ایجاد استراتژی‌های موثر دفاع سایبری برای محافظت از سازمان‌ها

ترجمه و تالیف: بهنام عباسی وندا

سرشناسه	:	عباسی وندا، بهنام، ۱۳۷۰-
عنوان و نام پدیدآور	:	ایجاد استراتژی‌های موثر دفاع سایبری برای محافظت از سازمان‌ها/مترجم و تالیف بهنام عباسی‌وندا.
مشخصات نشر	:	تهران: موسسه آموزشی تالیفی ارشدان، ۱۳۹۸.
مشخصات ظاهری	:	۲۳۰ ص.
شابک	:	۹۷۸-۶۰۰-۹۹۵-۷۲۵-۵
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	بخش اعظم کتاب تالیف است و بخشهایی از Privileged attack vectors : building effective cyber-strategies to protect organizations defense ترجمه شده است.
موضوع	:	جنگ سایبری — Cyberspace operations (Military science)
موضوع	:	کامپیوترها -- ایمنی اطلاعات -- تدابیر ایمنی — Computer security -- Security measures
موضوع	:	شبکه‌های کامپیوتری -- تدابیر ایمنی — Computer networks -- Security measures
موضوع	:	تروریسم رایانه‌ای -- پیشگیری — Cyberterrorism -- Prevention
موضوع	:	جرایم کامپیوتری -- پیشگیری — Computer crimes -- Prevention
موضوع	:	حفاظت داده‌ها — Data protection
رده بندی کنگره	:	U۱۶۷/
رده بندی دیویی	:	۳۵۵/۰۳
شماره کتابشناسی ملی	:	۵۷۲۶۵۹

مؤسسه آموزشی تألیفی ارشدان

- نام کتاب: ایجاد استراتژیهای موثر دفاع سایبری برای محافظت از سازمانها
- ترجمه و تالیف: مهندس بهنام عباسی وندا
- ناشر: آموزشی تألیفی ارشدان
- ویرایش: اول
- نوبت چاپ: اول ۱۳۹۸
- حروفچینی و صفحه آرایی: www.irantypist.com
- طراح و گرافیست: www.irantypist.com
- شابک: ۹۷۸-۶۰۰-۹۹۵-۷۲۵-۵
- شمارگان: ۱۰۰۰
- مرکز خرید آنلاین: www.arshadan.com www.arshadan.net
- مرکز پخش و توزیع: ۰۲۱۴۷۶۲۵۵
- قیمت: ۱۷۰۰۰ تومان

پیشگفتار

در این کتاب به بررسی مدیریت دسترسی های ممتاز (PAM) پرداخته و تلاش می شود تا اقدامات دفاعی که سازمان ها باید برای محافظت در مقابل تهدیدات دسترسی های ممتاز در نظر بگیرند ارایه شود. مدیریت دسترسی های ممتاز (PAM) تحت عناوینی مانند مدیریت حساب های ممتاز و یا مدیریت هویت های ممتاز (PIM) نیز شناخته می‌شود. این موضوع زیرمجموعه‌ای از مدیریت دسترسی هویت (IAM) است که به وسیله تحلیلگران پیشروی این حوزه تعریف شده است. هدف اصلی PAM آن است تا سازمان شما را از سؤاستفاده اتفاقی یا برنامه‌ریزی شده اعتبارنامه‌های ممتاز ایمن نگه دارد، این تهدید مخصوصاً زمانی آشکار می‌شود که سازمان شما به سبب رشد، بازارهای جدید و دیگر ابتکارات توسعه‌ای کسب و کار تغییراتی را تجربه می‌کند. در این کتاب ما به بررسی این موضوع می پردازیم که چگونه هویت ها، اعتبارنامه ها، رمزهای عبور و هویت ها می توانند در طی یک حمله باعث ارتقا سطح دسترسی شوند. راهکارهای دفاعی جهت کاهش این تهدیدات به چه صورت است و در نهایت با در نظر گرفتن ریسک ها، تهدیدات، خطرات و راهکارهای نظارتی در استقرار و محدوده PAM یک برنامه ۱۲ مرحله ای برای پیاده سازی مدیریت دسترسی های ممتاز در سازمان ارایه می شود.

در ترجمه این کتاب سعی شده است تا حد امکان مطالب به صورت روان آورده شوند ولی مطمنا بی نقص نبوده و امکان وجود اشکالاتی در آن می باشد بدین جهت، از همه ی دانش پژوهان و خوانندگان عزیزی که از این کتاب استفاده می نمایند، صمیمانه تقاضامندم که نظرات خود را برای بهبود در ویرایش بعدی، عنوان نمایند.

بهنام عباسی وندا

behnam_abasi@alumni.iust.ac.ir

بهار ۹۸

فهرست مطالب

مقدمه

همان‌طور که در بسیاری از مقالات، مطالعات انجام‌شده و گزارش‌های مربوط به رخنه‌های امنیتی نشان داده شده است، اغلب حملات سایبری از بیرون سازمان‌ها نشئت می‌گیرند اگرچه ممکن است تاکتیک‌های خاص این حملات متفاوت باشد ولی مراحل مختلف حملات از بیرون مشابه هم است (شکل ۱).

۱. ابتدا شبکه هدف‌های را هک می‌کنند

مهاجمان و هکرها می‌توانند به‌طور مستقیم به این محیط نفوذ کنند ولی معمولاً ابتدا کاری می‌کنند تا کاربر به‌طور درخواسته فایل آلوده‌کننده‌ای را دانلود کند و یا حمله فیشینگی را برای آلوده کردن سیستم کاربر انجام می‌دهند و سپس پایگاهی را درون شبکه قربانی ایجاد می‌کنند. در تمام این مدت مهاجمان این کارها را به‌گونه‌ای انجام می‌دهند که اکثر سیستم‌های امنیتی متوجه حملات نمی‌شوند.

۲. سپس اتصالی را ایجاد می‌کنند

مهاجم به‌سرعت اتصالی را به یک سرور فرمان و کنترل (C&C[1]) برای دانلود جعبه‌ابزارها[2]، کدهای مخرب و همچنین دریافت دستورالعمل‌های اضافی ایجاد می‌کند، البته به‌جز در مواردی که باج‌افزار یا بدافزارهای خودکار و کاملی را اجرا کرده باشد.

---

[1] Commond and Control
[2] toolkits

نکته: حملات مهندسی اجتماعی در ۴۳٪ از نقض‌های امنیتی گزارش شده و موجود در پایگاه داده شرکت Verizon در سال ۲۰۱۷ مورد استفاده قرار گرفته‌اند. تقریباً تمامی حملات فیشینگ که به رخنه‌ای ختم شدند با انواع بدافزارها همراه بودند که ۲۸٪ از این رخنه‌ها مربوط به حملات فیشینگ است. فیشینگ معمول‌ترین تاکتیک مهندسی اجتماعی در پایگاه داده DBIR شرکت Verizon است.

۳. مهاجم وارد شبکه شده است و وارد عمل می‌شود

مهاجمان شروع به جمع‌آوری اطلاعات درباره شبکه، معماری و دارایی‌های آن می‌کنند سپس به دیگر سیستم‌ها رفته و به دنبال فرصت‌هایی برای جمع‌آوری اعتبارنامه‌های[1] بیشتر و ارتقاء حقوق ویژه هستند و یا تنها از حقوقی استفاده می‌کنند که برای دسترسی به سیستم‌ها، برنامه‌ها و داده‌های آلوده به کار برده‌اند. دقت شود که افراد درون‌سازمانی هم می‌توانند یک مهاجم باشند و اگر امتیاز، دسترسی ویژه‌ای را داشته باشند، می‌توانند مستقیما مرحله چهارم را اجرا کنند.

[1] Credentials