تهدید ۱ سور

تهدیدات ناشناسوری در فضای سایبر

به همراه راهکارهایی آسان برای حفاظت در مقابل تهدیدات سایبری

ترجمه: علیرضا صالحی

عنوان و نام پدیدآور: تهدیداسور: تهدیدات دایناسوری در فضای سایبر به همراه راهکارهای آسان برای حفاظت در مقابل تهدیدات سایبری/ ترجمه علیرضا صالحی.
مشخصات نشر: تهران: شایبان، ۱۳۹۴.
مشخصات ظاهری: ۱۴۴ ص.: مصور (رنگی) ؛ ۱۱×۱۷ س‌م.
شابک: ۱-۰۰-۹۶۲۴۲-۶۰۰-۹۷۸ : ۰۰۰ ریال
وضعیت فهرست نویسی: فیپا
یادداشت: عنوان اصلی: Threatsaurus The A-Z of computer and data security threats.
یادداشت: چاپ قبلی: علیرضا صالحی درجزینی، ۱۳۹۴.
عنوان دیگر: تهدیدات دایناسوری در فضای سایبر به همراه راهکارهای آسان برای حفاظت در مقابل تهدیدات سایبری.
موضوع: شبکه‌های کامپیوتری -- تدابیر ایمنی
موضوع: کامپیوترها -- ایمنی اطلاعات
موضوع: فضای مجازی -- تدابیر ایمنی
موضوع: جنگ اطلاعاتی
موضوع: تکنولوژی اطلاعات -- تدابیر ایمنی
موضوع: حفاظت اطلاعات
شناسه افزوده: صالحی درجزینی، علیرضا، ۱۳۵۲ -، مترجم
شناسه افزوده: یاراحمدی، فریبا، ۱۳۵۱ -، ویراستار
رده‌بندی کنگره: ۱۳۹۴ ۹۴ت/TK۵۱۰۵/۵۹
رده‌بندی دیویی: ۰۰۵/۸
شماره کتابشناسی ملی: ۳۸۸۹۲۱۴

تهدیداسور (تهدیدات دایناسوری در فضای سایبر)

به همراه راهکارهایی آسان برای حفاظت در مقابل تهدیدات سایبری

این کتاب ترجمه ای است از:

Threatsaurus: The A-Z of co[illegible]er and [illegible]ata [illegible]curity threats

ترجمه: علیرضا صبحی

ویراستار: فریبا یاراحمدی

طراحی، صفحه آرایی و [illegible]رت چاپ: مؤسسه فرهنگی هنری دیده‌بان ایما تدبیر

ناشر: سایبان-۱۳۹۴ **[illegible]رافیک:** شمیم **چاپ:** یسنا

شمارگان: ۲۰۰۰ جلد

چاپ: اول انتشارات سایبان۱۳۹۴

چاپ: چهارم کتاب (چاپ قبلی: علیرضا صبحی؛ پاییز و زمستان ۱۳۹۲، زمستان ۱۳۹۳)

شابک: ۱-۰۰-۹۶۲۴۲-۶۰۰-۹۷۸

نشانی: تهران - خیابان سهروردی شمالی- کوچه حاج حسنی- شماره ۵۵- طبقه اول

تلفن: ۸۸۷۴۹۴۱۰ **فکس:** ۸۸۷۴۹۴۱۵

www.sayebaan.ir فروش آنلاین: www.mrcenter.ir

قیمت: ۸۰۰۰۰ ریال

درباره موسسه دیده‌بان آی‌تی

www.didehban.com

موسسه دیده‌بان آی‌تی با بهره‌گیری از بیش از بیست سال سابقه و تجربه مدیران و متخصصان روزنامه‌نگاری، گرافیک و آی‌تی و همچنین حضور موثر و مستمر در دوره‌های مختلف نمایشگاه‌های داخلی و منطقه‌ای از سال ۱۳۸۶ فعالیت رسمی خود را به عنوان تنها موسسه روابط عمومی کشور در حوزه آی‌تی، آغاز کرده است.

به موازات رشد صنعت آی‌تی در کشور و همچنین ضرورت امر اطلاع‌رسانی و آگاهی‌رسانی در این حوزه، موسسه دیده‌بان آی‌تی نیز فعالیت‌های خود را در این حوزه گسترده‌تر کرد.

در حال حاضر مشاوره تخصصی در زمینه طرح‌های اطلاع‌رسانی و روابط عمومی، برگزاری سمینارهای عمومی و تخصصی، طراحی، نگارش، تدوین، انتشار و توزیع نشریات و خبرنامه‌های اختصاصی، حضور در رویدادهای نمایشگاهی به همراه پوشش خبری، و انتشار کتاب از جمله فعالیت‌های این موسسه است.

ترکیب تجربه و توانایی روزنامه‌نگاری با دانش فنی و شناخت کامل حوزه آی‌تی و همچنین حضور فعال در مجامع صنفی و تشکل‌های آی‌تی، سه ضلع تشکیل دهنده مثلث توانمندی‌های موسسه دیده‌بان آی‌تی به شمار می‌رود.

فهرست مطالب

شرکت گسترش خدمات تجارت الکترونیک ایرانیان (ایدکو)

www.iedco.ir

بدون شک دنیای امروز، دنیای فناوری اطلاعات است. نیاز روزافزون شرکت‌ها به فناوری اطلاعات و کاربردهای آن بر هیچ‌کس پوشیده نیست. این نیاز با که در برخی زمینه‌ها با رشدی انفجاری روبروست، وجود شرکت‌هایی کارآمد و قوی را می‌طلبد که بتوانند همگام با پیشرفت فناوری و ورود تکنولوژی‌های نوین، آن‌ها را به‌کار گیرند و در خدمت سازمان‌ها قرار دهند.

اما همزمان با این رشد، موضوع امنیت داده‌ها و امن‌سازی فضای تبادل اطلاعات نیز بیش از پیش مورد توجه قرار گرفت به طوری که امروزه، شبکه‌های داده‌ای بدون وجود راهکارهای امنیتی قابل تصور نیست. شرکت گسترش خدمات تجارت الکترونیک ایرانیان (ایدکو) با همین هدف و با پشتوانه علمی نخبگان و مدیران خود و بهره‌گیری از نظرات کارشناسان توانسته است ارائه دهنده راه‌حل‌های جامع امنیت فناوری اطلاعات باشد. به‌طوری که هم اکنون بیش از دو هزار سازمان و شرکت دولتی و خصوصی را به عنوان مشتری در کنار خود دارد. از دیگر سوی فناوری، که با سرعتی شگفت در حال رشد است، نیازمند فرهنگ‌سازی و به‌کارگیری انواع ابزارهای اطلاع‌رسانی برای عموم آن است. به همین سبب، این شرکت براساس شعار «ایدکو، وفاداربه تعهدات»، خود را متعهد به آگاهی‌رسانی و بالابردن سطح دانش مخاطبان و فراتر از آن عموم آحاد جامعه می‌داند و حمایت از فعالیت‌هایی نظیر نشر کتب و مقالات نیز در همین راستا تعریف می‌گردد.

شرکت ایدکو با هدف بالابردن سطح دانش جامعه و در راستای ایفای مسئولیت اجتماعی خود، این کتاب را به عموم خوانندگان تقدیم می‌نماید.

مقدمه

سی سال قبل، اولین ویروس کامپیوتر متولد شد. الک کلونر توانست کامپیوتری که آلوده شده بود را در پنجاهمین مرتبه‌ای که بوت می‌شد، وادار به نمایش یک شعر کوتاه بنماید. از آن زمان به‌بعد تبهکاران دنیای سایبری، میلیون‌ها ویروس و بدافزار را در قالب‌های مختلفی از جمله تروجان، کرم اینترنتی، جاسوس‌افزار و ... روانه سیستم‌ها کرده‌اند. در بسیاری از اوقات هم به تیتر اول خبرهای جهان تبدیل شده‌اند.

افراد بسیاری از ویروس‌ها و عملکرد آن‌ها چیزهایی شنیده‌اند. ویروس‌هایی که اطلاعات کامپیوترها را پاک می‌کنند یا پیام‌های عجیب و غریبی روی صفحه نمایش نشان می‌دهند. نزد عامه مردم، هنوز هم ویروس‌ها یا کارکرد سربه سر گذاشتن دارند و یا عامل تخریب هستند.

در اوایل دهه اول میلادی، ویروس میکل آنژ، وحشتی عمومی را سبب شد. در سال‌های بعد هم میلیون‌ها کامپیوتر توسط ویروس SoBig.F آلوده شدند و ناخواسته شروع به دانلود برنامه‌های ناشناخته‌ای

از وب نمود. همین امر سبب شد که تعداد بسیاری از سرمایه‌گذاران دهنده‌ها ناچار به خاموش‌کردن سرورهایشان بشوند. حتی صنعت فیلم‌سازی نیز با ساخت فیلم‌هایی مانند «روز استقلال» حملات ویروسی این چنین را به اکران سینماها آورد.

هرچند سناریوهای این چنینی را در بیشتر فیلم‌ها می‌بینیم، اما خطرات و تهدیدات سایبری به تنها کمتر نشده‌اند که افزایش چشمگیری هم یافته‌اند؛ اما خاموش‌تر، با شناسایی اهداف دقیق‌تر و برای کسب درآمدهای بیشتر.

امروز بدافزارها چندان به دنبال تخریب یا هدف فایل‌های کامپیوترها یا نمایش پیام‌های مسخره نیستند. خرابکاران سایبری راه‌های دیگری را در پیش گرفته‌اند. مثلا همه فایل‌های سیستم را رمزنگاری می‌کنند، یک حمله سراسری به یک شرکت بزرگ را طرح‌ریزی می‌کنند یا مانع دست‌یابی مشتریان به وب‌سایت یک شرکت خاص می‌شوند. حتی بدافزارها تمایل چندانی به آشکارسازی حضورشان ندارند. بلکه حتی بی سروصدا یک ثبت‌کننده ضرب کلید روی سیستم نصب می‌کنند و منتظر می‌مانند تا شما به سایت بانک مورد نظرتان سر بزنید و شماره کارت و رمز عبورتان را وارد کنید.

هکرها امروزه ترجیح می‌دهند هویت دیجیتالی شما را سرقت کنند و یا چند کپی از کارت بانکی‌تان بسازند و به حساب‌های بانکی شما سرک بکشند. دیگر نیاز نیست که ویروس روی کامپیوتر شما باقی بماند. همین که به هدفش برسد، خودش را از سیستم پاک می‌کند تا ردپایی باقی نماند.

خطر دیگری که بدافزارهای امروزی ایجاد می‌کنند، تمایل سیستم‌ها به زامبی‌هایی با کنترل از راه دور است. میلیون‌ها کامپیوتر بدون اینکه خودشان بدانند، در خدمت اهداف نفوذگران قرار می‌گیرند و فرامین آنها را اجرا می‌کنند.

در شبکه‌های اجتماعی مانند فیس‌بوک و توییتر هم خطرات افزایش یافته است. هکرها و تبهکاران سایبری این شبکه‌ها را به عنوان محل‌های جدیدی برای آلوده کردن کامپیوترها کشف کرده و مورد

استفاده قرار می‌دهند. هکرها حتی حملات گسترده و در مقیاس بزرگ را هم به کناری گذاشته‌اند. زیرا این کارها باعث [illegible] توجه شده و شرکت‌های سازنده ضد ویروس را به تلاش بیشتر وا می‌دارد. در نتیجه حملات به سمت هدف‌های خاص‌تر و به‌منظور سرقت داده‌ها، متمرکز شده است. حملات فیشینگ خاص یا انواع کلاهبرداری، نمونه‌ای از این رویکرد جدید است. فیشینگ‌ها به طور عام از طریق ارسال انبوه ایمیل‌های جعلی از طرف بانک‌ها صورت می‌گیرد تا کاربران با مراجعه به سایت جعلی مورد نظر، اطلاعات خود را وارد کنند. اما در فیشینگ‌های خاص، تنها تعداد محدودی از کاربران مورد هدف هستند. این ایمیل‌ها به نظر می‌آید که از طرف همکار شما یا فردی مورد اعتماد در سازمان شما ارسال شده که درخواست ارسال رمز عبور یا سایر اطلاعات مهم را دارد. طبیعی است که این قبیل حملات با موفقیت بیشتری روبرو می‌شوند زیرا قربانی فکرمی‌کند که ایمیل دریافتی از داخل سازمان بوده و باید به آن اعتماد کند. در حقیقت حملات در اندازه کوچک و هدفمند، رویکرد جدید تهدیدات دنیای سایبری هستند. اما در آینده چه اتفاقی خواهد افتاد؟ برخی فکر می‌کنند که تهدیدات بیش از این گسترش نخواهد یافت و در اینده از تعداد ویروس ها به شدت کاسته خواهد شد. برخی دیگر معتقدند که می‌توان مشکل هرزنامه‌ها و اسپم‌ها را برای همیشه حل‌کرد. در مقابل هم بعضی عقیده دارند که اوضاع خیلی بدتر از آنچه که تاکنون بوده خواهد شد و تهدیدات سایبری به یکی از گرفتاری‌های مهم تبدیل خواهد شد. اما صرف‌نظر از همه این پیش‌بینی‌ها، آنچه که مهم است آن است که هر جا که امکان کسب درآمد باشد هکرها و تبهکاران هم هستند و داده‌ها همواره در خطر خواهند بود.

کتابی که پیش رو دارید، ضمن آنکه شما را با انواع تهدیدات دنیای سایبری آشنا می‌کند، راهکارهایی را نیز برای حفاظت به شما ارائه می‌نماید.