

تهدید سایبری و پدافند سایبری ۲

www.ketab.ir

گرد آوری و تألیف :

مهندس حمید اسکندری

سرشناسه	اسکندری، حمید، ۱۳۳۸ -
عنوان و نام پدیدآور	تهدید سایبری و پدافند سایبری ۲ / گردآوری و تألیف حمید اسکندری
مشخصات نشر	تهران: بوستان حمید، ۱۳۹۸.
مشخصات ظاهری	۱۷۶ ص.: جدول.
شابک	۹۷۸-۶۰۰-۶۴۱۲-۶۷-۲ :
وضعیت فهرست نویسی: فیپا	
یادداشت	: کتابنامه.
موضوع	کامپیوترها -- ایمنی اطلاعات
موضوع	Computer security:
موضوع	شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع	Computer networks -- Security measures:
موضوع	فضای مجازی -- تدابیر ایمنی
موضوع	Cyberspace -- Security measures:
رده بندی کنگره	TK ۸۱۰۵/۰۰۰
رده بندی دیویی	۰۰۰ ۵۰
شماره کتابشناسی ملی	۵۰۱۴۱۷۷



انتشارات

عنوان : تهدید سایبری و پدافند سایبری
تألیف و گردآوری : مهندس حمید اسکندری
ویراستار : مهندس محمد صادق اسکندری
ناشر : بوستان حمید
چاپ : اول ۱۳۹۸
شمارگان : ۸۰۰

قیمت : ۲۰۰۰۰ تومان

• کلیه حقوق اعم از چاپ و تکثیر، نسخه برداری برای ناشر محفوظ است.

تلفن ناشر و پخش کتاب: ۶۶۴۸۲۳۸۹ ۰۹۱۲۲۳۷۵۰۳۹ ۰۹۱۲۷۷۵۷۸۳۸
آدرس فروشگاه اینترنتی: boostanhamid-pub.ir
«این کتاب با کاغذ حمایتی منتشر شده است»

پیش گفتار

اکنون جامعه مدرن ما از بسیاری جنبه‌ها به فناوری اطلاعات بصورت مستقیم یا غیر مستقیم وابسته است. بدین ترتیب، به خطر افتادن دسترس پذیری و صحت اطلاعات در سیستم‌ها و زیرساخت‌ها (مانند بانکداری، دولت الکترونیک، ارتباطات و ...) می‌تواند پیامدهای ناگواری از بعد اجتماعی داشته باشند.

با توجه به آسیب پذیری‌های ذاتی موجود در فضای سایبری و روند رو به رشد مهاجرت از دنیای سنتی به این فضا، ریسک سامانه‌های مبتنی بر فناوری اطلاعات، که برای اقتصاد کشور حیاتی می‌باشد، را افزایش می‌دهد. پیچیدگی روزافزون و رو به ازدیاد سامانه‌ها و شبکه‌های مبتنی بر فناوری اطلاعات چالش‌های امنیتی را برای کشور در بر دارد. نگاه راهبردی به جنگ سایبری

حوادث سایبری سال‌های ۱۳۸۹ و ۱۳۹۰ در زیرساخت‌های مهم صنعتی کشور، نمونه‌های از این دشمنی‌ها است که از سوی آمریکا علیه جمهوری اسلامی ایران انجام شد. این حملات سایبری تلاش ناموفقی از سوی آنان بود که ناکامی در رسیدن به اهداف از پیش طراحی شده آن، یکی از دلایل تغییر و عزل فرمانده آمریکایی قرارگاه سایبری این کشور شد. اکنون فضای سایبری برخلاف تعاریف اولیه، فضای جنگ و دفاع است و تمامی سیاست‌های دفاعی کشور ما در این حوزه صادق است، بطوریکه بریکرد و راهبرد جمهوری اسلامی ایران در پاسخ به حملات سایبری دشمنان نظام اسلامی، یک اقدام متقابل است.

دیدگاه فرهنگی تهدیدات سایبری

امروزه کشورهای سلطه‌گر تلاش بر این دارند تا از انواع فرهنگی مانند سینما و فیلم‌سازی و اسباب‌بازی و بازی‌های رایانه‌ای و ماهواره‌ها و شبکه‌های اجتماعی در رابطه با نفوذ فرهنگی خود استفاده نمایند و به دنبال این هستند تا با گسترش انواع رسانه‌های نوین و سنتی از قبیل پیام‌رسان‌ها (تلگرام و ...)، رادیو و تلویزیون‌های در حال گسترش و

خبرگزاری‌ها، برای نیل به اهداف خود هر زمان که لازم دیدند به توسعه کیفی و کمی این ابزار، پردازند و همچنین تلاش می‌کنند تا با استفاده از انواع سرویس‌هایی که در اینترنت ارائه می‌گردد از قبیل: سایت‌های خبری و خبرگزاری‌ها - سایت‌های ارتباطی و شبکه‌های اجتماعی - وبلاگ‌ها و ... دیگران را به استفاده از این ابزار تشویق و ترغیب نموده تا به اهداف خود برسند.

- مواردی از سیاست‌های کلی برنامه ششم توسعه ابلاغی مقام معظم رهبری در حوزه دفاعی و امنیتی^۱

بند ۱۳-۱- اشاء توان بازدارندگی کشور با:

۱-۵۳- توسعه توان مملکتی و فناوری‌ها و ظرفیت تولید سلاح‌ها و تجهیزات عمده‌ی دفاعی برترساز با توان بازدارندگی، متناسب با انواع تهدیدات.

۲-۵۳- گسترش هوشمندی و مدرن‌سازی پدافند غیرعامل با اجرای کامل پدافند غیرعامل در مراکز حیاتی و حساس کشور.

۳-۵۳- افزایش ظرفیت‌های قدرت نرم و فعال سایبری و تأمین پدافند و امنیت سایبری برای زیرساخت‌های کشور در چارچوب سیاست‌های کلی مصوب.

سعی شده مطالب مورد نیاز در مورد تهدیدات سایبری، پدافند سایبری و راهکارها، آشنایی با آسیب‌های شبکه‌های اجتماعی، بدافزارهای تلفن همراه، همچنین مدیریت امنیت اطلاعات در قالب این کتاب ارائه گردد، امیدواریم مورد استقبال مدیران، کارشناسان دستگاه‌های اجرایی و شرکت‌ها به‌عنوان کاربران عمومی و سایر علاقه‌مندان قرار گیرد.

فهرست

فصل اول تهدیدات سایبر - جنگ سایبر

- ۱- کلیات ۹
- ۲- مواردی از نظرات جدید ریاست محترم سازمان پدافند غیرعامل کشور ۱۳
- ۳- اشار اجمالی به رویداد ها و گزارش های تهدیدات سایبری ۲۲
- ۴- طرح سایبری (بدافزارها و نرم افزارهای مخرب) ۲۸
- ۵- منابع تهدیدات انواع روش های حملات سایبری و ۳۳
- ۶- سایر تهدیدات سایبر (حملات مهندسی اجتماعی، انواع هکرها) ۴۰
- ۷- تهدیدات شبکه های رایانه ای سیم ۵۰
- ۸- شبکه جاسوسی اشلون ۵۴

فصل دوم پدافند سایبری

- ۱- مقدمه ۵۵
- ۲- اسناد بالا دستی پدافند سایبری (مرکز ملی فضای مجازی و...) ۵۶
- ۳- موادی از سند راهبردی پدافند سایبری کشور (اهداف، راهبردها، مأموریت...) ۶۰
- ۴- چرخه پدافند سایبری ۶۶
- ۵- تاب آوری سایبری ۶۷
- ۶- بررسی حمله به سامانه اسکادا و مقابله با ویروس استاکس نت و ۷۱
- ۷- سایر راهکارهای مقابله با بدافزارها (فایروال ها و...) ۸۰

فصل سوم آسیب‌های شبکه‌های اجتماعی و اینترنت

- ۱- مقدمه ۸۹
- ۲- شبکه‌های اجتماعی و تهدید امنیت محیط‌های سازمانی ۹۱
- ۳- معضلات فرهنگی اینترنت و شبکه‌های مجازی ۹۴
- ۴- نتیجه‌گیری و پیشنهاد ۱۰۹

فصل چهارم مدیریت امنیت اطلاعات (ISMS)

- ۱- مقدمه ۱۱۳
- ۲- کلیات ۱۱۷
- ۳- استانداردهای ISMS ۱۱۹
- ۴- دستورالعمل‌های امنیت اطلاعات (مواردی از توصیه‌نامه‌ها) ۱۲۴

فصل پنجم مباحث مرتبط با امنیت داده (رمزنگاری، مدیریت نفوذ و ...)

- ۱- رمزنگاری ۱۴۹
- ۲- کشف و مدیریت نفوذ ۱۶۰
- ۳- مدیریت رخدادها و پاسخگویی به آن ۱۶۶
- ۴- بدافزارهای تلفن همراه ۱۷۱
- کتابنامه ۱۷۵