

تهدید سایبری و پدافند سایبری

گرد آوری و تألیف :

مهندس حمید اسکندری

مهندس رحمت اله امیر صوفی

سرشناسه : اسکندری، حمید، ۱۳۳۸ -
 عنوان و نام پدیدآور : تهدید سایبری و پدافند سایبری / گردآوری و تألیف حمید اسکندری،
 رحمت اله امیرصوفی.
 مشخصات نشر : تهران: بوستان حمید، ۱۳۹۴.
 مشخصات ظاهری : ۱۷۶ ص.: جدول.
 شابک : ۹۷۸-۶۰۰-۶۴۱۲-۴۸-۱
 وضعیت فهرست نویسی: فیبا
 یادداشت : کتابنامه. ۱۷۵-۱۷۶
 موضوع : کامپیوترها -- ایمنی اطلاعات
 موضوع : شبکه‌های کامپیوتری -- تدابیر ایمنی
 مرصوع : فضای مجازی -- تدابیر ایمنی
 شناسه افزوده : امیرصوفی، رحمت‌الله، ۱۳۴۱ -
 رده بندی کتبه : ۱۳۹۴ ت ۵۴الف/۵/۵۱۰۵ TK
 رده بندی دیویی : ۰۰۵۸
 شماره کتابشناسی ملی : ۴۰۰۰۷۹



انتشارات

عنوان : تهدید سایبری و پدافند سایبری
 تألیف و گردآوری : مهندس حمید اسکندری - مهندس رحمت اله امیرصوفی
 ویراستار : مهندس محمد صادق اسکندری
 ناشر : بوستان حمید
 چاپ : اول ۱۳۹۴
 شمارگان : ۱۴۰۰
 قیمت : ۱۰۰۰۰ تومان

• کلیه حقوق اعم از چاپ و تکثیر، نسخه‌برداری برای ناشر محفوظ است. (نقل مطالب با ذکر مأخذ بلامانع است).

۰۹۱۲۷۷۵۷۸۳۸

۰۹۱۲۲۳۷۵۰۳۹

تلفن ناشر: ۳۳۷۰۰۹۲۷

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 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 سایبری

حوادث سایبری سال‌های ۱۳۸۹ و ۱۳۹۰ در زیر ساخت‌های مهم صنعتی کشور، نمونه‌های از این دشمنی‌ها است که از سوی آمریکا و همکارانش علیه جمهوری اسلامی ایران انجام شد. این حملات سایبری تلاش ناموفقی از سری 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 راهبردهای راهبرد جمهوری اسلامی ایران در پاسخ به حملات سایبری دشمنان نظام اسلامی، یک اقدام قابل ملاحظه است.

دیدگاه فرهنگی تهدیدات سایبری

امروزه کشورهای سلطه‌گر تلاش بر این دارند تا از انواع ابزار فرهنگی مانند سینما و فیلم سازی و اسباب بازی و بازی‌های رایانه‌ای و ماهواره‌ها و حتی موسیقی در رابطه با نفوذ فرهنگی خود استفاده نمایند و به دنبال این هستند تا با استفاده از انواع رسانه‌های نوین و سنتی از قبیل مطبوعات و رادیوها و تلویزیون‌های در حال گسترش و خبرگزاری‌ها در این رابطه استفاده

نمایند و هر زمان که لازم دیدند برای نیل به اهداف خود، به توسعه کیفی و کمی این ابزار، پردازند 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 - رسانه های اجتماعی - 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.

در بند ۱۱ سیاست های کلی نظام در خصوص پدافند غیرعامل این چنین آمده است:

« اصول و ضوابط مقابله با تهدیدات نرم افزاری و الکترونیکی و سایر تهدیدات جدید دشمن به منظور: نظم، صیانت شبکه های اطلاع رسانی، مخابراتی و رایانه ای.»

مواردی از راهبرد های پدافند سایبری:

(۱) طراحی پیاده سازی و راهبری نظام جامع بومی پدافند سایبری هوشمند، پایدار و مقاوم، انحصاری، انتزاعی، لایه به لایه، پیش گیرانه، شبکه ای، چابک و منعطف در سطوح ملی، دستگاه و استانی.

(۲) طراحی، پیاده سازی و راهبری طرح ها و برنامه های پدافند سایبری از زیرساخت های کشور برای سود سازی زیست بوم سایبری در برابر تهدیدات و تهاجم سایبری متناسب با سطح اهمیت آنها.

(۳) الزام و همراه سازی سازمان های متولی زیر ساخت های حیاتی و حساس کشور در استفاده از محصولات سایبری امن بومی.

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.

فهرست

فصل اول تهدیدات سایبر - جنگ سایبر

- ۱- کلیات ۱۱
- ۲- مواردی از نظرات ریاست محترم سازمان پدافند غیرعامل کشور ۱۵
- ۳- اشاره جمالی به رویداد ها و گزارش ها در داخل و خارج کشور ۲۰
- ۴- سلا- سایبری (بدافزارها و نرم افزار های مخرب) ۲۶
- ۵- منابع تهدیدات، انواع حملات سایبری ۳۳
- ۶- سایر تهدیدات سایبری (- حملات مهندسی اجتماعی و...) ۴۲
- ۷- تهدیدات شبکه های رایانه ای بی سیم ۴۶
- ۸- شبکه جاسوسی اشلون ۵۰

فصل دوم پدافند سایبری

- ۱- مقدمه ۵۳
- ۲- اسناد بالا دستی پدافند سایبری ۵۳
- ۳- موادی از سند راهبردی پدافند سایبری کشور (اهداف، راهبردها، مأموریت...) ۵۵
- ۴- بررسی حمله به سامانه اسکادا و مقابله با ویروس استاکس نت و ۶۱
- ۵- سایر راهکارهای مقابله با بدافزارها (فایروال ها و...) ۷۰

فصل دوم آسیب های شبکه های اجتماعی و اینترنت

- ۱- مقدمه ۸۱

- ۲- شبکه های اجتماعی و تهدید امنیت محیط های سازمانی ۸۴
- ۳- معضلات فرهنگی اینترنت و شبکه های مجازی ۸۷
- ۴- نتیجه گیری ۱۰۰

فصل چهارم مدیریت امنیت اطلاعات (ISMS)

- ۱- مقدمه ۱۰۵
- ۲- کلیات ۱۰۹
- ۳- استانداردهای ISMS ۱۱۱
- ۴- دستور العمل های امنیت اطلاعات (مواردی از توصیه نامه ها) ۱۱۶

فصل پنجم مهندسی امنیت و ملاءمات

- ۱- کلیات ۱۳۹
- ۲- چرخه ی حیات مهندسی امنیت ۱۴۰
- ۳- مباحث مرتبط امنیت اطلاعات ۱۴۵
- ۱-۳- مدیریت رخداد ها و پاسخگویی به آزار ۱۴۵
- ۲-۳- رمزنگاری ۱۵۰
- ۳-۳- کشف و مدیریت نفوذ ۱۶۱
- ۴-۳- بدافزارهای تلفن همراه ۱۷۰
- کتابنامه ۱۷۵