حریم خصوصی و امنیت

اینترنت

مطابق با سرفصل وزارت علوم، تحقیقات و فناوری

مؤلف:

دکتر محمدعلی ترکمانی

سرشناسه : ترکمانی، محمدعلی، ۱۳۵۴ -
عنوان و نام پدیدآور : حریم خصوصی و امنیت اینترنت/مؤلف محمدعلی ترکمانی.
مشخصات نشر : مشهد: ارسطو، ۱۳۹۵
مشخصات ظاهری : ۲۰۲ ص .: مصور.
شابک : ۱-۹۲-۷۹۴۰-۶۰۰-۹۷۸
وضعیت فهرست‌نویسی : فیپا
موضوع: اینترنت -- تدابیر ایمنی
موضوع: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع: کامپیوترها -- ایمنی اطلاعات
موضوع: پایگاه‌های اطلاعاتی – امنیت
رده‌بندی کنگره: ۱۳۹۴ ۴ح۴ت/TK۵۱۰۵/۵۹
رده‌بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی : ۴۱۱۱۳۳۱

نام کتاب : حریم خصوصی و امنیت اینترنت
مؤلف : دکتر محمدعلی ترکمانی
ناشر : ارسطو (باهمکاری سامانه اطلاع‌رسانی چاپ و نشر ایران)
صفحه‌آرایی: محمدعلی ترکمانی
تنظیم و طرح جلد : محمدعلی ترکمانی و علی بیات
تیراژ : ۱۰۰۰ جلد
نوبت چاپ : چهارم– ۱۳۹۸
چاپ : مدیران
قیمت : ۳۶۰۰۰ تومان
تلفن‌های مرکز پخش : ۳۵۰۹۶۱۴۵ – ۳۵۰۹۶۱۴۶ - ۰۵۱ -۰۹۱۷۷۱۶۴۹۴۰
وب‌سایت: www.chaponashr.ir/Torkamani

فهرست مطالب

فصل شانزدهم: مراقبت از فرزندان در فضای مجازی .. ۱۷۲

مقدمه:

امروزه با گسترش روزافزون اینترنت ، تجارت الکترونیک و بانکداری مبتنی بر اینترنت، سازمان‌ها بسیاری از سرویس‌های خود را از طریق اینترنت ارائه می‌دهند. همچنین تعداد فروشگاه‌های اینترنتی نیز به‌شدت افزایش‌یافته است. اما وجود آسیب‌پذیری در سیستم‌های کامپیوتری باعث شده است که کاربران اینترنت با تهدیدهای زیادی روبرو باشند. نفوذ گران از بد ابزارها و مکانیزم‌های تهاجمی مختلفی برای نفوذ، آسیب‌رسانی یا سرقت اطلاعات استفاده می‌کنند. لذا همه کاربران اینترنت باید دانش موردنیاز در زمینه حریم خصوصی و امنیت اینترنت را کسب نمایند. با توجه به نیاز کاربران اینترنت به منبعی کاربردی و جامع این کتاب را تألیف نمودم. در این کتاب سعی شده است که مطالب با زبانی ساده ارائه گردد که تمامی مخاطبین بتوانند از آن استفاده نمایند. همچنین این کتاب سرفصل‌های وزارت علوم، تحقیقات و فناوری برای درس حریم خصوصی و امنیت اینترنت را پوشش می‌دهد. در پایان هر فصل نیز تعدادی سؤال تشریحی و چهارگزینه‌ای تألیفی وجود دارد تا دانشجویان گرامی بهتر بتوانند خود را برای آزمون‌های پیش رو آماده نمایند. از مخاطبین گرامی تقاضا دارم نقطه نظرات خود را از طریق ایمیل m.a.torkamani@gmail.com با اینجانب در میان بگذارند تا انشالله در ویرایش‌های بعدی کتاب اشکالات یا کاستی‌های احتمالی آن، مورد تجدیدنظر قرار گیرد. در پایان وظیفه خود می‌دانم از زحمات همکار گرامی، آقای مهندس علی بیات به خاطر طراحی جلد کتاب و همچنین مدیریت انتشارات ارسطو جناب آقای حسین قنبری به خاطر مساعدت در کار چاپ تشکر و قدردانی نمایم.

محمدعلی ترکمانی

اسفند ۹۶

فصل اول

مفاهیم و اصول امنیت اطلاعات

۱-۱-امنیت اطلاعات چیست؟

امنیت اطلاعات عبارت است از حفاظت اطلاعات در مقابل‌دسترسی‌های غیرمجاز، 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 می‌تواند مشمول این حفاظت باشند.

۱-۱-۱-خصوصیات سیستم امن

- **محرمانگی:**[۱] اطلاعات باید تنها توسط افرادی که تائید صلاحیت شده‌اند، قابل‌دیدن باشد. به‌عنوان‌مثال در یک سایت دانشگاه که تنها دانشجویان و اساتید و کارمندان دانشگاه حق ورود به سایت رادارند.
- **صحت:**[۲] داده‌ها نباید به‌صورت تصادفی یا عمدی تغییر داده شوند، نابودشده و یا گم شوند.

---

۱ Confidentiality
۲ Integrity

- **دسترسی‌پذیری:**[۱] هرگاه کاربر به سیستم نیاز داشت سیستم وجود داشته باشد. به‌عبارت‌دیگر سیستم باید قادر باشد هنگام درخواست کاربر، سرویس یا سرویس‌های موردنظر را ارائه دهد.

۲-۱-اصطلاحات امنیتی

۱-۲-۱-آسیب‌پذیری[۲]

آسیب‌پذیری، یک خطا یا نقص در طراحی، پیاده‌سازی یا عملیات سیستم است.

۲-۲-۱-حمله[۳]

حمله عبارت است از بهره‌برداری از آسیب‌پذیری‌های یک سیستم.

۳-۲-۱-تهدید[۴]

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 امکان‌یک حمله را فراهم می‌کند یک تهدید است.

۴-۲-۱-مفهوم AAA در امنیت اطلاعات

در دنیای امنیت اطلاعات واژه مخفف AAA مخفف سه کلمه ذیل است:

- Authentication: تائید هویت (احراز هویت) مکانیزمی است که هویت حقیقی افراد بر اساس آن اثبات می‌شود. احراز هویت مکانیزمی است که بر اساس آن هر

۱Availability
۲Vulnerability
۳Attack
۴Threat

- موجودیت(مانند یک شخص یا یک سرویس‌دهنده بانکی) بررسی می‌کند که آیا شریک او در یک ارتباط، همان فردی است که ادعا می‌کند یا یک شخص اخلال‌گر ثالث است که خود را به‌جای طرف واقعی جا زده است.
- Authorization: اجازه[۱] مکانیزمی است که بر اساس آن مشخص می‌شود فرد یا موجودیتی که هویت آن احرازشده، مجوز انجام چه‌کارها و عملیاتی را در سیستم دارد.
- Accounting: حسابداری مکانیزمی است که مشخص می‌کند فرد موردنظر چه سهمی از منابع سیستمی و خدماتی را می‌برد. یعنی به‌عنوان‌مثال اعتبار کافی دارد یا خیر.

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

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

در خصوص حسابداری نیز به این مثال توجه کنید. فرض کنید شخصی تائید 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 قابل‌انکار نباشد (سرویسی که از انکار فرستنده و گیرنده جلوگیری می‌کند.) ازاین‌رو، وقتی پیامی ارسال گردید، فرستنده می‌تواند ثابت کند که گیرنده پیام را دریافت کرده است.

۳-۱-نفوذ گر یا هکر[۲]

هکر در لغت به معنی نفوذ گر است. هکرها به ۴ گروه نفوذ گران کلاه‌سفید، نفوذ گران کلاه‌سیاه، نفوذ گران کلاه خاکستری و نفوذ گران کلاه صورتی تقسیم‌بندی می‌شوند که در ادامه هر یک از این موارد شرح داده می‌شود.

۴-۱-دسته‌بندی کلی حملات

۴-۱- ۱-دسته‌بندی ازنظر تغییر دادن اطلاعات

حملات را می‌توان به دودسته کلی فعال[۳] و غیرفعال[۴] تقسیم نمود. در حمله غیرفعال مهاجم صرفاً پیام‌های ارسالی را بازبینی و استراق سمع می‌نماید. حمله فعال زمانی رخ می‌دهد که حمله‌کننده علاوه بر استراق سمع یا دریافت پیام، آن را تغییر داده و برای گیرنده ارسال نماید. ازآنجاکه در حمله غیرفعال تغییری در داده‌ها رخ نمی‌دهد، تشخیص آن‌ها خیلی مشکل است.

---

۱ Non-repudiation
۲ hacker
۳ Active Attack
۴ Passive Attack

۲-۴-۱-دسته‌بندی ازنظر 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 باهدف دستیابی غیرمجاز، تکرار گویند. محرمانگی را به چالش می‌کشد.
- **نقاب زنی یا بدل:**[۸] حمله‌ای است که در آن حمله‌کننده خودش را جای فرد دیگری جا می‌زند. درواقع حمله‌کننده 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 را به‌جای قربانی جا بزند، در ادامه می‌تواند اطلاعات محرمانه قربانی را خوانده (عدم محرمانگی) و یا با ارسال بسته‌های زیاد قابلیت دسترسی را به چالش بکشد.

---

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

۱-۵-یک Hacker از چه راهی وارد سیستم می‌شود؟

برخی از روش‌هایی که ممکن است کامپیوتر شما از طریق آن هک یا ویروسی شود

- هکر می‌تواند در موارد ذیل IP کامپیوتر شمارا به دست آورده و پورت‌های باز کامپیوتر شمارا شناسایی نماید:
- زمانی که روی یک لینک کلیک می‌کنید.
- وارد یک سایت می‌شوید .
- با مسنجر در حال چت کردن هستید.
- هکر می‌تواند برای شما یک بدافزار را در قالب یک تصویر یا فایل اجرایی ایمیل کند و شما به‌محض باز کردن آن فایل هک می‌شوید.
- نهایتاً هکرها می‌توانند به‌حساب بانکی و پسوردهای شما دسترسی پیدا کند و یا اینکه خسارت‌های جبران‌ناپذیری به شما وارد کند

۱-۶- سؤالات تشریحی

۱-اصطلاحات زیر را توضیح دهید؟

الف-Confidentiality ب-Reply Attack

۲- شش مورد از نیازمندی‌های امنیتی یک سیستم را نام‌برده و توضیح دهید.

۳- در هر یک از موارد زیر مشخص کنید کدام‌یک از سه اصل امنیت اطلاعات به چالش کشیده شده است؟

الف- جواد تمرین‌های مریم را کپی کرد.

ب- علی سیستم مهسا را از کار انداخت.

ج-فریدون مقدار موجودی حساب زهرا را از ۱۰۰ دلار به ۱۰۰۰ دلار تغییر داد.

د- داریوش امضای خودش را به‌جای امضای رضا گذاشت.

ه-بهرام یک دامنه بانام Yahoo.comثبت کرد و با استفاده از آن جلوی سرویس Yahoo Buy را گرفت.