



انتشارات امین روز

امنیت تجارت الکترونیکی

ا. د. ذریعہ عرب سرخی
(عضو هیات علمی پژوهشگاه ارتباطات و فناوری اطلاعات)
مینو غریبی سبیل
رقیہ قربانلو

سرشناسه : غرب سرخی، ابوذر، ۱۳۶۰ -
 عنوان و نام پدیدآور : امنیت تجارت الکترونیکی / ابوذر غرب سرخی، مینو غربی سیل، رقیه قربانلو.
 مشخصات نشر : تهران: ادیبان روز، ۱۳۹۶.
 مشخصات ظاهری : ۵۱۲ ص.
 شابک : ۹۷۸-۶۰۰-۸۱۹۰-۲۳-۳
 وضعیت فهرست نویسی : فیا
 موضوع : بازرگانی الکترونیکی -- تدابیر ایمنی
 موضوع : Electronic commerce -- Security measures
 شناسه افزوده : غربی سیل، مینو، ۱۳۶۶ -
 شناسه افزوده : قربانلو، رقیه، ۱۳۶۶ -
 رده بندی کنگره : ۱۳۹۶ الف ۳۶/ع HF۵۵۴۸۳۲
 رده دیو : ۶۵۸/۸۷۲
 شماره کتابت سی : ۴۳۷۵۵۱

مؤلفین : ابوذر غرب سرخی - مینو غربی سیل - رقیه قربانلو
 گرافیک و صفحه آرا : مریم علیزاده پناه
 طراح جلد : حیدر علی شایان
 شمارگان : ۱۰۰۰
 قیمت : ۳۹۰۰۰ تومان
 شابک : ۹۷۸-۶۰۰-۸۱۹۰-۲۳-۳
 تاریخ انتشار : ۹۶
 نوبت چاپ : اول
 چاپ و صحافی : طوس

کلیه حقوق این اثر متعلق به انتشارات ادیبان روز می باشد و در صورت استفاده از این کتاب (کپی تکثیر، استفاده در کارگاه های آموزشی) بدون اجازه ناشر پیگرد قانونی دارد.

تلفن : ۶۶۹۵۶۸۱۲-۱۵

خرید اینترنتی از طریق:

www.adibanbook.com

www.adibanbook.ir



انتشارات ادیبان روز

پیشگفتار

امروزه سیلان از فعالیت‌های فردی، اجتماعی و حرفه‌ای در بستر ارتباطات و فن‌آوری اطلاعات انجام می‌شود که از آن با نام فضای سایبر یاد می‌شود. فضای سایبر و بستر وب به‌عنوان محمل تعامل و تبادل در فضای شخصی و کاری مدرنی شناخته می‌شود. این فضا به‌واسطه قابلیت‌ها و خدمات منحصر به فردی که دارد بسیاری از کاربران را به سمت خود جذب نموده است لیکن فضای سایبر و وب بهترین محمل برای دسترسی مهاجم به تمام چیزهایی است که کاربر را مجاب به حضور در این فضا نموده است. در واقع، اگرچه فضای سایبر به‌عنوان یک توانمندساز در دنیای کسب و کار امروز عمل می‌کند اما نمی‌تواند زمینه‌ساز بروز و ظهور تهدیدهایی باشد که منشاء آن‌ها خود این فضا است. اگر نگاهی به روند توسعه این فضا داشته باشیم خواهیم دید که توسعه فضای سایبر به‌واسطه افزایش دامنه کارایی آن و به تبع آن، افزایش روزافزون حجم سرمایه‌گذاری در چنین محیطی است.

بخش قابل توجهی از این سرمایه‌گذاری در حوزه تجارت الکترونیکی انجام می‌شود؛ جایی که سازمان با ارائه مجموعه‌ای از کالاها و خدمات به دنبال کسب منفعت از حامیان مشتریان خود است. وجود پول و گردش مالی در چنین فضایی انگیزه‌های مهاجم برای دست بردن به چنین محیطی را افزایش می‌دهد. بنابراین بروز و ظهور تهدیدهای امنیتی در چنین فضایی و مواجهه کارآمد با آن‌ها مستلزم توجه به سه مقوله مشخص است. اولین موضوع ماهیت، زیرساخت‌ها و کارکردهای رایج در فضای تجارت الکترونیکی است که ضعف در طراحی، پیاده‌سازی، مدیریت و یا بهره‌برداری از آن‌ها زمینه‌ساز سوءاستفاده مهاجم می‌شود. اهمیت آسیب‌پذیری‌های امنیتی از آن جهت است که این موارد تأثیری کارکردی بر تهدیدهای امنیتی حوزه تجارت الکترونیکی دارند؛ بدین

معنا که عدم وجود آسیب‌پذیری با عدم بروز تهدید همراه است. دومین موضوع به رفتار سوء یا منابع تهدیدی اشاره دارد که برای تحقق اهداف بدخواه خود از آسیب‌پذیری‌های موجود در زیرساخت‌ها، کارکردهای سیستم‌های تجارت الکترونیکی استفاده می‌کنند. موضوع سوم نیز به کنترل‌های فنی، مدیریتی و اقدام‌های امنیتی اشاره دارد که راه نفوذ تهدید یا بهره‌برداری از آسیب‌پذیری را مسدود می‌نمایند. توجه به هر سه مورد فوق از الزام‌های برقراری شرایط امن در فضای تجارت الکترونیکی امروزی است. ما زمانی شاهد حضور مستمر مشتریان در وبسایت تجارت الکترونیکی خود هستیم که ضعف‌های سیستم‌ها و خدمات خود را شناخته، نحوه سوءاستفاده از آن‌ها را رصد کنیم و حداقل‌های لازم برای مواجهه با چنین شرایطی را پیش‌بینی و عملیاتی نماییم.

در این کتاب برآنیم تا ضمن بررسی مفاهیم پایه، امنیت اطلاعات و تجارت الکترونیکی به موضوع تهدیدها و آسیب‌پذیری‌های رایج در این فضا پرداخته و راهکارهای لازم را برای رفع و مواجهه با آن‌ها پیشنهاد نماییم. در این راه مقوله کنترل‌ها، سازوکارها، خدمات و فن‌آوری‌های امنیتی مورد ارزیابی و تحلیل قرار خواهند گرفت.

ابوذر عرب‌سرخی

زمستان ۱۳۹۵

مقدمه‌ای بر کتاب امنیت تجارت الکترونیکی

امروز خدمات و فعالیت‌های تجارت الکترونیکی به معنای واقعی کلمه فراگیر شده‌اند به گونه‌ای که تمام یا بخشی از کارهای روزانه ما در این فضا انجام می‌شود. ابزارهای ارتباطی امروزه در جیب یا کیف هر مشتری یا مصرف‌کننده‌ای قرار دارد و بدین ترتیب این قابلیت برای وی فراهم می‌شود تا در هر زمان و مکانی به خرید چیزهایی بپردازد که مدنظر وی قرار دارد. تجارت الکترونیکی در دنیای امروز یکی جدا از زندگی و کار افراد نیست بلکه یکی از الزام‌های چنین فضایی محسوب می‌شود. دلیل این امر به واسطه توسعه تجهیزات کاربری و فن‌آوری‌های ارتباطی و اطلاعاتی قابل‌حملی است که خدمات تجارت الکترونیکی را تسهیل و تسریع می‌کنند. جدا از این موضوع، گسترش روز افزون تجارت الکترونیکی تا حد زیادی مدیون ورود فعالیت‌های مالی و تجاری در سطح شبکه‌های اجتماعی است. اگرچه شبکه‌های اجتماعی موجب افزایش حجم تراکنش‌های مالی و تجاری در دنیای دیجیتال شده‌اند اما تهدیدهای امنیتی خاص خود را نیز به این فضا وارد نموده‌اند. به‌رحال، درک دغدغه‌ها، امنیت تجارت الکترونیکی و حرکت درست در این فضا مستلزم توجه به کلیه سیستم‌ها، زیرسیستم‌ها و فعالیتهای رایج در این حوزه است.

تأمین امنیت در فضای تجارت الکترونیکی از نگاه دی‌فعال مختلف باهم تفاوت دارد. طراح سیستم، امنیت را یک مقوله پیچیده می‌بیند. از این منظر، تأمین امنیت مستلزم طراحی مجموعه‌ای از سیستم‌های منفرد است که باید به گونه‌ای طراحی شوند که عملکرد درست سیستم را تضمین نمایند. مالک سیستم تجارت الکترونیکی نگاه متفاوتی دارد. از نظر وی امنیت بر آن چیزی تمرکز دارد که وجهه کسب‌وکار را ارتقاء و اعتماد مشتری و وب‌سایت را بهبود می‌بخشد. کاربر نهایی دیدی ساده‌تر به این موضوع دارد. کاربر می‌خواهد با سیستمی کار کند که مطمئن و ایمن باشد و کارکرد صحیحی از خود ارائه دهد. همانطور که مشخص است مقوله امنیت تنها در نظر گرفتن یک مقوله خاص و استقرار یک سازوکار حفاظتی مشخص نیست بلکه یک موضوع چندوجهی است.

در راستای تأمین امنیت در فضای تجارت الکترونیکی کتاب حاضر به معرفی اصول، سازوکارها و معیارهایی می‌پردازد که عمده آن‌ها به شرح زیر هستند:

- توجه به کاربر باید در اولویت همه امور تجارت الکترونیکی قرار گیرد. شما به عنوان متولی امنیت وبسایت خود هر اقدامی که انجام می‌دهید باید به تأیید کاربر نهایی رسیده و مورد پذیرش وی قرار گیرد. تأمین و استقرار خدمات امنیتی بدون استفاده آسان آن‌ها توسط کاربر، شکست است.
- شما در این کتاب خواهید آموخت که چگونه وبسایت و زیرساخت تجارت الکترونیکی خود را ایمن سازید. در این راه، شما ضمن آگاهی از مفاهیم پایه و الزام‌های امنیتی با استراتژی‌ها، تکنیک‌ها و سازوکارهای کاربردی امنیت آشنا خواهید شد.
- یکی از ملاحظات اصلی بامنیت در فضای تجارت الکترونیکی موضوع مقیاس‌پذیری زیرساخت‌ها و خدمات است. در این کتاب شما براساس رویکردهای مبتنی بر تحلیل مخاطره نحوه طراحی و استقرار چنین زیرساخت‌هایی را خواهید آموخت.
- دسترس‌پذیری بالا یکی از الزام‌های اساسی در حوزه تجارت الکترونیکی است. براین اساس، شما خواهید آموخت که چگونه سیستم‌های تجارت الکترونیکی خود را توسعه دهید به گونه‌ای که توان مدیریت حجم بالای درخواست‌های مشتریان را داشته باشد.
- مواجهه کارآمد با تهدیدهای امنیتی مستلزم شناسایی آسیب‌پذیری‌های سیستم‌های تجارت الکترونیکی است. هرچه این ضعف‌ها جدی‌تر باشند امکان سوءاستفاده از آن‌ها بیشتر است. بنابراین شما باید روش‌هایی را بیاموزید که ضمن آن آسیب‌پذیری‌ها و روش‌های رفع آن‌ها شناسایی و تعیین گردد.

مجموعه موارد فوق به خواننده این امکان را می‌دهد تا با درک شرایط حاکم بر فضای تجارت الکترونیکی رفتاری مناسب جهت مواجهه با ملاحظات امنیتی این فضا داشته باشد.

درک بهتر ساختار و محتوای کتاب حاضر مستلزم نگاهی اجمالی به مواردی است که در قالب فصول مختلف مطرح شده است. برای این منظور در ادامه به بررسی مطالب اصلی هر فصل پرداخته خواهد شد.

فصل اول: در این فصل بر مفاهیم پایه تجارت (از سنتی به الکترونیکی)، توسعه الگوهای رایانشی و معماری‌های شبکه، فن‌آوری‌های ارتباطی و اطلاعاتی و جایگاه آن در شکل‌گیری و گسترش الکترونیکی تأکید می‌شود. نحوه نقش‌آفرینی مؤلفه‌های سازنده تجارت نظیر کالاها (سخت و دیجیتال)، تجهیزات (کلاسیک و فناورانه) و نحوه تعامل‌ها (از مواجهه رودررو تا مجازی) از دیگر مواردی هستند که در این فصل مورد توجه قرار می‌گیرند.

فصل دوم: در این فصل با نون جدید تجارت الکترونیکی یعنی تجارت سیار پرداخته می‌شود. در این راستا، نحوه شکل‌گیری، دامنه تجارت سیار و چگونگی ایفای نقش تجهیزات الکترونیکی کاربر در این فضا ترسیم شده است. در واقع، فصل دوم به مرور تجهیزات و زیرساخت‌هایی می‌پردازد که نقشی حیاتی را در توسعه تجارت سیار ایفا می‌کنند.

فصل سوم: این فصل به تبیین قابلیت‌هایی می‌پردازد که عامل موفقیت یا شکست خدمات و سیستم‌های تجارت الکترونیکی محسوب می‌شوند. ارکان امنیت (دسترس‌پذیری و محرمانگی)، قابلیت‌های توسعه‌پذیری، تحمل خطا و تعامل‌پذیری و نیز قابلیت‌های تعمیر و عملیاتی‌شدن همگی از خصیصه‌هایی هستند که در توسعه سیستم‌های تجارت الکترونیکی پیش‌بینی و عملیاتی شوند. تعریف، انواع و ابعاد هریک از این قابلیت‌ها و نقش آن‌ها در توسعه کاربری تجارت الکترونیکی از دیگر مواردی هستند که در قالب فصل سوم به آن پرداخته می‌شود.

فصل چهارم: این فصل با بهره‌گیری از مضامین به‌دست آمده در فصول قبلی به تبیین جایگاه و اهمیت امنیت در فضای تجارت الکترونیکی می‌پردازد. رویکردهای مختلف امن‌سازی این فضا با محوریت تحلیل مخاطره در فصل چهارم تشریح می‌شود. علاوه بر این، به موضوع قابلیت استفاده از سیستم و تأثیر امنیت بر آن پرداخته می‌شود. این مطالب برای طرح موضوع مقیاس‌پذیر

نمودن امنیت به کار گرفته می‌شود. در نهایت نیز ملاحظات اصلی مرتبط با امن‌سازی تراکنش‌های تجارت‌الکترونیکی طرح و صورت‌بندی می‌شود.

فصل پنجم: این فصل به بررسی سازوکارهایی می‌پردازد که به‌عنوان بلوک‌های سازنده امنیت تجارت‌الکترونیکی شناخته می‌شوند. تکنیک‌ها، استانداردها و ابزارهای رمزنگاری و کنترل دسترسی از عمده روش‌هایی هستند که نقش به‌سزایی در پروسه امن‌سازی سیستم‌ها و خدمات وبسایت شما ایفا می‌کنند. خدمات و سیستم‌های تجارت‌الکترونیکی در سطوح مختلف (میزبان، شبکه و خدمت) درگیر دغدغه‌های امنیتی خاص خود بوده و با تهدیدها و حوادث امنیتی متنوعی مواجه هستند. تحلیل تهدیدهای شناخته‌شده در این سطوح و نحوه مواجهه مؤثر با آن‌ها از طریق به‌کارگیری ابزارهای امنیتی نیز در قالب این فصل تشریح گردیده‌است.

فصل ششم: اصول و مؤلفه‌های امنیت تجارت‌الکترونیکی در قالب این فصل تشریح گردیده‌اند. مواردی همچون احراز هویت، حیثیت اختار، عدم انکار، امنیت ارتباطات و محرمانگی از الزام‌های امنیتی یک وبسایت تجارت‌الکترونیکی محسوب می‌شوند که تأمین آن‌ها مستلزم به‌کارگیری یک یا مجموعه‌ای از خدمات است که ضابطاً همین نام و تحت عنوان مؤلفه‌های امنیتی سیستم شناخته می‌شوند. در کنار این موارد، به شرح نظام‌های امنیتی و برخی از اصول (نظیر اصل حداقل دسترسی و ممیزی امنیت) و استراتژی‌های امنیتی رایج (نظیر دفاع در عمق و جداسازی) در قالب این فصل معرفی شده و به آن‌ها پرداخته می‌شود.

فصل هفتم: تأمین کارآمد امنیت در سطح منابع اطلاعاتی سیستم تجارت‌الکترونیکی مستلزم شناخت آسیب‌پذیری‌های این حوزه و بررسی نحوه سوءاستفاده از آن‌ها است. این کار از طریق به‌کارگیری تکنیک‌های مختلفی انجام می‌شود که ارزیابی آسیب‌پذیری، تشخیص و پیش‌گیری از نفوذ، سازوکارهای شناسایی و آزمون نفوذپذیری از عمده این موارد هستند. طرح موضوعی، کارکردهای اصلی و مصادیق شناخته‌شده ابزارها و تکنیک‌های پوشش و ارزیابی امنیتی در قالب فصل هفتم کتاب تبیین می‌شود.

فصل هشتم: تحلیل آسیب‌پذیری‌های امنیتی یک امکان خاص را برای متخصص امنیت فراهم می‌آورد و آن برآورد تهدیدهایی است که از چنین ضعف‌هایی بهره‌برداری می‌کنند. این تهدیدها در فصل هشتم مورد بررسی و تحلیل قرار می‌گیرند. معرفی این تهدیدها صرفاً براساس رایج بودن آن‌ها در فضای تجارت الکترونیکی انجام شده است. نوع و گونه تهدید، دلایل بروز تهدید و کنترل‌های لازم برای مواجهه با آن از عمده مواردی هستند که در تشریح تهدیدهای امنیتی مورد توجه قرار گرفته‌اند.

فصل نهم: تصمیم کارآمدی تصمیم‌ها و اقدام‌های امنیتی در فضای تجارت الکترونیکی مستلزم واریسی آن‌ها در قالب یک فرآیند رسمی صدور گواهی و اعتباردهی است که این موارد در قالب فصل نهم کتاب تبیین می‌شود. در این فصل، مجموعه‌ای از روش‌ها، استانداردها، تکنیک‌ها و سازوکارهای تضمین و صحت‌سنجی معرفی شده و حوزه کاربرد و کارکردهای هریک از آن‌ها تبیین می‌شود.

محتوای ارائه شده در این کتاب برای گسترش وسیعی از ذی‌نفعان سازمانی و امنیتی مفید خواهد بود. این فرد ممکن است مالک سیستم، توسعه دهنده سیستم، معمار سیستم، معمار امنیت، مهندس نرم‌افزار، مدیر پروژه امنیت، تحلیل‌گر امنیت، متخصص فنی سیستم، مدیر فنی و یا حتی مسئول تدوین استراتژی‌های شرکت باشد.

براساس آنچه در بخش قبلی پیشگفتار بدان اشاره شد، محتوای فصل کتاب را می‌توان در دو محور مبانی تجارت الکترونیکی و مبانی امنیت تجارت الکترونیکی سازماندهی نمود. هریک از این محورها که بخش اول و دوم این کتاب را تشکیل می‌دهند سرفصل‌هایی را در زمینه مفاهیم پایه، اصول و خط‌مشی‌های کاری، سازوکارهای فنی، تکنیک‌ها و استانداردها دارند. از این‌رو، هریک از ذی‌نفعان تجارت الکترونیکی براساس نیاز کاری خود می‌توانند به بخش‌های خاصی از این کتاب رجوع نمایند.

۲۹	بخش اول	مقدمه‌ای بر تجارت
۳۱	فصل اول	عصر اینترنت-تجارت الکترونیکی
۳۲		❖ تکامل تجارت
۳۳		○ تجارت الکترونیکی در مقابل تجارت سنتی
۳۴		○ کالاهای سخت در مقابل کالاهای دیجیتالی
۳۵		○ مزایای استفاده از تجارت الکترونیکی در مقابل تجارت سنتی
۳۸		○ پرداخت
۳۸		○ پول
۳۹		○ نقش بانک ساسی پول
۴۱		○ بانک‌های تخصصی پول
۴۲		○ شبکه بانکی الی
۴۷		■ رایانش ابری
۵۴		○ پرداخت و تجارت الکترونیک
۵۸		❖ رایانش توزیع‌شده-افزودن ارزش به تجارت
۵۸		○ سرویس‌دهنده/ مشتری
۶۱		○ رایانش شبکه‌ای
۶۳		○ رایانش ابری
۶۹		○ مشخصه‌های سازنده رایانش ابری
۷۳		○ امنیت ابر
۷۴		■ بازیگری معماری
۷۵		■ احراز هویت متمرکز
۷۵		■ ورود یکپارچه و تفویض اختیار
۷۶		■ کنترل دسترسی مبتنی بر نقش
۷۶		■ مخزن گواهی
۷۷		■ ارتباطات و ذخیره‌سازی امن
۷۷		■ مدیریت مجزا



۷۷	▪ مطابقت با مقررات (پیروی قانونی)
۷۸	▪ اعتماد توزیع شده (توزیع اعتماد)
۷۸	▪ تازگی
۷۸	▪ اعتماد
۷۹	▪ جداسازی امن
۸۱	▪ تفویض اختیار
۸۳	▪ تهدیدها
۸۹	▪ جنبه‌های عملیاتی
۹۲	▪ حاکمیت

فصل دوم تجارت سیار

۹۷	❖ مفهوم و جایگاه تجارت سیار
۹۹	○ مشخصه‌های تجارت سیار
۱۰۰	○ حوزه‌های کاربرد تجارت سیار
۱۰۱	○ عوامل بازدارنده و محدودیت‌های تجارت سیار
۱۰۲	❖ دستگاه‌های الکترونیکی کاربری
۱۰۴	❖ گوشی تلفن همراه و تجارت سیار
۱۰۴	○ چشم‌انداز
۱۰۹	○ تجارت سیار در مقابل تجارت الکترونیکی
۱۱۰	▪ سخت‌افزار سیار
۱۱۱	▪ سازنده دستگاه
۱۱۲	▪ سیستم عامل
۱۱۳	▪ پشته
۱۱۴	▪ مدل کاربرد
۱۱۸	▪ حالت سیار
۱۲۰	❖ فن‌آوری‌های سیار: پشته روی استروئیدها
۱۲۰	○ شبکه‌های حامل



۱۲۴	○ پشته‌های سیار
۱۲۵	■ نسخه میکروی جاوا
۱۳۱	■ اندروید
۱۳۹	■ بلک‌بری
۱۴۱	■ آیفون
۱۴۶	■ سیمبین
۱۴۸	○ پشته‌های دیگر

۱۵۱	نقش قابلیت‌ها در امنیت تجارت الکترونیکی
۱۵۲	❖ رمزنگاری، صحت و دسترس‌پذیری
۱۵۲	○ محرمانگی
۱۵۴	○ صحت
۱۵۵	○ دسترس‌پذیری
۱۵۶	❖ توسعه‌پذیری
۱۵۷	○ توسعه‌پذیری جعبه‌سیاه
۱۵۸	○ توسعه‌پذیری جعبه‌سفید
۱۵۸	○ توسعه‌پذیری جعبه شیشه‌ای
۱۶۰	○ توسعه‌پذیری جعبه خاکستری
۱۶۱	❖ قابلیت تحمل خطا
۱۶۱	○ دسترس‌پذیری بالا
۱۶۲	■ پرش الکترونیکی
۱۶۲	■ رخدادنگاری از راه‌دور
۱۶۲	■ ایجاد پایگاه‌داده سایه
۱۶۲	■ سرویس‌دهنده افزونه
۱۶۳	■ خوشه‌بندی سرویس‌دهنده
۱۶۳	■ خطوط ارتباطی افزونه
۱۶۳	○ تحمل خطا در شبکه ارتباطات از راه‌دور



۱۶۴	❖ قابلیت تعامل پذیری
۱۶۴	○ استانداردهای تعامل پذیری
۱۶۵	○ آزمون قابلیت تعامل پذیری
۱۶۶	❖ قابلیت نگهداری
۱۶۷	❖ قابلیت اداره / مدیریت پذیری
۱۶۸	❖ مازولار بودن / پیمانه‌ای بودن
۱۶۸	○ قابلیت پایش
۱۷۰	○ تشخیص نفوذ
۱۷۱	○ آزمون ردپذیری
۱۷۱	○ تحمیل انحراف / خلف
۱۷۳	❖ قابلیت عملیاتی شدن
۱۷۳	○ حفاظت از منابع و موجودی‌های ممتاز
۱۷۴	○ دسته‌بندی‌های کنترل‌سی مربوط به قابلیت عملیاتی شدن تجارت الکترونیکی
۱۷۶	❖ قابلیت حمل
۱۷۷	❖ قابلیت پیش‌بینی
۱۷۸	❖ قابلیت اطمینان
۱۸۰	❖ همه‌جا حاضر
۱۸۱	❖ قابلیت استفاده
۱۸۱	❖ مقیاس پذیری
۱۸۳	❖ پاسخگویی
۱۸۴	❖ قابلیت ممیزی
۱۸۶	❖ قابلیت ردیابی



۱۸۹	بخش دوم امنیت تجارت الکترونیکی
۱۹۱	فصل چهارم مبانی تجارت الکترونیکی
۱۹۳	❖ چگونه یک سیستم امن می‌شود
۱۹۶	❖ امنیت مخاطره‌محور (مبتنی بر مخاطره)
۱۹۹	❖ امنیت و قابلیت استفاده
۱۹۹	○ قابلیت استفاده از کلمه‌های عبور
۲۰۰	○ نکات کاربردی
۲۰۰	❖ امنیت مقیاس‌پذیر
۲۰۱	❖ تراکنش‌ها را چطور امن کنید
۲۰۵	فصل پنجم بلوک‌های سازنده: ابزارهای امنیتی در اختیار شما
۲۰۶	❖ رمزنگاری
۲۰۶	○ نقش رمزنگاری
۲۰۷	○ سیستم‌های رمزنگاری متقارن
۲۰۸	▪ اصول رمزنگاری با کلید متقارن
۲۰۹	○ نمونه‌هایی از سیستم‌های رمزنگاری داده
۲۰۹	▪ سیستم رمز سزار
۲۱۱	▪ سیستم رمز وینگر
۲۱۳	▪ رمزنگاری از طریق جابجایی (تبدیل)
۲۱۴	▪ سیستم رمز ورنام (کلید رمز یک‌بار مصرف)
۲۱۶	▪ رمزهای بلوکی
۲۱۹	▪ بردار مقداردهی اولیه
۲۲۰	▪ رمزهای دنباله‌ای
۲۲۱	▪ استاندارد رمزنگاری داده‌ها
۲۲۳	▪ استاندارد رمزنگاری سه‌گانه داده‌ها
۲۲۳	▪ استاندارد رمزنگاری پیشرفته
۲۲۵	▪ الگوریتم بین‌المللی رمزنگاری داده‌ها



۲۲۵	○ سیستم‌های رمزنگاری نامتقارن
۲۲۶	▪ توابع رمزنگاری یک‌طرفه
۲۲۷	▪ الگوریتم‌های کلید عمومی
۲۲۸	• الگوریتم آراس‌ای
۲۲۸	• الگوریتم ال‌جمال
۲۲۹	• الگوریتم منحنی بیضوی
۲۳۰	▪ مقایسه طول کلید در الگوریتم‌های رمزنگاری متقارن و نامتقارن
۲۳۰	▪ امضاء دیجیتالی
۲۳۱	▪ خلاصه پیام
۲۳۲	▪ ویژگی‌های درهم‌ریزی
۲۳۴	▪ استانداردهای امضاء دیجیتالی و درهم‌ریزی امن
۲۳۶	▪ کد احراز هویت پیام درهم‌ریزی شده
۲۳۶	○ تبادل کلید دفی-هلمن
۲۳۸	○ زیرساخت کلید عمومی
۲۳۸	▪ گواهی دیجیتالی
۲۳۹	▪ دایرکتوری‌ها و X.500
۲۴۰	▪ پروتکل سبک‌وزن دسترسی به دایرکتوری
۲۴۰	▪ گواهی‌نامه‌های X.509
۲۴۲	▪ فهرست ابطال گواهی
۲۴۲	▪ الحاقیه‌های گواهی‌نامه X.509
۲۴۴	○ تولید اعداد تصادفی
۲۴۶	○ سیستم‌های صدور گواهی کلید عمومی - گواهی‌نامه دیجیتالی
۲۴۷	▪ مدیریت کلید
۲۴۷	▪ توزیع کلید
۲۴۸	• ابطال کلید
۲۴۸	• بازیابی کلید

۲۴۹	• تجدید یا تغییر کلید
۲۴۹	• از بین بردن یا تخریب کلید
۲۵۰	• کلیدهای چندگانه
۲۵۰	• توزیع شدگی در مقابل مدیریت متمرکز کلید
۲۵۰	○ حفاظت از داده‌ها
۲۵۰	▪ مقابله با از دست دادن داده‌ها
۲۵۲	▪ امنیت پایگاه داده
۲۵۴	کنترل دسترسی
۲۵۴	○ کنترل دسترسی
۲۵۵	کنترل دسترسی
۲۵۵	▪ کنترل دسترسی اجباری
۲۵۷	▪ کنترل دسترسی خیمه‌ای
۲۵۷	▪ کنترل دسترسی غیر متقابل (ممنوعی بر نقش)
۲۵۸	▪ کنترل دسترسی وب
۲۵۹	▪ جایگاه کنترل دسترسی در امنیت تجارت الکترونیکی
۲۶۰	❖ مقاومت‌سازی سیستم
۲۶۰	○ امنیت سطح خدمت
۲۶۰	▪ سرویس دهنده‌های وب
۲۶۲	▪ امنیت سرویس دهنده وب
۲۷۱	▪ خدمات وب
۲۷۵	▪ کاربردهای تحت وب
۲۸۰	○ امنیت در سطح میزبان
۲۸۰	▪ سیستم‌های عامل
۲۸۱	▪ مرورگر کاربران
۲۸۲	▪ کاربر محلی
۲۸۴	○ امنیت شبکه



۲۸۴	▪ دیواره آتش
۲۸۷	▪ پروتکل‌ها
۲۹۹	▪ پست الکترونیکی
۳۰۰	▪ مشکل‌های بدافزاری

۳۰۷	فصل ششم مؤلفه‌های سیستم: نحوه اجرا و پیاده‌سازی
۳۰۸	❖ احراز هویت
۳۰۸	○ احراز هویت کاربر
۳۰۹	▪ نام‌ها، عبور
۳۱۱	▪ پروتکل
۳۱۳	○ احراز هویت شبکه
۳۱۶	○ احراز هویت دستگاه
۳۱۸	○ احراز هویت واسطه نامه، پروتکل
۳۱۸	▪ احراز هویت پایه HTTP
۳۱۸	▪ احراز هویت دسترسی محدود HTTP
۳۱۹	▪ الگوی احراز هویت درخواست- پاسخ سیستم عامل، ویندوز
۳۲۰	▪ احراز هویت براساس تابع AuthSub
۳۲۱	○ احراز هویت فرآیند
۳۲۳	❖ تفویض اختیار
۳۲۴	❖ عدم انکار
۳۲۴	❖ حریم خصوصی
۳۲۵	○ خط‌مشی حریم خصوصی
۳۲۶	○ قوانین و رهنمودهای مرتبط با حریم خصوصی
۳۲۷	○ اصول اتحادیه اروپا
۳۲۸	○ مسائل حریم خصوصی مرتبط با امور پزشکی
۳۲۹	○ پلت‌فرمی برای توصیف اولویت‌های حریم خصوصی
۳۳۰	○ پایش الکترونیکی

۳۳۲	❖ امنیت اطلاعات
۳۳۲	○ مفاهیم مدیریت امنیت
۳۳۳	▪ چرخه عمر امنیت سیستم
۳۳۳	▪ محرمانگی، صحت و دسترس پذیری
۳۳۵	▪ معماری امنیتی چندلایه
۳۳۶	▪ کنترل های امنیتی
۳۳۷	○ طبقه بندی داده ها و اطلاعات
۳۳۷	○ مزایای طبقه بندی اطلاعات
۳۳۸	○ مفاهیم طبقه بندی اطلاعات
۳۳۸	▪ اصطلاحات ای طبقه بندی
۳۴۰	▪ معیارهای طبقه بندی اطلاعات
۳۴۰	▪ روندهای طبقه بندی اطلاعات
۳۴۱	▪ توزیع اطلاعات طبقه بندی شده
۳۴۱	▪ نقش های مرتبط با طبقه بندی اطلاعات
۳۴۵	○ دسته بندی داده
۳۴۶	○ مدل Bell-LaPadula
۳۴۸	❖ تمیزی داده ها و سیستم
۳۴۹	○ پروتکل سیس لاگ
۳۵۲	○ سامانه SIEM
۳۵۴	❖ دفاع در عمق
۳۵۸	❖ اصل حداقل حقوق دسترسی
۳۶۰	❖ اعتماد
۳۶۲	❖ جداسازی
۳۶۲	○ مجازی سازی
۳۶۳	○ جعبه شنی
۳۶۳	○ جداسازی دامنه امنیتی پروتکل اینترنت



۳۶۴	❖ خط‌مشی امنیتی
۳۶۵	○ بیانیه خط‌مشی مدیریت ارشد
۳۶۵	■ خط‌مشی‌های توصیه‌ای
۳۶۵	■ خط‌مشی‌های مقرراتی
۳۶۵	■ خط‌مشی‌های آگاهی‌رسانی
۳۶۶	○ طبقه‌بندی خط‌مشی توسط مؤسسه استانداردها و فن‌آوری
۳۶۷	امنیت ارتباطات
۳۶۷	○ امنیت بین‌شبکه‌ای
۳۶۹	■ شبکه‌های همگن
۳۷۰	■ شبکه‌های ناهمگن

فصل هفتم اعتماد کنید اما بررسی کنید شرایط امنیتی را کنترل نمایید

۳۷۴	❖ ابزارهای بررسی امنیت
۳۷۷	○ ارزیابی آسیب‌پذیری و تحلیل ریسک
۳۷۸	○ تشخیص و جلوگیری از نفوذ با استفاده از اسنورت
۳۸۱	○ پویش شبکه با استفاده از ان‌مپ
۳۸۲	○ پویش آسیب‌پذیری
۳۸۲	■ نسوس
۳۸۴	■ نیک‌تو
۳۸۴	■ وایرشارک
۳۸۵	○ آزمون نفوذپذیری
۳۸۶	■ متاسپلویت
۳۸۷	■ ایرکزک-ان‌جی
۳۸۹	○ شناسایی شبکه‌های بی‌سیم
۳۸۹	■ نت‌استامپلر
۳۹۰	■ کیزمت
۳۹۱	■ تحلیل‌گر شبکه‌های وای‌فای شرکت ایرمگنت

۳۹۳	○ بررسی کاربردهای تحت وب
۳۹۳	▪ لینکس
۳۹۴	▪ وی جت
۳۹۶	▪ تلپورت
۳۹۶	▪ بلک ویندو
۳۹۸	▪ براون ریکلیز

فصل هشتم: تهدیدها و حمله‌ها: آنچه مهاجمان انجام می‌دهند

۴۰۳	◆ مفاهیم پایه
۴۰۳	○ هدف
۴۰۴	○ تهدید
۴۰۵	○ حمله
۴۰۶	○ کنترل
۴۰۷	○ خط‌مشی یکسان و همسو برای منابع
۴۰۸	◆ حمله‌های رایج در حوزه تجارت الکترونیکی
۴۰۸	○ حمله دورزدن سازوکارهای احراز هویت و مدیریت نشست
۴۱۰	○ جعل درخواست/ کلاهبرداری از طریق ارسال درخواست کد بین‌سایتی
۴۱۵	○ حمله ارسال کد بین‌سایتی
۴۱۶	▪ ارسال کد دائمی/ ذخیره‌شده بین‌سایتی
۴۱۶	▪ ارسال کد غیردائمی/ انعکاسی بین‌سایتی
۴۱۷	▪ ارسال کد بین‌سایتی مبتنی بر مدل شیء هستند
۴۲۱	○ حمله سرقت از سیستم نام دامنه
۴۲۲	○ حمله نقض محدودیت دسترسی به URL
۴۲۳	○ رخنه‌های تزریقی
۴۲۸	○ حفاظت نامناسب از لایه انتقال
۴۲۸	○ حمله ذخیره‌ساز ناامن رمزنگاری
۴۳۰	○ حمله ارجاع ناامن مستقیم به شیء



۴۳۱	○ حمل‌های کلاهبرداری و ارسال هرزنامه
۴۳۲	○ رخنه‌افزار و حمله‌های مرتبط با آن
۴۳۳	○ حمله‌های مرتبط با پیکربندی ضعیف امنیتی
۴۳۳	○ حمله راهبری و هدایت غیرمعتبر

۴۳۷	فصل نهم صدور گواهی: تضمین
۴۳۸	❖ صدور گواهی و اعتباردهی
۴۳۸	○ فرایند صدور گواهی
۴۳۹	■ ارزیابی کنترل‌های امنیتی
۴۴۲	❖ استانداردها و رهنمودهای مربوطه
۴۴۲	○ معیارهای ارزیابی سیستم‌های رایانه‌ای مورداعتماد
۴۴۳	○ معیارهای مشترک (استاندارد ۱۵۴۰ سازمان بین‌المللی استاندارد)
۴۴۴	○ فرایند صدور گواهی و اعتباردهی در حوزه تضمین اطلاعات دفاعی
۴۴۷	○ بخشنامه شماره A-130-130 در خصوص امنیت و بودجه
۴۴۸	○ فرایند ملی صدور گواهی و اعتباردهی در حوزه تضمین اطلاعات
۴۵۲	○ قانون مدیریت امنیت اطلاعات فدرال
۴۵۳	○ چارچوب ارزیابی امنیت فن‌آوری اطلاعات فدرال
۴۵۴	○ استاندارد شماره ۱۹۹ پردازش اطلاعات فدرال
۴۵۵	○ استاندارد شماره ۲۰۰ پردازش اطلاعات فدرال
۴۵۷	○ سایر منابع و رهنمودها
۴۵۷	❖ سازمان‌ها و نهادهای استانداردگذاری مرتبط
۴۵۸	○ انجمن جریکو
۴۵۸	○ کارگروه مدیریت توزیع شده
۴۵۹	○ سازمان بین‌المللی استاندارد/ کمیسیون بین‌المللی برق
۴۶۳	○ مؤسسه استانداردهای مخابراتی اروپا
۴۶۳	○ انجمن صنعتی شبکه‌های ذخیره‌سازی
۴۶۴	○ پروژه امنیت برنامه‌های کاربردی متن‌باز

۴۶۸	○ سند ۳۰-۸۰۰ مؤسسه استانداردها و فناوری ایالات متحده آمریکا
۴۷۱	❖ آزمایشگاه‌های صدور گواهی
۴۷۱	○ آزمایشگاه تضمین مرکز مهندسی نرم‌افزار
۴۷۲	○ سایک (مؤسسه بین‌المللی کاربردهای علم)
۴۷۲	○ آزمایشگاه‌های انجمن بین‌المللی امنیت رایانه
۴۷۳	❖ مدل بلوغ ظرفیت مهندسی امنیت سیستم‌ها
۴۷۶	❖ ارزش صدور گواهی
۴۷۷	○ وقتی که صدور گواهی اهمیت دارد
۴۷۸	○ وقتی که صدور گواهی اهمیتی ندارد
۴۷۸	❖ انواع گواهی‌ها
۴۷۸	○ معیارهای مشترک
۴۷۹	○ آزمون سازگاری و امنیت کارت هوشمند
۴۸۰	○ پرداخت اروپایی، کارت هوشمند و ویزا
۴۸۰	■ کارت اعتباری/ پدهی هوشمند و ویزا
۴۸۱	■ کارت هوشمند/ پردازنده
۴۸۱	○ مدل ترکیبی پلت‌فرم جهانی
۴۸۲	○ سایر معیارهای ارزیابی
۴۸۴	○ آژانس امنیت ملی آمریکا
۴۸۵	○ گواهی‌نامه شماره ۱۴۰

۴۸۸ علائم اختصاری

۵۰۷ منابع