انتشارات امیدان روز

امنیت تجارت الکترونیکی

دکتر عرب‌سرخی
(عضو هیات علمی پژوهشگاه ارتباطات و فناوری اطلاعات)
مینو غریبی سبیل
رقیه قربانلو

سرشناسه :	عرب‌سرخی، ابوذر، ۱۳۶۰ -
عنوان و نام پدیدآور :	امنیت تجارت‌الکترونیکی/ابوذر عرب‌سرخی، مینو غریبی‌سبیل، رقیه قربانلو.
مشخصات نشر :	تهران: ادیبان روز،۱۳۹۶.
مشخصات ظاهری :	۵۱۲ ص.
شابک :	۹۷۸-۶۰۰-۸۱۹۰-۲۳-۳
وضعیت فهرست نویسی :	فیپا
موضوع :	بازرگانی الکترونیکی -- تدابیر ایمنی
موضوع :	Electronic commerce -- Security measures
شناسه افزوده :	غریبی سبیل، مینو، ۱۳۶۶ -
شناسه افزوده :	قربانلو، رقیه، ۱۳۶۶ -
رده بندی کنگره :	۱۳۹۶ ۸الف۳۶ع/HF۵۵۴۸/۳۲
رده بندی دیویی :	۶۵۸/۸۷۲
شماره کتابشناسی ملی :	۴۳۷۵۵۵۱

مؤلفین :	ابوذر عرب‌سرخی - مینو غریبی سبیل - رقیه قربانلو
گرافیست و صفحه آرا :	مرتضی عبّاده پناه
طراح جلد :	حمید رضا شاکل
شمارگان :	۱۰۰۰
قیمت :	۳۹۰۰۰ تومان
شابک :	۹۷۸-۶۰۰-۸۱۹۰-۲۳-۳
تاریخ انتشار :	۹۶
نوبت چاپ:	اول
چاپ و صحافی:	طوس

تلفن : ۶۶۹۵۶۸۱۲-۱۵

خرید اینترنتی از طریق:

www.adibanbook.com

www.adibanbook.ir

انتشارات ادیبان روز

پیشگفتار

امروزه بسیاری 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 منحصربه‌فردی که دارد بسیاری از کاربران را به‌سمت خود جذب نموده‌است لیکن فضای سایبر و وب بهترین محل برای دسترسی مهاجم به تمام چیزهایی است که کاربر را مجاب به حضور در این فضا نموده‌است. در واقع، اگرچه فضای سایبر به‌عنوان یک توانمندساز در دنیای کسب‌وکار 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 داشته‌باشیم خواهیم دید که توسعه فضای سایبر به‌واسطه افزایش دامنه کاربران آن و به تبع آن، افزایش روزافزون حجم سرمایه‌گذاری در چنین محیطی است.

بخش قابل‌توجهی از این سرمایه‌گذاری در حوزه تجارت‌الکترونیکی انجام می‌شود؛ جایی‌که سازمان با ارائه مجموعه‌ای از کالاها و خدمات به‌دنبال کسب منفعت از جانب مشتریان خود است. وجود پول و گردش مالی در چنین فضایی انگیزه‌های مهاجم برای دستیابی 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 تجارت‌الکترونیکی 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 تجارت‌الکترونیکی دارند؛ بدین

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

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

ابوذر عرب‌سرخی

زمستان ۱۳۹۵

مقدمه‌ای بر کتاب امنیت تجارت‌الکترونیکی

امروز خدمات و فعالیت‌های تجارت‌الکترونیکی به معنای واقعی کلمه فراگیر شده‌اند به‌گونه‌ای 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. تجارت‌الکترونیکی در دنیای امروز چیزی جدا از زندگی و کار افراد نیست بلکه یکی از الزام‌های چنین فضایی محسوب می‌شود. دلیل این امر به‌واسطه توسعه تجهیزات کاربری و فن‌آوری‌های ارتباطی و اطلاعاتی قابل‌حملی است که خدمات تجارت‌الکترونیکی 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 دیجیتالی شده‌اند اما تهدیدهای امنیتی خاص خود را نیز به این فضا وارد نموده‌اند. به‌هرحال، درک دغدغه‌های امنیتی تجارت‌الکترونیکی و حرکت درست در این فضا مستلزم توجه به کلیه سیستم‌ها، زیرسیستم‌ها و فعالیت‌های رایج در این حوزه است.

تأمین امنیت در فضای تجارت‌الکترونیکی از نگاه دو دیدگاه 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 به‌گونه‌ای طراحی شوند که عملکرد درست سیستم را تضمین نمایند. مالک سیستم تجارت‌الکترونیکی نگاه متفاوتی دارد. از منظر وی امنیت بر آن چیزی تمرکز دارد که وجهه کسب‌وکار را ارتقاء و اعتماد مشتری 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 ارائه‌دهد. 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 تجارت‌الکترونیکی کتاب حاضر به معرفی اصول، سازوکارها و معیارهایی می‌پردازد که عمده آن‌ها به‌شرح زیر هستند:

- توجه به کاربر باید در اولویت همه امور تجارت‌الکترونیکی قرار گیرد. شما به‌عنوان 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، محکوم به شکست است.
- شما در این کتاب خواهید آموخت که چگونه وب‌سایت و زیرساخت تجارت‌الکترونیکی 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 تأمین امنیت در فضای تجارت‌الکترونیکی موضوع مقیاس‌پذیری زیرساخت‌ها و خدمات است. در این کتاب شما براساس رویکردهای مبتنی بر تحلیل مخاطره نحوه طراحی و استقرار چنین زیرساختی را خواهید آموخت.
- دسترس‌پذیری بالا یکی از الزام‌های اساسی در حوزه تجارت‌الکترونیکی است. براین اساس، شما خواهید آموخت که چگونه سیستم‌های تجارت‌الکترونیکی خود را توسعه‌دهید به‌گونه‌ای که توان مدیریت حجم بالای درخواست‌های مشتریان را داشته باشد.
- مواجهه کارآمد با تهدیدهای امنیتی مستلزم شناسایی آسیب‌پذیری‌های سیستم‌های تجارت‌الکترونیکی 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 تجارت‌الکترونیکی رفتاری مناسب جهت مواجهه با ملاحظات امنیتی این فضا داشته‌باشد.

درک بهتر ساختار و محتوای کتاب حاضر مستلزم نگاهی اجمالی به مواردی است که در قالب فصول مختلف مطرح شده‌است. 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 دیجیتالی)، 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 به نوع جدید تجارت‌الکترونیکی یعنی تجارت سیّار پرداخته می‌شود. در این راستا، نحوه شکل‌گیری و تحاما تجارت سیّار و چگونگی ایفای نقش تجهیزات الکترونیکی کاربر در این فضا ترسیم شده‌است. در واقع، فصل دوم به مرور تجهیزات و زیرساخت‌هایی می‌پردازد که نقشی حیاتی را در توسعه تجارت سیّار ایفا می‌کنند.

فصل سوم: این فصل به تبیین قابلیت‌هایی می‌پردازد که عامل موفقیت یا شکست خدمات و سیستم‌های تجارت‌الکترونیکی محسوب می‌شوند. ارکان امنیت (صحت، دسترس‌پذیری و محرمانگی)، قابلیت‌های توسعه‌پذیری، تحمل خطا و تعامل‌پذیری و نیز قابلیت‌های تسهیم و عملیاتی‌شدن همگی از خصیصه‌هایی هستند که در توسعه سیستم‌های تجارت‌الکترونیکی پیش‌بینی و عملیاتی شوند. تعریف، انواع و ابعاد هریک از این قابلیت‌ها و نقش آن‌ها در توسعه کاربری سیستم‌های تجارت‌الکترونیکی 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 تجارت‌الکترونیکی می‌پردازد. رویکردهای مختلف امن‌سازی این فضا با محوریت تحلیل مخاطره در فصل چهارم تشریح می‌شود. علاوه براین، به موضوع قابلیت استفاده از سیستم و تأثیر امنیت بر آن پرداخته می‌شود. این مطالب برای طرح موضوع مقیاس‌پذیر

نمودن امنیت به‌کار 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 کنترل‌دسترسی 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 سازنده امنیت تجارت‌الکترونیکی در قالب این فصل تشریح گردیده‌اند. مواردی همچون احراز هویت، تفویض اختیار، عدم‌انکار، امنیت ارتباطات و محرمانگی از الزام‌های امنیتی یک وب‌سایت تجارت‌الکترونیکی محسوب می‌شوند که تأمین آن‌ها مستلزم به‌کارگیری یک یا مجموعه‌ای از خدمات است که عموماً با همین نام و تحت‌عنوان مؤلفه‌های امنیتی سیستم شناخته می‌شوند. در کنار این موارد، مبانی خط‌مشی‌های امنیتی و برخی از اصول (نظیر اصل حداقل‌دسترسی و ممیزی امنیت) و استراتژی‌های امنیتی رایج (نظیر دفاع در عمق و جداسازی) در قالب این فصل معرفی‌شده 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. این‌کار 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 پویش 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 تجارت‌الکترونیکی انجام‌شده 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: تضمین کارآمدی تصمیم‌ها و اقدام‌های امنیتی در فضای تجارت‌الکترونیکی مستلزم وارسی آن‌ها در قالب یک فرآیند رسمی صدورگواهی و اعتباردهی است که این موارد در قالب فصل نهم کتاب تبیین می‌شوند. در این فصل، مجموعه‌ای از روش‌ها، استانداردها، تکنیک‌ها و سازوکارهای تضمین و صدور گواهی حرفی‌شده و حوزه کاربرد و کارکردهای هریک از آن‌ها تبیین می‌شود.

محتوای ارائه‌شده در این کتاب برای گستره وسیعی از ذی‌نفعان سازمانی و امنیتی مفید خواهد بود. این فرد ممکن است مالک سیستم، توسعه‌دهنده سیستم، معمار سیستم، معمار امنیت، مهندس نرم‌افزار، مدیر پروژه امنیت، تحلیل‌گر امنیت، کنسول فنی سیستم، مدیر فنی و یا حتی مسئول تدوین استراتژی‌های شرکت باشد.

براساس آنچه در بخش قبلی پیشگفتار بدان اشاره‌شد، محتوای فصول کتاب را می‌توان در دو محور مبانی تجارت‌الکترونیکی و مبانی امنیت تجارت‌الکترونیکی 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 تجارت‌الکترونیکی براساس نیاز کاری خود می‌توانند به بخش‌های خاصی از این کتاب رجوع نمایند.