دفاع در عمق

مبتنی بر پیاده‌سازی استاندارد سیستم مدیریت امنیت اطلاعات

تالیف:

مهندس علی نایب پور

مهندس علیرضا صاحب‌جمعی

سرشناسه	: نایب پور، علی، ۱۳۶۵.
عنوان و نام پدیدآور	: دفاع در عمق مبتنی بر پیاده سازی استاندارد سیستم مدیریت امنیت اطلاعات تالیف علی نایب پور، علیرضا صاحب جمعی
مشخصات نشر	: تهران : ناقوس ، ۱۴۰۱.
مشخصات ظاهری	: ۴۹۸ص.: مصور ، جدول
شابک نسخه چاپی	: 978-600-473-453-0 : ۱،۵۰۰،۰۰۰ریال
وضعیت فهرست‌نویسی	: فیپا
یادداشت	: کتابنامه: ص . ۴۹۵- ۴۹۶ .
موضوع	: کامپیوترها – ایمنی اطلاعات — مدیریت
موضوع	: Computer security – Management
موضوع	: کامپیوترها – ایمنی اطلاعات – تدابیر ایمنی
موضوع	: Computer security – Measures
موضوع	: کامپیوترها – ایمنی اطلاعات – مدیریت — استانداردها
موضوع	: Computer security–Manage ment – Standards
موضوع	: کامپیوترها – کنترل دستیابی
موضوع	: Computer – Access control
موضوع	: کامپیوترها — کنترل دستیابی — رمزگان
موضوع	: Computers – Access control – Code words
شناسه افزوده	: صاحب جمعی ، علیرضا ، ۱۳۵۶.
رده بندی کنگره	: QA۷۶/۹
رده بندی دیویی	: ۰۰۵/۸
شماره کتابشناسی ملی	: ۸۸۱۲۱۷۱

انتشارات ناقوس

نام کتاب	: دفاع در عمق مبتنی بر پیاده سازی استاندارد سیستم مدیریت امنیت اطلاعات
ناشر	: انتشارات ناقوس
مولفین	: مهندس علی نایب پور ، مهندس علیرضا صاحب جمعی
چاپ اول	: ۱۴۰۱
تیراژ	: ۵۰۰ جلد
چاپ و صحافی	: نقشینه
ناظر چاپ	: یاسمن تجلی محدث
قیمت	: ۱،۵۰۰،۰۰۰ریال
شابک	: ۰- ۴۵۳ - ۴۷۳-۶۰۰- ۹۷۸
ISBN	: 978 – 600 – 473- 453- 0

انتشارات ناقوس
خیابان انقلاب ابتدای وصال شیرازی ساختمان شماره ۷ طبقه اول
تلفاکس : ۶۶۴۷۸۹۵۸ - ۶۶۴۷۸۹۵۷ - ۶۶۹۶۵۳۹۱

فهرست مطالب

فصل چهارم: رویکرد دفاع در عمق مبتنی بر پیاده‌سازی سیستم مدیریت امنیت اطلاعات

فصل پنجم: پیاده‌سازی استراتژی دفاع در عمق در لایه امنیت فیزیکی و محیطی

فصل ششم: پیاده‌سازی استراتژی دفاع در عمق در لایه امنیت عملیات

فصل هفتم: پیاده‌سازی استراتژی دفاع در عمق در لایه مدیریت امنیت

پیش گفتار

رشد و گسترش روزافزون فناوری اطلاعات، انقلابی را در ابعاد مختلف زندگی انسان‌ها و عملکرد سازمان‌ها ایجاد کرده است. امروزه داده‌های بسیار ارزشمندی توسط زیرساخت‌های اطلاعاتی سازمان‌های دولتی، شرکت‌های خصوصی و همچنین مراکز عمومی میزبانی می‌شود. علاوه براین، بسیاری از مراکز داده خدماتی را به مشتریان و کاربرهای خود ارائه می کنند که توقف هرچند کوتاه مدت ارائه خدمات، خسارت سنگین مالی و اعتباری به همراه دارد و این خسارت‌ها می‌تواند شامل از دست‌دادن داده‌های ارزشمند، مشتریان و اعتبار سازمان باشد. بنابراین کسب آمادگی کافی جهت مقابله یا اتخاذ تصمیم‌های مناسب در مقابل حوادث، جرائم سایبری، اختلال‌های ناشی از تغییرات و غیره، رهیافتی اجتناب‌ناپذیر برای تضمین تداوم کسب‌وکار است. لذا امن‌سازی شبکه و سیستم‌های اطلاعاتی به یکی از مسائل مهم پیش رو و دغدغه‌های مدیرهای امنیت و فناوری اطلاعات سازمان‌ها تبدیل شده است و مهم‌ترین اقدام در راستای امن‌سازی یک سازمان، ایجاد یک چارچوب قدرتمند جهت مدیریت اقدام‌های امنیتی است و باید اذعان داشت که فرآیند امن‌سازی سازمان بدون لحاظ نمودن مسائل مدیریت امنیت و بسط و گسترش آن در سطح تمامی بخش‌های حساس و استراتژیک سازمان امکان‌پذیر نمی‌باشد.

سیستم مدیریت امنیت اطلاعات یا «ISMS» باهدف تبیین شفاف راهکارهای امن‌سازی، به منظور مدیریت مخاطره‌های امنیت اطلاعات سازمان‌ها در چارچوب مجموعه مخاطره‌های کسب‌وکار و با عنوان ارزیابی، راهبری و پشتیبانی امنیت فناوری اطلاعات درون‌سازمانی و برون‌سازمانی در یک سطح مورد توافق مطرح شده است و مجموعه‌ای از سیاست‌ها، اهداف، استراتژی‌ها، مستندات شناخت و ارزیابی مخاطرات، دستورالعمل‌های سیستمی و غیره را شامل می‌شود که متناسب با اندازه و زمینه کاری سازمان طراحی و پیاده سازی می‌شود.

استراتژی دفاع در عمق یا «DID» در حوزه امنیت سایبری، استفاده هماهنگ از اقدامات متقابل امنیتی چندگانه به منظور دفاع از تمامیت دارایی‌های اطلاعاتی در یک سازمان در برابر مهاجم‌های سایبری است. دفاع در عمق می‌تواند ساختار امنیتی سازمان را به طور قابل‌توجهی بهبود بخشد. از سویی پیاده‌سازی استاندارد سیستم مدیریت امنیت اطلاعات، امکان پیاده‌سازی امنیت لایه‌ای مبتنی بر استراتژی دفاع در عمق را فراهم می کند.