امنیت شبکه: چالشها و راهکارها

نوشته: علیرضا گنجی کارشناس ارشد کتابداری و اطلاع‌رسانی دانشگاه فردوسی مشهد

چکیده

این مقاله به طور کلی به چالشها و راهکارها در امنیت شبکه می‌پردازد. در ابتدای مقاله به مباحثی چون: امنیت شبکه‌های اطلاعاتی و ارتباطی، اهمیت امنیت شبکه، سابقهٔ امنیت شبکه، پیدایش جرایم رایانه‌ای، طبقه‌بندی جرایم رایانه‌ای، و راهکارهایی که برای این چالش پیشنهاد شده است از جمله کنترل دولتی، کنترل سازمانی، کنترل فردی، تقویت اینترانتها، وجود یک نظام قدرتمند و کار گسترده فرهنگی برای آگاهی کاربران و فایروالها پرداخته می‌شود. در آخر نیز به مسأله «اینترنت و امنیت فرهنگی در ایران و چالشهایی که در این زمینه مطرح گردیده پرداخته شده و برای رفع این مشکل پیشنهاداتی نیز ارائه گردیده است .

1 مقدمه :

اینترنت یک شبکهٔ عظیم اطلاع‌رسانی و یک بانک وسیع اطلاعاتی است که در آینده نزدیک دسترسی به آن برای تک‌تک افراد ممکن خواهد شد. کارشناسان ارتباطات، بهره‌گیری از این شبکه را یک ضرورت در عصر اطلاعات می‌دانند .

این شبکه که از هزاران شبکه کوچکتر تشکیل شده، فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته است. طبق آخرین آمار بیش از شصت میلیون رایانه از تمام نقاط جهان در این شبکهٔ گسترده به یکدیگر متصل شده‌اند که اطلاعات بی‌شماری را در تمامی زمینه‌ها از هر سنخ و نوعی به اشتراک گذاشته‌اند .گفته می‌شود نزدیک به یک میلیارد صفحه اطلاعات با موضوعات گوناگون از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است .

این اطلاعات با سرعت تمام در بزرگراههای اطلاعاتی بین کاربران رد و بدل می‌شود و تقریباً هیچ گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده‌ها اعمال نمی‌شود .

حمایت از جریان آزاد اطلاعات، گسترش روزافزون فنآوری اطلاعات و بسترسازی برای اتصال به شبکه‌های اطلاع‌رسانی شعار دولتهاست. این در حالی است که گستردگی و تنوع اطلاعات آلوده روی اینترنت، موجب بروز نگرانی در بین کشورهای مختلف شده است. انتشار تصاویر مستهجن، ایجاد پایگاههایی با مضامین پورنوگرافی و سایتهای سوءاستفاده از کودکان و انواع قاچاق در کشورهای پیشرفته

صنعتی بخصوص در خاستگاه این شبکهٔ جهانی یعنی آمریکا، کارشناسان اجتماعی را بشدت نگران کرده، به گونه‌ای که هیأت حاکمه را مجبور به تصویب قوانینی مبنی بر کنترل این شبکه در سطح آمریکا نموده است. هشدار، جریمه و بازداشت برای برپاکنندگان پایگاههای مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء اینترنت اتخاذ کرده‌اند .

ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشی منطقی است، زیرا هر جامعه‌ای چارچوبهای اطلاعاتی خاص خود را دارد و طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند می‌تواند سلامت و امنیت جامعه را به خطر اندازد. علی‌الرغم وجود جنبه‌ای مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد بزهکار، امنیت ملی را در کشورهای مختلف با خطر روبرو ساخته است. از این رو بکارگیری فیلترها و فایر وال‌های مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است .

خوشبختانه با وجود هیاهوی بسیاری که شبکهٔ اینترنت را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل است .

2 امنیت شبکه‌های اطلاعاتی و ارتباطی:

2-1 اهمیت امنیت شبکه:

چنانچه به اهمیت شبکه‌های اطلاعاتی (الکترونیکی) و نقش اساسی آن دریافت اجتماعی آینده پی برده باشیم، اهمیت امنیت این شبکه‌ها مشخص می‌گردد. اگر امنیت شبکه برقرار نگردد، مزیتهای فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعاتی عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوءاستفاده‌های مادی و معنوی هستند. همچنین دستکاری اطلاعات- به عنوان زیربنای فکری ملت‌ها توسط گروههای سازماندهی شده بین‌المللی، به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولت‌ها و تهدیدی ملی محسوب می‌شود . برای کشور ما که بسیاری از نرم‌افزارهای پایه از قبیل سیستم عامل و نرم‌افزارهای کاربردی و اینترنتی، از طریق واسطه‌ها و شرکتهای خارجی تهیه می‌شود، بیم نفوذ از طریق راههای مخفی وجود دارد. در آینده که بانکها و بسیاری از نهادها و دستگاههای دیگر از طریق شبکهٔ به فعالیت می‌پردازند، جلوگیری از نفوذ عوامل مخرب در شبکه بصورت مسئله‌ای استراتژیک درخواهد آمد که نپرداختن به آن باعث ایراد خساراتی خواهد شد که بعضاً جبران‌ناپذیر خواهد بود. چنانچه یک پیغام خاص، مثلاً از طرف شرکت مایکروسافت، به کلیه سایتهای ایرانی ارسال شود و سیستم عاملها در واکنش به این پیغام سیستمها را خراب کنند و از کار بیندازند، چه ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد؟

نکته جالب اینکه بزرگترین شرکت تولید نرم‌افزارهای امنیت شبکه، شرکت چک پوینت است که شعبهٔ اصلی آن در اسرائیل می‌باشد. مسأله امنیت شبکهٔ برای کشورها، مسأله‌ای استراتژیک است؛ بنابراین کشور ما نیز باید به آخرین تکنولوژیهای امنیت شبکه مجهز شود و از آنجایی که این تکنولوژیها به صورت محصولات نرم‌افزاری قابل خریداری نیستند، پس می‌بایست محققین کشور این مهم را بدست بگیرند و در آن فعالیت نمایند .

امروزه اینترنت آنقدر قابل دسترس شده که هرکس بدون توجه به محل زندگی، ملیت، شغل و زمان میتواند به آن راه یابد و از آن بهره ببرد. همین سهولت دسترسی آن را در معرض خطراتی چون گم شدن، ربوده شدن، مخدوش شدن یا سوءاستفاده از اطلاعات موجود در آن قرار می‌دهد. اگر اطلاعات روی کاغذ چاپ شده بود و در قفسه‌ای از اتاقهای محفوظ اداره مربوطه نگهداری می‌شد، برای دسترسی به آنها افراد غیرمجاز می‌بایست از حصارهای مختلف عبور می‌کردند، اما اکنون چند اشاره به کلیدهای رایانه‌ای برای این منظور کافی است .

2-2 سابقه امنیت شبکه:

اینترنت در سال 1969 بصورت شبکه‌های بنام آرپانت که مربوط به وزارت دفاع آمریکا بود راه‌اندازی شد. هدف این بود که با استفاده از رایانه‌های متصل به هم، شرایطی ایجاد شود که حتی اگر، بخشهای عمده‌ای از سیستم اطلاعاتی به هر دلیلی از کار بیفتد، کل شبکه بتواند به کار خود ادامه دهد، تا این اطلاعات حفظ شود. از همان ابتدا، فکر ایجاد شبکه، برای جلوگیری از اثرات مخرب حملات اطلاعاتی بود .

در سال 1971 تعدادی از رایانه‌های دانشگاهها و مراکز دولتی به این شبکه متصل شدند و محققین از این طریق شروع به تبادل اطلاعات کردند .

با بروز رخدادهای غیرمنتظره در اطلاعات، توجه به مسأله امنیت بیش از پیش اوج گرفت. در سال 1988، آرپانت برای اولین بار با یک حادثه امنیتی سراسری در شبکه، مواجه شد که بعداً، «کرم موریس» نام گرفت. رابرت موریس که یک دانشجو در نیویورک بود، برنامه‌هایی نوشت که می‌توانست به یک رایانه‌ای دیگر راه یابد و در آن تکثیر شود و به همین ترتیب به رایانه‌های دیگر هم نفوذ کند و بصورت هندسی تکثیر شود. آن زمان 88000 رایانه به این شبکه وصل بود. این برنامه سبب شد طی مدت کوتاهی ده درصد از رایانه‌های متصل به شبکه در آمریکا از کار بیفتد .

به دنبال این حادثه، بنیاد مقابله با حوادث امنیتی (IRST) شکل گرفت که در هماهنگی فعالیتهای مقابله با حملات ضد امنیتی، آموزش و تجهیز شبکه‌ها و روشهای پیشگیرانه نقش مؤثری داشت. با رایج‌تر شدن و

استفاده عام از اینترنت، مسأله امنیت خود را بهتر و بیشتر نشان داد. از جمله این حوادث، اختلال در امنیت شبکه، WINK/OILS WORMدر سال1989 ، Sniff packetدر سال 1994 بود که مورد اخیر از طریق پست الکترونیک منتشر می‌شد و باعث افشای اطلاعات مربوط به اسامی شماره رمز کاربران می‌شد. از آن زمان حملات امنیتی- اطلاعاتی به شبکه‌ها و شبکه جهانی روزبه‌روز افزایش یافته است . گرچه اینترنت در ابتدا، با هدف آموزشی و تحقیقاتی گسترش یافت، امروزه کاربردهای تجاری، پزشکی، ارتباطی و شخصی فراوانی پیدا کرده است که ضرورت افزایش ضریب اطمینان آن را بیش از پیش روشن نموده است .