نمونه سوالات درس معماری امنیت استاد فراهانی

۱- اهمیت امنیت اطلاعات در عصر دیجیتال را توضیح دهید؟

عصر حاضر را عصر الکترونیک یا دیجیتال می نامند. امروزه استفاده از کامپیوتر و اینترنت بصورت روز افزون افزایش یافته است و اکثر اطلاعات در کامپیوتر ها و رسانه های ذخیره سازی بصورت دیجیتال ذخیره می گردد و از طریق خطوط ارتباطی مبادله می شود ولی با اینحال همواره مخاطراتی جدی مانند از دست دادن سوابق، حملات تخریب سرویس، خراب شدن اطلاعات و سایر انواع حملات خصمانه وجود دارد. از دست رفتن تمام یا بخشی از سوابق الکترونیکی می تواند یک شرکت را زمین گیر کند. برای کشوری که امنیت فناوری اطلاعات آن ضعیف است این احتمال وجود دارد که منابع حیاتی آن در معرض خطر قرار گیرند و به آنها صدمات جبران ناپذیری وارد شود. عدم توجه کافی به امنیت برای کشورهایی که به روابط خارجی در صنایع خود اهمیت می دهند می تواند موجب خسارتهای جدی و پیش بینی نشده ای گردد . نیل به اهداف به توانایی کشورهای درحال توسعه توسعهٔ هزاره استفادهٔ مؤثر از فناوری اطلاعات و افزایش بودجهٔ آنها با عضویت دائمی در سازمان تجارت جهانی بستگی دارد.

۲- امنیت را در فضای سایبر توضیح دهید؟

هنگامی در فضای سایبر ایمن هستید که دسترسی به منابع اطلاعاتی شما تحت کنترل خودتان باشد، یعنی هیچ کس بدون کسب اجازه از جانب شما قادر به دسترسی به این منابع اطلاعاتی نباشد. این منابع شامل داده‌ها و منابع رایانه ای، شبکه ای، تراکنشی، پردازشی، و اطلاعاتی می باشند. طبیعتًا ممکن است برخی از این منابع از جانب دیگران و برای استفادهٔ شما ارائه شده باشند، مثل حساب کاربری در یک رایانهٔ اشتراکی یا دسترسی به اینترنت از طریق یک ارائه کنندهٔ خدمات اینترنتی (ISP) . از آنجا که این موارد هیچگاه کاملا ایمن نیستند، تنها تا وقتیکه دستورالعملهای فروشندهٔ خدمات برای استفادهٔ صحیح از آنها را دنبال کنید می توانید بر دسترسی مداوم و استفادهٔ مناسب از خدمات اشراف داشته باشید. از نظر مفهومی میان ماهیت تهدیدات فضای سایبر و تهدیداتی که در دنیای واقعی وجود دارند هیچ تفاوتی نیست ، بلکه تفاوت این دو مقوله برخاسته از خصوصیات فضای الکترونیکی و تهدیدات این حوزه است.

۳- تفاوت های میان فضای واقعی با فضای سایبر را بیان کنید؟

۱. هر نوع نقض امنیت در فضای سایبر می تواند بسیار سریع اتفاق بیافتد؛ یعنی تا زمانیکه بخواهید آگاه شوید چه اتفاقی برای سرمایه های شما افتاده، ممکن است دیگر برای جلوگیری از وارد آمدن خسارت بسیار دیر شده باشد .
۲. لازم نیست شما در یک محل بصورت فیزیکی حضور داشته باشید تا بتوانید امنیت فضای سایبر را خدشه دار کنید. این بدان معناست که مثلا یک نفر در اروپا می تواند امنیت رایانه های یک هدف در هند را خدشه دار نماید .
۳. فضای سایبر محیطی قدرتمند اما پیچیده را بوجود آورده که در آن نقش تأمین امنیت بر عهدهٔ چند گروه از افراد است . مثلا اگر شما یکی از کاربران ISP باشید، راههای مختلفی برای حفاظت از خود و رایانه شخصی تان پیش رو دارید اگرچه نمی توانید سیاستهای امنیتی ISP مورد استفادهٔ خود یا نحوهٔ پیاده سازی آنرا کنترل کنید . همچنین نمی توانید نرم‌افزارهای مشتریان خود را تحت کنترل داشته باشید؛ حتی اگر در ارتباط نزدیک با سیستم های آنها باشید .

۴- سیاست امنیت گمنامی را تعریف کنید و بکارگیری این سیاست را بین فضای سایبر و واقعی مقایسه کنید؟

اطلاعاتی که خصوصی بشمار می روند تنها زمانی می توانند واقعًا خصوصی بمانند که بصورت ایمن ذخیره شده باشند . برای این منظور در دنیای واقعی بگونه ای رفتار می کنیم که گویی چنین اطلاعاتی وجود خارجی ندارند . این سیاست را امنیت گمنامی می نامند . به همین ترتیب اطلاعاتی که باید بصورت محرمانه به اشتراک گذارده شوند باید برای کسانیکه آنها را به اشتراک گذاشته اند بصورت ایمن باقی بمانند و هنگام انتقال این اطلاعات باید سیاستهای امنیتی کافی در مورد آنها اعمال شود.

موقعیتهایی نظیر این مسئله در فضای سایبر نیز وجود دارد، ولی با فرض طبیعت خاص فضای سایبر و ارتباط میان رایانه های موجود در آن، امنیت گمنامی یا استفاده از پنهان سازی سیاستی ضعیف می نماید و باید از آن اجتناب کنیم. مفاهیم رایانه ، شبکه و امنیت داده‌ها در فضای سایبر همانند دنیای واقعی هستند، ولی مکانیزمهای پیاده سازی روال‌های مرتبط با آنها متفاوت است. مثلا برای استفاده از حسابهای کاربری که اجازهٔ دسترسی به اطلاعات یا خدمات را فراهم می آورند، به جای کلیدهای فیزیکی یا الکترونیکی، دارای شناسهٔ کاربری و رمز عبور هستیم و بجای استفاده از پاکتهای دربسته برای انتقال اطلاعات می توانیم دادهٔ انتقالی را به نحوی رمزگذاری کنیم که توسط افراد ناشناس، غیرقابل خواندن باشد. در مقایسهٔ دنیای واقعی با فضای سایبر می توانیم تخلفات مشابهی را در مورد قابلیت اطمینان و محرمانگی ببینیم. در هر دوی آنها ممکن است آدرسهای نادرست و یا امضاهای جعلی وجود داشته باشد .در هر دو فضا امکان ارائه اطلاعات غلط یا گمراه کننده نیز وجود خواهد داشت .همچنین امکان به اشتباه انداختن اشخاص با اطلاعات -چه بصورت تصادفی و چه از روی عمد -وجود دارد که باعث می شود نتوان تعیین کرد که چه اطلاعاتی مهم و قابل تأیید هستند. دست آخر اینکه در هر دو فضا امکان دسترسی غیرمجاز به اطلاعات محرمانه و استفاده از آنها برای مقاصد غیرقانونی نیز وجود دارد.

۵- خطرات احتمالی که در فضای سایبر در صورتیکه ملاحضات امنیتی در نظر گرفته نشود را نام ببرید؟

۱. تخریب اطلاعات
۲. سرقت اطلاعات و نقض حریم خصوصی
۳. نقض یکپارچگی اطلاعات
۴. نقض انسجام شبکه از طریق سایر سیستمها و شبکه ها
۵. ثبت کلیدها
۶. منع دسترسی

۶- خطر نقض یکپارچگی اطلاعات و نقض انسجام شبکه از طریق سایر سیستم ها و شبکه ها را شرح دهید؟

۱. نقض یکپارچگی اطلاعات : اطلاعات موجود در رایانه ممکن است بدون اطلاع شما تغییر کنند و دستکاری شوند. بر اساس نوع اطلاعاتی که نگهداری می کنید نتایج این دستکاری می تواند مقطعی یا درازمدت باشد. اگر این داده‌ها شامل سوابق مالی ، اطلاعات مشتریان ، وضعیت سفارشات یا پرونده های کارمندان باشند، پیامدهای نقض یکپارچگی آنها ممکن است بسیار پرهزینه و زیانبار باشد.
۲. نقض انسجام شبکه از طریق سایر سیستم ها و شبکه ها: هرچند در این مورد به طور مستقیم مورد حمله قرار نگرفتهاید، ولی ممکن است رایانه های دیگری که به آنها دسترسی داشته اید مورد حمله قرار گیرند و این مسئله روی شما نیز تأثیرگذار باشد . در اینصورت اگر مثلا عنصر یک مؤسسهٔ مالی و اعتباری باشید حین دورهٔ بازیابی اطلاعات قادر به تکمیل تراکنشهای مالی خود نخواهید بود.

۷- انگیزه خرابکاری در فضای سایبر را شرح دهید؟

فضای سایبر برای گروهی از افراد – که اصطلاحا "خرابکار "نامیده می شوند یک محیط چالش انگیز است که وارد حسابهای کاربری افراد شوند و یا بعنوان تفریح و سرگرمی به افراد دیگر آسیب برسانند.

برخی از خرابکارها از ابزارهای نفوذی استفاده می کنند. که این ابزارها حتی به نفوذگران تازه کار هم امکان می دهد که از آسیب پذیری ها سیستم بهره برداری نمایند. از آنجا که بسیاری از این ابزارها ممکن است بدون خطر باشند، هرگز کسی مطمئن نیست آثار استفاده از هریک از آنها دقیقًا چیست . علاوه بر آن این امکان وجود دارد که با انجام تغییراتی در بعضی از این ابزار به

اصطلاح بی خطر بتوان به رایانه ها و حسابهای کاربری که از طریق آنها مورد دسترسی قرار گرفته اند آسیب وارد کرد . برخی سازمان‌ها علاقه داشته باشند که نتیجهٔ یک نظرسنجی یا حتی انتخابات را دستکاری کنند تا به نتایج مطلوب خود برسند واضح است که منافع بالقوهٔ موجود در عصر نوین دیجیتال بسیار است .

۸- سیستم های محصول محور یا مشتری مدار را تعریف کنید؟ بخش امنیت را در هر یک از آنها را شرح دهید؟

سیستم های مستقل عموما محصول محور یا فرآیند محور هستند (مثل انبارداری، سفارشات یا فرآیندهایی نظیر تولید، ثبت در دفاتر عمومی، و حسابهای پرداختنی و دریافتنی)، اما سیستم های موفق تجارت الکترونیکی آنلاین (برخط) به روش دیگری سازماندهی می شوند. در این سیستمها برای کسب موفقیت لازم است که طراحی مشتری مدار باشد و سیستم به تعقیب رفتار مشتری در فرآیندهای جستجو و ارزیابی محصولات، ارائه سفارش، تکمیل تراکنشهای مالی و ردگیری محصول ارسال شده بپردازد. این روش اگر بدون توجه کافی به امنیت پیاده سازی شود ممکن است راه را برای روش های جدید نفوذ های امنیتی باز بگذارد. سازمان‌های کوچک و متوسط باید آگاه باشند که اصلاح نگرش سیستمهای تجاری برای بکارگیری اینترنت، خطرات جدیدی برای آنها به همراه دارد . یکی از این خطرات احتمال به سرقت رفتن و در معرض فروش قرار گرفتن سرمایه های موجود در شرکت.

۹- نقش سیاست های دولت در امنیت فناوری اطلاعات را شرح دهید؟

سیاست های دولت نیز نقش مهمی در مقوله امنیت فناوری اطلاعات ایفا می کند. با اینحال در این مورد باید با احتیاط اظهار نظر کرد، چراکه یک چا رچوب عمومی سیاست می تواند امنیت را تقویت کند ؛ اما اشکالاتی که در اثر مقررات نادرست دولتی بوجود می آید بیش از مزایای چنین مقرراتی است. فناوری اطلاعات بسرعت درحال تغییر است و تهدیدات سایبری جدید نیز با چنان سرعتی انتشار می یابند که برخی از مقررات دولتی براحتی می توانند تبدیل به موانعی برای ارائه سریع پاسخهای مبتکرانه شوند. بنابراین بهترین راه این است که میان معیارهای قانون گذاری و غیر قانونی یک نقطهٔ تعادل پیدا کنیم. برای دستیابی به چنین تعادلی، سیاستگذاران باید به برخی ویژگیهای ذاتی و منحصر به فرد اینترنت توجه کنند.

۱۰- ایجاد یک محیط قابل اطمینان در فضای سایبر نیازمند تطبیق قوانین و سیاست های دولتی با چه حوزه هایی از امنیت سایبر است؟

این زمینه ها شامل حمایت از مصرف کننده، خصوصی ماندن داده‌ها و ارتباطات، حقوق مالکیت معنوی و چارچوب تجارت الکترونیکی می باشد . در حقیقت کشورهایی که علاقه مند به گسترش تجارت الکترونیکی هستند ممکن است دریابند که قوانین آنها در مورد خدمات مالی، مالکیت سایبر و حمایت از مصرف کننده از اعتماد یا پشتیبانی لازم برای تعاملات خارج از دنیای اینترنت برخوردار نیست. اصلاح قوانین دنیای سایبر ممکن است بعنوان بخشی از اصلاحات روی قوانین کلی تر انجام شود.

۱۱- مفهوم زیر ساخت های حیاتی را شرح دهید ؟

در تعدادی از کشورها روال‌های واکنشی دولت به مشکلات امنیتی رایانه ها زیرساختهای حیاتی گفته می شود. زیرساخت حیاتی، شبکه ای از سرمایه های فیزیکی و سیستم هایی است که نقش بسزایی در اقتصاد یا رفاه یک کشور دارند. بعنوان مثال شبکهٔ خدمات مالی یک زیرساخت حیاتی است که شامل تمامی بانکهای خصوصی، بانک مرکزی، بازارهای مبادلات کالا، سازمان‌های تبادل چک، و دیگر نهادهایی که درگیر خدمات مالی و اعتباری هستند می شود. تقریبا در تمامی کشورهای جهان این عملیات با استفاده از رایانه ها انجام می گیرد. شبکهٔ حمل و نقل نیز زیرساخت حیاتی دیگری است که از جاده ها، پلها، کانالها، خطوط راه آهن و فرودگاهها تشکیل شده است.

۱۲- گروه های زیر ساخت حیاتی که توسط استراتژی امنیت سایبر آمریکا مشخص شده است را نام ببرید؟

به ۱۳ گروه زیرساخت حیاتی تقسیم شد

۱- کشاورزی،۲- تغذیه،۳- آب، ۴- بهداشت عمومی، ۵- خدمات اضطراری، ۶- دولت، ۷- صنایع دفاعی، ۸- اطلاعات و ارتباطات راه دور، ۹- انرژی، ۱۰ - حمل و نقل، ۱۱- بانکداری و امور مالی، ۱۲ - مواد شیمیایی و پرخطر، ۱۳ - خدمات پستی و کشتیرانی

۱۳- دلایل اهمیت مشخص کردن مفهوم زیر ساخت های حیاتی را شرح دهید؟

۱. به روشن شدن این مسئله کمک می کند که چرا امنیت رایانه ای مهم است. اگر سیاستگذاران درک کنند که درصورت خرابی رایانه ها، پول در بانکها غیر قابل پرداخت می شود، قطارها قادر به ترک ایستگاه نمی باشند و حتی آب آشامیدنی و برق قطع می شود، آنگاه بهتر خواهند توانست آثار ناشی از مشکلات امنیتی را درک کنند.
۲. گروه های زیرساختی به این دلیل اهمیت دارند که به تعریف مسئولیتهای جوامع کمک می کنند و جوامعی با علایق مشترک که برای ارتقای امنیت نیاز به همکاری با یکدیگر دارند بوجود می آورند. عنوان مثال صنعتگران صنعت برق و مستشاران دولتی می توانند با مشارکت یکدیگر نقش مثبتی در رفع آسیب پذیریهای سیستم برق داشته باشند . معیارهای امنیت رایانه ای از جمله شناسایی الگوهای بهینه و اشتراک اطلاعات در مورد آسیب پذیریها تا حدودی می تواند در محدوده مؤسسات و خطوط تولید صنعتی موجود بکار رود .

۱۴- ۵ مورد از اصول توسعهٔ استراتژی کاهش مخاطرهٔ زیر ساخت اطلاعاتی حساس که توسط گروه G8 مشخص شده است را بنویسید؟

۱. کشورها باید دارای شبکه های هشدار دهندهٔ اضطراری برای تهدیدات و حوادث دنیای سایبر باشند.
۲. کشورها باید سطح آگاهی و دانش خود را ارتقا دهند تا به درک افراد از ماهیت و وسعت زیرساخت اطلاعات حساس خود کمک نمایند و نقش آنها را در راستای حفاظت از این اطلاعات تعریف کنند.
۳. کشورها باید زیرساختهای خود را مورد مطالعه قرار دهند و ارتباطات متقابل میان آنها را مشخص سازند و بدینوسیله حفاظت از این زیرساختها را افزایش دهند.
۴. کشورها باید مشارکت میان بخش عمومی و بخش خصوصی را افزایش داده و اطلاعات زیرساختی مهم خود را مورد تجزیه و تحلیل قرار دهند و آنها را به اشتراک بگذارند تا بتوانند از آسیب دیدن آنها تا حد امکان جلوگیری نمایند و نسبت به آسیبهای وارده واکنش نشان دهند.
۵. کشورها باید شبکه های ارتباطی مخصوصی برای زمان بحران ایجاد و از آن نگهداری کنند، و آنها را موردارزیابی قرار دهند تا اطمینان یابند که در موقعیتهای اضطراری همچنان امن و پایدار باقی می مانند و می توان از آنها استفاده کرد.
۶. کشورها باید اطمینان یابند که سیاستهای در دسترس بودن داده ، امنیت زیرساختهای اطلا عات حساس را نیز مد نظر قرار داده اند.

۱۵- مسئولیت دولت در قبال امنیت رایانه های خود را شرح دهید؟

تمامی موضوعاتی که در مورد امنیت سیستم‌های سازمان‌های کوچک و بزرگ مطرح می باشد در سیستمهای دولتی نیز قابل استفاده هستند . همانطور که شرکتها نیازمند محافظت از خود، تهیه کنندگان و مصرف کنندگان هستند، دولت نیز باید از سیستمها و شهروندان در برابر تهدیدهای فیزیکی و تهدیدات امنیت سایبر محافظت نماید . دولتهای محلی و ملی نمی توانند جلوی بحرانهای شدید مثل وقوع وقفه در عملیات رایانه ای، از بین رفتن داده‌های محرمانه و یا سرقت منابع رایانه ای را بگیرند. انتشار اخبار رخدادهای امنیتی برای عموم باعث کاهش اعتماد مردم می شود و تبدیل به مانعی برای پیشرفت اقدامات دولت

الکترونیکی می گردد. معمولا اولین مسئولیت دولت در امنیت رایانه همان " تنظیم امور مربوط به خود " آن است؛ بدین معنا که سازمان‌های دولتی در تمامی سطوح (ملی، منطقه ای و محلی) باید از سیستمهای رایانه ای که مورد استفادهٔ آنان قرار دارد حفاظت بعمل آورند . اینکار شامل سیستمهای رایانه ای مورد استفادهٔ سازمان‌های دولتی و یا وزارتخانه ها از جمله نیروهای نظامی و انتظامی، سازمان‌های بهداشت و سلامت عمومی، مراکز واکنشهای اضطراری، و همچنین بانکهای مرکزی می شود.

۱۶- مسئولیت رهبری ساختار ملی امنیت رایانه ای دولت برعهده کیست؟ شرح دهید؟

انتخاب محل فرماندهی امنیت الکترونیکی در دولت اهمیت زیادی دارد . بعنوان مثال تصمیم گیری در مورد زمان انتشار اطلاعات در مورد آسیب پذیریهای امنیت سایبر برای عموم، نیازمند بررسیهای چندجانبه است . قرار دادن این مسئولیت در وزارت دفاع که معمولا مسئول حفظ اسرار امنیت ملی است ممکن است انتشار اطلاعات را دچار اختلال کند و باعث شود مطالب کافی برای بالا بردن سطح آگاهی های عمومی منتشر نشود. از آنجا که همکاری بخش دولتی و بخش خصوصی جزء مهمی از آنچه که معتقدیم مؤثرین استراتژی امنیت رایانه ای است می باشد، شاید بهتر باشد رهبری امنیت سایبر در یک سازمان اقتصادی یا شرکت وابسته به دولت و تحت نظارت بالاترین مقام اجرایی کشور قرار گیرد. اما مهمتر از اینکه کدام سازمان یا سازمان‌ها باید مسئولیت امنیت رایانه ای را بر عهده گیرند این است که باید نوعی "فرماندهی ملی " ایجاد شود تا بتوان کسب اطمینان کرد که امنیت رایانه ای از سوی اجزای دولت به اندازهٔ کافی مورد توجه قرار خواهد گرفت.

۱۷- راهکارهای الزام وزارتخانه ها به طبیعت و موافقت با استانداردهای امنیت رایانه ای را شرح دهید؟

۱. یک روش برای الزام وزارتخانه ها به تبعیت و موافقت با استانداردهای امنیت رایانه ای می تواند این باشد که یک مقام مسئول در ادارهٔ مرکزی امنیت در دولت بتواند سفارشات خرید سازمان‌های دولتی که از استانداردهای امنیتی تبعیت نکرده اند را رد کند.
۲. یک اقدام دیگر می تواند الزام وزارتخانه ها و سازمان‌های دولتی به اجرای ممیزی سالانهٔ امنیت سایبر و گزارش نتایج آن به ادارهٔ امنیت سایبر باشد . هر ساختاری که انتخاب شود، مدیر ارشد آن باید از طرف دفتر ریاست جمهوری یا نخست وزیری تعیین گردد تا تمامی ادارات و سازمان‌ها آنرا جدی بگیرند.

۱۸- مشکل منابع انسانی دولت در تامین امنیت و فضای سایبر را شرح دهید؟

یک چالش سازمانی دیگر برای دولت، مشکل منابع انسانی است . دولتها برای جذب و نگهداری پرسنل متخصص در زمینهٔ امنیت رایانه ای مشکل دارند . یکی از راه حلها می تواند ارائه بورس تحصیلی برای مطالعات امنیت رایانه ای باشد که با استفاده از این بورسها، افراد برای سالهای مشخصی تعهد خدمت به دولت پیدا خواهند کرد . یک راه حل کوتاه مدت نیز می تواند اجرای برنامه ای دو مرحله ای با کمک بخش خصوصی باشد که در آن متخصصان امنیت سایبر برای دولت کار کنند، اما تمام یا بخشی از حقوقشان توسط کارفرمای بخش خصوصی آنها پرداخت گردد . مشکل منابع انسانی در امنیت سایبر هم در کشورهای توسعه یافته و هم در کشورهای درحال توسعه ممکن است منجر به مواجههٔ دولت با مشکل اساسی دیگری شود، چراکه دولت در مقایسه با بخش خصوصی نمی‌تواند به متخصصین این رشته دستمزد قابل توجهی بپردازد.

۱۹- بخشهای مشترک استراتژی های ملی امنیت فضای سایبر را شرح دهید؟

۱. ارزیابی آسیب پذیریهای ملی و انتشار گزارشهای عمومی که کلیت موضوع را به تصویر می کشند و برای سیاستگذاران و مردم آگاهی بوجود می آورند؛
۲. ایجاد ساختار فرماندهی در بخش اجرایی دولت برای نظارت بر تهیه و اجرای سیاستها؛
۳. تهیهٔ یک طرح تفصیلی ملی با تبادل نظر با بخش خصوصی؛
۴. تطبیق مقررات و راهبردهای مرتبط با مسائلی نظیر اشتراک و دسترسی به اطلاعات برای بوجود آوردن پاسخگویی

۲۰- خط مشی هایی که برای دولتها و شرکت های خصوصی در خصوص تهیه استراتژیهای امنیت سایبر توسط OECD تعیین گردیده شامل چه مواردی است؟ ۴ مورد را شرح دهید؟

۱- مشارکت بخشهای عمومی و خصوصی : امنیت سایبر نیازمند همکاری بخشهای عمومی و خصوصی است . بخش خصوصی مسئولیت اصلی اطمینان از امنیت سیستمها و شبکه های خود را بر عهده دارد.

۲- آگاهی عمومی: استفاده کنندگان از شبکه از جمله تولیدکنندگان، راهبران، اپراتورها و یا کاربران شخصی باید نسبت به تهدیدات وارده و آسیب پذیریهای شبکه آگاه باشند و مسئولیت حفاظت از شبکه را بر اساس موقعیتها و نقش خود بر عهده گیرند.

۳- تجربیات، راهبردها و استاندار دهای بین المللی: امنیت سایبر باید بر ا ساس تعداد رو به رشد استانداردها و الگوهای سرآمدی، بصورت داوطلبانه و مبتنی بر توافق جمعی تهیه شود و تجربیات از طریق مؤسسات مشاور و سازمان‌های استاندارد بین المللی توسعه یابد. این استانداردها راهنمای مهمی برای سیاستهای داخلی دولت هستند. دولت نیازی ندارد و نبای د استانداردهای فنی برای بخش خصوصی تعیین کند.

۴- اشتراک اطلاعات: کاملا مشخص شده که تلا ش برای ایجاد امنیت سایبر با بی توجهی کاربران نسبت به آسیب پذیریها و حملات مواجه شده است . سازمان‌های بخش خصوصی باید تشویق شوند که اطلاعات رخدادهای امنیتی را با سایر سازمان‌های این بخش، با دولت، و نیز با سایر کشورها به اشتراک بگذارند.

۵- آموزش و پرورش: استراتژیهای سازمان همکاری اقتصادی آسیا (APEC) میگوید: توسعهٔ منابع انسانی برای به ثمر رسیدن تلاشها در جهت ارتقای سطح امنیت امری ضروری است. بمنظور تأمین امنیت فضای سایبر، دولتها و شرکتهای همکار آنها باید کارکنان خود را در مورد موضوعات پیچیدهٔ فنی و قانونی با پشتیبانی از زیرساختهای حیاتی و جرائم فضای سایبر آموزش دهند.

۶- اهمیت حریم خصوصی: شبکه های ICT داده‌های بسیار حساس شخصی را انتقال می دهند و ذخیره می سازند. حریم خصوصی جزء ضروری اعتماد در فضای سایبر است و استراتژیهای امنیت فضای سایبر باید به روشهای سازگار با ارزشهای مهم جامعه پیاده سازی شود.

۷- ارزیابی آسیب پذیری، هشدار و عکس العمل: همانطور که استراتژیهای سازمان همکاری اقتصادی آسیا نیز ابراز داشت : مبارزهٔ مؤثر با تخلفات فضای سایبر و حفاظت از اطلاعات زیرساختی، وابسته به اقتصادهایی است که سیستم هایی برای ارزیابی تهدیدها و آسیب پذیریها دارند و هشدارهای لازم را صادر می کنند. با شناسایی و اشتراک اطلاعات در مورد یک تهدید قبل از آنکه موجب آسیب گسترده ای شود، شبکه ها بهتر محافظت می شوند.

۸- همکاری بین المللی: برای ساده تر کردن تبادل نظر و همکاری در مورد گسترش یک "فرهنگ امنیتی " میان دولت و بخش خصوصی در سطح بین المللی، دولتها باید با یکدیگر همکاری کنند تا برای جرائم دنیای سایبر قوانین سازگاری به تصویب برسانند و نیروهای انتظامی کشورهای مختلف باید از طریق سازمان‌های بین المللی به یکدیگر کمک نمایند.

۲۱- روند توسعه و اجرای استراتژیهای امنیت سایبر برای دولت ها چه عناصر مشترکی است؟

۱. ارزیابی آسیب پذیریها؛
۲. افزایش سطح آگاهی؛
۳. گماردن یک نفر بعنوان فرمانده برای ایجاد هماهنگی در سیاستها؛
۴. توسعهٔ برنامهٔ مدیریت مخاطره
۵. تطبیق خط مشی های امنیتی مناسب؛
۶. توجیه ساختاری
۷. ارزیابی مجدد دورهای و ارتقای مداوم

۲۲- هدف مدیریت امنیت اطلاعات فدرال فیسما را بنویسید؟

هدف مشخص مدیریت امنیت رایانه ای فدرال فیسما FISMA ، مدیریت امنیت رایانه ای در گسترهٔ دولت است، و باعث می شود همهٔ تلاشهای انجام شده برای ایمن سازی اطلاعات با یکدیگر هماهنگ شوند و نیز راهکاری برای تهیه و پشتیبانی حداقل کنترلهای لازم جهت حفاظت از سیستم های اطلاعاتی دولت ارائه گردد . قانون تصدیق می کند که محصولات تجاری راه حلهای مؤثر و پویایی برای دولت فراهم می سازند و انتخاب راه حلهای امنیتی سخت افزاری و نرم‌افزاری خاص به سازمان‌های تخصصی واگذار می گردد.

ضمیما می گویند که رئیس هر سازمان باید یک برنامه امنیت اطلاعات در حیطهٔ سازمان خود تهیه، مستندسازی و اجرا کند.

۲۳- فیسما برنامه ای که برای امنیت اطلاعات برای در سازمان ها تعیین کرده شامل چه مواردی می باشد ۵ مورد را بنویسید؟

۱- ارزیابی متناوب مخاطرات و میزان آسیبی که ممکن است به دلایلی چون دسترسی غیرمجاز به اطلاعات واقع شود.

۲- تدوین سیاستها و روال‌هایی که: بر اساس فرآیند ارزیابی مخاطره هستند؛ منجر به کاهش هزینه های مخاطرات امنیتی می شوند؛ اطمینان می دهند که امنیت اطلاعات در چرخهٔ حیات سیستم اطلاعاتی هر سازمان بصورت کامل درنظر گرفته شده است؛ و اطمینان می دهند که الزامات و استانداردهای امنیتی ادارهٔ مدیریت و برنامه ریزی براورده می شود.

۳- تهیهٔ طرحهای فرعی برای فراهم کردن امنیت اطلاعات در سطح کافی برای شبکه ها، امکانات، و سیستمها یا گروههای سیستمهای اطلاعاتی؛

۴- برگزاری دوره های آموزشی برای افزایش آگاهی امنیتی کارکنان سازمان، پیمانکاران و سایر کاربران سیستمهای اطلاعاتی که در سازمان کار می کنند؛

۵- سنجش و ارزیابی متناوب اثربخشی سیاستهای امنیت اطلاعات، روال‌ها و تجربیات، که شامل آزمودن کنترلهای مدیریتی، عملکردی و فنی می باشد؛

۶- یک فرآیند برای طراحی، اجرا، ارزیابی و مستندسازی عملیات برای جبران نقائص در سیاستها، روال‌ها، و عملکردهای امنیت اطلاعاتی سازمان؛

۷- روال‌هایی برای شناسایی، گزارش و پاسخ به وقایع امنیتی؛ و

۸- طرحها و روال‌هایی برای اطمینان از تداوم فعالیت سیستم های اطلاعاتی سازمان.

۲۴- در خصوص کیفیت و اثر بخشی سیاست ها، فرایندها و عملکردهای امنیت اطلاعات سازمان ها باید چه اقداماتی را انجام دهد؟

هر سازمان باید به نمایندهٔ ادارهٔ مدیریت و بودجه ریزی و کمیته‌های کنگره‌ای، یک گزارش سالیانه ارائه نماید . علاوه بر آن میزان کفایت و تأثیرگذاری سیاست های امنیت اطلاعات، روندها و عملکردها باید در تعدادی از طرح ها و گزارشات ارائه گردد از جمله آن دسته که وابسته به بودجهٔ سالیانهٔ سازمان، مدیریت مالی، حسابرسی داخلی و کنترل های راهبری هستند . چنانچه در سیاست ها، روال‌ها و عملکردها هرگونه اشکالی پیدا شود باید این اشکال به ادارهٔ مدیریت و برنامه‌ریزی گزارش شود. سازمان‌ها باید همه ساله ارزیابی امنیتی مستقلی را برای مشخص کردن تأثیر برنامهٔ امنیت اطلاعاتی و عملکردهای خود ارائه دهند. هر ارزیابی دو قسمت دارد : قسمت اول شامل بررسی تأثیر سیاستها، فرآیندها و عملکردهای امنیت اطلاعاتی هر زیربخش سیستم اطلاعاتی سازمان است و قسمت دوم یک ارزیابی از سیاست‌ها، روال‌ها، استانداردهای و خط‌مشی‌های امنیت اطلاعات مرتبط است.

۲۵- دولت ها در انتقال مسئولیت های قانونی سنتی به حوزهٔ فضای سایبر چه نقشی دارند؟

۱- نحوهٔ تطبیق مسئولیت‌های سنتی قانونی به حوزهٔ مسائل امنیت سایبر

۲- قوانین مرتبط با ادارهٔ سازمان، حسابداری، و ثبت و فروش اوراق بهادار

۳- قانون قرارداد

۴- قانون جرائم غیرعمدی

۲۶- قوانین مرتبط با ادارهٔ سازمان، حسابداری، و ثبت و فروش اوراق بهادار را شرح دهید؟

طبق قوانین سازمان، مدیران و مسئولان ممکن است در قبال سازمان و سهامداران آن تعهد کنند که پیش بینی دقیقی از عملیات تجاری سازمان ارائه نمایند . این پیش بینی، شامل موضوعاتی چون امنیت رایانه‌ای نیز می شود. برخی صاحب نظران معتقد هستند اگر مدیران از برداشتن گام های مناسب برای ارزیابی تهدیدات امنیتی خودداری کنند، درصورت متضرر شدن، در قبال سهامداران شرکت، مسئول خواهند بود. در ایالات متحده امریکا تصویب شده است که امنیت الکترونیکی برای ارزیابی داده‌های مالی شرکتها ضروری است. همچنین طبق قانون عام شرکتها، سازمان‌های تجاری عمومی باید توسط حسابرسان غیروابسته تحت حسابرسی مالی قرار گیرند. درصورتیکه حسابرسان متوجه شوند آسیب پذیریهای الکترونیکی اسناد مالی شرکت را تهدید می کنند، شاخصهای امنیت الکترونیکی را نیز به حیطهٔ حسابرسی خود اضافه می سازند.

۲۷- قانون قرار داد را شرح دهید؟

طبق قانون قرارداد، سازمان‌ها باید مسئولیت دسترسی غیرقانونی به داده مشتریان یا آسیب های ناشی از نقائص امنیت الکترونیکی به داده‌های مشتریان را بر عهده گیرند . طبق این قانون، شرکتی که در متون الکترونیکی اعلام می دارد که "از یک سیستم ایمن برخوردار است "، اینگونه فرض می شود که با مشتری خود وارد یک توافق دوطرفه شده است که طبق آن شرکت موظف به تعامل با مشتریان در محیطی امن است. در چنین حالتی، درصورتیکه امنیت اطلاعات مشتری با حملات الکترونیکی به خطر بیافتد مشتری می تواند ادعای نقض تعهدات کند . همچنین شرکتهایی که خدمات مبتنی بر وب ارائه می نمایند بر حسب قرارداد ممکن است ، مسئولیت در دسترس بودن خدمات خود را بر عهده گرفته باشد . در اینحالت نیز درصورتیکه پایگاه وب در اثر حملات DOS (تخریب سرویس) از فعالیت و ارائه سرویس باز بماند، مشتریان می توانند ادعای نقض تعهدات بنمایند.

۲۸- قانون جرائم غیرعمدی را شرح دهید؟

از نظر حقوقی، مفهوم جرائم غیرعمدی (مسئولیت مدنی در قبال خسارت های عمدی) در مورد انواع آسیب های امنیت رایانه ای بکار می رود. بعنوان مثال با درنظر گرفتن قانون سنتی جرائم برای جرائم رایانه ای، درصورتیکه شرکت اقدامات منطقی برای حفاظت از اطلاعات مشتری در مقابل حملات الکترونیکی در پیش نگیرد، مشتریان می توانند نقض تعهدات نمایند. هنگامی که رایانه های یک شرکت برای انجام حملات الکترونیکی به یک مقصد ثالث بکار گرفته می شوند، درصورتیکه اقدامات مؤثر برای جلوگیری از سرقت رایانه ای انجام نشده باشد، ممکن است هم شرکت و هم شرکت ثالث مقصر شناخته شود . زمانیکه حمله ای توسط یکی از کارمندان شرکت صورت گرفته باشد قربانیان می تواند با اثبات این موضوع شرکت را متهم به نادیده گرفتن ضوابط و معیارهای لازم استخدامی یا نظارتی نیز نمایند.

۲۹- نقش های غیر قانونی گذاری دولت در امنیت سیستم های رایانه ای بخش خصوصی را بنویسید؟

حذف

۳۰- NIST یا موسسه ملی استاندارد و فناوری ایالات متحده برای ارتقای امنیت سیستم های اطلاعاتی چه فعالیت هایی انجام می دهند؟

۱- افزایش آگاهی دربارهٔ خطرات فناوری اطلاعات، آسیب پذیریها و نیازمندیهای حفاظتی؛

۲- تحقیق، مطالعه و ارائه توصیه به سازمان‌هایی که در معرض آسیب پذیریهای فناوری اطلاعات هستند؛

۳- ایجاد راهکارهایی برای برقراری امنیت در سیستم های حساس دولت؛

۴- تهیهٔ استانداردها، معیار ها، آزمونها و برنامه های اعتبارسنجی برای ارتقا، اندازه گیری و ارزشیابی امنیت در سیستم ها و سرویس ها؛
۵- تأمین حداقل نیازمندیهای امنیتی برای سیستم های دولت؛
۶- ارائه راهنماییهایی برای ایمن کردن فرآیندهای طراحی، پیاده سازی، مدیریت، و نیز عملیات فناوری اطلاعات؛

۳۱- استاندارد سازی را شرح دهید؟

دولت همچنین یکی از تصمیم گیرندگان مهم در تعیین استانداردهای بخش خصوصی است . استانداردسازی یک فرآیند غیر قانونی، داوطلبانه و مبتنی بر توافق جمعی است، اما متخصصان دولتی هم می توانند در این زمینه مشارکت کنند. بویژه اگر دولت از انجام تحقیقات امنیت رایانه‌ای بخش دولتی حمایت کند.

۳۲- نقش دولت ها در آموزش، آگاهی و ظرفیت سازی را شرح دهید؟

یکی دیگر از نقشهای غیرقانون گذاری دولت، آموزش عمومی و همکاری با بخش های خصوصی برای ارتقای آگاهی نسبت به آسیب پذیریها و روشهای پیشگیری است . مطالعات موردی و گزارش ها از ابزارهای اجرایی این هدف می باشند. اتحادیه اروپا از اعضای خود خواسته که برنامهای برای آموزش و آگاهی عمومی تدوین کنند که همهٔ طیف های مخاطبین را در بر بگیرد . ارائه گزارشها و استراتژیهای مسئول به متخصصین در افزایش آگاهی مؤثر است . همچنین شامل بورسهای تحصیلی و برنامه های توسعه ای و افزایش سطح دانش منابع انسانی نیز می باشد.

۳۳- نقش دولت ها در اشتراک اطلاعات برای تامین امنیت اطلاعات بخش خصوصی را شرح دهید؟

یکی دیگر از نقشهای مهم دولت، اشتراک اطلاعات دربارهٔ آسیب پذیریهای امنیت رایانه ای، اخطار در مورد ویروسها و حملات جدید، ارائه پیشنهادات برای حل مشکلات، حمله های های امنیتی و الگوهای سلامت می باشد. دولت می تواند بودجهٔ مراکز تبادل اطلاعات نظیر مرکز فوریتهای امنیت رایانه ای (CERT) و مراکز همکاری که در سراسر جهان برپا شده اندرا تامین می سازد. دولتهای سراسر جهان ممکن است به اشکال مختلف در بخش خصوصی مؤسساتی ایجاد نماید که سیستم های اشتراک داوطلبانهٔ اطلاعات را راه اندازی کنند همچون مراکز اشتراک و تحلیل اطلاعات (ISAC) همچنین دولت می تواند برای تبادل بهتر اطلاعات امنیتی کمیته های خصوصی و عمومی ایجاد کند نظیر کمیتهٔ مشاوران امنیت ملی مخابرات (NSTAC) که متشکل از سی نمایندهٔ مهم صنعت ارتباطات، ارائه کنندگان خدمات شبکه ای، شرکتهای فناوری اطلاعات، و مقامات مسئول امنیت ملی و سیستم های ارتباطی اضطراری است. NSTAC همچنین مشاور صنعتی رئیس جمهور در خصوص مشکلات مرتبط با امنیت ملی و آمادگی در شرایط اضطراری در سیستم های ارتباطی است.

۳۴- دولت ها چگونه توسط منع قوانین جرائم می توانند از سیستم های بخش خصوصی پشتیبانی کنند؟
حذف

۳۵- انواع قوانینی که در مورد جرائم الکترونیکی هستند را شرح دهید؟

۱- دزدی داده ها : نسخه برداری تعمدی یا عمدی و غیرمجاز از داده های خصوصی رایانه ای افراد نظیر نسخه برداری از ایمیل اشخاص این قوانین به قصد حفاظت از محرمانگی اطلاعات تهیه می شوند. در این مورد می توان به این نکته اشاره کرد که بیشتر نظام های قانونی دنیا، ردیابی بدون مجوز مکالمات تلفنی را جرم می دانند؛ و این مفهوم در جهان ارتباطات تلفنی می تواند کارکرد در حوزهٔ فضای سایبر نیز عملکرد مشابه داشته باشد.
۲- تداخل داده ها : تخریب، حذف، یا تغییر تعمدی و غیرمجاز داده ها در رایانهٔ دیگران نظیرارسال ویروسهایی که فایلها را حذف می کنند، یا به رایانه ای نفوذ کرده و باعث تغییر داده ها می شوند، یا به یک پایگاه وب نفوذ کرده و شکل ظاهری آن را تغییر

می دهند، همه جزء این دسته محسوب می شوند . شناسایی عنصر قصد و نیت برای تمایز میان فعالیتهای تبهکارانه و اشتباهات معمول و یا ارسال تصادفی ویروسها بسیار حیاتی است.

۳- تداخل سیستم : جلوگیری غیرمجاز از فعالیت سیستم رایانه ای بصورت تعمدی از طریق ورود، انتقال، تخریب، حذف، یا تغییر داده های رایانه ای است. نظیر حملات DOS یا ورود ویروس به یک سیستم به گونه ای که با کارکرد طبیعی آن تداخل داشته باشد باشیم.

۴- دسترسی غیرقانونی : دسترسی تعمدی و غیرمجاز به سیستم رایانه ای شخصی دیگر که در فضای الکترونیکی مترادف مفهوم تعدی است. در برخی سیستم های حقوقی تعریف دسترسی غیرقانونی محدود به موقعیتهایی است که اطلاعات محرمانه مثل اطلاعات پزشکی یا مالی دریافت، نسخه برداری یا مشاهده می شوند.

۳۶- منظور از جرائم تسهیل شده توسط رایانه ها را شرح دهید؟ دولت در اینگونه موارد چه کمکی می تواند جهت حفظ امنیت را انجام دهد؟

تخلفاتی همچون سرقتهای ادبی و فکری یا نمایش تصاویر مبتذل جرائم رایانه ای محسوب نمی شوند، بلکه تخلفاتی هستند که توسط رایانه تسهیل می شوند. در بسیاری موارد، مجازات های جرائم موجود، در فضای واقعی برای جرائم اینترنتی نیز اجرا گردد تحلیل دقیق عوامل مختلف اینگونه جرائم نیازمند بررسی تطبیقی قوانین جنایی موجود در حوزۀ جرائم فضای سایبر است، و در این راستا باید میان تخلفات رایانه ای و جرائمی که توسط رایانه تسهیل می شوند تفاوت قائل شد. ممکن است در برخی نظام های حقوقی، بکارگیری ضوابط خاص برای جرائمی که بوسیلۀ رایانه تسهیل می شوند ضروری نباشد. همچنین ممکن است این قوانین با درنظر گرفتن مجازات های نامتناسب جرائم در فضای سایبر را بدتر از جرائم دنیای واقعی جلوه دهد.

۳۷- کاربرد مفاهیم پایه ای قانون جزائی در فضای سایبر را شرح دهید؟

کشورها ممکن است بخواهند مفاهیم معمول در قوانین جرائم نظیر در جرم یا قصد انجام جرم را نیز در حوزۀ جرائم الکترونیکی در نظر بگیرید. بنابراین در صورتیکه قانون جرائم عادی مفهوم قصد تخلف را تعریف کرده باشد، در مورد جرائم الکترونیکی نیز می توان همان مفهوم را بکار برد . بعنوان مثال فرستادن یک ویروس به قصد تخریب سرویس حتی اگر ویروس بدرستی عمل نکند ممکن است تحت عنوان جرم و یا قصد انجام جرم مطرح شود. به همین ترتیب اگر قوانین مفهوم معاونت در جرم تعریف شده باشد، در حوزه جرائم الکترونیکی نیز از همان تعاریف استفاده کردیم، بطور مثال اگر کسی بصورت عمدی یک ویروس تولید کند، حتی اگر ویروس توسط شخص دیگری به یک شبکه منتقل کرده باشد، باز هم شخص تولیدکننده در قبال خرابی هایی که آن ویروس در داده ها و شبکه ایجاد می کند مقصر شناخته می شود.

۳۸- نقش دولت ها در حفاظت از حریم خصوصی افراد را شرح دهید؟

بسیاری از کشورها روال های قانونی دارند که به دولت اجازه می دهد اطلاعات ذخیره شده در رایانه ها را بررسی کند. نظیر دستورات قضایی برای بررسی داده های ذخیره شده و یا حکم تصرف و انجام تحقیقات روی رایانه ها و داده های رایانه ای باشند . همچنین بسیاری از کشورها اجازه ردیابی بلادرنگ ارتباطات و داده های انتقالی را می دهند که نشان دهندۀ مبدأ و مقصد ارتباطات است. معاهدۀ اتحادیه اروپا در مورد جرائم الکترونیکی، دولت ها را ملزم می کند که برای تحقیق و ردیابی اسناد رایانه ای، ردیابی ارتباطات، و گزارش هر نوع ثبت رایانه ای به دولت از قوانین خاصی استفاده کنند. گزارشگیری اجباری از داده های ذخیره شده در رایانه ها و ردیابی ارتباطات و داده های انتقالی توسط دولت منجر به نقض حریم خصوصی افراد می شود و بنابراین نیاز به استفاده از روال های محافظتی بیش از پیش احساس می گردد. همانگونه که OECD در خط مشی های خود در مورد امنیت شبکه ها و سیستم های اطلاعاتی اظهار می کند : معیارهای امنیتی باید بگونه ای پیاده سازی شوند که در راستای ارزشهای مشخص شده از طرف جوامع دموکراتیک از جمله آزادی تبادل افکار و ایده ها، جریان آزاد اطلاعات، محرمانه بودن اطلاعات و ارتباطات، حفاظت مناسب از اطلاعات شخصی، و شفافیت باشد.

۳۹- اتحادیه اروپا در بند ۱۵ معاهده جرائم الکترونیکی چه نکاتی را شرح می دهد؟

۱- هر سازمان باید به تدوین، پیاده سازی و کاربرد این روال هایی در ضوابط و قوانین محلی خود برای تأمین حفاظت مناسب از حقوق و آزادیهای بشر، توجه لازم را کرده باشد.

۲- این ضوابط باید به همان اندازه که طبیعت آنها ایجاب می کند نظارتهای قضایی و سایر نظارت های مستقل را در بر بگیرند، باعث تنظیم کاربردها شوند، و موجب کاهش محدودیت های دامنه ای و زمانی روالها را فراهم کند.

۴۰- ۶ روش های ردیابی قانونمند ارتباطات بر اساس استانداردهای ملی و بین المللی را بنویسید؟

۱- استانداردهای ردیابی شفاف و قوانین در دسترس عموم باشند؛ و بطور کامل، دقیق و شفاف شهروندان را از چگونگی و شرایط نظارت آگاه سازند؛

۲- تأیید ردیابی بصورت کتبی و از طریق یک مقام مستقل صورت گیرد و بر اساس تقاضای کتبی و ارائه دلایل و اسناد معتبر و قابل قبول انجام شود؛

۳- نظارت تنها محدود به بررسی درگیریهای جدی و خاص باشد؛

۴- تأیید تنها درصورت وجود دلایل قوی که نشاندهندهٔ لزوم انجام تحقیق درباره تخلفات است صورت پذیرد؛

۵- تأیید ردیابی تنها در مواردی انجام گیرد که استفاده از سایر فنون برای کسب اطلاعات کافی نباشد؛

۶- اشخاص و مواردی که باید تحت نظر قرار بگیرند با جزئیات کامل مشخص شوند و در این خصوص موارد کلی به هیچوجه قابل قبول نباشند؛

۷- ضوابط از نظر فناوری خنثی باشند یعنی با تمامی ارتباطات اعم از تلفنی، تصویری، داده خطوط سیمی به یک شکل برخورد شده باشد؛

۸- حوزه و مدت زمان انجام نظارت محدود باشد و در هیچ موردی طولانی تر از زمان لازم برای کسب اطلاعات مورد نظر نباشد؛

۹- نظارتها به طریقی انجام گیرد که حداقل نقض حریم خصوصی را در پی داشته باشد؛

۱۰- قوانین، کاربرد اطلاعات حاصل از ردیابی را توضیح داده باشند؛ و آن اطلاعات برای اهداف دیگری اطلاعات استفاده نشود؛

۱۱- قانون روالهای صدور حکم برای متهم را مشخص کرده باشد؛

۱۲- چنانچه طبق استانداردها حریم خصوصی کسی در جریان انجام عملیات ردیابی مورد تجاوز قرار بگیرد، طبق قانون، جبران کلیهٔ خسارت های وارده الزامی باشد.

۴۱- مواردی که موسسات مالی باید در حفظ امنیت رعایت کنند را بنویسید؟

- سیستم های نرم افزاری و دیواره های آتش باید به بالاترین درجهٔ امنیت مورد نیاز مجهز شوند، و در جهت تقویت، به روزرسانی و اقدامات پیشنهادی دیگر از طرف فروشندگان سیستم گام بردارند؛
- تمامی رمزهای عبور اولیه در سیستم های جدید باید فورا پس از نصب تغییر داده شوند؛ چراکه مهاجمین در حد وسیعی از آنها آگاهی دارند؛

- دیواره های آتش باید در میان شبکه های داخلی و خارجی و همچنین در میان پایگاههایی که از نظر جغرافیایی مجزا هستند نصب شوند؛
- نرم افزارهای ضد ویروس باید نصب و اجرا گردند.

۴۲- برنامه ای که بانک ها باید اجرا کنند شامل چه مواردی است؟

- تهدیدهای داخلی و خارجی قابل پیش بینی که منجر به افشا سازی غیرقانونی، سوء استفاده، تغییر و یا انهدام اطلاعات خریداران یا سیستم های اطلاعاتی خریداران است را مشخص سازد.
- احتمال و پتانسیل به فعلیت نرسیدن این تهدیدها را با توجه به حساسیت اطلاعات خریداران ارزیابی نماید.
- کفایت سیاستها، فرآیندها، سیستم های اطلاعات خریداران و سایر اقدامات کنترل مخاطره را ارزیابی کند.

۴۳- برای اجرای قوانین و برنامه امنیت چه تدابیری لازم است؟

- کنترل دسترسی به سیستم های اطلاعات خریداران (تصدیق هویت و مجوزهای دسترسی)؛
- محدودیت دسترسی به مکانهای فیزیکی؛
- رمزگذاری اطلاعات الکترونیکی خریداران؛
- تغییر روالهای مدیریتی؛
- استفاده از روالهای کنترل دوگانه (سیاست جداسازی وظایف و بررسی سوابق) برای کارمندانی که به اطلاعات خریدران، دسترسی دارند؛
- سیستم های نظارت بر نفوذ؛
- برنامه‌های واکنش به نفوذ ؛
- پیش بینی تدابیری برای حفاظت در برابر تخریب، دستکاری، یا حذف اطلاعات خریداران.

۴۴- کمیسیون تجارت ملی موسسات مالی تحت قلمرو خود را به تهیه چه طراحی وادار کند؟

- یک یا چند کارمند را برای تأمین امنیت انتخاب کنند؛
- در هر بخش از حوز ه های عملیاتی شرکت مخاطراتی که اطلاعات خریداران را تهدید می کند مشخص و ارزیابی کنند و اثربخشی سیستم کنونی برای کنترل آن مخاطرات را ارزیابی نمایند؛
- یک برنامهٔ حفاظتی را طراحی و اجرا کنند و آنرا بطور منظم مورد آزمایش و اصلاح قرار دهند؛
- ارائه کنندگان مناسب خدمات را انتخاب و با آنها برای پیاده سازی سیستم های امنیتی قرا رداد ببندند؛
- برنامه ها را در شرایط واقعی (مثل تغییر ساختار یا عملیات سازمان) ارزیابی و اصلاح کنند و با توجه به نتایج آزمایش، فرآیند نظارت را نیز ارزیابی و اصلاح نمایند.

۴۵- نکات اصلی قوانین امنیتی که باید مورد توجه موسسات قرارگیری را بنویسید؟

حذف