امنیت در

تجارت الکترونیک

مطابق با سرفصل وزارت علوم، تحقیقات و فناوری برای رشته‌های کامپیوتر و فناوری اطلاعات

مولف:

دکتر محمد علی ترکمانی

سرشناسه	:	ترکمانی، محمدعلی، ۱۳۵۴ -
عنوان و نام پدیدآور	:	امنیت در تجارت الکترونیک [کتاب]/ مولف محمدعلی ترکمانی.
مشخصات نشر	:	مشهد: ارسطو، ۱۳۹۶.
مشخصات ظاهری	:	۲۳۱ ص.: مصور، جدول، نمودار.
شابک	:	978-600-432-180-8
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه: ص. ۲۳۰ - ۲۳۱.
موضوع	:	بازرگانی الکترونیکی -- تدابیر ایمنی
موضوع	:	Electronic commerce -- Security measures
موضوع	:	بازرگانی الکترونیکی -- الگوهای ریاضی
موضوع	:	Electronic commerce -- Mathematical models
موضوع	:	رمزگذاری داده‌ها
موضوع	:	Data encryption (Computer science)
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	:	Computer networks -- Security measures
رده بندی کنگره	:	HF۵۵۴۸/۳۲/ت۴۴الف۸ ۱۳۹۶
رده بندی دیویی	:	۶۵۸/۸۴
شماره کتابشناسی ملی	:	۴۸۱۷۷۷۶

نام کتاب : امنیت در تجارت الکترونیک

مولف :دکتر محمد علی ترکمانی

موضوع: امنیت شبکه های کامپیوتری.

ناشر : ارسطو (با همکاری سامانه اطلاع رسانی چاپ و نشر ایران)

صفحه آرایی، تنظیم و طرح جلد : علی بیات

تیراژ : ۱۰۰۰ جلد

نوبت چاپ : دوم – ۱۳۹۸

تعداد صفحات: ۲۳۸ ص

چاپ : مدیران

قیمت : ۴۶۰۰۰ تومان

تلفن های مرکز پخش : ۳۵۰۹۶۱۴۵ – ۳۵۰۹۶۱۴۶ - ۰۵۱ -۰۹۱۷۷۱۶۴۹۴۰

وب سایت: www.chaponashr.ir/Torkamani

فهرست مطالب

فصل دوم: انواع حملات در شبکه‌های کامپیوتری..... ۲۷

مقدمه:

امروزه کسب و کارهای مبتنی بر وب و تجارت الکترونیکی بـا تهدیـدهای زیـادی روبـرو هسـتند. نفوذگران از بد ابزارها و مکانیزم‌های تهاجمی مختلفی برای نفوذ، آسیب رسانی یا سرقت اطلاعات استفاده می‌کنند. لذا متخصصان تجارت الکترونیک باید دانش مورد نیاز در زمینه امنیت شـبکه را کسب نمایند. به همین علـت درس امنیـت در تجـارت الکترونیکـی در برنامـه درسـی رشـته‌های مهندسی IT گرایش تجارت الکترونیک قرار گرفته است. علیرغم اینکه این درس یکـی از دروس اصلی این رشته‌ها محسوب می‌شود، اما مرجع مناسبی برای آن وجود ندارد. حجم مراجـع معرفـی شده برای این درس بسیار زیاد است و تدریس این مطالب در یک نیم سال تحصیلی دشوار است.

در این کتاب سعی شده است که مطالب با زبانی ساده ارائه گردد. در انتهای هر فصل مجموعه سئوالات تشریحی و چهارگزینه‌ای به همراه حل آنها آورده شده است تا دانشـجویان گرامـی بهتـر بتوانند خود را برای آزمون‌هایی که در پیش رو دارند آماده نمایند. از آنجا که تاکید این کتـاب بـر روی اصول و مفاهیم رمزنگاری نیست، مباحث مربوط به رمزنگـاری بسـیار مختصـر و مفیـد و در حدی که خوانندگان برای فهم مباحث مربوط به امنیت شبکه و بررسی کاربردهـای رمزنگـاری در امنیت شبکه به آن نیاز دارند، بیان شده است. علاقه مندان بـه مباحـث رمزنگـاری و دانشـجویان درس رمزنگاری می‌توانند برای مطالعه مباحث مقدماتی تا پیشرفته این علم به کتاب رمزنگـاری از همین مولف مراجعه نمایند. امید است این اثر مورد توجه همکاران و دانشجویان گرامی قرار گیرد. از اسـاتید و دانشـجویان گرامـی تقاضـا دارم نقطـه نظـرات خـود را از طریـق ایمیـل m.a.torkamani@gmail.com با اینجانب در میان بگذارند تا انشالله در ویرایش‌هـای بعـدی کتاب اشکالات یا کاستی‌های احتمالی آن، مورد تجدید نظـر قـرار گیـرد. در پایـان وظیفـه خـود می‌دانم از زحمات همکار گرامی، آقای مهندس علی بیات به خاطر طراحی جلد کتاب و همچنـین مدیریت انتشارات ارسطو جناب آقای حسین قنبری تشکر و قدردانی نمایم.

محمد علی ترکمانی

پاییز ۱۳۹۴

فصل اول

مفاهیم و اصول امنیت اطلاعات

۱-۱-امنیت اطلاعات چیست؟

امنیت اطلاعات عبارت است از حفاظت اطلاعات در مقابل دسترسی های غیر مجاز، استفاده، افشاء، اختلال، اصلاح، مطالعه، بازرسی، ضبط یا تخریب، همچنین علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر تغییرات غیرمجاز از محرمانگی، تمامیت و دسترس‌پذیری اطلاعات. سایر ویژگی‌های دیگر امنیت اطلاعات از قبیل اصالت، اعتبار، انکارناپذیری، قابلیت جوابگویی و قابلیت اطمینان اطلاعات نیز می تواند مشمول این حفاظت باشند.

یک سیستم درست سیستمی است که اگر ورودی خوب و درست به آن داده شود خروجی درست به ما می‌دهد.

اما سیستم امن سیستمی است که اگر حمله کننده به آن ورودی بد بدهد، سیستم خراب نشود. به طور کلی طراحی امکانات بیشتر در یک سیستم از نظر امنیت اطلاعات دردسر ساز است. زیرا باید کنترل روی ورودی‌ها بیشتر باشد.

در امنیت اطلاعات به دنبال ساده بودن و مینیمم بودن سیستم هستیم. در صورتی که در یک سیستم خوب همیشه به دنبال امکانات بیشتر هستیم. در کل هدف ما این است که یک سیستمی داشته باشیم که هم درست و هم امن باشد.

۱-۱-۱-خصوصیات سیستم امن

- **محرمانگی:**[۱] اطلاعات باید تنها توسط افرادی که تأیید صلاحیت شده‌اند، قابل دیدن باشد. به عنوان مثال در یک سایت دانشگاه که تنها دانشجویان و اساتید و کارمندان دانشگاه حق ورود به سایت را دارند.
- **صحت:**[۲] داده‌ها نباید به صورت تصادفی یا عمدی تغییر داده شوند، نابود شده و یا گم شوند.
- **دسترسی پذیری:**[۳] هرگاه کاربر به سیستم نیاز داشت سیستم وجود داشته باشد. به عبارت دیگر سیستم باید قادر باشد هنگام درخواست کاربر، سرویس یا سرویس‌های مورد نظر را ارائه دهد.

۱-۲-اصطلاحات امنیتی

۱-۲-۱-آسیب‌پذیری[۴]

آسیب‌پذیری، یک خطا یا نقص در طراحی، پیاده‌سازی یا عملیات سیستم است. آسیب‌پذیری می‌تواند در یکی از موارد زیر باشد:

- طراحی سیستم: در این حالت پروتکل یا الگوریتم ایراد دارد. به عنوان مثال طراحی پروتکل TCP/IP درست انجام نشده و بسته‌های TCP/IP به صورت متن ساده[۵](رمز نشده) هستند. این یک ایراد طراحی است که یک آسیب‌پذیری را برای این پروتکل به وجود آورده است و باعث شده است که اگر یک نفر گوش کند، بتواند محتوای بسته‌های IP را ببیند.

۱Confidentiality
۲Integrity
۳Availability
۴Vulnerability
۵Clear Text

- پیاده‌سازی: به عنوان مثال فرض کنید در برنامه نویسی یک پروتکل، مواردی (نظیر اصول یا استانداردهای کدنویسی امن) را رعایت نکرده‌ایم، یا اشتباهاتی داریم. علاوه بر
- این، در پیاده‌سازی TCP/IP با توابع C یک سری آسیب‌پذیری‌هایی دیده می‌شود که علت آن اشکالات موجود در زبان C است. برای رفع این مورد باید از نسخه‌های جدیدتر این زبان و یا زبان جاوا استفاده کرد.
- عملیات سیستم ایراد دارد: فرآیندها درست انجام نمی‌شود. به عنوان مثال یک فرم پر شده و باید به دست یک نفر برسد ولی به فرد دیگری می‌رسد که نباید آنرا ببیند.

۲-۲-۱-حمله[۱]

حمله عبارتست از بهره برداری از آسیب‌پذیری‌های یک سیستم.

۳-۲-۱-تهدید[۲]

مجموعه‌ای از شرایط و پیشامدها که پتانسیل صدمه زدن به سیستم را دارد. فردی بدخواه که انگیزه و توانایی حمله را داشته باشد و یا یک سیستم که امکان یک حمله را فراهم می‌کند یک تهدید است.

۴-۲-۱-مفهوم AAA در امنیت اطلاعات

در دنیای امنیت اطلاعات به واژه مخفف AAA برخورد می‌کنیم که مخفف سه کلمه ذیل است:

- Authentication: تأیید هویت (احراز هویت) مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود. احراز هویت مکانیزمی است که بر اساس آن هر موجودیت(مانند یک شخص یا یک سرویس دهنده بانکی) بررسی می‌کند که آیا

۱Attack
۲Threat

شریک او در یک ارتباط، همان فردی است که ادعا می‌کند یا یک شخص اخلال‌گر ثالث است که خود را به جای طرف واقعی جا زده است.

- Authorization: اجازه[۱] مکانیزمی است که بر اساس آن مشخص می‌شود فرد یا موجودیتی که هویت آن احراز شده، مجوز انجام چه کارها و عملیاتی را در سیستم دارد.
- Accounting: حسابداری مکانیزمی است که مشخص می‌کند فرد مورد نظر چه سهمی از منابع سیستمی و خدماتی را می‌برد. یعنی به عنوان مثال اعتبار کافی دارد یا خیر.

در میان این سه واژه، مهمترین مرحله Authentication است که تامین دو مورد دیگر را نیز بسیار ساده می‌سازد.

به عنوان مثال وقتی فردی می‌خواهد به سیستم دسترسی پیداکند، ما می‌خواهیم بدانیم آیا همان فرد مورد نظر است یا خیر، تایید هویت انجام می‌دهیم. اما اجازه، بیشتر مفهوم کنترل سطح دسترسی را می‌دهد. به عنوان مثال، در سیستم اینترنتی یک دانشگاه، کاربر هنگام ورود ابتدا تایید هویت می‌شود که مشخص شود کاربری مجاز است یا خیر. در این سیستم اساتید و دانشجویان و سایر پرسنل دانشگاه مجاز به ورود هستند. اما در خصوص اجازه دسترسی، واضح است که یک دانشجو تایید هویت شده و وارد سیستم می‌شود ولی اجازه ویرایش نمرات را ندارد.

در خصوص حسابداری نیز به این مثال توجه کنید. فرض کنید شخصی تایید هویت می‌شود و وارد یک فروشگاه الکترونیکی می‌شود. وی اجازه خرید کردن را دارد. بنابراین Authorization نیز با موفقیت انجام میشود. اما ممکن است موجودی این فرد در سایت برای خرید کردن کافی نباشد. بنابراین فرایند Accounting به وی اجازه خرید را نخواهد داد.

۱Authorization

۵-۲-۱-عدم انکار (سندیت)[۱]

عدم انکار یعنی عمل ارسال و دریافت پیام و نیز محتوای داده و پیام توسط فرستنده و گیرنده قابل انکار نباشد (سرویسی که از انکار فرستنده و گیرنده جلوگیری می‌کند.) از این رو، وقتی پیامی ارسال گردید، فرستنده می‌تواند ثابت کند که گیرنده پیام را دریافت کرده است.

۳-۱-نفوذگر یا هکر[۲]

هکر در لغت به معنی نفوذگر است. هکرها به ۴ گروه نفوذگران کلاه سفید، نفوذگران کلاه سیاه، نفوذگران کلاه خاکستری و نفوذگران کلاه صورتی تقسیم بندی می‌شوند که در ادامه هر یک از این موارد شرح داده می‌شود.

۱-۳-۱- نفوذگران کلاه سفید[۳]

هدف این گونه از هکرها نشان دادن ضعف سیستم‌های امنیتی و شبکه‌های کامپیوتری می‌باشد. این گروه به نام هکرهای خوب معروف هستند. این دسته نه تنها به سیستم آسیب نمی‌رسانند، بلکه در تحکیم دیواره حفاظتی شبکه‌ها نقش اساسی دارند. کلاه سفید ها دارای خلاقیت عجیبی هستند و هر بار با روش جدیدی از دیواره امنیتی عبور می‌کنند.

۲-۳-۱-نفوذگران کلاه سیاه[۴]

نام دیگر این گروه Cracker است. کراکرها خرابکارانه ترین نوع هکرها هستند. این گروه به طور کاملا پنهانی اقدام به عملیات خرابکارانه می‌کنند. کلاه سیاه‌ها اولین چیزی که به فکرشان

۱Non-repudiation
۲hacker
۳White hat Hacker Group
۴Black Hat Hacker Group

می‌رسد نفوذ به سیستم قربانی است. کلاه سیاه‌ها می‌توانند با ارسال ویروسی که خودشان تهیه نموده‌اند،کنترل سیستم قربانی را در دست بگیرند. همیشه هویت اصلی کلاه سیاه‌ها پنهان است.

۳-۳-۱- نفوذگران کلاه خاکستری[۱]

نام دیگر این گروه Whacker است. هدف اصلی واکرها استفاده از اطلاعات سایر کامپیوترها می‌باشد و صدمه‌ای به کامپیوترها وارد نمی‌کنند. این گروه کدهای ورودی به سیستم‌های امنیتی را پیدا کرده و به داخل آن نفوذ می‌کنند، اما سرقت و خرابکاری جزء کارهای کلاه خاکستری‌ها نیست. آنها معمولا اطلاعات فنی را در اختیار عموم مردم قرار می‌دهند.

۴-۳-۱-نفوذگران کلاه صورتی[۲]

نام دیگر این گروه Booter می‌باشد. بوترها افراد بی سوادی هستند که فقط قادرند در سیستم‌ها اختلال به وجود آورند و یا مزاحم سایر کاربران در اتاق‌های چت شوند. کلاه صورتی‌ها اغلب از نرم‌افزارهای دیگران استفاده می‌کنند و خود سواد برنامه‌نویسی ندارند. البته در بعضی مواقع همین هکرهای کم سواد می‌توانند خطرهای جدی برای امنیت باشند.

۴-۱-دسته‌بندی کلی حملات

۴-۱- ۱-دسته بندی از نظر تغییر دادن اطلاعات

حملات را می‌توان به دو دسته کلی فعال[۳] و غیر فعال[۴] تقسیم نمود. در حمله غیر فعال مهاجم صرفا پیام‌های ارسالی را بازبینی و استراق سمع می‌نماید. حمله فعال زمانی رخ می‌دهد

۱Gray Hat Hacker Group
۲Pink Hat Hacker Group
۳Active Attack
۴Passive Attack

که حمله کننده علاوه بر استراق سمع یا دریافت پیام، آنرا تغییر داده و برای گیرنده ارسال نماید. از آنجا که در حمله غیر فعال تغییری در داده‌ها رخ نمی‌دهد، تشخیص آنها خیلی مشکل است.

۲-۴-۱-دسته‌بندی از نظر به چالش کشیدن اصول امنیت

- **افشای پیام[۱] یا سرقت اطلاعات:**[۲] خواندن یک ایمیل محرمانه یا شنود یک ارتباط تلفنی نمونه‌ای از این نوع حمله است. واضح است که این حمله عدم محرمانگی را فراهم می‌کند. (محرمانگی را به چالش می‌کشد).
- **قطع ارتباط:**[۳] عدم دسترسی‌پذیری را فراهم می‌کند.
- **تغییر اطلاعات:**[۴] صحت را به هم می‌زند.
- **جعل اطلاعات:**[۵] عدم صحت اطلاعات و عدم اعتبار را فراهم می‌کند.
- **انکار سرویس (رد درخواست):**[۶] عدم دسترسی را فراهم می‌کند. سیستم را از سرویس خارج می‌کند.
- **حمله تکرار:**[۷] به عمل دریافت داده در بین راه و ارسال مجدد آن با هدف دستیابی غیر مجاز، تکرار گویند. محرمانگی را به چالش می‌کشد.
- **نقاب‌زنی یا بدل:**[۸] حمله‌ای است که در آن حمله کننده خودش را جای فرد دیگری جا می‌زند. در واقع حمله کننده هویت فرد دیگری را سرقت می‌نماید. این حمله نوعی جعل اطلاعات است و عدم صحت را به دنبال دارد. اما چون مهاجم موفق شده خودش

---

۱ Release of Message
۲ Interception
۳ Interruption
۴ Modification
۵ Fabrication
۶ Denial of Service
۷ Reply
۸ Masquerade