



Namatek
True Education

Network Security

www.namatek.com

آشنایی با مفهوم
امنیت شبکه

فهرست مطالب

۱. شبکه چیست؟
۲. اینترنت چیست؟
۳. امنیت داده ها چیست؟
۴. اهمیت امنیت شبکه
۵. راه حل افزایش امنیت شبکه

با پیشرفت تکنولوژی علی رغم ساده شدن کارهایی از قبیل ذخیره سازی و انتقال اطلاعات، احتمال ربوده شدن داده ها نیز بسیار بیشتر شده است. به همین دلیل راهکارهای افزایش امنیت شبکه ها به شدت مهم و ضروری شدند. در این مقاله ابتدا معرفی مفهوم شبکه و اهمیت امنیت آن پرداخته و سپس راه کار های ساده و ضروری برای برقراری آن معرفی می کنیم.



قبل از توضیح شبکه، اجازه دهید داده های دیجیتالی را تعریف کنیم. در علم کامپیوتر و مخابرات به کلیه محصولات دیجیتالی که در قالب عکس، متن، فیلم، فایل، کدهای برنامه نویسی و به طور کلی تمامی اطلاعاتی که توسط رایانه ها تولید می شوند و می توان آنها را از یک رایانه به رایانه دیگر منتقل نمود به اصطلاح داده یا داده های دیجیتالی می گویند.

اس بی انجام داده اید. این کابل در واقع یک شبکه کوچک است که به واسطه آن می توان داده ها را بین کامپیوتر و موبایل منتقل کرد. حال فرض کنید در یک سازمان تعداد ۵۰ کامپیوتر موجود است و شما بخواهید هر روز داده های زیادی بین کامپیوترها منتقل کنید که در این صورت می بایست ارتباط کامپیوترها را توسط کابل های مخصوصی برقرار کنید. این کابل های مخصوص اصطلاحاً کابل های شبکه نامیده می شوند.

نکته : برای ایجاد شبکه بین کامپیوترها روش های مختلفی استفاده می شود (مثلاً روش های شبکه سازی سری، موازی و...) که بسیار گسترده است و البته خارج از بحث ماست، به همین دلیل به آن نمی پردازیم.

اینترنت چیست؟



اکنون فرض کنید می خواهیم بین تمام لوازم دیجیتالی و مخابراتی مانند کامپیوترها، تبلت ها، موبایل ها و... در سراسر جهان ارتباط برقرار کنیم. در این صورت از بزرگترین شبکه موجود در جهان که همان شبکه جهانی یا

اینترنت است استفاده می کنیم، در این شبکه می توانیم داده های مختلفی را توسط وب سایت ها، اپلیکیشن ها، فضاها، اینترنتی و ... در سراسر دنیا منتقل کنیم.

یعنی داده هایی را به اشتراک گذاریم و یا از داده هایی که دیگران به اشتراک گذاشته اند استفاده کنیم. هر وسیله ای که به اینترنت وصل شده باشد در واقع عضوی از شبکه جهانی شده که می تواند داده هایی را وارد این شبکه کند (آپلود کند) و یا داده هایی را دریافت کند (دانلود کند). در این فضا می توان داده ها یا اطلاعاتی را به اشتراک گذاشت تا همه (یا افراد به خصوصی) از آن استفاده کنند.

امنیت داده ها چیست؟



بعضی از داده ها به اختیار خود کاربر در شبکه جهانی به اشتراک گذاشته می شود و بعضی دیگر داده ها بدون اجازه کاربر، تلاش برای امنیت داده ها به این معنی است که در این فضا، اطلاعات و داده های هیچ کاربری بدون اجازه آن کاربر در دسترس دیگران قرار نگیرد و به اصطلاح سرقت نشود.

اهمیت امنیت شبکه



از زمان به کارگیری شبکه همواره بحث امنیت شبکه و داده های موجود در شبکه مطرح بوده است. فرض کنید در یک سازمان، کارمندی بدون اجازه رئیس سازمان به تمام اطلاعات محرمانه رایانه رئیس دسترسی پیدا کند. این کارمند ممکن است مرخصی ها، حقوق و دستمزد خود و یا همکارانش را تغییر بدهد، اطلاعات محرمانه ای را پخش کند، داده هایی که در رایانه رئیس سازمان وجود دارد را از بین ببرد، جابه جا کند و...

طبیعتاً اهمیت شبکه برای هر ارگان، سازمان، نهاد و هر محلی که از شبکه استفاده می کند حرف اول را میزند، خصوصاً شبکه جهانی اینترنت.

در اینترنت بحث امنیت شبکه اهمیت بسیار بیشتری دارد تا شبکه های محلی و کوچک که به عنوان مثالی از شبکه محلی می توان شبکه داخلی یک اداره یا سازمان را نام برد. تقریباً تمامی کامپیوترهای موجود در بانک ها، بازار بورس، اداره جات، نهادهای امنیتی، صنایع حساس و... به اینترنت وصل بوده و داده هایی را دریافت یا ارسال می کنند. قطعاً داخل این رایانه ها اطلاعات و داده های حساسی وجود دارند که سرقت آن اطلاعات ضرر هنگفتی به آن سازمان وارد می سازد.

مثلاً سرقت اطلاعات یک ابر کامپیوتر بانک به قیمت خالی شدن حساب چند هزار نفر تمام می شود که در آن بانک حساب دارند یا اطلاعات حسابشان در آن بانک موجود است. تنها سازمان های حساس نیستند که به امنیت شبکه احتیاج دارند، اکثر کاربران در رایانه و تلفن همراه خود، اطلاعات و داده هایی دارند که دوست ندارند در اینترنت به اشتراک گذاشته شود و سرقت آن اطلاعات به ضررشان تمام می شود.

راه حل افزایش امنیت شبکه



تا اینجا با ضرورت امنیت شبکه آشنا شدید. در اینجا راه حل هایی برای کاهش خطرات شبکه و سرقت اطلاعات را معرفی می کنیم.

تقسیم بندی اطلاعاتی رایانه ها

فرض کنید در یک سازمان یا شرکت، تمامی رایانه ها حاوی اطلاعات یا داده های محرمانه باشند و تمامی آنها به اینترنت متصل باشند، در این صورت احتمال سرقت اطلاعات مهم شرکت یا سازمان افزایش می یابد ولی اگر تمام اطلاعات محرمانه فقط در یک کامپیوتر موجود باشد و آن کامپیوتر به شبکه وصل نباشد احتمال سرقت اطلاعات به شدت کاهش پیدا می کند.

در اکثر شرکت ها و سازمان ها بدین گونه عمل می کنند که رایانه هایی که اطلاعات محرمانه تر در داخل آنها وجود دارد دسترسی محدودتری به شبکه دارند.

محدودیت عملکرد برنامه ها

بسیاری از ویروس ها و بدافزارها برای خرابکاری، ایجاد تغییرات یا سرقت اطلاعات نیاز دارند تا به قسمت های مهم کامپیوتر دسترسی داشته باشند. کامپیوترها توسط بخش ویندوز فایروال خود (fire wall) به طور پیش فرض اجازه دسترسی هیچ نرم افزاری را به قسمت های حساس خود نمی دهند.

اگر برنامه ای قصد دسترسی به قسمت های حیاتی کامپیوتر را داشته باشد فایروال اجازه نمی دهد مگر اینکه کاربر این اجازه را شخصا صادر کند. نکته: فایروال کاربردهای دیگری نیز دارد و علاوه بر ایجاد محدودیت در دسترسی برنامه ها به قسمت های حساس، محدودیت هایی نیز در شبکه ایجاد می کنند.

محدودیت اختیارات کاربران

هر کاربر تنها باید به قسمتی از شبکه دسترسی داشته باشد که به آن نیاز دارد مثلا در یک اداره دولتی باید دسترسی کارمندان به قسمت های حیاتی سیستم خودشان، کامپیوترهای سرور و یا رایانه هایی که اطلاعات حساس در آنها وجود دارد محدود شود. چون اولاً کارمندان نیاز به استفاده از این قسمت ها را ندارند و مهمتر اینکه این کار امنیت شبکه را افزایش می دهد. در شبکه جهانی نیز به مانند شبکه های محلی دسترسی کاربران محدود می شود، مثلا بازدید کنندگان سایت تنها می توانند از سایت بازدید کنند و اجازه

دسترسی به فولدرها، کامپوننت ها و سایر قسمت های مدیریتی سایت را ندارند.

استفاده از آنتی ویروس

در کنار استفاده از فایروال کامپیوتر، استفاده از آنتی ویروس ضروریست چون ممکن است یک بدافزار (ویروس مخرب) بدون نیاز به قسمت های حساس کامپیوتر اقدامات خرابکارانه یا سرقت اطلاعات را انجام دهد حتی بدون اینکه کاربر رایانه از این سرقت یا نفوذ ویروس اطلاع پیدا کند. اقدامات نام برده شده حداقل کاریست که برای افزایش امنیت شبکه انجام می شود. متخصصان این حوزه اقدامات فراوانی برای این هدف انجام می دهند و با گذر زمان و پیشرفت تکنولوژی روش های جدیدتری برای امنیت شبکه ابداع شده و بکار گرفته می شود.