فهرست عناوین

Chapter 1

امنیت فن آوری

اهداف فصل

- آشنایی با ضرورت و اهمیت مطالعه امنیت فن آوری
- بررسی مفاهیم پایه به کار رفته در علم امنیت فن آوری اطلاعات و ارتباطات
- بررسی چگونگی ارتباط مفاهیم پایه و چگونگی استفاده از این مفاهیم
- شناخت معنای صحیح چارچوب و مفاهیم اولیه مدیریت ریسک
- مطالعه متریک‌های امنیتی، چگونگی تعریف، طراحی، استفاده و بیان متریک‌ها
- آشنایی با برخی مدل‌های ارزیابی و تحلیل ریسک
- آشنایی با برخی مدل‌های برگشت سرمایه در حوزه امنیت فن آوری

1. امنیت فن آوری

پروفسور رونالد ریوست Prof Ronald L. Rivest

استاد دانشکده کامپیوتر و الکترونیک دانشگاه MIT

از پیشگامان الگوریتم RSA**، رمزنگاری، الگوریتم‌های رمز و محرمانگی داده‌ها**

1.1. خلاصه فصل

با گسترش روز افزون تجهیزات فن آوری اطلاعات و ارتباطات در طی سالهای اخیر و وابستگی هرچه بیشتر حیات بشری به این سیستم‌ها، جنبه‌های بسیار زیادی از این تعامل تنگاتنگ و غیر قابل انکار مورد مطالعه و ارزیابی قرار گرفته است.

امنیت سیستم‌های کامپیوتری تنها یکی از زمینه‌های مورد بحث در این علم می‌باشد که شرایط نادر و پیچیده‌ای برآن حکم فرماست. ایده‌های طلایی مطرح شده در این حوزه به سرعت مورد استقبال قرار گرفته و در صنعت، تجارت، پزشکی و غیره مورد استفاده قرار می‌گیرد، ولی ناگهان و با همان سرعتی که رشد یافته است رو به افول نهاده و چالشهای بسیاری را پیش روی سرمایه گذاران قرار می‌دهد. در این فصل ابتدا به بیان برخی ضرورتها پرداخته و پس از بیان مفاهیم بنیادی حوزه امنیت فن آوری اطلاعات، مدل‌های مدیریت ریسک، متریک‌ها و بازگشت سرمایه معرفی می‌گردد.

1.2. مقدمه

جوامع مدرن بشری عمیقاً و به شکل غیر قابل انکاری وابسته به سیستم‌های نرم افزاری در همه ابعاد زندگی مدرن خود هستند. این آمیختگی در همه وجوه حیاتی زندگی بشر امروز از تعاملات کوچک در سطح اجتماع گرفته تا اجرای امورات کلانی چون انرژی، حمل و نقل، صناع دفاعی ارتباطات، صنایع تولیدی سبک و سنگین و مسائل مالی به شکل روز افزونی به چشم می‌خورد.

مسلم است که در این میان امنیت و صحت کارکرد این سیستمها بسیار حائز اهمیت و بنیادی است و نبود و یا وجود کاستیهایی در مقوله امنیت و کارکرد صحیح این سیستم‌ها بصورت فاجعه باری می‌تواند دنباله ای زخرابی و خسارت را بوجود بیاورد که نهایتاً زندگی و حیات بشریت را تحت الشعاع قرار خواهد داد.

تا زمانی که این سیستم‌های نرم افزاری (در حقیقت مجموعه تجهیزات فناوری اطلاعات و ارتباطات) آسیب‌پذیری‌ها و حفره‌ها را به همراه خود داشته باشند قطعا طعمه‌ای برای مهاجمان و سوداگران خواهند بود. مهاجمان اثرات بسیار مخربی و زیانباری بر سازمانهایی که دست‌اندرکار تولید این سیستمها هستند و یا سازمانهایی که این سیستم‌های اطلاعاتی را به خدمت گرفته‌اند خواهند گذاشت و البته قصه به همین جا ختم نمی‌شود، به هر حال طرف دیگر این خسارت مشتریان (عموم کاربران در هر شکل) و نهایتا تجارت است که تحت این ضرر و زیان‌ها قرار خواهد گرفت و دیری نمی‌پاید که سایه زوال بر صنعت انفورماتیک افکنده خواهد شد.

1.3. معرفی موسسه پونمن[1]

قبل از بیان اهمیت و الزام بررسی و مطالعه مهندسی امنیت و ارائه تعاریف، راه کارهای این صنعت، که پیشگامان عرصه فن آوری اطلاعات در سراسر جهان را مجبور به مطالعه و صرف هزینه‌های بسیار گزاف در حوزه‌های مختلف مهندسی امنیت ساخته است، کوتاهانه به معرفی موسسه پونمن وابسته به دانشگاه میشیگان می‌پردازیم.

فعالیت محققان این موسسه در مورد بررسی مسائل مختلف در محرمانگی داده‌ها[2]، حفاظت از داده‌ها[3] و تدوین سیاست‌های امنیتی[4] است و نتایج این تحقیقات ماهانه برای دولت مردان و شرکت‌های بزرگ بعنوان یک معیار سنجش موثق به کار می‌رود. اکنون به تازه‌ترین گزارش این موسسه که در انتهای سال 2011 ارائه شده است توجه کنید[4]:

1.3.1. هزینه‌های ناشی از سرقت اطلاعات

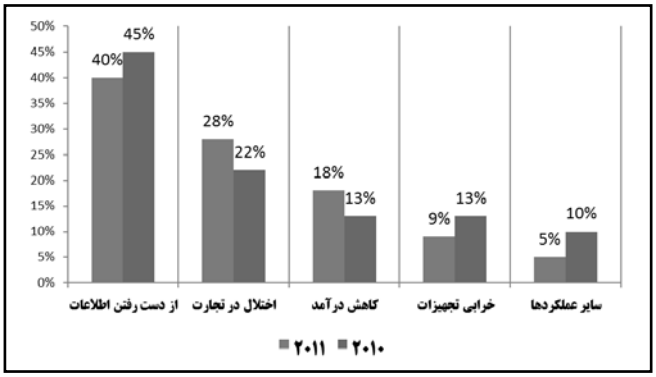
همواره مهمترین بخش از هر تخلف رایانه‌ای خارجی سرقت اطلاعات مهم سازمانها است، در یک گزارش سالانه اطلاعات به سرقت رفته حدود 40 درصد از کل هزینه‌های تخلف رایانه‌ای خارجی این سازمانها را در بر داشته که نسبت به سال قبل 2 درصد کاهش را نشان می‌دهد.

ایجاد اختلال در فرایندهای کسب و کار حدود 28٪ که نسبت به سال قبل حدود 6 درصد افزایش را نشان می‌دهد، کاهش درآمد 18 درصد، خرابی تجهیزات و اثراتی که سایر عملکردها داشته اند تا حدی کاهش قابل توجه داشته است.

---

1. کلیه مطالب این زیر بخش از Ponemon Institute LLC منبع شماره سه شیوه دستیابی به این اطلاعات ذکر شده است.

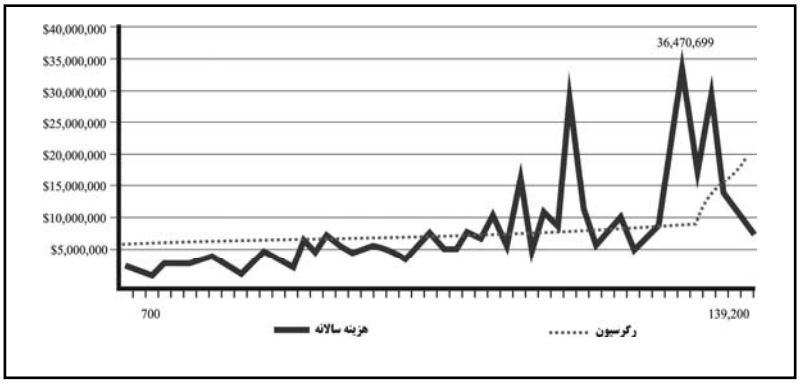
2. Data Privacy
3. Data Protection
4. Security Policy



شکل1-1 هزینه‌های ناشی از سرقت اطلاعات

1.3.2. توزیع هزینه‌های تخلفات رایانه‌ای بر اساس اندازه سازمان

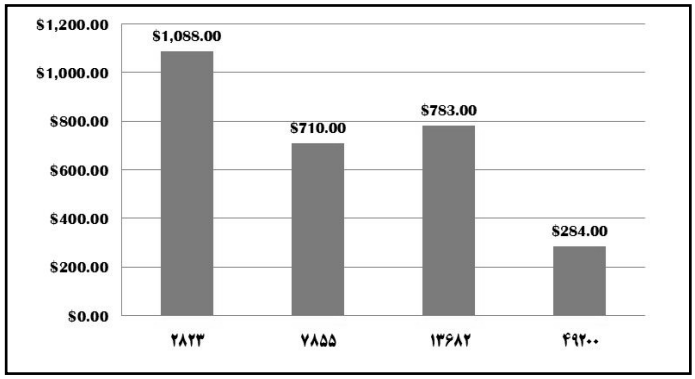
در این گراف اندازه سازمان بر اساس میزان پرسنل سازمانی تعیین شده است، همانطور که در مشاهده گراف می‌کنید، به طور محسوسی با رشد سازمان میزان هزینه جرایم و مشکلات امنیتی هم رشد می‌یابد و این روند طی رگرسیون خطی رشد یابنده (مثبت) نشان داده شده است.



شکل1-2 توزیع هزینه‌های تخلفات رایانه‌ای بر اساس اندازه سازمان

1.3.3. تحلیل‌های هزینه بر اساس تعداد پست سازمانی

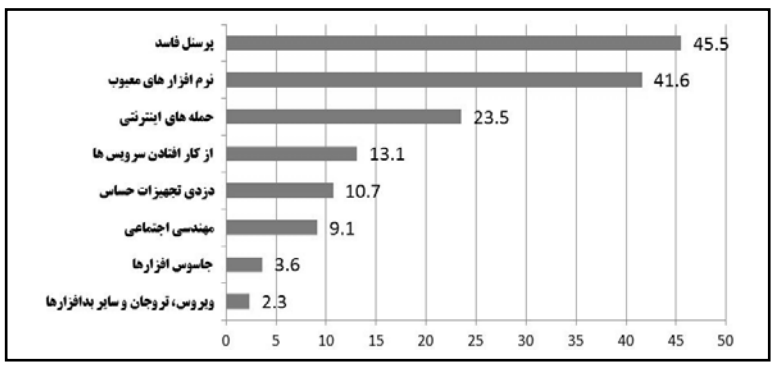
در شکل زیر خلاصه‌ای از تحلیلهای سالانه هزینه‌های سازمان به نسبت تعداد پست‌های پرسنلی نشان داده شده است، بنابر این نمودار که سازمانها را به چهار دسته تقسیم کرده است، متوسط هزینه سازمان‌های کوچک برای هر پست تقریبا 3.8 برابر متوسط هزینه‌ای است که سازمانهای خیلی بزرگ برای هر پست در مقوله تخلفات و ملاحظات امنیتی تحمل می‌کنند!



شکل 1-3 تحلیل‌های هزینه سازمان بر اساس تعداد پست پرسنلی

1.3.4. متوسط زمان بازیابی سرویس‌ها

دراین گزارش که 50 شرکت چند ملیتی درآن شرکت کرده اند،همانطورکه ملاحظه می کنید،میزان متوسط زمان لازم برای مواردپرسنل مختلف وپس ازآن نرم افزارهای وحملات به ترتیب بیشترین هزینه های مالی وزمانی برای کشف،خنثی سازی وبازیابی سرویس هاپس از ایجاد خسارات رابرسازمان تحمیل می کند.



شکل1-4 تحلیل‌های هزینه سازمان بر اساس تعداد پست پرسنلی

مشاهده می‌شود که با گسترش فناوری، مصدومیت در برابر حملات نیز گسترش یافته است، باید تدابیر امنیتی جدیدی در عرصه فن آوری اطلاعات در نظر گرفت ومهمتر از همه اینکه امنیت نرم افزار بعنوان بخش جدا ناپذیر فرایند تولید و توسعه فن آوری اطلاعات است و همه و همه به این معنا است که نیازمند مهندسی امنیت نرم افزار هستیم.

1.4. مفاهیم پایه

در این بخش مفاهیم اصلی که در کلیه مباحث این کتاب به وفور تکرار می‌شوند، مطابق تعاریف ذکر شده در استانداردهای امنیتی بیان می‌شود.

1.4.1. ریسک

ریسک‌های کسب و کار هر سازمان بطور مستقیم بر یک یا چند مشتری هدف آن سازمان اثر می‌گذارد، تشخیص ریسک می‌تواند به شفاف‌سازی و اینکه رویدادهای پیرامون سازمان به چه میزان بر کسب و کار سازمان اثر دارند، کمک کند. ریسک‌های تجاری می‌توانند شامل خسارت‌های مالی، بی اعتباری مارک[1]، تجاوز به حقوق مشتریان[2]، نقض مواضع قانونی، افشاء اسرار مالی و قرار دادی، افزایش هزینه‌های توسعه محصولات و نگه‌داری سیستم‌های اطلاعاتی جاری وغیره شود. مسئله مهم دیگر شیوه بیان شدت ریسک است که از طریق لغت‌های جاری در دنیای مالی و حسابرسی و متریک‌های مدیریت پروژه همانند ارزش سهام، سود مستقیم، سطح تولید، و هزینه تولید مجدد وغیره بیانشود.

مدیران، خصوصا مدیرانی که پاسخ گوی سرمایه گذاری‌های کلان هستند از مدیریت ریسک بعنوان چارچوبی برای اتخاذ تصمیم‌های مناسب جهت تشخیص، تسهیل، طبقه‌بندی و اولویت‌بندی ریسک استفاده می‌کنند همانگونه که در سالهای اخیر مدیریت ریسک، موفقیت‌های زیادی را خصوصا در سرمایه گذاری‌های حوزه امنیت فناوری اطلاعات داشته است.

❖ تعریف

تعاریف بسیار زیادی در مورد ریسک وجود دارد. در ذیل چند تعریف استاندارد و جهانی را ارائه می‌دهیم.

الف) تعریف *NIST*:

ریسک تابع احتمال این است که یک منبع تهدید داده شده از پتانسیل آسیب‌پذیری خاصی استفاده کندو نتیجه اثرات آن به شکل حوادث مضر در سازمان اتفاق بیافتد[3].

ب) تعریف NASA

این سازمان ترکیب احتمال (بطور کیفی یا کمی) اینکه یک برنامه یا پروژه حوادث ناخواسته‌ای را تجربه کند و نتیجه، اثر، یا شدت حادثه ناخواسته در جایی که اتفاق افتاده است را ریسک می‌نامد [8].

1. Brand

2. نقض مشتری مداری