

به نام خدا



معماری امنیت اطلاعات

سیستم مدیریت امنیت اطلاعات

مؤلف:

مهندس علی ثاقب موفق



هرگونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

عنوان کتاب: معماری امنیت اطلاعات سیستم مدیریت امنیت اطلاعات

مؤلف: مهندس علیرضا ثاقب موفق

ناشر: موسسه فرهنگی رز دبیر گران تهران

صفحه آرای: فرنوش عبدالمی

طراح جلد: داریوش فرسای

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۹

چاپ و صحافی: صدف

تیراژ: ۱۰۰۰ جلد

قیمت: ۴۰۰۰۰۰ ریال

شابک: ۹۷۸-۶۲۲-۲۱۸-۳۰۵-۹

نشانی واحد فروش: تهران، میدان انقلاب،

خیابان کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۰۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibbook.ir

www.dibagarantehran.com

نشانی تلگرام: @mftbook

نشانی اینستاگرام: dibagaran_publishing

هر کتاب دیباگران، یک فرصت جدید شغلی.

هرگوشی همراه، یک فروشگاه کتاب دیباگران تهران.

از طریق سایتهای و اپ دیباگران، در هر جای ایران به کتابهای ما دسترسی دارید.

سرشناسه: ثاقب موفق، علی، ۱۳۳۸-

عنوان و نام پدیدآور: معماری امنیت اطلاعات-سیستم

مدیریت امنیت اطلاعات / مؤلف: علی ثاقب موفق.

مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۹

مشخصات ظاهری: ۱۳۸ص: مصور.

شابک: ۹۷۸-۶۲۲-۲۱۸-۳۰۵-۹

وضعیت فهرست نویسی: فیا

موضوع: کتاب: ترها-ایمنی اطلاعات-مدیریت

موضوع: computer security-management

موضوع: مراکز داده پردازش-تدابیر ایمنی

موضوع: electronic data processing

موضوع: department security measures

موضوع: شبکه های کامپیوتری-تدابیر ایمنی

موضوع: computer network security measures

رده بندی کنگره: QA ۷۶/۹

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۶۱۵۶۸۷۳

فهرست مطالب

۸	فصل اول / مدیریت امنیت اطلاعات
۹	معماری امنیت شبکه
۹	مدیریت دارایی‌ها
۱۰	کنترل دسترسی
۱۱	تفکیک وظایف
۱۴	ثبت فعالیت‌های کاربران و ابزارهای سیستم
۱۶	مدیریت تغییرات
۱۸	مدیریت تغییرات در خدمات اشخاص ثالث
۲۰	مدیریت رسانه‌های ذخیره‌سازی اطلاعات
۲۲	مدیریت ظرفیت
۲۵	فصل دوم / امنیت فیزیکی تجهیزات رایانه‌ای
۲۶	امنیت فیزیکی پیرامونی
۲۸	امنیت کابل‌کشی
۳۳	رسانه‌های ذخیره‌سازی فیزیکی حین حمل و نقل
۳۴	حفاظت در مقابل تهدیدهای محیطی و خارجی
۳۷	جداسازی تجهیزات آزمایشی از عملیاتی
۳۹	خروج دارایی
۴۱	دسترسی عمومی، نواحی ارسال و بارگیری
۴۳	کار در نواحی امن
۴۵	کنترل فیزیکی ورودی‌ها
۴۷	نگهداری تجهیزات
۵۰	امنیت تجهیزات خارج از ابنیه

۵۲	خارج از رده سازی و استفاده مجدد
۵۳	استقرار و حفاظت تجهیزات
۵۵	امکانات پشتیبانی
۵۸	فصل سوم / امنیت مستندات و شواهد
۵۹	امنیت مستندات سیستم
۶۱	تهیه نسخه پشتیبان اطلاعات
۶۲	جمع آوری شواهد و مدارک
۶۴	حفاظت از اطلاعات ثبت شده وقایع
۶۶	سیاست گذاری مدیریت حوادث امنیت اطلاعات
۶۸	گزارش ضعف های امنیت اطلاعات
۷۰	مسئولیت ها و روش های اجرایی مدیریت بحران
۷۲	یادگیری از حوادث امنیت اطلاعات
۷۵	فصل چهارم / امنیت اطلاعات و سرویس
۷۶	اطلاعات در دسترس عموم
۷۷	امحای رسانه های ذخیره سازی
۷۹	امنیت سرویس های شبکه
۸۴	امنیت سیستم های اطلاعاتی کاربردی
۸۷	امنیت سیستم های الکترونیک دفتری
۸۹	پایش کاربرد سیستم ها
۹۱	پایش و بازنگری خدمات شخص ثالث
۹۳	پذیرش سیستم
۹۵	امن سازی دفاتر، اتاق ها و امکانات
۹۸	فصل پنجم / امنیت تجارت الکترونیک
۹۹	تجارت الکترونیک
۱۰۱	تحويل خدمت
۱۰۳	توافق نامه های تبادل

۱۰۵	خط‌مشی‌ها و روش‌های اجرایی تبادل اطلاعات
۱۰۷	داد و ستدهای برخط (متصل و مستقیم)
۱۱۰	روش‌های اجرایی مدیریت و نگهداری اطلاعات
۱۱۲	رویه‌های عملیاتی مستند
۱۱۴	فصل ششم / امنیت در کدهای برنامه‌نویسی شبکه‌ای
۱۱۵	کنترل کدهای سیار
۱۱۷	کنترل کدهای مخرب
۱۲۰	کنترل‌های شبکه
۱۲۵	واقع‌نگاری خیابانی
۱۲۶	واقع‌نگاری ممیزی
۱۲۹	همزمان‌سازی سازه‌ها
۱۳۲	فصل هفتم / مدل‌ها و استانداردهای امنیت اطلاعات
۱۳۳	مدل‌ها و استانداردهای امنیت اطلاعات
۱۳۳	تعریف مدل‌ها و استانداردهای امنیت شبکه
۱۳۴	انواع استانداردهای امنیت
۱۳۶	تهدیدات امنیتی
۱۳۷	ایجاد سیستم مدیریت امنیت اطلاعات

❖ مقدمه مولف

امروزه با افزایش حجم اطلاعات قابل تبادل و از طرفی گسترش روزافزون استفاده از شبکه‌ها، به‌خصوص شبکه‌های کامپیوتری و همچنین ایجاد شبکه‌های جهانی، چالش بزرگی برای صاحبان اطلاعات به لحاظ تهدیدات امنیتی این حوزه به وجود آمده که به مثابه زنگ خطری برای تمامی افراد و کاربران است.

در حال حاضر سرقت دانش و اطلاعاتی که برای آن هزینه و وقت زیادی صرف شده، یکی از خطرات بالقوه در شبکه‌های کامپیوتری است. متأسفانه این خطرات از طریق افرادی تحمیل می‌شود که باهوش‌تر از دیگر افراد هستند و قدرت نفوذ و ضربه به شبکه را دارند.

تهدیدهای تازه برای امنیت شبکه‌های کامپیوتری، به صورت عمده شامل افزایش غیرمجاز اطلاعات، قطع ارتباط و اختلال در شبکه، سر و دستکاری غیرمجاز اطلاعات و... است. یکی از مهم‌ترین مؤلفه‌های ایجاد سیستم امنیت شبکه، ارائه سیاست‌ری در این خصوص است.

در واقع خط‌مشی یا سیاست‌گذاری برای حفظ امنیت شبکه، انتظارات یک سازمان به‌منظور ایجاد امنیت در شبکه‌های مختلف آن سازمان را، تعریف و در عین حال روند پیشگیری از حوادث امنیتی شبکه را مشخص می‌کند. تعیین خط‌مشی امنیت در شبکه بنیان اساس امنیت شبکه است، زیرا دارایی‌ها و سرمایه‌های اصلی یک شبکه و سازمان که باید در امان باشند، با این خامش مشخص می‌شود.

سیاست‌گذاری در قالب مؤلفه‌هایی چون تحلیل تهدیدات امنیتی، تحلیل آسیب‌پذیری‌ها، سیاست‌گذاری امنیتی در خصوص محافظت از دارایی‌های اطلاعاتی، تجهیز و... صورت می‌گیرد. امروزه ناگزیر امنیت ملی و اقتدار سیاسی و اقتصادی به‌صورت پیچیده‌ای به امنیت اطلاعات گره خورده است و نه تنها دولت‌ها، بلکه تک‌تک افراد را نیز تهدید می‌کند.

از طرفی از آنجا که شبکه‌های نسل جدید تقریباً از تمامی امکانات مخابراتی، سرویس‌های یکپارچه و مجتمع استفاده کرده و با به‌کارگیری پروتکل‌های مختلف انواع سرویس‌های مورد نظر مشترک را ارائه می‌کنند، از این‌رو ضروری است برای پیاده‌سازی این نوع فناوری‌ها نیز دقت و هشیاری از دیدگاه امنیت مورد توجه قرار گیرد.