راهکار امنیت شبکه

راهکار امنیت شبکه

همه کاربران رایانه می دانند که آلوده شدن کامپیوترها سرورها به بدافزارهایی مانند انواع ویروس ها ، انواع کرمهای شبکه ، انواع باج افزارها ، از جمله مسائلی ممکن است همه اطلاعات کسب و کار را از بین ببرند و پیامدهای گاهاً جبران ناپذیری را برای سازمان و کاربران شبکه های به دنبال داشته باشد .

اهمیت امنیت شبکه و سرور ها

در فضای کسب و کار امروزی به علت گسترده شدن شبکه هاي کامپیوتری و عدم رعایت مسائل امنیت شبکه ، خطر آلوده شدن سیستمها و سرورها به شدت افزایش پیدا کرده است . افرادی که در بحث تولید فایلهای مخرب و ویروسها فعالیت دارند رو بروز قوی تر شده و ما هر روزه شاهد آلودگی های جدید در دنیای فناوری اطلاعات می باشیم . وجود حفره های باز امنیتی و عدم آشنائی کاربران با ویروسهای جدید باعث شده تا امنیت سیستم ها به شدت کاهش یافته و این امر موجب بروز مشکلات عدیده ای در عملکرد سیستم می گردد .

گسترش سامانه های اینترنتی که در حوضه دولت الکترونیک و سازمان هوشمند فعال هستند باعث گردیده که کسب و کارهای هر روز بیشتر وابسته به فضای اینترنت جهانی گردند و جلوگیری از دسترسی کاربران شبکه به اینترنت در برخی از مواقع کاری غیر ممکن می باشد .

درست است که ویروس های رایانه ای روبروز گسترش پیدا میکنند اما ردیابی و کنترل شبکه برای جلوگیری از آلودگی ها نیز امری عملی و قابل اجرا می باشد . کافیست سیستم های شبکه و سرورهای مورد استفاده در شبکه به نرم افزارهاي امنیتی مورد اطمینان و بروز شده مجهز گردند و مجموعه راهکارهای امنیت اطلاعات در شبکه شما اجرا گردد .

امنیت شبکه چیست؟

با گسترش استفاده از کامپیوترها در سازمانها و پس از آن مطرح شدن بحث نصب شبکه هاي کامپیوتري و همچنین بدنبال آن گسترش فضای اینترنت که بزرگترین شبکه جهای می باشد ، عملکرد رایانه ها و کاربران شبکه ها نیز دستخوش تغییرات اساسی گردیده است .

اهمیت امنیت اطلاعات شبکه و ایمن سازي شبکه هاي رایانه ای از جمله این مباحث می باشد که نمی توان آن را وظیفه یک فرد در شرکت شما و یا یک سازمان بیرونی دانست . پرداختن به موضوع امنیت اطلاعات شبکه و سرورها و همچنی امنیت اطلاعات سازمانی امری بین بخشی و فراگیر در سازمان ها می باشد و همه کاربران شبکه و مدیران سازمانها باید در آن دخیل باشند .

وظیفه بخش فناوری اطلاعات در موضوع امنیت اطلاعات بستر سازی و اجرای سیاستهای امنیتی بر پایه سیستمهای رایانه ای و شبکه می باشد اما این نکته شایان ذکر است که در بسیاری از سازمانها نیز که همه موارد امنیتی را رعایت کرده اند بیشترین ضربه های امنیتی مانند افشای اطلاعات کسب و کار از طریق کارمندان و کاربران داخلی سازمان انجام گرفته است .

امنیت اطلاعات شبکه و سرورها شامل چه نوع خدماتی می باشد ؟

مرکز پشتیبانی انفورماتیک ایران ، دارای بخش ویژه ای در شرکت خود می باشد که شامل تیمی از مجموعه متخصصین شبکه ، نرم افزار ، سخت افزار و امنیت اطلاعات می باشند . تیم امنیت اطلاعات شبکه خدمات خود را در قالب قرارداد انجام کار بصورت پروژه های کوتاه و بلند مدت و یا بصورت مشاوره امنیت اطلاعات ، ارائه می دهد .

خدماتی که در این بخش ارائه می گردد در قالب 4 سرفصل تعریف میگردند :

خدمات امنیت فیزیکی شبکه

علی رغم پیاده سازی همه مسائل امنیتی در شبکه ها این نکته غیر قابل انکار است که هر گونه طرح امنیتی در سازمان با داشتن دسترسی فیزیکی به منابع شبکه ، قابلنفوذ و شکننده می باشد .

بررسی امنیت فیزیکی سرورها ، اتاق سرور ، سوئیچ های شبکه ، روترهای شبکه و فایروال ها و ارائه راهکار عملی جهت اجرا

بررسی و ارائه راهکار جهت امنیت فیزیکی ایستگاه هاي کاري کاربران

بررسی امنیت فیزیکی زیر ساخت شبکه کابلی و شبکه های بی سیم و ارائه راهکار امنیت شبکه برای رفع مشکلات موجود در این حوضه

بررسی و ارائه راهکار در بخش سیستمهای نظارت تصویری مانند دوربین مداربسته و سیستمهای ضد سرقت

بررسی و ارائه راهکار در خصوص نصب سیستمهای اعلام حریق

خدمات امنیت سرور

در هر سازمانی که درای شبکه است حتماًسرور یا سرورهایی جهت ارائه سرویس هاي مختلف نرم افزاری به کاربران شبکه وجود دارد . سرورها در واقع قبل تپنده سازمان های هوشمند می باشند . عدم سرویس دهی سرورها می تواند خسارتهای زیادی را به سازمان وارد کند . لذا اهمیت امنیت سرورها بسیار زیاد و حتی به مراتب بیشتر از امنیت سایر تجهیزات موجود در شبکه های می باشند .

در بخش امنیت سرور خدماتی که تیم امنیت اطلاعات ما ارائه میدهد شامل موارد زیر می باشد :

بررسی سیستم عامل سرورها و نصب پتچ های امنیتی بر روی سیستم عاملهای سرور ویندوز و لینوکس با هدف پیشگیری از حملات روزمره هکرها و ایجاد دیوار قوی امنیتی بر روی سرور ها

ارائه راهکارهای امنیتی جدید با متدهای نوین توسط بخش امنیت ما بر روی همه سرورهای ویندوزی و لینوکسی

خدمات مشاوره امنیتی بمنظور جلوگیری از حملات از نوع مهندسی اجتماعی و آموزش و آگاه سازی کارشناسان شبکه

ارائه راهکار جهت امن سازی سرویسهای تحت شبکه سرورها و خصوصاً سرویسهای تحت وب از جمله سرورهای WEB – سرور ایمیل – فایل سرورها – سرورهای اتوماسیون که در اینترنت نیز فعال می باشند .

نصب و کانفیگ فایروال مخصوص سرور به منظور جلوگیری از حملات از داخل و بیرون شبکه

انجام تست نفوذ و ارائه راهکار در صورت وجود حفره های نفوذ به سرورها

نصب نرم افزارهای مانیتورینگ سرورها بمنظور مانیتور کردن ورود و خروج داده ها در شبکه و ارائه گزارش روزانه

خدمات امنیت ایستگاههای کاری کاربران شبکه

وجود یک رایانه در شبکه بدون داشتن اپراتور یا کاربر رایانه ممکن نیست و یکی از مهمترین دلایل بوجود آمدن مشکلات امنیتی در شبکه ، کامپیوترهاي کاربرانی می باشد که بدون انجام تنظیمات امنیتی مورد نیاز و مهم ، در شبکه مشغول بکار هستند. یکی از کارهائی که بخش IT در هر سازمانی باید با هدف ایجاد امنیت شبکه انجام دهد انجام تنظیمات امنیتی خاص آن شبکه بر روی ایستگاههای کاری می باشد . یاد آوری این نکته ضروری است که بسیاری از کارشناسان شبکه سیستمهای کاربران را پس از نصب سیستم عامل و نرم افزارهای مورد نیاز تحویل کاربر میدهند این نکته را در نظر نمیگیرند که تنظیمات امنیتی روی آن سیستم بصورت پیش فرض بوده و باید آن را با توجه به سیاستهای امنیتی سازمان خود تغییر دهیم .

در بخش امنیت سیستمهای کاربری نیز تیم فنی مرکز پشتیبانی انفورماتیک ایران خدمات زیر را ارئه می دهد :

بررسی سیستم عاملها و انجام بروز رسانی آنها

راه اندازی سیستم آپدیت خودکار سیستم عاملهای ویندوز در شبکه با نصب WSUS

نصب آنتی ویروس تحت شبکه بر روی سیستمهای کاربران و بروز رسانی آن

راه اندازی سرویس آنتی ویروس تحت شبکه EndPoint با استفاده از آنتی ویروسهای اورجینال

حذف نرم افزارهای اضافه از سیستمها و بررسی همه نرم افزارهای نصب شده

راه اندازی سیستم مانیتورینگ سیستمهای کاربران در شبکه و مانیتور کردن عملکرد سیستمها

آموزش و آگاهی رسانی به کاربران سیستمها برای آشنائی با مباحث اولیه امنیت اطلاعات و نفوذهائی که ممکن است از طریق مهندسی اجتماعی در شبکه صورت گیرد

امنیت ارتباطات شبکه

همانطور که در مباحث بالا اشاره شد نشت اطلاعات سازمان از مهم ترین تهدیدات امنیتی در یک کسب و کار می باشد . تصور کنید تیم تحقیقات شما مدتها برروی تولید یک محصول جدید تحقیق و پژوهش کرده و پس از به نتیجه رسیدن آن شما متوجه شوید که شرکت رقیب شما این محصول را با همان مشخصات تولید و روانه بازار کرده است .
یکی از راههای نشت اطلاعات به بیرون سازمان عدم نصب و پیکربندی مناسب تجهیزات ارتباطی شبکه از جمله ارتباطات کابلی و یا بی سیم می باشد . در اینجا وجود شبکه بسیار بزرگی بنام اینترنت نیز نباید فراموش گردد و اینکه ممکن است همه سرورها و سیستمهای کاربران شما نیز به اینترنت دسترسی داشته باشند .
در نتیجه وضیفه ماست تا با پیکربندي مناسب تجهیزات ارتباطی شبکه ، تمام ارتباطات سازمانی شماامن شود

خدمات ما در بخش امنیت ارتباطات شبکه بشرح زیر می باشد :

خدمات مشاوره امنیت شبکه :

بررسی و شناخت تجهیزات امنیت شبکه موجود در سازمان

بررسی و شناخت فرآیندهی انتقال اطلاعات در داخل و بیرون شبکه

ارائه راهکار و مشاوره در طراحی زیرساختهای امنیت شبکه و اینترنت

بررسی سیاستهای امنیتی سازمان و تعریف مجدد سیاستها ی امنیتی مرتبط با سرویس های شبکه

بررسی تنظیمات تجهیزات IP/IDSجهت تشخیص و جلوگیری از حملات به شبکه

مشاوره جهت راه اندازی مرکز جمع آوری یکپارچه رخدادها و وقایع امنیتی

مشاوره و ارائه راهکار جهت ایجاد بستری امن برای کاربران در دسترسی به

مشاوره و ارائه راهکار جهت زیرساخت شبکه ایمن با هدف جلوگیری از دسترسی ها غیرمجاز به منابع شبکه و سروها

مشاوره و ارائه پیشنهاد فنی در انتخاب تجهیزات امنیتی مانند UTM ، Firewall و IPS

خدمات پیاده سازی و اجرای امنیت شبکه :

نصب و راه اندازی تجهیزات امنیت شبکه شامل فایروال IPS و IDS

نصب و کانفیگ و بهینه سازی تجهیزات امنیت شبکه مانند UTM- IPS و IDS

نصب و اجرای روشهای دسترسی کاربران به منابع شبکه از راه مانند client-Based VPN یا SSL VPN

طراحی و اجرای زیر ساخت ایمن ارتباطات مبتنی بر روشهای مبتنی بر پروتکل IPsec

انجام خدمات تست نفوذ جهت بررسی میزان استحکام سازی تجهیزات امنیتی نصب شده در شبکه

طراحی و اجرای چک لیستهای امنیتی با هدف افزایش بهره وری تجهیزات امنیت شبکه

نصب و راه اندازی راه کارهای مانیتورینگ شبکه و آنالیز ترافیک شبکه

نصب و راه اندازی آنتی ویروس تحت شبکه End Point Protection

ارائه راهکار جهت پیشگیری از ورود باج افزار به شبکه

تیم امنیت شبکه در بخشهای زیر بررسی هاي کارشناسی لازم را انجام داده و گزارش جامعی را براي برطرف نمودن آنها به مدیر سازمان و یا مدیر بخش IT ارائه می دهد :