

ایجاد استراتژی‌های موثر دفاع سایبری برای محافظت از سازمان‌ها

۲۰۳۹۴۰۵

ترجمه و تالیف: بهنام عباسی و ندا

سرشناسه	:	عباسی وندا، بهنام، ۱۳۷۰-
عنوان و نام پدیدآور	:	ایجاد استراتژی‌های موثر دفاع سایبری برای محافظت از سازمان‌ها/مترجم و تالیف بهنام عباسی وندا.
مشخصات نشر	:	تهران: موسسه آموزشی تألیفی 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	:	U۱۶۷/۸
رده بندی دیویی	:	۳۰۵/۱۳۳
شماره کتابشناسی ملی	:	۵۷۲ ۶۵۹

ارشدان

مؤسسه آموزشی تألیفی ارشدان

ایجاد استراتژی‌های موثر دفاع سایبری برای محافظت از سازمانها

مهندس بهنام عباسی وندا

آموزشی تألیفی ارشدان

اول

اول ۱۳۹۸

www.irantypist.com

www.irantypist.com

۹۷۸-۶۰۰-۹۹۵-۷۲۵-۵

۱۰۰۰

www.arshadan.com

www.arshadan.net

۰۲۱۴۷۶۲۵۵

۱۷۰۰۰ تومان

■ نام کتاب:

■ ترجمه و تالیف:

■ ناشر:

■ ویرایش:

■ نوبت چاپ:

■ حروفچینی و صفحه آرایی:

■ طراح و گرافیکست:

■ شابک:

■ شمارگان:

■ مرکز خرید آنلاین:

■ مرکز پخش و توزیع:

■ قیمت:

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 ارائه شود. مدیریت دسترسی های ممتاز (PAM) تحت عناوینی مانند مدیریت حساب های ممتاز و یا مدیریت هویت های ممتاز (PIM) نیز شناخته می شود. این موضوع زیرمجموعه ای 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 سوءاستفاده اتفاقی یا برنامه ریزی شده اعتبارنامه های ممتاز ایمن نگه دارد، این تهدید مخصوصاً زمانی آشکار می شود که سازمان شما به سبب رشد، بازارهای جدید و دیگر ابتکارات توسعه ای کسب و کار تغییراتی را تجربه می کند. در این کتاب ما به بررسی این موضوع می پردازیم که چگونه هویت ها، اعتبارنامه ها، رمزهای عبور و دسترسی 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، تفرقات و راهکارهای نظارتی در استقرار و محدوده PAM یک برنامه ۱۲ مرحله ای برای پیاده سازی مدیریت دسترسی های ممتاز در سازمان ارائه می شود.

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

بهنام عباسی وندا

behnam_abasi@alumni.iust.ac.ir

بهار ۹۸

فهرست مطالب

۱۲	 مقدمه
۱۵	 کاراکترهای تهدید
۲۰	 فصل ۱: حقوق ویژه
۲۲	 کاربران مهمان
۲۲	 کاربران استاندارد
۲۷	 مدیران
۲۷	 مدیریت هویت
۲۹	 هویت‌ها
۲۹	 حساب‌ها
۳۰	 اعتبارنامه‌ها
۳۱	 اعتبارنامه‌های پیش‌فرض
۳۲	 دسترسی ناشناس
۳۳	 رمز عبور خالی
۳۴	 رمز عبور پیش‌فرض
۳۶	 رمز عبور تصادفی پیش‌فرض
۳۷	 رمز عبور تولیدی پیش‌فرض
۳۹	 شرکت‌های ثالث
۴۲	 فصل ۲: اعتبارنامه‌های اشتراکی کاربر
۴۳	 اعتبارنامه‌های حساب کاربری
۴۴	 اعتبارنامه‌های اشتراکی مدیر
۴۶	 حساب‌های موقت
۴۷	 رمز عبورهای شخصی و کاری
۴۷	 برنامه‌ها
۴۹	 دستگاه‌ها
۵۱	 نام‌های مستعار
۵۳	 SSH کلیدهای

۵۵	فصل ۳: هک کردن رمز عبور
۵۵	حدس زدن
۵۶	ایستادن کنار قربانی
۵۷	حملات با استفاده از فرهنگ لغات
۵۸	حمله جستجوی فراگیر
۵۹	پاس کردن هش
۵۹	سوالات امنیتی
۶۱	تنظیم مجدد رمزهای عبور
۶۵	فصل ۴: احراز هویت بدون رمز عبور
۷۰	فصل ۵: ارتقاء حق ویژه
۷۱	رمزهای عبور
۷۲	آسیب پذیری ها
۷۶	پیکربندی ها
۷۶	اکسپلویت ها
۷۷	بدافزارها
۷۸	مهندسی اجتماعی
۸۱	احراز هویت چند مرحله ای
۸۳	حقوق ویژه محلی در برابر حقوق ویژه متمرکز
۸۵	فصل ۶: تهدیدهای داخلی و درون سازمانی
۹۰	فصل ۷: شکار تهدید
۹۴	فصل ۸: بازرسی و حفاظت داده محور
۹۸	فصل ۹: نظارت بر حقوق ویژه
۹۸	ضبط نشست
۱۰۱	ثبت کلیدهای فشرده شده
۱۰۲	نظارت بر ایلکیشن
۱۰۵	فصل ۱۰: مدیریت دسترسی های ممتاز
۱۰۷	چالش های PAM
۱۱۰	مدیریت رمز عبور
۱۱۱	مدیریت حقوق ویژه حداقلی

۱۱۲.....	خودکار سازی حقوق ویژه اپلیکیشن به اپلیکیشن
۱۱۴.....	مدیریت کلید SSH
۱۱۵.....	پل زدن بین دایرکتوری‌ها
۱۱۶.....	حسابرسی و گزارش
۱۱۷.....	تحلیل تهدیدات حقوق ویژه
۱۱۹.....	فصل ۱۱: معماری مدیریت دسترسی‌های ممتاز (PAM)
۱۲۵.....	درون محیطی
۱۲۵.....	ابر
۱۲۶.....	زیرساخت به عنوان سرویس (IAAS)
۱۲۷.....	نرم‌افزار به عنوان سرویس (SAAS)
۱۲۸.....	فصل ۱۲: BREAK GLASS
۱۲۹.....	فرآیند BREAK GLASS
۱۳۰.....	BREAK GLASS با استفاده از نرم‌افزار مدیریت رمز عبور
۱۳۲.....	مدیریت نشست
۱۳۳.....	رمزهای عبور قدیمی
۱۳۴.....	رمزهای عبور اپلیکیشن به اپلیکیشن
۱۳۵.....	فضای ذخیره‌ساز فیزیکی رمز عبور
۱۳۶.....	آگاهی از زمینه
۱۳۶.....	معماری
۱۳۷.....	بازبایی BREAK GLASS
۱۳۹.....	فصل ۱۳: سیستم‌های کنترل صنعتی (ICS)
۱۴۵.....	فصل ۱۴: اینترنت اشیاء (IOT)
۱۴۹.....	فصل ۱۵: فضای ابری
۱۵۰.....	نیروی کار سیار
۱۵۲.....	فناوری اطلاعات توزیع شده
۱۵۳.....	همکاری فناوری اطلاعات
۱۵۶.....	مدل‌های فضای ابری
۱۵۷.....	زیرساخت به عنوان سرویس (IAAS)
۱۵۸.....	نرم‌افزار به عنوان سرویس (SAAS)
۱۶۰.....	پلتفرم به عنوان سرویس (PAAS)

فصل ۱۶: دستگاه‌های موبایل.....	۱۶۱
فصل ۱۷: باج‌افزارها.....	۱۶۶
فصل ۱۸: عملیات توسعه‌ای امن (SDEVOPS).....	۱۶۹
فصل ۱۹: سازگاری با قوانین.....	۱۷۲
صنعت کارت پرداخت (PCI).....	۱۷۳
HIPAA.....	۱۷۵
SOX.....	۱۷۷
GLBA.....	۱۷۸
NIST.....	۱۷۹
ISO.....	۱۸۰
ASD.....	۱۸۴
MAS.....	۱۸۵
GDPR.....	۱۸۶
SWIFT.....	۱۸۷
فصل ۲۰: نمونه کاربردهای مدیریت دسترسی‌های ممتاز (PAM).....	۱۹۰
فصل ۲۱: ملاحظات اجرایی.....	۲۰۲
اولویت‌بندی ریسک.....	۲۰۲
بررسی اعتبارنامه‌های ممتاز.....	۲۰۳
اشتراک گذاری حساب.....	۲۰۴
اعتبارنامه‌های تعبیه‌شده.....	۲۰۴
کلیدهای SSH.....	۲۰۵
اعتبارنامه‌های ممتاز در فضای ابری.....	۲۰۵
برنامه‌ها.....	۲۰۶
حساب‌های فروشنده‌ها و دسترسی از راه دور.....	۲۰۷
فصل ۲۲: پیاده‌سازی مدیریت حسابهای ممتاز.....	۲۰۸
گام ۱: بهبود مسئولیت‌پذیری برای رمزهای عبور ممتاز.....	۲۰۹
گام ۲: پیاده‌سازی حقوق ویژه حداقلی در دستکاپ‌ها.....	۲۱۱
گام ۳: بهره‌مندی از سطوح ریسک اپلیکیشن.....	۲۱۲
گام ۴: پیاده‌سازی حقوق ویژه حداقلی در سرورها.....	۲۱۳

۲۱۵.....	گام ۵: تجهیزات شبکه
۲۱۶.....	گام ۶: مراکز داده مجازی و ابری
۲۱۸.....	گام ۷: دستگاه‌های اینترنت اشیاء
۲۱۸.....	گام ۸: عملیات توسعه‌ای (DEVOPS)
۲۲۰.....	گام ۹: یکپارچه‌سازی مدیریت
۲۲۱.....	گام ۱۰: یکپارچه‌سازی حساب‌های ممتاز
۲۲۲.....	گام ۱۱: حسابرسی و بازیابی
۲۲۴.....	گام ۱۲: به‌کارگیری پشته هویت
۲۲۵.....	فصل ۲۳: نکات کلیدی
۲۲۹.....	فصل ۲۴: نتیجه‌گیری
۲۲۹.....	PAM یک لایه امنیتی است
۲۲۹.....	ساده‌سازی PAM
۲۳۰.....	سازگاری به‌عنوان یک معیار
۲۳۰.....	سیاست پویا
۲۳۰.....	تحلیل‌های پیشگیرانه

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 اکتیک‌های خاص این حملات متفاوت باشد ولی مراحل مختلف حملات از بیرون مشابه هم است (شکل ۱).

۱. ابتدا شبکه میزبان را هدف می‌کنند

مهاجمان و هکرها می‌توانند به‌طور مستقیم به این محیط نفوذ کنند ولی معمولاً ابتدا کاری می‌کنند تا کاربر به‌طور ناخواسته عامل آلوده‌کننده‌ای را دانلود کند و یا حمله فیشینگ 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 اتصالاتی را ایجاد می‌کنند

مهاجم به‌سرعت اتصالاتی را به یک سرور فرمان و کنترل^۱ (C&C) برای دانلود جعبه‌ابزارها^۲، کدهای مخرب و همچنین دریافت دستورالعمل‌های اضافی ایجاد می‌کند، البته به‌جز در مواردی که باج‌افزار یا بدافزارهای خودکار و کاملی را اجرا کرده باشند.

¹Command and Control

²toolkits

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^۱ بیشتر و ارتقاء حقوق ویژه هستند و با تنها از حقوقی استفاده می‌کنند که برای دسترسی به سیستم‌ها، برنامه‌ها و داده‌های الوده^۲ کار برده‌اند. دقت شود که افراد درون سازمانی هم می‌توانند یک مهاجم باشند و اگر امکان دسترسی ویژه‌ای را داشته باشند، می‌توانند مستقیماً مرحله چهارم را اجرا کنند.

^۱Credentials