به نام خدا

معماری امنیت اطلاعات

سیستم مدیریت امنیت اطلاعات

مؤلف:

مهندس علی ثاقب موفق

موسسه فرهنگی هنری دیباگران تهران

عنوان کتاب:

معماری امنیت اطلاعات
سیستم مدیریت امنیت اطلاعات

مولف : مهندس علی ثاقب موفق

ناشر: موسسه فرهنگی هنری دیباگران تهران

صفحه آرایی:فرنوش عبدالهی

طراح جلد:داریوش فرسایی

نوبت چاپ: اول

تاریخ نشر: ۱۳۹۹

چاپ و صحافی:صدف

تیراژ:۱۰۰ جلد

قیمت:۴۰۰۰۰۰ ریال

شابک: ۹-۳۰۵-۲۱۸-۶۲۲-۹۷۸

نشانی واحد فروش: تهران، میدان انقلاب، خ کارگر جنوبی، روبروی پاساژ مهستان، پلاک ۱۲۵۱

تلفن: ۶۶۴۱۰۰۴۶-۲۲۰۸۵۱۱۱

فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibbook.ir

www.dibagarantehran.com

نشانی تلگرام:@mftbook نشانی اینستاگرام دیبا dibagaran_publishing

سرشناسه:ثاقب موفق،علی،۱۳۴۸-

عنوان و نام پدیدآور:معماری امنیت اطلاعات-سیستم مدیریت امنیت اطلاعات/مولف:علی ثاقب موفق.

مشخصات نشر: تهران : دیباگران تهران :۱۳۹۹

مشخصات ظاهری:۱۳۸ص:مصور،

شابک: ۹-۳۰۵-۲۱۸-۶۲۲-۹۷۸

وضعیت فهرست نویسی: فیپا

موضوع:کامپیوترها-ایمنی اطلاعات-مدیریت

موضوع:computer security-management

موضوع:مراکز داده پردازش-تدابیر ایمنی

موضوع: electronic data processing departments security measures

موضوع: شبکه های کامپیوتری-تدابیر ایمنی

موضوع:computer networks-security measures

رده بندی کنگره:QA ۷۶/۹

رده بندی دیویی:۰۰۵/۸

شماره کتابشناسی ملی:۶۱۵۶۸۷۳

فهرست مطالب

❖ مقدمه‌مولف

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 موجود برای امنیت شبکه‌های کامپیوتری، به صورت عمده شامل افشای غیرمجاز اطلاعات، قطع ارتباط و اختلال در شبکه، تغییر و دستکاری غیرمجاز اطلاعات و... است. یکی از مهم‌ترین مؤلفه‌های ایجاد سیستم امنیت شبکه، ارائه سیاست‌گذاری 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 و اساس امنیت شبکه است، زیرا دارایی‌ها و سرمایه‌های اصلی یک شبکه و سازمان که باید در امان باشند، با این خط‌مشی مشخص می‌شود.

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

از طرفی از آنجا که شبکه‌های نسل جدید تقریباً از تمامی امکانات مخابراتی به صورت 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.