

امنیت در فناوری اطلاعات

عبدالله بن منشی

محمد یوسف زاده

بهار ۱۳۹۳

سرشناسه	: طحان منش، علیرضا ۱۳۵۶-
عنوان و نام پدیدآور	: امنیت در فناوری اطلاعات/علیرضا طحان منش، محمد یوسف زاده
مشخصات نشر	: تهران: دانشکده علوم و فنون فارابی ۱۳۹۲.
مشخصات ظاهری	: ۲۲۳ ص، مصور.
شابک	: ۹۷۸-۶۰۰-۶۰۲۸-۱۹-۴
قیمت	: ۱۴۰۰۰۰ ریال
وضعیت فهرست نویسی:	فیا
موضوع	: شبکه های کامپیوتری - اقدامات تأمینی
موضوع	: تکنولوژی اطلاعات - اقدامات تأمینی
موضوع	: کامپیوترها - تأمین ضلعات
نسخه افزوده	: یوسف زاده، محمد. ۱۳۶۰-
نسخه افزوده	: دانشکده علوم و فنون فارابی، معاونت پژوهش
رده بندی کتبی	: ۸ الف ۳ ط/TK۵۱۰۵/۵۹
رده بندی دیسی	: 005/8
شماره کتابشناسی	: ۲۱۷۰۷



انتشارات شبکه فارابی

نام کتاب: امنیت در فناوری اطلاعات

تدوین: علیرضا طحان منش - محمد یوسف زاده

ویراستار علمی: سیروس بیرانوند - مهرداد زالی

ویراستار ادبی: عقیل توسلی

مدیر اجرایی: مجید نصر اصفهانی

طرح جلد: محمد عزیزی

تنظیم: اصغر گازرگر

شمارگان: ۱۰۰۰ جلد

قیمت: ۱۴۰۰۰۰ ریال

نوبت چاپ: اول ۱۳۹۳

❖ کلیه حقوق اعم از چاپ، تکثیر و نسخه برداری برای ناشر محفوظ است. (نقل مطالب با ذکر ماخذ بلامانع است).

تلفن ناشر: ۲۹۹۴۲۶۵۸ صندوق پستی: ۱۹۳۹۵-۴۵۷۳

فهرست مطالب

صفحه	عنوان
ج	فهرست مطالب
صفحه	عنوان
ز	پیشگفتار
۱	فصل اول شبکه‌های رایانه‌ای
۳	مقدمه
۳	سخت‌افزار شبکه
۴	مزایای محیط شبکه
۵	مزایای محیط مستقل
۶	تقسیم‌بندی شبکه‌ها
۱۶	عوامل موثر بر انتقال داده‌ها
۱۹	کارت‌های شبکه (NIC)
۲۰	ارتباط و سامانه‌های اطلاعاتی
۲۱	اینترنت
۲۷	فصل دوم ارتباط رایانه‌ها در ویندوز XP
۲۸	انواع ارتباط بین رایانه‌ها
۳۰	روش‌های ایجاد ارتباط مستقیم بین رایانه‌ها
	نحوه به اشتراک گذاشتن منابع در شبکه‌های نظیر به نظیر
۷۳	برقراری امنیت در شبکه
۷۳	چگونگی فعال کردن دیوار آتش

۷۴	تنظیم امنیت مرورگر اینترنت
۷۵	فصل سوم امنیت شبکه
۷۷	مقدمه
۷۸	تعاریف و مفاهیم
۸۰	اسب‌پذیری شبکه‌های رایانه‌ای
۸۳	چگونگی حمله به سامانه‌های شبکه‌ای
۹۸	سرورها، ابزارها و فنون حمله
۱۰۲	یک شمارش ساده تجاوز
۱۰۵	دفاع از حمله
۱۱۱	کلاس‌های معیار ارزیابی
۱۱۳	کنترل‌های دفاعی
۱۱۴	نکات مهم
۱۱۶	فصل چهارم امنیت در فناوری اطلاعات
۱۱۹	دقت اطلاعات
۱۲۰	طبقه‌بندی اطلاعات
۱۲۰	مدیران و مسایل امنیت و حفاظت اطلاعات رایانه‌ای
۱۲۱	اشتباه‌های متداول مدیران سامانه
۱۲۱	اشتباه‌های مدیران در بحث امنیت فناوری اطلاعات
۱۲۲	وظایف مدیران در رابطه با برقراری امنیت اطلاعات
۱۲۳	اشتباه‌های متداول کاربران معمولی
۱۲۴	راهکارهای بهبود وضعیت امنیتی سامانه‌های اطلاعاتی
۱۲۶	فهرست‌های کنترل مدیریت امنیت

۱۲۹	فصل پنجم راهکارهایی در امنیت رایانه و داده‌ها
۱۳۱	امنیت فیزیکی و حفاظت محیطی
۱۲۳	شناسایی و تصدیق هویت
۱۵۳	نرم افزار تولیدکننده کلمه عبور
۱۵۷	فصل ششم دیوار آتش
۱۶۰	انواع دیوار آتش
۱۶۱	لایه اول دیوار آتش
۱۶۲	لایه دوم دیوار آتش
۱۶۲	لایه سوم دیوار آتش
۱۶۳	اجزای جانبی یک دیوار آتش
۱۶۵	نمونه‌های عملی تنظیم دیوار آتش
۱۸۱	فصل هفتم رمزنگاری
۱۹۲	SSL
۱۹۸	امضای دیجیتال
۲۰۲	IPSEC و VPN
۲۱۸	نرم افزارهای کمکی برای رمزگذاری Folder Lock
۲۲۱	فصل هشتم برنامه‌های مخرب و جرایم رایانه‌ای
۲۲۳	نرم افزار مخرب
۲۲۵	عملکرد نرم افزارهای مخرب
۲۳۱	جرم‌های مرتبط با فناوری اطلاعات
۲۳۴	کنترل بازرسی

فصل نهم نکات عملی برقراری امنیت در ویندوز ۲۴۲

- قسمت اول: اقدامات امنیتی ابتدایی (Basic Security Action) ۲۴۵
- ۱- امنیت فیزیکی رایانه‌ها را تامین کنید ۲۴۵
 - ۲- برای همه پارتیشن‌ها از NTFS استفاده کنید ۲۴۵
 - ۳- Simple File Sharing را غیر فعال کنید ۲۴۶
 - ۴- User Account خود کلمه عبور بگذارید ۲۴۸
 - ۵- از گروه Administrator به دقت استفاده کنید ۲۴۹
 - ۶- در صورت اتصال دائم به اینترنت از Firewall استفاده کنید ۲۴۹
 - ۷- روی رایانه خود ضدویروس نصب کنید ۲۵۰
 - ۸- همیشه ضدویروس خود را بروز نگه دارید ۲۵۰
 - ۹- در Password protected screensaver را فعال کنید ۲۵۲
 - ۱۰- شبکه‌های بیسیم خود را امن کنید ۲۵۲
 - ۱۱- نسخه‌های پشتیبان خود را در جای امن قرار دهید ۲۵۲
- قسمت دوم: اقدامات متوسط امنیتی (Intermediate Security Action) ۲۶۵
- ۱- از Security Configuration Management استفاده کنید ۲۶۵
 - ۲- از password security مناسب استفاده کنید ۲۷۰
 - ۳- از Software Restriction Policy استفاده کنید ۲۷۲
 - ۴- تعداد Account غیر لازم را محدود کنید ۲۷۳
 - ۵- نام کاربر Administrator را تغییر دهید ۲۷۳
 - ۶- یک Administrator مصنوعی بسازید ۲۷۴
 - ۷- خودتان دسترسی فایل‌های Share شده را تعیین نمایید ۲۷۴
 - ۸- نام آخرین کاربری که به سامانه Log on نموده نمایش داده نشود ۲۷۴

- ۹- مطمئن شوید که Remote Desktop غیرفعال است. ۲۷۵
- ۱۰- سرویس‌های غیرضروری را از کار بپندازد. ۲۷۶
- ۱۱- از (encrypt file system) استفاده کنید. ۲۷۷
- ۱۲- اگر از Offline folder استفاده می‌کنید آنها را رمزگذاری کنید. ۲۷۹
- ۱۳- فولدرهای Temp را رمزگذاری کنید. ۲۸۱
- ۱۴- هنگام Shut down کردن ویندوز page File را پاک کنید. ۲۸۱
- ۱۵- سوم: اقدامات امنیتی پیشرفته (Advance Security Action) ۲۸۲
- ۱- Auditing را به رایانه فعال کنید. ۲۸۲
- ۲- Default Share ها را غیرفعال کنید. ۲۸۳
- ۳- Dump File را غیرفعال کنید. ۲۸۶
- ۴- قابلیت بالا آمدن ریم دیسک به Floppy یا CD را غیرفعال کنید. ۲۸۷
- ۵- قابلیت Auto Run را برای CD غیرفعال کنید. ۲۸۸
- ۶- از Smart Card یا سامانه‌های Biometric استفاده کنید. ۲۸۹
- ۷- سطح دسترسی به پوشه‌ها و درایوها را برای کاربران تعریف کنید. ۲۹۰
- ۸- درایوهای سامانه‌ای را مخفی کنید. ۲۹۲
- ۹- درایوهای مورد نظر را غیرفعال کنید. ۲۹۳
- ۱۰- دسترسی به رجیستری را محدود کنید. ۲۹۳
- ۱۱- بر روی Setup رایانه کلمه عبور قرار دهید. ۲۹۵
- ۱۲- System Restore را غیرفعال کنید. ۳۰۱
- ۱۳- سخت‌افزارهای خود را کنترل کنید. ۳۰۲
- ۱۴- راه‌های شکستن کلمه عبور Setup ۳۰۲
- ۱۵- پیکربندی دیسک‌سخت را تنظیم نمایید. ۳۰۳
- ۱۶- ردپا در اینترنت را حذف نمایید. ۳۰۴

۱۷- سطح امنیت در اینترنت (Internet Explore) را تنظیم نمایید. ۳۰۷

منابع و مآخذ ۳۱۱

www.ketab.ir

پیش‌گفتار

امروزه لازمه پیشرفت حرکت به‌سوی فناوری است و بالا‌جبار فناوری‌های رایانه‌ای تمام ابعاد زندگی را تحت تأثیر قرار می‌دهند. بی‌شک هر گونه تغییری که آگاهانه و با درایت صورت نپذیرد، نه تنها منجر به پیشرفت و تکامل نمی‌شود بلکه مخاطرات زیادی هم به همراه دارد.

جیتا شدن اطلاعات به اشتراک‌گذاری و نگهداری آنها را با هزینه بسیار کمتر و رعایت بیشتر امکان‌پذیر ساخته است. با وارد شدن شبکه‌های کامپیوتری، به سازمان‌ها و تشکیلات اداری اقتصادی نقش پر ارزش آنها در کاهش گردش کاغذ و نامه‌نگاری‌های بیهوده آشکار شد. شبکه کامپیوتری هدیه بزرگی به سازمان‌ها داد و در عین حال نیازمند مراقبت‌های بیشتر برای رفع خطراتی چون نفوذ امنیتی بود. به موازات پیشرفت علوم شبکه کامپیوتری علوم دیگری نیز برای برقرار کردن امنیت پیشرفت نمودند.

منابع زیادی برای سرعت بخشیدن به رایانه‌ای شدن امور تهیه شده است، لیکن منابعی که به زبان کاربردی به بررسی مسائلی از ابعاد مختلف بپردازند و برای آنها راه حل‌های کاربردی ارائه دهند بسیار محدود هستند. این کتاب را بر آن داشت تا با جمع‌آوری مطالب کاربردی گامی در جهت ادای مسوولیت خویش بردارد.

دنای گسترده اطلاعات و فناوری اطلاعات ابتدا مبتنی بر مدار است. مشخص است که اگر بخواهیم کتابی بنگاریم که تمام این دنیا را پوشش دهد، چه به‌طور هم‌کفایت امر نمی‌کند. از این جهت نگارندگان این اثر تصمیم گرفتند بجای پوشش دادن تمام ابعاد این دنیای وسیع، آن بخشی را که در دوره‌های آموزشی عالی رسته‌ای و کارشناسی دانشگاه تدریس می‌شوند مد نظر قرار دهند. در کنار سرفصل‌های ذکر شده، به‌طور سه‌درج پیش‌نیازهای علمی مباحث هم شدیم. در فصل آخر کتاب راه کارهای عملی برقرار کردن امنیت در ویندوز بیان شده است و با ذکر مثال و شکل کاربر در فضای واقعی قرار می‌گیرد. مطالب این کتاب علاوه بر کاربرد نظری، کاربری عملی در راستای آگاه سازی کارکنان سازمان هم دارد.

در این کتاب سعی شده است مطالب از منابع علمی معتبر جمع‌آوری و به زبان ساده و کاربردی بازنویسی گردد. البته بر حسب موضوع در برخی فصول به ناچار برای درک مطالب، به مباحث فنی نیز پرداخته شده است.