

فهرست مطالب

13	فصل اول
15	1. بررسی تاثیرات اجتماعی امنیت
15	1.1. خلاصه فصل
16	1.2. مقدمه
17	1.3. جرائم کامپیوتری
19	1.4. نقش رایانه‌ها در جرائم
19	1.5. نقش فن آوری نوین در جرائم رایانه‌ای
20	1.6. انواع جرائم رایانه‌ای
21	1.7. امنیت فضای سایبر
23	1.8. راهکارهای امنیت فضای سایبر
26	1.9. منابعی برای مطالعه بیشتر
27	فصل دوم
29	2. استانداردهای امنیتی شبکه‌های کامپیوتری
29	2.1. خلاصه فصل
29	2.2. مقدمه
30	2.3. استانداردهای مدیریت امنیت اطلاعات
36	2.4. استاندارد BS7799 و لزوم پیاده سازی
37	2.5. سیستم مدیریت امنیت اطلاعات ISMS
40	2.6. تعاریف
41	2.7. مراحل اجرای نظام مدیریت امنیت اطلاعات
47	2.8. الزامات مستند سازی
48	2.9. مسئولیتهای مدیریتی
50	2.10. ممیزی داخلی ISMS

2.11	بازنگری مدیریتی ISMS	51
2.12	بهینه سازی ISMS	52
2.13	کنترلها و تعاریف A مربوط به ISMS	53
2.14	منابعی برای مطالعه بیشتر	74
77	فصل سوم	
79	3. مدیریت شبکه های کامپیوتری	
79	3.1 خلاصه فصل	
79	3.2 مقدمه	
81	3.3 اصول طراحی شبکه و لایه بندی	
81	3.4 تجهیزات شبکه	
84	3.5 تقسیم بندی شبکه ها	
84	3.6 طراحی و پیاده سازی مبتنی بر سرور	
87	3.7 کاربرد مدیریت شبکه	
88	3.8 سطوح مدیریتی	
91	3.9 منابعی برای مطالعه بیشتر	
93	فصل چهارم	
95	4. روشهای حمله به شبکههای کامپیوتری	
95	4.1 خلاصه فصل	
95	4.2 مقدمه	
97	4.3 انواع حملات در محیطهای کامپیوتری	
107	4.4 راهکارهای پیشگیری از حملات	
108	4.5 منابعی برای مطالعه بیشتر	
109	فصل پنجم	



5.	نفوذگرهای شبکه های کامپیوتری	112
5.1	خلاصه فصل	112
5.2	مقدمه	112
5.3	سناریوی کلی نفوذ	113
5.4	دستورالعملهای پیشگیرانه برای مقابله با نفوذگران	115
5.5	مفهوم تست نفوذ پذیری	129
	ابزار تست نفوذ پذیری به صورت Black Box	131
5.6	دستورالعملهای کاهش نفوذ	134
5.7	منابعی برای مطالعه بیشتر	135
فصل ششم		135
6.	امنیت فیزیکی شبکه های کامپیوتری	138
6.1	خلاصه فصل	138
6.2	امنیت فیزیکی و ساختمانی شبکهها	138
6.3	منابعی برای مطالعه بیشتر	146
فصل هفتم		145
7.	طبقه‌بندی و شناخت کاستیهای شبکههای کامپیوتری	150
7.1	خلاصه فصل	150
7.2	مقدمه	150
7.3	نفوذپذیری	151
7.4	طبقه‌بندی نفوذپذیری‌ها	152
7.5	آمار نفوذپذیری‌ها	164
7.6	طبقه‌بندی شرکت CISCO از نفوذپذیری‌ها	165
7.7	منابعی برای مطالعه بیشتر	166
فصل هشتم		167

8. تهدیدات سایتهای کامپیوتری 170

- 8.1 خلاصه فصل 170
- 8.2 مقدمه 170
- 8.3 طراحی سایت اطلاع رسانی 171
- 8.4 انواع سایتها و خدمات قابل ارائه 173
- 8.5 ضرورت تامین امنیت در محیط سایتها 177
- 8.6 تعریف سیاستهای امنیتی شبکه 178
- 8.7 استراتژی طرح سایت 181
- 8.8 هدایت و کنترل سایت 182
- 8.9 پروتکلهای و استانداردهای مدیریت سایت 182
- 8.10 سطوح امنیت در سایت بر اساس قواعد کلی CISCO 184
- 8.11 گسترش سیاست های امنیت یک سایت 186
- 8.12 پشتیبانی سایت و تجهیزات 187
- 8.13 مراحل پیاده سازی امنیت 188
- 8.14 منابعی برای مطالعه بیشتر 193

فصل نهم 193

9. روشهای شناسایی شبکه های کامپیوتری 196

- 9.1 خلاصه فصل 196
- 9.2 مقدمه 197
- 9.3 پورت چیست 197
- 9.4 عمل Port Scanning 198
- 9.5 روشهای Port Scanning 200
- 9.6 نرم افزارهای Port Scanning 203
- 9.7 Port Scanning در مقابل Firewall 203
- 9.8 نرم افزار Nmap 204



9.9	منابعی برای مطالعه بیشتر.....	205
فصل دهم 207		
10	چیدمان شبکه های کامپیوتری.....	209
10.1	خلاصه فصل.....	209
10.2	مقدمه.....	210
10.3	دیدگاه معماری (overview).....	211
10.4	قواعد کلی SAFE.....	215
10.5	ماژول طرح.....	223
10.6	Enterprise Campus.....	224
10.7	ماژول مدیریت.....	225
10.8	ماژول هسته.....	228
10.9	ساختمان ماژول توزیع.....	229
10.10	ماژول ساختمان.....	230
10.11	ماژول سرور.....	231
10.12	ماژول توزیع حاشیه ای.....	232
10.13	Enterprise edge.....	234
10.14	ماژولهای متحد اینترنتی.....	235
10.15	ماژولهای دسترسی از راه دور و VPN.....	238
10.16	ماژول شبکه گسترده.....	239
10.17	تهدیدات کاهش داده شده.....	240
10.18	ماژول تجارت الکترونیکی.....	240
10.19	منابعی برای مطالعه بیشتر.....	242
فصل یازدهم 243		
11	پدافند غیرعامل در شبکه های کامپیوتری.....	246

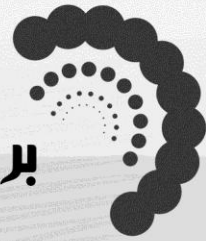
11.1	خلاصه فصل	246
11.2	مقدمه	246
11.3	ضرورت وجود پدافند غیر عامل	248
11.4	قابلیت های پدافند غیر عامل	248
11.5	اصول پدافند غیر عامل	249
11.6	اهداف کلان	249
11.7	راهبردها	250
11.8	پدافند غیر عامل در محیط IT	251
11.9	تقسیم بندی تدابیر ایمنی پدافند غیر عامل در زمینه IT	252
11.10	استراتژی ایمن سازی فضای سایر	272
11.11	منابعی برای مطالعه بیشتر	273
275	ضمیمه اول	
275	نمونه سؤالات مهندسی امنیت	



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 تأثیرات اجتماعی امنیت

**Risto Siilasmaa**

مدیر عامل و CEO شرکت تولید کننده ضد ویروس

F-Secure

و عضو هیئت 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 گسترده 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 توسعه 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 تأثیرات اجتماعی آن پرداخته می‌شود. 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 وسیله 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 (EDI¹) 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 توسعه 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 می‌شوند، 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 مرحله 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 کامپیوتری

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 پردازیم، 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 سیستم های رایانه ای، هم بعنوان وسیله جرم و هم بعنوان مقصد و هدف جرم استفاده می کنند. عوامل نفوذی و ویروس های رایانه ای به نوعی به کاربران رایانه ها خدمت بزرگی نموده اند، زیرا سبب شده اند تا استفاده کنندگان از این فن آوری دریابند، سیستم هایشان چقدر آسیب پذیرند و اطلاعات جمع آوری شده در پرونده های رایانه ای، نیاز به پشتیبانی و حفاظت دارند. عوامل دیگری نیز سیستم های رایانه ای را تهدید می کنند که خطراتشان و آسیب هایی که می رسانند بسیار بیش از ویروس ها و نفوذی ها است. از جمله آنها می توان به موارد زیر اشاره نمود:

- کلاهبرداریهای مرتبط با رایانه (بوژه توسط کارکنان داخل سازمانها)
 - اعمال انتقام جویانه و کینه توزانه (توسط کارکنان سابق و ناراضی سازمانها)
 - جاسوسی های صنعتی و صنفی (افشاء شدن اسرار صنعتی و صنفی)
 - سوء استفاده های مالی حین نقل و انتقال الکترونیکی وجوه
 - خطاهای رایانه ای و از بین رفتن برنامه ها و اطلاعات
 - تجاوز رایانه ای به حریم خصوصی اشخاص
- با یک نگاه کلی می توان خطرات حاصل از جرائم رایانه ای 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 نفوذی ها و ویروس ها می باشد.

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 با استعداد گرفته تا پرسنل شاغل در بانکها و مؤسسات مالی، یا حتی افرادی که از طریق رایانه شخصی خود به طریقی وارد شبکه مورد نظر شده و هر یک به نوعی با دست‌کاری یا اعمال تغییر در اطلاعات، باعث عملکرد غلط نقل و انتقالات 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 راه‌اندازی سیستم‌های رایانه‌ای خود با اطمینان به اینکه رایانه‌ها اشتباه نمی‌کنند، بخشی را که قبلاً 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 می‌باشد. این سرزمین شامل عناصر و اشیاء خاص خود می‌باشد مانند فایل‌ها، پیغام‌های الکترونیکی، عکس‌ها و ... این فضا دارای مدل‌های انتقالی و حمل و نقل نیز می‌باشد.



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.
- به عنوان محل وقوع جرم: مثل تغییرمحتویات یک پرونده رایانه‌ای
- به عنوان 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.
- به عنوان 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 آوری نوین در جرائم رایانه‌ای

در گذشته 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 اجرای عملیات 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. نسل جدید 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