

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: فیا	
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 ۵۱۰۵/۵
رده بندی دیویی	: ۸۰۰۵
شماره کتابشناسی ملی	: ۵۷۱۴۷۷۷



انتشارات

عنوان: تهدید سایبری و پدافند سایبری ۲
تألیف و گردآوری: مهندس حمید اسکندری
ویراستار: مهندس محمد صادق اسکندری
ناشر: بوستان حمید
چاپ: دوم ۱۴۰۳
شمارگان: ۶۰۰
قیمت: ۱۶۰۰۰۰ تومان

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

تلفن ناشر و پخش کتاب: ۶۶۴۸۲۳۸۹ ۰۹۱۲۲۳۷۵۰۳۹
آدرس فروشگاه اینترنتی: boostanhamid-pub.ir

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 آسیب‌پذیری‌های 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 می‌باشند، 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 سایبر

حوادث سایبری سال‌های ۱۳۸۹ و ۱۳۹۰ در زیرساخت‌های مهم صنعتی کشور، نمونه‌های از این دشمنی‌ها است که از سوی آمریکایی‌ها علیه جمهوری اسلامی ایران انجام شد. این حملات سایبری تلاش ناموفقی از سوی آنان بود که تا کما می‌رسیدن 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 رویکرد 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 ابزار 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، بپردازند و همچنین -

تلاش می کنند تا با استفاده از انواع سرویس هایی که در اینترنت ارائه می گردد از قبیل :
سایت های خبری و خبرگزاری ها - سایت های ارتباطی و شبکه های اجتماعی - وبلاگ ها و ...
دیگران را به استفاده از این ابزار تشویق و ترغیب نموده تا به اهداف خود برسند.

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

بند ۵۳ - ارتقاء توان بازدارندگی کشور با:

۵۳-۲ - گسترش هوشمندانه و مصون سازی پدافند غیرعامل با اجرای کامل پدافند غیرعامل در
مراکز حیاتی و حساس کشور.

۵۳-۳ - افزایش ظرفیت های قدرت نرم و دفاع سایبری و تأمین پدافند و امنیت سایبری برای
زیرساخت های کشور در چارچوب سیاست های کلی مصوب.

موارد مرتبط از طرح راهبردی حفاظت از زیرساخت های کشور

- مصون سازی سایبری همه جانبه، چندلایه و تطبیق پذیر زیرساخت های حائز اهمیت سایبری
و وابسته به سایر کشور در مقابل تهدیدات سایبری دشمن از طریق:

۱. شناسایی و ارزیابی دارایی های سایبری و تعیین سطح اهمیت آن ها،

۲. رصد، پایش، برآورد تهدیدات و اشتراک گذاری اطلاعات،

۳. رفع یا کاهش آسیب پذیری ها سایبری دارایی های سایبری و وابسته به سایر،

۴. برآورد، تحلیل و مدیریت مخاطرات سایبری زیرساخت و پیامدهای آشناری آن،

۵. نظام مند کردن ساختار امنیت و پدافند سایبری و فرآیندها و نیروی انسانی،

سعی شده مطالب مورد نیاز در مورد تهدیدات سایبری، پدافند سایبری و راهکارها، آشنایی
با آسیب های شبکه های اجتماعی، بدافزارهای تلفن همراه و همچنین مدیریت امنیت اطلاعات در
قالب این کتاب ارائه گردد، امیدواریم مورد استفاده مدیران، کارشناسان دستگاه های اجرایی و
شرکت ها به عنوان کاربران عمومی و سایر علاقه مندان قرار گیرد.

۱- از سیاست های کلی برنامه ششم توسعه ابلاغی - سال ۱۳۹۴ - سایت سازمان مدیریت و برنامه ریزی کشور

فهرست

فصل اول تهدیدات سایبر - جنگ سایبر

- ۱- کلیات ۹
- ۲- مواردی از نظرات جدید ریاست محترم سازمان پدافند غیرعامل کشور ۱۳
- ۳- اشاره اجمالی به رویدادها و گزارش‌های تهدیدات سایبری ۲۲
- ۴- سلاح سایبری (بدافزارها و نرم‌افزارهای مخرب) ۲۸
- ۵- منابع تهدیدات، انواع روش‌های حملات سایبری و ۳۳
- ۶- سایر تهدیدات سایبری (حملات مهندسی اجتماعی، انواع هکرها) ۴۰
- ۷- تهدیدات شبکه‌های رایانه‌ای بی‌سیم 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- تاب‌آوری 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 داده‌رمنگاری، مدیریت نفوذ و ...)

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