
مجله اینترنتی
iT PORT
آی تی پورت
ما در گاه اتصال شما به
دهکده جهانی خواهیم بود!
مهمترین اخبار دنیای فناوری
بررسی تخصصی مباحث آی تی
و...
www.itport.ir

در سال های اخیر افزایش قابل توجهی در تعداد وب سایت های هک شده ثبت گردیده است. یکی از دلایل این افزایش تمایل افراد و شرکت ها به انتشار بد افزار ها و جهت دادن به نتایج جستجو در اینترنت به نفع خود است. و به این ترتیب با اهداف سود جویانه انگیزه هک کردن وب سایت ها افزایش یافته است .اگر شما هم یک مدیر وب سایت هستید اکنون وقت خوبی است تا با هم نکاتی را مرور کنیم که با رعایت آنها وب سایت خود را در ناحیه کم خطر قرار داده اید. البته امنیت یک وب سایت موضوعی پویاست و اگر به آن اهمیت می دهید بهتر است فقط به این مقاله بسنده نکنید و به عنوان یک مدیر سایت باید همیشه آخرین اطلاعات و اخبار امنیتی را داشته باشید.

موضوعاتی که در این مقاله می خوانید

اصول امنیت وب سایت

قبل از اینکه درباره امنیت وب سایت صحبت کنیم باید بگویم حمله ای که به یک وب سایت انجام می شود با حمله ویروس ها و کرم های اینترنتی متفاوت است.

حمله به وب سایت ها یا هک کردن یک وب سایت زمانی اتفاق می افتد که افرادی سعی می کنند با هدف خرابکاری یا دسترسی یا سوء استفاده از اطلاعات ذخیره شده در سرور آن وب سایت به سایت مذکور نفوذ کنند.

هر شخصی برای هک کردن وب سایت شما احتیاج به یک ورودی حفاظت نشده دارد تا از این طریق به سرور وب سایت شما نفوذ کند.

این ورودی ها سه محل هستند:

1-کامپیوتر شخصی شما که برای ارسال فایل های جدید به سرور (وب سایت) خود از آن استفاده می کنید.

2-از طریق هر فرمی که برای جمع آوری اطلاعات از بازدید کنندگان و کاربران استفاده می کنید.

3-از محل فیزیکی و جاییکه سرور وب سایت شما قرار دارد.

البته هنوز حفره هایی از طریق ویروس و کرم ها برای نفوذ به وب سایت شما وجود دارد اما این حفره ها در نرم افزارهایی که بازدید کنندگان سایت شما برای مشاهده وب سایت استفاده می کنند، مانند فایرفاکس، یا اینترنت اکسپلورر و ... وجود دارند و نه در خود وب سایت.

شما می توانید با استفاده از فایر وال مانع نفوذ و تکثیر کرم ها در شبکه خود شوید و می توانید جلوی ویروسی شدن سرور ایمیل خود را بگیرید. برای این منظور باید به کلیه همکاران خود آموزش لازم را بدهید و همیشه آخرین وصله های امنیتی را نصب کنید.

به عبارت دیگر اگر برای وب سایت خود یک سرور اختصاصی دارید و خود آنرا اداره می کنید باید از آخرین دستاوردهای فناوری های امنیتی بهره بگیرید و از افرادی که چنین دانشی دارند برای حفاظت اطلاعات خود استفاده کنید.

بعد از همه این حرفها باید بگویم اوضاع آنقدر هم خراب نیست و با استفاده از روش های ساده و مداوم می توانید احتمال هک شدن وب سایت خود را تا حد زیادی پایین بیاورید. و حفره ها را تا حد امکان مسدود کنید. سعی داریم در آینده اطلاعات بیشتری درباره امنیت وب سایت در یاد بگیر دات کام قرار دهیم.

چک لیست امنیتی برای مدیر یک وب سایت

تنظیمات سرور خود را چک کنید.

آپاچی در وب سایت خود نکاتی برای تنظیمات امنیتی ارائه داده است و اگر سیستم عامل سرور شما لینوکس است باید از آن مطلع باشید و همینطور مایکروسافت برای IIS منابع امنیتی مختلفی در وب سایت خود ارائه داده است. این اطلاعات و نکات درباره موضوعاتی از قبیل مجوزها، include سمت سرور ، معتبر ساختن و رمزگذاری می باشد.

باید آخرین وصله های منیتی را نصب کنید و نرم افزار ها را به روز رسانی نمایید.

تله ای که بیشتر مدیران وب سایت ها در آن گیر می افتند نصب یک انجمن یا بلاگ در وب سایت خود و سپس به امان خدا گذاشتن آن است. این مانند این است که یک اتومبیل گرانقیمت بخرید ولی برای آن هیچ دزدگیری نصب نکنید و آنرا شب ها بیرون از خانه پارک کنید. اولین قدم برای حفظ امنیت یک وب سایت این است که لیستی از نرم افزار ها و Plug in های نصب شده تهیه کنید و برای خود یک برنامه منظم برای بررسی آخرین نسخه ها و Update ها مشخص کنید تا در صورت لزوم آنها را به روز رسانی نمایید. یکی از ساده ترین راههای ردگیری این نرم افزار ها استفاده از فید یا RSS وب سایت هایی است که در زمینه امنیت فعالیت می کنند. بدین ترتیب در کمترین زمان مهمترین اخبار و رویداد های امنیتی را بدست می آورید.

به طور منظم فایل های Log خود را بررسی کنید.

اگر این کار را تبدیل به عادت کنید منافع زیادی کسب خواهید کرد. که یکی از آنها امنیت مضاعف است. و از اطلاعاتی که بدست خواهید آورد شگفت زده خواهید شد.

نقاط آسیب پذیر معمول را بررسی کنید

از ایجاد دایرکتوری های با مجوز آزاد برای همه اجتناب کنید. این مانند این است که در اصلی خانه خود را باز بگذارید و بالای آن بنویسید بفرمایید تو و از خودتان پذیرایی کنید.همچنین مراقب نقاط آسیب پذیری مانند XSS یا Cross-site scripting و SQL Injection باشید. و در نهایت یک پسورد خوب انتخاب کنید که هم از حروف و هم از اعداد تشکیل شده باشد و کلمه ای معنی دار نباشد.

مراقب محتویات تولید شده توسط افراد ثالث باشید

در اینترنت تعداد زیادی ابزار های کاربردی وجود دارد که می توانید آنها را دانلود کرده و به راحتی در وب سایت خود نصب کنید. از آن جمله می توان به ابزار های اندازه گیری ترافیک اشاره کرد هر چند ابزار های با ارزشی در اینترنت برای یک وب سایت پیدا می شود ولی بعضی از انها با اهداف نفوذ به وب سایت شما یا خرابکاری طراحی شده اند. آنها می خواهند اهداف خرابکارانه و آلوده کردن تعداد زیادی کامپیوتر را از طریق وب سایت شما انجام دهند بدون اینکه شما به عنوان یک مدیر وب سایت از این موضوع مطلع شوید. بنابراین باید در دانلود و نصب این ابزار ها باید بسیار محتاط باشید.

گوگل استفاده کنید site: از جستجوی

این کار بسیار بدیهی به نظر می رسد ولی معمولاً نادیده گرفته می شود. خوب عاقلانه است اگر هر از چند گاهی وب سایت خود را برای عاری بودن از بدافزار ها بگردید. فرض کنید نام وب سایت شما Yadbegir.com است کافیست در باکس جستجوی گوگل تایپ کنید

site: yadbegir.com

از Webmasters Tools گوگل استفاده کنید

اینجا جایی است که ابزار های رایگان و مفید متنوعی برای یک مدیر وب سایت وجود دارد. و درباره اینکه googlebot چگونه در وب سایت شما پرسه می زند هم اطلاعات جالبی بدست خواهید آورد. یکی از قابلیت های خوب Webmasters Tools این است که اگر گوگل بد افزاری را در وب سایت شما پیدا کند از آن اطلاع خواهید یافت. و زمانیکه مشکل وب سایت خود را برطرف کردید می توانید درخواستی برای بررسی مجدد وب سایت خود بفرستید. به این ترتیب علاوه بر اطلاع زود هنگام از بروز مشکل احتمال از دست دادن بازدید کنندگان وب سایت از سمت گوگل را به کمترین حد کاهش خواهید داد.

از پروتکل های امن استفاده کنید

برای انتقال اطلاعات بهتر است از SFTP و SSH به جای پرتکل های متنی ساده استفاده کنید. SFTP و SSH اطلاعات را کدگذاری می کنند و بسیار مطمئن تر هستند.

وبلاگ امنیتی گوگل را مطالعه کنید.

در این وبلاگ اطلاعات امنیتی با ارزشی وجود دارد همینطور منابع مختلفی به شما معرفی می کند.

از هاستینگ خود پشتیبانی بخواهید.

اکثر شرکت های هاستینگ معتبر که دومین و فضای وب سایت را به شما اجاره می دهند دارای متخصصین خبره ای در زمینه امنیت هستند. و هر گاه درباره امنیت وب سایت خود به مشکلی برخورد کردید یا دچار شک و تردید شدید کافیست به وب سایت آنها مراجعه کنید و یک پیغام بگذارید مطمئن باشید آنها برای امنیت سرور خود ارزش زیادی قائل هستند و برای بهبود آن کمک خواهند کرد.

امیدوارم این نکات به شما در بهبود امنیت وب سایت تان کمک کرده باشد خوب حال با بکار گیری این نکات و افزایش دانش خود مدیریت امن وب سایت خود را آغاز کنید.

رعایت نکات امنیتی برای مدیران وبلاگ

۱ -اغلب دوستانی از کلمه عبور ساده استفاده می کنند مثلا دوستی برای رمز عبورش از سال تولدش(۱۳۵۹) استفاده کرده بود یا رمز عبور دوست دیگری به صورت ۹۹۹۹ بود و دوست دیگری دوبار نام کاربری خود را انتخاب کرده بود که همانطور میبینید حدس زدن اینگونه رمزها برای کسانی که در صدد فرصت طلبی هستند زیاد هم دشوار نیست بنا براین توصیه می شود که از انتخاب رمزهای ساده جدا بپرهیزید و حتما از یک رمز با ترکیب عدد و حرف و سیمبل (symbol)استفاده کنید زیرا اغلب کاربران از فراموش کردن رمزشان می ترسند در حالی که هک شدن وبلاگ بسیار ترستناکتر است و در ضمن برای فراموش کردن میتوان به راحتی راهی پیدا کرد ولی برای هک شدن نه. (مثلا می توانید درخواست دهید تا رمز به ایمیل خصوصی شما ارسال شود) مثلا این رمز نمونه از امنیت بالایی برخوردار است.

مثال: h3&7pzn۲[۹#

حال اگر ایمیل خصوصی شما هک شود چه ؟ هک شدن ایمیل خصوصی تقریبا مساوی با هک شدن وبلاگ هم هست پس به شدت مواظب ایمیل خصوصی خود باشید و هیچگاه از آن جز برای کارهای بسیار خصوصی استفاده نکنید مثلا هیچگاه از آی دی خود در مسنجرها و خصوصا یاهو مسنجر استفاده نکنید زیرا حتما خودتان هم میدانید که هک شدن در مسنجری مانند یاهومسنجر چقدر راحت اتفاق می افتد.

۲ -مهمترین راه هک کردن یک ویلاگ این است که یک نرم افزار جاسوسی به سیستم کاربر راه یابد و همه اطلاعات محرمانه مانند رمزعبورها را جمع آوری کرده (بصورت خودکار) و سپس در هنگام اتصال به اینترنت بدون آنکه هرگز قربانی به چیزی مشکوک شود رمزعبورها را به ایمیل هکر ارسال کند پس همیشه یکی از آنتی ویروسهای معتبر دنیا را بر روی سیستم خود داشته باشید و در این رابطه بروز بودن آنتی ویروس شما از نوع آن مهمتر است . این آنتی ویروسها معمولا در خود یک فایروال هم دارند که مانع از نصب برنامه بدون اجازه ی شما حتی برنامه های مفید میشوند و قبل از آنکه شما بخواهید برنامه ای را آگاهانه یا غیرآگاهانه نصب کنید به شما اخطار خواهد داد که برنامه ای با فلان اسم قصد نصب شدن دارد پس همیشه مواظب پیامهایی که از طرف آنتی ویروس شما صادر می شود باشید و بدون اطلاع آنها را تایید نکنید شما اگرحتی کمی با زبان انگلیسی آشنا باشید می توانید معنی پیامها را درک کنید.

۳ -اگر از کامپیوترهای عمومی (کافی نت ها یا کامپیوتر دانشگاه و اداره) استفاده می کنید از پاک بودن آنها از هرگونه ویروس ، تروجان و برنامه ی جاسوسی اطمینان حاصل کنید و در صورتی که مطمئن نیستید از آن برای وارد شدن به مدیریت وبلاگتان استفاده نکنید . و در ضمن مواظب باشید که به سوالاتی که از شما برای بخاطر آوردنتان در یک سیستم کامپیوتری مشخص می شود پاسخ منفی بدهید (مثلا اگر برای اولین بار از یک سیستم کامپیوتری وارد بلاگفا شوید از شما سوال می شود که آیا می خواهید این کامپیوتر نام کاربری و پسورد شما را بخاطر بیاورد) و همچنین مراقب باشید که گزینه ی بخاطر سپاری شما که معمولا در کنار قسمت ورود هر سایت قرار دارد تیک نخورده باشد (مثلا یاهو مسنجر) . در ضمن آخرین رمزی که در بسیاری سایت ها وارد می کنید در ریجستری ویندوز باقی می ماند و بسادگی قابل دسترسی است برای جلوگیری از سواستفاده از این را در هنگام ترک کامپیوتر یکبار نام و رمز خود را اشتباه وارد کنید و تا به شما اخطار اشتباه بودن داده شود به این ترتیب رمزی که در ریجستری ویندوز باقی می ماند یک رمز اشتباه است.

۴ -همیشه هنگام وبگردی مراقب صفحه هایی که به آنها وارد می شوید باشید و روی هر لینکی کلیک نکنید و هنگام چت با دوستان اگر دوستتان برایتان لینکی فرستاد حتما از او بپرسید که او چنین لینکی فرستاده زیرا ویروسهایی هستند که با هک کردن دوستتان بدون اینکه خود دوست شما بداند خود را جای دوستتان جا می زنند و به این ترتیب به صورت

درختی و براحتی گسترش میابند زیرا شما نمی دانید که این لینک را واقعا دوستتان نفرستاده و ممکن است ویروسی وحشتناک در پشت لینک مخفی شده باشد.

۵ -هیچگاه به فردی که رمز عبور شما را از هر طریقی و با هر عنوانی درخواست می کند اعتماد نکنید و سعی کنید فاصله ی زمانی بین تغییر رمز خود را بسیار کوتاه کنید مثلا هر هفته یا حداقل هر ماه از یک رمز عبور استفاده کنید . البته بیشتر افراد سواستفاده گر از طریق ارسال ایمیل سعی می کنند رمز عبور شما را بدست آورند پس باز هم تاکید میکنم به ایمیلهایتان حساس باشید و در هیچ صورت ایمیلهایی که با خود فایل ضمیمه دارند را اگر از طرف افراد ناشناس است یه از طرف کسی است که به او اعتماد کامل ندارید باز نکنید حتی ممکن است که دوستان شما هم بخواهند برای شوخی کردن با شما وبلاگتان را هک کرد و مدتی به قول خودشان شما را اذیت کنند پس مراقب باشید.

چند نکته را باید رعایت کنند

- اسکریپت هایی را که میخواهید استفاده کنید حتما از سایت اصلی و پشتیبان دانلود و نصب کنید.
- بعضی اسکریپت ها که از سایت های مخصوص اسکریپت دانلود و نصب می شود مشکلات امنیتی دارند و به سایت و سرور صدمه وارد میکنند.
- در هنگام نصب اسکریپت از پلاگین های و ماژول های معتبر استفاده کنید.
- بعضی پلاگین ها و ماژول ها به سرور فشار زیادی وارد میکنند و بهتر است بی موردو برای تست از این نوع پلاگین ها استفاده نشود.

جلوگیری از هک شدن یاهو آیدیِ شما

در ابتدا به بررسی تمامی راههای هک و نفوذ یاهو میپردازم و سپس نکات مربوطه و امنیتی رو بیان میکنم :

1 – هک دیتابیس یاهو :

اولین راهی که به نظر هر فردی میرسد هک خود یاهو هستش که باید بگم ، عمرا ، این کار مستلزم دانش بسیار بالایی در هک هستش و اینگونه افراد یا پیدا نمیشوند و اگر هم پیدا شوند هیچ گاه دست به انجام این کار نخواهند زد ، چون این کار برای کِرَکر ها هستش نه یک هکر واقعی ، حالا اگر چنین شخصی هم پیدا بشود بیشتر از ۱ ثانیه نخواهد توانست که یاهو را هک کند ، به این دلیل که سیستم مانیتورینگ بسیار بالایی دارد و در ۱ ثانیه شناسایی تون میکنه و ریجکتتون خواهد کرد ،

2 – استفاده از صفحات LOGIN تقلبی :

که در این روش شخص مهاجم صفحه ی لاگین شبیه به لاگین یاهو رو ساخته و حالا به ترفند های مختلف شما رو تشویق به Login شدن با اون میکنه که در صورت Login شدن پسورد شما برای شخص ارسال میشود ..

3 – استفاده از "تروجان ها" ، "کی لاگرها" ، "Spy Ware ها" :

در این روش شخص کرکر باید با روش های مختلفی فایل مخرب خودش رو به سیستم شخص قربانی ارسال کند و اون رو آلوده کند که در صورت موفق بودن میتونه کنترل سیستم رو در دست بگیره و پسورد یاهو یا هر چیز دیگری رو بدست بیاره .. (در ادامه راه‌های انجام این کار رو بیان خواهم کرد)

4 – استفاده از Cracker های تشخیص پسورد :

که هم اکنون از رایج ترین روش ها به حساب می آید و به این صورت که شخص با دادن اصلاعات شخصی مثل تاریخ تولد و ... شما به نرم افزار کرکر از هوش مصنوعی اون استفاده میکند تا پسورد شما رو تشخیص بده که در صورت ساده بودن پسورد شما موفق هم خواهد بود ،

روش های دیگری هم وجود دارد که لازم به گفتنشون نیست و کلا از کار افتاده اند و من سعی کردم خلاصه راه ها رو بیان کنم ،،

ادامه‌ی بحث:

همانطور که گفتم روش ۱ به هیچ وجع امکان پذیر نیست و باید دورش خط کشید و روش ۲ هم دیگه Lose شده و همه میدونند و می‌مونه روش‌های ۳ و ۴ ،،

کرکرها در روش سوم از راه های مختلفی عمل میکنند ، که بستگی به قدرت برنامه نویسیشون داره ، و برای آشنا شدن شما با اون ها ، بیان میکنم :

– با ارسال فایل تروجان با پسوند اجرایی به ایمیل شما یا لینک دادن به صورت PM و با ترفندی شما رو ترغیب به دانلود فایل میکنند که در صورت دانلود شما و اجرای اون ، آلوده خواهید شد ..

– با استفاده از زبان برنامه نویسی وب مانند PHP یا Cgi فایل مخرب خودشون رو تحت وب به اجرا در می‌آوردند و شما تنها با باز کردن لینک اون سایت (بدون دانلود هیچ فایلی) آلوده خواهید شد .

– با دعوت شما به روم و با استفاده از spyware آلوده‌تون خواهند کرد ،

– با استفاده از تروجان سازهایی مانند magice_ps ، Jps1 ، yahoo spy ، Key loger 2 و ... و ارسال اون که کاره جوجه کرکرها هستش و اکثرا توسط آنتی ویروس‌ها شناسایی میشه (نکات امنیتی در این مورد رو هم در ادامه ذکر خواهم کرد و فعلا در حال معرفی هستم)

روش چهارم هم فقط و فقط به قدرت پسورد شما بستگی داره و البته تواناییه نرم افزار CracKer ..

کاربران یاهو به دو دسته تقسیم میشوند :

1 – افرادی که با PC آنلاین میشوند .

۲ – آفرادی که با Mobile توسط نرم افزار های رابط آنلاین میشوند .

که هر کدوم نکاتی جدا رو هم باید رعایت کنند ..

همیشه افرادی که با سیستم آنلاین میشن خطر بیشتری تهدیدشون میکنه تا افرادی که با Mob آنلاین میشوند ،

حالا نکاتی رو میگم که در ۲ گروه باید ٪۱۰۰ انجام بدند و رعایت کنند ..

1 – بخش اطلاعات (account info) ایمیل :

اول اینکه در هنگام ساخت آی دی یاهو هیچ کدام از گزینه ها را دست کم نگیرید ، به خصوص بخش ایمیل دوم و سول و جواب‌های امنیتی که به نظر من از خود پسود هم مهمتر هستش ، این قسمت ها رو به دقت وارد کنید و هیچ‌گاه از یاد نبرید (بهتره یک جا یادداشت کنید اگه یادتون میره) ، ایمیل دوم رو یک ایمیل مطمئا که واسه خودتون یا آشنایان نزدیک (در صورت امکان Gmail) وارد کنید ،، کارایی ایمیل دوم این هستش که در صورت هک آی دی یا فراموش کردن پسورد ، پسورد جدید به ایمیل دوم ارسال خواهد شد .. و همچنین در انتخاب پسوردتون بسیار دقت کنید (باز هم در ادامه توضیح خواهم داد)

اگر این کارها رو در هنگام ساخت آی دی انجام ندادید نگران نباشید ، به طریقه ی زیر عمل کنید :

– از طریق Yahoo! Messenger ، Sign In بشید و از منوی بالا بخش Messenger ، My account info رو انتخاب کنید ، یا از طریق سایت خود یاهو Sign In بشید ، در صفحه‌ی اصلی یاهو روی جایی که به شما سلام داده (Hi , Your Name) کلیک کنید و بعد روی account info کلیک کنید ..

- در هر ۲ حال صفحه‌ای در مرورگر شما باز خواهد شد که از شما پسوردتون رو میخواد ، پسورد رو وارد کنید و اینتر بزنید ..

- وارد صفحه‌ای خواهد شد که همون صفحه‌ی اطلاعات ایمیلتون هستش که دارای قسمت‌های زیادی هستش که مربوط به اطلاعات شخصی و ... میشه ، ما فقط با بخش Sign-In and Security کار داریم و دارای پنل های مختلفی هستش ،

- در قسمت اول (Change your password) شما میتونید پسوردی که در هنگام ساخت ایمیل انتخاب کرده بودید رو تغییر بدید و پسورد جدیدتون رو جایگزین کنید ..

- در قسمت دوم (Update password-reset info) شما خواهید توانست که سوال های امنیتی و جوابهاش رو تغیر بدید و همچنین ایمیل‌های دیگه‌ای رو به عنوان ایمیل دوم و سوم و بیشتر اضافه کنید ، حتما در این بخش آدرس ایمیل دیگه‌ای وارد کنید ، ایمیلی برای تایید به اون ایمیل ارسال میشه ، اون رو تایید کنید و اون ایمیل به عنوان ایمیل دیگه‌ی شما اضافه خوهاد شد که برای ریست پسوردتون به دردتون خواهد خورد ..

- قسمت های دیگر مربوط به چیزهایه دیگه هستش که تا همین جا کافی هستش ..

2 – انتخاب پسورد :

این همه حرف‌ها و صحبت‌های ما برای همین مسئله هستش ، شما باید تمام سعی تون رو در انتخاب پسوردی قوی‌تر بکنید ، در انتخاب پسورد به نکات زیر توجه کنید :

در پسودتون حتما از کارکترهای & (امپرساید) ، # (نامبرساید) و امثالش استفاده کنید که قدرت پسورد رو خیلی بالا خواهد برد ..

در انتهای پسوردتون از تعدادی Space (فاصله‌ی خالی) استفاده کنید ، در صورت هک شدن پسورد این فضا خالی ها ارسال نخواهد شد و تیر کرکر به سنگ خواهد خورد ..

پسورد یاهو آیدیتون رو از سایر پسوردهاتون که برای ثبت نام در سایر سایت ها استفاده میکنید متفاوت در نظر بگیرید ..

3 – یک آنتی ویروس خوب برای کامپیوترتان :

حتما یک آنتی ویروس خوب و آپدیت شده بر روی PC تون داشته باشید که کارش و به درستی انجام بده (نود رو پیشنهاد میکنم ، البته آپدیت شدش) به اضافه‌ی یه آنتی تروجان که Anti Trojan Elite در بینشون بهترین هستش ..

آنتی ویروس ها معمولا تروجان‌هارو شناسایی و پاک میکنند و به سادگی جلوگیری میکنند ، حتی اگه بخواد اجرا بشه ،، مگر اینکه تروجان با قدرت برنامه نویسی جدید و بالایی نوشته شده باشه که معمولا اینها به صورت Free وجود ندارند و هزینه‌های بالایی دارند ..

4 – از دریافت فایل‌ها و لینک‌های ناخواسته خودداری کنید :

هر فایل و لینکی رو از اینترنت دریافت نکنید ، به پسوند و فرمت هر فایل دقت کنید ، فرمت فایل ها مشخص هستش ، فرمت های اجرایی Pif , exe , com , bat , scr هستش که هیچ گاه نباید دریافت کنید ،، تروجان ها به این صورت برای شما ارسال میشوند ..

دقت کنید گول پسوندهایی به این صورت FileNaMe.jpg.scr رو نخورید ، این همون تروجان هستش و یه عکس نیست ..

گول آیکون فایل رو هم نخورید و حتما از فایل Properties بگیرید و نام کامل و پسوندش رو مشاهده کنید ..

در صورت ارسال چنین فایل‌هایی به شما به هیچ وجع دریافتش نکنید و صفحه‌ی مربوطه رو ببندید.

هیچ وقت از یک صفحه‌ی مشکوک یک سایت بازدید نکنید ..

در صورت Pm گرفتن‌های مشکوک از یک شخص مشکوک شخص رو Add نکرده و ignore بکنیدش .

اگه از روم یاهو استفاده میکنید اصلا با غریبه چت نکنید ..

۵ – پسوردتون رو در هر کاپیوتری وارد نکنید ، به خصوص در کافی نت ها :

کافی نت ها قاتل پسورد هستند ، امکان داره هر نوع تروجان یا spyware بر روی آنها فعال باشد و بقیش رو هم خودتون میدونید ..

حتی اگه سیستم عاری از هرگونه فایل مخرب باشه ، با دنبال مسیر :

Hkey_current_user/Software/Yahoo/pager/ و قرار دادن مقدار Save Password در ۱ ، در ریجستری ، پسورد شخص قبلی که Sign in شده بود در یاهو ظاهر خواهد شد ..

پس حتما بعد از اتمام کارتون با یاهو Sign out بشید و بعد با یک آیدی‌ه پیش فرض داخل بشید ..

و همیشه کوکی‌هارو کامل پاک کنید ..

کاربرانی که با موبایل آنلاین میشن :

دوستانی که با موبایل از یاهو استفاده میکنند معمولا باید از یه نرم افزار رابط برای اینکار استفاده کنند ، که برای استفاده از امکاناتشون باید عضو شد و با پسورد اون هم داخل شد ، این نرم افزارها عبارت اند از :

NimBuzz و shmessenger و yahoo mobile و Ytiny و ... که پیشنهاد من اینه که از یه نرم‌افزار معروف و سرور مطمئن مثل نیمباز یا اس اچ استفاده کنید و پسورد این‌هارو هم طبق راه‌هایی که قبلا گفتم یه پسورد قوی انتخاب کنید ..

تمامی تروجان‌ها و فایل‌های مخرب و نرم افزارهای جاسوسی روی موبایل کار نمیکنه و از این بابت باید خیالتون راحت باشه که فایل های مخرب روی موبایل هیچ کاری از پیش نمیبرند ، مگر اینکه فایل مخصوص موبایل طراحی شده باشه که فعلا موجود نیست ..

حمله DDOS چیست و چگونه از آن جلوگیری کنیم؟

امروزه مقوله امنیت و شاخه های آن در فضای وب به امری حیاتی و همه گیر تبدیل شده است، مخصوصا برای صاحبان سایت ها و مهم تر از آن برای مدیران سرورهای وب، چرا که آسیب پذیری و ضعف امنیتی به عنوان عاملی بازدارنده در مسیر پیشرفت و توسعه اهدافشان در وب است، بعضا شاهد هستیم که افراد مختلف با انگیزه های متفاوت اقدام به هک و ایجاد اختلال در سایت ها و سرورها و در نتیجه باعث از دسترس خارج شدن و یا در حالتی پیشرفته تر از کنترل خارج شدن آنها می شوند، این افراد برای رسیدن به مقاصدشان از شیوه های متفاوتی استفاده می کنند که البته بسته به میزان

هوشمندی مدیران سرور و رعایت نکات امنیتی در سیستم های مدیریت محتوا، خیلی از این روش ها به راحتی قابل پیشگیری است؛ اما آنچه در این مطلب قصد داریم به آن بپردازیم، آشنا کردن شما با نوعی از ایجاد اختلال در وب موسوم به حمله های DDOS یا distributed denial of service attack است که بیشترین شیوع را دارد.

حمله DDOS چیست؟

حمله ddosیا dos مخفف (denial of service attack) به زبان ساده یعنی سرازیر کردن تقاضاهای زیاد به یک سرور (کامپیوتر قربانی یا هدف) و استفاده بیش از حد از منابع (پردازنده، پایگاه داده، پهنای باند، حافظه و...) به طوری که سرویس دهی عادی آن به کاربرانش دچار اختلال شده یا از دسترس خارج شود (به دلیل حجم بالای پردازش یا به اصطلاح overload شدن عملیات های سرور)، در این نوع حمله ها در یک لحظه یا در طی یک زمان به صورت مداوم از طریق کامپیوترهای مختلف که ممکن است خواسته یا حتی ناخواسته مورد استفاده قرار گرفته باشند، به یک سرور (با آی پی مشخص) درخواست دریافت اطلاعات می شود و به دلیل محدود بودن قدرت پردازش سرور به کاربران در وضعیت عادی (یعنی قدرت سرور را به تعداد کاربرانش در حالت عادی در نظر گرفته اند نه حالت غیر طبیعی)، مثل حالاتی که کامپیوترهای رومیزی دچار کندی یا توقف کامل می شوند، دچار وقفه در سرویس دهی یا حتی down شدن آن می شود.

چه کسانی حمله ddos را انجام می دهند؟

اصولا حمله های ddos با انگیزه های متفاوت ممکن است توسط یک یا چند نفر و یا حتی گروهی از افراد صورت گیرد، اما آماری که تا به امروز به ثبت رسیده، حکایت از انگیزه های بیشتر فردی یا چند نفره داشته است، مثلا ممکن است افرادی برای از سر راه برداشتن ناجوانمردانه رقیبشان در وب، دست به این نوع اعمال بزنند تا مخاطبان آن سایت یا سرور دچار دلسردی شده و از آن فاصله بگیرند یا برعکس عده ای هکر، خیرخواهانه به سایتی ضد اجتماعی یا مثلا جنگ طلب حمله ddosکنند، لذا گستره افراد و انگیزه ها، بسته به نوع مورد، متفاوت خواهد بود، اما آنچه مسلم است معمولا انسان ها پشت این حملات هستند یا ترکیبی از اندیشه انسان و به کارگیری سیستم، سرور و ابزارهای خاص (DDOS tools)دست به دست هم می دهند تا یک حمله ddos شکل بگیرد.

علائم حمله ddos چیست؟

خوشبختانه یکی از موارد مثبت این نوع حملات این است که به سرعت می توان به نحوه عملکرد سرویس مشکوک شد و

جلوی اختلال بیشتر را گرفت، پس از اینکه سروری مورد حمله ddos قرار می گیرد ممکن است با توجه به اهداف و شیوه به کار رفته یک قسمت از منابع یا همه ی قسمت های آن دچار اختلال شود، در زیر لیستی از این علائم را ذکر می کنیم.

-کندی در پاسخگویی به درخواست ها

سروری که مود حمله قرار گرفته باشد، معمولا خیلی کند و با وقفه به درخواست بارگذاری صفحات پاسخ می دهد، البته این نشانه همیشه دلیل حمله ddos نیست، چرا که این اتفاق به طور طبیعی نیز برای سرورها و سایتهای با بازدید بالا ممکن است رخ دهد یا کنترل این امر بستگی زیادی به قدرت سخت افزاری سرور و تنظیمات آن دارد.

-عدم اتصال به پایگاه داده

گاهی ممکن است صفحات استاتیک که نیازی به اتصال پایگاه داده ندارند به راحتی بارگذاری شوند، ولی اتصال به پایگاه داده برای صفحات داینامیک برقرار نشود، در چنین مواقعی معمولا پیام تکمیل ظرفیت اتصال به پایگاه داده یا too many connectionظاهر خواهد شد، بهترین کار در چنین حالتی این است که با تنظیم یک دستور هِدر HTTP500 ، به ربات های جستجوگر بگوییم که سایت ما فعلا دچار مشکلی است و بعدا مراجعه نمائید!، چرا که در غیر اینصورت با وجود down بودن دیتابیس سرور، ربات ها با دریافت وضعیتHTTP 200 ، صفحه خالی را ایندکس می کنند که این حالت اصلا مناسب نیست، در php این کار را با دستورات header می توان انجام داد.

```
header('HTTP/1.0 500 Internal Server Error');
```

-مصرف بیش از حد منابع سرور

یکی دیگر از نشانه های حمله ddos می تواند مصرف بیش از حد و غیر طبیعی منابع سرور مثل حافظه و یا پهنای باند در یک بازه زمانی کوتاه باشد.

-افزایش انفجاری درخواست ها

یکی دیگر از نشانه های حملهddos ، وجود شمار زیادی درخواست http به سرور است که با مشاهده فایل log و قسمت آمار، می توان به این موضوع پی برد.

-اختلالات در سرویس های جانبی نظیر ایمیل

گاهی مواقع حملات ddos سرویس های جانبی یک سرور نظیر سرویس ایمیل را هدف می گیرند، در این مواقع ارسال و دریافت ایمیل ممکن است به کندی صورت گیرد یا دچار وقفه شود، البته همانطور که گفتیم، هر وقفه و اختلالی به معنی حمله ddosنیست، تنها به عنوان یک نشانه می توان آن را محسوب کرد.

در حمله ddos از چه روش هایی استفاده می شود؟

چند روش به عنوان شایع ترین ها در این نوع حملات استفده می شود، که در زیر به آنها به طور مختصر و جهت آشنایی اشاره می کنیم:

-روش Ping Flood یا طوفان درخواست ها

در این شیوه مهاجم سعی می کند با ارسال درخواست ها (یا بسته های ping به سمت کامپیوتر هدف (قربانی)، و با تکرار این عمل، کل منابع سرور را اشغال کند تا در نهایت آن را به طور کامل از کار بیندازد، در این شیوه معمولا از کامپیوترهای موجود در یک شبکه یا از سرورهایی به طور هم زمان درخواست به سمت سرور قربانی ارسال می شود تا در نهایت موجب از کار افتادن آن شود.

-روش Smurf attack یا استفاده از نقص تنظیمات

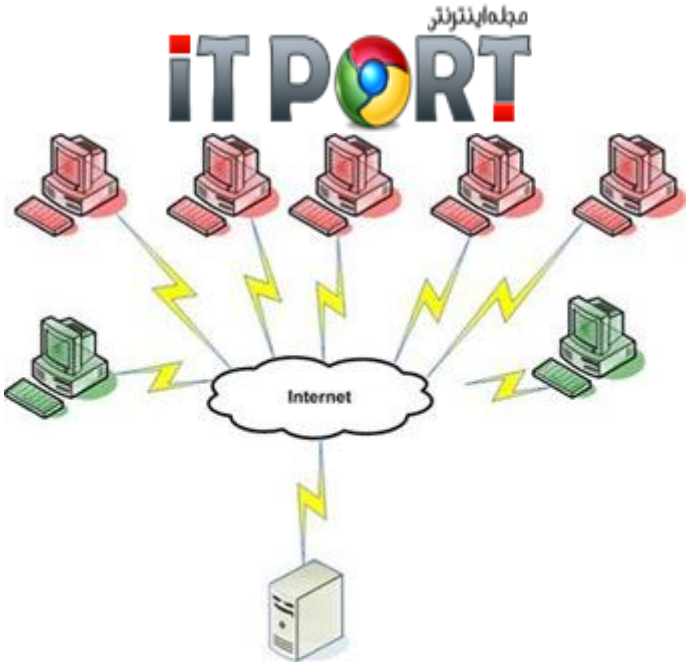
یک Smurf attackنوع خاصی از طوفان درخواستها به یک سرور است که طی آن به دلیل وجود ضعف در تنظیمات سرویس، اجازه ارسال بسته هایی از اطلاعات به تمام کامپیوتر های موجود در یک شبکه در عوض ارسال آن به یک کامپیوتر خاص از طریق آدرس Broadcast آنها است، آدرس Broadcast می تواند به عنوان مثال آی پی اشتراکی سایت های موجود در یک سرور باشد؛ در این حالت اگر تنظیمات سرور به درستی انجام نشده باشد، ارسال یک درخواست به این آی پی، موجب تقسیم شدن آن بین تمام زیر شاخه ها و در نتیجه overload شدن سرور شود.

-حملات موسوم به SYN یاSYN flood

روش اخیر نیز در عمل مشابه با موارد گفته شده است، با این تفاوت که در اینجا مهاجم با ارسال درخواستهایی از نوع بسته های TCP/SYN در پشت چهره ای عادی و تایید شده به عنوان یک کاربر معمولی، از سرور تقاضای اتصال می کند که پس از ارسال پاسخ درخواست، هیچ جوابی به پاسخ سرور داده نمی شود تا اتصال نیمه باز همچنان برقرار باشد (سرور در انتظار پاسخ مهاجم مدتی صبر می کند)، در این بین با افزایش این اتصالات نیمه باز، منابع سرور اشغال شده و نهایتا موجب بروز اختلال و از کار افتادن آن می شود.

-روش Teardrop یاTeardrop attacks

در این شیوه رشته ای از آی پی های ناقص به هم متصل شده و شبیه به هم را به سرور ارسال می کنند که اگر تنظیمات قسمت TCP/IP fragmentation re-assembly سرور دچار نقص در تشخیص آنها باشد، موجب بروز مشکل اضافه بار یا overload در سرور خواهد شد.



حمله ddos چقدر طول می کشد؟

یکی از سوال های همیشگی در چنین موقعیت هایی این است که یک حمله ddos چقدر طول می کشد و ظرف چه مدتی به پایان می رسد، پاسخ این سوال نیز می تواند یک جمله باشد: تا زمانی که به پایان رسد! این موضع بستگی به میزان سماجت مهاجم و ضعف مدافع دارد، یعنی اگر مهاجم بر ادامه حملات خود اصرار داشته باشد و در مقابل مدافع که همان مدیران سرور هستند نتوانند از عهده کنترل اوضاع بر آیند، ممکن است حمله ddos ساعت ها یا روزها به طول انجامد، در خوش بینانه ترین حالت ظرف چند دقیقه و در بدترین حالت چندین و چند روز و به دفعات ممکن است طول بکشد.

برای جلوگیری از حمله ddos چه کارهایی را انجام دهیم؟

واقعیت این است که کنترل حمله های ddos پس از وقوع کمی دشوارتر از پیشگیری از آن است، امروزه در سایتها و انجمن های زیادی به افراد آموزش شیوه های هک و ایجاد حمله های ddos داده می شود که این امر با افزایش شمار کاربران اینترنت (که می توانند میانجی و قربانی بالقوه برای حمله به سرورها باشند (رو به گسترش است، البته آسیب پذیری در این رابطه، بیشتر به امنیت سرور برمی گردد تا به امنیت سایت شما، در مورد سرور می توان پس از اطمینان از حمله ddos، آی پی هایی را که بیشترین تقاضا را به سرور داشته اند و ناشناس هستند، توسط فایروال ها بلاک و مسدود کرد، یا با نصب بسته های امنیتی خاص و به روزرسانی و ارتقا سخت افزاری و نرم افزاری، آسیب پذیری سرور را کاهش داد، آگاهی از روند عادی سرور نیز می تواند کمک بزرگی در این خصوص محسوب شود، چرا که اگر مدیر سرور نسبت به عادی یا غیر عادی بودن ترافیک آن، آشنایی داشته باشد، به سرعت می تواند پی به وجود این نوع حمله ها ببرد و در

جهت رفع آن برآید، به عنوان یک کاربر در سرویس های میزبانی وب، بهترین کار این است که به محض مشکوک بودن به چنین حمله هایی، موضوع را به هاست خود اطلاع دهید تا در کوتاه ترین زمان جلوی آن گرفته شود.

فرایند جلوگیری از جعل اوراق مرتبط با سیستم

با توجه به اینکه پاره ای از اوراق یا خروجی های چاپی (بطور مثال لیست نمره/انواع گواهی ها و ...) نرم افزارهای شرکت دارای ارزش و اعتبار خاصی برای مخاطبان سیستم (ارباب رجوع/ دانشجو...) است و با توجه به کاربردها و مزایای مرتبط احتمال وجود سوء رفتار و جعل یا دست کاری این خروجی ها زیاد است. نرم افزاری سماسامانه اقدام به تدوین این توصیه نامه کرده است تا بتواند با آموزش و اطلاع رسانی شیوه های کاری پیشگیرانه تا جایی که امکان دارد جلوی این موارد را بگیرد و ضریب امنیت را در این خصوص ارتقا دهد. این متن تنها می تواند شروعی باشد برای تفکر عمیق تر شما به این مساله در سازمان خود. متن هایی از این دست که در وب سایت شرکت قرار می گیرد در طول زمان به روز رسانی شده و مشتریان محترم ضروری است تا هر از گاهی به قسمت امنیت سایت مراجعه کرده و براساس تاریخ آخرین ویرایش از آخرین اطلاعات و راهکارها مطلع شوند.

1) گزارشها و خروجی های نرم افزار را به لحاظ اهمیت و امنیت دسته بندی کنید.

دسته بندی گزارشها و خروجی های چاپی سیستم به شما کمک می کند تا خروجی ها و اوراق مهم سیستم را شناسایی کرده و بتوانید تمهیدات لازم برای جلوگیری از سو استفاده و جعل آنها را در نظر بگیرید و اهمیت آنها را به کاربران و کارمندان خود گوشزد کنید.

2) اهمیت امضا و مهر های مورد استفاده را درک کنید.

با درک اهمیت امضا ها و مهر ها شما کمتر دچار سهل انگاری، خطا در عملکرد و آسیب پذیری های مرتبط می شوید.مهر ها را در دسترس افراد و ارباب رجوع قرارندهید.اتاق خود را درحالی که محل مهر ها امن نیست (روی میز، داخل کشو بدون قفل و ...) حتا برای یک لحظه هم ترک نکنید.مهر را به کسی نسپارید .نقل و انتقال مهر را از روش های کاملا مطمئن انجام دهید. هرگز برگه های خالی و سفید را مهر نکنید.

3) امضا و مهر مدیران و همکاران مجموعه خود را بشناسید

برای شناسایی برگه های جعلی ضروری است مهرو امضا صحیح مدیران و همکاران خود را بشناسید

4) امضاهای متفاوت برای کارهای متفاوت (به لحاظ اهمیت) داشته باشید

اصلا دلیلی ندارد همان امضایی که با آن یک برگه مهم (چک، کارنامه تحصیلی، (...را امضا می کنید با امضا شما برای ارجاع یک نامه معمولی که در دسترس عموم خواهد بود یکی باشد. این کار ضریب ایمنی امضا شما را بالا خواهد برد.

5) امضا خود را کدگذاری کنید و از سیستم کد امضا استفاده کنید.

به سادگی می توانید همین امضا خود را کد گذاری کنید بطوری که تنها خودتان تمایز آن را با دیگر امضاهایتان درک کنید. بطور مثال امضا شما می تواند در چهار هفته ماه متفاوت باشد. یعنی هفته اول یک کد هفته دوم یک کد و الاآخر. به این ترتیب شما براساس تاریخ برگه و مقایسه کد امضا خود می توانید صحت برگه را چک کنید.کد گذاری می تواند به سادگی گذاشتن یک نقطه در قسمت های مختلف امضا، یا پیچیده تر و در ساختار منحنی های امضا باشد.

6) ورود ارباب رجوع را به محل های مهم (بایگانی، دبیرخانه، اتاق سرور ها) ممنوع یا کنترل کنید

بهر حال محل های مهم و حاوی اطلاعات و اسناد مهم باید بشدت تحت کنترل باشد و ورود و خروج آنها طبق قاعده و اصول خاصی باشد. کلید و مجوز ورود به این محل ها باید با شرایط ویژه مدیریت شود.

7) گردش نامه های مهم را امن کنید

گردش نامه های مهم و با ارزش (کارنامه، لیست نمره، ریزنمرات،...) بطور فیزیکی در سازمان باید با دقت انجام شده و بخوبی ایمن شود. این دسته از نامه ها نباید هرگز توسط ارباب رجوع (دانشجو،...) منتقل، ازسال یا دریافت شود. برای نمونه جعل نامه مربوط به اعلام نمرات دانشجویان میهمان توسط دانشجویان بارها اتفاق افتاده است. استفاده از سیستم های اتوماسیون اداری که گردش فیزیکی نامه را حذف می کنند بشرط رعایت نکات امنیتی در آنها در این زمینه راهگشا خواهد بود.

8) صحت اطلاعات نامه های دریافتی و فرایندهای مهم را استعلام کنید.

در صورتی که اطلاعات مهمی را از طریق نامه دریافت می کنید صحت اطلاعات مندرج در آن را بطور مکتوب یا تلفنی کنترل کنید. بدین شکل اگر در طول مسیر انتقال تغییر یا جعلی رخ داده باشد بسادگی قابل شناسایی خواهد بود.همچنین در فرایندهای مهم همچون انتقال یا جابجایی دانشجو به دانشگاه شما، قبولی دانشجو در دانشگاه شما و مواردی از این دست باید صحت مشخصات و اعتبار شخص بصورت مجزا از سازمان اصلی استعلام شود. باید دقت کنید که ممکن است مدارک انتقال از دانشگاه دیگر جعلی باشد و یا دانشجو اصلا در کنکور قبول نشده باشد و از مکانیزم های غیرمتعارف در دانشگاه ثبت نام کرده باشد!

9) موارد امنیتی نگهداری و ورود و خروج پرونده ها را رعایت کنید.

قوه قضاویه دستورالعملی برای حفاظت از اسناد و اطلاعات و ادله پرونده‌های قضایی در سال ۱۳۸۵ منتشر کرده که مطالعه و ایده گرفتن از آن می تواند برای شما بسیار راهگشا باشد. متن این دستور العمل حفاظت از اسناد و ادله پرونده های قضایی (http://www.hoqouq.com/law/article602.html) را می توانید در این سایت مطالعه

کنید. مواردی چون ماده 10 نحوه نگهداری پرونده‌ها، ماده 17 شرایط حفاظت فیزیکی بایگانی، ... با کمی تعدیل برای شما مفید خواهد بود. استفاده از سیستم های بایگانی دیجیتال نیز به شما در این امر بسیار کمک خواهد کرد. در صورت نیاز به تهیه سیستم بایگانی دیجیتال سما با شرکت تماس بگیرید .

10) از تجهیزات کنترل ورود و خروج (دروبین های مداربسته،...) برای محل های مهم استفاده کنید.

11) از آموزش و تفهیم کارمندان و کاربران نسبت به موارد امنیتی اطمینان حاصل کنید.
ضروری است که کارمندان و کاربران سیستم ها از اهمیت کار خود و خروجی های مختلف سیستم و سو رفتارهای احتمالی کاملا آگاه باشند تا بتوانند رفتاری درست و مناسب داشته باشند. بهتر است نکات مهم به آنها بصورت مکتوب اعلام شود. هیچ چیز را بدیهی و گفته شده تلقی نکنید.

12) استفاده از چاپ ترام آرم سازمان در کاغذها و ایجاد تمایز و مدت اعتبار
یکی از راه های جلوگیری از جعل ایجاد تمایز در نوع کاغذ ها می باشد. با چاپ ترام آرم دانشگاه بر روی کاغذهای A4 معمولی شما بسادگی می توانید تمایز ایجاد کنید.این فرم ها بهتر است کارکردی محدود در یک بازه زمانی شش ماهه یا یک ساله داشته باشند و با درج کد فرم متمایز شوند. هیچگاه این فرم ها به خودی خود نباید مرجع صحت و درستی اطلاعات چاپ شده روی آنها باشند. این کار شرایط جعل را سخت تر می کند.

13) سربرگ ها و برگه های سازمان را در محلی امن و مناسب نگهداری کنید.
بدیهی است کسی که برگه ها و فرم های شما را در اختیار داشته باشد می تواند با چاپ اطلاعات مورد نیاز خود مدرکی در حد اعتبار برگه های شما داشته باشد.پس ضروری است که از برگه ها و فرمهای خود بخوبی مراقبت کنید.

14)از هولوگرام برای گزارشها و خروجی های خیلی مهم استفاده کنید.
چسباندن هولوگرام برروی خروجی چاپی (گواهی پایان تحصیلات،...) و اضافه کردن جمله ای که بدون هولوگرام فاقد اعتبار است می تواند ضریب امنیتی بسیار بالایی برای مدارک شما ایجاد کند.

15)اطلاعات گزارشهای چاپی را با اطلاعات داخل سیستم مقایسه کنید.
همیشه این تصور را داشته باشید که ممکن است اطلاعات چاپ شده صحیح نباشند. پس براساس یک خروجی چاپ شده تصمیم نگیرید. شما همیشه می توانید بطور تصادفی اطلاعات چاپی را با اطلاعات سیستمی چک کنید.

16) برای نقاط پایانی (دانش آموختگی دانشجویان، اتمام خدمت کاربر سیستم،اتمام کار ارباب رجوع) فهرستی از چیزهایی که باید کنترل شود تهیه کنید.
در نقاط پایانی همچون زمانی که یک دانشجو دانش آموخته می شود یا یک کارمند مدت خدمت اش تمام می شود کنترل هایی را در نظر گرفته، فهرست کنید و از کارمندان و کاربران مسول بخواهید در این نقاط بصورت سیستمیک آنها را

چک کنند.بطور مثال هنگام دانش آموختگی دانشجو ضروری است تمامی نمرات ثبت شده در کامپیوتر با نمرات موجود در لیست های نمره دستنویس استاد تطبیق داده شود.این باعث می شود که کنترلی دوطرفه رخ دهد هم برای جعل های کاغذی و هم برای خطاهای کاربری یا مسائلی از این دست.

17)دستورالعمل امنیتی مطابق با نیازهای مجموعه خود و حساسیت های سازمانی خود تنظیم کنید

بهتر است شما برای سازمان خود دستورالعمل امنیتی مشخصی را تدوین کنید تا کارمندان و کاربران بسادگی بتوانند از آن اطلاع داشته و استفاده کنند. مکتوب کردن این دستورالعمل مزایای زیادی برای شما بهمراه خواهد داشت. شما مطمئن می شوید چیزی از قلم نمی افتد،انتقال و آموزش به افراد جدید راحت تر می شود و شفافیت و امنیت در سازمان شما بالا می رود.