فهرست مطالب

CHAPTER

1

بررسی تاثیرات اجتماعی امنیت

فصل اول

اهداف فصل

- شناخت انواع جرائم کامپیوتری
- بررسی نقش فن آوری‌های نوین و کامپیوترها در جرائم
- تبعات اعتماد زیاد به عملکرد صحیح سیستم‌های کامپیوتری
- ملزومات امنیت در فضای سایبر
- شناخت انواع خسارت ناشی از جرائم کامپیوتری
- بررسی راهکارهای پیشنهادی برای امنیت فضای سایبر

1. بررسی تاثیرات اجتماعی امنیت

Risto Siilasmaa
مدیر عامل و CEO شرکت تولیده کننده ضد ویروس
F-Secure
و عضو هئیت مدیره شرکت Nokia

1.1. خلاصه فصل

بهره‌گیری از فن‌آوری سیستم‌های اطلاعاتی برای افزایش کارایی و بهره‌وری مناسب در اغلب زمینه‌ها به سرعت در حال گسترش است. شبکه‌های گستردهٔ کامپیوتری با انواع روش‌ها و ابزارهای دستیابی به اطلاعات، قدرت و توانایی کامپیوترهای موجود در شبکه را فارغ از مکان فیزیکی آن‌ها در دسترس استفاده‌کنندگان قرار داده است. از طرفی اتکای روزافزون به فن‌آوری اطلاعات، افزایش احتمال خطر ناشی از کاربرد آن را نیز در پی دارد. همزمان با پیشرفت و توسعهٔ قابل توجه فن‌آوری کامپیوتر در زمینه‌های مختلف نرم‌افزار و سخت‌افزار، زمینه کوشش جدی برای ایجاد امنیت لازم برای حفظ داده‌ها و سیستم‌ها فراهم شده است. در این فصل در ابتدا به تعریف جرائم کامپیوتری و نقش کامپیوترها در این جرائم پرداخته خواهد شد و در ادامه به انواع جرائم کامپیوتری و تاثیرات اجتماعی آن پرداخته می شود. در این مورد اصطلاحاتی همچون فضای سایبر و جنگ سایبر توضیح داده خواهد شد و ملزومات ایجاد امنیت در فضای سایبر ارائه می‌گردد.

1.2. مقدمه

امروزه ضرورت حفظ داده‌ها و سیستم‌ها به این دلیل قابل توجه است که ره‌آوردهای فن‌آوری معاصر عموماً در تصمیم‌گیری‌های مهم اتخاذ شده به وسیلهٔ حکومت‌ها و همچنین سازمان‌های معتبر جهانی نقش اساسی ایفا می‌کنند. به علاوه فن‌آوری پیشرفته صنعتی نیز مبتنی بر سیستم‌های اطلاعاتی قابل اطمینان، کارایی بهینه دارد. امروزه حجم قابل توجهی از مبادلات بازرگانی و مالی بین‌المللی با استفاده از فن‌آوری تبادل الکترونیکی داده‌ها (EDI[1]) انجام می‌شود. ایجاد کوچکترین خللی در این سیستم مبادلاتی، ضررهای هنگفتی را به طرفین مبادله تحمیل خواهد کرد که بعضاً ممکن است به ورشکستگی آنها بیانجامد. بیشتر سیستم‌های کنترل حمل و نقل، نیروگاهها و کارخانجات بزرگ امروزی از پایگاه‌های اطلاعاتی خود به صورت لحظه‌ای و پیوسته استفاده می‌کنند. بدیهی است که یک لحظه توقف سیستم و یا بروز کوچکترین خطا در داده‌ها می‌تواند خسارات غیر قابل جبرانی در هر یک از این سیستم‌ها بوجود آورد. همچنین بروز اشکال در نرم‌افزار و یا سخت‌افزارهای به کار گرفته شده در تجهیزات مدرن پزشکی، به علت در نظر نگرفتن ضروریات امنیت داده‌ها و سیستم‌ها، ممکن است صدمات غیرقابل جبرانی به وجود آورد. به رغم توسعهٔ صنعت کامپیوتر، تلاش اندکی برای آگاه کردن کاربران از آسیب‌پذیری داده‌ها و سیستم‌ها ناشی از تغییرات و تخریب‌های غیر مجاز عمدی و یا سهوی، صورت گرفته است. همچنان که حوادث و عوامل مخرب علیه سیستم‌های اطلاعاتی با وضوح بیشتری آشکار می شوند، کاربران این سیستم‌ها نیز تمایل بیشتری نسبت به حل مشکلات وابسته به تامین امنیت سیستم‌ها از خود نشان می‌دهند. به طور معمول در اغلب سیستم‌ها مسأله امنیت تا قبل از مرحلهٔ تعریف نیازمندی‌های عملیاتی به طور جدی مد نظر قرار نمی‌گیرد و سیستم به طور مستقیم وارد مرحله پیاده‌سازی می‌شود. بدین ترتیب دستیابی به یک سطح مناسب امنیتی برای سیستم در حال اجرا به ندرت امکان پذیر است. حتی در صورت امکان عملی شدن چنین امنیتی، هزینه‌های ناشی از این امر در مقایسه با سیستم‌هایی که از ابتدای طراحی، ملاحظات امنیتی را در نظر گرفته‌اند، بسیار بالاتر خواهد بود.

بنابراین ضروریات امنیتی هر سیستمی می‌بایست در مرحله تعریف نیازمندی‌های کاربران در نظر گرفته شود و در طراحی سیستم لحاظ شود.

---

[1] *Electronic Data Interchange*

1.3. جرائم کامپیوتري

در ابتدا باید تعریفی از جرائم کامپیوتری ارائه نمود. این عرصه از حقوق چون بسیار نوپا است، توسط دولت های مختلف بصورت های گوناگونی قابل تعریف است. بدیهی است که با توجه به گستردگی تعاریف جرائم کامپیوتری و نقص سیستم های امنیتی طراحی شده، برای جلوگیری از وقوع جرائم و حذف کامل آنها، حتی در صورتی که در شرایطی بسیار کنترل شده به تعریف جرائم بپردازیم، امکان پذیر نیست. شرکت های بزرگ کامپیوتری امروزه در پی روشهایی چون اثر انگشت کامپیوتری و تلفیق نرم افزار و سخت افزار برای شناسائی کامل فعالیت کاربران نهائی هستند.

جرمهای مرتبط با فن آوری اطلاعات

جرمهای مرتبط با فن آوری اطلاعات، جرائمی هستند که از سیستم‌های رایانه‌ای، هم بعنوان وسیله جرم و هم بعنوان مقصد و هدف جرم استفاده می‌کنند. عوامل نفوذی و ویروسهای رایانه‌ای به نوعی به کاربران رایانه‌ها خدمت بزرگی نموده‌اند، زیرا سبب شده‌اند تا استفاده‌کنندگان از این فن‌آوری دریابند، سیستم‌هایشان چقدر آسیب پذیرند و اطلاعات جمع آوری شده در پرونده‌های رایانه‌ای، نیاز به‌پشتیبانی و حفاظت دارند. عوامل دیگری نیز سیستم‌های رایانه‌ای را تهدید می‌کنند که خطراتشان و آسیب‌هایی که می‌رسانند بسیار بیش از ویروس‌ها و نفوذی‌ها است. از جمله آنها می‌توان به موارد زیر اشاره نمود:

- کلاهبرداریهای مرتبط با رایانه (بویژه توسط کارکنان داخل سازمانها)
- اعمال انتقام جویانه و کینه توزانه (توسط کارکنان سابق و ناراضی سازمانها)
- جاسوسی‌های صنعتی و صنفی (افشاء شدن اسرار صنعتی و صنفی)
- سوء استفاده‌های مالی حین نقل و انتقال الکترونیکی وجوه
- خطاهای رایانه‌ای و از بین رفتن برنامه‌ها و اطلاعات
- تجاوز رایانه‌ای به حریم خصوصی اشخاص

با یک نگاه کلی می‌توان خطرات حاصل از جرائم رایانه‌ای را به دو دسته تقسیم بندی نمود:

- دسته اول: شامل خطرات عمده نظیر کلاهبرداری، انتقام جویی و کینه توزی، جاسوسی صنعتی و تجاوز به حریم خصوصی است.
- دسته دوم: شامل خطرات جزئی نظیر نفوذی‌ها و ویروس‌ها می‌باشد.

جهت کاهش جرائم رایانه‌ای و جلوگیری از بروز برخی وقایع ناگوار بهتر است، قبل از وقوع حوادث پیشگیری‌های لازم صورت گیرد.

مراقبت و هوشیاری نسبت به کارکنان سابق

کارکنان ناراضی فعلی و کارکنان سابق سازمان می‌توانند بیشترین خطر را متوجه سیستم‌های رایانه‌ای بنمایند. چنین کارکنانی بدلیل آشنایی کامل با طرز کار و عملکرد سیستم‌ها اغلب جزئیات کار هر سیستم را بخوبی می‌دانند و می‌توانند باعث بروز مشکلات اساسی در سیستم‌های اطلاعاتی گردند و یا به بهترین شکل اطلاعات را دست‌کاری نمایند. مدیریت به نحو احسن می‌تواند با فراهم ساختن محیط مناسب از بروز این نوع جرائم رایانه‌ای جلوگیری نماید.

نقل و انتقال وجوه

نقل و انتقال الکترونیکی وجوه، زمینه مناسبی را برای جرائم رایانه‌ای فراهم می‌نماید. این گونه جرائم، طیف گسترده‌ای از مجرمین را در برمی‌گیرد. از دانش‌آموزان کنجکاو و بااستعداد گرفته تا پرسنل شاغل در بانکها و مؤسسات مالی، یا حتی افرادی که از طریق رایانه شخصی خود به طریقی وارد شبکه مورد نظرشده و هر یک به نوعی با دست کاری یا اعمال تغییر در اطلاعات، باعث عملکرد غلط نقل وانتقالات شده و بسته به نوع کار مبالغی را به حساب مشخصی واریز می‌نمایند.

اعتماد زیاد به عملکرد صحیح سیستم‌های رایانه‌ای

بسیاری از سازمان‌ها پس از نصب و راه اندازی سیستم‌های رایانه‌ای خود با اطمینان به اینکه رایانه‌ها اشتباه نمی‌کنند، بخشی را که قبلا به رسیدگی و بازرسی سیستم‌های دستی می‌پرداخته است، بلا استفاده می‌دانند. در اینگونه نگرش‌ها باید به این نکته اشاره کرد که گرچه سیستم‌های رایانه‌ای و ابزارهای سخت‌افزاری اغلب قابل اعتماد هستند، ولی همه توسط افراد و انسانها بکار گرفته می‌شوند و یک ماشین قابل اعتماد چنانچه توسط فردی غیرقابل اعتماد بکار گرفته شود، نمی‌توان زیاد به عملکرد آن اعتماد نمود.

فضای سایبر

Cyber Space یا همان فضای سایبری، استعاره‌ای برای تشریح سرزمین غیر فیزیکی تشکیل شده توسط سیستم‌های کامپیوتری می باشد. این سرزمین شامل عناصر و اشیاء خاص خود می‌باشد مانند فایل ها، پیغام های الکترونیکی، عکس ها و ... این فضا دارای مدل های انتقالی و حمل و نقل نیز می باشد.

1.4. نقش رایانه‌ها در جرائم

جرائم رایانه‌ای همیشه ضرر و زیان‌های مالی، اختلاس، رشوه و سوء استفاده‌های مالی به دنبال ندارد، گاه ممکن است این گونه جرائم باعث ضررهای جانی غیر قابل جبرانی گردند. بعنوان مثال چنانچه یکی از کارکنان ناراضی بیمارستان در پرونده پزشکی و دارویی بیماران تغییرات بی‌موردی اعمال نماید یا آنها را جابجا کند، مشکلاتی که بروز می‌کند، غیرقابل جبران است. رایانه‌ها چهار نقش اصلی را در جرائم ایفاء می‌کنند:

- به عنوان یک شیء: مجرمین اغلب برنامه‌ها، داده‌ها و گاه کل رایانه‌ها را خراب می‌کنند. بعنوان مثال، برای وارد آوردن خسارت به اطلاعات، زمانی که برنامه‌ها و داده‌ها در حافظه فعال هستند برق رایانه‌ها را قطع می‌کنند، یا در رایانه‌های حساس به درجه رطوبت و دما، دستگاه‌های تهویه را از کار می‌اندازند.
- به‌عنوان محل وقوع جرم: مثل تغییرمحتویات یک پرونده رایانه‌ای
- به‌عنوان وسیله جرم: برخی از جرائم اغلب بدون در اختیار داشتن رایانه‌ها امکان‌پذیر نیستند. مثل شبیه‌سازی ترازنامه یک شرکت با استفاده از یک پرونده جایگزین رایانه‌ای.
- به‌عنوان یک دام: در چنین مواردی از رایانه‌ها برای گول زدن و تهدید استفاده می‌شود. مثل آگهی‌های دروغ یا ارسال پیامهای کذب.

1.5. نقش فن آوري نوين در جرائم رايانه‌اي

درگذشتهٔ نه چندان دور، فردی که می‌خواست به سیستم رایانه‌ای سازمانی نفوذ کند تا آسیبی به اطلاعات برساند، ناگزیر بود حداقل یک خط تلفن جهت برقراری ارتباط و متصل شدن به شبکه داخلی آن سازمان در اختیار داشته باشد، حال با فراهم آمدن فن‌آوری‌های نوین ارتباطی، چنین شخصی می‌تواند عملیات مورد نظر خود را از فاصله دور با استفاده از تجهیزات در دسترس عامه مردم به انجام برساند.

عوامل نفوذی که به حریم سیستم‌ها تجاوز می‌کنند، ویروس‌ها را در رایانه‌ها جای می‌دهند یا در اجرای‌عملیات رایانه‌ای خلل وارد می‌کنند، در گذشته همگی در یک وجه مشترک بودند و همه به یک خط تلفن، کابل شبکه یا اتصال فیزیکی دیگری از این قبیل نیاز داشتند. در حال حاضر دیگر وجود چنین تجهیزاتی ضروری نیست. نسل‌جدید عوامل نفوذی، راه‌های جدیدی برای به انجام رساندن اعمال مخرب خود یافته‌اند. با ابزارهای نوین، آنان از درون اتومبیل خود یا حتی دفتر کاری که در اختیار دارند، می‌توانند