فصل هشتم:

مدیریت امنیت

ارایه دهندگان:

عطیه بزرگی زاده - آروز اخوان

- هنگام اجرای یک سیستم آنلاین یاددهی – یادگیری ، امنیت از اولویت خاصی برخوردار است. و همواره خطر هکرهای اینترنتی و صدها ویروس مخرب وجود دارد.

- مشکلات امنیتی می‌تواند در قسمت‌های متعددی از سیستم آنلاین یاددهی-یادگیری از قبیل شبکه ، سرویس وب ، سیستم‌های کامپیوتر سرور و سیستم‌های کامپیوتر کلاینت ، سیستم های پایگاه داده و غیره روی دهند.

- تیمی متشکل از مدیران شبکه ، مربیان و مدیران دانشگاه می بایست بر اساس قوانین دانشگاه و آسیب پذیری‌های احتمالی، سیاست‌های امنیتی سیستم یاددهی-یادگیری آنلاین را وضع کنند. این سیاست امنیتی ، به عنوان یک راهنما ، در چگونگی مقابله با مسائل مربوط به دسترسی، اطمینان، یکپارچگی و محرمانه بودن سیستم را شرح می دهد.

- ما برای تقویت معیارهای امنیتی به ابزارهای مدیریت امنیت نیاز خواهیم داشت که در این فصل مورد بررسی قرار خواهند گرفت.

پیش زمینه:

اجرای اقدامات امنیتی اغلب مستلزم تلاش زیاد تیمی متشکل از :

- ✓ کارمندان خدمات کامپیوتری
- ✓ مدیران دانشگاه
- ✓ اعضای کادر آموزشی دانشگاه
- ✓ کارکنان بخش پشتیبانی آموزش آنلاین

می باشند.

ارزیابی آسیب پذیری:

برخی عواملی که ممکن است موجب ضعف امنیتی شوند:

- وب سرور و سرویس هایی که توسط وب سرور میزبانی می شوند.
- سیستم مدیریت پایگاه داده و سرویس دستیابی از راه دور
- سیستم عامل و سرویس دایرکتوری یا فهرست ارائه شده توسط سیستم عامل میتواند عامی برای کمک به آسیب پذیری امنیتی باشد. فایلهای به اشتراک گذاشته شده با امنیت کم و دایرکتوری‌های میزبانی شده توسط سیستم عامل
- سیستم مدیریت یادگیری و سرویس های دست یابی از راه دور آن
- پیکر بندی نادرست دستگاه ها، پروتکل ها و سرویس های شبکه
- نقاط دسترسی در شبکهٔ بی سیم و انتقال داده از طریق فضا
- دانلود نرم افزار و نصب نرم افزار دانلود شده از اینترنت
- سیاستهای امنیتی ضعیف

- مشکلات امنیتی عمدتا به دلیل حملات هکرها و ویروس های کامپیوتری می باشند. با وجود اینکه اکثر حملات هکرها از اینترنت ناشی میگردند اما با اینحال تعدادی هکر داخلی خطرناک نیز وجود دارند. که به تعدادی از آنها اشاره می کنیم:

* هکرها اغلب یه حملهٔ محروم سازی از سرویس (DoS) را راه اندازی میکند که یکی از ساده ترین و متداول ترین روش های مورد استفاده بشمار می رود. یک DoS شبکه را با ترافیک شبکهٔ غیر قابل استفاده مواجه ساختته که این امر پهنای باند شبکه را اشغال می کند و به ایت ترتیب سرویس شبکه دچار ترافیک شدید شده و سرویس از کار می افتد.

* هکرها قادرند با امتحان کردن ترکیب های گوناگون رمز عبور وارد سیستم سرور شوند. همچنین می توانند از برخی نرم افزارهای رایگان برای اممتحان سریع تعداد بیشماری از رمزعبور ها استفاده کنند.

* هکرها ممکن است از جاسوس نرم افزار برای حمله استفاده کنند.

* هکرها قادرند با امتحان کردن ترکیب های گوناگون رمز عبور وارد سیستم سرور شوند. همچنین می توانند از برخی نرم افزارهای رایگان برای اممتحان سریع تعداد بیشماری از رمزعبور ها استفاده کنند.

* هکرها ممکن است از جاسوس افزار برای حمله استفاده کنند. آنها می توانند تعدادی وب سایت درست کرده و منتظر بمانند تا اشخاص به جستجو در اینترنت پرداخته و با نرم افزار کاربردی آنها تعامل برقرار کنند یا فایل های رایگانشان را دانلود نمایند. این تعاملات با نرم افزار کاربردی و یا فایلهای دانلود شده جاسوس افزار را به کامپیوتر وارد خواهد کرد. سپس جاسوس افزار به طور پنهانی اطلاعات افراد و کامپیوترشان را جمع آوری نموده و به آدرس وب سایت یا ایمیل هکرها انتقال می دهد.

* هکرها همچنین قادرند تا از حسابهای عمومی تهیه شده توسط وب سرورها، سرورهای پایگاه داده، سیستم های مدیریت یادگیری و سیستم های عامل استفاده کنند.

* هکرها می توانند بدون اتصال فیزیکی به شبکه، یک شبکهٔ بی سیم را شنود کنند.

* ابزارهای رایگان نظارت بر شبکهٔ متعددی در اینترنت قابل دسترس هستند. یک هکر میتواند یکی از اینها را دانلود و نصب کند تا ترافیک شبکه را به دست گیرد. اگر داده ها رمزگذاری نشده باشند، هکر قادر است تا تمامی اطلاعات انتقال یافته توسط یک پروتکل ارسال شبکه، حتی نام کاربری و رمزعبور را بخواند.

* اجزای تعاملی وب مانند کنترل های ActiveX و اپلت های جاوا میتوانند مشکلات امنیتی مهمی را موجب شوند. هکر ها می توانند از این برنامه ها جهت گذر از یک فایروال به منظور نفوذ به یک شبکهٔ خصوصی استفاده کنند.

* راه دیگر آسیب رساندن به سیستم استفاده از اشکالات نرم افزاری است. این اشکالات باعث ایجاد شکاف امنیتی می شوند که هکر را قادر به می سازد اطلاعات مربوط به کاربران را جمع آوری کند.

* هکرها ممکن است قادر باشند ابزارهای کاربردی آنلاین تهیه شده توسط سیستم مدیریت پایگاه داده یا سیستم مدیریت یادگیری را به کار گیرند و اسکریپت های مضری را که به منظور آسیب رسانی ایجاد شده اند اجرا کنند.

می توان با پیکربندی صحیح سیستم‌عامل و نرم‌افزار کاربردی از اکثر مشکلات امنیتی ایجاد شده توسط هکرها اجتناب ورزید.

فایروال ها نخستین محافظ یک سیستم یاددهی – یادگیری آنلاین محسوب می شوند.

- برای حفاظت از شبکهٔ دانشگاه در برابر وب سایتهای مستهجن و هکرهای آسیب رسان
- بعنوان یک فیلتر جهت محدود کردن بسته ها و پروتکل های شبکه
- شناسایی آسیب پذیری های امنیتی از طریق مقایسهٔ ترافیک شبکهٔ وارده با اطلاعات معتبر

برای جلوگیری از ورود هکر به سیستم با استفاده از امتحان کردن رمز عبورهای متعدد سیستم باید یک سیاست قوی رمز عبور به اجرا بگذارد و دفعاتی که یک کاربر قادر است رمز عبور نادرست وارد کند را محدود سازد. و با افزایش تعداد دفعات، سیستم ورود کاربر را مسدود می نماید.

علاوه بر حملات هکرها، یک سیستم یاددهی-یادگیری آنلاین ممکن است دچار آلودگی به ویروس کامپیوتری گردد. آلودگی ویروس کامپیوتری می تواند از طرق مختلف، از گم کردن فایلها گرفته تا از کار انداختن کل سیستم، آسیب رساند. به چند نوع از ویروسها اشاره میکنیم:

ویروس راه اندازی: می تواند از فرایند راه اندازی یک کامپیوتر آغاز شود. قادر است با بازنویسی یا جایگزینی برنامه راه انداز به کامپیوتر صدمه بزند. ویروس خود را در حافظه کامپیوتر بارگذاری میکند تا مانع اجرای راهاندازی به صورت طبیعی شود.

ویروس برنامه: زمانی فعال می شود که کامپیوتر در حال اجرای فایلی با پسوندهایی مثل BIN, COM, EXE, OVL, DRV, DLL,SYS است. این ویروس میتواند داخل حافظه بارگذاری شود و سایر فایل های اجرایی، که پیش از فایل آلوده اجرا شده اند را آلوده سازد. با کپی شدن برنامه آلوده در کامپوترهای دیگر نیز این ویروس منتقل می شود.
معروف ترین این ویروسها SUNDAY و Cascade می باشند.

ویروس اسب تروا: همانند یک ویروس برنامه، فایلی اجرایی می باشد. تفاوت آن در این است که اسب تروا خود را در حافظه بارگذاری نمی کند. در عوض خود را به جای یک بازی جا میزند یا ادعای انجام کارهای مفید مثل ویروس کشی میکند. سپس منتظر میماند تا کسی انرا دانلود و باز کند. معروفترین این دسته Beastو Biforse هستند.

ویروس مخفی‌کار: کامپیوتر را به شکلی مخفیانه آلوده میکند و متعاقبا شناسایی آن دشوار است. قادر است خود را در فایلی معمولی پنهان کند و اندازه فایل را به گونه ای تغییر دهد که با اندازه فایل اصلی یکسان باشد و به این ترتیب نرم افزار آنتی ویروس نمیتواند آنرا پیدا کند. معروف ترین این ویروسها Joshiو Whaleمی باشند.

ویروس چندشکلی: مثل ویروس مخفی کارهویت خود را پنهان میکند. و قادر است ظاهر خود را هربار هنگام آلوده سازی تغییر دهد. ممکن است نرم افزار آنتی ویروس قادر به شناسایی همه انواع ویروسها نباشد. بنابراین برخی از این ویروسها ممکن است باقی بمانند و به اسیب رسانی ادامه دهند. حذف این ویروس بسیار مشکل است. معروف ترین این ویروسها Cascade و Virus 101می باشند.

ویروس ماکرو: این ویروس زمانی فعال میشود که یک فرد فایل آلوده دارای ماکرو را باز میکند. فایلهایی مثل فایهای پردازش کلمات، یا فایلهای صفحه گسترده ممکن است شامل ماکروها باشند. با کپی شدن فایلهلی آلوده در کامپوترهای دیگر نیز این ویروس آن کامپیوتر را نیز آلوده خواهد کرد. معروفترین این دسته WM/Helper.C;D;E و W97M/kiamهستند.

ویروس جاوا یا اکتیو اکس: این ویروسها میتوانند از طریق مرورگرهای وب گسترش یابند. با کلیک کردن کاربر روی کلید یا لینک که ویروس پشت آن مخفی شده، ویروس به وسیله صفحه وب باز شده، کنترل کامپیوتر را در دست می گیرد. معروف ترین این ویروسها JS. Exception و Bubbleboy می باشند.

ویروس ایمیل: این ویروسها میتوانند از طریق پیامهای ایمیل انتشار یابند. قادر است به صورت خودکار خود را به تمامی ایمیلهای ثبت شده در فهرست پستهای الکترونیکی کامپیوتر مورد تهاجم ارسال نماید. با کپی شدن فایلهلی آلوده در کامپوترهای دیگر نیز این ویروس آن کامپیوتر را نیز آلوده خواهد کرد. معروف ترین این ویروسها W32/Mytob.gen@MM و Mimailمی باشند.

ویروس کرم: کرم نوعی ویروس است که اغلب یک شبکه را آلوده میکند. کرم بعد از ورود به شبکه آن را اسکن میکند تا شکافهای امنیتی آن را بیاید. همچنین میتواند از طریق مصرف پهنای باند به شبکه آسیب بزند. برخلاف سایر ویروسها که اغلب نیازمند حمل شدن توسط برنامه های دیگر هستند تا خود را منتشر کنند، کرم میتواند خود را تکثیر کند.

معروفترین این دسته W32/Bolgimoو Supernova Wormهستند.

هریک از انواع این ویروس‌ها می‌توانند خسارات جبران ناپذیری به سیستم وارد کنند. باید اقدامات امنیتی مناسبی را اجرا کرد تا از آلوده شدن کامپیوترها و شبکه ها توسط این ویروسها جلوگیری نمود.

نکاتی جهت کاهش احتمال آلودگی کامپیوترها به وسیله ویروس:

دانلود فایل: دانلود و نصب فایل از اصلی ترین راه های ورود ویروس به کامپیوتر است. باید توجه کنیم که از سایتهای مورد اطمینان دانلود انجام دهیم و همچنین با نحوه پاک کردن فایلهای آلوده آشنا شویم.

سرور وب و مرورگر وب: تکنولوژی های مرتبط با وب جزو آسیب پذیر ترین قسمتها در برابر حملات ویروسی بشمار می روند. ویروسها میتوانند از طریق مرورگرهای وب در یک سیستم کلاینت یا سرور دانلود شوند. برخی ویروسها قادرند تا در فایلهای چندرسانه ای و فایلهای کاربردی دسکتاپ همچون فایلهای صفحه گسترده و واژه پرداز پنهان شوند. بمحض اینکه مرورگر وب این فایلها را باز کند سیستم کامپیوتر به این ویروس ها آلوده خواهد شد. کاربر باید مراقب باشدتا فایلها را از منابع ناشناس دانلود و اجرا ننمایند.

نرم افزار کاربردی: نرم افزار کاربردی در حال اجرا مثل نرم افزار چند رسانه ای، سیستم های مدیریت پایگاه داده، سیستم های مدیریت یادگیری و همچنین برنامه های دسکتاپ می توانند باعث ایجاد خطرات امنیتی شوند.

سیاست های امنیتی

یک سیاست امنیتی، مجموعه ای از مقررات و تکنینک ها، در خصوص آنچه که باید محافظت شوند و چگونگی محافظت از آنها می باشد. که این سیاستها توسط تیمی متشکل از مدیران سیستم و شبکه، روسای موسسه، توسعه دهندگان نرم افزار، اعضای هیئت علمی و کارکنان بخش پشتیبانی آموزشی وضع می گردد.

این تیم باید هنگام وضع سیاست های امنیتی این مسائل را مدنظر قرار دهد:

- **محرمانه بودن:** اطلاعات محرمانه را دور از دسترس افراد غیر مجاز نگه دارد.
- **یکپارچگی:** از تغییر عمدی و غیر عمدی اطلاعات محرمانه جلوگیری شود.
- **دسترس پذیری:** از قابلت مشاهده و اصلاح اطلاعات توسط افراد مجاز در هر زمان که بخواهند اطمینان حاصل نماید.

محرمانه بودن

برای افزایش محرمانه بودن در سیستم آنلاین یاددهی-یادگیری سیاست امنیتی میتواند برخی مقررات را وضع نماید:

- سیاست امنیتی در خصوص مقررات مربوط به تایید سیستم، واضح و آشکار باشد. و مشخص باشد چه کسانی به کدام اطلاعات و کدام کامپیوتر و دستگاه های شبکه حق دسترسی دارند.

- سیاست امنیتی باید دستورالعمل هایی را به منظور چگونگی حفاظت داده ها از دستیابی افراد غیرمجاز به آن تهیه نماید.
- سیاست امنیتی باید شامل قواعد رمز عبور قوی ای باشد تا دستیابی به رمزهای عبورهای کاربر را دشوار سازد.
- سیاست امنیتی باید قوانینی را در خصوص چگونگی نظارت و بازرسی سیستم یاددهی-یادگیری آنلاین در برگیرد. و مشخص کند که چه کسی میتواند فرایند نظارت و بازرسی را اجرا کند.

یکپارچگی

برای جلوگیری از تغییر عمدی و غیرعمدی داده ها به وسیله افراد غیر مجاز، سیاستهای امنیتی باید مجموعه ای از مقررات را وضع کند که مشخص می سازد کاربر چه دادههایی را می تواند اصلاح کند و چگونه این داده ها انتقال یافته در شبکه را می تواند محافظت نماید. برخی دستورالعمل ها:

- سیاست امنیتی مشخص کند که چه افرادی اجازه چه کارهایی را دارند.
- سیاست امنیتی پروتکل ها و روشهای رمز گذاری شده که جهت انتقال داده ها در اینترنت استفاده می شود را توصیه می نماید.
- سیاست امنیتی همچنین باید فرایندهایی را شامل شود تا از سرقت و تغییر اطلاعات حساس توسط هکرها جلوگیری نماید.

دسترس پذیری

برای حصول اطمینان از دسترس پذیر بودن اطلاعات برای کاربران مجاز، قوانین دسترس پذیری باید در سیاست امنیتی مشخص شده باشد. برخی دستورالعمل ها:

- سیاست امنیتی باید چهارچوب زمانی مناسبی رامشخص کند که بر اساس آن اطلاعات معین باید در دسترس کاربران واجد شرایط قرار گیرند.
- سیاست امنیتی باید مشخص کند که اطلاعات کجا در دسترس کاربران واجد شرایط قرار خواهند گرفت.
- سیاست امنیتی ممکن است چگونگی تحویل اطلاعات به کاربران واجد شرایط را مشخص سازد. مثلا از وب، ایمیل، ....

- ایجاد سیاست امنیتی یک فعالیت تیمی است و اجرای موفق آن به طور زیادی به میزان آموزش کاربران، درک و پیروی آنها از قوانین آن سیاست بستگی دارد.

هنگام ایجاد یک سیستم یاددهی-یادگیری آنلاین، سیاست امنیتی می بایست سیاست حفظ حریم شخصی را نیز شامل شود.

- سیاست امنیتی را می توان در مورد آزمونها، تکالیف، پروژه ها ونمرات دانشجویان اعمال کرد.

از توجه شما سپاسگزارم