تهدید امنیتی ۲۰۱۴-۲۰۱۲

گزارش امنیت رایانه‌ای SOPHOS

به انضمام روندهای تهدید امنیتی ۲۰۱۵

نویسنده: گرهارد اسلاتیر
مترجم: مهدی تهرانی
ناظر علمی: محسن زارع تاجیک

سرشناسه:اشلبک، گرهارد(Gerhard Eschelbeck) / مترجم: مهدی تهرانی/ناظر علمی: محسن زارع تاجیک
عنوان و نام پدیدآور: تهدید امنیتی ۲۰۱۴-۲۰۱۲:گزارش شرکت رایانه‌ای سوفوس(SOPHOS)
مشخصات نشر: تهران،انتشارات دیده‌بان
مشخصات ظاهری: ۱۶۲ ص. مصور، جدول
وضعیت فهرست‌نویسی: فیپا
موضوع: شبکه‌های کامپیوتری- تدابیر امنیتی- تروریسم رایانه‌ای- کامپیوترها- ایمنی اطلاعات- اینترنت- ایالات متحده
رده‌بندی کنگره: ۱۳۹۴ ۹ت۵۵الف/TK۵۱۰۵/۵۹ - رده‌بندی دیویی: ۰۰۵/۸- کتابشناسی ملی: ۳۹۱۶۷۸۴

انتشارات دیده‌بان

❖عنوان کتاب:تهدید امنیتی ۲۰۱۴-۲۰۱۲ گزارش شرکت رایانه‌ای سوفوس(SOPHOS)
❖نویسنده: اشلبک، گرهارد
❖ناشر: انتشارات دیده‌بان
❖مترجم: مهدی تهرانی
❖ناظرعلمی: محسن زارع تاجیک
❖ ویراستارادبی: میترا مشهدی‌رجب
❖طرح روی جلد: رضا حسنی
❖لیتوگرافی،چاپ و صحافی: انتشارات دیده‌بان
❖شمارگان:۵۰۰ جلد
❖نوبت چاپ: اول، پاییز ۹۴
❖قیمت:۱۵۰۰۰۰ ریال

شابک: ۳-۲-۹۵۵۲۰-۶۰۰-۹۷۸ ISBN: 978-600-95520-2-3

آدرس: تهران، چهارراه پاسداران، انتشارات دیده‌بان، تلفن: ۲۲۷۶۲۸۳۷

فهرست مطالب

سخن ناشر

همان‌طور که فضای مجازی دارای ویژگی‌های متعددی است و به‌صورت روزمره در زندگی اشخاص، حاکمیت و خدمات دولت‌ها، عملکرد نهادها و سازمان‌ها و بسیاری دیگر از موضوعات، مورد استفاده قرار می‌گیرد، فقدان امنیت آن باعث گردیده تا صدمات جبران ناپذیری به کاربران آن اعم از حقیقی و حقوقی، وارد گردد. همچنان که گزارش‌های متعددی از نقض‌های امنیتی در فضای سایبر را در این گزارش خواهید دید.

امروزه تأمین امنیت فضای سایبر و ارتقاء آن، مسئله اصلی دولت‌ها، نیروهای نظامی و امنیتی، سازمان‌های اطلاعاتی، شرکت‌ها، نهادها، اشخاص و... بوده و این مسأله بر شناسایی نقاط ضعف امنیتی در فضای سایبر و بررسی گزارشات اتفاقات امنیتی رخ داده، راه‌حل دیگری نمی‌تواند داشته باشد تا ضمن آشنایی با راه‌های نفوذ، هوشیاری در کاربران فناوری اطلاعات که بالاترین درجه آسیب‌رسانی را در فضای سایبر دارند، بالا رود.

کتاب حاضر، مشتمل بر گزارش‌هایی از نقض امنیت در حوزه فناوری اطلاعات و رویکردهای امنیتی در سراسر دنیا از سال‌های ۲۰۱۲ تا ۲۰۱۵ بوده که توسط شرکت سوفوس، به صورت سالانه و به همراه تحلیل‌های تخصصی خود و برآورد وقوع تهدیدات و نقاط آسیب‌پذیر جدید ارائه شده در سال‌های مذکور ارائه شده است. این شرکت، توصیه‌های امنیتی به منظور ارتقاء سطح امنیت فناوری اطلاعات را نیز مطرح کرده است. انتشارات دیده‌بان با تجمیع ۴ ساله گزارش‌های یادشده، آن را در قالب این کتاب گردآوری نموده است.

این نکته نیز قابل‌ذکر است که گزارش‌های ارائه‌شده توسط این شرکت بصورت جامع و با رصد کل رخدادهای امنیتی در حوزه فناوری اطلاعات در سراسر جهان نمی‌باشد و بیشتر کشورهای حوزه آمریکا را مورد پایش و بررسی قرار داده است. به عنوان مثال می‌توان به اتفاق امنیتی HeartBleed[1] در اینترنت اشاره نمود که در اوائل سال ۲۰۱۴ رخ داد (تا دو سال قبل از ۲۰۱۴، این آسیب‌پذیری روی سرورهای آژانس امنیتی ملی آمریکا وجود داشته است) و این آسیب‌پذیری موجب شد تا کل ارتباطات رمز Open SSL مورد حمله و شنود هکرها قرار گیرد. آسیب‌پذیری یادشده به اندازه‌ای عمیق و گسترده بود که امنیت بسیاری از وب‌سایت‌های بزرگی مانند یاهو، گوگل، جی‌میل، فیسبوک، توئیتر، ویرچوال‌باکس و دراپ‌باکس به خطر انداخت و به "خونریزی قلبی اینترنت" معروف شد.

اما با در نظر گرفتن کل مطالب می‌توان گفت این گزارش‌ها، با توجه به این‌که فناوری اطلاعات در تمامی کشورها و نقاط جهان رخنه کرده است و بالتبع آن آسیب‌پذیری‌ها نیز به همین منوال منتقل‌شده است، لذا تقریبا به بیشتر نقص‌های امنیتی در حوزه فناوری اطلاعات اشاره داشته است.

از جمله نکاتی که در این گزارش می‌توان به صورت اجمالی به آنها پرداخت شامل: شنود قانونی اطلاعات توسط پلیس (یا به عبارت دیگر توسط آژانس امنیت ملی آمریکا)، حضور و پیشرفت روزافزون باج‌افزارها، سرقت اطلاعات خصوصی افراد، سرقت اطلاعات افراد و سازمانها در فضای پردازش ابری، سرقت حسابهای بانکی، زنده‌شدن دوباره شبکه‌های بات‌نت به منظور ارسال پیام‌های آلوده، حملات هکری سیاسی علیه دولت‌ها مانند فلیم[2]، حضور بدافزارها در سیستم‌های عامل OS X و MAC و Unix با الگوگیری از بدافزارهای سیستم عامل ویندوز، حمله به سرورهای اینترنتی (علی‌رغم این‌که تعداد آنها نسبت به ویندوز کمتر است، اما دارای اطلاعات و ارتباطات با اهمیتری هستند)، حضور گسترده بدافزارهای اندروید، پیچیده‌ترشدن بدافزارها از لحاظ چندریختی عمل‌کرد و رمزنگاری و جلوگیری از مهندسی معکوس خود، تبلیغ محصولات شرکت سوفوس و ضعف همیشگی در ارائه راه‌حل‌های امنیتی توسط شرکت‌های تولیدکننده نرم‌افزار و از همه مهم‌تر عدم توجه کاربران به نصب این وصله‌ها می‌باشد.

همچنین راه‌حل‌های کلی نیز برای رفع اشکالات و جلوگیری از صدمه و ضربه آسیب‌پذیری‌ها در حوزه فناوری اطلاعات توسط شرکت سوفوس مطرح گردیده است.
اما مهمترین نکته‌ای که در الزامات و اقدامات امنیتی به آن اشاره شده و بارها در گزارش مورد تأکید قرار گرفته، توجیه کاربران و افراد استفاده‌کننده از فناوری اطلاعات می‌باشد و شاید بتوان گفت بزرگترین ابزاری

۱- خونریزی قلبی

2 -Flame

که می‌تواند جلوی بیشتر حملات را بگیرد، کاربر می‌باشد. چرا که اگر کاربر رمز خود را ساده انتخاب کند، یا در محیط‌های ناامن حضور پیدا کند، یا وصله‌های امنیتی را نصب نکند، یا تنظیمات امنیتی لازم را انجام ندهد، یا ضدبدافزار را غیرفعال و بروزرسانی نکند و یا... باعث بروز صدماتی می‌گردد که به هیچ عنوان ابزارهای امنیتی نمی‌توانند جلوی این حملات را بگیرند.

در هر صورت امیدواریم کاربران، مدیران، روسا، مدیران فناوری اطلاعات، مدیران امنیتی فناوری اطلاعات با مطالعه این گزارش‌ها از وضعیت آسیب‌پذیری‌های امنیتی در حوزه فناوری اطلاعات مطلع شده و در جهت ارتقاء سطح امنیت فناوری اطلاعات در حوزه اطلاعات شخصی، سازمانی، مأموریتی و غیره استفاده نمایند.