

۴۲۸۹۷۵۱

دفاع در عمق

مبثنی بر پیاده‌سازی استاندارد سیستم مدیریت امنیت اطلاعات

www.ketab.ir

تالیف:

مهندس علی نایب پور

مهندس علیرضا صاحب جمعی

سرشناسه	: نایب پور، علی، ۱۳۶۵.
عنوان و نام پدیدآور	: دفاع در عمق مبتنی بر پیاده سازی استاندارد سیستم مدیریت امنیت اطلاعات
مشخصات نشر	: تهران: ناخوس، ۱۴۰۱.
مشخصات ظاهری	: ۴۹۸ص: مصور، جدول
شابک نسخه چاپی	: 978-600-473-453-0 : ۵۰۰,۰۰۰ ریال
وضعیت فهرست نویسی: فیا	
یادداشت	: کتابنامه: ص. ۳۹۵-۴۹۶.
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-Management - 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



**NAGHOOS
PUBLICATION**

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghooospress.ir

انتشارات ناخوس

نام کتاب	: دفاع در عمق مبتنی بر پیاده سازی استاندارد سیستم مدیریت امنیت اطلاعات
ناشر	: انتشارات ناخوس
مؤلفین	: مهندس علی نایب پور، مهندس علیرضا صاحب جمعی
چاپ اول	: ۱۴۰۱
تیراژ	: ۵۰۰ جلد
چاپ و صحافی	: نقشبند
ناظر چاپ	: یاسمن تجملی محدث
قیمت	: ۵۰۰,۰۰۰ ریال
شابک	: ۹۷۸-۶۰۰-۴۷۳-۲۵۳-۰
ISBN	: 978-600-473-453-0

کلیه حقوق برای سرمایه گذار محفوظ است. تکثیر تمامی یا قسمتی از این اثر به صورت حرفه چینی یا چاپ مجدد چاپ المست. پلی کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

انتشارات ناخوس

خیابان انقلاب ابتدای وصال شیرازی ساختمان شماره ۷ طبقه اول

تلفاکس: ۶۶۴۷۸۹۵۸ - ۶۶۴۷۸۹۵۷ - ۶۶۹۶۵۳۹۱

فهرست مطالب

پیشگفتار.....	۲۱
---------------	----

فصل اول: مقدمه و ضرورت امنیت اطلاعات

۱.۱. فضای سایبری.....	۲۳
۲.۱. امنیت سایبری.....	۲۴
۳.۱. تهدیدها و حمله‌های سایبری.....	۳۴
۱.۳.۱. تهدیدهای امنیت سایبری.....	۳۵
۲.۳.۱. حمله‌های امنیت سایبری.....	۳۸
۴.۱. مدیریت امنیت سایبری، سرویس‌ها و تجهیزات امنیت سایبری.....	۵۳
۱.۴.۱. مدیریت امنیت سایبری.....	۵۴
۲.۴.۱. سرویس‌ها و تجهیزات امنیت سایبری.....	۵۹
۱.۲.۴.۱. سرویس‌های امنیت سایبری.....	۶۰
۲.۲.۴.۱. مکانیزم‌ها و تجهیزات امنیت سایبری.....	۶۱
۳.۲.۴.۱. تجهیزات امنیت سایبری.....	۶۲

فصل دوم: استراتژی دفاع در عمق

۱.۲. مفهوم دفاع در عمق.....	۷۳
۲.۲. اصول پیاده‌سازی استراتژی دفاع در عمق در امنیت سایبری.....	۷۷
۳.۲. ساختار استراتژی دفاع در عمق.....	۸۰
۴.۲. مروری بر رویکردهای موجود.....	۱۱۷

فصل سوم: استاندارد سیستم مدیریت امنیت اطلاعات

۱.۳. مقدمه‌ای از سیستم مدیریت امنیت اطلاعات.....	۱۲۴
۲.۳. خانواده استاندارد ISO 27000.....	۱۲۵
۳.۳. پیاده‌سازی سیستم مدیریت امنیت اطلاعات.....	۱۳۷
۴.۳. استاندارد مورد کاربرد در مدل دفاع در عمق.....	۱۴۵

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

۱. معماری چهار لایه دفاع در عمق..... ۱۵۰
۲. بررسی معماری امنیتی چهار لایه..... ۱۵۳
- ۱،۲،۴. پیاده‌سازی استراتژی دفاع در عمق در لایه امنیت فیزیکی و محیطی..... ۱۵۳
- ۲،۲،۴. پیاده‌سازی استراتژی دفاع در عمق در لایه امنیت عملیات..... ۱۵۵
- ۳،۲،۴. پیاده‌سازی استراتژی دفاع در عمق در لایه مدیریت امنیت..... ۱۵۷
- ۴،۲،۴. پیاده‌سازی استراتژی دفاع در عمق در لایه حاکمیت امنیت..... ۱۵۹

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

۱. لایه امنیت فیزیکی و محیطی در یک نگاه..... ۱۶۰
۲. نواحی امن در لایه امنیت فیزیکی..... ۱۶۲
- ۱،۲،۵. زیرساخت فیزیکی امنیت در لایه امنیت فیزیکی و محیطی..... ۱۶۲
- ۱،۱،۲،۵. مرکز عملیات شبکه..... ۱۶۳
- ۱،۱،۱،۲،۵. ساختار مرکز عملیات شبکه..... ۱۶۴
- ۲،۱،۱،۲،۵. ابزارهای مرکز عملیات شبکه..... ۱۶۶
- ۲،۱،۲،۵. مرکز عملیات امنیت..... ۱۶۹
- ۱،۲،۱،۲،۵. پیاده‌سازی مرکز عملیات امنیت..... ۱۷۰
- ۲،۲،۱،۲،۵. ویژگی‌های کلیدی مرکز عملیات امنیت..... ۱۷۵
- ۳،۲،۱،۲،۵. سیستم امنیت اطلاعات و مدیریت رخداد..... ۱۷۸
- ۴،۲،۱،۲،۵. مرکز عملیات امنیت نسل آینده..... ۱۸۱
- ۳،۱،۲،۵. حراست فیزیکی..... ۱۸۳
- ۲،۲،۵. محیط‌های امن..... ۱۸۴
- ۱،۲،۲،۵. مرکز داده..... ۱۸۴
- ۱،۱،۲،۲،۵. انواع مراکز داده..... ۱۸۶
- ۲،۱،۲،۲،۵. سیستم‌های مکمل مراکز داده..... ۱۸۸
- ۲،۲،۲،۵. تأسیسات پشتیبانی..... ۱۸۹
- ۳،۱،۲،۲،۵. کنترل‌های فیزیکی..... ۱۹۱

۹۱	۱.۳.۵. نواحی امن.....
۹۲	۱.۱.۳.۵. حصار امنیت فیزیکی.....
۹۴	۲.۱.۳.۵. کنترل‌های ورودی فیزیکی.....
۹۶	۳.۱.۳.۵. امن‌سازی دفاتر، اتاق‌ها و تأسیسات.....
۹۷	۴.۱.۳.۵. محافظت در برابر تهدیدهای بیرونی و محیطی.....
۹۹	۵.۱.۳.۵. کار در نواحی امن.....
۱۰۰	۲.۳.۵. امنیت تجهیزات.....
۱۰۱	۱.۲.۳.۵. استقرار و حفاظت تجهیزات.....
۱۰۲	۲.۲.۳.۵. امکانات پشتیبانی.....
۱۰۳	۳.۲.۳.۵. امنیت کابل‌کشی.....
۱۰۴	۴.۲.۳.۵. نگهداری تجهیزات.....
۱۰۵	۵.۲.۳.۵. امنیت تجهیزات خارج از ابنیه.....
۱۰۶	۶.۲.۳.۵. امحاء یا استفاده مجدد از تجهیزات به صورت امن.....
۱۰۸	۷.۲.۳.۵. میز پاک و صفحه پاک.....
۱۰۹	۸.۲.۳.۵. رسانه‌های ذخیره‌سازی.....
۱۱۲	۹.۲.۳.۵. نظارت بر امنیت فیزیکی.....

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

۱۴	۱.۶. لایه امنیت عملیات در یک نگاه.....
۱۶	۲.۶. الزامات تکنولوژیک در لایه امنیت عملیات.....
۱۶	۱.۲.۶. مدیریت شبکه و نقطه نهایی.....
۱۷	۱.۱.۲.۶. کنترل دسترسی از راه دور.....
۱۹	۲.۱.۲.۶. سنسور و ابزارهای شبکه.....
۲۱	۳.۱.۲.۶. کشف دارایی.....
۲۲	۴.۱.۲.۶. مدیریت وصله.....
۲۳	۵.۱.۲.۶. مدیریت درخواست.....
۲۴	۶.۱.۲.۶. مدیریت پیکربندی.....

۲۲۵	 ۷.۱.۲.۶. آنتی ویروس مدیریت شده و نرم افزار محافظت از بدافزار
۲۲۷	 ۸.۱.۲.۶. پیشگیری از اتلاف/نشت اطلاعات
۲۲۸	 ۹.۱.۲.۶. کنترل دسترسی به شبکه
۲۲۹	 ۱۰.۱.۲.۶. رمزگذاری دیسک
۲۳۰	 ۱۱.۱.۲.۶. دروازه ایمیل امن
۲۳۱	 ۲.۲.۶. مدیریت برنامه کاربردی و داده
۲۳۱	 ۱.۲.۲.۶. مانیتورینگ فعالیت پایگاه داده
۲۳۳	 ۲.۲.۲.۶. محافظت از درگاه API
۲۳۴	 ۳.۲.۲.۶. کنترل کننده تحویل برنامه
۲۳۶	 ۴.۲.۲.۶. برنامه خودکار حفاظت از خود
۲۳۷	 ۵.۲.۲.۶. نظارت بر یکپارچگی و فعالیت فایل
۲۳۸	 ۶.۲.۲.۶. مدیریت بات
۲۳۹	 ۳.۲.۶. مدیریت امنیت
۲۴۰	 ۱.۳.۲.۶. ارزیابی و مدیریت آسیب پذیری
۲۴۲	 ۲.۳.۲.۶. سازمان دهی امنیت، خودکارسازی و پاسخ
۲۴۴	 ۳.۳.۲.۶. آنالیز رفتار موجودیت کاربر
۲۴۶	 ۴.۳.۲.۶. مدیریت دسترسی ویژه
۲۴۸	 ۵.۳.۲.۶. مدیریت حوادث
۲۵۰	 ۶.۳.۲.۶. مانیتورینگ و تشخیص رخداد
۲۵۳	 ۷.۳.۲.۶. هویت به عنوان سرویس
۲۵۶	 ۸.۳.۲.۶. مدیریت هویت
۲۵۷	 ۹.۳.۲.۶. پوشش آسیب پذیری
۲۵۸	 ۱۰.۳.۲.۶. فایروال برنامه کاربردی وب
۲۶۰	 ۱۱.۳.۲.۶. فناوری فریب
۲۶۱	 ۳.۶. کنترل های تکنولوژیک
۲۶۲	 ۱.۳.۶. کنترل های دسترسی

۱،۱،۳،۶	حقوق دسترسی ویژه	۲
۲،۱،۳،۶	احراز هویت امن	۶
۳،۱،۳،۶	محدودسازی دسترسی به اطلاعات	۹
۴،۱،۳،۶	به کارگیری برنامه های کمکی ویژه	۲
۵،۱،۳،۶	دسترسی به کد منبع	۳
۶،۱،۳،۶	ابزارهای نقطه پایانی کاربر	۵
۲،۳،۶	کنترل های عملیات	۷۹
۱،۲،۳،۶	جداسازی محیط توسعه، آزمون و عملیات	۷۹
۲،۲،۳،۶	محافظت در برابر بدافزار	۲۸۱
۳،۲،۳،۶	ثبت و نظارت بر فعالیت ها	۲۸۴
۴،۲،۳،۶	بسته های گیری از اطلاعات	۲۸۷
۵،۲،۳،۶	هم زمان سازی ساعت	۲۹۰
۶،۲،۳،۶	نصب نرم افزار در سامانه های عملیاتی	۲۹۱
۷،۲،۳،۶	مدیریت آسیب پذیری های فنی	۲۹۳
۸،۲،۳،۶	مدیریت پیکربندی	۲۹۶
۹،۲،۳،۶	حذف اطلاعات	۲۹۹
۱۰،۲،۳،۶	پنهان سازی اطلاعات	۳۰۲
۱۱،۲،۳،۶	پیشگیری از نشت داده	۳۰۶
۳،۳،۶	کنترل های ارتباطات	۳۰۸
۱،۳،۳،۶	کنترل های شبکه	۳۰۹
۲،۳،۳،۶	امنیت سرویس های شبکه	۳۱۲
۳،۳،۳،۶	تفکیک شبکه ها	۳۱۶
۴،۳،۶	کنترل های توسعه و نگهداری	۳۱۹
۱،۴،۳،۶	الزامات امنیتی برنامه کاربردی	۳۱۹
۲،۴،۳،۶	چرخه عمر توسعه امن	۳۲۳
۳،۴،۳،۶	معماری سیستم و اصول مهندسی نرم افزار امن	۳۲۶

۳۲۸.....	توسعه برون‌سپاری‌شده..... ۴،۴،۳،۶
۳۳۰.....	کد نویسی امن و آزمون امنیت در توسعه و پذیرش..... ۵،۴،۳،۶
۳۳۶.....	محافظت از داده‌ها و سیستم‌ها در آزمون..... ۶،۴،۳،۶
۳۳۷.....	افزودگی امکانات پردازش اطلاعات..... ۷،۴،۳،۶
۳۳۹.....	استفاده از رمزنگاری..... ۸،۴،۳،۶
۳۴۱.....	فیلترگذاری وب..... ۹،۴،۳،۶

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

۳۴۴.....	۱،۷. لایه مدیریت امنیت در یک، نگاه.....
۳۴۶.....	۲،۷. ساختار امنیت در لایه مدیریت امنیت.....
۳۴۶.....	۱،۲،۷. ساختار اجرایی امنیت در لایه مدیریت امنیت.....
۳۴۶.....	۱،۱،۲،۷. مدیر امنیت.....
۳۴۷.....	۲،۱،۲،۷. واحد سیاست‌گذاری امنیت.....
۳۴۷.....	۱،۲،۱،۲،۷. گروه سیستم‌ها و روش‌های امنیت.....
۳۴۸.....	۲،۲،۱،۲،۷. گروه برنامه‌ریزی امنیت.....
۳۴۸.....	۳،۲،۱،۲،۷. گروه ممیزی امنیت.....
۳۴۸.....	۳،۱،۲،۷. واحد زیرساخت امنیت.....
۳۴۸.....	۱،۳،۱،۲،۷. گروه معماری امنیت.....
۳۴۹.....	۲،۳،۱،۲،۷. گروه پشتیبانی امنیت.....
۳۴۹.....	۴،۱،۲،۷. واحد مهندسی امنیت.....
۳۴۹.....	۱،۴،۱،۲،۷. گروه آزمون امنیت.....
۳۵۰.....	۲،۴،۱،۲،۷. گروه امنیت نرم‌افزار و سیستم عامل.....
۳۵۱.....	۳،۴،۱،۲،۷. گروه امنیت پایگاه داده.....
۳۵۱.....	۵،۱،۲،۷. واحد مدیریت رخداد امنیت.....
۳۵۲.....	۶،۱،۲،۷. واحد مرکز عملیات امنیت.....
۳۵۳.....	۷،۱،۲،۷. واحد مدیریت ریسک.....
۳۵۴.....	۲،۲،۷. ساختار مدیریتی امنیت 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 بر این، بسیاری از مراکز داده خدماتی را به مشتریان و کاربرهای خود ارائه می‌کنند که توقف هرچند کوتاه مدت ارائه خدمات، خسارت سنگین مالی و اعتباری به همراه دارد و این خسارت‌ها می‌تواند شامل از دست دادن 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 کسب و کار 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 کسب و کار 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 قابل توجهی بهبود بخشد. از سویی پیاده‌سازی استاندارد سیستم مدیریت امنیت اطلاعات، امکان پیاده‌سازی امنیت لایه‌ای مبتنی بر استراتژی دفاع در عمق را فراهم می‌کند.