مرتب گزارشات و هشدارهای ویروس‌ها را جمع‌آوری می‌کند؟		

چک لیست شماره بیست شش: نقاط ضعف و آسیب‌پذیری حوزه تست نفوذ پذیری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تست نفوذ پذیری	بله	خیر
۱	اگر نفوذی اتفاق بیفتد و رخنه‌ای ایجاد می‌شود، آیا کارمندان دارای صلاحیت در دسترس هستند تا در صورت نیاز سیستم را به حالت اول برگردانند؟		
۲	آیا به منظور به حداقل رساندن خسارات، اقلام یا مواردی مثل تست سرویس‌ها و خدمات در خارج از وقت مقرر انجام می‌شوند؟		
۳	آیا پشتیبان‌ها، روش‌های واکنش دربرابرحادثه و کشف تخلفات به روز و مقرر شده‌اند؟		
۴	آیا فرم‌های مناسب معرفی کننده برای مجریان تست نفوذ تعیین شده‌اند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تست نفوذ پذیری	بله	خیر
۵	آیا قراردادهای امنیتی نیز جزء موارد تست کننده به حساب می‌آیند؟		
۶	آیا قراردادهای جبران خسارت و افشا نکردن جزئیات و اطلاعات طبقع بندی شده تعیین و امضا شده‌اند؟		
۷	آیا کارمندان کلیدی و مهم آگاهی دارند که تست نفوذ در حال برگزاری است؟		
۸	آیا مراحل یا گام‌هایی به منظور تشخیص تست‌ها از حملات واقعی در نظر گرفته شده است؟		
۹	آیا همه تست‌ها و کارهای مهم و برجسته ثبت شده‌اند؟		
۱۰	آیا همه مجوزهای مناسب شناخته شده و واگذار شده‌اند؟		

چک لیست شماره بیست هفت: نقاط ضعف و آسیب‌پذیری حوزه تست و پاک‌سازی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تست و پاک‌سازی	بله	خیر
۱	آیا نرم‌افزارهای ضد ویروس به طور متناوب بر روی تجهیزات کاربران در مقابله با آسیب‌پذیری‌های شناخته‌شده آزمایش می‌شود؟		
۲	در صورت حمله ویروسی آیا تست‌هایی جهت تعیین سطح خسارتی که می‌تواند واردآید، به اجرا درآمده است؟		
۳	آیا طرحی برای رایانه‌های آلوده وجود دارد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تست و پاک‌سازی	بله	خیر
۴	آیا طرف ثالثی که در ارتباط با نرم‌افزار ضد ویروس خدمات ارائه می‌دهد آزمایش شده است؟		
۵	آیا رایانه‌های آلوده جهت اطمینان از پاک‌سازی کامل ویروس‌ها به طور مجدد چک می‌شوند؟		
۶	آیا رایانه‌ها به ترتیب حافظه، فایل‌های بوت، رجیستری، فایل‌های سیستم عامل، فایل‌های برنامه، و فایل‌های داده برای یافتن ویروس اسکن می‌شوند؟		
۷	آیا پس از هر تغییری در نمایه تهدید سازمان، امنیت ضد ویروس مورد آزمایش قرار می‌گیرد؟		
۸	آیا پس از افزایش ترافیک شبکه راه‌حل ضد ویروس تست می‌شود یا جمعیت کاربران مورد توجه قرار دارد؟		
۹	آیا ویروس‌کش کلیه ویروس‌ها را در طول اسکن‌های تستی، شناسایی و آشکار می‌نماید و آیا هشدارهای مورد انتظاررا اعلام می‌نماید؟		

چک لیست شماره بیست هشت: نقاط ضعف و آسیب‌پذیری حوزه تعمیر و نگهداری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تعمیر و نگهداری	بله	خیر
۱	آیا برای بازیابی و تعمیر نرم‌افزار صدمه دیده از دیسکت اورژینال استفاده می‌کنید؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تعمیر و نگهداری	بله	خیر
۲	آیا پس از خرید نگارش‌های ارتقاء یافته نرم‌افزارها، جهت دور ریزی نسخه قدیمی بر اساس موافقت‌نامه لیسانس نرم‌افزار عمل می‌کنید؟		
۳	آیا رفتار کاربران نهایی از لحاظ خطرات ویروسی مربوط به دانلود کردن برنامه‌های اشتراکی، بازی‌ها و برنامه‌های دمو، مورد بازرسی قرار می‌گیرد؟		
۴	آیا سرویس پک‌های فروشنده تست می‌شوند؟		
۵	آیا نرم‌افزارهای جدید یا آن‌ها که اصلاحات اساسی بر آن‌ها اعمال شده یا آن‌ها که خیلی کاربری حساسی دارند قبل از اجرا کاملاً تست می‌گردند؟		
۶	آیا همه تغییرات یا اصلاحات امنیتی را که فروشنده توصیه می‌کند بلافاصله پس از دریافت رسمی آن‌ها اجرا می‌کنید؟		
۷	آیا همه دستورالعمل‌های فروشنده پیروی می‌شوند؟		
۸	پس از اجرا آیا عمل‌کردها و نقش‌های کاربر و حفاظت‌های مدیریتی، فنی و فیزیکی چک می‌شوند (از لحاظ وجود داشتن و درست کارکردن)؟		
۹	قبل از اجرا یا اعمال تغییرات آیا روندی در دست دارید که بازگشت به حالت پایدار را میسر سازد؟		
۱۰	قبل از اجرا یا اعمال تغییرات آیا ساعت‌ها و روزهای عملیات مدنظر می‌باشند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تعمیر و نگهداری	بله	خیر
۱۱	قبل از نصب آیا نرم‌افزارها در یک محیط مناسب جهت تضمین کیفیت تست می‌شوند؟		

چک لیست شماره بیست نه: نقاط ضعف و آسیب‌پذیری حوزه تغییر کلمه عبور

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تغییر کلمه عبور	بله	خیر
۱	آیا الزام در تغییر گذر واژه‌ها بر اساس موضوعی نظیر سطح لازم امنیتی می‌باشد؟		
۲	آیا بعد از گذشت حداکثر تعداد روز مشخص، گذرواژه‌ها باید تغییر داده شوند ؟		
۳	آیا سیستم طوری طراحی شده است که حداقل پنج گذرواژه قبلی را نتوان دوباره استفاده نمود؟		
۴	آیا گذرواژه‌های پیش فرض درنرم افزار، سخت افزار و غیره به سرعت تغییر داده می‌شوند ؟		
۵	آیا هنگامی که گذرواژه‌ها منقضی شده و نیاز به تغییر دارند، کاربر تنها می‌تواند با یک حساب موقت محدود شده به سیستم وارد شود ؟		

چک لیست شماره سی: نقاط ضعف و آسیب‌پذیری حوزه تهیه وآماده سازی طرح تست نفوذ پذیری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تهیه وآماده سازی طرح تست نفوذ پذیری	بله	خیر
۱	اگر سطح غیرقابل قبولی از ریسک اتفاق بیفتد آیا راهی برای مداخله کردن یا متوقف کردن تست‌ها وجود دارد؟		
۲	آیا اعمال و کارهای ویژه تعریف شده‌اند؟		
۳	آیا اهداف و مقاصد ویژه‌ای برای مجریان تست نفوذ در نظر گرفته شده است؟		
۴	آیا اهداف و نتایج تست‌ها مشخص و ثبت شده است؟		
۵	آیا پیمان‌کار انتخاب شده دارای بیمه مسئولیت می‌باشد؟		
۶	آیا تحقیقات مناسبی برای هر یک از فروشندگان نرم‌افزار یا شرکت‌ها یا موسسات اجرا کننده تست نفوذ انجام شده است؟		
۷	آیا تحلیلی از سود / هزینه در مورد اجرای روند تست نفوذ به صورت داخلی در مقابل اجرای آن به صورت خارجی انجام شده است؟		
۸	آیا تست کننده برای انجام تست نفوذ، علاوه بر یک سری ابزارهای موثر و متعارف، از ابزارهای استاندارد نیز استفاده می‌نماید؟		
۹	آیا تست نفوذپذیری با یک روش سازمان یافته برنامه‌ریزی و مدیریت می‌شود؟		
۱۰	آیا تهدیدات واقعی مورد تست قرار گرفته‌اند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تهیه وآماده سازی طرح تست نفوذ پذیری	بله	خیر
۱۱	آیا حدودی برای تست‌ها و دسترسی نرم‌افزاری تعیین شده است؟		
۱۲	آیا خروجی‌های نهایی تست نفوذ قابل درک می‌باشند ؟		
۱۳	آیا روند پردازشی به منظور حفاظت در برابر تست در هنگامی که کارمندان غیر حرفه‌ای به جاری کارمندان حرفه‌ای کار می‌کنند ایجاد شده است؟		
۱۴	آیا ریسک‌های مربوط به انجام تست نفوذ مشخص شده است؟		
۱۵	آیا سطح مهارت مجریان تست نفوذ به صورت خاص ذکر شده است؟		
۱۶	آیا صلاحیت ومهارت‌های تست کننده، تائید شده است؟		
۱۷	آیا فرد / نرم‌افزار تست کننده از یک متدولوژی استاندارد مناسب پیروی می‌کند؟		
۱۸	آیا فرم‌های خاصی به‌عنوان گواه و مدرک مورد نیاز است؟		
۱۹	آیا لیستی از فروشندگان نرم‌افزار و فروشندگان تست‌های دارای منابع خارجی برای تست نفوذپذیری تهیه شده است؟		
۲۰	آیا لیستی از مشتریان به وسیله فروشندگان / شرکت‌های برگزار کننده تست نفوذ تهیه شده است؟		
۲۱	آیا مواردی که در تست نفوذ مورد بررسی قرار می‌گیرند، به تفصیل بیان شده‌اند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه تهیه وآماده سازی طرح تست نفوذ پذیری	بله	خیر
۲۲	آیا نظارت داخلی (از داخل سازمان) در حین انجام تست‌ها ادامه می‌یابد؟		
۲۳	آیا همه کارمندان کلیدی IT راجع به عوامل ریسک بالقوه مورد مشورت قرار گرفته‌اند؟		
۲۴	آیا همه نقاط ورودی غیرمنتظره داخل سازمان تعریف شده‌اند؟		

چک لیست شماره سی یک: نقاط ضعف و آسیب‌پذیری حوزه توسعه و استقرار

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه توسعه و استقرار	بله	خیر
۱	آیا بسته‌های نرم‌افزارهای خریداری شده برای استفاده سازمان اصطلاح شده و تغییر یافته‌اند؟		
۲	آیا فروشنده نرم‌افزهای کاربردی وب نظارت متعارف خود را برای جلوگیری از سوءاستفاده انجام می‌دهد؟		
۳	آیا کنترل‌های دسترسی به منظور محافظت از منابع کد مرجع یا پایگاه داده‌ها در نظر گرفته شده و وجود دارد؟		
۴	آیا کنترل‌های مسیریابی شبکه وجود دارد؟		
۵	آیا لاگ‌های ثبت شده نرم‌افزار کاربردی وب به طور منظم بررسی می‌شوند تا فعالیت غیرعادی آن‌ها مشخص شود؟		
۶	آیا لاگ‌های ثبت شده نرم‌افزارها کاربردی وب به طور منظم بررسی می‌شوند تا از کارکرد مناسب آن‌ها اطمینان حاصل شود؟		
۷	آیا محیط‌های توسعه یا آزمایش از سرورهای تولید مجزا شده‌اند؟		
۸	آیا نسخه‌ها/ بروزشدن‌های جدید به طور کامل قبل از به‌کارگیری مورد آزمایش قرار گرفته‌اند؟		
۹	آیا نوارهای پشتیبان برای نرم‌افزارهای کاربردی که تغییرات متعددی بر روی آن‌ها اعمال شده یا نسخه‌های جدیدی تولید شده‌اند، مورد حفاظت		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه توسعه و استقرار	بله	خیر
	و نگهداری قرار می‌گیرند؟		
۱۰	آیا همه اسکریپت‌های نرم‌افزار کاربردی وب در برابر حملات شناخته شده، قبل از به‌کارگیری آن‌ها مورد تست و آزمایش قرار گرفته‌اند؟		
۱۱	آیا همه کاربردهای وب خارج از کنترل گروه توسعه وب سازمان تعریف و تعیین شده‌اند؟		
۱۲	آیا همه نرم‌افزارها (اختصاصی و خریداری شده) قبل از نصب بر روی رایانه‌های عملیاتی، برای یافتن ویروس‌ها مورد آزمایش قرار گرفته‌اند؟		
۱۳	آیا همه ویژگی‌های نرم‌افزاری کاربردی تحت وب به منظور اطمینان از صحت اطلاعات امنیتی مستند شده‌اند؟		

چک لیست شماره سی دو: نقاط ضعف و آسیب‌پذیری حوزه ثبت وقایع و گزارش

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه ثبت وقایع و گزارش	بله	خیر
۱	آیا اهمیت حفاظ‌های امنیتی پست الکترونیک‌ها درک شده است؟		
۲	آیا به نمایندگی از تیم امنیت، سوابق نگهداری می‌شوند؟		
۳	آیا حوادث گزارش می‌شوند؟		
۴	آیا خط سیر بازرسی پست الکترونیک برقرار می‌باشد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه ثبت وقایع و گزارش	بله	خیر
۵	آیا زمانی که کاربران صرف پست الکترونیک می‌کنند در روز یا ماه مونیتور می‌شود؟		
۶	آیا طرح گزارش دهی دارید؟		
۷	آیا لاگ برای پیدا کردن و حل مسائل به‌کار گرفته می‌شود؟		
۸	آیا مستندسازی اجرا می‌شود؟		
۹	آیا موثرترین و کم اثرترین روش‌های بلوکه کردن شناسایی شده است؟		
۱۰	آیا نرخ‌های موفقیت در مقابله با هرزنامه مونیتور شده و گزارش می‌شوند؟		

چک لیست شماره سی سه: نقاط ضعف و آسیب‌پذیری حوزه ثبت‌ها

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه ثبت‌ها	بله	خیر
۱	آیا زمانی برای نگهداری و ذخیره لاگ‌ها تعیین شده است؟		
۲	آیا فضای ذخیره کافی در سرور میان پشتیبان‌های اصلی به منظور حفظ و گرفتن فایل‌های لاگ، موجود می‌باشد؟		
۳	آیا کلیه بسته‌های رد شده ثبت می‌شوند؟		
۴	آیا کلیه جلسات شروع شده، موفقیت آمیز یا ناموفق ثبت می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه ثبت‌ها	بله	خیر
۵	آیا کلیه وقایع و خطاها مونیتور و ثبت می‌شوند؟		
۶	آیا لاگ‌های دیواره آتش حتی اگر دیواره آتش خاموش باشد قابل دست‌یابی است؟		

چک لیست شماره سی چهار: نقاط ضعف و آسیب‌پذیری حوزه چک کردن ویروس‌ها

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه چک کردن ویروس‌ها	بله	خیر
۱	آیا نرم‌افزارهای کاربردی قبل از استفاده در شبکه سازمان بر روی یک pc خارج از شبکه تست می‌شوند؟		
۲	آیا نرم‌افزارهای مُهر و مُوم شده آماده استفاده نیز قبل از کاربری با ضد ویروس اسکن می‌شوند؟		
۳	آیا همه مدیاها قبل از اولین استفاده با نرم‌افزارهای ضد ویروس اسکن می‌شوند؟		
۴	آیا هنگام تست نرم‌افزار جدید، از دسترسی مهمان استفاده می‌شود؟		

چک لیست شماره سی پنج: نقاط ضعف و آسیب‌پذیری حوزه حذف یا دسترسی کلمات عبور

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حذف یا دسترسی کلمات عبور	بله	خیر
۱	آیا خروج از سیستم به‌طور اتوماتیک تنظیم شده است؟		
۲	آیا رکوردهای افرادی که قبلا جزء کارمندان سازمان بوده‌اند، مورد بررسی قرار می‌گیرد تا این اطمینان حاصل شود که امتیازات دسترسی ایستگاه‌های کاری آن‌ها حذف شده است؟		
۳	آیا رونده‌ای ابطال یا متوقف کردن امتیازات دسترسی یا کلمات عبور اجرا می‌شوند؟		
۴	آیا شناسه‌های ورود به سیستم هنگامی که افراد دیگر به آن‌ها احتیاج ندارند غیرفعال می‌شوند ؟		
۵	آیا شناسه‌های ورود به سیستم هنگامی که برای بیش از یک دوره‌ی زمانی مشخص بدون فعالیت باشند، حذف شده یا از کار می‌افتند؟		
۶	آیا هنگامی که یک شکاف امنیتی مشکوک یافت می‌شود یا یک رمز مورد حمله قرار می‌گیرد، سیاست‌ها و رونده‌ای خاصی دنبال می‌شوند؟		
۷	هنگامی که یک ایستگاه کاری برای مدت زمان خاصی غیرفعال شده است آیا صلاحیت‌های دسترسی آن ایستگاه‌های کاری لغو می‌شوند؟		

چک لیست شماره سی شش: نقاط ضعف و آسیب‌پذیری حوزه حفاظت از دارائی‌های ایستگاه کاری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظت از دارائی‌های ایستگاه کاری	بله	خیر
۱	اگر چیزی گم شود آیا بلافاصله به کارکنان امنیتی اطلاع داده می‌شود؟		
۲	آیا ابزارهای قفلی مختلف برای وسایل جانبی تعبیه شده است؟		
۳	آیا امنیت ساختمان و دفتر به طور مناسب تأمین است؟		
۴	آیا اموال شخصی در کمدهای خاص نگهداری شده و قفل می‌شوند؟		
۵	آیا بیگانگان و/یا فعالیت‌های عجیب به چالش کشیده می‌شوند؟		
۶	آیا تنها آن‌چه مورد نیاز می‌باشد در رک‌استیشن‌ها نصب می‌باشند؟		
۷	آیا جابه‌جایی، قطع اتصال یا ایجاد تغییر در تجهیزات IT یا ارتباط از راه دور (مخابرات) نیازمند کسب مجوز قبلی است؟		
۸	آیا در هنگامی‌که کسی در سازمان نیست درها و پنجره‌ها بسته است؟		
۹	آیا درهای خروجی در همه ساعات بسته است؟		
۱۰	آیا دیسکت‌ها،سی دی‌ها، دیسک‌های فشرده شده یا فایل‌های الکترونیکی که از خارج از سایت برگشت داده می‌شوند با ضد ویروس چک می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظت از دارائی‌های ایستگاه کاری	بله	خیر
۱۱	آیا رایانه‌ها، موبایل‌ها و PDAها بایک کد عبور قفل می‌شوند؟		
۱۲	آیا رسانه‌های قابل حمل در جای خاصی قفل می‌شوند؟		
۱۳	آیا سوابق پرسنل به‌لحاظ سپردن منابع IT به آن‌ها بررسی می‌شود؟		
۱۴	آیا کارکنان از پروتکل تعمیر چیزی می‌دانند تا تحت این عنوان چیزی بیرون برده نشود؟		
۱۵	آیا کلیه سخت‌افزارها برچسب اموال دارند؟		
۱۶	آیا لیستی از اشیاء ایستگاه کاری هرسال با یک لیست اصلی و اولیه مقایسه می‌شوند؟		
۱۷	درجائی‌که عملی باشد آیا برای نگهداری رایانه‌ها از ابزارهای قفلی استفاده می‌کنید؟		
۱۸	هنگامی‌که به‌مدت طولانی تعطیلی است آیا کلیدها، پاس‌کارت‌ها، کیف‌ها، تلفن‌همراه، PDAها وغیره به‌همراه برده شده یا در کمدها قفل می‌شوند؟		
۱۹	هنگامی‌که به‌مدت طولانی در اتاق‌ها کسی حضور ندارد آیا میزها و کابینت‌ها قفل می‌باشند؟		

چک لیست شماره سی هفت: نقاط ضعف و آسیب‌پذیری حوزه حفاظت‌های امنیتی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظت‌های امنیتی	بله	خیر
۱	آیا ابزارها و تکنیک‌هایی که برای پشتیبانی از سیاست‌های امنیتی اطلاعات به‌کار می‌آیند شناسایی شده‌اند؟		
۲	آیا الزامات قانونی و حقوقی جهت امنیت اسناد شناخته شده و پیروی می‌شوند؟		
۳	آیا تهدیدات، ریسک‌ها و خطرات بالقوه شناخته شده‌اند؟		
۴	آیا توانایی در ارسال، چاپ‌کردن، قطع کردن و کپی کردن و مشاهده اسناد کسب و کاری توسط پست الکترونیک تحت کنترل می‌باشد؟		
۵	آیا در محیط شما رمزنگاری شدنی و به صرفه می‌باشد؟		
۶	آیا دسته‌بندی امنیتی، سطح تأثیرگذاری و برآوردهای محیطی تا مرحله انتخاب کنترل‌های امنیتی لازم برای هر سیستم ترسیم شده‌اند؟		
۷	آیا رمزنگاری جهت حفاظت از اسناد مورد نیاز است؟		
۸	آیا رهنمودهایی در دست دارید که ارسال امن اسناد تجاری یا کسب و کاری را بیان کند؟		
۹	آیا سطح حفاظت تا سطح ریسک و بزرگی خسارت به صورت نقشه ترسیم و تبیین شده است؟		
۱۰	آیا سطح خسارت بر اساس مواردی از قبیل توانایی در اجرای کارهای اصلی و مهم، ایراد خسارت به دارایی‌ها، ضرر مالی، از بین بردن حسن شهرت و. . . شناسایی شده است ؟		
۱۱	آیا قواعد ازطریق اعمال جریمه و تحریم به‌خصوص بر اساس سیستم		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظت‌های امنیتی	بله	خیر
	مورد حمله و طبیعت حادثه اتفاق افتاده به‌اندازه کافی قدرت اجرایی دارند؟		
۱۲	آیا قواعد آئین‌نامه نشان دهنده کنترل‌های امنیتی فنی موجود در سیستم می‌باشند؟		
۱۳	آیا کارکنان در کاربری رمزنگاری مهارت دارند؟		
۱۴	آیا محتوای رکوردها تحت کنترل است؟		
۱۵	آیا نوع و میزان حفاظت می‌تواند متفاوت باشد؟		

چک لیست شماره سی هشت: نقاط ضعف و آسیب‌پذیری حوزه حفاظ‌های امنیتی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظ‌های امنیتی	بله	خیر
۱	آیا از داده‌های صندوق صوتی سازمان به طور کامل قبل از ایجاد تغییرات یا اصلاحات نسخه پشتیبان گرفته می‌شود؟		
۲	آیا انتقال مکالمه محدود شده است؟		
۳	آیا پرسنل تعمیر و نگه‌داری خارج سازمان در صندوق صوتی سازمان در مدت تعمیرات همراهی می‌شوند؟		
۴	آیا پورت نگه‌داری از راه دور غیرفعال شده است؟ (در صورت لزوم)		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظ‌های امنیتی	بله	خیر
۵	آیا کارمندان می‌توانند آزادانه تماس‌های تلفنی بین شهری و موبایل انجام دهند ؟		
۶	آیا گذرواژه پیش‌فرض صندوق صوتی سازمان بلافاصله پس از نصب تغییر یافته است؟		
۷	آیا گذرواژه‌های کاربر بر اساس خط‌مشی امنیتی سازمان تنظیم شده‌اند؟		
۸	آیا مودم‌های دسترسی از راه دور در هنگامی که مورد استفاده قرار ندارند غیرفعال می‌شوند؟		
۹	آیا نوارهای مکالمات به صورت روزانه ضبط می‌شوند و در یک محل امن ذخیره می‌شوند؟		
۱۰	آیا همه تلفن‌ها توسط صندوق صوتی سازمان به‌طور دقیق جهت مسیریابی کنترل شده‌اند؟		

چک لیست شماره سی نه: نقاط ضعف و آسیب‌پذیری حوزه حفاظ‌های امنیتی نرم افزاری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظ‌های امنیتی نرم افزاری	بله	خیر
۱	اگر نرم‌افزار برای تست به شخص ثالث ارسال شود، آیا برنامه برگردانده شده، برای یافتن ویروس‌ها، کدهای مخرب و سایر موارد اسکن می‌شود؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظ‌های امنیتی نرم افزاری	بله	خیر
۲	آیا تجهیزات و سیستم‌های پردازشی جانشین، همانند تجهیزات و سیستم‌های اصلی مورد بررسی و آزمایش قرار می‌گیرند؟		
۳	آیا تعامل و اثر متقابل نرم‌افزارهای کاربردی بر یکدیگر برای یافتن ضعف‌ها و نواقص مورد بررسی قرار گرفته است؟		
۴	آیا در هنگام رفع آسیب‌پذیری‌های نرم افزار، منابع حفره‌های امنیتی مورد توجه قرار می‌گیرند؟		
۵	آیا روش‌های سوء استفاده هکرها از رونده‌ای مبتنی بر مجوز دهی مورد بازبینی و رسیدگی قرار گرفته‌اند؟		
۶	آیا روند ارزیابی ریسک انجام گرفته است؟		
۷	آیا فرآیندی به منظور تضمین امنیت و کنترل مناسب همه پشتیبان‌ها و کتابخانه‌ها در تمام مدت چرخه عمر آن‌ها در نظر گرفته شده است؟		
۸	آیا فرایندی به منظور جلوگیری از دست‌کاری کدهای برنامه در سمت کاربر مورد بازبینی و رسیدگی قرار گرفته‌است؟		
۹	آیا کد جدید برنامه (نسخه به تا) برای تست از محیط توسعه مجزا شده است؟		
۱۰	آیا مراحل اعتبارسنجی نرم‌افزارکاربردی به منظور جلوگیری از ورود تصادفی یا تعمدی کدهای مخرب مورد بازبینی و رسیدگی قرار گرفته‌اند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه حفاظ‌های امنیتی نرم افزاری	بله	خیر
۱۱	به منظور انجام آزمایش‌های امنیتی، آیا بررسی جامعی از محیط توسعه نرم افزار برای استخراج نقاط ضعف موجود در کد برنامه انجام می‌شود؟		

چک لیست شماره چهل: نقاط ضعف و آسیب‌پذیری حوزه خدمات وب

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خدمات وب	بله	خیر
۱	اگر سرویس‌های وب نتواند به وسیله دیواره آتش محافظت شود، آیا برنامه استمرارپذیری ای وجود دارد که از این نرم‌افزارها محافظت نماید؟		
۲	آیا پیام‌های XML دریافتی به طور کامل بررسی یا فیل‌تر شده‌اند تا از زیان‌آور نبودن آن‌ها اطمینان حاصل شود؟		
۳	آیا سرویس‌های وب موجود در برابر حمله فرهنگ لغت یا حمله ورود به زور آسیب می‌باشند؟		
۴	آیا معاملات پولی یا داده‌های شخصی حساس که از طریق سرویس‌های وب منتشر می‌شوند مورد محافظت قرار می‌گیرند؟		
۵	آیا مقیاسی به منظور تعیین حملات عدم سرویس دهی XML محتمل، گردآوری و تحلیل شده‌است؟		

چک لیست شماره چهل یک: نقاط ضعف و آسیب‌پذیری حوزه خرید

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خرید	بله	خیر
۱	آیا از سوابق فروشنده تحقیقات کامل(نرم‌افزارهای فروخته، مشتریان دیگر، شهرت و. . .) به‌عمل آمده است؟		
۲	آیا از فروشنده‌ها خواسته می‌شود که نرم‌افزار خود را روی رایانه غیرشبکه‌ای نمایش دهند؟		
۳	آیا اسناد تهیه نرم‌افزارها دارای این الزام می‌باشد که فروشنده از رونده‌ای ضد ویروس برای حصول اطمینان از آلوده نبودن مدیای فروخته شده استفاده می‌کند؟		
۴	آیا این نرم‌افزار کاربردی مدت زیادی در بازار بوده است؟		
۵	آیا پشتیبانی فنی و خدمات پس از فروش برای نرم‌افزار موجود است؟		
۶	آیا خرید نرم‌افزار بر اساس قاعده است؟		
۷	آیا فهرستی از نرم‌افزارهای ممنوع و مجاز تهیه شده است؟		
۸	آیا نگارش‌های قبلی به طور نسبی بدون سرویس پک یا آپ‌گرید بوده‌اند؟		
۹	برای حفاظت در مقابل ویروس‌ها آیا نرم‌افزارها و فایل‌های داده‌ای از منابع مطمئن خریداری می‌شوند؟		
۱۰	قبل از خرید نرم‌افزار جدید آیا تحقیق گسترده صورت می‌گیرد؟		

چک لیست شماره چهل دو: نقاط ضعف و آسیب‌پذیری حوزه خط مشی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی	بله	خیر
۱	آیا خط مشی‌ها و موافقت نامه‌های کارکنان درباره کاربری و پیکربندی دیواره آتش به لحاظ قانونی هم‌خوانی دارند؟		
۲	آیا خط‌مشی امنیتی به نحوی مکتوب گردیده است که با خط‌مشی‌های کاربری قابل قبول اینترنت و پست الکترونیک هم‌خوانی داشته باشد؟		
۳	آیا خط‌مشی امنیتی به وضوح آن‌چه را که توسط دیواره آتش محافظت می‌شود و دلیل آن را بیان می‌نماید؟		
۴	آیا خط‌مشی امنیتی به وضوح ترافیک و اطلاعاتی را که قانونی است و آن چیزهایی را که مونیتور می‌شود بیان می‌نماید؟		
۵	آیا خط‌مشی مورد تجدید نظر و به‌روز رسانی قرار می‌گیرد؟		
۶	آیا رونده‌ای رسمی کنترل تغییرات وجود دارد؟		
۷	آیا طرحی وجود دارد که آگاهی ثابت و مداوم کاربر نسبت به دیواره آتش و کارکرد آن‌را تأمین کند؟		
۸	آیا کلیه کارکنان مرتبط خط‌مشی امنیتی سازمان را که مربوط به دیواره آتش می‌شود خوانده و فهمیده‌اند؟		
۹	آیا یک خط‌مشی امنیتی که توسط همه کارکنان مربوط امضا شده باشد وجود دارد؟		

چک لیست شماره چهل سه: نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی بی سیم

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی بی سیم	بله	خیر
۱	آیا بازبینی از همه اجزا امنیتی مرتبط با بی‌سیم انجام گرفته است؟		
۲	آیا تعداد نقاط دسترسی هم برای ایمنی و هم برای قابلیت دسترسی مورد نیاز مناسب می‌باشد؟		
۳	آیا جلسات آموزشی منظم برای همه کارمندان در مورد اهمیت و روش‌های امنیتی در نظر گرفته شده است؟		
۴	آیا خط‌مشی بی‌سیم به منظور معرفی و تعیین کاربران سیستم ایجاد شده است؟		
۵	آیا کارمندان شایسته و واجد شرایط، راهبردها و راهنماهای مناسب و نقشه‌های اجرایی برای هر یک از موضوعات بی‌سیم در اختیار دارند؟		
۶	آیا نقاط دسترسی مرتبط با دیواره آتش به صورت مستند درآمده‌اند؟		
۷	آیا همه نقاط دسترسی به داخل شبکه محلی سازمان شناخته شده و مورد بررسی و تحلیل قرار گرفته‌اند؟		
۸	آیا یک برنامه کاری اضطراری در مورد گم شدن یا دزدیدن تجهیزات موبایل تهیه شده است؟		
۹	آیا یک برنامه کاری تفضیلی برای تعیین تلاش‌های صورت گرفته جهت نفوذ به داخل سازمان با استفاده از سیستم‌های سیستم شبکه بی‌سیم از قبیل همه اجزا شبکه بی‌سیم و تجهیزات موبایل، تهیه شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی بی سیم	بله	خیر
۱۰	آیا یک شناسایی واضح و روشن از اختیارات و ارتباطات مناسب برای شفاف سازی و تحلیل موضوعی بی‌سیم وجود دارد؟		
۱۱	آیا یک لیست کامل از همه نرم‌افزارها و سخت‌افزارهای کشف تهاجم بی‌سیم مورد توجه قرار گرفته است؟		
۱۲	آیا یک لیست کامل از همه نرم‌افزارها و سخت‌افزارهای وابسته و مربوط به سیستم بی‌سیم نوشته و ثبت شده است؟		

چک لیست شماره چهل چهار: نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پست الکترونیک

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پست الکترونیک	بله	خیر
۱	آیا استثنائات تعریف شده‌اند؟		
۲	آیا اقدامات امنیتی پست الکترونیک به طور موثر در همه کاربری‌ها اعمال می‌شود؟		
۳	آیا آئین‌نامه‌های دسترسی، حریم خصوصی، مونیتورینگ و افشا تهیه کرده‌اید؟		
۴	آیا پیام‌های رسیده، فرستاده شده و پست الکترونیک‌های داخلی آرشیو می‌شوند؟		
۵	آیا تضمینی وجود دارد که کارکنان خط مشی‌ها را درک کرده‌اند؟		
۶	آیا خط مشی‌ها و قواعد به صورت دوره‌ای مرور می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پست الکترونیک	بله	خیر
۷	آیا خط‌مشی پست الکترونیک درباره موضوعات محرمانه بودن مطالبی دارد؟		
۸	آیا خط‌مشی حفاظت در مقابل ویروس‌ها برای شناسایی پست الکترونیک‌ها و ضمیمه‌های پست الکترونیک مظنون برقرار شده است؟		
۹	آیا خط‌مشی کاربری موثر پست الکترونیک برقرار شده است؟		
۱۰	آیا خط‌مشی‌ای که پیوست‌های نامه‌ها را محدود نماید و راهنمایی در این مورد باشد دارید؟		
۱۱	آیا دارایی‌های فرهنگی محافظت می‌شوند؟		
۱۲	آیا دسترسی داشتن به پیام‌های پست الکترونیک ذخیره شده در فولدرهای مشترک محدود به افراد مجاز می‌باشد؟		
۱۳	آیا راهنمائی مربوط به نحوه رفتار در زمینه پست الکترونیک تهیه کرده‌اید؟		
۱۴	آیا رهنمودهای کلی در زمینه کاربری پست الکترونیک برای استفاده در کسب و کار سازمان ارائه شده است؟		
۱۵	آیا رهنمودهایی در زمینه ذخیره یا پاک‌کردن پیام‌ها دارید؟		
۱۶	آیا سوابق پست الکترونیک را می‌توان به صورت کم هزینه تولید کرد؟		
۱۷	آیا کارکنان درباره خط مشی‌ها آموزش دیده‌اند؟		
۱۸	آیا کارکنان مسئول گذرواژه‌هایشان برای بازکردن نرم‌افزار پست		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پست الکترونیک	بله	خیر
	الکترونیک می‌باشند؟		
۱۹	آیا محتواهای مهم پست الکترونیک‌ها ذخیره می‌شوند؟		
۲۰	آیا محتوای پست الکترونیک مهم محافظت می‌شوند؟		
۲۱	آیا محتوای پست الکترونیکی حساس به طور دوره‌ای پاک می‌شوند؟		
۲۲	آیا نقش‌ها و مسئولیت‌های کاربران نهایی و کارکنان فنی تعریف شده‌اند؟		

چک لیست شماره چهل پنج: نقاط ضعف و آسیب‌پذیری حوزه پست صوتی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پست صوتی	بله	خیر
۱	آیا خط‌مشی صندوق صوتی سازمان منجر به استفاده مناسب و جریمه برای سوءاستفاده شده است؟		
۲	آیا خط‌مشی‌ای برای پست صوتی وجود دارد؟		
۳	آیا خط‌مشی‌ای برای صندوق صوتی سازمان و نحوه استفاده ازآن ایجاد شده و به وسیله همه کارمندان امضا شده است؟		
۴	آیا روش‌های کنترل تغییرات به طور رسمی ایجاد شده است؟		
۵	آیا روندی برای جلوگیری از آشکار شدن گذرواژه‌های پست صوتی به		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پست صوتی	بله	خیر
	عمل آمده است؟ (مثلا با استفاده از یک شماره اضافی)		
۶	آیا سیاست‌ها و توافقات کارمندان در مورد فواید صندوق صوتی سازمان و نظارت‌های قانونی آماده انجام می‌باشد؟		
۷	آیا یک خط‌مشی تعیین گذرواژه ایجاد شده است؟		

چک لیست شماره چهل شش: نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پشتیبان گیری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پشتیبان گیری	بله	خیر
۱	آیا برآوردی از حجم پشتیبان گیری‌ای که مورد نیاز است دارید؟		
۲	آیا برای روش‌های ذخیره‌سازی گوناگون وسایل مختلفی در نظر گرفته شده است؟ (مثلاً برای ذخیره کوتاه مدت از نوار و برای ذخیره بلندمدت از دیسک‌های نوری استفاده شود)؟		
۳	آیا برای نیازهای پشتیبان گیری گیری بودجه‌ای پیش‌بینی شده است؟		
۴	آیا برای وضعیت‌های بازیابی معمولی یا ناشی از حوادث ناگوار یک طرح بازیابی دارید؟		
۵	آیا به کلیه پرسنل تجهیزات پشتیبان‌گیری گوشزد شده است که اطلاعاتی که با آن سر و کار دارند محرمانه می‌باشد؟		
۶	آیا تناقضات میان نسخه‌های سیستم /فایل جدیدتر با قدیمی در زمانی‌که بازیابی پشتیبان گیری مورد نیاز می‌شود شناسایی شده است؟		
۷	آیا جهت حفاظت از اسناد طبقه‌بندی شده یا سوابق حیاتی یک طرح امنیتی دارید؟		
۸	آیا خط‌مشی ذخیره‌سازی فایل جهت به حداکثر رسانی اثربخشی پشتیبان گیری و به حداقل رسانی کپی‌برداری موجود است ؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پشتیبان گیری	بله	خیر
۹	آیا درطرح بازیابی جزئیات مشخصی در مورد ترتیب بازیابی وجود دارد؟		
۱۰	آیا دستورالعمل‌های مکتوب که مسئولیت‌های کاربران را در قبال گرفتن پشتیبان از فایل‌هایشان مشخص نماید موجود است ؟		
۱۱	آیا روندها و استانداردهای پشتیبان گیری جهت مرور به تمام پرسنل مربوط ارسال شده است؟		
۱۲	آیا فضای مناسب برای پشتیبان گیری کوتاه مدت تا بلند مدت تدارک شده است؟		
۱۳	آیا کل اسناد سیستم پشتیبان گیری در زمانی‌که مورد استفاده نمی‌باشند در جای امنی نگهداری می‌شوند؟		
۱۴	آیا مراحل و دستورالعمل‌های بازیابی موقعیت‌های مکانی سرورهای خاص فایل‌های مربوط را که بایستی بازیابی شوند (در صورت یک نقض امنیتی که منجر به ازبین رفتن خیلی از داده‌ها می‌شود) را مشخص کرده‌اند؟		
۱۵	آیا نرم‌افزار قوی و مناسب پشتیبان گیری بر اساس قابل اعتماد بودن فروشنده، سهولت کاربری، وغیره انتخاب شده است؟		
۱۶	آیا همه پرسنلی که پشتیبان گیری‌ها را انجام می‌دهند به طور مناسب آموزش دیده‌اند؟		
۱۷	آیا همه کاربران سیار از موقعیت‌های سرور پشتیبان گیری و زمان‌بندی‌ها آگاهی دارند تا بتوانند داده‌هایشان را در شبکه جهت پشتیبان گیری ذخیره نمایند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی پشتیبان گیری	بله	خیر
۱۸	آیا یک خط‌مشی روشن در زمینه نوع اطلاعاتی که به صورت محلی پشتیبان گیری می‌شود در مقابل اطلاعاتی که به‌صورت غیرمحلی ذخیره می‌شوند وجود دارد؟ (مثلا پشتیبان گیری‌های روزانه محلی، و پشتیبان گیری‌های هفتگی/ ماهانه غیر محلی؟		
۱۹	آیا یک راه‌حل برون‌سپاری موردنظر می‌باشد؟		
۲۰	آیا یک طرح برقراری ارتباط جهت فایل‌هایی که نیازمند بازیابی سریع می‌باشند موجود است ؟		

چک لیست شماره چهل هفت: نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی تعیین کلمات عبور اجباری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی‌های تعیین کلمات عبور اجباری	بله	خیر
۱	آیا اقدامات انضباطی برای تخلف در به اشتراک گذاشتن گذرواژه در نظر گرفته شده است؟		
۲	آیا برای سوءاستفاده از گذرواژه‌ها مجازات قانونی وضع شده است؟		
۳	آیا قوانین مدیریت گذرواژه ازنقطه نظر انطباق با سیاست‌ها آزمایش شده است؟		
۴	آیا کارمندان جواب‌گوی حفاظت و مدیریت گذرواژه‌های خودشان هستند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی‌های تعیین کلمات عبور اجباری	بله	خیر
۵	آیا کارمندان در مورد روش‌های امنیت IT و استفاده از گذرواژه به طور مناسب آموزش دیده‌اند؟		
۶	آیا کارمندان در مورد میزان مطالبی که در مورد خط‌مشی‌های گذرواژه باید بدانند مورد آزمایش و امتحان قرار گرفته‌اند؟		

چک لیست شماره چهل هشت: نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی عمومی (ضد ویروسی)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی عمومی (ضد ویروسی)	بله	خیر
۱	آیا خط‌مشی امنیتی آن‌چه را که توسط راه‌حل ضد ویروسی محافظت می‌شود را منعکس می‌کند و این که چرا چنین می‌کند را نشان می‌دهد؟		
۲	آیا خط‌مشی امنیتی برای نرم‌افزار ضد ویروس به وضوح مشخص می‌نماید که کدام موارد فایل‌های ضمیمه‌ای پست‌های الکترونیک مناسب بوده و کدام بایستی فیل‌تر شوند؟		
۳	آیا خط‌مشی ضد ویروس با سیاست‌های استفاده قابل قبول اینترنت و پست الکترونیکی سازمان هم‌خوانی دارد؟		
۴	آیا خط‌مشی ضد ویروس، زمانی که تهدیدات مربوط به مسائل ضد		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی عمومی (ضد ویروسی)	بله	خیر
	ویروس تغییر می‌کنند به طور مرتب به‌روز می‌شود؟		
۵	آیا روال‌های به منظور استفاده مداوم از راه‌حل‌ها و خدمات ضد ویروسی در سازمان وجود دارد؟		
۶	آیا کلیه اطلاعات و داده‌های گرفته‌شده از منابع بیرونی غیرقابل اعتماد تلقی می‌شوند؟		
۷	آیا گزینش و فراهم ساختن خدمات / محصولات ضد ویروسی یک کار مدیریتی است؟		
۸	آیا مدیریت سطح بالا از این موضوع آگاهی داردکه حفاظت ضد ویروسی علاوه بر فن‌آوری شامل آگاهی کاربر، سیاست‌گذاری‌ها و استانداردها نیز می‌شود؟		
۹	آیا همه کارکنان خط‌مشی امنیتی سازمان را که مربوط به امنیت ضد ویروس می‌باشد خوانده و فهمیده‌اند؟		
۱۰	آیا یک خط‌مشی ضد ویروسی که به امضا کلیه کارکنان مربوط رسیده باشد موجود است؟		

چک لیست شماره چهل نه: نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی کاربران (کارمندان)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی کاربران (کارمندان)	بله	خیر
۱	اگر استفاده از نرم‌افزارهای شخصی مجاز دانسته شده است آیا کارکنان بایستی لیسانس نرم‌افزار را نشان داده و حقوق کپی‌رایت را رعایت کنند؟		
۲	آیا استانداردهای اخلاقی برای رفتارهای کسب وکاری عنوان شده است؟		
۳	آیا اطلاعات مربوط به تماس‌های اضطراری به سهولت در دسترس می‌باشد؟		
۴	آیا افراد از نصب کردن نرم‌افزارهای شخصی بر روی تجهیزات سازمان منع شده‌اند؟		
۵	آیا برای همه روشن و واضح است که چه کسی مسئول شکایات و وادار کردن است؟		
۶	آیا برخورد با نرم‌افزارهای نوشته شده در سازمان برطبق خط‌مشی‌های مصوب است؟		
۷	آیا پرسنل بخش حقوقی و نیروی انسانی چک کردن خط‌مشی‌های و روال‌های راهبردی را انجام می‌دهند؟		
۸	آیا خط‌مشی‌های راهبردی به طور دوره‌ای به روز آوری و بازبینی می‌شوند؟		
۹	آیا خط‌مشی‌های نرم‌افزاری تصویب شده در دست دارید؟		
۱۰	آیا خط‌مشی‌هایی برای ارتباط با مراجع قانونی وقضایی وجود دارد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی کاربران (کارمندان)	بله	خیر
۱۱	آیا خط‌مشی‌هایی برای بررسی موارد و موضوعات مختلف وجود دارد؟		
۱۲	آیا خط‌مشی‌هایی برای بررسی و رسیدگی به تبعیض‌ها ایجاد شده است؟		
۱۳	آیا خط‌مشی‌هایی برای تبیین و حل موارد ناسازگاری و اختلافات تدوین شده است؟		
۱۴	آیا دفاتر مربوط به وقایع ثبت شده‌اند؟		
۱۵	آیا راهبردهای هدایت رفتاری قرارداده شده‌اند؟		
۱۶	آیا راهبردهایی برای نحوه برخورد با موارد مرتبط با افشا/ گمنامی وجود دارد؟		
۱۷	آیا روال‌ها و خط مشی‌ها به وسیله کارمندان به خوبی درک شده‌اند؟		
۱۸	آیا روال‌هایی برای بررسی خسارت‌های وارده بر دارایی‌ها و اموال سازمان وجود دارد؟		
۱۹	آیا روال‌هایی برای بررسی موارد ناسازگاری و اختلافات کارکنان با سرپرستان و مسئولین بخش‌های مختلف سازمان در نظر گرفته شده است؟		
۲۰	آیا روال‌هایی برای پی آمده‌ای رفتار نامناسب مدون شده است؟		
۲۱	آیا روال‌هایی برای شکایت وجود دارد؟		
۲۲	آیا طرف‌های ثالث نیز از استانداردهای سازمان و این که از آن‌ها انتظار		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی کاربران (کارمندان)	بله	خیر
	دارند که این استانداردها را رعایت کنند آگاهی دارند؟		
۲۳	آیا قبل از نصب هرگونه نرم‌افزار جدید ارائه توجیهات لازم الزامی است؟		
۲۴	آیا کارکنان از نصب و دانلود کردن نرم‌افزارها با منبع‌های ناشناخته منع شده‌اند؟		
۲۵	آیا کارمندان از قرض دادن نرم‌افزار به غیرکارمندان منع شده‌اند؟		
۲۶	آیا کارمندان از کپی گرفتن از نرم‌افزارها به‌دلیل قانون کپی‌رایت، منع شده‌اند؟		
۲۷	آیا کارمندان از نصب یا دانلود کردن نرم‌افزار بر روی تجهیزات سازمان منع شده‌اند؟		
۲۸	آیا کارمندان مطالب آموزش داده شده را همان‌طور که انتظار می‌رفت درک کرده‌اند؟		
۲۹	آیا محدودیت‌هایی برای تحریم و قدغن کردن مواد غیرمجاز یا قاچاق تعیین شده است؟		
۳۰	آیا مراجع بازرسی سازمان مسئول پیگیری تخلفات می‌باشند؟		
۳۱	آیا هیچ راهنمایی برای بررسی رفتارهای نامناسب کارمندان وجود دارد؟		
۳۲	آیا وقایع و حوادث ثبت می‌شوند؟		
۳۴	آیاخط‌مشی‌هایی برای بررسی و رسیدگی به سوءاستفاده یا بدرفتاری		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه خط‌مشی کاربران (کارمندان)	بله	خیر
	لفظی وجود دارد؟		

چک لیست شماره پنجاه: نقاط ضعف و آسیب‌پذیری حوزه دسترسی بی سیم

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه دسترسی بی سیم	بله	خیر
۱	آیا برای داده‌های امن و بسیار محرمانه، عبور و مرور آن‌ها در شبکه با استفاده از یک مانیتور شبکه مورد پیگیری قرار می‌گیرد؟		
۲	آیا برای رمزنگاری شبکه/ انتقال داده‌ها، پروتکل تونل زدن و رمزکننده‌ها مورداستفاده قرار گرفته است؟		
۳	آیا به منظور دسترسی فایل‌های شبکه، به‌جای استفاده ازنرم‌افزاری که از قبل روی ایستگاه کاری را ه دور کاربر یا لب‌تاپ کاربر بارگذاری شده، از SSL VPN استفاده می‌شود؟		
۴	آیا دسترسی‌های بی‌سیم به داخل مسیریاب‌ها از طریق یک پورت خاص انجام می‌شود؟		
۵	آیا روش‌های تصدیق و احراز هویت مناسب مثل کلید مشترک، SSL login،VPN، EAP و غیره وجود دارد؟		
۶	آیا روش‌های کنترل دسترسی مناسب مثل MAC ACLs،۸۰۲.۱X، SSL portal،WEP و فیل‌تر کردن IP و غیره وجود دارد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه دسترسی بی سیم	بله	خیر
۷	آیا روند ورود به داخل سیستم امنیتی مناسب و روش‌های رمزنگاری متناسبی برای دسترسی VPN به کار گرفته شده است؟		
۸	آیا سطح قوی‌تری از دسترسی ایمنی برای منابع شبکه‌ای حساس خارجی مثل VPN وجود دارد؟		
۹	آیا لازم است سیستم‌های احراز هویت / احراز اصالت اضافی برای نقاط دسترسی خاص در نظر گرفته شود؟		
۱۰	آیا یک بازبینی از سطوح امنیتی دسترسی برای همه کاربران و گروه‌هایی که به داخل شبکه بی‌سیم دسترسی دارند انجام شده است؟		
۱۱	آیا یک بازبینی از کاربرانی که دارای امتیازات مدیریت شبکه اجزا بی‌سیم می‌باشند، انجام گرفته است؟		
۱۲	آیا یک خط‌مشی کلمه عبور مناسب برای همه سخت‌افزارها و نرم‌افزارهای بی‌سیم به کار گرفته شده، وجود دارد؟		
۱۳	در صورت استفاده از WEP آیا ارتقا آن از ۴۰ بیت به ۱۲۸ بیت برای ایمنی بیش‌تر مدنظر قرار گرفته است؟		
۱۴	در مورد رمزنگاری داده‌های موجود در لایه لینک ارتباطی، آیا برای ایمنی بیش‌تر از دسترسی حفاظت شده Fi-Wi استفاده شده است؟		

چک لیست شماره پنجاه یک: نقاط ضعف و آسیب‌پذیری حوزه دستگاه‌های قابل حمل

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه دستگاه‌های قابل حمل	بله	خیر
۱	آیا امنیت نرم‌افزاری مناسب خدمات پیام‌رسانی فوری را نیز شامل می‌شود؟		
۲	آیا اندازه‌گیری‌های امنیتی برای دستگاه‌های موبایل که به طور موقت به شبکه داخلی وصل می‌شوند و پروتکل‌های امنیتی بی‌سیم را به کار نمی‌گیرند انجام می‌شود؟		
۳	آیا بررسی‌هایی در این مورد انجام شده است که روش‌های امنیتی بی‌سیم بر روی طول عمر باتری دستگاه موبایل به علت زیاد بودن حجم پردازش آن‌ها تأثیر منفی نداشته باشند؟		
۴	آیا به کارمندان اجازه داده نشده است موبایل‌های شخصی خود را به محیط شبکه سازمان متصل نمایند؟		
۵	آیا دسترسی بی‌سیم به همه اطلاعات مهم موجود بر روی سرور سازمان از طریق وب و VPN فقط به صورت دسترسی خواندنی می‌باشد؟		
۶	آیا دستگاه‌های موبایل پروتکل‌های امنیتی بی‌سیم فعلی و آینده مربوط به محیط سازمان را پشتیبانی می‌کنند؟		
۷	آیا دستگاه‌های موبایل دارای روند حفاظت خاص خودشان به منظور جلوگیری از دسترسی غیرمجاز وسایل بی سیمی می‌باشند؟		
۸	آیا فقط دستگاه‌های موبایل مربوط به فروشندگان شناخته شده که دارای سطوح امنیتی ذاتی یا اضافی مناسبی می‌باشند، مورد استفاده قرار می‌گیرند؟		
۹	آیا مدارک و مستندات حساس مورد بررسی قرار می‌گیرند که در صورت		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه دستگاه‌های قابل حمل	بله	خیر
	امکان بر روی موبایل‌ها ذخیره نشوند؟		
۱۰	آیا همه دستگاه‌های بی‌سیم موجود قادرند به یک نقطه دسترسی بی‌سیم که نیازمند انتشار SSID/WAP نیست متصل شوند؟		
۱۱	آیا همه دستگاه‌های موبایل دارای روال‌های محافظت در برابر ویروس، دیواره آتش شخصی و انواع متداول کدهای مخرب می‌باشند؟		
۱۲	آیا همه کاربران موبایل در مورد خودداری از ذخیره هر گونه اطلاعات اختصاصی سازمان مثل اطلاعات محرمانه، رمزهای شبکه، اطلاعات کارمندان و غیره بر روی تجهیزات موبایل آگاهی یافته‌اند؟		

چک لیست شماره پنجاه دو: نقاط ضعف و آسیب‌پذیری حوزه دغدغه‌های عملیاتی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه دغدغه‌های عملیاتی	بله	خیر
۱	آیا اقدامات ضد آتش‌سوزی انجام شده است؟		
۲	آیا بازرسی‌های آتش‌نشانی به طور دوره‌ای اجرا می‌شود؟		
۳	آیا تعداد رایانه‌ها و دیگر امکانات وتجهیزاتی که از یک پریز استفاده می‌کنند کنترل می‌شود؟		
۴	آیا جنس موادی که برای ساخت درها، پنجره‌ها و قفل‌ها به‌کارگرفته شده از لحاظ استحکام و پایداری چک شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه دغدغه‌های عملیاتی	بله	خیر
۵	آیا درهای اضافی داخل ساختمان کامپیوتر مجهز به قفل‌های فقط خروج و زنگ خطرهای رسا می‌باشند؟		
۶	آیا دیوارها و پنجره‌های اتاق کامپیوتر دسترسی افراد غیرمجاز را محدود می‌کنند؟		
۷	آیا روشنایی کافی به ویژه در نواحی حساس وجود دارد؟		
۸	آیا ساختار کلی دیواره‌های درونی طراحی صوتی دارند؟		
۹	آیا سیستم‌های تهویه مطبوع به خوبی تعمیر و نگهداری می‌شود؟		
۱۰	آیا سیم‌کشی تلفن یا شبکه محلی ازدید آشکار با حفاظ پوشیده می‌باشد؟		
۱۱	آیا سیم‌ها طوری نصب شده‌اند که در معرض کشش فیزیکی قرار نگیرند؟		
۱۲	آیا کف مقداری از سطح زمین بلندتر می‌باشد اگر چنین است ارتفاع مناسب می‌باشد؟		
۱۳	آیا کلیه رایانه‌ها به محافظ‌های افزایش آمپر برق مجهز می‌باشند؟		
۱۴	آیا لوله‌های کاملاً محافظت شده برای سیم‌کشی شبکه استفاده شده است؟		
۱۵	آیا لوله‌های کاملاً محافظت شده برای سیم‌کشی محل استفاده شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه دغدغه‌های عملیاتی	بله	خیر
۱۶	آیا محیط محلی حفاظت کافی در برابر مشکلات برق، ناآرامی‌های مدنی و حوادث طبیعی فراهم می‌آورد؟		
۱۷	آیا نگهبان برای ساختمان و فضای دفتری دارید؟		
۱۸	آیا نیاز به یک منبع برق غیرقابل قطع هرچند وقت یک‌بار چک شده و به‌روز می‌شود؟		

چک لیست شماره پنجاه سه: نقاط ضعف و آسیب‌پذیری حوزه راهبری و مدیریت شبکه

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه راهبری و مدیریت شبکه	بله	خیر
۱	آیا امور مربوط به مدیریت دیواره آتش فقط از طریق یک ایستگاه کاری مجاز و به صورت رمز شده و یا از طریق کنسول دیواره آتش انجام می‌شود؟		
۲	آیا تمامی تغییر و تحول پرسنل و کاربرها به دقت در قواعد دسترسی دیواره آتش و مستندات مدیریت در هنگام مناسب منعکس می‌شود؟		
۳	آیا کار پرسنل مرتبط با دیواره آتش توسط همکاران مرور و بررسی می‌شود؟		
۴	آیا کلیه پرسنل مرتبط با دیواره آتش بر اساس اصل حداقل دسترسی کار می‌کنند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه راهبری و مدیریت شبکه	بله	خیر
۵	آیا گذرواژه‌های دیواره آتش‌ها به طور دوره‌ای نیازمند عوض شدن می‌باشند؟		
۶	آیا گذرواژه‌های دیواره آتش‌ها به قدر کافی پیچیده و طولانی می‌باشند؟		
۷	آیا مولفه‌های دیواره آتش به طور مستمر با آخرین وصله‌ها و نسخه‌ها به‌روز می‌شوند؟		
۸	آیا همه پرسنل دیواره آتش مجاز و مورد اطمینان می‌باشند؟		
۹	آیا همه پرسنل مرتبط با دیواره آتش فرم‌های مناسب توافق‌نامه کارمندان را امضا کرده‌اند؟		

چک لیست شماره پنجاه چهار: نقاط ضعف و آسیب‌پذیری حوزه رسانه‌های پشتیبان گیری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری رسانه‌های پشتیبان گیری	بله	خیر
۱	آیا برچسب‌های مناسبی که نام سرور، فایل‌ها وتاریخ پشتیبان گیری‌ها را نشان دهد روی آن‌ها نصب است؟		
۲	آیا بررسی‌های مرتب از رسانه‌های مختلف به عمل می‌آید تا مواردی از قبیل هزینه، آسانی ذخیره‌سازی، طول عمر فن‌آوری، رونده‌ای فعلی و آتی، طول عمر و غیره مورد بررسی قرار گیرند؟		
۳	آیا تعداد مناسبی رسانه بر اساس حجم نیازمندی‌های پشتیبان گیری حال و آینده که در خط‌مشی پشتیبان گیری معین شده خریداری گردیده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری رسانه‌های پشتیبان گیری	بله	خیر
۴	آیا جهت خرید اقسام رسانه‌های پشتیبان گیر، فروشنده‌های موثق با گارانتی مناسب مد نظر قرار می‌گیرند؟		
۵	آیا رسانه‌ها به طور مرتب چک می‌شوند تا صحت داده‌های آن‌ها مشخص شود؟		
۶	آیا رسانه‌ها در یک اتاق که به طور مجزا کنترل شود در درون محوطه امن نگهداری می‌شود؟		
۷	آیا رسانه‌ها در یک صندوق امن ضد آتش نگهداری می‌شوند؟		
۸	آیا ساماندهی رسانه‌ها به طور مناسب و هوشمندانه به‌جهت تسهیل دسترسی و بازیابی صورت گرفته است؟		
۹	آیا یک لیست کامل از کلیه رسانه‌ها، فایل‌ها و غیره تجهیزات پشتیبان گیری گرفته شده است؟		
۱۰	برای رسانه‌های ذخیره شده که به پایان عمر خود می‌رسند آیا طرحی دارید که داده‌های پشتیبان گیری آن‌ها به روی رسانه‌های دیگر انتقال داده شود؟		

چک لیست شماره پنجاه پنج: نقاط ضعف و آسیب‌پذیری حوزه رسانه‌های ذخیره‌سازی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه رسانه‌های ذخیره‌سازی	بله	خیر
۱	آگر اطلاعاتی از روی رسانه پاک می‌شود آیا کلیه گام‌های لازم برای کسب اطمینان از این که همه اطلاعات به طور مناسب پاک شده‌اند و هیچ باقیمانده‌ای بر جای نمانده است برداشته می‌شود؟		
۲	آیا از شرکت‌های پستی مورد اطمینان جهت حمل و نقل رسانه‌های مورد استفاده در سازمان استفاده می‌شود؟		
۳	آیا از ظرف‌های ویژه یا ضد دست‌کاری ذخیره برای داده‌های خیلی حساس یا حیاتی روی رسانه استفاده می‌شود؟		
۴	آیا بسته‌بندی رسانه به‌قدرکافی رسانه را از آسیب فیزیکی حفظ می‌کند؟		
۵	آیا به‌طور مرتب با فروشندگان رسانه‌ها ارتباط برقرار می‌شود تا این اطمینان حاصل شود که آخرین اطلاعات در مورد رسانه‌های موجود همواره در اختیار مدیران سازمان قرار دارند؟		
۶	آیا توزیع رسانه با رعایت حداقل جابه‌جائی با ثبت مناسب ورود و خروج انجام می‌شود؟		
۷	آیا جهت استفاده اطلاعات حساس از رسانه‌های دارای مکانیزم غیرقابل نوشتن استفاده می‌شود؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه رسانه‌های ذخیره‌سازی	بله	خیر
۸	آیا رسانه‌های ذخیره شده به طور منطقی ذخیره شده‌اند تا سهولت دسترسی و بازیافت اطلاعات تأمین شده باشد؟		
۹	آیا رونده‌ای واضح و روشنی برای خرید و دور ریزی رسانه موجود است ؟		
۱۰	آیا سابقه بازرسی برای ردگیری خریدها، مکان استقرار و روند منفک‌سازی رسانه‌ها تهیه کرده‌اید؟		
۱۱	آیا فهرست رسانه‌های جداشدنی به طور مرتب برای اعمال تغییرات، دورریزی و غیره بر روی رسانه مورد بررسی قرار می‌گیرد؟		
۱۲	آیا مناطق ذخیره رسانه دارای مکانیزم‌های قفلی مناسب برای ایجاد دسترسی کنترل شده می‌باشند؟		
۱۳	آیا منطقه در نظر گرفته شده برای ذخیره رسانه محل مناسب و محافظت شده‌ای در برابر خسارات محیطی می‌باشد؟		
۱۴	آیا منفک‌سازی رسانه توسط یک فرد مجاز در داخل سازمان اجرا می‌شود؟		
۱۵	آیا همه رسانه‌ها با برچسب‌ها و اطلاعات مربوط مورد شناسایی قرار گرفته‌اند؟		
۱۶	آیا یک روندی تکنولوژیکی جهت حرکت از رسانه‌های قدیمی به‌سوی رسانه‌های جدید موجود است ؟		
۱۷	آیا یک فهرست کامل از رسانه‌های جداشدنی دارید؟		
۱۸	آیا یک لیست کامل از تمام فروشندگان رسانه‌های مورد استفاده در		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه رسانه‌های ذخیره‌سازی	بله	خیر
	سازمان موجود است ؟		

چک لیست شماره پنجاه شش: نقاط ضعف و آسیب‌پذیری حوزه رونده‌ای پشتیبان گیری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه رونده‌ای پشتیبان گیری	بله	خیر
۱	اگر فایل‌هایی پشتیبان گیری نشده باشند آیا روندهایی دارید که به این موضوع رسیدگی شده و پشتیبان گیری گرفته شود؟		
۲	آیا اطلاعاتی که بایستی پشتیبان گیری شوند به صورت اطلاعاتی که برخی بایستی به طور کامل، برخی به صورت فقط تغییرات داده شده و برخی به صورت تکه‌ای پشتیبان گیری شوند، طبقه‌بندی شده‌اند؟		
۳	آیا به‌طور دوره‌ای لیست پشتیبان گیری‌ها مرور می‌شوند تا این اطمینان حاصل شود که هیچ فایل یا برنامه‌کاربردی از قلم نیفتاده است ؟		
۴	آیا پشتیبان گیری‌ها در طول زمان بیکاری رایانه زمان‌بندی شده‌اند ؟		
۵	آیا پشتیبان گیری‌های مربوط به کل سازمان به‌صورت سالانه / سه‌ماهه/ و غیره زمان‌بندی شده‌اند؟		
۶	آیا روندهایی برای ارسال مرتب و دوره‌ای ادوات پشتیبان گیری به یک محل دیگر برای ذخیره موجود است ؟		
۷	آیا زمان‌های پشتیبان گیری به قدر کافی از یک‌دیگر فاصله دارند		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه رونده‌ای پشتیبان گیری	بله	خیر
	به‌طوری‌که هیچ تداخلی میان جداول زمان‌بندی پشتیبان گیری نباشد؟		
۸	آیا سیستم پشتیبان گیری بر اساس زمان‌بندی تنظیم شده اجرا می‌شود (مثلاًپشتیبان گیری کامل هفتگی، فایل‌های متغیر روزانه و غیره)؟		
۹	آیا لاگ پشتیبان گیری‌ها به طور مرتب چک می‌شوند تا از کامل بودن آن‌ها اطمینان حاصل شود؟		
۱۰	آیا لاگ پشتیبان گیری‌ها به نحوی تنظیم شده است که رونده‌ای پشتیبان گیری داده‌ها شامل کلیه سرورها، حجم‌ها، مکان فایل‌ها و مسیر فایل‌ها باشد؟		
۱۱	آیا یک برنامه زمان‌بندی شده مفصل جهت پشتیبان گیری دارید؟		
۱۲	آیا یک تست واقعی بازیابی، اجرا و مرور شده است تا بدین‌وسیله میزان موثر بودن و در زمان مناسب به‌کار آمدن آن ثابت شود؟		
۱۳	آیا یک جدول چرخشی وسایل رسانه‌ای برای پشتیبان گیری‌ها تنظیم شده و رعایت می‌شود؟		
۱۴	آیا یک طرح انتقال و مهاجرت برای جابه‌جا کردن داده‌ها به روی ادوات جدید در مواقع لزوم آماده کرده‌اید؟		
۱۵	آیا یک لیست اولویت‌بندی به‌منظور شناسایی اطلاعاتی که نیازمند قرارگیری در ادوات پشتیبان گیری می‌باشند موجود است ؟		

چک لیست شماره پنجاه هفت: نقاط ضعف و آسیب‌پذیری حوزه سازگار بودن محتوا

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سازگار بودن محتوا	بله	خیر
۱	آیا اقداماتی برای ایمن‌سازی محتوای پست الکترونیک انجام داده‌اید؟		
۲	آیا اقدامی در جهت تخفیف مسئولیت نقض قوانین مربوط به محتوا صورت گرفته است؟		
۳	آیا اقدامی در جهت تضمین آن‌که خط‌مشی‌های نگهداری پیغام رعایت می‌شود صورت گرفته است؟		
۴	آیا پست الکترونیک‌ها برای جلوگیری از محتوای ممنوع مونیتور می‌شوند؟		
۵	آیا خط‌مشی پست الکترونیکی سازمان و محدودیت‌های محتوایی ضمانت اجرایی دارند؟		
۶	آیا محتوای پست الکترونیک‌ها برای جلوگیری از نشر مطالب محرمانه مونیتور می‌شوند؟		
۷	آیا محتوای پست الکترونیک‌ها به لحاظ هتاکی مونیتور می‌شوند؟		
۸	آیا محتوای پست الکترونیک‌ها دسته‌بندی، مونیتور و فیل‌تر می‌شوند؟		

چک لیست شماره پنجاه هشت: نقاط ضعف و آسیب‌پذیری حوزه سخت افزار شبکه

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سخت افزار شبکه	بله	خیر

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سخت افزار شبکه	بله	خیر
۱	آیا اتصال چند شبکه محلی LAN از طریق سخت افزار، مورد بازبینی و بازرسی قرار گرفته است ؟		
۲	آیا حفاظت فیزیکی کافی از رسانه‌ها و وسایل فیزیکی شبکه محلی LAN وجود دارد؟		
۳	آیا در رابطه با قابلیت‌های امنیتی سخت افزار خریداری شده برای شبکه محلی LAN بررسی مناسب انجام شده است؟		
۴	آیا روترها به‌طور صحیحی ترکیب بندی شده‌اند تا شبکه‌های محلی را از یک‌دیگر جدا نموده و در صورت امکان دسترسی‌های مشخصی را بلوکه نمایند؟ (مثلا اجازه دسترسی را فقط از طریق یک‌سری آدرس‌های IP خاص بدهند)		
۵	آیا سخت افزار شبکه محلی LAN در محل امنی به منظور جلوگیری از دسترسی غیر مجاز واقع شده است ؟		
۶	آیا شبکه‌های محلی متصل شده به هاب یا روتر متفاوت، به طور مجزا از هم می‌باشند؟		
۷	آیا کاربران راه دور برای دسترسی به شبکه باید ترکیبی از کلمه عبور و نام کاربری را وارد کنند؟		
۸	آیا کنترل‌های امنیتی مناسب بر روی سخت افزار به منظور جلوگیری از ترکیب بندی مجدد تجهیزات قرار داده شده است؟		
۹	ایا مودم‌هایی که اتصال کاربران به شبکه محلی LAN را فراهم می‌کنند حفاظت اضافی دارند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سخت افزار شبکه	بله	خیر
۱۰	آیا هاب / پورت به کار رفته برای دسترسی خارجی به وسیله کلمه عبور به‌طور مناسبی امن شده است؟		

چک لیست شماره پنجاه نه: نقاط ضعف و آسیب‌پذیری حوزه سرور FTP

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سرور FTP	بله	خیر
۱	اگر دسترسی ناشناس نیست، آیا احتیاطات امنیتی نام کاربری/ گذرواژه مناسب جهت دسترسی کاربر در نظر گرفته شده است (غیرفعال کردن حساب پس از ۳ الی ۵ اقدام به ورود ناموفق و غیره) ؟		
۲	آیا احتیاط لازم برای تضمین آن‌که سرور FTP برای استفاده در دسترسی به فایل سیستم‌های سازمان به‌کار نمی‌رود به عمل آورده‌اید؟		
۳	آیا برای جلسات FTP رمزی سازی در نظر گرفته‌اید تا از تغییر دادن مکرر نام کاربر و گذرواژه اجتناب شود؟		
۴	آیا به‌عنوان یک اقدام امنیتی نحوه دسترسی به FTP را فقط محدود به دسترسی از طریق VPN نموده‌اید ؟		
۵	آیا دسترسی از طریق سرور FTP محدود شده است و دسترسی ناشناس غیرفعال شده است؟		
۶	آیا سرور FTP در یک ناحیه غیرنظامی دور از سرور(های) اصلی سازمان قرار دارد؟		
۷	آیا سرور FTP طوری پیکربندی گردیده است که تنها اجازه ایجاد		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سرور FTP	بله	خیر
	ارتباط به منظور ارسال یا دریافت اطلاعات فقط با IP هایی ممکن باشد که جزو ارتباطات مجاز باشند؟		
۸	آیا کلیه بارگزاری‌ها و وصله‌های سیستم FTP به‌روز می‌باشند؟		
۹	آیا گروه‌ها و کاربرانی که از سرور FTP استفاده می‌کنند از نظر امنیتی مورد بررسی قرار می‌گیرند؟		
۱۰	آیا نرم‌افزار امنیتی خاصی برای سرور FTP خریداری و نصب گردیده است؟		
۱۱	آیا همه فولدرهای روی سرور FTP دسترسی محدود دارند؟		

چک لیست شماره شصت: نقاط ضعف و آسیب‌پذیری حوزه سرورهای عمومی پایگاه داده

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سرورهای عمومی پایگاه داده	بله	خیر
۱	اگر از پایگاه داده خارج از سایت استفاده می‌شود آیا روند پشتیبان گیری مرتب و منظمی از داده‌های موجود سیستم درحال کار بر روی سیستم پشتیبان اجرا می‌شود؟		
۲	اگر تکنیک‌های رمزنگاری استفاده می‌شود، آیا اثرات آن بر عمل‌کرد پردازش‌گر مورد بررسی قرار گرفته است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سرورهای عمومی پایگاه داده	بله	خیر
۳	آیا آزمایش تزریق کدهای SQL جهت جلوگیری از دنباله‌های داده‌ای غیرمجاز چندگانه اجرا شده است؟		
۴	آیا آزمایشی برای بررسی استنتاج مستقیم و غیرمستقیم که ممکن است به نواحی امن پایگاه داده دسترسی یابد اجرا شده است؟		
۵	آیا بر روی همه سرورها پشتیبان‌ها و فایل‌های بروز رسانی لازم را از فروشنده‌ها تهیه ونصب شده‌اند؟		
۶	آیا برای داده‌های بسیار حساس، رمزنگاری داده‌های داخل جدول، سطر یا ستون مدنظر قرار گرفته است؟		
۷	آیا برای دسترسی به سرور پایگاه داده، نیاز به نام کاربری و ورود به سیستم می‌باشد؟		
۸	آیا بسته پایگاه داده‌ای انتخاب شده دارای طرح‌های دسترسی و مجازسازی کاملاً امن می‌باشد؟		
۹	آیا به طور مرتب گذرواژه کاربر عوض شده است؟		
۱۰	آیا پایگاه داده خارج از سایت دارای همان سطوح امنیتی است که سیستم درحال کار دارا می‌باشد؟		
۱۱	آیا تحقیقی در زمینه کرم‌های پایگاه داده و نحوه مبارزه با آن‌ها انجام شده است؟		
۱۲	آیا جا دادن داده‌های خیلی مهم و حساس به طور جداگانه بر روی یک		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سرورهای عمومی پایگاه داده	بله	خیر
	سرور بسیار امن مورد بررسی قرار گرفته است؟		
۱۳	آیا در میان مدیران شبکه پایگاه داده یک مدیر امنیتی پایگاه داده منصوب شده‌است؟		
۱۴	آیا در هنگام انتقال داده‌ها از/ به سرورهای پایگاه داده رمزنگاری مدنظر قرار گرفته است؟		
۱۵	آیا دفتر ثبت وقایع به طور مرتب برای دسترسی‌های غیرمجاز یا اعمال غیرمجاز مرور می‌شود؟		
۱۶	آیا روش‌های تفکیک جداول پایگاه داده برای جداسازی دسترسی جدول داده امن از دسترسی‌های جدول داده غیرامن به‌کار می‌روند؟		
۱۷	آیا رونده‌ای امنیتی پایگاه داده‌ای توسط کلیه مدیران شبکه مرور شده است؟		
۱۸	آیا روی سیستم پایگاه داده آزمایشی همان سیستم غربال‌گری امنیتی که روی سیستم درحال کار اجرا می‌شود، انجام می‌شود؟		
۱۹	آیا سرورهای پایگاه داده در یک ناحیه امن جای داده شده‌اند؟		
۲۰	آیا طرح بازیابی از نظر زمان، کیفیت و غیره آزمایش شده است؟		
۲۱	آیا طرح بازیابی برای سناریوهای خرابی پایگاه داده موجود است ؟		
۲۲	آیا فرمان‌های دسترسی پایگاه داده مورد بررسی قرار گرفته است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سرورهای عمومی پایگاه داده	بله	خیر
۲۳	آیا فهرستی از کاربرانی که به سرورهای پایگاه داده دسترسی دارند دراختیار دارید؟		
۲۴	آیا کلیه دیدگاه‌ها مورد بررسی قرار گرفته‌اند تا اطمینان حاصل شود که تنها داده‌های مناسب نمایش داده می‌شوند و دسترسی جهت دیدن داده‌های خیلی خیلی حساس، محدود شده است؟		
۲۵	آیا کنترل‌های دقیق در میان محیط تستی و سیستم‌های پایگاه داده در حال کار وجود دارد؟		
۲۶	آیا مرور کافی از دسترسی و مجوزهای کلیه کاربران پایگاه داده صورت گرفته است؟		
۲۷	آیا مکانی جهت پایگاه داده خارج از سایت موردنظر قرار گرفته است؟		
۲۸	آیا ناحیه سرور پایگاه داده دارای تجهیزات و روندهای اضطراری می‌باشد؟		
۲۹	آیا نام کاربری پیش‌فرض اصلی را عوض کرده‌اید؟		
۳۰	آیا نسخه‌های امنیتی نرم‌افزار پایگاه داده به طور مرتب مورد تجدید نظر قرار می‌گیرند؟		
۳۱	آیا همه مدیران شبکه پایگاه داده دارای مهارت کافی برای انجام کارهای محوله می‌باشند؟		
۳۲	آیا یک LAN پشتیبان برای دسترسی به پایگاه داده در هنگام ازکار		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سرورهای عمومی پایگاه داده	بله	خیر
	افتادن LAN اصلی دارید؟		
۳۳	آیا یک بررسی مناسب از روند احراز هویت پایگاه داده انجام گرفته است؟		
۳۴	آیا یک جدول پشتیبان گیری مناسب برای کلیه پایگاه‌های داده تنظیم شده‌است؟		
۳۵	آیا یک درایو پشتیبان روی سرور پایگاه داده برای فعال کردن خاصیت mirroring اطلاعات دارید؟		
۳۶	آیا یک سرور پایگاه داده پشتیبان مجزا در اختیار دارید؟		
۳۷	آیا یک سیستم مونیتورینگ مناسب برای mirroring سرور پشتیبان دارید؟		

چک لیست شماره شصت یک: نقاط ضعف و آسیب‌پذیری حوزه سیاست گذرواژه

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیاست گذرواژه	بله	خیر
۱	آیا اختیارات و مسئولیت‌ها واگذار شده‌اند؟		
۲	آیا استثناهای مربوطه به قواعد دسترسی مستندسازی شده است؟		
۳	آیا اطلاعات مجزا شده‌اند و نیز دسترسی به نوع خاصی از داده‌ها به		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیاست گذرواژه	بله	خیر
	وسیله کلمات عبور، قابل کنترل است یا خیر؟		
۴	آیا الزامات تصدیق هویت مستند شده است؟		
۵	آیا امتیازات دسترسی‌های پیش‌فرض تنظیم شده است؟		
۶	آیا تصدیق کاربر برای انواع مختلف دسترسی لازم است؟		
۷	آیا تعهد مدیریت نسبت به سیاست‌های داخلی کنترل گذرواژه وجود دارد؟		
۸	آیا تغییرات ترکیب‌بندی امنیتی از نظر صحت و درستی مورد بازبینی قرار می‌گیرند؟		
۹	آیا تغییرات مربوط به امتیازات دسترسی‌ها ثبت می‌شود؟		
۱۰	آیا تغییرات مربوط به پروفایل‌های کاربران ثبت شده است؟		
۱۱	آیا تغییرات مربوط به پیکربندی‌های امنیتی ثبت شده است؟		
۱۲	آیا تلاش‌های اشتباه برای ورود به سیستم یا خروج از آن مورد بازبینی قرار گرفته‌اند؟		
۱۳	آیا دسترسی به شبکه به وسیله ترمینال یا آدرس IP از نظر اعتبار بررسی می‌شوند؟		
۱۴	آیا دسترسی به معاملات امنیتی کلیدی و تنظیمات ترکیب بندی کنترل شده است؟		
۱۵	آیا دسترسی خارجی به رایانه و سیستم‌های ارتباط از راه دور تحت نظر		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیاست گذرواژه	بله	خیر
	هستند؟		
۱۶	آیا دسترسی‌های موفق به منابع سیستم‌های امنیتی حیاتی ثبت شده است؟		
۱۷	آیا روال‌های سیاستی بر اساس مرجع خاصی هستند؟		
۱۸	آیا سیاست‌ها برای کنترل دسترسی‌ها به کل سیستم از طریق گذرواژه‌ها و کدهای مجاز تعیین شده‌اند؟		
۱۹	آیا سیاست‌ها بعد از تغییرات عمده در عمل‌کردها و انتصاب کارمندان، مورد بازبینی و به روزآوری قرار می‌گیرند؟		
۲۰	آیا سیاست‌های امنیتی گذرواژه بازبینی، ارزیابی و به روزآوری شده‌اند؟		
۲۱	آیا طرح، توصیه‌های پذیرفته شده توسط مدیر را که مربوط به بازبینی‌ها و ممیزی‌های امنیتی قبلی گذرواژه می‌باشد، نشان می‌دهد؟		
۲۲	آیا علاوه بر گذرواژه‌ها، معیارهای امنیتی دیگری مثل کارت‌های هوشمند مورد استفاده قرار می‌گیرند؟		
۲۳	آیا فعالیت‌های کاربران دارای امتیاز ویژه مورد بررسی قرار می‌گیرد؟		
۲۴	آیا مجازات تنبیهی برای نقض خط‌مشی گذرواژه در نظر گرفته شده است؟		
۲۵	آیا مستندات و وقایع ثبت شده به منظور اطمینان از این که فقط به افراد مجاز دسترسی‌های مناسب اعطا شده است، مورد بازبینی قرار می‌گیرند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیاست گذرواژه	بله	خیر
۲۶	آیا موارد استثنایی قوانین، مستندسازی شده‌اند؟		

چک لیست شماره شصت دو: نقاط ضعف و آسیب‌پذیری حوزه سیستم عامل NT/WIN ۲ K

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیستم عامل NT/WIN ۲ K	بله	خیر
۱	آیا از داده‌های وضعیت سیستم کنترل کننده دامنه هر روز پشتیبان گرفته می‌شود یا خیر؟		
۲	آیا ایمنی گروه‌های عمومی برای جلوگیری از دسترسی‌های غیرمجاز به فایل‌های سیستمی و غیره مورد بررسی قرار می‌گیرد؟		
۳	آیا با استفاده از ابزارخط مشی ممیزی، استفاده از امتیازات کاربر برای تشخیص نقایص مورد بررسی قرار می‌گیرد؟		
۴	آیا با استفاده از ابزارخط مشی ممیزی، دسترسی به فایل و اشیا برای بررسی موارد موفق و ناموفق مورد بررسی قرار می‌گیرند ؟		
۵	آیا با استفاده از ابزارخط مشی ممیزی، کل وقایع سیستم به منظور ممیزی خرابی‌ها مورد بررسی قرار می‌گیرد؟		
۶	آیا با استفاده از ابزارخط مشی ممیزی، موارد موفق و ناموفق پیگیری روندها مورد بررسی قرار می‌گیرند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیستم عامل NT/WIN ۲ K	بله	خیر
۷	آیا با استفاده از ابزارخط مشی ممیزی، موارد موفق و ناموفق تغییرات سیاست امنیتی مورد ممیزی قرار می‌گیرند؟		
۸	آیا با استفاده از ابزارخط مشی ممیزی، موارد موفق و ناموفق شروع مجدد،خاموش کردن کامپیوتر و سیستم مورد ممیزی قرار می‌گیرند؟		
۹	آیا با استفاده از ابزارخط مشی ممیزی، موارد موفق و ناموفق کاربر و گروه مدیریتی مورد ممیزی قرار می‌گیرند؟		
۱۰	آیا با استفاده از ابزارخط مشی ممیزی، ورود به سیستم و خروج از سیستم برای بررسی موارد موفق و ناموفق مورد ممیزی قرار می‌گیرند؟		
۱۱	آیا با استفاده از مدیر مسئول امنیتی، بازبینی جامعی از پروفایل‌های کاربران و گروه‌ها انجام شده است تا اطمینان حاصل شود هیچ‌گونه دسترسی غیر مجازی وجود نداشته باشد؟		
۱۲	آیا بازبینی جامع و فراگیری از بخش‌های مختلف دیسک انجام شده است تا از صحت سازماندهی فایل‌های سیستمی اطمینان حاصل شود؟		
۱۳	آیا بازبینی جامعی از ارتباطات حوزه‌ها انجام شده است؟		
۱۴	آیا بازبینی جامعی از گروه‌ها و کاربران درون گروه‌ها انجام شده است؟		
۱۵	آیا پروفایل‌های امنیتی موجود در حوزه‌های مورد اعتماد مورد بررسی قرار گرفته‌اند؟		
۱۶	آیا تا به حال به صورت آزمایشی انتقال کنترل کننده‌های دامنه ثانویه به دامنه اصلی به منظور تعیین نقص‌های کنترلرهای اصلی مورد آزمایش		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیستم عامل NT/WIN ۲ K	بله	خیر
	قرار گرفته است؟		
۱۷	آیا حق دسترسی به کامپیوتر از طریق شبکه از روی سروروب فقط به کاربران مدیریتی مناسب محدود شده است؟		
۱۸	آیا خطمشی‌های کاربران محلی در برابر عمل‌کرد مناسب کاربر از قبیل مدیریت سیستم، خاموش کردن، پشتیبان گیری و غیره مورد بررسی قرار می‌گیرد؟		
۱۹	آیا دسترسی از راه دور به سرور در صورتی که نیاز نباشد غیرفعال می‌شود؟		
۲۰	آیا دسترسی به حساب مهمان تا زمانی که نیاز به فعال شدن داشته باشد غیرفعال است؟		
۲۱	آیا دیسک‌های تعمیر و بازیابی اضطراری، به‌طور مناسبی نگهداری شده‌اند؟		
۲۲	آیا سرور در ابتدا از روی دیسک سخت بوت می‌شود و سپس از روی درایو فلاپی یا سی دی و ترتیب بوت شدن در بایاس سیستم تعبیه شده است؟		
۲۳	آیا سطح مناسبی درخط مشی ممیزی به منظور جلوگیری یا گرفتن دسترسی غیرمجاز قرار داده شده است؟		
۲۴	آیا فایل‌های سیستمی REGEDIT۳۲. EXE از کلیه ایستگاه‌های کاری حذف شده است تا سیستم عامل ایستگاه کاری محلی را در برابر آسیب		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیستم عامل NT/WIN ۲ K	بله	خیر
	و خسارت محافظت شوند؟		
۲۵	آیا فلاپی درایورها در صورتی که امکان شیوع ویروس‌ها یا اشکالات از طریق نصب نرم افزار روی فلاپی دیسک وجود داشته باشند از کار می‌افتد و غیرفعال می‌شوند؟		
۲۶	آیا کلمه عبور بایاس برای جلوگیری از تغییر یافتن ترتیب بوت شدن سیستم یا سایر بخش‌ها تنظیم شده است؟		
۲۷	آیا گزینه RUN (اجرا) در منوی file برای ایستگاه‌های کاری کاربر غیرفعال است؟		
۲۸	آیا مجوزهای مناسبی بر روی فایل‌های سیستمی با عنوان REGEDIT۳۲. EXE فقط برای دسترسی‌ها مجاز قرار داده شده است؟		
۲۹	آیا مدت زمان‌های تنظیم شده در لاگ های رخداد، سیستم و برنامه کاربردی به منظور جلوگیری از نوشتن مجدد بر روی داده‌های قبلی به اندازه کافی طولانی هستند؟		
۳۰	آیا نمادها و نمایش دهنده‌های ثبت وقایع از قبیل لاگ های رخداد، سیستم و برنامه کاربردی فعال شده‌اند؟		
۳۱	برای هر یک از عمل‌کردها مانند مدیریت لاگ ها، مدیریت سیستم، خاموش کردن، پشتیبان گیری و غیره آیا دسترسی‌های مجاز کاربران و گروه‌ها مورد بررسی قرار گرفته است؟		

چک لیست شماره شصت سه: نقاط ضعف و آسیب‌پذیری حوزه سیستم عامل UNIX

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیستم عامل UNIX	بله	خیر
۱	(sbin/ ،root/، der/ ،tmp، /usr/ bin/ etc/)		
۲	اگر ابرکاربر به طور موقت نیاز به مجوز دسترسی به دایرکتوری یا فایل داشته باشد، بعد از این که نیاز وی برطرف شد، آیا مجوز او لغو می‌شود؟		
۳	آیا اسکریپت های موجود طوری تنظیم شده‌اند که به‌طور اتوماتیک صحت داده‌های وارد شده درpasword/etc/ را چک نمایند و همچنین مجوزهای روی فایل‌های سیستم را چک می‌کنند؟		
۴	آیا با کمک دستور cron زمانبدی منظمی به منظور کپی کردن فایل‌های ثبت شده امنیتی در یک فضای جداگانه برای بازبینی انجام گرفته است ؟		
۵	آیا بازبینی از فایل passwd/etc به منظور اطمینان از این که کاربران به گروه‌های مناسب خود و مسیر پیش‌فرض مناسب نسبت داده شده‌اند یا خیر انجام شده است؟		
۶	آیا بازبینی از مجوزهای موجود در دایرکتوری‌های سیستم انجام گرفته است؟		
۷	آیا بازبینی منظمی از فایل‌ها و دایرکتوریها به منظور تعیین دسترسی غیرمجاز کاربر یا گروه انجام گرفته است؟		
۸	آیا در صورت امکان گزینه‌هایی مثل اجرا در سطوح فوق‌العاده امنیتی در		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه سیستم عامل UNIX	بله	خیر
	نسخه Unix موجود هستند؟		
۹	آیا رمزنگاری قوی برای کلمات عبور مورد استفاده قرار گرفته است؟		
۱۰	آیا رویه‌هایی به منظور مشکل‌تر کردن و ایمن‌تر کردن سیستم‌عامل از وضعیت پیش‌فرض آن بعد از نصب تعیین شده‌اند؟		
۱۱	آیا کلمه عبور ابرکاربر به طور مرتب تغییر می‌یابد؟		
۱۲	آیا گزینه‌هایی مثل شناسه‌های تصادفی فعال شده‌اند؟		
۱۳	آیا مخفی کردن کلمات عبور فعال شده است؟		
۱۴	آیا مکانیزم‌های به منظور محدود کردن مقدار منابعی که برای کاربر قابل استفاده است قرارداده شده‌اند؟		
۱۵	آیا نقشه تفضیلی از گروه‌های کاربری دارای دسترسی به جزئیات دایرکتوری‌های سیستم‌عامل وجود دارد؟		
۱۶	آیا همه‌ی مجوزهای قبلی در صورتیکه به دلیل یک ویرایش موقت تغییر یافته باشند، در دایرکتوری‌ها یا فایل‌ها دوباره بازیابی می‌شوند؟		

چک لیست شماره شصت چهار: نقاط ضعف و آسیب‌پذیری حوزه شناسایی و احراز هویت

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه شناسایی و احراز هویت	بله	خیر

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه شناسایی و احراز هویت	بله	خیر
۱	آیا استفاده از مکانیزم‌های خاص (کارت‌های هوشمند، بیومتریک وغیره) به خاطر آسیب‌پذیری‌های مکانیزم‌های دارای کلمه عبور مورد توجه قرارگرفته است؟		
۲	آیا برای امنیت بیش‌تر، رمزکردن به وسیله کلیدهای کاربری یکتا مورد توجه قرار گرفته است؟		
۳	آیا برای ورود به سیستم‌های از راه دور سطح ایمنی اضافی به کار گرفته می‌شود؟		
۴	آیا خط‌مشی شبکه محلی LAN به منظور تعیین نوع اطلاعاتی که بین سرورها مبادله خواهند شد وجود دارد؟		
۵	آیا خط‌مشی‌ای وجود دارد که تعیین کند کدام کاربران به کدام شبکه‌ها دسترسی داشته باشند؟		
۶	آیا دسترسی شبکه محلی LAN از دست‌یابی‌های غیر مجاز با استفاده از پایان دادن به ارتباط بعد از چند ورود ناموفق محافظت می‌شود؟		
۷	آیا دسترسی شبکه محلی LAN تحت نظارت و پایش جهت آگاهی از آخرین ورود موفق به سیستم و تعداد ورودهای ناموفق می‌شود ؟		
۸	آیا دسترسی مدیر شبکه محلی LAN به منظور شناخت کاربران واقعی مورد بازبینی قرار گرفته است ؟		
۹	آیا مدیریت کلمه عبور وجود دارد، مخصوصاً در جائی که خط‌مشی شبکه محلی LAN تعیین می‌کند که تنها سیستم‌های کلمه عبوردار قابل قبول هستند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه شناسایی و احراز هویت	بله	خیر
۱۰	آیا مکانیزم قفل شدن برای تجهیزاتی که نیاز به تصدیق کاربردارد مورد توجه قرار گرفته است؟		
۱۱	آیا نقشه کاربری مرتبط با دسترسی شبکه محلی LAN وجود دارد که به طور مرتب بازبینی شده باشد؟		

چک لیست شماره شصت پنج: نقاط ضعف و آسیب‌پذیری حوزه صحت و درستی پیام و تاریخ

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه صحت و درستی پیام و تاریخ	بله	خیر
۱	آیا احراز هویت فایل‌ها (نرم افرار و غیره) با استفاده از امضاهای رمز شده مثل توابع درهم ساز MD۵ مورد بررسی قرار گرفته است؟		
۲	آیا استفاده از امضاهای دیجیتالی کلید عمومی مورد بررسی قرار گرفته است؟		
۳	آیا استفاده از امضاهای دیجیتالی مبتنی بر کلید امن مورد توجه قرار گرفته است ؟		
۴	آیا با به کار گیری سیستم کنترل تغییر، از تغییرات تصادفی (ناخواسته) داده‌ها یا فایل‌ها جلوگیری شده است؟		
۵	آیا حفاظت مناسبی برای کپی‌های پشتیبان وجود دارد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه صحت و درستی پیام و تاریخ	بله	خیر
۶	آیا فن‌آوری مناسبی برای رمزنگاری پیام و فایل مورد استفاده قرار گرفته است ؟		

چک لیست شماره شصت شش: نقاط ضعف و آسیب‌پذیری حوزه ضمانت اجرایی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه ضمانت اجرایی	بله	خیر
۱	آیا بازدیدهای از پیش اعلام نشده در ساعات شیفت‌های غیراصلی جهت بررسی این که رونده‌ای کنترل دسترسی به خوبی رعایت می‌شود، صورت می‌گیرد؟		
۲	آیا برآوردهای مستقل بیرونی یا بررسی‌های بازرسی بیرونی در نظر گرفته می‌شود؟		
۳	آیا محیط امنیتی فیزیکی به طور مرتبط بررسی می‌شود؟		

چک لیست شماره شصت هفت: نقاط ضعف و آسیب‌پذیری حوزه فرآیند توسعه نرم افزاری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محیط توسعه نرم افزاری	بله	خیر
۱	اگر برنامه‌های خارجی مورد استفاده قرار گرفته شوند، آیا سطح مناسبی		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محیط توسعه نرم افزاری	بله	خیر
	از احراز هویت و رمزنگاری وجود دارد؟		
۲	اگر توسعه خارج از سایت انجام شود، آیا ارتباط بین سایت راه دور و سرور اصلی به صورت رمزشده و امن است؟		
۳	آیا بررسی‌های مداوم و بازبینی وقایع ثبت شده به صورت به جا و به موقع اتفاق می‌افتد؟		
۴	آیا برنامه تشخیص نفوذ و پاسخ‌گویی به آن‌ها، قابلیت دسترسی به منابع و تغییرات سیستم که ممکن است در هنگام جابه‌جایی و تعویض امکانات استفاده شوند را مورد توجه قرارداده است؟		
۵	آیا توسعه دهندگان نرم‌افزار یک شناسه دسترسی یکتا برای ورود به محیط تولید / توسعه دارند؟		
۶	آیا روش‌های تصدیق موجود به صورت دوره‌ای برای بررسی میزان انعطاف آن‌ها مورد تست قرار می‌گیرند؟		
۷	آیا عمل ورود به سیستم کاربر دارای یک تابع پایان زمان کار که نشان دهنده تمام شدن وقت می‌باشد، است؟		
۸	آیا فرآیندی به منظور اعطای دسترسی موقت به هر یک از کارمندان پشتیبانی کننده که در حین اجرای نرم‌افزار جدید نیازمند دسترسی به سیستم باشند، وجود دارد؟		
۹	آیا فردی که در حال برقراری و برآوردن نیازهای امنیتی است، دارای گواهی‌نامه مناسب، زمینه یا آموزش مناسب می‌باشد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محیط توسعه نرم افزاری	بله	خیر
۱۰	آیا کاربران یاد گرفته‌اند که چگونه وضعیت مشکوک شبکه را در محیط توسعه یافته گزارش دهند؟		
۱۱	آیا کتابخانه نرم‌افزار دارای کنترل دسترسی مناسب می‌باشد؟		
۱۲	آیا محیط توسعه بخش‌بندی شده یا به صورت فیزیکی از زیرساخت مشترک سازمان مجزا شده است؟		
۱۳	آیا نام کاربر/ کلمه‌های عبور واگذار شده به گروه طراحی و توسعه، نگهداری شده و به صورت منظم مورد بازبینی مداوم قرار می‌گیرد؟		
۱۴	آیا نرم‌افزار کنترل امنیتی، بررسی‌های مداوم و ثبت فعالیت‌ها را به طور مناسب با هم می‌آمیزد؟		
۱۵	در هنگام توسعه نرم‌افزاری آیا نیازهای امنیتی تعیین شده‌اند؟		

چک لیست شماره شصت هشت: نقاط ضعف و آسیب‌پذیری حوزه کاربردهای سرور وب

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کاربردهای سرور وب	بله	خیر
۱	آیا ابزارهای امنیتی برای تحت نظر گرفتن فعالیت سرور وب مورد استفاده قرار می‌گیرند؟		
۲	آیا اطلاعات سرور وب و سیستم عامل از دید عموم مخفی شده‌اند؟		
۳	آیا اطلاعات/ داده‌های در حال انتقال بین سرور وب و جست‌جوگر به		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کاربردهای سرور وب	بله	خیر
	طور مناسب و کافی حفاظت می‌شود؟		
۴	آیا به روز شدن‌های امنیتی به محض این که در دسترس قرار بگیرند بر روی سرور وب اعمال می‌شوند؟		
۵	آیا پروتکل‌های انتقال شبکه که مورد استفاده قرار نمی‌گیرند،غیر فعال شده‌اند؟		
۶	آیا پشتیبان‌های سرور وب هنگامی که یک حادثه امنیتی ناگوار روی داده باشد، به طور مرتب مورد آزمایش قرار می‌گیرند؟		
۷	آیا حساب دسترسی پیش فرض مدیرشبکه به منظور جلوگیری از سوءاستفاده یا حمله به سرور تغییر نام داده شده است؟		
۸	آیا دایرکتوری FTP بی‌نام از شبکه داخلی مجزا شده است؟		
۹	آیا روابط مطمئنی در مدل دامنه تعیین شده است؟		
۱۰	آیا سرور وب در طرح‌های بازیابی حوادث فاجعه آمیز دیده شده است؟		
۱۱	آیا سرورهای تولید و توسعه در پشت دیواره‌آتش سازمان قرار دارند؟		
۱۲	آیا سرورهای شبکه که فقط مختص اطلاعات هستند در خارج از دیواره آتش سازمان قرار دارند؟		
۱۳	آیا سرورهای وب حساس یا حیاتی به طور مناسب به وسیله دیواره آتش پوشیده شده‌اند؟		
۱۴	آیا سرورهای وب طوری تنظیم شده‌اند که اسکریپت های CGI را فقط		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کاربردهای سرور وب	بله	خیر
	به وسیله کاربران مجاز بتوان به آن‌ها اضافه نمود؟		
۱۵	آیا قابلیت‌های جست‌جوی دایرکتوری بر روی پوشه‌ها غیرفعال شده است؟		
۱۶	آیا کنترل‌های امنیتی ایجاد شده برای خدمات دسترسی از راه دور، برای ایجاد تغییرات در سرور وب مورد استفاده قرار گرفته‌اند؟		
۱۷	آیا لیست‌های کنترل دسترسی فهرست‌بندی و ایجاد شده‌اند؟		
۱۸	آیا همه داده‌های مقیم روی سرور وب بر اساس میزان حساسیت رده‌بندی شده‌اند؟		
۱۹	آیا وقایع امنیتی ثبت شده برای همه سرورهای وب نگهداری شده و بر اساس یک برنامه منظم آزمایش می‌شوند؟		

چک لیست شماره شصت نه: نقاط ضعف و آسیب‌پذیری حوزه کاربردهای عمومی وب

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کاربردهای عمومی وب	بله	خیر
۱	آیا انتشار اطلاعات طبقه بندی شده سازمان ممنوع بوده و در برنامه‌های کاربردی و سایت اینترنتی سازمان قرار داده نمی‌شوند؟		
۲	آیا دسترسی به کاربردهای وب تنها به کاربران و پرسنل مناسب محدود شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کاربردهای عمومی وب	بله	خیر
۳	آیا زمان‌های اتمام جلسه پیاده‌سازی و اجرا شده است؟		
۴	آیا عمل ورود به شبکه ازخارج سازمان جهت دسترسی به نرم‌افزارهای کاربردی وب تحت نظر قرار گرفته است؟		
۵	آیا کاربردهای وب داده‌های کاربر را تائید می‌کنند؟		
۶	آیا کنترل‌های دسترسی قرارداده شده برای کاربران بر اساس نیازهای کاری فردی و سیاست سازمانی در نظر گرفته شده‌اند؟		
۷	آیا وقایع ثبت شده از ورود به شبکه ازخارج سازمان، نگهداری و تحلیل می‌شوند؟		

چک لیست شماره هفتاد: نقاط ضعف و آسیب‌پذیری حوزه کارکنان: کنترل‌های دسترسی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کارکنان: کنترل‌های دسترسی	بله	خیر
۱	آیا اقدامات خاصی جهت شناسایی هویت مثبت صورت گرفته است؟		
۲	آیا برای کنترل ورود و خروج‌ها بسته‌ها به نواحی ممنوعه سیستمی دارید؟		
۳	آیا برای ملاقات کنندگان از محل رایانه‌ها برچسب سینه و ثبت‌نام به‌عمل می‌آید؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کارکنان: کنترل‌های دسترسی	بله	خیر
۴	آیا برچسب‌ها و گذر کدها عاری از نام و لوگوی سازمان می‌باشد؟		
۵	آیا برچسب‌های سینه و مجوز عبورها بررسی می‌شوند؟		
۶	آیا به کارکنان در زمینه گزارش اشیا گمشده، دخول غیر مجاز و دیگر حوادث می‌توان اطمینان کرد؟		
۷	آیا ترتیباتی برای مقابله با خشونت اتخاذ شده است؟		
۸	آیا تنها پرسنل مجاز به ورود به مکان‌هایی که در آن‌ها امکانات و تجهیزات قرار دارند می‌باشند که مسئولیت و دانش مربوط را داشته باشند؟		
۹	آیا ثبت ورود و خروج‌ها مکرر بررسی می‌شود؟		
۱۰	آیا حمل کیف و کوله‌پشتی به نواحی امن کنترل می‌شود؟		
۱۱	آیا رفتار غیرعادی مثل ورود پرسنل شیفت روز در ساعت بعد از شیفت مورد بررسی قرار می‌گیرد؟		
۱۲	آیا روندهایی برای کلیدهای مفقودی یا دزدیده شده دارید؟		
۱۳	آیا سوابق پرسنلی که مسئولیت‌های کلیدی امنیتی دارند بررسی شده است؟		
۱۴	آیا سیاست‌هایی دارید که از اموال سازمان در مقابل خسارت‌های وارده از سوی کارمندان منفصل از خدمت محافظت شود؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کارکنان: کنترل‌های دسترسی	بله	خیر
۱۵	آیا شماره سریال کلیدهای کارتی به افراد نسبت داده شده و ثبت شده است؟		
۱۶	آیا عکس پرسنل روی کلید کارتی دیده می‌شود؟		
۱۷	آیا کلیدهای کارتی به طور دوره‌ای عوض شد یا دوباره برنامه‌ریزی می‌شوند؟		
۱۸	آیا کلیدهای کارتی عاریتی دارید و نحوه استفاده از آن‌ها ردگیری می‌شود؟		
۱۹	آیا کلیدهای کارتی که در اختیار کارکنان سابق بوده، بلافاصله از کار انداخته شده‌اند؟		
۲۰	آیا کلیدهای کارتی گوناگونی برای سطوح امنیتی مختلف وجود دارد؟		
۲۱	آیا کلیدهای مفقودی سریعاً اعلام می‌شوند؟		
۲۲	آیا کلیه افرادی که دارای کلیدهای دسترسی در همه اوقات می‌باشند شناسایی شده‌اند؟		
۲۳	آیا لیست افرادی که حق دسترسی دارند به طور مکرر بررسی می‌شود تا معلوم شود کلیه افراد هنوز کارکنان مجاز می‌باشند؟		
۲۴	آیا مسئولیت‌های امنیتی و بازداشتی به متصدی‌های آن محول شده است؟		
۲۵	آیا هشدار دهنده امنیتی ویژه برای ورود به یک ناحیه امن یا اقدام به		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کارکنان: کنترل‌های دسترسی	بله	خیر
	ورود غیرمجاز به منطقه امن دارید؟		
۲۶	آیا هشدار دهنده ویژه برای اقدام به استفاده غیرمجاز از امکانات وتجهیزات با کارت‌خوان وجود دارد؟		
۲۷	آیا هویت پرسنلی که از کلید کارتی استفاده می‌کنند توسط نرم‌افزار امنیتی ضبط می‌شود؟		
۲۸	آیا ورود دوربین‌های موبایل و دیجیتال به مراکز ممنوعه قدغن می‌باشد؟		
۲۹	برای مناطقی که دسترسی کلید کارتی دارند آیا مناطق مشترک در طول ساعات قفل می‌باشد؟		
۳۰	در زمان‌های مناسب آیا کیف افراد در هنگام ورود و خروج بازرسی می‌شود؟		
۳۱	وقتی کار با یک کارمند به اتمام می‌رسد آیا بلافاصله به بیرون محوطه همراهی می‌شود؟		
۳۲	وقتی کار با یک کارمند تمام می‌شود آیا کلیه حقوق دسترسی بلافاصله ملغی می‌گردد؟		

چک لیست شماره هفتاد یک: نقاط ضعف و آسیب‌پذیری حوزه کپی کردن

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کپی کردن	بله	خیر
۱	اگر فروشنده‌ای اجازه تهیه کپی پشتیبان را پیشاپیش نداده باشد آیا کارکنان رضایت او را قبل از این کار جلب می‌کنند؟		
۲	اگر مجوز برای کاربران چندگانه باشد آیا تعداد مجاز از کپی تهیه می‌شود؟		
۳	آیا از رایانه خارج از شبکه برای تهیه کپی جهت توزیع استفاده می‌شود؟		
۴	آیا از نرم‌افزارهای کپی‌رایت شده به تعداد مجوز داده شده کپی گرفته می‌شود؟		
۵	آیا توزیع نرم‌افزار از طریق دفتر ثبت وقایع کنترل می‌شود؟		
۶	آیا فقط مدیای نو برای کپی کردن نرم‌افزار برای ذخیره پشتیبان و توزیع به‌کار می‌رود؟		
۷	آیا یک کپی پشتیبان از همه نرم‌افزارهای جدید گرفته شده است؟		
۸	قبل از تهیه کپی پشتیبان، آیا نسخه اصلی آن‌ها غیرقابل نوشتن می‌باشند؟		
۹	هنگام کپی‌کردن نرم‌افزار جهت توزیع یا پشتیبان آیا از ایستگاه‌های کاری با دسترسی باز پرهیز می‌شود؟		

چک لیست شماره هفتاد دو: نقاط ضعف و آسیب‌پذیری حوزه کنترل‌های خارج از سایت

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کنترل‌های خارج از سایت	بله	خیر
۱	آیا پشتیبان‌ها و مدیای آرشیو شده به طور امن ذخیره شده‌اند؟		
۲	آیا ناحیه ذخیره مدیاها نیازهای پناهگاه معمول، جعبه‌های نگهداری یا پناهگاه الکترونیک را برآورده می‌کند؟		
۳	آیا نیازهای امنیتی انبار خارج از محوطه از طریق به‌کارگیری نگهبان، مونیتورهای تلویزیونی، نظارت طرف ثالث، سیستم‌های امنیتی خودکار برآورده می‌شوند؟		
۴	در مورد طرح‌های بازیابی پس از حوادث آیا پرسنل کلیدی، مقامات مسئول و روندها مستند شده‌اند؟		
۵	در مورد طرح‌های بازیابی پس از حوادث، آیا تمرینی اجرا کرده‌اید که بازیافت و به‌کارگیری مجدد پشتیبان‌ها را نشان دهد؟		

چک لیست شماره هفتاد سه: نقاط ضعف و آسیب‌پذیری حوزه کاربران و پرسنل (صندوق صوتی)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کاربران و پرسنل (صندوق صوتی)	بله	خیر
۱	آیا کار کارمندان صندوق صوتی سازمان تحت کنترل و بازبینی قرار می‌گیرد؟		
۲	آیا همه تغییرات کارمندان و کاربران به طور دقیق در پیکربندی صندوق صوتی سازمان به موقع منعکس شده است؟		
۳	آیا همه کارمندان صندوق صوتی سازمان فرم‌های قرارداد استخدام مناسبی ر ا امضا کرده‌اند؟		
۴	آیا همه کارمندان صندوق صوتی سازمان مجاز و مورد اطمینان هستند؟		
۵	آیا همه کارمندان موافقند که استفاده از صندوق صوتی سازمان و تلفن ممکن است بعضی اوقات تحت نظر قرار بگیرد؟		

چک لیست شماره هفتاد چهار: نقاط ضعف و آسیب‌پذیری حوزه کشف و جلوگیری از تقلب

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کشف و جلوگیری از تقلب	بله	خیر
۱	آیا الگوها و خطاهای فراخوانی تحت نظارت قرار گرفته و ثبت می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کشف و جلوگیری از تقلب	بله	خیر
۲	آیا برنامه ارتباطات راه دور قادر است استفاده غیرعادی و متناقص را تحت نظارت خود قرار دهد؟		
۳	آیا حق بیمه‌ای به منظور حفاظت سازمان در برابر کلاه‌برداری و استفاده نامناسب از صندوق صوتی سازمان پرداخت شده است؟		
۴	آیا روال‌هایی برای برطرف ساختن صورت‌حساب‌های قابل اعتراض یا هزینه‌ها وجود دارد؟		
۵	آیا کنترل‌هایی به منظور جلوگیری از تغییرات غیرمجاز در نرم‌افزار و سخت‌افزار صندوق صوتی سازمان در نظر گرفته شده است؟		
۶	آیا مدیر صندوق صوتی سازمان ساختارهای صدور صورت‌حساب را درک می‌کند (مسائل مالی و حساب‌داری) و آیا قادر است اشتباهات و موارد غیر متعارف را در بازبینی ماهانه برطرف سازد؟		
۷	آیا هزینه‌های عوارض با گزارش‌های صندوق صوتی سازمان به منظور اطمینان از صحت آن‌ها مقایسه شده‌اند؟		
۸	آیا همه حساب‌های پست صوتی فهرست‌بندی شده و در دفتر ثبت شده و در برابر کاربران مجاز به منظور رفع اختلاف مورد مقایسه قرار گرفته است؟		

چک لیست شماره هفتاد پنج: نقاط ضعف و آسیب‌پذیری حوزه کلمات عبوری محافظت کننده

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کلمات عبوری محافظت کننده	بله	خیر
۱	اگر گذرواژه‌ها به صورت کتبی نوشته شده باشند، آیا دسترسی به این اسناد محافظت شده و دسترسی‌ها محدود می‌شود؟		
۲	آیا استفاده از قابلیت حفظ کردن گذرواژه‌ها در نرم‌افزارهای کاربردی ممنوع است؟		
۳	آیا تلاشی به منظور بازداشتن کاربران از آشکارسازی گذرواژه‌ها به طور غیرعمدی صورت گرفته است؟		
۴	آیا رایانه‌های شخصی طوری چیدمان شده‌اند که نفرات عبوری قادر به دیدن گذرواژه‌های تایپ شده نباشند؟		
۵	آیا عمل وارد کردن گذرواژه‌ها قابل دیدن است؟		
۶	آیا گذرواژه‌ها از فایل‌های دسته‌ای و دنباله‌های ممیزی مستثنی شده‌اند؟		
۷	آیا گذرواژه‌ها به صورت دوره‌ای برای برآوردن سیاست‌ها مورد رسیدگی قرار می‌گیرند؟		
۸	آیا گذرواژه‌ها طوری محافظت می‌شوند که هنگام وارد کردن آن‌ها در روی صفحه قابل مشاهده نباشند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کلمات عبوری محافظت کننده	بله	خیر
۹	آیا مکانیزم قفل کردن سیستم بعد از چند تلاش ناموفق برای ورود به سیستم (مثلا ۳ یا ۵ مرتبه) فعال می‌شود؟		

چک لیست شماره هفتاد شش: نقاط ضعف و آسیب‌پذیری حوزه کنترل دسترسی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کنترل دسترسی	بله	خیر
۱	آیا اتصال از راه دور به شبکه محلی LAN از نظر حفره‌های امنیتی به طور دوره‌ای مورد بررسی و بازبینی قرار می‌گیرند؟		
۲	آیا بازبینی مناسبی از دسترسی شبکه محلی LAN در مدتی که مجوزهای کاربر اجرا می‌شوند، وجود دارند؟		
۳	آیا تغییرات مربوط به کنترل دسترسی اطلاعات انجام شده است؟		
۴	آیا دستورات مشترک شبکه و فایل سیستم‌ها به منظور جلوگیری از دسترسی غیر مجاز به‌طور مناسب ترکیب بندی شده‌اند؟		
۵	آیا فلاپی درایوها در صورت نیاز به منظور جلوگیری از معرفی نرم افزارهای مورد شک (که احتمال خرابی دارند)ازکار افتاده‌اند؟		
۶	آیا کنترل‌های دسترسی به منظور جلب اطمینان کاربران از اجرای منظم کارهای آنان با به کارگیری قانون حداقل امتیاز شکل گرفته‌اند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه کنترل دسترسی	بله	خیر
۷	آیا کاربران ایستگاه کاری در برابر ذخیره فایل‌های شبکه روی درایو محلی به منظور کنترل آدرس و موضوعات پشتیبانی منع شده‌اند؟		
۷	آیا مکانیزم‌های کنترل دسترسی و حق ویژه برای محدود کردن دسترسی کاربر قرار داده شده است ؟		
۸	آیا یک سیستم تصدیق بر مبنای توکن برای تائید کاربر مورد استفاده قرار گرفته است؟		

چک لیست شماره هفتاد هفت: نقاط ضعف و آسیب‌پذیری حوزه مجموع روترها، هاب‌ها و سوئیچ

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مجموع روترها، هاب‌ها و سوئیچ	بله	خیر
۱	آیا VLANها به منظور ایزوله کردن شبکه محلی LAN شکل گرفته‌اند؟		
۲	آیا آدرس‌های روترها/سوئیچ‌ها تقریباً با محدوده آدرس IP مجاز شکل گرفته تفاوت دارند؟		
۳	آیا پورت‌های سوئیچ / روتر به‌طور مناسبی ترکیب بندی شده‌اند تا امکان اشتراک گذاری نظیر به نظیر و اجرای الگوهای حمله عدم سرویس دهی بر روی آن‌ها وجود نداشته باشد؟		
۴	آیا ثبت وقایع همراه با تعیین میزبان‌های مقصد دایر می‌باشد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مجموع روترها، هاب‌ها و سوئیچ	بله	خیر
۵	آیا دسترسی به روترها و سوئیچ‌ها بر اساس آدرس IPها ترکیب بندی شده است؟		
۶	آیا روتر و سوئیچ‌ها برای ایجاد فیلترینگ به منظور محدود کردن انتشار به کار گرفته شده‌اند؟		
۷	آیا روترها و سوئیچ‌ها به منظور جلوگیری از ترافیک، طوری تنظیم شده‌اند که پروتکل‌هایی که در شبکه محلی LAN استفاده نمی‌شوند را قبول ننمایند؟		
۸	آیا روترها و سوئیچ‌ها به‌منظور جلوگیری از حجم بالای انتشار به‌طور مناسبی ترکیب بندی شده‌اند؟		
۹	آیا سرویس‌های غیر ضروری موجود بر روی روترها و سوئیچ‌ها غیر فعال شده‌اند؟		
۱۰	آیا قابلیت "فعال کردن کلمه عبور محرمانه " در روتر، فعال شده و به صورت مناسبی ترکیب بندی شده است ؟		
۱۱	ایا کلیه واسط‌های بدون استفاده، بسته شده‌اند؟		
۱۲	آیا گواهی‌نامه‌های بکار رفته (نام کاربر و کلمه عبور) برای مدیریت روترها/سوئیچ‌ها متمایز از موارد مربوط به حساب کاربران محلی است؟		

چک لیست شماره هفتاد هشت: نقاط ضعف و آسیب‌پذیری حوزه محافظت از ویروس

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محافظت از ویروس	بله	خیر
۱	آیا اطلاعات مرتبط با حوادث و ویروس‌ها برای تمامی کاربران به اشتراک گذاشته می‌شوند؟		
۲	آیا پیام‌های پست الکترونیک بر اساس وضعیت تشخیص ویروس آن‌ها دسته بندی و مسیردهی می‌شوند؟		
۳	آیا دنباله‌های پست الکترونیک به منظور تهدیدات ویروسی در مرزهای شبکه با استفاده از موتور جست‌جوکننده مناسب، مورد بازدید و بررسی قرار می‌گیرند ؟		
۴	آیا روشی دارید که شما را در جهت محافظت در برابر ویروس‌ها به‌روز نگه دارد؟		
۵	آیا مکانیزم‌های مناسبی جهت برخورد با ویروس‌های تشخیص داده شده‌ای که قابل حدف شدن نمی‌باشند، در نظر گرفته شده است؟		

چک لیست شماره هفتاد نه: نقاط ضعف و آسیب‌پذیری حوزه محافظت در برابر هرزنامه

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محافظت در برابر هرزنامه	بله	خیر
۱	آیا بیش از یک سرور برای کنترل هرزنامه‌ها به‌کار گرفته می‌شود؟		
۲	آیا پست الکترونیک از طریق درگاه‌های چندگانه در موقعیت‌های مکانی چندگانه مسیر دهی می‌شود؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محافظت در برابر هرزنامه	بله	خیر
۳	آیا حفاظی در سطح سرور پست الکترونیک و در سطح نرم‌افزار دارید تا حملات عدم سرویس دهی را آشکار سازد؟		
۴	آیا راهی برای سفارشی کردن یا دور زدن سیاست‌ها (خط مشی‌ها) و فیل‌ترها وجود دارد؟		
۵	آیا طرحی در دسترس دارید که پست الکترونیک‌های مسئله‌دار را که از سایت‌های خاص می‌آید مدیریت کند؟		
۶	آیا نرم‌افزاری دارید که هرزنامه‌ها را شناسایی و مدیریت کند؟		
۷	آیا وسیله‌ای دارید که شما را در مقابل فن‌آوری‌های جدید هرزنامه به‌روز نگه دارد؟		
۸	آیا یک سطح آستانه تحمل برای هرزنامه‌ها در نظر گرفته‌اید؟		

چک لیست شماره هشتاد: نقاط ضعف و آسیب‌پذیری حوزه محل‌های پشتیبان گیری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محل‌های پشتیبان گیری	بله	خیر
۱	اگر از نگهبان استفاده می‌شود آیا به صورت نوبتی دور ساختمان چرخ می‌زنند؟		
۲	اگر از هیچ نگهبانی استفاده نمی‌شود آیا افرادی که مسئول امنیت می‌باشند توسط حرفه‌ای‌ها آموزش دیده‌اند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محل‌های پشتیبان گیری	بله	خیر
۳	آگر محل پشتیبان گیری در ساختمانی با چندین مستأجر قرار دارد آیا اطراف آن از امنیت کافی برخوردار است؟		
۴	آیا از ملاقات کنندگان خواسته می‌شود که با ارائه نام و رمز وارد و خارج شوند (یا ورود و خروج آن‌ها ثبت می‌شود)؟		
۵	آیا به وسیله کارت دسترسی می‌توان به مکان‌های گوناگون دسترسی داشت؟		
۶	آیا پرسنل امنیتی یا پرسنل اتاق رایانه در همه اوقات در اتاق رایانه یا در سایت حضور دارند؟		
۷	آیا چراغ‌های اضطراری در مواقع قطع برق در محل پشتیبان گیری قرار دارند؟		
۸	آیا در منطقه ملاقات موارد امنیتی در نظر گرفته شده است؟		
۹	آیا ساختمان توسط نگهبان، فنس، سیستم‌های هشدار دهنده یا مونیتورینگ مداربسته نگهبانی می‌شود؟		
۱۰	آیا سیستم ارتباطی محل پشتیبان گیری کاملاً تست شده است؟		
۱۱	آیا سیم‌کشی سیستم‌های امنیتی و هشدار دهنده از داخل لوله‌کشی حفاظتی عبور کرده است؟		
۱۲	آیا علاوه بر محوطه پشتیبان گیری یک محوطه ذخیره‌ی دور از سایت هم ایجاد شده است؟		
۱۳	آیا علائمی در بیرون برای شناساندن محل و امکانات پشتیبان گیری		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محل‌های پشتیبان گیری	بله	خیر
	نصب می‌باشد؟		
۱۴	آیا فضای مناسب جهت نیازمندی‌های فعلی و آتی پشتیبان گیری موجود است؟		
۱۵	آیا کارت شناسایی به سینه کلیه کارکنان جهت دسترسی مجاز نصب می‌باشد؟		
۱۶	آیا کلیه آزمایش‌های ایمنی که برای محوطه اصلی پشتیبان گیری انجام شده برای امکانات و محوطه خارج از محوطه اصلی هم اجرا شده است؟		
۱۷	آیا کلیه پنجره‌هایی که به بیرون راه دارند از لحاظ نفوذ سارق امنیت دارند؟		
۱۸	آیا محل پشتیبان گیری از لحاظ ضد آتش بودن، ضد آب بودن، مقاوم در برابر زلزله، ضد بخار آب و غیره مورد بررسی قرار گرفته‌اند؟		
۱۹	آیا محوطه پشتیبان گیری در فاصله مناسبی از تجهیزات و امکانات شبانه روزی امنیتی فیزیکی، پناه‌گاه ایمنی، حفاظت از آتش، سرویس پستی و دسترسی افراد مجاز قرار دارد؟		
۲۰	آیا مروری از سیستم‌های پشتیبانی اضطراری از جمله سیستم‌های محیط‌زیستی، سخت‌افزاری، سیستم‌های هشدار دهنده چه از نوع آشکار ساز و چه از نوع اطفا خطر صورت گرفته است؟		
۲۱	آیا یک فرد معین یا عده‌ای معین مسئول امنیت محل پشتیبان گیری قرار داده‌شده‌اند؟		

چک لیست شماره هشتاد یک: نقاط ضعف و آسیب‌پذیری حوزه محیط توسعه نرم افزاری

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه فرآیند توسعه نرم افزاری	بله	خیر
۱	اگر سورس برنامه قابل بررسی نباشد، آیا سایر تست‌ها برای آزمودن ضعف‌های امنیتی نرم‌افزار اجرا می‌شود؟		
۲	آیا بررسی حفاظتی مستقلی قبل از منتشر ساختن نمونه اولیه نرم افزار انجام گرفته است؟		
۳	آیا پشتیبان‌ها به صورت منظم تهیه شده و در برابر قابلیت دسترسی خارجی محافظت می‌شوند؟		
۴	آیا تغییرات اعمال شده بر روی کدهای موجود و کدهای جدید، قبل از به‌کارگیری در سیستم مورد آزمایش قرار می‌گیرند ؟		
۵	آیا خرابی‌ها و نقص‌های وابسته (مربوط) به داخل حساب (account) برده شده‌اند؟		
۶	آیا شگردها و تکنیک‌های هکرها مورد بررسی قرار گرفته و درک شده‌اند؟		
۷	آیا فرآیند کنترل تغییر در هنگام بروز کردن نرم افزار مورد استفاده قرار می‌گیرد؟		
۸	آیا فرآیندی وجود دارد که این اطمینان را فراهم آورد که رونده‌ای کنترل تغییر، باعث به خطر انداختن امنیت موجود نمی‌شوند؟		
۹	آیا فروشندگان تست‌های امنیتی برای محیط‌های توسعه برای پروژه‌های		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه فرآیند توسعه نرم افزاری	بله	خیر
	بزرگ‌تر مدنظر قرار گرفته‌اند؟		
۱۰	آیا منابع بیش‌تر به مواردی که احتمال آسیب‌پذیری شان بیش‌تر است اختصاص داده شده است؟		
۱۱	آیا نرم‌افزار کنترل تغییر می‌تواند بر اساس تکنیک‌های رمزنگاری موجود کار کند؟		
۱۲	آیا یک روند پیشرفت ثابت به منظور افزایش امنیت از طریق تقویت امنیت تکنیک‌های کدگذاری مورد توجه قرار گرفته است؟		

چک لیست شماره هشتاد دو: نقاط ضعف و آسیب‌پذیری حوزه محیط سیستم عامل

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محیط سیستم عامل	بله	خیر
۱	آیا از طرح‌های بازیابی به هنگام حادثه، طرحی را برای بازیابی سیستم عامل شامل سرپرستی بازیابی، طرح گام به گام، جایگاه نرم افزارهای پشتیبان گیری، وصله‌ها و. . . آماده دارید؟		
۲	آیا بازبینی کلی از سیستم به منظور تأیید روش‌ها برای دست‌یابی به سیستم عامل، مدیریت آن به روزآوری آن، مشخصات حساب‌ها، کلمات عبور و غیره وجود دارد؟		
۳	آیا بازبینی مجدد هدایت شده‌ای از ثبت وقایع مربوط به سیستم عامل وجود دارد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محیط سیستم عامل	بله	خیر
۴	آیا بازبینی منظمی از فروشنده‌های سیستم عامل برای اطلاعات گذشته حال و آینده موضوعات مربوط به سیستم عامل وجود دارد؟		
۵	آیا خط‌مشی کلی سیستم، برای شرح جزئیات روش‌های دست‌یابی به سیستم عامل، مدیریت، به روزآوری‌ها، مشخصات حساب‌ها، کلمات عبور، پشتیبان گیری و غیره وجود دارد؟		
۶	آیا رسانه‌های پشتیبان گیری سیستم عامل در محیط امنی به طور مناسب ذخیره شده‌اند؟		
۷	آیا رسانه‌های نصب شده در محیط امنی هستند؟		
۸	آیا روش‌های مناسب و جدیدی برای نصب/ نصب مجدد سیستم عامل شامل کلیه بسته‌های به روزآوری شده و اطلاعات برداشته شده مورد نیاز وجود دارد؟		
۹	آیا فایل‌های سیستم عامل روی یک بخش جداگانه، دیسک یا سرور بارگذاری می‌شوند؟		
۱۰	آیا فرآیندی برای بازبینی منظم کسی که دارای مجوز سطح مدیریتی است وجود دارد؟		
۱۱	آیا کلمات عبوری مدیریتی مختلفی وجود دارد؟		
۱۲	آیا کلمه‌های عبور پیش فرض مربوط به کاربران superuser و administrator را برای جلوگیری از هر نوع دسترسی داخلی و خارجی توسط افراد آشنا به کلمه‌های عبور پیش فرض، تغییر داده و ثبت می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه محیط سیستم عامل	بله	خیر
۱۳	آیا گذرواژه مدیر سیستم عامل با یک عضو ارشد مدیریت به اشتراک گذاشته می‌شود؟		
۱۴	آیا مدیر ارشد شبکه شرایط ومهارت‌های مورد نیاز برای سیستم عامل را دارا می‌باشد؟		
۱۵	آیا مستندات تهیه شده به منظور شرح جزئیات سیستم‌های عامل مختلف یا نسخه‌های متفاوت سیستم‌های عامل وجود دارد؟		
۱۶	آیا مستنداتی برای زمان‌بندی پشتیبان گیری و به روزآوری منظم سیستم / بخش‌هایی از سیستم نگه‌داشته شده است؟		
۱۷	آیا واقعه نگاری (ثبت وقایع) به منظور گرفتن رویدادهای مربوط به سیستم عامل موجود است؟		
۱۸	آیا یک طرح برگشت به قبل برای وقتی که برنامه بروزرسانی سیستم عامل با خطا مواجه شد، وجود داردتا بتواند اجرا شود و اطلاعات را برگرداند؟		

چک لیست شماره هشتاد سه: نقاط ضعف و آسیب‌پذیری حوزه مدیریت

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت	بله	خیر
۱	آیا برای ذخیره لیست‌های ضد ویروس یک زمان نگهداری تهیه شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت	بله	خیر
۲	آیا برنامه ضد ویروس، لیست مشروح رایانه‌ها و ادوات تحت مدیریت خود را تولید و تهیه می‌نماید؟		
۳	آیا کار پیکربندی پرسنل متصدی امور ضد ویروس، به منظور بالا بردن دقت مورد بازبینی و تجدید نظر قرار می‌گیرد؟		
۴	آیا کارکنان امنیت IT تیم مدیریت را درجریان تغییرات فن‌آوری ضد ویروس قرار می‌دهند؟		
۵	آیا کارکنان امنیتی می‌توانند از اسکنرهای کدهای زیان‌بار استفاده نمایند؟		
۶	آیا کلیه تغییرات در پرسنل و کاربران دقیقاً در پیکربندی ضد ویروس و به موقع لحاظ می‌شوند؟		
۷	آیا کلیه کارکنانی که در موضوعات ضد ویروسی کار می‌کنند بر اساس اصل حداقل مزایا کار می‌کنند؟		
۸	آیا نقش میز امدادهایIT جهت ردگیری، گزارش و هشدار حمله ویروسی تعریف شده است؟		

چک لیست شماره هشتاد چهار: نقاط ضعف و آسیب‌پذیری حوزه مدیریت بی سیم

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت بی سیم	بله	خیر

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت بی سیم	بله	خیر
۱	آیا ابزارهای امنیتی به منظور شناسایی دسترسی غیرمجاز به وسیله تحت نظر گرفتن آدرس‌های MAC مورد استفاده قرار گرفته‌اند؟		
۲	آیا برای هر یک از دسترسی‌های بی‌سیم یک راه حل امنیتی مناسب وجود دارد؟		
۳	آیا پروتکل‌های موجود در سخت‌افزار بی‌سیم در صورتی که مورد استفاده قرار نگیرند غیر فعال می‌شوند؟		
۴	آیا تمامی افراد و سازمان‌هایی که به نوعی در شبکه بی سیم سازمان فعال هستند، شناسائی شده و مشخصات آن‌ها در فایل‌هایی نگهداری می‌شوند ؟		
۵	آیا جدا کردن شبکه‌ها از نقاط دسترسی بی‌سیم موردتوجه قرار گرفته است؟		
۶	آیا دیواره آتش برای مسیریاب‌های بی‌سیم پیاده‌سازی و اجرا شده است؟		
۷	آیا روندی به منظور خاموش کردن مسیریاب یا یک پورت دسترسی در صورتی که دسترسی غیرمجاز به آن‌ها صورت گیرد وجود دارد؟		
۸	آیا شبکه بی‌سیم به منظور محدود کردن تعداد نقاط دسترسی، فقط به یک زیر شبکه ایزوله شده است؟		
۹	آیا شناسایی نقاط دسترسی غیرمجاز از طریق بازرسی فیزیکی انجام شده است؟		
۱۰	آیا فعالیت‌های ورود به سیستم موفق و ناموفق به منظور شناسایی همه دسترسی‌های از راه دور به داخل شبکه سازمان، بررسی و ثبت		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت بی سیم	بله	خیر
	می‌شوند؟		
۱۱	آیا فقط نرم‌افزار/ سخت‌افزار فروشندگان شناخته شده و دارای سطوح مناسبی از امنیت مورد استفاده قرار می‌گیرد؟		
۱۲	آیا لیستی از پروفایل‌های امنیتی گروه و کاربر تهیه شده است که در آن سطوح امنیتی، امتیازات دسترسی و مجوزهای از پیش تعیین شده به همه نقاط قابل دسترسی تعیین شده باشد؟		
۱۳	آیا هر محیط بی‌سیم به صورت جداگانه به شبکه با سیم با فیل‌ترهای دیواره آتش متفاوتی متصل شده و نیازمندی‌های امنیتی و کلمه عبور برای آن‌ها در نظر گرفته شده است؟		
۱۴	آیا همه افزایش‌های جدید همگی از یک خط‌مشی سازگار با زیرساخت بی سیمی موجود در سازمان پیروی می‌کنند؟		
۱۵	آیا همه کلمه‌های عبور مدیریتی پیش‌فرض به سرعت تغییر داده شده‌اند؟		
۱۶	آیا یک تست نفوذپذیری WLAN به منظور تشخیص و رفع آسیب‌پذیری‌ها انجام شده است؟		
۱۷	برای مسیریاب‌ها و سوئیچ‌های سیسکو، آیا پروتکل CDP در صورتی که مورد نیاز نباشد غیر فعال می‌شود؟		

چک لیست شماره هشتاد پنج: نقاط ضعف و آسیب‌پذیری حوزه مدیریت سیستم عامل

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت سیستم عامل	بله	خیر
۱	اگر تهیه کننده شخص ثالثی به شبکه یا فایل‌های سیستمی دسترسی پیدا کند سطوح مناسبی از ایمنی در اینجا وجود دارد؟		
۲	اگر یک سیستم پشتیبان وجود داشته باشد، امتحان کنید، در صورت بروز یک خرابی و مشکل عمدی در سیستم عامل، آیا مشکل قابل بازیابی و بهبود خواهد بود؟		
۳	آیا بازبینی از مشخصات کاربران یا گروه آن‌ها موجود است تا از این که هیچ دسترسی غیرمجازی نمی‌تواند انجام شود، اطمینان حاصل کند؟		
۳	آیا بازبینی کاملی از همه نرم افزارهای بارگزاری شده در سیستم عامل و اثرات آن در محیط سیستم عامل انجام شده است؟		
۴	آیا بازبینی منظمی از بسته‌های نرم افزاری و زمانبندی‌های استخراج شده مورد نیاز سیستم عامل وجود دارد؟		
۵	آیا بازبینی منظمی از کلمات عبوری مدیریتی به عمل می‌آید؟		
۶	آیا پشتیبان گیری فایل سیستم عامل به طور منظم انجام می‌شود؟		
۷	آیا تأثیر پروفایل امنیتی بر روی کارایی سیستم عامل برای برنامه‌های کاربردی مانند:Oracle، Sybase و غیره مورد بازبینی قرار گرفته است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت سیستم عامل	بله	خیر
۸	آیا تغییرات امنیتی خطاها و آسیب‌پذیری‌ها کشف شده به وسیله فروشنده‌های شخص ثالث ثبت و مکاتبه شده و به طور مناسب با آن‌ها برخورد شده است؟		
۹	آیا در صورت ایجاد تغییرات درمجوزهای پیش فرض فایل‌ها و شاخه‌ها درنتیجه اعمال تنظیمات موقتی، در پایان کارمجوزها به حالت قبل برمیگردند؟		
۱۰	آیا روش‌های برای مواجهه با دسترسی غیرمجاز به محیط فایل‌های سیستم عامل وجود دارد؟		
۱۱	آیا روش‌های جبران رویدادهای ناگوار مستند شده به طور رسمی برای سرورهای بسیار حساس آماده شده‌اند؟		
۱۲	آیا فایل سیستم‌ها مجوزهای مناسبی دارند؟		
۱۳	آیا فرآیند مدیریت بسته‌های نرم افزاری به منظور حذف به روزآوری‌های بسته‌ها وجود دارد تا به این ترتیب زمان را کاهش داده و فرآیند را ساده و موثر نماید؟		
۱۴	آیا کاربرانی که دارای مجوز (اختیار) مدیر هستند زمینه و آموزش لازم بر مبنای نیازهای کاری‌شان را دارند؟		
۱۵	آیا کلمات عبوری مدیریتی به طور منظم و مرتب تغییر می‌یابند؟		
۱۶	آیا مدیر سیستم دو ترکیب متفاوت از نام کاربر/ کلمه عبور دارد؟		
۱۷	آیا معیارهای امنیتی مناسبی برای اتصالات شبکه نقاط دسترسی و کامپیوترهای میزبان در نظر گرفته شده که در برگیرنده اهمیت شخص		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت سیستم عامل	بله	خیر
	ثالث باشد؟		
۱۸	آیا همه بسته‌های نرم افزاری یا مورد استخراج شده مورد نیاز سیستم عامل در روی سیستم نصب شده‌اند؟		

چک لیست شماره هشتاد شش: نقاط ضعف و آسیب‌پذیری حوزه مدیریت شبکه محلی LAN

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت شبکه محلی LAN	بله	خیر
۱	آیا ابزارهای مدیریتی شبکه محلی LAN مورد استفاده قرار گرفته‌اند؟		
۲	آیا اطلاعات محرمانه شبکه محلی LAN به طور صحیح تنها به کاربران مجاز تعمیم داده شده است؟		
۳	آیا اطلاعاتی که نیاز به اشتراک بین سرورها ندارند محدود شده‌اند؟		
۴	آیا آموزش و گواهینامه‌های ضروری مناسب برای مدیریت شبکه‌های محلی وجود دارد؟		
۵	آیا آموزش‌های مناسب به کاربران معینی در رابطه با امنیت شبکه، دسترسی به فایل و سایر موارد داده شده است؟		
۶	آیا بازبینی از نوع سرویس‌های شبکه‌ای نصب شده روی کارت‌های شبکه انجام شده است؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت شبکه محلی LAN	بله	خیر
۷	آیا بازبینی منظم از خط‌مشی امنیتی شبکه محلی LAN وجود دارد؟		
۸	آیا بازبینی منظم از نقشه توپولوژی شبکه محلی LAN انجام شده است؟		
۹	آیا بازبینی منظمی از داده‌های ثبت شده امنیتی به عمل می‌آید؟		
۱۰	آیا برچسب مناسبی روی همه کابل‌های شبکه محلی LAN نصب شده است؟		
۱۱	آیا توپولوژی شبکه محلی LAN ترسیم شده است ؟		
۱۲	آیا ثبت تغییرات ایجاد شده برای نرم افزارهای بسیار حساس و بحرانی انجام شده است؟		
۱۳	آیا ثبت کلیه وقایع امنیتی برای راه‌اندازی شبکه محلی LAN مناسب است؟		
۱۴	آیا حدود IP آدرس استاتیک برای کنترل شبکه به نسبت پروتکل پیکربندی میزبان پویا قرار داده شده است؟		
۱۵	آیا سایت سرورها و مانیتورهای شبکه محلی LAN در محیطی امن واقع شده است؟		
۱۶	آیا سیاست امنیتی شبکه محلی LAN به تفصیل بیان شده است ؟		
۱۷	آیا فایل‌ها و پوشه‌های حساس قابل دسترسی ثبت شده‌اند؟		
۱۸	آیا یک استراتژی تخصیص IP برای شبکه‌های محلی گوناگون برنامه		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مدیریت شبکه محلی LAN	بله	خیر
	ریزی و اجرا شده است ؟		
۱۹	آیا یک سیستم پشتیبان شبکه محلی LAN ایجاد شده است؟		
۲۰	آیا یک نقشه پشتیبان برای بازبینی سطوح امنیتی مربوطه وجود دارد؟		
۲۱	آیا یک نقشه پشتیبان برای مواقعی که شبکه محلی LAN دچار نقص می‌شود وجود دارد؟		
۲۲	آیا یک نقشه کاربری به منظور تعیین جزئیات دسترسی به شبکه محلی LAN ایجاد شده است تا از دسترسی غیر مجاز به سرورهای معین جلو گیری به عمل آید؟		
۲۳	آیا یک نقشه و برنامه‌ای برای رفع عیب شبکه محلی LAN وجود دارد ؟		

چک لیست شماره هشتاد هفت: نقاط ضعف و آسیب‌پذیری حوزه مستندات

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مستندات	بله	خیر
۱	آیا به طور کامل اطلاعات مربوط به فروشنده دیواره آتش، سابقه تنظیم اولیه و پیکربندی داده‌ها مستندسازی شده‌اند؟		
۲	آیا توپولوژی شبکه به وضوح چیدمان دیواره آتش را تشریح می‌نماید؟		
۳	آیا کتاب راهنمای امنیتی و عملیاتی به راحتی در دسترس می‌باشند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مستندات	بله	خیر
۴	آیا کلیه تغییرات دیواره آتش توسط ناظران مجاز امضا می‌شوند؟		
۵	آیا کلیه تغییرات دیواره آتش کاملاً ثبت می‌شود؟		
۶	آیا کلیه دیاگرام‌ها بخش‌ها، سطوح نگارش، نام میزبان‌ها، آدرس‌ها IP و ارتباط‌ها و اتصالات کاملاً مستندسازی می‌شوند؟		
۷	آیا لیست تماس‌های تلفنی در وضعیت اضطراری وقوع مشکلات و تخلف‌های امنیتی دیواره آتش مورد استفاده می‌باشد ؟		
۸	آیا لیست کاملی از همه سخت‌افزارهای مجاز، نرم‌افزار، روترها و محل آن‌ها وجود دارد؟		
۹	آیا یک توپولوژی یا رده‌بندی از قواعد دسترسی دیواره آتش دارید؟		
۱	آیا یک روند ثابت برای جمع‌آوری مستندات در صورت وقوع یک حادثه امنیتی وجود دارد؟		
۱۱	آیا یک لیست دسترسی کاربران مجاز دیواره آتش وجود دارد؟		

چک لیست شماره هشتاد هشت: نقاط ضعف و آسیب‌پذیری حوزه مستندسازی (صندوق صوتی)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مستندسازی (صندوق صوتی)	بله	خیر
۱	آیا فهرستی از همه تجهیزات مجاز تلفن‌های سازمان به طور رسمی تهیه		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مستندسازی (صندوق صوتی)	بله	خیر
	شده و محل‌های آن‌ها وجود دارد؟		
۲	آیا کلیه تغییرات، جابه‌جائی‌ها، افزودن‌های صندوق صوتی سازمان به وسیله مسئول مجاز مربوطه تصویب شده است؟		
۳	آیا کلیه تغییرات، جابه‌جائی‌ها، افزودن‌های صندوق صوتی سازمان مستند شده است؟		
۴	آیا کنترل‌های دسترسی به طور منظم مورد بازبینی و ثبت (بایگانی) قرار می‌گیرد؟ (مثلا از طریق ثبت ورود/خروج‌ها)		
۵	آیا لیست کاربران مجاز مورد استفاده قرار گرفته و حفظ شده است؟		
۶	آیا لیست‌های تماس فوری مورد استفاده قرار گرفته و نگهداری می‌شود؟		
۷	آیا یک پرینتر اختصاصی برای تولید گزارش‌های صندوق صوتی سازمان وجود دارد؟		
۸	آیا یک نقشه توپولوژی گرافیکی از همه خطوط محل کار و پورت‌های متناظر آن‌ها در مورد صندوق صوتی سازمان وجود دارد؟		
۹	آیا یک نمودار شبکه مستند از طرح بندی صندوق صوتی سازمان وجود دارد؟		

چک لیست شماره هشتاد نه: نقاط ضعف و آسیب‌پذیری حوزه مستندسازی (ضد ویروس)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مستندسازی (ضد ویروس)	بله	خیر
۱	آیا اسناد راهنمای انجام امور ضد ویروس به‌راحتی در دسترس می‌باشند؟		
۲	آیا دارای یک فرم یا الگو که به راحتی برای ثبت حملات ویروسی به‌کار رود می‌باشید؟		
۳	آیا در صورت بروز یک حادثه ویروسی یک روند پایدار جهت برخورد وجود دارد؟		
۴	آیا محیط‌های طراحی و توسعه نرم‌افزار ضد ویروس کاملاً مستندسازی و به روز شده است؟		
۵	آیا همه اطلاعات مربوط به فروشنده ضد ویروس، رونده‌ای آماده‌سازی و نصب و داده‌های مربوط به پیکربندی به طور کامل مستند و مکتوب شده است؟		
۶	آیا همه تغییرات ضد ویروس به طور کامل مستند شده‌اند؟		
۷	آیا همه تغییرات ضد ویروس توسط ناظران مسئول و مجاز انتخاب شده‌اند؟		
۸	آیا همه نقاط مستعد ورود کد یا ویروس‌های مضر شناسایی شده و مستند گردیده‌اند؟		

چک لیست شماره نود: نقاط ضعف و آسیب‌پذیری حوزه مسئولیت‌های کاربران

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مسئولیت‌های کاربران	بله	خیر
۱	آیا به کاربران توصیه شده یا دستور داده‌شده که هرگز نرم‌افزار غیرمجاز یا بدون مجوز دانلود نکنند؟		
۲	آیا به کاربران دستور داده شده است که حادثه ویروسی را تا زمانی‌که تأیید نشده است به کاربران دیگر اطلاع ندهند؟		
۳	آیا به کاربران دستور داده شده است که نرم افزار ضد ویروس روی رایانه‌های خود را تغییر نداده یا از کار نیندازند؟		
۴	آیا به کاربران دستور داده شده است که هرگونه حادثه ویروسی را فوراً به بخش IT گزارش کنند؟		
۵	آیا به کارکنان توصیه/دستور داده‌شده است که هرگز پیوست پست الکترونیک‌ها را که از فرستنده‌های ناشناس می‌آید باز نکنند؟		
۶	آیا طرحی برای ایجاد آگاهی مستمر در کاربر نسبت به راه‌حل ضد ویروس و کارکردهای آن وجود دارد؟		
۷	آیا کاربران از محدودیت‌های در نظر گرفته شده برای هرزنامه‌ها، نامه‌های زنجیره‌ای، پست الکترونیک‌های شیادی و دیگر منابع ویروس‌ها مطلع می‌باشند؟		
۸	آیا کاربران از منابع احتمالی یک ویروس آگاهی دارند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مسئولیت‌های کاربران	بله	خیر
۹	آیا کاربران به طور واضح از اثرات فاجعه‌آمیز حمله ویروسی و پردازش‌های غلط داده‌ها که از آن حاصل می‌آید آگاهی دارند؟		
۱۰	آیا کاربران می‌دانند که پس از سوءظن به آلودگی ویروسی رایانه‌های خود را خاموش نکنند مگر آنکه بخش IT طور دیگری دستور داده باشد؟		
۱۱	آیا کاربران می‌دانند که نباید نرم‌افزارها یا دیسکت‌هایی را که از منابع غیرقابل اعتماد می‌آید اجرا کنند؟		

چک لیست شماره نود یک: نقاط ضعف و آسیب‌پذیری حوزه مشخصات کلمه عبور

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه مشخصات کلمه عبور	بله	خیر
۱	آیا استفاده مجدد از کلمه عبور سازمان غیرمجاز است؟		
۲	آیا گذرواژه‌ها الزامات پیچیده بودن را برآورده می‌کنند؟		
۳	آیا گذرواژه‌ها باید طول حداقلی داشته باشند؟		
۴	آیا گذرواژه‌ها در برابر تکنیک مهندسی اجتماعی دیدن کلمه عبور تایپ شده مصون می‌باشند؟		
۵	آیا گذرواژه‌های واضح و معلوم به‌عنوان غیرمجاز تلقی می‌شوند ؟		

چک لیست شماره نود دو: نقاط ضعف و آسیب‌پذیری حوزه موارد عمومی سرورها

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه موارد عمومی سرورها	بله	خیر
۱	آیا Wrapper TCPها به‌منظور شناسایی دسترسی غیرمجاز در صورت استفاده شدن فیلترینگ IP مورد استفاده قرار می‌گیرد؟		
۲	آیا اجازه‌های کاربرها و گروه‌ها به‌طور کامل تجدیدنظر شده‌اند؟		
۳	آیا اقدامات امنیتی در سطح بایاس برای همه سرورها اجرا گردیده است؟		
۴	آیا اقدامات حفاظتی از قبیل فایروال‌ها، رمزنگاری، محدودسازی دسترسی کاربران، پشتیبان گیری و غیره برای سرورها انجام شده است؟		
۵	آیا ثبت وقایع رخدادها به‌منظور کشف اقدام به دسترسی‌های غیرمجاز به فایل‌های ممنوع فعال شده است؟		
۶	آیا حساب پیش‌فرض مدیر سیستم به طور مرتب از نو با اسم و رمز جدید عوض می‌شود؟		
۷	آیا حساب کاربری مهمان حذف شده است؟		
۸	آیا خصوصیت Routing IP غیر فعال شده است؟		
۹	آیا دامنه سرور مخصوص به خودش بوده و با دامنه‌های دیگر مشترک نمی‌باشد؟		
۱۰	آیا رونده‌ای پشتیبان گیری و بازیابی در فواصل مرتب اجرا می‌گردد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه موارد عمومی سرورها	بله	خیر
۱۱	آیا سرور دارای یک لیست دسترسی از طریق فیلترینگ IP می‌باشد تا اجازه دسترسی به کاربر غیرمجاز ندهد؟		
۱۲	آیا سرورهای فایل به‌صورت فیزیکی قفل شده‌اند؟		
۱۳	آیا فایل‌های آغازین به‌منظور یافتن نرم‌افزار هکر به طور مرتب چک می‌شوند؟		
۱۴	آیا فایل‌های پشتیبان و بازیابی شده تست می‌شوند؟		
۱۵	آیا فایل‌های ثبت رخدادها را به طور دوره‌ای چک می‌کنید تا هرگونه فعالیت مشکوک معلوم شود؟		
۱۶	آیا کلیه اطلاعات مربوط به سرور به طور مناسبی نگهداری می‌شوند؟		
۱۷	آیا کلیه به‌روز سازی‌های مهم از وب‌سایت فروشنده سرور دریافت و نصب شده است؟		
۱۸	آیا کلیه سرورها در یک محیط مناسب و امن جای داده شده‌اند؟		
۱۹	آیا کلیه سرویس‌هایی که روی سرور اجرا می‌شوند، به منظور تضمین آن که تنها سرویس‌های مناسب اجرا می‌گردند، مورد تجدید نظر قرار می‌گیرند؟		
۲۰	آیا کلیه کاربران و حقوق دسترسی مربوط به آن‌ها به هر سرور تعیین شده است؟		
۲۱	آیا گروه "every one" برای همه سرورها برداشته شده یا حداقل دارای مجوز"deny" می‌باشد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه موارد عمومی سرورها	بله	خیر
۲۲	آیا نرم‌افزار امنیتی سرور مورد بررسی و جست‌جو قرار گرفته است؟		
۲۳	آیا همه پورت‌های باز IP/TCP تجدیدنظر شده و رونده‌ای دسترسی مورد بازبینی و ثبت قرار می‌گیرند؟		
۲۴	آیا یک خط‌مشی مناسبی برای ایجاد گذرواژه جهت دسترسی به درون سرورها دارید؟		

چک لیست شماره نود سه: نقاط ضعف و آسیب‌پذیری حوزه موانع فیزیکی: قفل کردن

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه موانع فیزیکی: قفل کردن	بله	خیر
۱	آیا ابزارهای امنیتی اضافی مورد نظر بوده و به‌کار گرفته می‌شوند؟		
۲	آیا از قفل‌های لازم برای امن ساختن سیستم‌های خیلی مهم مینی/مایکرو کامپیوتر خارج از شبکه استفاده می‌کنید؟		
۳	آیا تنظیمات قفل‌های اتاق کامپیوتر به‌صورت دوره‌ای تغییر داده می‌شود؟		
۴	آیا در طول ساعات غیرکاری دارایی‌های IT کاملاً در جایی قفل می‌شوند؟		
۵	آیا در مواقع اضطراری قفل‌ها به طور خودکار باز می‌شوند؟		
۶	آیا کلیدهای قفل کننده در طول ساعات غیرکاری به طور مناسب		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه موانع فیزیکی: قفل کردن	بله	خیر
	محافظت می‌شوند؟		
۷	برای محدود کردن دسترسی اتاق کامپیوتر به افراد مجاز آیا از مکانیزم‌های قفل ضد دست‌کاری استفاده می‌شود؟		
۸	یا شاسی‌های سیستم‌های کامپیوتری برای جلوگیری از برداشتن بردها و کارهای غیرمجاز قفل می‌شوند؟		

چک لیست شماره نود چهار: نقاط ضعف و آسیب‌پذیری حوزه موضوعات مربوط به خط‌مشی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه موضوعات مربوط به خط‌مشی	بله	خیر
۱	آیا به طور دوره‌ای روندها و سیاست‌های امنیتی فیزیکی مرور می‌شوند؟		
۲	آیا سطوح تهدید برای تهیه روندها مورد نظر قرار می‌گیرند؟		
۳	آیا سیاست‌های امنیتی فیزیکی با مشورت بخش حقوقی تدوین شده است؟		
۴	آیا منابع کافی برای تکمیل کلیه کارهای امنیتی فیزیکی اختصاص یافته است؟		
۵	آیا هنگام طراحی رونده‌ای امنیتی فیزیکی، سطوح هم‌خوانی واقعی در نظر گرفته می‌شوند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه موضوعات مربوط به خط‌مشی	بله	خیر
۶	به هنگام طراحی روندها آیا بهره‌وری در نظر گرفته می‌شود، مثلاً حداکثر استفاده را از امکانات وتجهیزات مد نظر قرار گرفته شده است؟		
۷	به هنگام طراحی روندهای امنیتی فیزیکی آیا شرایط ویژه در نظر گرفته می‌شوند؟		
۸	به‌هنگام طراحی روندها آیا ساعات عملیات در نظر گرفته می‌شوند؟		

چک لیست شماره نود پنج: نقاط ضعف و آسیب‌پذیری حوزه میزبان وب

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه میزبان وب	بله	خیر
۱	آیا جریان داده‌های حساس بین میزبان وب و نرم‌افزار کاربردی وب تحت نظارت قرار می‌گیرد؟		
۲	آیا خط‌مشی امنیتی خود میزبان وب، پیمانکاران و سایر اشخاص ثالث را نیز شامل می‌شود؟		
۳	آیا داده‌ها در همه نقاط عبور مسیر انتقال امن هستند؟		
۴	آیا در قرارداد توافقنامه سطح سرویس میزبان وب به وضوح مسئولیت‌های امنیتی آن‌ها نسبت به شما تعیین شده است؟		
۵	آیا روال‌هایی برای رفع مشکلات مرتبط با نقل و انتقالات داده‌های مالی		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه میزبان وب	بله	خیر
	از طریق وب سایت یا هزینه‌های سایت شبکه تعیین شده است؟		
۶	آیا سازمان در برابر استفاده فریب‌کارانه از کاربردهای وب ازطریق میزبان وب توسط بیمه یا قراردادی حفاظت می‌شود؟		
۷	آیا کنترل‌هایی به منظور جلوگیری از اعمال تغییرات غیرمجاز نرم‌افزارها یا سخت‌افزارهای کاربردی وب به وسیله میزبان وب در نظر گرفته شده است؟		
۸	آیا میزبان وب (در داخل سازمان یا خارج) افزونگی لازم برای قابلیت دسترسی راحت را فراهم می‌کند؟		
۹	آیا میزبان وب بر اساس ضوابط و قوانین موجود در کشور فعالیت می‌کند ؟		
۱۰	آیا میزبان وب هنگامی که یک رویداد امنیتی رخ دهد شما را آگاه می‌سازد؟		

چک لیست شماره نود شش: نقاط ضعف و آسیب‌پذیری حوزه نصب

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه نصب	بله	خیر
۱	اگر میسر باشد آیا فقط پرسنل آموزش دیده و مجاز نرم‌افزارها را نصب و پشتیبانی می‌کنند؟		
۲	آیا فایل‌های سیستم عامل و دیگر فایل‌های اجرایی فقط قابل خواندن می‌باشند؟		
۳	آیا کنترل‌هایی برای شبکه‌های LAN قرار داده‌اید که به جزء افراد مجاز، از لود کردن نرم‌افزار روی سرورها به‌وسیله دیگران جلوگیری کند؟		
۴	آیا نرم‌افزارهای قابل دانلود شدن روی درایو جداگانه یا پارتیشن جداگانه از فایل‌های سیستمی و فایل‌های مهم کاربردی نگهداری می‌شوند؟		
۵	آیا نرم‌افزارهای کاربردی از نرم‌افزارهای سیستمی مجزا می‌باشند؟		
۶	قبل از نصب نرم‌افزار آیا چک دوباره‌ای از صحت لیسانس آن می‌کنید؟		

چک لیست شماره نود هفت: نقاط ضعف و آسیب‌پذیری حوزه نقض خط‌مشی

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه نقض خط‌مشی	بله	خیر

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه نقض خط‌مشی	بله	خیر
۱	آیا اطلاعات مجزا شده بر اساس سطح امنیت مورد نیاز جدا شده‌اند؟		
۲	آیا اعلام‌های محرمانه بودن در دست دارید؟		
۳	آیا اعلام‌های مربوط به موضوعات درستی و وثاق موضوعات در دست دارید؟		
۴	آیا اقسام اطلاعات شناسایی شده‌اند (مثل خصوصی، پزشکی، ملکی، مالی، بازرسی، پیمانکاری)؟		
۵	آیا آیین‌نامه‌ها عواقب رفتار ناهماهنگ را مشخص کرده است؟		
۶	آیا تمام دلایل لازم برای تأمین امنیت اسناد بیان شده و درک شده است؟		
۷	آیا خط مشی‌ها به همه کاربران اسناد ابلاغ شده‌است؟		
۸	آیا دستورالعمل‌ها جامع می‌باشند و کلیه اشکال دسترسی به اسناد تجاری و کسب و کاری هم‌چون کار در خانه، دسترسی از طریق شماره‌گیری، استفاده از کارهایی که کپی‌رایت دارند، استفاده غیراداری از تجهیزات و غیره را پوشش می‌دهند؟		
۹	آیا رهنمودهای مربوط به اطلاعات حساس در دست دارید؟		
۱۰	آیا سیستم‌های اطلاعات شناسایی شده‌اند؟		
۱۱	آیا صاحبان اطلاعات مورد مشورت قرار می‌گیرند؟		
۱۲	آیا قواعد رفتاری که مسئولیت‌ها و رفتار مورد انتظار افراد را مشخص		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه نقض خط‌مشی	بله	خیر
	کند تعیین شده‌اند؟		
۱۳	آیا محدوده‌های زمانی در نظر گرفته شده است (مثلاً پروژه‌های اقتصادی/کالاهای مصرفی پس از علنی شدن و انتشار یافتن)؟		
۱۴	آیا همه پرسنل کلیدی IT که درگیر کار با مطالب محرمانه و ارسال آن‌ها می‌باشند مورد مشورت قرار می‌گیرند؟		
۱۵	آیا یک برنامه امنیتی برای اسناد و مدارک در دست دارید؟		
۱۶	آیا یک تحلیل کامل سود- هزینه به‌منظور کسب اطمینان از این که هزینه صرف شده برای تأمین امنیت تناسب لازم با درجه زیان دارد، انجام شده است؟		
۱۷	آیا یک سطح قابل قبول ریسک تعیین کرده‌اید؟		

چک لیست شماره نود هشت: نقاط ضعف و آسیب‌پذیری حوزه نگهداری از اسناد محرمانه

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه نگهداری از اسناد محرمانه	بله	خیر
۱	آیا اجازه قرار دادن داده‌های حساسی که بر روی درایوهای به اشتراک گذاشته شده وجود دارند، تنها در اختیار یک نفرمی باشد؟		
۲	آیا اسناد و مدیاها طوری مورد استفاده قرار می‌گیرند و به نحو مناسبی دور ریخته می‌شوند که الزامات امنیتی رعایت شده باشد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه نگهداری از اسناد محرمانه	بله	خیر
۳	آیا دیسک‌ها و پرینت‌ها برچسب خورده و بر اساس سطح امنیتی‌شان ذخیره می‌شوند؟		
۴	آیا روندی در نظر گرفته شده است که کاربران همیشه با کمک CTRL+ALT+DEL وارد سیستم شوند حتی اگر پنجره ورود هنوز بر روی صفحه نمایش دیده شود؟		
۵	آیا عادات کاری وجدانی مورد تقدیر و تشویق قرار می‌گیرد؟		
۶	آیا غریبه‌ها اجازه دارند از رایانه‌ها استفاده کنند؟		
۷	آیا فایل‌های موقت رایانه‌ها و حافظه روی وسایل مثل چاپ‌گرها، به طور مرتب پاک می‌شوند؟		
۸	آیا فولدرها در کشوهای فایل با سطوح امنیتی متفاوت گذاشته شده و کشوها در هنگامی‌که استفاده نمی‌شوند قفل می‌شوند؟		
۹	آیا گذرواژه‌ها به حافظه سپرده می‌شوند؟		
	آیا مدیاهای قابل حمل و نقل در کمدهای قفل شده می‌باشند؟		
۱۰	آیا مونیتورها طوری قرار داده شده یا این که از اسکرین فیل‌تر استفاده می‌شود تا رهگذرها نتوانند صفحه را ببینند؟		
۱۱	آیا میزها و مبلمان طوری ترتیب داده شده که صفحه رایانه از پنجره یا سالن قابل رؤیت نباشد؟		
۱۲	در ایستگاه‌های کاری که دو یا چند نفر مشترکاً کار می‌کنند آیا هر کدام که دست از کار می‌کشد، از سیستم خارج می‌شود یا خیر؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه نگهداری از اسناد محرمانه	بله	خیر
۱۳	هنگام ترک رایانه‌ها آیا آن‌ها قفل می‌شوند، خاموش می‌شوند یا در حالت اسکرین سیور دارای گذرواژه قرار داده می‌شوند؟		

چک لیست شماره نود نه: نقاط ضعف و آسیب‌پذیری حوزه نگهداری سوابق

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه نگهداری سوابق	بله	خیر
۱	اگر به صرفه باشد آیا نرم‌افزار خاصی که از کلیه نرم‌افزارهای موجود روی رایانه‌ها لیست برداری می‌کند، خریداری می‌نمایید؟		
۲	آیا به طور سالیانه بررسی می‌نمایید که فقط نرم‌افزارهای قانونی و مصوب نصب شده و مورد بهره‌برداری قرار گیرند؟		
۳	آیا سوابق نوشته شده از هر نرم‌افزار بر روی هر کامپیوتر نگهداری می‌شود؟		
۴	آیا کلیه کپی‌های غیرقانونی نرم‌افزارها بلافاصله پاک می‌شوند؟		

چک لیست شماره صد: نقاط ضعف و آسیب‌پذیری حوزه واکنش به حادثه (دیواره آتش)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حادثه (دیواره آتش)	بله	خیر

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حادثه (دیواره آتش)	بله	خیر
۱	آیا افراد مسئول واکنش در مقابل حوادث دیواره آتش ابزارهای مناسب برای این کار در اختیار دارند؟		
۲	آیا برای آزمایش میزان سرعت عکس‌العمل دیواره آتش‌های گاه‌به‌گاه عملیات نفوذ به دیواره آتش اجرا می‌شود؟		
۳	آیا برای تضمین زمان اقدام واکنشی مناسب و سریع از سوی مسئولین دیواره آتش یک توافق نامه سطح سرویس دهی وجود دارد؟		
۴	آیا پرسنل مسئول واکنش به حوادث دسترسی آسان به لاگ‌های گزارش رخدادها و داده‌های دیواره آتش‌ها دارند؟		
۵	آیا خط‌مشی دیواره آتش و اساس قواعد تنظیم شده آن، بر طبق وضعیت تهدیدات موجود برای سازمان و نیز بر اساس دیگر خط‌مشی‌های امنیتی سازمان نوشته شده است؟		
۶	آیا دوره‌های زمانی مشخص برای بازیابی و تنظیم مجدد دیواره آتش در صورت وقوع حوادثی که منجر به خرابی یا از کار افتادن دیواره آتش گردد، تعریف نموده‌اید؟		
۷	آیا راه‌حل‌های مربوط به آسیب‌پذیری‌های شناسایی شده بر اساس شدت تهدید اولویت‌بندی شده‌اند؟		
۸	آیا رونده‌ای مقابله با تشدید مشکلات وجود دارد؟		
۹	آیا مدیر دیواره آتش برای اتخاذ تصمیمات مناسب در جهت واکنش نسبت به تهدیدات از اطلاعات به‌روز و قابل اعتماد درباره انواع		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حادثه (دیواره آتش)	بله	خیر
	آسیب‌پذیری‌ها و تهدیدات استفاده می‌کند؟		
۱۰	آیا یک طرح بازیابی حوادث فاجعه آمیز در مورد دیواره آتش وجود دارد؟		

چک لیست شماره صد یک: نقاط ضعف و آسیب‌پذیری حوزه واکنش به حادثه (صندوق صوتی)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حادثه (صندوق صوتی)	بله	خیر
۱	آیا افراد متصدی پاسخ‌های ضمنی دسترسی آسان به داده‌های گزارش صندوق صوتی سازمان و وقایع ثبت شده دارند؟		
۲	آیا افراد متصدی واکنش به حوادث ابزارهای مناسب برای انجام این کار را در اختیار دارند؟		
۳	آیا افراد متصدی واکنش به حوادث، روش‌های مستندسازی شده برای انجام کارشان دارند؟		
۴	آیا سیستمی برای ایجاد، پیگیری و بازبینی تلفن‌های مزاحم وجود دارد؟		
۵	آیا فایل‌های پشتیبان صندوق صوتی سازمان به صورت دوره‌ای آزمایش می‌شوند در صورتی که یک واقعه امنیتی/حادثه بد رخ داده باشد؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حادثه (صندوق صوتی)	بله	خیر
۶	آیا کارمندان ارتباطات راه دور به وسیله سیستم‌های احضار یا موبایل قابل دسترسی هستند؟		
۷	آیا یک برنامه و نقشه جهت کشف مشکلات صندوق صوتی سازمان وجود دارد؟		

چک لیست شماره صد دو: نقاط ضعف و آسیب‌پذیری حوزه واکنش به حادثه (IT)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حوادث (IT)	بله	خیر
۱	آیا تیم مسئول واکنش در برابر حادثه، امور مربوط به هشدار ویروسی و موارد آلودگی را انجام می‌دهد؟		
۲	آیا تیم واکنش برعلیه حوادث مجهز به ادواتی می‌باشند که بلافاصله اعلامیه هشدار یا حملات ویروسی را در شبکه دریافت نمایند؟		
۳	آیا در صورت حمله ویروسی موافقت‌نامه‌های سطح سرویس دهی برای رایانه‌ها یا سرویس بازیابی دارید؟		
۴	آیا رونده‌ای حل مسائل بحرانی وجود دارد؟		
۵	آیا رونده‌ای واکنش نسبت به حوادث در میان تیم‌های گوناگون IT و ادارات منطقه‌ای هماهنگ گردیده‌اند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حوادث (IT)	بله	خیر
۶	آیا روندهایی دارید که سریعاً سخت‌افزار آلوده به ویروس را از شبکه قطع کند؟		
۷	آیا فردی را در اختیار دارید که کاربران از راه دور را در مشکلات ویروسی راهبری کند؟		
۸	آیا کارکنان IT دارای پیجرهای اضطراری دارای شماره‌های پیجری که در دسترس بقیه افراد سازمان باشند، می‌باشند؟		
۹	آیا گاه به گاه تمرینات آتش‌نشانی به‌منظور آزمایش زمان‌های واکنش به حوادث را اجرا می‌کنید؟		
۱۰	آیا مدیر ضد ویروس دارای اطلاعات جاری و قابل اعتماد در زمینه تهدیدات و آسیب‌پذیری‌های مربوطه برای اتخاذ تصمیمات مناسب می‌باشد؟		
۱۱	آیا نفرات متصدی واکنش در مقابل حوادث ویروسی ابزارهای لازم برای این کار را دارند؟		

چک لیست شماره صد سه: نقاط ضعف و آسیب‌پذیری حوزه واکنش به حوادث (اسناد)

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حوادث (اسناد)	بله	خیر
۱	آیا برای پی‌گیری شکایت‌های حقوقی کمک و امدادی دارید؟		
۲	آیا چرخه حیات اطلاعات مد نظر قرار دارد؟		
۳	آیا حفاظت قوی از گذر واژه برای جلوگیری از دسترسی غیرمجاز در دست دارید؟		
۴	آیا در همه حوزه‌ها کنترل‌های لازم وجود دارد؟		
۵	آیا ردگیری موضوعات مدنظر می‌باشد؟		
۶	آیا قابلیتی برای به اشتراک گذاری اطلاعات مربوط به تهدیدات و آسیب‌پذیری‌های رایج در اسناد کسب و کاری وجود دارد؟		
۷	آیا کارکنان آموزش‌دیده بر ارسال اسناد نظارت دارند؟		
۸	آیا موضوعت پردازش‌گری مدنظر می‌باشد؟		
۹	آیا نیازها و الزامات تعامل با جمعیت‌های ویژه مثل کودکان مدنظر می‌باشد؟		
۱۰	آیا همه فن‌آوری‌های جدید کار با اسناد به‌منظور برآورد آسیب‌پذیری‌های امنیتی آن‌ها مورد ارزیابی قرار گرفته‌اند؟		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به حوادث (اسناد)	بله	خیر
۱۱	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش به مانیتورینگ		

چک لیست شماره صد چهار: نقاط ضعف و آسیب‌پذیری حوزه واکنش دربرابرحادثه

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش در برابر حادثه	بله	خیر
۱	آیا افرادی که مسئول پاسخ‌گویی به حوادث هستند ابزارهای مناسبی در رابطه با کارشان در اختیار دارند؟		
۲	آیا برنامه بازیابی حوادث فاجعه آمیز نرم‌افزارهای تحت وب وجود دارد؟		
۳	آیا پشتیبان‌های نرم‌افزاری کاربردی وب به صورت دوره‌ای در مواقعی که یک حادثه امنیتی یا فاجعه آمیز روی می‌دهد مورد آزمایش و تست قرار می‌گیرند؟		
۴	آیا در توافق نامه‌های سطح سرویس دهی، زمان‌های پاسخ‌گویی افراد مسئول نرم‌افزاهای کاربردی وب به‌طور مناسبی تعریف شده است؟		
۵	آیا روش‌هایی برای تعدیل مشکل وجود دارد؟		
۶	آیا سیستمی برای ایجاد، پیگیری و بازبینی موارد مزاحم و آزاردهنده وجود دارد؟		
۷	آیا فرد یا افراد مسئول پاسخ‌گویی به حوادث، دسترسی آسان به نرم‌افزارهای کاربردی وب، داده‌های گزارش و لاگ های وقایع ثبت شده		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واکنش در برابر حادثه	بله	خیر
	دارند؟		
۸	آیا فرد یا افرادی که مسئول پاسخ‌گویی به حوادث هستند، روش‌های مستند برای انجام کارشان در اختیار دارند؟		
۹	آیا کارمندان امنیت/توسعه وب بعد از چند ساعت از طریق موبایل یا پیجر قابل دسترسی هستند؟		

چک لیست شماره صد پنج: نقاط ضعف و آسیب‌پذیری حوزه واگذاری گذرواژه

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واگذاری گذرواژه	بله	خیر
۱	آیا از استفاده شناسه‌های ورود به سیستم هم‌زمان ممانعت شده است؟		
۲	آیا استفاده ازشناسه های ورود به سیستم مشترک ممنوع است؟		
۳	آیا درخواست کتبی برای ورود به سیستم با استفاده از شناسه‌ها مورد نیاز است؟		
۴	آیا دسترسی‌های داده شده به افراد بر اساس نیاز کاری آن‌ها صورت می‌گیرد؟		
۵	آیا گذرواژه‌های جداگانه‌ای بر اساس مقاصد متفاوت یا گروه‌های متفاوت مورد استفاده قرار می‌گیرد؟		
۶	آیا لیست کاربران دارای دسترسی به نرم‌افزارهای کاربردی به طور		

ردیف	چک لیست نقاط ضعف و آسیب‌پذیری حوزه واگذاری گذرواژه	بله	خیر
	دوره‌ای مورد بازبینی قرار می‌گیرد؟		
۷	آیا همه کاربران نهایی محتمل، به وسیله خط‌مشی گذرواژه پوشش داده شده‌اند؟		
۸	قبل از تخصیص دسترسی ،آیا سطح ریسک درک شده است و اگر ریسک بالایی وجود دارد، آیا بررسی سوابق فردی مورد نیاز است؟		
۹	قبل از تخصیص گذرواژه‌ها آیا لازم است که کاربران مستندات مربوط به سیاست‌ها و روش‌ها را مطالعه کرده و امضا کنند؟		

واژه نامه:

حساب دارای اجازه ورود به سیستم	account
مدیریتی	administrative
نرم افزار کاربردی	application
ارزیابی	assessment
قابلیت ارائه	availability
درب پشتی (نوعی تروجان)	backdoor
استفاده کننده	client
محرمانگی	confidentiality
پیکر بندی	configuration

رمز شکنی	crack
به هم ریختگی - خرابی	crash
پایگاه اطلاعاتی	database
اثر انگشت	fingerprint
صحت	integrity
نفوذ	penetration
نوعی گول زدن سیستم	phishing
نوعی از تروجان که در سیستم عامل پنهان می شود	rootkit
آسیب پذیری	vulnerability
ارزابی آسیب پذیری	vulnerabilityassessment

منابع:

en Wikipedia. org. (سایت ویکی پدیا)

www. Vulnerabilityassessment. co. uk

Microsoft Windows ۲۰۰۰ Security Configuration guide

WWW. CiSecurity . org

WWW. nsa. gov

آنالیز ریسک امنیت اطلاعات، مترجمین: دکتر حسین شیرازی، مهندس سید محمد رضوی عمرانی- ۱۳۸۷-انتشارات دانشگاه صنعتی مالک اشتر

اصول و مبانی پدافند غیرعامل، جعفر موحدی نیا،۱۳۸۸- انتشارات دانشگاه صنعتی مالک اشتر

D. L. (۲۰۰۰). Information security" new jersey: Prentice Hall. ،Pipkin

، (۲۰۰۹) " Network Security Against Today's Threats"،Samara Lynn
۲۰۰۹،http://www. crn. com/security/۲۱۲۷۰۱۶۵۷ Jan. ۰۹

(۲۰۰۷) " The role of external and internal ، Donna Cooke، Paul Hart،Qing Hu influences on information systems security – a neo-institutional perspective ، pp ۱۵۳-۱۷۲، Vol. ۱۶ No. ۲، The Journal of Strategic Information Systems،" June ۲۰۰۷