ایجاد استراتژی های موثر دفاع سایبری برای محافظت از سازمان ها

ترجمه و تالیف:
بهنام عباسی وندا

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	:	U۱۶۷/۵
رده بندی دیویی	:	۳۵۵/۳۴۳
شماره کتابشناسی ملی	:	۵۷۲۳۶۵۹

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

تقدیم به:

پدرم با بوسه بر دستانش که وجودش مایه دلگرمی‌ام است و مادرم، بلندترین تکیه‌گاهم که دلمان پر مهرش یگانه پناهم است.

و تقدیم به:

همسر عزیزم به پاس قدردانی از قلبی آکنده از عشق، کسی که مسیح‌وار با صبرش در تمام لحظات رفیق راهم بود.

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 اکسپلویت 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، مقررات 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 محیطی را هک 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 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[1] (C&C) 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.

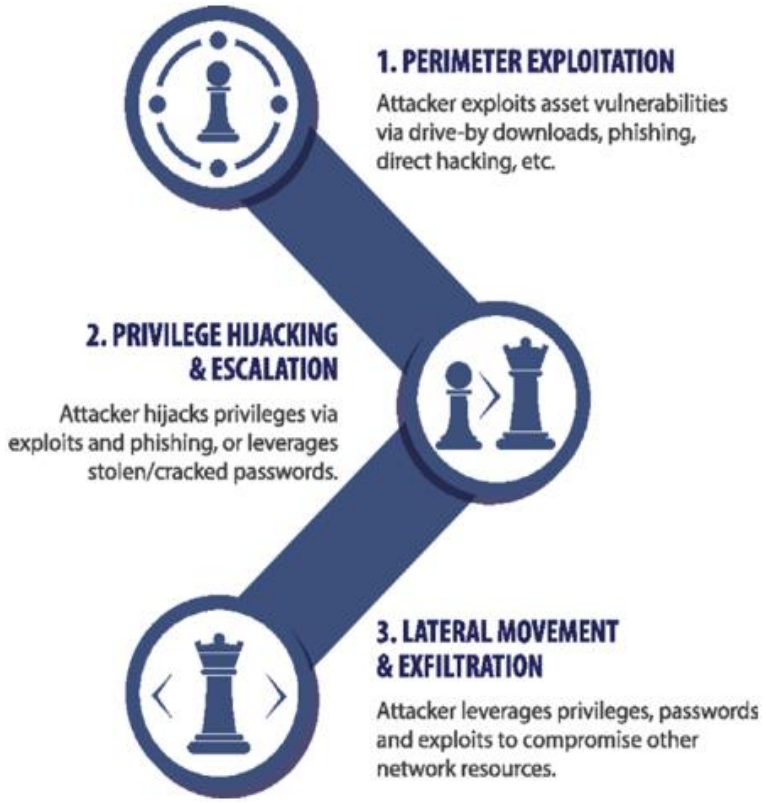
[1] Commond and Control
[2] toolkits

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 امتیازهای دسترسی ویژه‌ای را داشته باشند، می‌توانند مستقیما مرحله چهارم را اجرا کنند.

[1] Credentials



شکل ۱. مراحل یک حمله از بیرون سازمان

اکسپلویت کردن شبکه محیطی، مهاجم آسیب‌پذیری دارایی‌ها را با استفاده از دانلودهای ناخواسته، حمله فیشینگ، هک کردن مستقیم و غیره اکسپلویت می‌کند.
ربودن و ارتقاء حقوق ویژه، مهاجم ازطریق اکسپلویت کردن وحمله فیشینگ، حقوق ویژه را می‌رباید ویا از رمزهای عبور دزدیده‌شده یا کِرَک‌شده بهره‌می‌برد.
اقدامات بعدی و برداشت اطلاعات، مهاجم از حقوق ویژه، رمزهای عبورها و اکسپلویت‌ها بهره می‌برد تا دیگر منابع شبکه را آلوده کند.

۴. پایان مأموریت

در آخر، مهاجم داده‌ها را جمع‌آوری و دسته‌بندی کرده و نهایتاً آن‌ها را برداشت می‌کند و یا در بدترین حالت، منابع اطلاعاتی را تخریب می‌نماید.

یک محصول امنیتی، قطعاً به‌تنهایی حفاظت کامل و موردنیاز شما را در برابر تمام مراحل حمله ارائه نمی‌کند. با وجود اینکه برخی از راهکارهای جدید و نوآورانه به حفاظت و یا شناسایی اولیه آلودگی کمک می‌کنند ولی به‌طور ۱۰۰٪ توقف یک فعالیت مخرب را تضمین نمی‌کنند. درواقع، این موضوع زمانی اهمیت پیدا می‌کند که این رخنه‌ها به‌طور موفقیت‌آمیزی مورد استفاده و حمله قرار گیرند. شما باید موارد پایه‌ای مانند وصله کردن[۱]، تنظیم دیواره‌های آتش[۲]، استفاده از آنتی‌ویروس‌ها برای نقاط انتهایی و شناسایی تهدید را رعایت کنید. همچنین باید حقوق ویژه دسترسی در محیط را محافظت و کنترل کرده و مورد بازرسی قرار دهید. مدیریت درست حقوق ویژه می‌تواند در تمام مراحل حمله، کمک‌کننده باشد. این کتاب از کاهش سطح حملات گرفته تا شناسایی و حفاظت در برابر نفوذ و فعالیت‌های پس از آن می‌پردازد، همچنین سعی در پاسخ و کاهش تأثیر نفوذ دارد و به بررسی این امر می‌پردازد که آسیب‌پذیری‌های حقوق ویژه در چه نقاطی از سازمان قرار دارند، مهاجمان چطور می‌توانند از آن‌ها بهره‌ببرند و مهم‌تر از همه اینکه شما چه اقداماتی را می‌توانید برای آن‌ها انجام دهید.

کاراکترهای[۳] تهدید

قبل از اینکه وارد جزئیات و بحث حقوق ویژه شویم، کمی به این موضوع می‌پردازیم که ما از خود در برابر چه کسانی محافظت می‌کنیم! باید در نظر داشت که نقطه آغاز و مبدأ حملات می‌تواند از درون یا بیرون سازمان باشد. این حملات ممکن است فرصت‌طلبانه بوده و یا حملاتی باشند که کاملاً با برنامه و به صورت هدفمند توسط فرد و یا گروهی از افراد انجام می‌گیرند. به‌منظور طبقه‌بندی آن‌ها بر اساس انگیزه‌ها و تاکتیک‌ها می‌توانیم آن‌ها را به‌صورت هکتیویست‌ها[۴]، تروریست‌ها، جاسوسان صنعتی، هکرهای حکومتی و یا به صورت هکرهای ساده دسته‌بندی کنیم. تفاوت اندکی بین یک هکر[۵]، مهاجم[۶]، عامل تهدید[۷] وجود دارد. اکثر اوقات، افراد حرفه‌ای حوزه امنیت این عبارات را به‌جای هم و با تمایز کمی بین تعاریف آن‌ها به کار می‌برند. ما به‌عنوان حرفه‌ای‌های حوزه امنیت، رخنه‌های امنیتی جدید را مورد مطالعه

[1] Patching
[2] Firewalls
[3] Personas
[4] Hacktivists
[5] Hacker
[6] Attacker
[7] Threat Actor

قرارداده، تحقیقات قانونی را انجام می‌دهیم و آن‌هایی که از این رخنه‌ها استفاده می کنند را ناکام می‌گذاریم. کمتر اتفاق می‌افتد که بزرگ‌ترین نفوذهای امنیتی، حل‌نشده باقی بمانند ولی بسته به قوانین استرداد مجرمین و اینکه دولتی در این کار دست دارد یا خیر، تحت تعقیب قرار دادن آن‌ها ممکن است چندین سال طول بکشد. در طی این مدت ما در مورد رویدادها، حوادث امنیتی و رخنه‌ها آگاهی پیدا می‌کنیم و متوجه می‌شویم که آیا این کار به‌وسیله عامل تهدید، هکر و یا حتی مهاجمی که فعالیت‌های مخربی را صورت داده است، انجام گرفته یا خیر؟

سؤال اینجاست که: تفاوت این کاراکترهای تهدید در چیست و آیا همه آن‌ها به یک معنا نیستند؟ حقیقت امر آن است که این مفاهیم یکسان نیستند و اکثر اوقات در گزارش یک رخنه یا حادثه امنیتی سایبری به‌صورت اشتباه به کار می‌روند. تعاریف معمول برای هر یک از کاراکترهای تهدید به صورت زیر است:

- **عامل تهدید**: طبق تعریف شرکت TechTarget، «عامل تهدیدکه عامل خرابکاری نیز نامیده می‌شود، فرد یا گروهی است که تا حدودی و یا به‌صورت کامل مسئول حادثه‌ای است که امنیت یک سازمان را تحت تأثیر قرار می‌دهد و یا پتانسیل انجام این کار را دارد.»
- **هکر:** طبق تعریف فرهنگ لغت Merriam-Webster، «هکر شخصی است که به صورت غیرقانونی دسترسی به یک سیستم کامپیوتری را به دست آورده و برخی اوقات اطلاعات موجود در آن سیستم کامپیوتری را تغییر می‌دهد.»
- **مهاجم**: در امنیت سایبری، یک مهاجم در واقع فرد، سازمان یا بدافزار مدیریت‌شده-ای است که سعی در تخریب، افشا، تغییر، غیر فعال‌سازی، مسدودسازی سرویس ها، سرقت یا به‌دست آوردن دسترسی غیرمجاز به منابع، دارایی‌ها یا داده‌ها را دارد.

همان‌طور که دیده می‌شود، تعریف جامع پذیرفته‌شده‌ای برای یک مهاجم وجود ندارد و به همین دلیل است که اکثر اوقات این کاراکترها به‌جای یکدیگر در خبرها آورده می‌شوند.

بر اساس این تعاریف،ممکن است هر رخنه یا حادثه‌ای به‌وسیله هریک از این سه طرف، مورد استفاده قرار گرفته و اجرا شود. برای صحبت در مورد حقوق ویژه به‌عنوان اهدافی برای

تهدیدات سایبری، به بیان تمایزی میان آن‌ها نیاز داریم زیرا تفکیک‌پذیری این روش برای هریک از آن‌ها متفاوت است.

عامل تهدید درمقایسه با یک هکر یا مهاجم الزاماً مجموعه مهارت‌های فنی را ندارد (جدول ۱). فرد یا سازمانی بداندیش که مأموریتی برای آلوده‌سازی داده‌های یک سازمان و تحت تاثیر قراردادن امنیت آن دارد، در این دسته قرار می‌گیرد. این مأموریت می‌تواند از تخریب فیزیکی گرفته تا کپی اطلاعات حساس باشد. این واژه (عامل تهدید) عبارت گسترده‌ای است که می‌توان آن را برای تهدیدات خارجی و داخلی و مأموریت‌های آن‌ها مانند هکتیویسم به کار برد.

جدول ۱. مثال‌هایی از عامل تهدید

عامل تهدید	مثال
بیرونی	حکومتی فعال سیاسی جرم‌های سازمان‌یافته سازمان تروریستی
درونی	مدیران توسعه‌دهندگان کاربران سیستم مالکان داده پیمانکاران شرکت‌های ثالث مورد اعتماد

هکرها و مهاجمان، کاربران فنی یا تیم‌های سازمان یافته ای هستند که برخی از فناوری‌ها را مورد هدف قرار می‌دهند و امیدوارند تا رخنه‌ای در آن بیابند. افراد، گروه‌ها یا حتی دولت‌ها با اهداف و مأموریت‌هایی از هر کجای جهان می‌توانند در این دسته قرار گیرند. اهداف آن‌ها می‌تواند بی‌ثبات کردن سازمان‌ها و دولت‌ها، انتشار اطلاعات آن‌ها و یا منافع مالی باشد.

به‌هرحال تفاوت بین یک مهاجم و هکر بسیار ظریف است. هکرها به‌طورمعمول از آسیب‌پذیری‌ها و اکسپلویت‌ها برای انجام فعالیت‌های خود استفاده می‌کنند که نتایج آن

می‌تواند تخریب و یا تنها در جهت کنجکاوی باشد. مهاجمان می‌توانند از ابزارهای موردنیاز برای اجرای فعالیت‌های ویرانگر خود استفاده کنند، برای مثال مهاجم می‌تواند از افراد ناراضی درون سازمان باشد که فایل‌های حساسی را حذف می‌کند و یا به هر وسیله‌ای در کسب‌وکار سازمان اختلال ایجاد می‌نماید تا به اهدافش برسد. دقت کنید که چون این افراد درون‌سازمانی به داده‌ها و سیستم‌های هدف دسترسی دارند، می‌توانند به‌سادگی از دسترسی خود برای انجام و حصول اهدافشان استفاده کنند. هکر می‌تواند کاری مشابه با آن‌ها را انجام دهد ولی آن‌ها از آسیب‌پذیری‌ها، اعتبارنامه‌های دزدیده‌شده، اکسپلویت‌ها و پیکربندی‌های ضعیف و اشتباه برای آلوده ساختن منبعی استفاده می‌کنند تا دسترسی لازم را پیدا نموده و مأموریت خود را تکمیل نمایند.

تفاوت بین این سه حوزه بسیار مهم است به همین جهت راهکارهای امنیتی برای حفاظت در برابر انواع سه‌گانه کاربران مخرب طراحی شده است و نتایج آن برای هر سازمانی متفاوت است:

- به‌منظور دفاع در برابر عاملان تهدید، راهکارهای مدیریت دسترسی ویژه[1] (PAM) می‌توانند دسترسی‌های ویژه را مدیریت کنند، تمام فعالیت‌ها را به شکل نشست‌ها[2] یا کلیدهای فشرده‌شده ثبت کنند و برنامه‌ها را مورد نظارت قرار دهند تا تضمین کندکه عامل تهدید، دسترسی نامناسبی به دست نیاورده و تمام نشست‌ها را به‌محض وقوع مستند می‌کند (تهدیدات درونی)؛
- به‌منظور دفاع در برابر هکر، راهکارهای مدیریت آسیب‌پذیری (VM) برای تشخیص آسیب‌پذیری‌هایی مانند وصله‌های اعمال‌نشده، رمز عبورهای ضعیف یا پیکربندی‌های ناامن در تمام سیستم‌عامل‌ها، برنامه‌ها و زیرساخت‌ها طراحی شده‌اند تا تضمین نمایند که می‌توان این آسیب‌پذیری‌ها را به‌موقع رفع نمود. اینکار راه‌های نفوذی را که یک هکر می‌تواند برای آلوده کردن محیط مورد استفاده قرار دهد، می‌بندد و با انجام به‌موقع وصله‌سازی سعی در تداوم کسب‌وکار سازمان دارد. راهکارهای شناسایی آسیب‌پذیری به سازمان‌ها کمک می‌کند تا ریسک مربوط به این آسیب‌پذیری‌ها را

[1]Privilaged Access Management
[2]Session

اندازه بگیرند و فعالیت‌های امن‌سازی و وصله کردن را مطابق با اندازه و سطح آسیب-پذیری‌ها، اولویت‌بندی نمایند و بدین صورت تاثیر حمله را تا حد امکان و به‌صورت خیلی سریع و مؤثر کاهش دهند؛

- به‌منظور دفاع در برابر مهاجم، راهکارهای حداقل حقوق ویژه و راهکارهای جلوگیری از نفوذ به شبکه و سیستم‌های میزبان را می‌توان با حذف سطح دسترسی که عاملان تهدید به منابع دارند، اجرا کرد و تأثیر این حملات را کاهش داد. اینکار شامل حذف حقوق غیرضروری مدیر[1] (روت[2]) به برنامه‌ها و سیستم‌های‌عامل است. این راهکارها می‌توانند حسابرسی از دسترسی و رفتارها را با جزئیات بیشتری اجرا کنند تا حساب‌های آلوده و حقوق ویژه نادرست را تشخیص دهند.

ترکیبی از این راهکارها نه‌تنها می‌تواند مانع از حملات بیرونی شود بلکه حقوق ویژه تخصیص یافته به دارایی‌ها و کاربران را نیز محدود می‌کند و بنابراین اقدامات بعدی آن‌ها را مهار می‌نماید. این کار مبنای حفاظت در برابر اهداف حمله دارای حقوق ویژه است و به‌طور دقیق در فصول بعدی مورد بحث قرار می‌گیرد.

به‌هرحال، ابتدا مروری بر عناصر پایه‌ای داشته و سپس سیستم دفاعی خود را تنظیم می‌کنیم و بهترین روش‌ها و اقدامات امنیتی را مورد بررسی قرار می‌دهیم. جدای از انگیزه‌های مالی، هکتیویسم‌ها و خرابکارهای دولتی همیشه مسیر با کمترین دشواری را برای انجام فعالیت‌های مخرب خود انتخاب می‌کنند، درحالی‌که ممکن است این مسیر هرازگاهی نشانه‌های آشکاری را برای مراجع قانونی بر جای بگذارد ولی هنر هک کردن آن است که خرابکاری (در صورت امکان) بدون شناسایی و گذاشتن ردی انجام گیرد و همیشه این فعالیت‌های مخرب به دور از چشم سیستم‌های دفاعی امنیتی باشد. مهاجمان مانند اغلب مردم، مسیری با کمترین دشواری را انتخاب می‌کنند. خوشبختانه روش‌های دستیابی به حقوق ویژه کاربر و اپلیکیشن به سبب حملات و اکسپلویت‌های متنوع به‌خوبی شناخته‌شده هستند. این کتاب به بررسی این قابلیت‌ها و سیستم‌های دفاعی محتمل می‌پردازد به‌گونه‌ای که این حقوق ویژه به اهداف حمله موفقی برای یک عامل تهدید درون‌سازمانی تبدیل نشود. به‌طورمعمول این کار مدیریت دسترسی ویژه (PAM) نام دارد.

[1] Administrator Rights
[2] Root

فصل ۱

حقوق ویژه

امروزه، حقوق ویژه مبتنی بر اعتبارنامه‌ها یکی از دست‌یافتنی‌ترین موارد در زنجیره حمله هستند. تهدیدات شامل موارد زیر است:

۱. افراد درون‌سازمانی که دسترسی اضافی و نظارت‌نشده‌ای به حساب‌ها دارند و راه را برای سوءاستفاده باز می‌کنند؛
۲. افراد درون‌سازمانی که حساب‌های آن‌ها از طریق حملات فیشینگ ، مهندسی اجتماعی و یا دیگر تاکتیک‌ها آلوده شده است؛
۳. حساب‌هایی که به دلیل اعتبارنامه‌ها، رمزها، ابزارها و اپلیکیشن‌های ضعیف تحت تأثیر قرار گرفته و به مهاجمان اجازه می‌دهند تا سیستم‌ها را آلوده سازند و حقوق ویژه‌ای را برای فعالیت‌های مخرب به دست آورند.

نکته:گزارش نفوذ به داده‌ها از شرکت Verizon در سال ۲۰۱۷ نشان داد که ۸۱٪ از نفوذهای خارجی صورت‌گرفته به سازمان‌ها از رمزهای عبور دزدیده‌شده و ضعیف بهره برده‌اند.

برای درک اینکه چطور می‌توان حقوق ویژه را به‌عنوان اهداف موفقیت‌آمیز حمله به کار برد، تعریف روشنی از حقوق ویژه را باید معرفی نمود. مطابق با یک تعریف پایه، حق ویژه، حقی خاص یا یک مزیت است که این حق یا مزیت بالاتر از حد نرمال بوده و حالت و مجوزی نیست که به عموم داده شود و مثالی از آن، تحصیل است. «تحصیل یک حق است ولی یک حق ویژه

نیست.»[1] هرکسی حق تحصیل دارد پس هر کاربر استاندارد، حقوقی یکسان با سایر کاربران استاندارد در سازمان دارد. تیم فناوری اطلاعات، برای تمام کاربران معتبر و احرازشده،حقوقی در نظر می‌گیرد که به‌صورت سراسری و کلی تعریف شده است. به محض اینکه این حساب‌های کاربری تدارک دیده می‌شوند، این حقوق استاندارد به آن‌ها اعطا می‌شود. این امر می‌تواند دسترسی پایه به کیبورد و موس، مرورگر اینترنت و یا حتی ایمیل باشد. کاربری با حقوق ویژه، دارای حقوقی فراتر از این موارد است و این حق می‌تواند توانایی نصب نرم‌افزارها و یا تنها تغییر ویژگی‌های تنظیماتی باشد و یا اینکه اجرای دیگر وظایف روتین نگهداری مانند مدیریت محتواهای پشتیبان باشد. این امر بدین معنا نیست که آن‌ها مدیر هستند بلکه یعنی حقوق ویژه‌ای به آن‌ها داده شده است و در سطحی بالاتر از کاربران استاندارد قرار گرفته‌اند. این سطح‌بندی ویژگی‌ها می‌تواند وابسته به نیازهای سازمان باشد که پایه‌ای‌ترین آن‌ها عبارت‌اند از:

۱. **کاربر استاندارد**: حقوق مشترکی که به تمام کاربران برای انجام وظایف اعطا می‌شود؛
۲. **مدیر**[2]: مجموعه گسترده‌ای از حقوق ویژه که برای مدیریت تمام جنبه‌های یک سیستم و منابع آن اعطا می‌شود که این موارد شامل نصب نرم‌افزار، مدیریت تنظیمات پیکربندی، اعمال وصله‌ها، مدیریت کاربران و غیره است.

اما ممکن است برخی از سازمان‌ها حقوق ویژه را به چهار سطح پایه تقسیم‌بندی نمایند:

۱. **بدون دسترسی**: این یعنی شما حساب کاربری ندارید و یا حساب شما غیرفعال شده یا پاک گردیده است و بدین معناست که هر نوع دسترسی ویژه حتی به‌صورت ناشناس[3]، مسدود شده باشد؛
۲. **مهمان:** دسترسی محدود و حقوقی کمتر از کاربر استاندارد دارد. اکثر اوقات این سطح همراه با دسترسی ناشناس است؛
۳. **کاربر استاندارد**: حقوق مشترکی که به تمام کاربران اعطا می‌شود؛

[1] http://www.globalpartnership.org/blog/education-right-not-privilege
[2] Administrator
[3] Anonymously

۴. **مدیر**: دارای حق امتیاز برای ایجاد تغییرات در پیکربندی‌ها، تنظیمات، مدیریت کاربران، دارایی‌ها، نصب نرم‌افزار و وصله‌سازی است. این سطح را می‌توان به حقوق مدیر محلی (local administrator) و حقوق مدیریت دامنه (domain administrative)تقسیم‌بندی کرد تا بر بیش از یک منبع تأثیر بگذارد.

درحالی‌که این چشم‌انداز از حقوق ویژه در سطح کلانی از کاربر است ولی درک سطح کلانی از مجوزها برای رسیدن به جزئیات در جهت تعیین سیستم دفاعی مناسب مهم است. درست نیست که حقوق ویژه را تنها بخشی از اپلیکیشنی که اجرا می‌شود در نظر بگیریم بلکه حقوق ویژه را باید درون سیستم‌عامل، فایل‌های سیستمی، اپلیکیشن، پایگاه‌داده، هایپروایزور[1]، پلتفرم مدیریت ابر و حتی شبکه همراه با تقسیم‌بندی در نظر گرفت تا برای ارتباطات کاربر و ارتباطات اپلیکیشن با اپلیکیشن مؤثر واقع شود. این امر زمانی صحیح است که احراز هویت به‌وسیله مکانیزمی با یک نام کاربری و رمز یا یک کلید گواهینامه[2]و یا هر دو اعطا شود. تحقق حقوق ویژه تنها در یک لایه واقعاً نمی‌تواند مؤثر باشد؛ بنابراین نگاهی عمیق‌تر به این مسئله خواهیم داشت.

کاربران مهمان

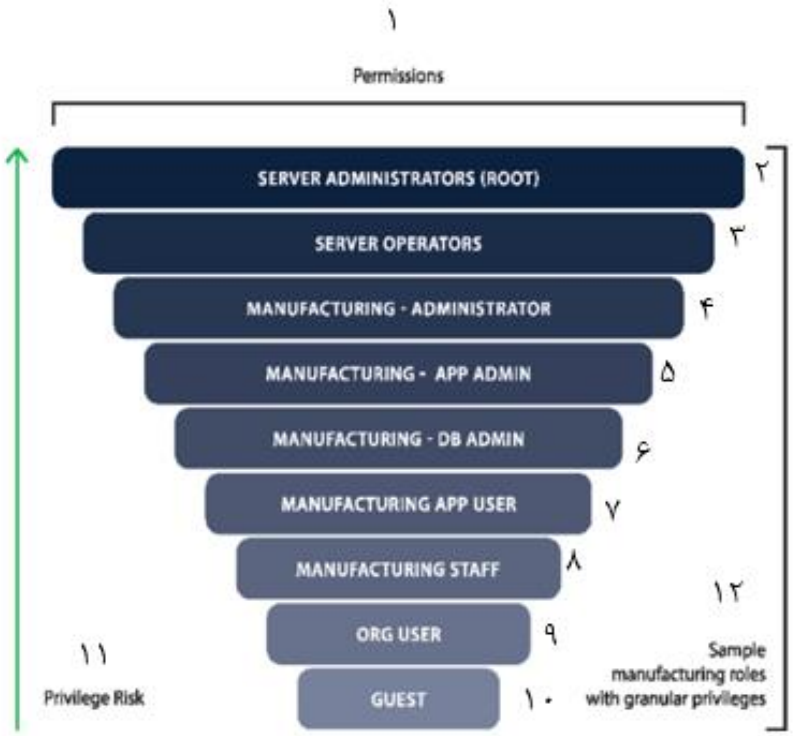
به‌عنوان کاربر مهمان، حقوق ویژه شما به‌طور سخت‌گیرانه‌ای به عملکردها و وظایف خاصی محدود شده است. در سازمان‌های زیادی، مهمان‌ها به قسمت‌های ایزوله‌شده‌ای از شبکه با دسترسی پایه محدود هستند که احتمالاً دسترسی به اینترنت است. اگر این کامپیوترهای مدیریت‌نشده، آلوده باشند و یا آلوده شوند، ریسک آن با دسترسی محدود به منابع سازمان، محدود است. برای مثال، پویش شبکه[3] از سوی ماشین آلوده مهمان، دسترسی مستقیمی را به مهاجم برای رسیدن به سیستم‌ها و داده‌های سازمان نمی‌دهد (حداقل نباید بدهد).

کاربران استاندارد

به‌عنوان کاربر استاندارد، حق امتیازهایی فراتر از کاربر مهمان برای اجرای وظایف و تحقق مأموریت‌هایی دارید که موردنیاز عملکرد یک وظیفه خاص است. با وجودی که ممکن است

[1]Hypervisor
[2]Certificate Key
[3]Network Scan

سازمان‌ها کاربران مهمان را در سطح‌بندی خود حذف کنند ولی معمولاً بین کاربر استاندارد و کاربر مدیر دارای حقوق کامل، سطح‌بندی مجزایی وجود دارد. سازمان‌ها معمولاً ممکن است ۱۰۰ یا حتی ۱۰۰۰ نقش کاربری استاندارد و متفاوت داشته باشند که برای متعادل کردن دسترسی‌ها طراحی شده‌اند. به هر نقش دسترسی خاصی به سیستم‌ها، برنامه‌ها و داده‌های موردنیاز برای وظیفه مخصوص آن‌ها اعطا می‌شود. در موارد زیاد، ممکن است یک کاربر عضوی از چندین نقش باشد که وابسته به الزامات خاص آن وظایف است. برای مثال، نقش‌های با دسترسی پایین (که نقش‌های پایه‌ای، حق امتیاز پایه و حقوق اولیه نیز نامیده می‌شوند) برای هر کاربر سازمانی ارائه می‌شود (اعم از کارمند، پیمانکار) تا دسترسی پایه آن‌ها را فراهم سازد. شاید اینکار دسترسی به حساب ایمیل و اینترنت برای جستجوی اطلاعات باشد. مورد بعدی نقش‌هایی است که دسترسی‌های بیشتری را بر اساس خود وظیفه طلب می‌کند. شکل (۱-۱) مثالی پایه‌ای از سلسله‌مراتب نقش در یک محیط تولیدی است.

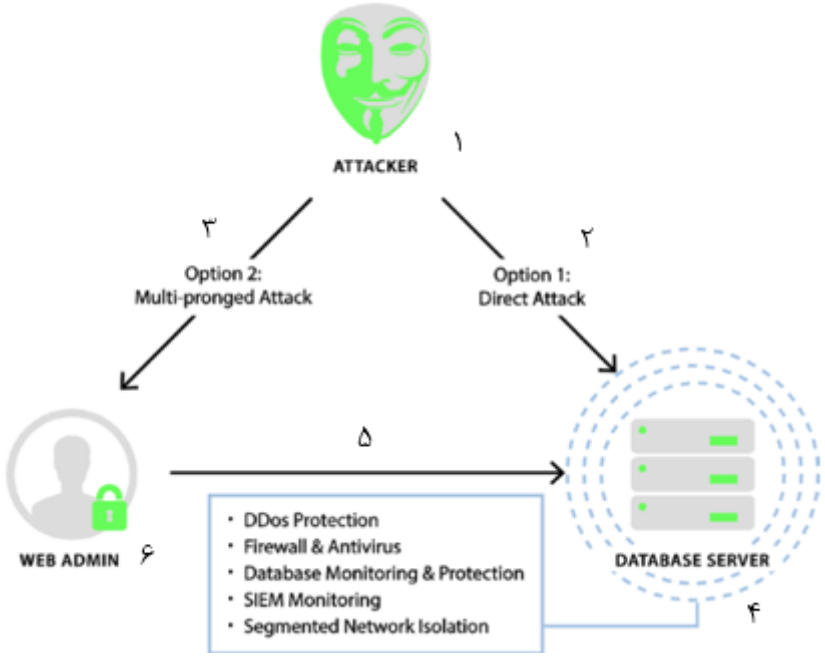


شکل (۱-۱). مثالی از سلسله‌مراتب نقش‌ها در یک محیط تولیدی

۱. مجوزها، ۲. مدیران سرور (روت)، ۳. اپراتورهای سرور، ۴. بخش تولید: مدیر، ۵. بخش تولید: مدیر اپلیکیشن، ۶. بخش تولید: مدیر پایگاه‌داده، ۷. بخش تولید: کاربر اپلیکیشن، ۸. کارکنان تولید، ۹. کاربر سازمان، ۱۰. مهمان، ۱۱. ریسک‌های حقوق ویژه، ۱۲. نمونه نقش‌های بخش تولید با حقوق ویژه طبقه‌بندی‌شده

در این مثال، ممکن است پیوند و ارتباط سلسله‌مراتبی مجوزهای مختلف درون نقش‌های کسب‌وکار سازمان به کاربران خاصی اجازه دهد تا به سِرور وب دسترسی داشته باشند ولی به پایگاه‌داده دسترسی نداشته باشند و یا برعکس آن هم ممکن است. از دید یک عامل تهدید، آلوده کردن حساب‌های با حقوق دسترسی بیشتر معمولاً همان هدفی است که مدنظر آن‌ها است زیرا این اعتبارنامه‌ها همان مواردی هستند که اجازه دسترسی به سیستم‌ها و داده‌های موردنظر آن‌ها را فراهم می‌کند.

فعالیت مخرب به حقوق حساب‌های مدیر دامنه یا روت نیاز ندارد (اگرچه اینکار موانع فنی را برای آن‌ها کاهش می‌دهد و کار را برای انجام فعالیت‌های ویرانگر آسان‌تر می‌کند). برای مثال، اگر کاربر یک کارگر در محوطه تولیدی کارخانه باشد، حقوق ویژه او با نقش کاری او محدود می‌شود (که مانع از آسیب‌پذیری و اکسپلویتی موفق می‌شود). اگر کاربر هدف، یک مدیر فناوری اطلاعات مثل مدیر سرور، مدیر دسکتاپ، مدیر پایگاه‌داده و مدیر اپلیکیشن باشد، ریسک حقوق ویژه آن‌ها بالاتر خواهد بود چراکه بنا به نقش آن‌ها، دسترسی‌های بیشتری به این کارکنان اعطا شده است. این امر، آن‌ها را به اهداف مطلوبی برای عاملان تهدید بدل می‌کند. برای مثال مهاجمی را در نظر بگیرید که می‌خواهد به پایگاه داده سازمان یا فایل سیستمی با اطلاعات حساس دسترسی پیدا کند (شکل (۱-۲)).



شکل (۱-۲). مثالی از یک مهاجم که می‌خواهد به پایگاه‌داده سازمان یا به فایل‌های سیستمی حساس دسترسی پیدا کند.

۱. مهاجم، ۲. گزینه یک: حمله مستقیم، ۳. گزینه دو: حمله چندجانبه، ۴. سرور پایگاه‌داده، ۵. حفاظت در برابر حملات DDoS، فایروال و ضدویروس، نظارت و حفاظت پایگاه‌داده، نظارت SIEM، ایزوله-سازی شبکه تقسیم‌بندی‌شده، ۶. مدیر وب

مهاجمین:

۱. به‌صورت مستقیم به پایگاه‌داده امن‌شده یا سیستم میزبان دارای داده‌های حساس حمله می‌کنند. سیستمی که احتمالاً وصله های امنیتی بر روی آن نصب شده است، مورد نظارت بوده و فناوری‌های تشخیص تهدید و سپر محافظتی در برابر حملات را در خود دارد؛

و یا:

۲. حمله فیشینگی را مورد استفاده قرار می‌دهند تا سیستم یا مدیر پایگاه‌داده را آلوده کنند و از اعتبارنامه‌های آن‌ها برای ورود مستقیم به سیستم هدف استفاده نمایند.

داشتن دسترسی ویژه در یک ارتباط اپلیکیشنی و پایگاه‌داده یا فایل‌های سیستمی، تمام آن چیزی است که برای استخراج اطلاعات پس از صورت گرفتن نفوذ داخلی، موردنیاز است و در ادامه مهاجم دستوراتی را اجرا کرده و اقدامات بعدی را انجام می‌دهد و درنهایت داده‌های مورد نیازش را برداشت می‌کند.

علاوه بر آن، سازمان‌های زیادی هستند که حقوق ویژه بیشتری نسبت به نیاز یک وظیفه خاص اعطا می‌کنند که به افزایش ریسک از سوی هکرها و افراد درون‌سازمانی منجر می‌شود. برای مثال، سازمان‌های زیادی هنوز به کاربران اجازه می‌دهند تا دسترسی مدیریتی به دسکتاپ‌هایشان داشته باشد.

شایان ذکر است که حملات اخیر، بر روی دارایی‌های غیرمرسومی تمرکز دارند که ممکن است فاقد انعطاف‌پذیری و کنترل‌های لازم در برابر تهدیدات پیچیده و پیشرفته امروزی باشند. برای برخی از سیستم‌ها، گزینه‌های دسترسی به صورت صفر و یک است یعنی شما یا دسترسی دارید و یا ندارید. وقتی دسترسی داشته باشید، یک مدیر هستید و کنترل کاملی در اختیار دارید. این امر در دستگاه‌هایی دیده می‌شود که فاقد مفاهیم کنترل دسترسی مبتنی بر نقش هستند، ازجمله در برخی از تجهیزات اینترنت اشیاء[1] (IoT) یا تعداد زیادی از سیستم‌های قدیمی و حتی تجهیزات شبکه‌ای‌که جریان داده اطلاعات حساس عبوری درون و بیرون شبکه سازمان را حفاظت می‌کنند نیز صادق است.

[1]Internet of Things

مدیران

به‌عنوان یک کاربر مدیر یا روت، شما صاحب سیستم هستید. تمام عملکردها، وظایف و قابلیت‌ها احتمالاً تحت کنترل شماست و حتی اگر فناوری برای مسدود کردن مدیر به وجود آید، باز هم به توجه قابلیت‌های مدیر بودن همیشه مسیر دیگری وجود خواهد داشت که بتوان از آن طریق این محدودیت‌ها را دور زد. به عبارتی وقتی شما مدیر هستید، هیچ راهی برای هیچ بازی امنیتی وجود ندارد و مدیر می‌تواند هر سیاست طراحی‌شده دفاعی را دور بزند، حتی اگر نتایج برای خود فرآیندها نیز مخرب باشد. دستیابی به دسترسی مدیر یا روت یک حق ویژه است و در واقع تاج پادشاهی برای مهاجم محسوب می‌شود. وقتی مهاجمی دسترسی روت دارد می‌تواند کارهای خود را بدون شناسایی انجام دهد و بدین معناست که هر سیستم، اپلیکیشن یا داده‌ای در دسترس اوست. این امر برخلاف تمام بدافزارها و حملات مدرنی است که ما به دفاع در برابر آن‌ها می‌پردازیم. دستیابی به حق ویژه نقطه غایی هدف حمله برای نفوذ به سازمان‌ها، دولت‌ها یا حتی دستگاههای رایانش مبتنی بر کاربر نهایی است. مجدد در اینجا بیان می‌کنیم که در سازمان‌ها حقوق ویژه اغلب به‌صورت مدیریت‌نشده اعطا می‌شوند و این امر می‌تواند به ریسک قابل‌توجهی از سوی عاملان تهدید و افراد درون‌سازمانی منجر شود.

مدیریت هویت[1]

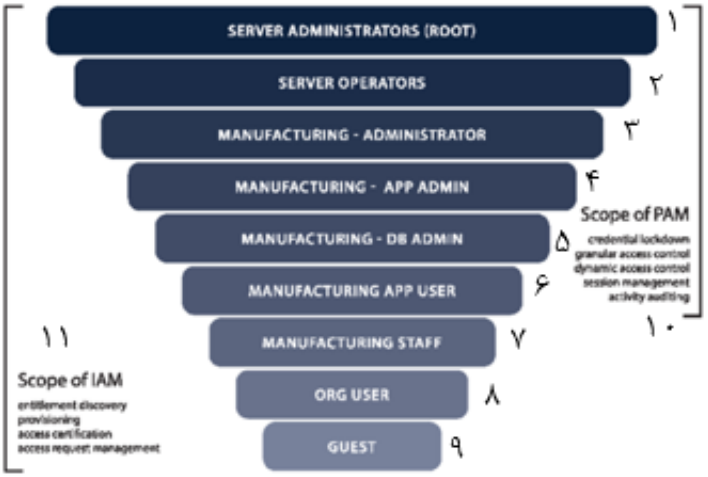
فرآیند تعریف، مدیریت و تخصیص این نقش‌ها برای اطمینان از اینکه فردی درست، دسترسی صحیحی را در زمان درست دارد، با عنوان مدیریت هویت و دسترسی یا IAM[2] نیز شناخته می‌شود.

مدیریت دسترسی ویژه معمولاً فرآیندها و راهکارهای مدیریت هویت و دسترسی (IAM) را با استفاده از لایه‌های اضافی بازرسی و کنترل حساب‌های ممتاز تکمیل می‌کند. این‌ها حساب‌هایی هستند که بزرگ‌ترین ریسک را برای سازمان به همراه دارند.

همان‌طور که به‌وضوح در شکل (۱-۳) دیده می‌شود، نداشتن دید و کنترل کافی روی حساب‌ها، کاربران و دارایی‌های ویژه، شما را در معرض رخنه داده‌ای مخرب و ویرانگر قرار می‌دهد. این رؤیت‌پذیری معمولاً با مانورهای اکتشافی ساده شروع می‌شوند؛ بنابراین اجازه

[1]Identity
[2]Identity and Access Management

دهید ابتدا نگاهی به مکان موجودیت این حساب‌های ویژه داشته باشیم سپس، زمانی که به دید کاملی از گستره این چالش رسیدیم، می‌توانیم استراتژی‌هایی را برای حل آن مورد بحث قرار دهیم.



شکل (۱-۳). نداشتن دید و کنترل روی حساب‌ها می‌تواند به نفوذ در داده‌ها منجر شود

۱. مدیران سرور (روت)، ۲. اپراتورهای سرور، ۳. بخش تولید: مدیر، ۴. بخش تولید: مدیر اپلیکیشن، ۵. بخش تولید: مدیر پایگاه‌داده، ۶. بخش تولید: کاربر اپلیکیشن، ۷. کارکنان تولید، ۸. کاربر سازمان، ۹. مهمان، ۱۰. گستره PAM: محافظت از اعتبارنامه، کنترل دسترسی سطح‌بندی شده، کنترل دسترسی پویا، مدیریت نشست، بازرسی فعالیت، ۱۱. گستره IAM: کشف حقوق، تدارک دیدن، گواهی دسترسی، مدیریت درخواست دسترسی

درحالی‌که این چشم‌انداز از حقوق ویژه در سطح کلانی از کاربر است (مدیریت هویت) ولی درک سطح جزئی‌تری از مجوزها تا رسیدن به توکن‌ها و فایل‌ها برای تعیین یک سیستم دفاعی مناسب مهم است. یادآوری می‌شود که در نظر گرفتن حقوق ویژه به‌صورت بخشی از اپلیکیشن اجرایی شما، کار اشتباهی است. حقوق ویژه باید درون سیستم‌عامل، فایل‌های سیستمی، اپلیکیشن و حتی شبکه‌های تقسیم‌بندی‌شده تعبیه شوند تا ارتباطات کاربر و ارتباطات اپلیکیشن با اپلیکیشن مؤثرتر انجام گیرد لذا این تفسیر منبع از حقوق ویژه نمی‌تواند برای مؤثر بودن تنها در یک لایه باشد. پس مدیریت هویت تنها دسترسی به منبع را به‌وسیله محدوده یا نقش فراهم می‌کند درحالی‌که مدیریت دسترسی ممتاز مجوزهای طبقه‌بندی‌شده

موردنیاز را وقتی ارائه می‌کند که سیستم‌عامل یا اپلیکشین، خود در ارائه این حقوق ویژه ناتوان هستند. کاملاً منطقی است که مدیریت دسترسی ویژه را زیرمجموعه‌ای از مدیریت دسترسی هویت (IAM) و توسعه‌ای جهت حفاظت از حقوق ویژه در هر سطحی بدانیم.

هویت‌ها

به خاطر تعاریف و معمولاً استفاده اشتباه در صنعت، هویت به‌طور ساده، شکلی بنیادی در دنیای امنیت دارد. این انسان یا کاربر است که با منابعی از برنامه‌ها یا سیستم‌های عامل تعامل دارد. این امر شامل دسترسی فیزیکی و الکترونیکی است و راهی ساده برای بیان شخصیت و هویت شما است. «من فکر می‌کنم، پس هستم» و یک هویت دارم، شایان ذکر است که هر کاربری باید یک هویت داشته باشد.

متأسفانه وقتی افراد از نام‌های مختلفی استفاده می‌کنند که شامل نام‌های جدید و ساختگی می‌شود، امنیت رنگ می‌بازد. در این صورت ممکن است دو هویت مشابه در یک سازمان داشته باشیم که به‌صورت الکترونیکی به آن‌ها ارجاع شود. این افراد تنها یک هویت دارند ولی ممکن است نمونه‌های الکترونیکی داشته باشند تا چندین هویت کسب کنند که نباید آن را با داشتن چندین حساب اشتباه گرفت. سازمان‌ها باید تنها یک هویت برای هر شخص داشته باشند، مانند شماره امنیتی اجتماعی آن‌ها (که به خاطر قابلیت شناسایی اطلاعات شخصی کار درستی نیست) یا ترجیحاً یک شماره پرسنلی داشته باشند. یک شخص، یک هویت و یک مرجع الکترونیکی که آن‌ها را با هم لینک می‌کند.

حساب‌ها

هر حساب نماینده‌ای از یک هویت یا مرجعی برای یک مجموعه از مجوزها و حقوق ویژه موردنیاز برای یک برنامه یا منبعی است که به‌منظور اتصال یا انجام کاری درون محدوده سیستم است. درحالی‌که تعریف حساب برای یک هویت روشن است ولی هنگام استفاده برای خدمات الکترونیکی، جعل هویت و عملیات اپلیکیشن به اپلیکیشن می‌تواند انواعی از شکل‌ها را به خود بگیرد. حساب‌ها می‌توانند یک یا تعداد زیادی رابطه با هویت‌هایی داشته باشند که باید به‌صورت محلی تعریف شوند، با هم گروه‌بندی شوند و یا از طریق سرویس‌های دایرکتوری[1]

[1]Directory

مدیریت شوند. حساب‌ها می‌توانند دسترسی مبتنی بر نقش داشته باشند که در سطح حساب، گروه و درون دایرکتوری اعمال می‌شود و این موارد می‌تواند محدوده‌ای از حساب‌های غیرفعال(با دسترسی مسدودشده) تا حساب‌های ویژه مثل روت، مدیر محلی یا مدیر دامنه باشند. سطح حقوق ویژه و دسترسی مبتنی بر نقش، وابسته به مدل امنیتی پیاده‌کننده آن‌ها دارد و ممکن است تفاوت‌های زیادی در یک نمونه با نمونه دیگر مشاهده شود.

بنابراین حساب‌هایی که به هویت‌ها لینک شده‌اند، نحوه دسترسی ما به منابع فناوری اطلاعات را مشخص می‌کنند. حق ویژه زیادی که به هر نوع از حساب داده شود، می‌تواند ریسک‌هایی را ایجاد کند و می‌توان حساب‌ها را عملاً به هر چیزی تخصیص و ارجاع داد که این امر هم به محدودیت‌های سیستم وابسته است. حساب در واقع مرجعی برای ارائه احرازهویت است و یک حساب ممکن است رمز یا کلیدی داشته و یا نداشته باشد. وقتی رمزی به آن تخصیص یابد، بدون در نظر گرفتن قدرت آن رمز، نوع و یا امنیت آن تبدیل به اعتبارنامه می‌شود.

اعتبارنامه‌ها

اعتبارنامه در اصل یک حساب کاربری است که با یک کلمه عبور، کد عبور، گواهی یا دیگر انواع کلید ترکیب می‌شود. اعتبارنامه‌ها می‌توانند بیش از یک مکانیزم امنیتی داشته باشند که برای احراز هویت دو یا چند مرحله‌ای مورد استفاده قرار می‌گیرند و یا می‌توانند اعتبارنامه‌های پایه‌ای مهمان برای دسترسی هر شخصی باشند. اعتبارنامه‌ها تنها نماینده‌ای برای ترکیب رمز عبور و حساب موردنیاز برای احراز هویت هستند، با این وجود جواهری برای عاملان تهدید به‌منظور افزایش حقوق ویژه هستند.

وقتی شخصی تعیین می‌کند که حسابی هک شده است یعنی هکرها اعتبارنامه‌های مربوط به حساب را هک کرده‌اند. از طرفی هک یک حساب ممکن است تنها به یک نام کاربری ختم شود. باید در نظر داشت هر دو مفهوم اشاره‌شده برای آلوده‌سازی موفقیت‌آمیز یک سیستم و احتمالاً داده‌های آن ضروری هستند. پس برای راحتی یادآوری در این کتاب، هک یک حساب همانند هک شدن اعتبارنامه‌های آن حساب است. حرفه‌ای‌های حوزه امنیت و اخبار آن، احتمالاً هرگز بیان خود را از «یک میلیون حساب کاربری آلوده شده‌اند» به «یک میلیون اعتبارنامه آلوده شده‌اند» تغییر نمی‌دهند. آیا شما تفاوتی بین آن‌ها می‌بینید؟

اعتبارنامه‌های پیش‌فرض

هر وقت شما منبع جدیدی را می‌خرید و یا مجوز آن را دریافت می‌کنید، حال چه تجهیزات باشد یا اپلیکیشن و یا حتی یک منبع ابری، طرح اعتبارنامه پیش‌فرضی برای دسترسی و پیکربندی اولیه همراه با آن است. معمولاً منبع حالتی دست‌نخورده داشته و بر روی آن امن‌سازی کامل صورت نگرفته است، همچنین نسبت به انواعی از حملات رمز عبور، مخصوصاً علیه حساب‌های روت یا مدیر پیش‌فرض آسیب‌پذیر است و ممکن است عامل تهدید کنترل تمام سیستم را در دست بگیرد. اگر این حساب آلوده شود انواع مختلفی از حملات ویژه ممکن است به وسیله عامل تهدید به‌صورت مداوم رخ دهد و برای سال‌ها تشخیص داده نشود زیرا پیش‌فرض‌های امن‌سازی بررسی و مدیریت نشده‌اند و مهم‌تر از آن، نگهداری درستی از آن‌ها انجام نگرفته و همچنین مورد نظارت قرار نگرفته‌اند. اعتبارنامه‌های پیش‌فرض موردنیاز هستند تا سازمان بتواند پیکربندی اولیه را به‌خوبی و به صورت مقاوم انجام دهد. به‌طور منطقی، برای استفاده از بهترین روش‌های امنیتی، اعتبارنامه‌های پیش‌فرض را باید تغییر داد ولی اکثر اوقات بدین صورت نیست. رها کردن این حساب‌های پیش‌فرض به حال خود، آن‌ها را در معرض اهداف حمله دارای حقوق ویژه قرار می‌دهد. امروزه، تولیدکنندگان برای انتقال تجهیزات، اپلیکیشن یا دیگر منابع، پنج انتخاب برای رمزها دارند:

۱. **دسترسی ناشناس**: دسترسی پیش‌فرض کاملاً نامحدود بدون هیچ اعتبارنامه‌ای؛
۲. **رمز عبور خالی**: نام کاربری پیش‌فرض بدون هیچ کلمه عبوری؛
۳. **رمز عبور پیش‌فرض**: اعتبارنامه‌های پیش‌فرض با نام کاربری و کلمه عبور قابل پیش‌بینی؛
۴. **رمز عبور تصادفی پیش‌فرض**: نام کاربری پیش‌فرض با کلمه عبور کاملاً تصادفی؛
۵. **رمز عبور تولیدی پیش‌فرض:** نام کاربری پیش‌فرض با کلمه عبور قابل پیش‌بینی.

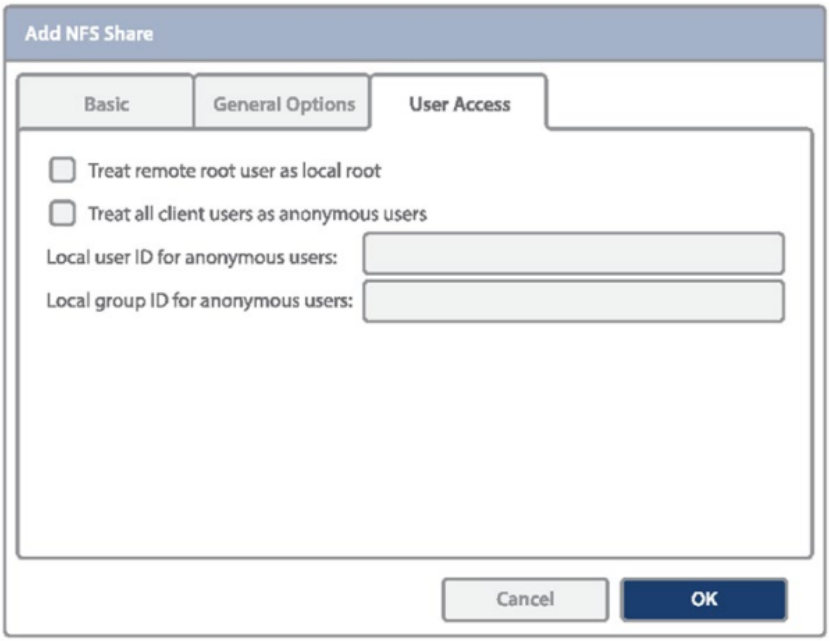
این گزینه‌ها به‌طور جزئی در ادامه بررسی می‌شوند و اگر به‌درستی پیکربندی شوند، هک کردن و تصاحب آن‌ها از نظر زمان و طولانی بودن آن اهمیت پیدا می‌کند. این موارد پایه‌های مدیریت حقوق ویژه هستند.

دسترسی ناشناس

دسترسی ناشناس، ساده و واضح است. در این نوع دسترسی، نیازی به احراز هویت برای آغاز تنظیمات منبع نیست و این تنظیمات شامل امن‌سازی منبع از عاملان تهدید آتی می‌شود درحالی‌که ممکن است این روش در دنیای امنیت امروزی کاملاً عجیب به نظر برسد ولی معمولاً تنها راه پیکربندی برای بار نخست است. خرید تلفن یا تبلت‌های جدید با سیستم عامل iOS و اندروید را در نظر بگیرید. پیکربندی اولیه آن‌ها امکان دسترسی ناشناس برای اتجام تنظیمات وای‌فای را ممکن می‌سازد. معمولاً این کار برای تکمیل پیکربندی لازم نیست ولی اگر پیکربندی اشتباه انجام شود، چه در ابتدا و چه در مراحل بعدی، ممکن است به حمله مرد میانی[1] منجر شود. به‌علاوه، حساب کاربری مدیر اصلی روی دستگاه را می‌توان با یک کلمه عبور خالی تنظیم کرد که اساساً دسترسی بدون محدودیتی را به آن دستگاه در هر زمانی ممکن می‌سازد. این دستگاه به‌طور پیش‌فرض هیچ رمزی را ندارد اگرچه توصیه می‌شود که رمز داشته باشد.

موردی که دسترسی ناشناس را به تهدید امنیتی وحشتناکی تبدیل می‌کند آن است که پس از پیکربندی اولیه، غیرفعال نشده و تغییر نمی‌کند. خوشبختانه، منابع فناوری اطلاعات زیادی وجود دارد که تنها از دسترسی ناشناس پشتیبانی می‌کنند. این موارد شامل حسگرهای SCADA مثل ترموکوپل‌ها، اینترنت اشیاء (اسباب‌بازی) بچه‌ها و دستیاران دیجیتال خانگی (پس از پیکربندی آن‌ها) می‌شوند که بر دستورات صوتی تکیه می‌کنند. این دستگاه‌ها هیچ درک برنامه‌نویسی‌شده‌ای از حساب‌ها و دسترسی مبتنی بر نقش ندارند و هر کاربری که با دستگاه تعامل دارد، سطح یکسانی از حقوق ویژه را دارد (شکل (۱-۴)).

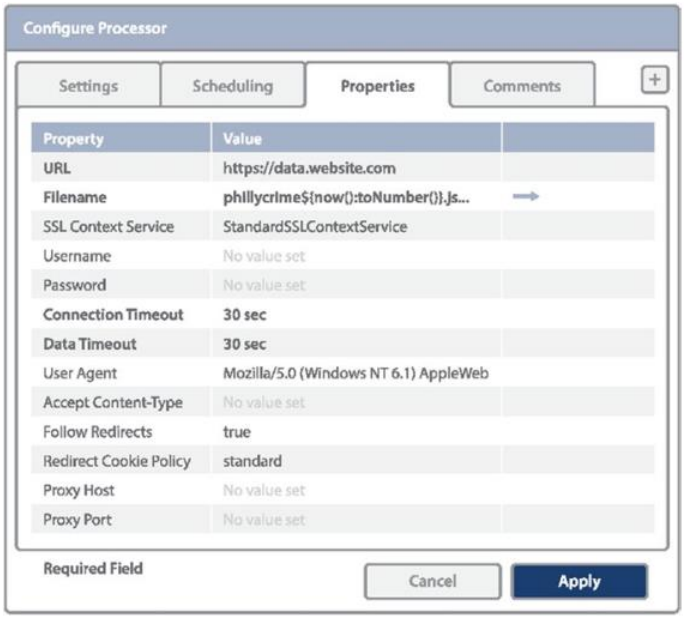
[1] Man-in-the-Middle Attack



شکل (۱-۴). گزینه ناشناس برای افزودن یک اشتراک NFS

رمز عبور خالی

رمز عبور خالی معمولاً در منابعی استفاده می‌شوند که چندین حساب دارند ولی به‌طور پیش‌فرض یک رمز عبور خالی دارند. پیکربندی اولیه و امنیت این منابع ممکن است به تخصیص کلمه عبور نیاز داشته باشد اما به هرحال، فناوری‌های زیادی شامل پایگاه‌های داده قدیمی‌تر، اقدامی برای تخصیص کلمه عبور حتی پس از نصب منبع و شروع عملکرد آن نمی‌کنند. این ریسک‌ها کاملاً آشکار است زیرا حساب‌ها به‌طور مناسبی پیکربندی نشده‌اند و بسته به حقوق ویژه دسترسی، می‌توانند اهداف ساده‌ای برای یک عامل تهدید باشند (شکل ۱-۵)).



شکل (۱-۵). بدون تنظیم حساب و کلمه عبور

ممکن است افراد، حساب‌های با رمز خالی را با دسترسی ناشناس اشتباه بگیرند اما دو تفاوت قابل‌توجه وجود دارد که باید به‌خوبی آن‌ها را درک کرد. در دسترسی ناشناس، هویت کاربر بررسی نمی‌شود و چنین دسترسی معمولاً در فعالیت‌های ریسک پایین قرار می‌گیرد. در حسابی که رمز خالی دارد، هویت کاربر بررسی می‌شود اما امنیت فرآیند احراز هویت کاهش می‌یابد و معمولاً هر غفلتی می‌تواند ریسکی غیرضروری را ایجاد کند. راهکارهای با رمزهای خالی به‌طور معمول‌تر و با استفاده گسترده‌تر، سیستم‌هایی هستند که از حساب‌های مهمان پشتیبانی می‌کنند. دسترسی ناشناس مستقل از آن است که حساب مهمان فعال شده است یا خیر و معمولاً برای تمام دسترسی‌ها رزرو شده است. نکته این است که دسترسی بدون احراز هویت معمولاً هدفمند بوده و برای عملیات‌ها موردنیاز است درحالی‌که کلمه عبور خالی معمولاً نشانه‌ای از یک آسیب‌پذیری ویژه است.

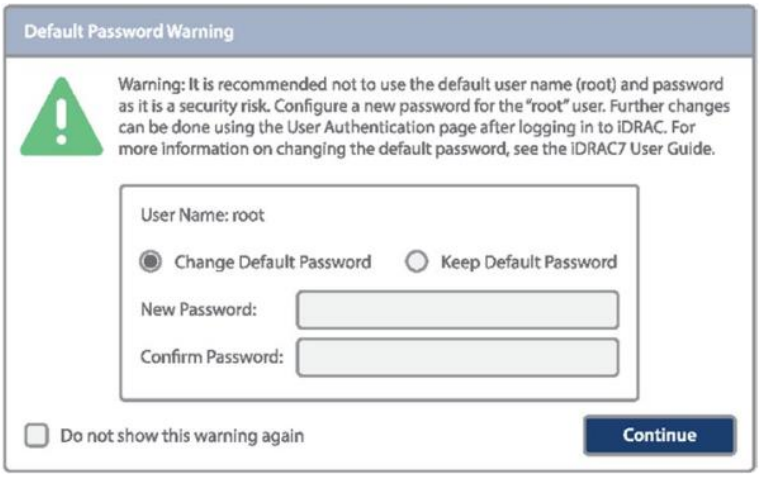
رمز عبور پیش‌فرض

برای سالیان زیادی، تولیدکنندگان، خدمات و محصولاتی را با کلمات عبور پیش‌فرض عرضه نمودند. هر سری مدل از دستگاهی، کلمه عبور منحصربه‌فردی داشت و تولیدکنندگان در

برخی موارد،کلمه عبور پیش‌فرضی را که برای هر منبعی تولید می‌کردند، یکسان بود. با وجود اینکه این روش یک راهکار امنیتی متداول است ولی یک مشکل امنیتی واضح دارد. حجم بزرگی از فهرست این کلمات عبور پیش‌فرض در اینترنت برای شرکت‌های مختلف وجود دارد و تمام کاری که عامل تهدید باید انجام دهد آن است تا آن‌ها را بر روی این تجهیزات امتحان کند و ببیند آیا هنوز از کلمات عبور پیش‌فرض استفاده می‌شود یا نه و بدین صورت دسترسی لازم را پیدا کند؛ به‌علاوه قوانین و مقرراتی که بعداً مورد بحث قرار می‌گیرد، وجود کلمات عبور پیش‌فرض (از هر نوعی) را به خاطر ریسکی که دارد، برای تولیدات ممنوع کرد پس به‌محض اتصال این دستگاه‌ها به شبکه یا اینترنت، در معرض آسیب قرار دارند و ممکن است به درستی پیکربندی نشوند و همچنان اعتبارنامه اولیه را پس از استقرار در خود داشته باشند و بدتر از همه اینکه ممکن است اجازه تغییر کلمه عبور پیش‌فرض را ندهند. مورد آخر هدف حمله ویژه‌ای را بیان می‌کند که درست مثل دسترسی ناشناس و یا با رمز عبور خالی به حساب روت، به‌شدت آسیب‌پذیر است.

شایان ذکر است که رمز عبور خالی (مثل پیش‌فرض) تنها تهدیدی برای نقاط انتهایی و تجهیزات شبکه‌ای نیست. دربیشتر موارد، شرکت‌ها بار پیاده‌سازی کنترل‌های امنیتی را روی دوش کاربران و توسعه‌دهندگان اپلیکیشن می‌گذارند. برای مثال، MongoDB یک پایگاه‌داده NoSQL محبوب است که به وسیله سازمان‌ها برای اجرای بارهای کاری کلان‌داده و تحلیل‌های سنگین مورد استفاده قرار می‌گیرد. نصب پیش‌فرضMongoDB روی نسخه‌های قدیمی‌تر در واقع به احرازهویت برای دسترسی به پایگاه‌داده نیاز نداشت. این امر به حمله گسترده‌ای در سال ۲۰۱۷ تبدیل شد که در آن مدیران اپلیکیشن و پایگاه‌داده قادر نبودند احراز هویتی را برای پایگاه‌داده فعال کنند و بدتر از آن اینکه، بیشتر این پایگاه‌های داده به‌صورت مستقیم ازطریق اینترنت دردسترس بودند. به همین خاطر درنظر گرفتن اقدامات امنیتی مناسب در تمام سطوح سازمان‌ها شامل کدنویسی امن به وسیله تیم‌های توسعه و اپلیکیشن، حیاتی است. شکل‌های(۱-۶) و (۱-۷) فناوری‌های واقعی را نشان می‌دهندکه به‌صورت تجاری در دسترس هستند و پیاده‌سازی ضعیف کلمه عبور پیش‌فرض را دارند.

شکل (۱-۶). مسیریاب خانگی با متنی در رابط کاربری آن که بیان می‌دارد رمز عبور به‌صورت پیش‌فرض آن است



شکل (۱-۷). راهکار سرور تجاری با یک گزینه برای حفظ اعتبارنامه پیش‌فرض

رمز عبور تصادفی پیش‌فرض

در دنیای مدرن، امن‌ترین رمزعبور پیش‌فرض، رمزعبوری است که منحصر به فرد بوده و به صورت تصادفی برای هر منبع تولیدی، مجوزدار یا فروخته‌شده وجود دارد. این رمزعبور باید به‌طور امن به مدیر یا سازمان برای تنظیم اولیه منتقل شود و باید به محض پیکربندی اولیه آن را تغییر داد. متأسفانه برخی از تولیدکنندگان این مفهوم را به سطحی برده‌اند که اگر دسترسی فیزیکی به دستگاه وجود داشته باشد، کاملاً ناامن است. این شرکت‌ها در کنار شماره

سریال، کلمات عبور پیش‌فرض را نوشته‌اند تا هرکسی بتواند آن‌ها را بخواند (شکل (۱-۸)). با یک فشار دادن و نگه داشتن ساده دکمه تنظیم مجدد، کلمه عبور به پیش‌فرض تغییر می‌کند و بسته به دستگاه، پیکربندی آن نیز ممکن است تنظیم مجدد گردد. زمانی که دستگاه تنظیم مجدد شود، عامل تهدید، دسترسی لازم را برای آلوده‌سازی دارد. کاهش این نوع از تهدید بسیار ساده است و راهکار آن،کپی (عکس گرفتن، اسکن کردن یا نوشتن) کلمه عبور پیش‌فرض نوشته شده روی منبع، ذخیره امن آن و سپس پوشاندن یا حذف برچسب دستگاه است. به‌علاوه، دسترسی فیزیکی به هر دستگاهی که امکان تنظیم مجدد را می‌دهد و یا می‌توان فقط کلمه عبور آن را تنظیم مجددکرد، بایستی امن‌سازی شود تا از این تهدید جلوگیری شود که اکثر قوانین و مقررات امنیت اطلاعات نیز این موضوع را ملزم می‌نمایند. رمزهای عبور تصادفی در حال حاضر یکی از امن‌ترین روش‌ها برای توزیع کلمات پیش‌فرض است ولی ممکن است ریسک‌های مشهودی را نیز بسته به نحوه توزیع اولیه کلمه عبور داشته باشد.

شکل (۱-۸). شماره سریال کارخانه

رمز عبورتولیدی پیش‌فرض

بسیاری از سازمان‌ها، فرآیندهایی را برای پذیرش کاربران جدید و ارائه دسترسی‌های لازم برای انجام وظایفشان تدارک دیده‌اند. این حساب‌ها اگر به‌درستی مدیریت نشوند، می‌توانند ریسک‌های امنیتی قابل توجهی داشته باشند. آیا شما تا به حال برای شرکتی کار کرده‌اید که

در آن سیستمی خودکار، نام کاربری و کلمه عبور پیش‌فرضی را مبتنی بر چیزی که هرکسی آن را می‌داند، مثلاً نام شما، ایجاد می‌کند؟ اکثر اوقات، بخش پشتیبانیIT بدین‌صورت دسترسی پیش‌فرض را برای کارکنان جدید تنظیم می‌کند چون مستندسازی، خودکارسازی و اعلام آن به کاربران جدید، با این روش آسان خواهد بود.

برای مثال اگر کاربر جدیدی با نام «John Titor» داشته باشیم، می‌توانیم الگوریتمی داشته باشیم که حساب و اعتبارنامه‌های ورودی را با استخراج مؤلفه‌های نام او تولید می‌کند. در اینجا، فرآیندی تدارک دیده شده است تارمز عبور را برای حساب کاربری او با استفاده از «حروف اول نام او به اضافه حرف اول نام خانوادگی او»، به همراه رمز عبور پیش‌فرض «New» و به اضافه عبارت «$2036!!!» انجام دهد ونتیجه این محاسبات رمز حساب کاربری او را می‌دهد.

حساب کاربری: JTitor

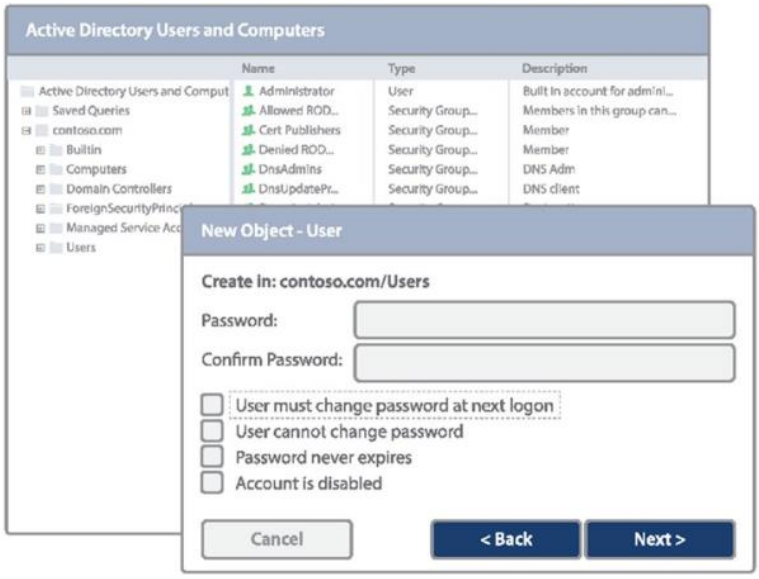
کلمه عبور: $JTNewT!!!2036

وقتی حساب ایجاد شد، می‌توان با یک تماس تلفنی، ایمیل، پیام یا دیگر ابزارهای موجود، نحوه ورود به حساب را به کاربری «جان» اطلاع داد. با وجودی که این روش امن به نظر می‌رسد ولی برای آنکه بتوان به‌طور مؤثری این حساب را هک کرد، تمام چیزی که نیاز است دانستن نام کاربر جدید و الگوریتمی است که برای تعریف حساب کاربری و رمز عبور پیش‌فرض استفاده می‌شود. اگر فردی درون‌سازمانی باشیم که این فرآیند را طی کرده است، کاملاً بر این قضیه اشراف داریم. ممکن است شما تصور کنید که درواقع این موضوع یک ریسک نیست چون می‌توانید حساب را به‌گونه‌ای تنظیم کنید که به‌محض اولین ورود نیاز به تغییر کلمه عبور باشد. این فرض درستی است اما باید دو مورد را مدنظر قرار دهید:

۱. این حساب قطعاً از زمانی که ایجاد شده است در معرض خطر قرار دارد و هکر می‌تواند رمز را به‌محض ورود تغییر دهد و این خطر تا زمانی که کارمند جدید متوجه شود که به حساب از پیش تعیین‌شده دسترسی ندارد و از تیم فناوری اطلاعات بخواهد تا آن را مجدداً تنظیم کند، وجود دارد؛

۲. در برخی موارد، ممکن است سازمان اجبار تنظیم مجدد این کلمات عبور پیش‌فرض را مدنظر قرار ندهد و بدتر از همه کارمندان به همان صورت به استفاده از آن ادامه می‌دهند و این امر واقعاً رخ می‌دهد.

البته برای کاهش این ریسک و حل این مشکل، راهکارهای امنیتی بهتری را می‌توان پیاده‌سازی نمود که شامل اجبار به تغییر کلمه عبور در ورود بعدی و احراز هویت چند مرحله‌ای است. در شکل (۱-۹) نحوه اجبار به تنظیم مجدد کلمه عبور در ورود بعدی نشان داده شده است.



شکل (۱-۹). تنظیم مجدد اجباری رمز عبور به هنگام ورود

شرکت‌های ثالث

پیمانکاران، شرکت‌های HVAC، ارائه‌دهندگان خدمات مدیریتی برای مسیریاب‌ها و دیوارهای آتش، فهرستی از شرکت‌های ثالثی است که ممکن است به شبکه شما در هر زمانی دسترسی داشته باشند و محدود به همین موارد هم نیست. اغلب شرکت‌ها به این سیستم‌ها از راه دور متصل می‌شوند تا عملیات پشتیبانی از سازمان شما را انجام دهند. مشکل در اینجاست که بیشتر سیستم‌هایی که با آن‌ها تعامل دارند نیز به شبکه سازمانی شما متصل است. رخنه‌های

مشهور زیادی نشان‌دهنده این است که امکان دارد شبکه‌های این شرکت‌ها (شرکت های ثالث) برای دستیابی و دسترسی به محیط مشتریان آن‌ها مورد استفاده قرار گیرد.

هکرها می‌توانند اعتبارنامه‌ها را بدزدند تا به سیستم‌های تحت کنترل شرکت‌های ثالث دسترسی داشته باشند و سپس از آسیب‌پذیری‌ها و یا حقوق ویژه یا پیکربندی‌های ضعیف بهره‌ببرند تا از سیستم‌های مختلف سازمان شما دسترسی بگیرند. باید در نظر داشت سازمان شما به اندازه ضعیف‌ترین لینک خود امنیت دارد و امنیت آن ممکن است بر پایه راهکارهای امنیتی و کنترل‌های یک شرکت ثالث باشد.

بزرگ‌ترین مسئله‌ای که بر امنیت سیاست‌های دو شرکت وارد است این است که اغلب اعتبارنامه‌های مورد استفاده به‌وسیله شرکت ثالث، تحت کنترل مستقیم مشتری نیست. دو شبکه مختلف با دو دایرکتوری کاربری متفاوت و شاید دو سیاست امنیتی مختلف، مسئله سازگاری امنیتی را به یک چالش بدل می‌کند. حتی اگر شما بهترین روش‌ها و اقدامات امنیتی را دنبال کرده باشید، باز هم هیچ دیدی بر فعالیتی که روی تجهیز متصل به شبکه شما انجام می‌شود، ندارید.

مشکلات را به صورت زیر تقسیم‌بندی می‌کنیم:

۱. **اعتبارنامه‌های شرکت ثالث**: به روشی برای اطمینان از اینکه کلمات عبور (الف) به‌طور مرتب عوض می‌شوند و (ب) هک نشده‌اند، نیاز داریم. قطعاً وجود سیستم مدیریت کلمه عبور ویژه در اینجا کمک‌کننده خواهد بود؛
۲. **دسترسی شبکه:** باید دسترسی ورودی به شبکه کنترل شود: یک VPN، دروازه[1] پروکسی و یا ترجیحاً هر دو و اگر بتوانیم دسترسی را مطابق با آدرس شبکه ورودی محدود کنیم، بسیار بهتر خواهد بود؛
۳. **نظارت:**کاربران هنگام اتصال چه کاری انجام می‌دهند. به ابزاری نیاز داریم تا وقتی نشستی شروع شد، مطلع شود و سپس فعالیت آن نشست را دنبال کند؛
۴. **کنترل**: چه می‌شود اگر ببینید چیزی که نباید رخ دهد، رخ می‌دهد؟ پس مکانیزمی برای قطع اتصال در این مواقع ضروری خواهد بود.

[1]Gateway Proxy

برای رفع این چالش‌ها، راهکارهای مدیریت حساب ویژه‌ای که شامل مدیریت و ثبت نشست است، می‌تواند دروازه اتصال امنی را ارائه کند که قابلیت دسترسی پروکسی به RDP، SSH و برنامه‌های ویندوز را دارد. کلمات عبور را می‌توان با استفاده از سیاست‌های قدرتمند و پیچیده به‌صورت منظم تغییر داد تا تضمین نمود که هر نفوذ اعتبارنامه‌ای، چه به‌صورت مستقیم و به‌وسیله کاربر و چه به‌صورت غیرمستقیم به‌وسیله بدافزار، توانایی محدودی در اکسپلویت کردن دارد. علاوه بر این مزایای امنیت، تمام فعالیت‌های شرکتی را که از طریق راهکار مدیریت دسترسی ویژه به شبکه سازمان دسترسی دارند، باید برای پشتیبانی از فعالیت‌های قانونی و شکایتی ثبت نمود.

فصل ۲

اعتبارنامه‌های اشتراکی کاربر

یکی از قوانین اصلی در امنیت سایبری آن است که هرگز رمز عبور خود را با هیچ‌کس و در هیچ زمانی به اشتراک نگذارید، چه آن فرد همکار ما باشد و چه یک پیمانکار، در هیچ زمانی و در هیچ صورتی درست نیست که اینکار انجام شود. کارکنان زیادی در زمان‌های اضطراری، رمزهای عبور خود را به اشتراک می‌گذارند تا وظایفشان را به افراد دیگر محول کنند یا مثلاًزمانی که برنامه‌ای برای ترک کار به خاطر بیماری یا مرخصی دارند، جهت انجام کارها، رمزهای عبورشان را به اشتراک می‌گذارند و این دو موضوع از عوامل اصلی این امر هستند.

مشکل آن است که با اشتراک‌گذاری اعتبارنامه‌ها احتمال دارد که آن‌ها به دست یک عامل تهدید بیفتند. اگر چندین کاربر از یک اعتبارنامه استفاده کنند که برای مثال می‌تواند حساب مدیر محلی[1] یا کلید SSH اشتراکی باشد، سازمان چطور می‌تواند به‌طور قابل اطمینانی رویدادهای دسترسی و تغییر را به هر فرد مرتبط سازد؟ متأسفانه، با وجودی که این ریسک‌ها و چالش‌ها وجود دارند، در جهان واقعی موارد استفاده زیادی وجود دارند که در آن‌ها، استفاده از اعتبارنامه‌های اشتراکی ضروری هستند، برای مثال اپلیکیشن‌هایی که باید در معماری‌های چندگانه کار کنند و یا اعتبارنامه‌های اشتراکی که برای ارتباط دستگاه‌ها به شبکه استفاده می‌شوند و نیز مدیریت چندین کاربر که باید از منابع یکسانی استفاده کنند. اعتبارنامه‌های اشتراکی یا عمل اشتراک‌گذاری اعتبارنامه‌ها یک مسئله حق ویژه اساسی است چون وقتی اطلاعات به اشتراک گذاشته شوند، محدود کردن افشاء آن و نیز اندازه‌گیری ریسک این افشاء،

[1] Local administrator

عمل شناسایی را سخت‌تر می‌کند. برای کمینه‌سازی ریسک حقوق ویژه نیاز به دانستن تمام مکان‌های موجود در سازمان است که از اعتبارنامه‌های اشتراکی استفاده می‌کنند و اینکه چه کاری می‌توان انجام داد تا انتشار سهوی آن‌ها را در هنگام اشتراک‌گذاری، کاهش داد. این موارد شامل مستندسازی:

- در زمانی است که اعتبارنامه‌های اشتراکی استفاده می‌شوند؛
- افرادی است که آن‌ها را درخواست داده‌اند؛
- کاری است که با آن انجام داده‌اند؛
- و تغییر رمزعبور به‌صورت متناوب به‌طوری‌که دزدیده نشدن آن را تضمین نماید.

اعتبارنامه‌های اشتراکی رابابد به‌منظور تأمین امنیت، در زمانی که رویدادهای سازمانی مانند تغییر کارکنان و دسترسی پیمانکاران رخ می‌دهند، تغییر داد.

اعتبارنامه‌های حساب کاربری

کاربران اطلاعات حساب خود را به طرق مختلف افشاء می‌کنند: برخی به‌صورت عمدی و برخی به‌صورت غیر عمد. معمول‌ترین روش‌ها شامل بیان شفاهی، از طریق ایمیل و از طریق پیام‌های متنی است. جدای از میکروفن‌هایی که کار پخش و ضبط صدا را انجام می‌دهند، دو مورد آخری، مستندات دائمی را درون فایل‌های پشتیبان، فایل‌های ثبتی و تاریخچه پیام‌های متنی ذخیره می‌کنند که برخی از آن‌ها به‌طور کامل خارج از کنترل سازمان است. افراد فراموش می‌کنند که تنها حذف ایمیل یا پیامک از یک دستگاه بدان معنی نیست که آن پیام به‌طورکلی از بین رفته است بلکه آن پیام تنها از دید شما خارج شده است. اگر رمز عبور از طریق یکی از این روش‌ها ارسال شده باشد، هنوز در جایی وجود خواهد داشت. جایی که رمز قرار دارد و ریسک افشاء متعاقب آن وابسته به نحوه ذخیره‌سازی رمز عبور است. ذخیره‌سازی رمز عبور و بازیابی آن می‌تواند صورت‌های مختلفی از جمله موارد زیر داشته باشد:

۱. ذهنی: تنها در ذهن انسان ذخیره می‌شود؛
۲. مستندسازی: بر روی یک کاغذ و یا یک فایل الکترونیکی. از محتوای آن‌ها می‌توان در یک گاوصندوق به صورت فیزیکی و یا با رمزگذاری فایل به‌صورت الکترونیکی در برابر عامل تهدید محافظت کرد؛

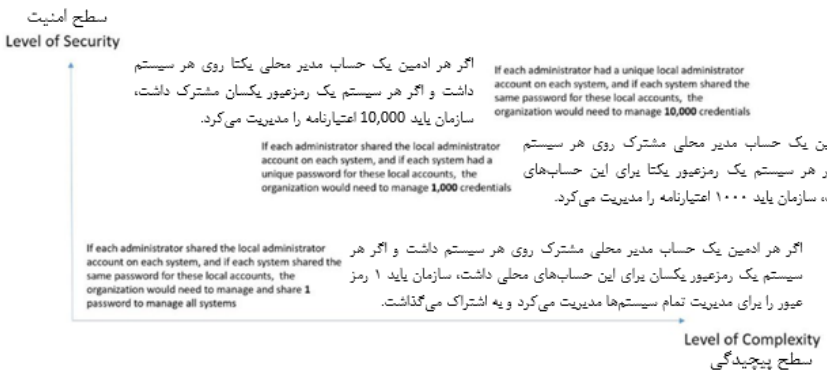
۳. برنامه مدیریت رمز عبور: یک راهکار فناوری برای ذخیره‌سازی و بازیابی اعتبارنامه‌ها و رمزهای عبور مربوط به آن‌هاست. نسخه‌های پیشرفته این فناوری می‌توانند به‌صورت تصادفی رمز عبور تولید کنند و نظارت بر نشست را انجام دهند.

با وجود اینکه ذخیره‌سازی اطلاعات به‌تنهایی در ذهن شما احتمالاً امن‌ترین روش است ولی با ریسک‌هایی همراه است، برای مثال آسیب دیدن شما و از یاد بردن اطلاعاتتان در اثر تصادف یکی از آن‌ها است. در اینجا ریسک از دست رفتن فرد ذخیره‌کننده رمز بسیار اهمیت پیدا می‌کند. مستندسازی و ایجاد حساب‌های خاص برای دسترسی ویژه اضطراری، یک روش مناسب برای دسترسی به اطلاعات است ولی اگر فایل‌ها در یک مکان ناامن به اشتراک گذاشته شده، کپی شوند و یا قرار گیرند، ریسک‌هایی را به همراه دارد. در این مورد، عامل تهدید می‌تواند دسترسی بدون محدودیتی به رمز عبور و منابعی داشته باشد که شما نیز به آن دسترسی داشته‌اید. برای کاهش این ریسک، بسیاری از کاربران نهایی ازبرنامه‌های مدیریت رمز عبور برای ذخیره‌سازی و بازیابی رمزهای عبور استفاده می‌کنند. این مورد یکی از بهترین راهکارها برای مدیریت دسترسی ویژه جهت کاهش حملات با این هدف است.

اعتبارنامه‌های اشتراکی مدیر

سرورها، محل‌های کاری، تجهیزات شبکه و بسیاری از برنامه‌ها با حساب‌های محلی کار می‌کنند و بر آن‌ها متکی هستند که دسترسی به موارد مدیریتی را به‌منظور انجام فعالیت‌های مدیریتی ارائه می‌کنند. در محیط‌های زیادی، چندین مدیر (administrator) سیستم از این حساب‌ها استفاده می‌کنند تا وظایف خاصی را انجام دهند. اشتراک این حساب‌ها و رمزهای عبور مربوط به آن‌ها، در برابر ایجاد یک روش ورود به سیستم یکتا برای هر مدیر ممکن است ناشی از محدودیت دستگاه و یا اپلیکیشنی باشد که پیشتر نیز بحث شد. به‌هرحال در موارد بسیاری، حساب‌ها و حتی رمزهای عبور حساب‌ها ممکن است به دلایل پیچیدگی و هزینه‌های مربوط به پیاده‌سازی اعتبارنامه‌های یکتا در سازمان، وظایف مدیریتی زیاد و غیره، بین مدیران به اشتراک گذاشته شوند.

برای مثال محیطی را در نظر بگیرید که در آن ۱۰ ادمین (مدیر)، ۱۰۰۰ سیستم را مدیریت می‌کنند، این موضوع در ادامه و در شکل (۲-۱) نشان داده شده است:



شکل (۲-۱). مدیریت ۱۰۰۰ سیستم توسط ۱۰ مدیر

همین‌طور برای بازدهی بهتر، سازمان‌های زیادی هستند که گزینه با امنیت کمتر، پیچیدگی پایین‌تر ولی با قابلیت مدیریت بهتر را انتخاب می‌کنند. حال ریسک‌های مربوط به هر گزینه در این مدل را بررسی می‌کنیم:

۱. استفاده از یک حساب روی هر سیستم در حالتی که هر حساب از یک رمز عبور یکسان استفاده می‌کند، راحت‌ترین راهکار از دیدی عملیاتی است چون مدیران تنها باید یک رمز عبور را به اشتراک گذاشته و با هم هماهنگ کنند. به‌هرحال، این گزینه به‌وضوح رویکردی با کمترین امنیت است. اگر رمز عبور یک مدیر هک شود و افشاء گردد، هکر می‌تواند به‌سادگی به تمام این ۱۰۰۰ سیستم دسترسی یابد؛
۲. اگر سیستم‌های تحت مدیریت، هر کدام یک رمز عبور یکتا برای این حساب اشتراکی داشته باشند، ریسک و احتمال تأثیرگذاری رخنه کاهش می‌یابد. در این مورد، اگر رمز عبور مدیری افشاء شود، تنها دسترسی به آن سیستم برای هکر مهیا می‌شود. تمام سیستم‌های دیگر، رمزهای عبور مخصوص به خود را دارند. تنها چالش همراه با این رویکرد که برای موارد با حساب اشتراکی وجود دارد، آن است که شما نمی‌توانید فعالیت‌های خاص یک حساب را به هر فرد خاص تخصیص دهید. در این مثال، تمام فعالیت‌ها از سوی تمام ادمین‌ها به‌عنوان «مدیر» ردیابی می‌شوند و به شخصی که آن فعالیت را انجام داده است، تخصیص نمی‌یابند. همچنین، دقت شود که هنگام استفاده از یک حساب اشتراکی، تنها در صورتی می‌توان رمز عبور را تغییر داد که این به‌روزرسانی‌ها به‌صورت کارآمد و با هر شخصی که از این حساب استفاده می‌کند،

هماهنگ شده و اعلان گردد. هرچه تعداد حساب‌ها و رمزهای عبور بیشتر باشد، انجام کار هماهنگی پیچیده‌تر می‌شود. در این مثال، باید ۱۰۰۰ رمز عبور را میان ۱۰۰۰ سیستم به‌روزرسانی کنیم و به شکل مناسبی ۱۰ مدیر را از به‌روزرسانی این رمزهای عبور مطلع سازیم. نتیجه این است که در اکثر اوقات، علاوه بر اشتراک این رمزهای عبور، به‌ندرت به‌روزرسانی می‌شوند که این امر خود ریسک هک شدن را بیشتر می‌کند. البته، برای اینکه چنین اقدامی کارآمد و مؤثر باشد، راه‌حل مدیریت خودکار رمز عبور برای به‌روزرسانی منظم این ۱۰۰۰ حساب محلی با رمزهای عبور یکتا و پیچیده می‌تواند مورد استفاده قرار گیرد؛

۳. گزینه سوم درواقع پیچیده‌ترین گزینه است. در این راهکار، کاربران از یک حساب محلی اشتراکی استفاده نمی‌کنند و به‌جای آن، هر کاربر با حساب مخصوص به خود دسترسی پیدا می‌کند. اینکار سبب می‌شود تا فعالیت‌ها را به فردی که مسئولیت انجام آن را بر عهده دارد، تخصیص داد و به نام او ثبت کرد. به‌هرحال در مثال ما یا باید ۱۰ حساب (برای هر مدیر یک حساب) روی هر ماشین محلی ایجاد شود و یا اینکه هر ماشین محلی به راهکارهای سرویس‌های دایرکتوری[1] یا هویت متمرکزی برای انجام فرآیند احراز هویت متکی باشد.

در ادامه در رابطه با راهکارهای هویتی و سرویس‌های دایرکتوری در این کتاب بحث خواهد شد.

حساب‌های موقت

حساب‌های موقت معمولاً مربوط به کارآموزان، پیمانکاران، کارکنان موقت و یا دیگر منابعی است که به دسترسی‌های موقت نیاز دارند. ممکن است این حساب‌ها به‌وسیله کاربران در یک عملیات کاری به اشتراک گذاشته شوند، مثلاً کارکنان موقتی که از یک کیوسک اشتراکی بهره‌می‌برند، پیمانکارانی که روی ماشین‌آلات کار می‌کنند، پیمانکاران خدمات حرفه‌ای، حسابرسان یا دیگر کارکنان موقتی که برای شروع کار باید به یک حساب موجود دسترسی داشته باشند. ریسک‌های مربوط به حساب‌های موقت شامل موارد زیر است:

[1]Directory Services

- نبود مسئولیت‌پذیری در مورد اینکه چه کسی چه کاری را با این حساب‌ها انجام داده است؛
- ممکن است کارکنان دسترسی طولانی‌تری نسبت به نیازشان داشته باشند؛
- دسترسی کنترل‌نشده در محیط‌هایی که در آن این رمزهای عبور به‌صورت مرتب تعویض نمی‌شوند؛
- حساب‌ها غیرفعال یا مدیریت نمی‌شوند که امکان دسترسی غیرمجاز پس از پایان دوره موقت را می‌دهد. این موارد در فرآیند تصفیه و حذف دسترسی، شکاف نامیده می‌شوند.

رمز عبورهای شخصی و کاری

همه ما چندین رمز عبور را حفظ کرده‌ایم و فراموش کردن آن‌ها نیز امری عادی است. به‌منظور کاهش ریسک و جلوگیری از فراموشی رمز عبور، کاربران زیادی به راهکارهای مدیریت رمز عبور روی آورده‌اند که این راهکارها تمام رمزهای عبور را لیست می‌کند و به‌صورت امن نگهداری می‌کند و برای دسترسی به تمام آن رمزهای عبور تنها باید یک رمز عبور اصلی را به خاطر بسپارید که این کار استراتژی مناسبی است. موضوعی که استراتژی خوبی به شمار نمی‌رود، استفاده مجدد از رمز عبوری یکسان برای چندین برنامه، سرویس و دیگر منابع است. رخنه‌های اخیری که در آن میلیون‌ها رمز عبور مشتریان افشاء شده است، به اندازه کافی بد بوده‌اند زیرا بسیاری از این رمزعبورها در دیگر حملات نیز مورد استفاده قرار گرفتند. این رمزهای عبور می‌توانند دسترسی به دیگر حساب‌های ایمیل، برنامه‌های بانکی، فیس‌بوک، توییتر و غیره را ممکن سازند. نیازی به ذکر این مورد نیست که نباید رمزهای عبور متداول را در حساب‌های شخصی و سازمانی به اشتراک بگذارید و استفاده کنید چون آلوده شدن حساب‌های شخصی می‌تواند شرکای کاری و کسب‌وکار سازمان شما را در معرض خطر قرار دهد.

برنامه‌ها

قانون اساسی دوم برای امنیت سایبری آن است که کاربران باید رمز عبور یکتایی را برای هر اپلیکیشن داشته و دو اپلیکیشن مختلف نباید اعتبارنامه‌های یکسانی را داشته باشند مگر اینکه

نیاز به ارتباط با هم داشته باشند. این امر استفاده دوباره از رمز عبور است و یکی از بزرگ‌ترین مشکلات حقوق ویژه در امنیت اطلاعات است. افراد از رمز عبور یکسانی در چندین اپلیکیشن، سیستم‌ها، منابع، زیرساخت‌ها و غیره استفاده می‌کنند و اگر هر یک از آن‌ها افشاء شود، می‌توان از همان رمز عبور در نفوذ به دستگاه‌های دیگر استفاده کرد. وقتی این امر با بهترین روش‌ها و اقدامات امنیتی برای تغییر مرتب رمزهای عبور همراه نشود، ریسک رمزهای عبور اشتراکی و دوباره استفاده‌شده و قدیمی به‌صورت نمایی به‌عنوان یک عامل تهدید تشدید می‌شود. وقتی یکی از آن‌ها افشاء شود، تمام منابع دیگر در معرض خطر قرار می‌گیرند.

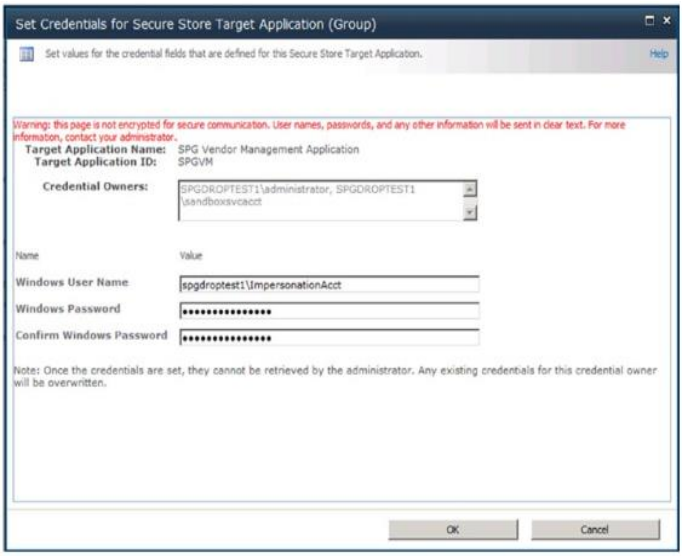
متأسفانه و برعکس این امر، کاربردهای معتبری وجود دارد که در آن اشتراک رمزهای عبور بین برنامه‌ها ضروری است و از این رو هدف تهدیدی منحصربه‌فرد را بیان می‌کند. هر اپلیکیشن باید اعتبارنامه‌های یکسانی داشته باشد و اگر با هم همگام نباشند، عملکرد مطلوب منابع مختل می‌شود. اگر یکی از منابع آلوده شوند، ممکن است مشکل مشابه با استفاده دوباره از رمزهای عبور رخ دهد چون احراز هویت با اعتبارنامه‌های اشتراکی یکسان را ممکن می‌سازد. از معمول‌ترین جاهایی که از این رمزهای عبور اشتراکی استفاده می‌شود، حساب‌های خدماتی، اسناد و احراز هویت اپلیکیشن به اپلیکیشن است. هیچ روش ساده‌ای برای حل این مشکل وجود ندارد ولی روش‌هایی وجود دارد تا تضمین نماید که این ریسک به‌صورت مناسبی مدیریت می‌شود:

- رمزهای عبور را در مستندات، برنامه‌ها یا رشته های اتصالی ننویسید؛
- تمام سرویس‌ها، برنامه‌ها و حساب‌هایی را که از اعتبارنامه‌های اشتراکی استفاده می‌کنند، ترسیم کنید؛
- هرگز رمزهای عبور را در فایل‌های متنی یا فایل‌هایی که می‌توان آن‌ها را به‌سادگی رمزگشایی کرد، قرار ندهید.

برای کاهش این تهدید، راهکارهای مدیریت رمز عبور، ابزاری را فراهم می‌کنند تا این ریسک‌ها را با استفاده از رابط‌های برنامه‌نویسی اپلیکیشن (API) کم کنند. به‌جای نوشتن رمز عبور، رابط برنامه‌نویسی اپلیکیشن به‌عنوان گاوصندوق رمز عبور یا ابزار مدیریت رمز عبور ساخته می‌شود تا به‌عنوان بخشی از یک راهکار مدیریت دسترسی ممتاز برای بازیابی صحیح رمز عبور استفاده شود. راهکارمدیریت دسترسی ممتاز پیوند و نگاشت راهکارهایی را که به رمزهای عبور یکسان نیاز دارند، درک می‌کند و آن‌ها را به‌طور صحیحی به محض فراخوانی رابط

برنامه‌نویسی اپلیکیشن توزیع می‌کند و یا به‌طور خودکار آن‌ها را بر اساس رابطه‌های یکسان تغییر می‌دهد. این فرآیند با استفاده از مکانیزم‌های احراز هویت خود که در این کتاب پوشش داده خواهد شد، در برابر عامل تهدید محافظت می‌شود.

یک راهکار ذخیره‌سازی رمز عبور (گاوصندوق، قفسه و یا کیف رمز عبور) مناسب‌ترین پیشنهاد برای ذخیره‌سازی رمز عبور اپلیکیشن به اپلیکیشن در برابر کدگذاری رمزهای عبور در این راهکار است. شکل(۲-۲) اپلیکیشنی را نشان می‌دهد که از اعتبارنامه‌ها برای امن‌سازی ارتباطات بعدی استفاده می‌کند. اگر اعتبارنامه‌ها کدگذاری شده یا در فایل جدایی ذخیره‌سازی شوند و یا اگر در طی زمان اجرای راهکار به کلید نیاز شود، آنگاه ریسک دزدیده شدن رمز عبور به‌وسیله عامل تهدید بر اساس اینکه رمز عبور در یک فایل مستند شده باشد و یا به‌صورت دستی وارد شده باشد و یا به‌وسیله یک نرم‌افزارِکیلاگر دریافت شده باشد، افزایش می‌یابد.



شکل (۲-۲). اعتبارنامه‌های استاتیک برای احراز هویت ذخیره‌ساز امن بین دو اپلیکیشن

دستگاه‌ها

دستگاه‌هایی که رمزهای عبور را به اشتراک می‌گذارند، بسیار شبیه به برنامه‌هایی هستند که اعتبارنامه‌ها را به اشتراک می‌گذارند ولی اعتبارنامه‌ها و رمز عبورها روی دستگاه (اغلب بدون امنیت) به‌منظور مصرف پیوسته ذخیره می‌شوند. این‌ها رمزهای عبوری نیستند که شما برای

ایمیل یا حساب‌های رسانه اجتماعی استفاده می‌کنید بلکه رمزهایی هستند که هر دستگاه ممکن است برای اتصال نیازداشته باشد که شامل موارد زیر است و تنها به این موارد محدود نمی‌شود:

- اگر WEP (که امیدواریم نباشد) یا WPA2 برای وای‌فای استفاده شده باشد، ممکن است کلید یا عبارت عبور[1] برای اتصال در تمام دستگاه‌ها یکسان باشد؛
- اگر از هیچ راهکار مدیریت دسترسی ممتازی(PAM) استفاده نشده باشد، ممکن است مدیر محلی مخفی بر روی تمام دستگاه‌های قابل‌حمل به‌صورت یکسان وجود داشته باشد؛
- ابزارهایی مثل پایشگرهای ارزیابی آسیب‌پذیری، مدیریت شبکه و راهکارهای امنیتی ممکن است اعتبارنامه‌ها و رمزهای عبور یکسانی را برای اتصال در تمام تجهیزات به اشتراک بگذارند؛
- مدیریت دستگاه‌های زیرساختی مثل مسیریاب‌ها و سوئیچ‌هایی که از رمز عبور روت یکسانی برای راهکارهای مدیریت شبکه استفاده می‌کنند.

رمزهای عبور دستگاه‌ها، هدف دیگری برای حملات با حقوق ویژه است. رمزهای عبور یا گواهی‌ها به‌ندرت تغییر می‌یابند و زمانی که عامل تهدید به آن دست یابد، روشی ساده و دائمی برای نفوذ به یک محیط دارد مگر اینکه این نفوذ تشخیص داده شود و به تبع آن سرویس‌ها متوقف شوند و یا رمزهای عبور دستگاه تغییر یابند. برای شبکه‌های بی‌سیم ناامنی که از WPA2 یا WEP استفاده می‌کنند، احتمال نشر یک عبارت عبور، به مرور زمان افزایش می‌یابد. هرچه دستگاه‌های بیشتری از آن استفاده کنند و افراد بیشتری از آن مطلع شوند، با احتمال بیشتری افراد غیرمجاز می‌توانند به آن متصل شوند. بهترین توصیه برای رمزهای عبور اشتراکی دستگاه‌ها این است که سعی شود تمام آن‌ها را منحصربه‌فرد حفظ کنیم و از فناوری‌های احراز هویت پیشرفته‌ای برای پرهیز از اشتراک رمز عبور دستگاه استفاده کنیم. یک لیست با شماره سریال‌های لپ‌تاپ‌ها و رمزهای عبورهای پشتیبان IT بسیار امن‌تر از آن است که همه لپ‌تاپ ها رمز عبور یکسانی داشته باشند، مخصوصاً اگر این رمزها هرگز تغییر نیابند. نگه داشتن تمام این اطلاعات در یک برنامه مدیریت رمز عبور، امن‌ترین رویکرد است و بهترین کار به‌جای هر نوع تکنیک Flat File است. جدول (۲-۱) این رویکرد را نشان می‌دهد

[1]Passphrase

ولی دقت شود که این رویکرد توصیه نمی‌شود چون تمام رمزهای عبور در صورت نشر در معرض خطر قرار دارند، به‌علاوه خارج از امنیت فایل، برای اینکه هر عامل تهدیدی بتواند از این داده‌ها استفاده کند باید از ارجاع متقابل[1] استفاده کند.

جدول (۲-۱). یک نمونه لیست

شماره سریال دستگاه	رمز عبور هِلپ‌دِسک	برچسب دارایی
XDM7GT	1503VaBm@!	2001
PLOOHG3	9802PbWd^%	2010
LKJ678	PbUI7650!!	2049
LM7WQ4	RnSs1209)*	1069

نام‌های مستعار

شما به‌عنوان خواننده این کتاب یک انسان منحصربه‌فرد هستید و حتی اگر دوقلو هم باشید شما خودتان هستید. هرچند که شیوه‌های تشخیص بیومتریک الزاماً نمی‌توانند صد درصد به‌درستی چهره شما را تشخیص دهند (مثلاً برای افراد دوقلو در آیفون که سیستم تشخیص چهره FaceID امکان تشخیص اشتباه وجود دارد). وقتی جنبه انسانی هویت‌های خود را به دنیای دیجیتالی برمی‌گردانیم، می‌توانیم چیزی بیشتر از نام‌های مستعار، شکلک‌ها، نمایه‌ها و یا حتی حقوق ویژه باشیم. کاربران فناوری اطلاعات می‌توانند چندین نام مستعار داشته باشند، درست مثل کسانی که بیشتر از یک آدرس ایمیل دارند. ممکن است یکی از ایمیل‌ها برای امور خانگی باشد و یکی برای کار سازمانی و همچنین ممکن است برای هر یک، چندین ایمیل داشته باشیم. این‌ها هویت‌های منحصربه‌فردی هستند ولی درنهایت تمام آن‌ها به شما برمی-گردند. همان‌طور که بحث کردیم، این نام‌های مستعار نباید هیچ‌گاه رمزهای عبور مشترکی داشته باشند.

چون این حساب‌ها به ما تعلق دارند و معمولاً حقوق ویژه‌ای را به خود اختصاص داده‌اند ممکن است بر اساس نام خود، یک حساب کاربری استاندارد داشته باشیم. همچنین ممکن است یک حساب مدیریتی (با حق امتیازهای بیشتر) داشته باشیم که بر اساس همان نام با پیشوندها یا پسوندهایی همراه باشد و مشخص کند این حساب ویژه است. برای مثال، ممکن است حساب

[1] Cross-Reference

کاربری استانداردی به‌صورت «jtitor» باشد و حساب کاربری مدیریتی آن به‌صورت «jtitor-admin» باشد. این دو نام‌های مستعاری برای هویت یک شخص هستند و نباید رمزهای عبور یکسانی داشته باشند. وقتی با سیستم‌عامل‌ها و سرویس‌های دایرکتوری زیادی کار می‌کنیم، ممکن است با چنین حساب‌هایی مواجه شویم که ذاتاً همگام نیستند و پلتفرم‌ها و برنامه‌ها را به هم متصل می‌کنند.

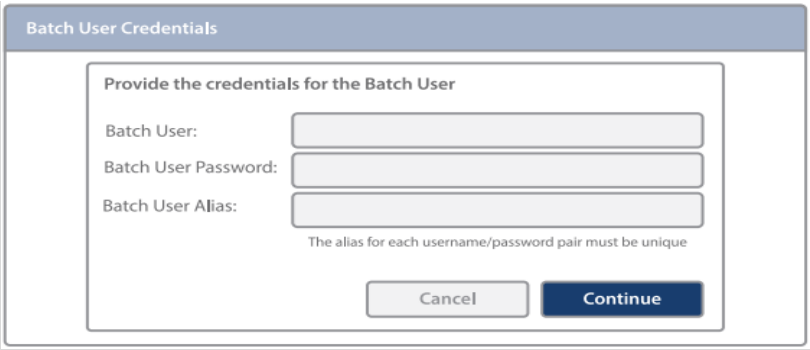
این امر ممکن است ما را با چندین نام مستعار برای یونیکس، لینوکس، ویندوز، مک، آی‌اواس، اندروید، رسانه‌های اجتماعی، برنامه‌ها و غیره مواجه کند. از دید عامل تهدید، نام‌های مستعار مانعی برای اهداف خرابکارانه آن‌ها هستند، مخصوصاً اگر الگوی نام‌گذاری این نام‌ها متفاوت باشد و دارای رمزهای عبور مختلفی هم باشند لذا برای عامل تهدید حرکت از یک منبع به منبعی دیگر به سبب فقدان حقوق ویژه و احراز هویت آن منبع، مشکل خواهد بود. داشتن صدها یا هزاران حساب ممتاز محلی ناهمگام در اختیار چندین کاربر یک کابوس است و می‌تواند مشکلات امنیتی را ایجاد کند. به همین دلیل بهترین روش‌های امنیتی برای مدیریت سیستم‌ها، حساب‌های مدیریتی دامنه[1] را به حساب‌های محلی[2] ترجیح می‌دهند. حساب‌های مدیریتی دامنه کنترل، مدیریت، ثبت و نگهداری ساده‌تری دارند.

از نظر هدف حمله دارای حقوق ویژه، هرچه تعداد حساب‌ها کمتر و دارای رؤیت‌پذیری بهتری باشند می‌توانند به کاهش این ریسک کمک کنند. در اینجاست که پل زدن بین سرویس‌های دایرکتوری وارد عمل می‌شود. اینکار به مخازن دایرکتوری مانند اکتیو دایرکتوری اجازه می‌دهد تا با استفاده از نام‌های مستعار یکسان و رمز عبور یکسان (دو عاملی)، عملیات لازم برای احراز هویت و حقوق ویژه را برای تمام پلتفرم‌ها و برنامه‌های مورد پشتیبانی آن انجام دهد؛ یعنی اینکه یک نام مستعار مدیریتی می‌تواند در هر جایی کار کند و احراز هویت شود (رمز عبور در این مدل به‌صورت محلی ذخیره نمی‌شود) وگرفتن گزارش در مورد هرکاربری می‌تواند در هر جایی و هر زمانی رخ دهد زیرا تمام چیزی که شما باید انجام بدهید جستجو برای همان نام مستعار در میان تمام منابع است. همین‌طور برای همان رمز عبور با چندین نام مستعار در چند جا، هر منبع باید آن رمز عبور را برای احراز هویت ذخیره کند. با این‌حال

[1] domain administrator accounts
[2] local accounts

این موضوع هدف حمله دیگری را برای عامل تهدید به‌منظور کِرک رمزهای عبور بیان می‌کند. با یک عمل پل زدن بین دایرکتوری‌ها می‌توان این ریسک را کاهش داد.

کمینه نمودن تعداد نام‌های مستعار به ازای هر کاربر انسانی از نظر استراتژیکی روشی عالی برای هر سازمانی است. حذف حساب‌های مدیریتی و نگه داشتن کاربران استاندارد نیز از آن بهتر است و در فصول حق امتیازهای حداقلی بررسی می‌شود. شکل (۲-۳) نشان می‌دهد که چگونه یک فرآیند دسته‌ای[1] می‌تواند به هر نام مستعاری تخصیص یابد به‌گونه‌ای که به‌طور واضحی با یک حساب مدیریتی همراه نیست.



شکل (۲-۳) تخصیص یک نام مستعار مدیریتی

کلیدهای SSH

کلیدهای پوسته امن[2] ابزارهای متداولی است که به‌وسیله مدیران سیستم‌های یونیکس جهت دسترسی به سرورهای یونیکسی استفاده می‌شوند. این کلیدها، وقتی با عبارت‌های عبور استفاده می‌شوند یک روش امن برای مدیران مهیا می‌سازند تا به سیستم‌ها و داده‌ها دسترسی داشته باشند. کلیدهایSSH استاندارد هستند و بیشتر در محیط‌های یونیکس و لینوکس کاربرد دارند ولی در ویندوز نیز استفاده می‌شوند. مدیران از کلیدهای SSH بهره می‌برند تا سیستم‌های عامل، شبکه‌ها، انتقال فایل‌ها، تونلینگ داده‌ها[3] و غیره را مدیریت کنند. کلیدهای SSH مانند دیگر اعتبارنامه‌های ویژه نیز الزاماً به یک کاربر ارتباط ندارند و ممکن است چندین فرد کلید خصوصی و عبارت عبور را با سروری که کلیدعمومی را نگهداری می‌کند، به اشتراک

[1]Batch Proccess
[2]Secure Shell
[3]Data Tunelling

بگذارند. همانند دیگراعتبارنامه‌های ویژه، وقتی سازمان‌ها به فرآیندهای دستی متکی هستند، تمایلی مشخص وجود دارد تا از یک عبارت عبور در کلیدهایSSH زیادی استفاده شود و یا از کلیدSSH عمومی یکسانی استفاده مجدد گردد و این یعنی اینکه یک کلید هک‌شده را می‌توان برای نفوذ به چندین سرور استفاده نمود البته راهکارهایی برای این موضوع وجود دارد که در فصول بعدی بیان خواهند شد.

فصل ۳

هک کردن رمز عبور

هک کردن رمز عبور به‌وسیله عامل تهدید ممکن است با تکنیک‌های مختلفی انجام گیرد. اگر موفقیت‌آمیز باشد، قطعاً به حقوق ویژه مدیر دسترسی پیدا می‌کند البته اگر حساب هک‌شده به این حقوق دسترسی لازم را داشته باشد. این امر دلیل دیگری برای محدود کردن تعداد حساب‌های مدیر در یک محیط است. اگر حساب هک‌شده مربوط به یک مدیر باشد، موانع برای هکر به‌منظور انجام اقدامات بعدی کمتر است پس تلاش می‌کند تا سایر رمزهای عبور مربوط به حساب‌های ممتاز را بر روی همان سیستم یا سیستم‌های در دسترس، کِرَک کند. دقت شود که هک رمز عبور را نباید با بحث‌های قبلی درباره افشاء رمز عبور مانند رمزهای عبور اشتراکی و مستندسازی ناامن رمزهای عبور، اشتباه گرفت. هک رمز عبور تهدیدی است که در آن مهاجمان سعی می‌کنند با استفاده از انواع تکنیک‌های برنامه‌نویسی و اجرای برنامه-های خودکار، رمز عبور را به دست آورند.

حدس زدن

یکی از موفق‌ترین تکنیک‌ها برای هک رمز عبور، روش ساده حدس زدن رمز عبور است. حدس تصادفی به‌تنهایی موفقیت کمی دارد مگر اینکه آن رمز عبور بسیار متداول باشد و یا بر اساس فرهنگ لغت (که در ادامه بیان می‌کنیم) باشد. ساده‌سازی حدس به‌نوعی یک هنر است اما دانستن اطلاعاتی درباره هویت هدف، فرآیند را راحت‌تر می‌کند و احتمال موفقیت عامل تهدید بیشتر می‌شود. این اطلاعات را می‌توان به‌وسیله شبکه‌های اجتماعی، تعامل مستقیم و یا حتی داده‌های به‌دست‌آمده و یا جمع‌آوری‌شده از رخنه‌های قبلی به دست آورد. متداول‌ترین نوع

رمزهای عبوری که حدس زدن آن‌ها آسان بوده و آسیب‌پذیر هستند، الگوهای رایجی را شامل می‌شوند. برای مثال:

- کلمه«Password»یا مشتقاتی از آن مثل «Passw0rd»؛
- مشتقاتی از نام کاربری صاحب حساب شامل حروف اول نام او؛
- تاریخ تولد عینی یا تغییر شکل یافته کاربران یا خویشاوندان آن‌ها؛
- مکان‌های به‌یادماندنی؛
- نام خویشاوندان و مشتقاتی از اعداد یا کاراکترهای خاص؛
- حیوانات خانگی، رنگ‌ها، غذاها یا دیگر اشیائی که برای فرد مهم هستند؛
- نام کاربر.

برای اینکه عامل تهدید در حدس زدن رمزعبور موفق شود، زمانی که از حدس هدف‌دار رمز عبور استفاده می‌کند، نباید از برنامه‌های خودکار استفاده کند درحالی‌که ممکن است این روش (استفاده از برنامه‌های خودکار) راحت بوده و احتمال موفقیت آن بالاتر باشد ولی ممکن است خطاهایی را نیز به همراه داشته باشد و ردهایی مانند مسدودسازی خودکار حساب بعد از n بار تلاش را بر جای بگذارد. برای یک عامل تهدید، گرفتن اطلاعات دقیق از هدف مورد نظر معمولاً شامل نظارت پیشرفته و یا مبتنی بر دانش خود او است. برای شخص معمولی ممکن است اینکار تنها یک آزمون و خطا باشد، به‌علاوه اگر صاحب حساب موارد امنیتی را رعایت نکند و از رمزهای عبور یکسان بین منابع استفاده نماید، خطرات حدس رمز عبور و اقدامات بعدی به‌شدت افزایش می‌یابند. برای مثال فردی را تصور کنید که تنها یک یا دو رمز ثابت را برای تمام حساب‌های خود در فضای دیجیتال استفاده می‌نماید.

ایستادن کنار قربانی[1]

ایستادن کنار قربانی به عامل تهدید اجازه می‌دهد تا از طریق مشاهده قربانی، اعتبارنامه‌های او را به دست آورد. اینکار شامل مشاهده رمزهای عبور، پین‌کدها و رمز عبورهای الگو مانند هنگام ورود آن‌ها است. اینکار حتی مشاهده نوشتن یک رمز عبور روی برگه یادداشت را نیز شامل می‌شود و مفهوم آن ساده است، عامل تهدید به‌صورت فیزیکی در حال مشاهده است و

[1]Shoulder Surfing

یا با دستگاهی مثل دوربین اینکار را به‌صورت الکترونیکی انجام می‌دهد و رمزهای عبور را به دست می‌آورد و از آن‌ها برای حملات بعدی استفاده می‌کند. به همین خاطر است که هنگام استفاده از دستگاه‌های خودپرداز توصیه می‌شود که همیشه هنگام ورود، رمز عددی خود را بپوشانید تا مانع از آن شوید که عامل تهدید رمز شما را به دست آورد. شایان ذکر است که اینکار یکی از قدیمی‌ترین و راحت‌ترین روش‌های حمله به حقوق ویژه است.

حملات با استفاده از فرهنگ لغات

حملات با استفاده از فرهنگ لغات یک تکنیک خودکار است که فهرستی از رمزهای عبور را برای حسابی معتبر استفاده می‌کند تا رمز عبور را هک کند. این لیست فرهنگ لغاتی از کلمات است (البته نه بدان مفهومی که در ذهن شماست) و افراد از این لیست‌ها استفاده می‌کنند تا حسابی را کرک کنند، لیست‌هایی که شامل کلماتی مانند «football» و سایر کلمات رایج است. اگر عامل تهدید، هدف موردنظر را بشناسد، مثلاً طول رمز عبور مورد استفاده و پیچیدگی‌های موردنیاز را بداند، می‌تواند فرهنگ لغت را به‌گونه‌ای سفارشی‌سازی نماید تا به‌صورت کارآمدتری کار خود را انجام دهد؛ بنابراین برنامه‌های پیشرفته‌تر اغلب ابتدا ترکیبی از اعداد و نشانه‌های متداول را استفاده می‌کنند و در انتها سعی می‌کنند تا رمز عبور واقعی با پیچیدگی‌های لازم را مورد آزمون قرار دهند. سیستم حمله‌ای خوب همراه با فرهنگ لغتی مناسب به عامل تهدید اجازه می‌دهد تا کارهای زیر را انجام دهد:

- الزامات مجموعه کاراکترها و الزامات پیچیدگی را برای طول رمز تنظیم نماید؛
- اجازه می‌دهد تا به‌صورت دستی کلماتی از قبیل نام‌ها و اطلاعات شخصی قابل تشخیص را وارد کند؛
- می‌تواند شامل جابجایی حروفی باشد که معمولاً مورد استفاده قرار می‌گیرند؛
- می‌تواند با فرهنگ لغاتی از زبان‌های مختلف کار کند.

متأسفانه ضعف حملات با فرهنگ لغت آن است که به دنیای واقعی و مشتقات ارائه شده به‌وسیله کاربر وابسته است. اگر رمز عبور استفاده شده تخیلی باشد و از چندین زبان استفاده کرده باشد یا از چند کلمه یا عبارت استفاده کرده باشد، حمله با فرهنگ لغت را خنثی می‌کند. تنها وجود و بررسی جایگشت‌های خیلی زیاد است که می‌تواند برای آن موفقیت‌آمیز باشد و این مساله خود بسیار زمانبر است.

در نهایت اینکه انواعی از حملات مبتنی بر دیکشنری‌ها وجود دارد که در دسترس عامل تهدید هستند. اگر مهاجم الگوریتم هَش رمز عبوری[1] را که برای رمزگذاری آن رمز عبور استفاده شده است، بداند، جداول رنگین‌کمانی[2] به او اجازه می‌دهد تا با مهندسی معکوس، آن هَش‌ها را به رمزهای عبور تبدیل کند. نفوذهای اخیر، جداول زیادی از هَش‌های رمز عبور را افشاء کرده است ولی بدون دانستن الگوریتم رمزگذاری، جداول رنگین‌کمانی و تکنیک‌های مشابه آن‌ها و بدون داشتن اطلاعاتی اولیه، قابلیت استفاده خاصی ندارند.

حمله جستجوی فراگیر[3]

حمله جستجوی فراگیر رمز عبور، روشی با کمترین کارایی برای هک رمز عبور است. بر اساس آمارها این روش جزء آخرین روش‌های انتخابی است. بنابه تعریف، جستجوی فراگیر حمله‌ای است که از یک روش برنامه‌نویسی‌شده استفاده می‌کند تا سعی کند تمام ترکیبات ممکن برای رمز عبور را تست کند. این روش برای رمزهای عبوری که طول آن‌ها کم است و پیچیدگی کمی دارند، کارآمد است ولی حتی برای سریع‌ترین سیستم‌های مدرن با رمز عبوری به طول ۷ یا تعداد بیشتری کاراکتر نیز شدنی نیست؛ بنابراین اگر رمز عبوری تنها کاراکترهای حروف الفبا را داشته باشد، مثلاً در انگلیسی همه به فرم بزرگ یا کوچک نوشته شده باشند (و ترکیبی از آن‌ها نباشد)، به $۲^{۷}$ (۱۷۶ ۳۱۸۱۰ ۸۰) حدس نیاز داریم (در این صورت شانس شما برای بردن لاتاری بیشتر از یافتن این رمز عبور است!) البته در اینجا تصور می‌شود که مهاجم طول رمز عبور را می‌داند. عامل‌های دیگر شامل اعداد، حساسیت به کوچک یا بزرگ بودن حروف و دیگر کاراکترهای خاص در زبان‌ها است. حقیقت آن است که حمله جستجوی فراگیر با وجود پارامترهایی مناسب همیشه می‌تواند رمز عبور را بیابد. مشکل زمان موردنیاز است که باعث می‌شود این نوع حمله اهمیت نداشته باشد و دلیلش به خاطر زمان زیادی است که طول می‌کشد تا رمز عبور را پیدا کند،

[1]Password Hashing
[2]Rainbow Tables
[3]Brute Force

پاس کردن هش[1]

پاس کردن هش (PtH) تکنیکی برای هک کردن است که به مهاجم اجازه می‌دهد تا به‌جای اینکه از خود رمزعبور حساب کاربر استفاده کرده باشد، از هَش NTLM مربوط به همان رمزعبور استفاده کند تا به منبع، احراز هویت یابد. بعد از اینکه عامل تهدید به نام کاربری معتبر و هَش رمز عبور دست پیدا کرد، با استفاده از انواع تکنیک‌هایی مانند استخراج حافظه فعال سیستم‌ها می‌تواند از اعتبارنامه‌ها استفاده کند تا به سرور یا سرویس‌های از راه دور با استفاده از احراز هویت LM یا NTLM وارد شود. این حمله از ضعف پیاده‌سازی در پروتکل احراز هویت بهره می‌برد که در آن هَش رمزهای عبور برای هر نشست تا زمانی که خود رمزعبور تغییرکند، ثابت باقی می‌ماند. تکنیک پاس کردن هش را می‌توان تقریباً برای هر سرور یا سرویسی که احراز LM یا NTLM را قبول می‌کند، به کار برد و مستقل از آن است که منبع از ویندوز، یونیکس، لینوکس یا هر نوع سیستم عامل دیگری استفاده کند. سیستم‌های مدرن می‌توانند با استفاده از انواع روش‌ها در برابر این نوع از حملات ایستادگی کنند ولی بر اساس این نقطه ضعف، تعویض رمز عبور به‌صورت مرتب (پس از هر بار نشست تعاملی) استراتژی دفاعی خوبی برای حفظ تفاوت بین خود نشست‌ها است. راهکارهای مدیریت رمز عبوری که می‌توانند رمزهای عبور را به‌طور مرتب عوض کنند یا رمز امنیتی را سفارشی‌سازی نمایند، راهکارهای دفاعی خوبی در برابر این حمله هستند. متأسفانه بدافزارهای مدرن می‌توانند شامل تکنیک‌هایی باشند که هَش‌ها را از حافظه استخراج نمایند و هر کاربر، اپلیکیشن، سرویس یا فرآیند در حال انجام را به یک هدف بالقوه تبدیل کنند. وقتی هَش به دست آمد، دستور و کنترل یا دیگر تنظیم‌های خودکار، اجازه انجام اقدامات بعدی یا برداشت داده‌ها را به عامل تهدید می‌دهد.

سؤالات امنیتی

یکی از تکنیک‌های اجتماعی معمول مورد استفاده به‌وسیله شرکت‌ها و مؤسسات مالی برای تأیید کاربر به‌وسیله حساب، آن است که از آن‌ها سؤالات امنیتی را درباره اطلاعات شخصی‌شان بپرسند. این اطلاعات هنگام تنظیم حسابی جدید به‌وسیله سازمان‌های زیادی به‌صورت احراز هویت دو مرحله‌ای موردنیاز است و در آن از پاسخ‌های چالشی استفاده می‌شود که تنها خود

[1]Pass the Hash

شما می‌دانید (یا تنها تعداد محدودی از افراد می‌دانند). سپس وقتی کاربر نهایی بخواهد از منبعی جدید وارد شود باید به آن سؤال پاسخ دهد، البته در مواردی که شما رمز عبور خود را فراموش کرده باشید و یا حتی وقتی بخواهید رمز عبور خود را بازیابی کنید نیاز به پاسخ به این سؤالات امنیتی دارید. برخی از متداول‌ترین سؤالات امنیتی عبارت‌اند از:

- شهری که در آن متولد شده‌اید؟
- رفیق دوران دبیرستان شما؟
- اولین ماشین شما؟
- غذای مورد علاقه شما؟
- نام معلم اول ابتدایی شما؟
- نام اولین حیوان خانگی شما؟

ریسک افشاء این سؤالات امنیتی و به دست آوردن رمزهای عبور کاربران، احتمال زیادی دارد. به این سناریوها فکر کنید:

- چه تعداد از افراد جواب هر یک از این سؤالات را می‌دانند؟
- آیا جواب‌های این سؤالات به‌صورت عمومی در شبکه‌های اجتماعی، زندگی‌نامه‌ها یا حتی اسناد مدرسه به‌صورت آنلاین در دسترس است؟
- آیا یک بازی را در شبکه‌های اجتماعی انجام داده‌اید که ممکن است این اطلاعات را در آن افشاء کرده باشد؟
- آیا سؤالات امنیتی و احتمالاً جواب آن‌ها در رخنه‌های قبلی دزدیده شده‌اند؟

رابطه آن روشن است. هرچه مکان‌ها و افرادی که جواب سؤال امنیتی شما را می‌دانند بیشتر باشد، احتمال بیشتری وجود دارد که شخصی دیگر بتواند آن‌ها را جواب دهد. به‌علاوه اگر این اطلاعات به‌صورت عمومی در دسترس باشد، در نتیجه این مورد اصلاً یک سؤال امنیتی تلقی نمی‌شود.

وقتی منبعی درخواست می‌کند که سؤالات امنیتی را کامل کرده و جواب دهید، بهترین توصیه آن است که از مبهم‌ترین سؤالاتی استفاده کنید که هیچ‌کس غیر خودتان جواب آن را نمی‌داند و به خاطر داشته باشید که هیچ‌گاه اطلاعاتی مشابه را به‌صورت آنلاین و یا با سایتی که از همان سؤالات امنیتی استفاده می‌کند، به اشتراک نگذارید.

این سناریو مشابه استفاده دوباره از رمز عبور و مهندسی اجتماعی است. سؤالات امنیتی حقایق اجتماعی درباره خودتان هستند و متأسفانه ممکن است در چندین سایت مورد استفاده قرار گیرند. اگر شخصی «فراموشی رمز عبور» در منبعی را درخواست دهد، ایمیل یا بستر پیام کوتاه شما را در اختیار داشته باشد و عبارت امنیتی که شما قبلاً استفاده کردید در چندین سایت یکسان باشد؛ بنابراین می‌تواند از طریق انجام اقدامات بعدی بین منابع مختلف، حساب شما را در دست بگیرد. انتخاب رمزهای عبور یکتا، استفاده از حساب‌های مختلف با ایمیل‌های متفاوت برای انواع منابع (بانک‌ها، مؤسسات، دوستان و غیره) و استفاده نکردن از سؤالات امنیتی یکسان سبب می‌شود که عامل تهدید نتواند سیستم‌های شما را هک کند.

تنظیم مجدد رمزهای عبور

در چه فاصله زمانی رمزهای عبور خود را عوض می‌کنید؟ هر ۳۰ یا ۹۰ روز برای موارد کاری؟ درباره موارد خانگی به چه صورت است؟ در چه فواصل زمانی رمزهای عبور حساب‌های بانکی یا شبکه‌های اجتماعی خود را عوض می‌کنید؟ احتمالاً اغلب این کار را نمی‌کنید و یا اصلاً تغییر نمی‌دهید.

منحصربه‌فرد نگه داشتن تمام رمزهای عبور، پیچیده انتخاب کردن آن‌ها و تغییر مرتب آن‌ها یک وظیفه دلهره‌آور حتی برای افراد حرفه‌ای حوزه امنیت است که از نرم‌افزارهای مدیریت رمز عبور استفاده نمی‌کنند و یا از نظر ذهنی آمادگی تغییر رمز عبور را ندارند. برای مثال، استفاده از ماه، سال، حروف ابتدایی و کمی کاراکترهای خاص برای هر بار، به‌گونه‌ای که الگوی آن را بتوان به یاد آورد روشی متداول است. اگر الگو منحصربه‌فرد باشد و به اشتراک گذاشته نشود، می‌توان ریسک را حداقل ساخت ولی همچنان می‌توان آن را حدس زد چون از الگویی تکراری استفاده می‌کند.

متأسفانه ریسکی متداول در تنظیم مجدد (که نباید با تغییر رمز اشتباه گرفته شود) وجود دارد که آن‌ها را به اهدافی برای عاملان تهدید بدل کرده است. این موارد عبارت‌اند از:

- رمزهای عبور مبتنی بر الگو هنگام تنظیم مجدد (همان‌طور که در بالا بحث شد)؛
- رمزهای عبوری که از طریق ایمیل بازیابی می‌شوند و به‌وسیله کاربر نهایی نگهداری می‌شوند؛

- بازیابی رمزهای عبوری که به‌وسیله هِلپ‌دِسک انجام می‌شوند و هر زمانی که بازیابی رمز عبور درخواست شود، رمز عبور یکسان دوباره مورد استفاده قرار می‌گیرد؛
- بازیابی رمز عبوری که به دلیل مسدود شدن حساب‌هایکاربری به‌صورت خودکار باید انجام شود.

هر زمانی که یک رمز عبور تنظیم مجدد شود، قانونی نانوشته وجود دارد که رمز عبور فعلی بنا به دلایلی برای هر کسی مناسب نیست، یا رمز عبور فعلی فراموش شده است و یا تاریخ آن به پایان رسیده است یا ممکن است به سبب تلاش‌های اشتباه فراوان مسدود شده باشد. بازیابی، انتقال و ذخیره‌سازی رمز عبور جدید یک ریسک است البته تا زمانی که به‌وسیله کاربر نهایی تغییر یابد و یا بدتر از آن کاربر نهایی اصلاً آن را تغییر ندهد. امنیت رمزعبور نامعلوم می‌شود و عامل تهدید می‌تواند از آن بهره ببرد و با درخواست تنظیم مجدد رمز عبور بتواند هویت را به دست آورد و سپس حساب را مطابق با اعتبارنامه‌های خود تغییر دهد و از آن برای فعالیت‌های مخرب بعدی بهره‌ببرد. هر زمانی که کاربری درخواست بازیابی رمز عبور را می‌دهد، همیشه باید از روش‌های مناسب زیر استفاده کرد:

- رمز عبور باید کاملاً تصادفی باشد و الزامات پیچیدگی به ازای هر سیاست سازمانی را محقق کند؛
- رمز عبور باید پس از اولین استفاده به‌وسیله کاربر نهایی تغییر یابد و در صورت امکان از احراز هویت دو یا چند مرحله‌ای برای اعتبارسنجی استفاده شود؛
- رمزهای عبوری که بازیابی آن‌ها به‌وسیله ایمیل انجام می‌شود، با این فرض است که کاربر نهایی هنوز به ایمیل دسترسی دارد تا بتواند به رمز عبور جدید دسترسی پیدا کند. اگر رمز عبور خود ایمیل نیاز به درخواست بازیابی داشته باشد، باید رابط دیگری تعریف شود که ترجیحاً تماس تلفنی است؛
- بازیابی رمز عبور همیشه باید از طرف یک مکان/سایت امن درخواست شود. هرگز نباید به لینک‌های فراموشی رمز عبور که از سمت سایت‌های عمومی وب درخواست می‌شوند، اعتماد کرد و بر روی آن‌ها کلیک کرده یا داده‌ای را وارد کنید؛
- پیامک‌های متنی برای ارسال اطلاعات بازیابی رمز عبور ایمنی لازم را ندارند.

درحالی‌که تغییر متناوب رمزهای عبور از بهترین روش‌ها و اقدامات امنیتی است ولی بازیابی رمزهای عبور و انتقال آن‌ها روش بهینه‌ای نیست. ریسک‌های انجام متناوب آن‌ها برای تعداد

زیادی از کاربران، ریسکی‌هایی بوده که اغلب خود کاربران را تحت تأثیر قرار می‌دهد زیرا اغلب این روش‌های بازیابی رمز عبور ناامن هستند. برای افراد، بازیابی ساده رمز عبور می‌تواند تفاوت عمده‌ای با یک عامل تهدید داشته باشد که سعی دارد تا حساب شما را با استفاده از این روش صاحب شود. سازمان‌ها باید بتوانند این دو کاربرد (تغییر متناوب رمزعبور یا بازیابی متناوب رمزعبور) را متمایز سازند.

تکنیک‌های دیگر

فرض کنید تمام کلمات این کتاب که دارای ۷ حرف یا کمتر هستند بتوانند در حمله هک رمز عبور مورد استفاده قرار گیرند البته اگر کاربر از نکات امنیتی (استفاده ترکیبی از حروف بزرگ و کوچک، ارقام و کاراکترهای خاص) بهره نبرده باشد. آنگاه کاربر یک کلمه انگلیسی ساده را به‌عنوان رمز عبور خود انتخاب کرده است که پایه‌ای‌ترین الزام پیچیدگی طول رمز را رعایت نمی‌کند. وقتی ما مشتقات ساده‌ای از این کلمات را اضافه می‌کنیم تا حروف بزرگ و کوچک را شامل شود و جایگزین‌های خاصی از حروف را برای اعداد در نظر می‌گیریم، مثلاً 0 را به‌جای حرف o، لیستی محدودی از کلمات داریم که افراد به‌صورت آماری برای رمز عبور انتخاب می‌کنند و می‌توان به‌وسیله برنامه‌ای از این کلمات به‌عنوان فرهنگ لغت استفاده کند تا آن‌هایی را که شامل رمزهای عبور قابل حدس زدن هستند، بر روی یک حساب بررسی کند و ببیند که آیا کاربر اشتباهی را مرتکب شده است یا خیر؟ با وجودی که این موارد فرضیاتی پایه‌ای برای هک رمز عبور هستند ولی مرتبط با رمزهای عبور و حقوق ویژه امنی هستند که از رمزهای عبور تصادفی و بسیار پیچیده‌ای استفاده می‌کنند و در راهکارهای مدیریت دسترسی ممتاز کاربرد دارند. رعایت کردن این موارد سبب می‌شود تنها انتخاب برای حدس رمز عبور، جستجوی فراگیر یا روش به دست آوردن هَش از حافظه مانند پاس کردن هش(PtH) باشد. استفاده دوباره از رمز عبور، رمزهای عبور پیش‌فرض و رمزهای عبور ضعیف، عمده رخنه‌های امنیتی مربوط به رمزهای عبور را در سازمان‌ها و دولت‌های مدرن تشکیل می‌دهند. شایان ذکر است که انواع مختلفی از تکنیک‌های دیگر وجود دارد تا بتوان با آن‌ها رمزهای عبور را دزدید که از چندین تکنیک مثل حملات Watering Holes یا Golden Ticket استفاده می‌کنند. لیست این حملات فراتر از آن است که بتوان در این کتاب آن‌ها را به‌صورت کامل پوشش داد. مهم‌ترین نکته در ارجاع به آن‌ها این است که این اهداف، اهداف اولیه حمله برای دزدیدن رمز عبور نیستند. تکنیک‌هایی مثل Watering Holes ابتدا بر آلوده

کردن یک وب‌سایت تکیه دارند تا بتوانند اعتبارنامه‌های ورود کاربر را به دست آورند. مهندسی اجتماعی می‌تواند نقشی داشته و یا نداشته باشد. حملات Golden Ticket تنها بعد از اینکه حقوق مدیریتی یک کنترل‌کننده دامنه هک شد، مورد استفاده قرار می‌گیرد. عامل تهدید باید در ابتدا حساب مدیر دامنه را هک کند تا بتواند گواهی‌های کرِبروس[1] اضافی را ایجاد کند. نکته کلیدی آن است که عاملان تهدید همیشه روش‌های دیگری را برای دزدیدن رمزهای عبور می‌یابند. ما به آن‌ها نام‌های جدید می‌دهیم، بهترین روش‌های مقابله را ارائه می‌کنیم ولی درنهایت، تکنیک هرچه که باشد، آن‌ها یک گام از ما جلو بوده و حساب‌های (با حق ویژه) ما را در اختیار می‌گیرند.

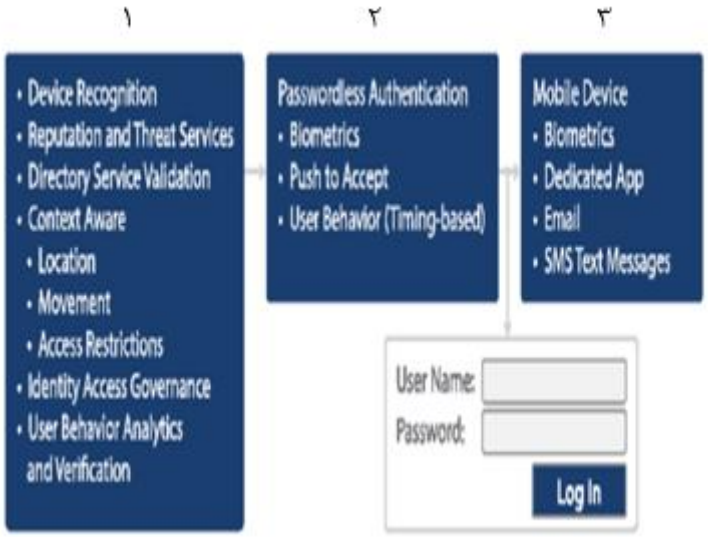
[1]Kerberos

فصل ۴

احراز هویت بدون رمز عبور

درحالی‌که حرکتی به‌سوی حذف رمزهای عبور و اعتبارنامه‌های مرسوم از فرآیند احراز هویت به وجود آمده است و راهکارهای نوظهور زیادی ادعای انجام این کار را دارند ولی متأسفانه حقیقت آن است که تمام این فناوری‌ها همچنان به طبیعت باینری سیستم‌های کامپیوتری متکی هستند. چه احراز هویت شما انجام شود و چه نشود، خروجی همیشه به‌صورت بولی[۱] است. با وجودی که می‌توانید از سناریوهای محتوا- محوری جهت محدودسازی دسترسی و حداقل رساندن ریسک استفاده کنید ولی کاربر هنوز با معیارهای «بله» یا «خیر» و صفر و یکی احراز هویت می‌شود. موقعیت آن‌ها می‌تواند دسترسی را محدود کند، ممکن است دستگاه برای دسترسی به منابع خاصی دسترسی نداشته باشد اما درنهایت، همچنان همه آن‌ها به‌صورت باینری احراز هویت می‌شوند. فناوری‌های نوظهوری که بر راهکارهای موجود ترجیح داده می‌شوند، مثل روش‌های زیست‌سنجی[۲]، سنجش زمان تایپ صفحه کلید و حتی احراز هویت چند مرحله‌ای، همچنان باید پاسخ «بله» یا «خیر» را برگردانند. برای بسیاری از این فناوری‌ها، نگرانی‌های امنیتی جدیدی به وجود آمده است و بقیه آن‌ها نیز ممکن است نقص‌های ذاتی در رویکرد خود داشته باشند (شکل (۴-۱)):

[1] Boolean
[2] Biometrics



شکل (۴-۱). نمونه‌هایی از مکانیزم‌های احراز هویت بدون رمز عبور

۱. شناسایی دستگاه، سرویس های اعتبار و تهدیدات، اعتبارسنجی سرویس‌های دایرکتوری، آگاهی از زمینه‌ها (موقعیت، تحرکات، محدودیت‌های دسترسی)، نظارت دسترسی شناسه، تحلیل و تأیید رفتاری کاربر؛
۲. احراز هویت بدون رمز عبور، زیست‌سنجی، فشار دادن برای پذیرش (Push to accept)، رفتار کاربر (مبتنی بر زمان)؛
۳. دستگاه موبایل، زیست‌سنجی، اپلیکیشن اختصاصی، ایمیل، پیامک‌های متنی.

- روش‌های زیست‌سنجی– این فناوری توسط متخصصان زیادی به‌عنوان جایگزینی مناسب برای اعتبارنامه‌ها در نظر گرفته می‌شود درحالی‌که در واقعیت، زیست‌سنجی‌ها باید برای هر هویت منحصربه‌فرد باشد ولی اثبات شده که می‌توان اثرانگشت را تکثیر کرد، شناسایی چهره را دور زد (مثلاً دوقلوها و شباهت‌ها با فرزند در FaceID) و یا ممکن است پایگاه‌های داده ذخیره‌کننده اطلاعات زیست‌سنجی برای فعالیت‌های خرابکارانه بعدی مورد دستبرد قرار گیرند. زیست‌سنجی‌ها به‌عنوان یک مکانیزم احراز هویت هیچ‌گاه به تنهایی گزینه مناسبی نیستند. همیشه باید آن‌ها را با فرآیندهای احراز هویت چند مرحله‌ای برای اعتبارسنجی یک حساب استفاده

کرد و بنابراین فناوری اعتبارنامه‌ای پایداری به‌عنوان جایگزین برای دنیای امروز نیستند؛

- زمان‌سنجی فشرده شدن کلیدها– فناوری نوظهور دیگری، احراز هویت را بر اساس سرعت تایپ و لمس کلیدهای روی صفحه کلید ارائه می‌دهد. خوشبختانه نتایج این روش بسیار خوب بوده است اما نشان داده شده هنگامی که کاربر در حالت طبیعی خود قرار ندارد و یا مشغول کاری است، سرعت‌های احراز هویت به طور معمول، خطاهای مثبت شناسایی را به همراه دارند. برای مثال اگر دست‌های کاربر شکسته باشد یا تنها با یک دست تایپ کند چون ممکن است با دست دیگر خود چیزی را حمل کند، این مدل‌ها در احراز هویت کاربر شکست می‌خورند چون الگوها و سرعت‌ها هرگز برای این موارد مستندسازی و ثبت نشده است. بخش یادگیری ماشینی باید برای این راهکار آموزش ببیند. در حال حاضر استفاده از اعتبارنامه‌های قدیمی، تنها مکانیزم قدیمی ممکن مورد استفاده است (که با همراه احراز هویت چند مرحله‌ای امن‌تر می‌شود)؛
- Federated Services - یکی از رویکردهای نویدبخش از رویکرد فناورانه، ترکیبی از شناسایی یگانه[1] و احراز هویت چند مرحله‌ای استفاده می‌کند. این رویکرد شما را قادر می‌سازد تا یک‌بار با استفاده از یک مکانیزم قابل اعتماد، به Federated Services احراز هویت انجام دهید. این سرویس ممکن است مبتنی بر اعتبارنامه‌های مرسوم بوده و دیگر فناوری‌های چند مرحله‌ای را شامل گردد که به‌طور معمول در فضای ابری میزبانی می‌شوند. زمانی که احراز هویت انجام شد، اطلاعات شما (موقعیت جغرافیایی، دستگاه، دارایی‌های ریسکی، زمان و تاریخ و غیره) برای احراز هویت دیگر سرویس‌ها و برنامه‌ها، مورد استفاده قرار می‌گیرد. اینکار می‌تواند بلادرنگ باشد و یا مبتنی بر کد دو مرحله‌ای ارسالی به یک اپلیکیشن اختصاصی موبایل، پیامک یا دیگر ابزارها برای اعتبارسنجی نشستی جدید انجام گیرد. حساب‌های رسانه‌های اجتماعی مثل فیس‌بوک و گوگل در این فناوری پیشرو بوده‌اند اما خارج از سرویس‌های Federation اکتیو دایرکتوری مایکروسافت (ADFS) و مایکروسافت لایو، مدل

[1] Single Sign-on

انطباقی در اعتماد به این رویکرد کُند عمل می‌کند مگر اینکه برنامه‌ای تجاری، اختصاصی و چند مرحله‌ای نصب گردد.

در این زمان، راهکارهای بدون نیاز به رمز عبور هدفی هستند که همچنان بر اعتبارنامه‌های سنتی مبتنی بر سیستم‌عامل، اپلیکیشن و استانداردهای احراز هویت تکیه دارند. این موارد تنها لایه‌های جدیدی برای احراز هویت هستند و در حال حاضر نمی‌توانند به‌طور کامل جایگزین اعتبارنامه‌ها شوند. مشکلات زیر مواردی هستند که برای رسیدن به امنیت بدون رمز عبور باید آن‌ها را به‌طور کامل رفع کنیم:

- هنگام خرابی لایه‌های بدون رمز عبور، اعتبارنامه‌ها به‌عنوان تنها روش پشتیبان هستند؛
- فناوری‌های پیشین (و هر فناوری که در زمان انتشار این کتاب ایجاد شده است) هنوز به اعتبارنامه‌ها نیاز دارند، حال چه حساب مدیریتی باشد و چه اعتبارنامه‌های خدماتی. راهکارهای بدون رمز عبور تنها لایه امنیتی جدیدی فراتر از این روش‌ها هستند؛
- ممکن است اعتبارنامه‌ها (همراه با چند مرحله‌ای‌ها) به‌عنوان اولین گام احراز هویت بدون رمز عبور به‌طور پیوسته با شناسایی یگانه یا دیگر سرویس‌های احراز هویت federated باشند. احراز هویت اولیه همچنان از رمز عبور استفاده می‌کند؛
- آسیب فیزیکی به دست، چشم یا صورت می‌تواند مانع عملکرد زیست‌سنجی‌ها شود. Microsoft Hello، گلکسی نوت سامسونگ و FaceID گوشی‌های آیفون شرکت اپل جزء اولین نسل‌هایی هستند که این خدمات را به مشتریان ارائه کرده‌اند و اینکه آیا سازمان‌ها آن‌ها را به‌عنوان مکانیزم‌های سازمانی برای احراز هویت بپذیرند، یک مسئله متکی به زمان است. قابلیت اطمینان آن‌ها، خطاهای مثبت شناسایی و احتمالاً خطاهای منفی شناسایی نیز از جمله عواملی هستند که در قابل‌پذیرش بودن این راهکارهای بدون رمز عبور تعیین‌کننده هستند.

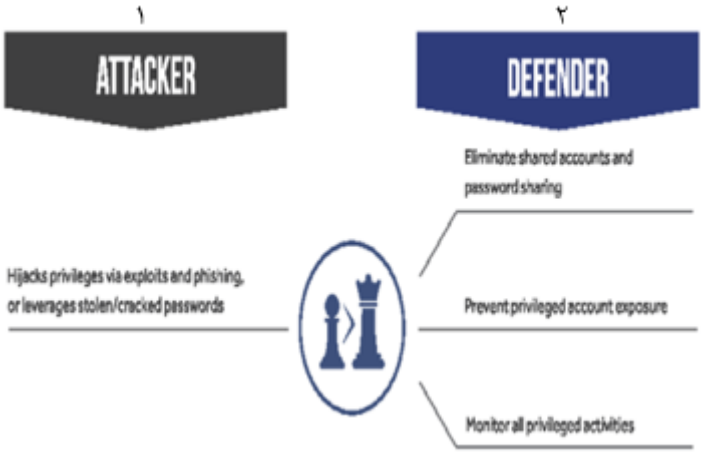
برای عامل تهدید، راهکارهای بدون رمز عبور در مقایسه با اعتبارنامه‌های متداول قدیمی، چالشی جدی را برای دسترسی به حساب‌های با حق ویژه فراهم می‌کنند. به‌هرحال، درست مثل مصیبت‌هایی که در ماجرای هک دوره انتخابات وجود داشت، هر از گاهی بهتر است تا به‌جای سعی در هک کردن سازمان‌های اجراکننده آن فناوری، به دنبال تأمین‌کننده آن

فناوری برویم. اگر شما بتوانید راهکارهای بدون رمز عبور را دور بزنید که می‌تواند با دزدیدن پایگاه‌داده، پیدا کردن اشتباهات یا آسیب‌پذیری‌های خود ابزار انجام شود یا بدافزاری را روی دستگاه موبایل نصب کنید، نتایج نهایی یک نفوذ عملاً یکسان خواهند بود و راهکار بدون رمز عبور واقعاً مزایایی فراتر از قابلیت حفظ رمز عبور به‌وسیله شخص به همراه ندارند.

فصل ۵

ارتقاء حق ویژه

زمانی که یک نشست احراز هویت شده را ایجاد کردیم، چه نشست قانونی باشد و یا چه از طریق هر نوع حمله‌ای هک شده باشد، هدف عامل تهدید آن است که حقوق ویژه خود را افزایش داده و داده‌های سازمان را به دست آورد(که فراتر از مباحث باج‌افزار بودن و یا ایجاد اختلالات در کسب‌وکار است). نگاهی به شکل (۵-۱) داشته باشید. کاربر استاندارد معمولاً حقوقی برای دسترسی به پایگاه‌داده، فایل‌های حساس یا هر چیز با ارزش دیگری در حجم بالا را ندارد پس عامل تهدید چطور محیط شبکه‌ای را کنترل می‌کند و حقوق ویژه مدیر یا روت را به دست می‌آورد تا از آن‌ها در راستای اهداف حمله خود بهره ببرد؟ شش روش اصلی وجود دارد: رمزهای عبور، آسیب‌پذیری‌ها، پیکربندی، اکسپلویت‌ها، بدافزارها و حملات مهندسی اجتماعی. به‌علاوه، نظام‌های احراز هویت ویژه‌ای وجود دارند که می‌توانند ریسک را حداقل سازند و یا برعکس ریسک‌های اضافی به همراه داشته باشند، به طور مثال: احراز هویت چند مرحله‌ای و حقوق ویژه محلی یا متمرکز.



شکل (۵-۱). ربودن و ارتقاءحق ویژه

۱. مهاجم: حقوق ویژه را از طریق اکسپلویت‌ها و حملات فیشینگ می‌رباید یا از رمزهای عبور دزدیده-شده یا کِرک‌شده بهره می‌برد.
۲. مدافع : حساب‌های مشترک و رمز عبورهای اشتراکی را از بین می‌برد. از افشاء حساب های ممتاز جلوگیری می‌کند. تمام فعالیت‌های ممتاز را رصد می‌کند.

رمزهای عبور

بیان کردیم که اعتبارنامه‌های معتبر به شما اجازه می‌دهند تا احراز هویت به منابع را انجام دهید. وقتی اعتبارنامه‌ای منتشر می‌شود معمولاً نام حساب کاربری همان عنوان پیشوند آدرس ایمیل است و به دست آوردن رمز عبور آن حساب،کاری است که هکر باید انجام دهد. حساب آلوده‌شده می‌تواند کاربری استاندارد (کارمندی معمولی)، یک مدیر یا کاربری دارای برخی از مجوزها و حقوق ویژه‌ای باشد که بین دو کاربر استاندارد یا مدیر باشد. اغلب عامل تهدید به‌طور مستقیم مدیر یا مدیر عامل را هدف قرار می‌دهد چون اعتبارنامه‌های آن‌ها، حقوق ویژه دسترسی مستقیم به داده‌ها و سیستم‌های حساس را فراهم می‌کند و می‌توانند با ریسک شناسایی کمتری کارهای بعدی را انجام دهند. متأسفانه یا خوشبختانه اینکار همیشه برای عامل تهدید ممکن نیست و آن‌ها برای این نفوذ باید ابتدا پایگاهی را در محیط سازمان به دست آورند. به دست آوردن این رخنه می‌تواند نتیجه بهره‌مندی از وصله امنیتی اعمال نشده-ای باشد که با حملات مهندسی اجتماعی ترکیب شده است. وقتی نفوذ اولیه با موفقیت انجام

شود، عاملان تهدید عملیات نظارت را انجام می‌دهند و منتظر فرصت مناسبی می‌مانند تا مأموریت خود را دنبال کنند. معمولاً عاملان تهدید مسیری با کمترین دشواری و مانع را انتخاب می‌کنند و اقداماتی را در پیش می‌گیرند تا ردهای به‌جامانده را پاک‌سازی نمایند تا بدین‌صورت ناشناس باقی بمانند. اینکار می‌تواند شامل مخفی کردن[1] آدرس IP منبع و یا پاک کردن داده‌های سابقه ورود به سیستم‌ها باشد چون هر سندی درباره حضور آن‌ها می‌تواند حرکت آن‌ها را متوقف سازد و یا به سازمان اجازه دهد تا به‌صورت جدی نظارت بر آن رخنه را رصد نماید.

چندین فلسفه در رابطه با کاری که باید هنگام تشخیص نفوذ انجام شود، وجود دارد و البته این موضوع خارج از گستره این کتاب است. جدای از آن، هنگام رویارویی با حقوق ویژه هک شده و رمزهای عبور دزدیده شده، هر مجوزی که به آن حساب اعطا شده است، هدفی دست-یافتنی برای یک مهاجم است. درصورتی‌که برای به دست آوردن شواهد بیشتر به آن‌ها برای ادامه کار اجازه داده شود، بایستی به‌طور شفاف ریسک مواردی را که در دسترس آن‌ها است، تعریف شود. بازیابی رمزهای عبور معمولاً بهترین استراتژی است و می‌توان سیستم‌هایی را نیز که به آن‌ها نفوذ شده است، به حالت استاندارد برگرداند (مخصوصاً اگر این سیستم‌ها همان سرورها باشند). اگر که اکسپلویت یا بدافزاری رمز عبور را به دست آورده باشد، انجام یک درخواست ساده از کاربر نهایی برای تغییر رمز عبور، ریسک را کاهش نمی‌دهد زیرا که عامل تهدید می‌تواند توسط بدافزار یا اکسپلویت مجدد رمزعبور را به دست آورد. رمزهای عبور هک‌شده، راحت‌ترین اهداف برای حمله به حقوق ویژه هستند و حساب‌های مربوط به آن‌ها تقریباً تمام جنبه‌های یک محیط فناوری اطلاعات را کنترل می‌کنند؛ بنابراین رمزهای هک-شده روی حساس‌ترین حساب‌ها می‌تواند شکستی برای برخی از سازمان‌ها و برای آن‌هایی باشد که باید همیشه با دقت عمل کنند و به‌طور مناسبی مدیریت رمز عبور و ارزیابی‌های ریسک را انجام دهند.

آسیب‌پذیری‌ها

در نظر داشته باشید که این خود آسیب‌پذیری نیست که اجازه می‌دهد حمله‌ای با اهداف حقوق ویژه، موفقیت‌آمیز باشد. درواقع، آسیب‌پذیری تنها یعنی ریسکی وجود داردو آن چیزی

[1]Masking

جز اشتباهاتی در کدنویسی، طراحی، پیاده‌سازی یا پیکربندی نیست. آسیب‌پذیری به عاملان تهدید اجازه می‌دهد تا احتمالاً به‌وسیله اکسپلویتی کار خود را انجام دهند. پس بدون اکسپلویت، آسیب‌پذیری تنها یک مشکل بالقوه است و در ارزیابی ریسک استفاده می‌شود تا چیزی که می‌تواند رخ دهد را اندازه‌گیری نماید. بسته به آسیب‌پذیری‌ها و اکسپلویت‌های موجود، می‌توان ریسک را محدود کرد و یا آن را فاجعه‌ای مورد انتظار تلقی نمود. با وجودی که اینکار تنها یک ارزیابی ریسک ساده و واقعی است ولی اساس حقوق ویژه به‌عنوان اهدافی برای حمله را ارائه می‌کند. تمام آسیب‌پذیری‌ها و اکسپلویت‌ها یکسان نیستند و بسته به حقوق ویژه کاربر یا اپلیکیشنی که همراه با آن آسیب‌پذیری کار می‌کنند، ممکن است ارتقاء یابند و کارایی اهداف حمله نیز تغییر کند. برای مثال، آسیب‌پذیری Word Proccessor که به‌وسیله کاربری استاندارد اجرا می‌شود، در مقایسه با یک حساب مدیریتی می‌تواند دو مجموعه کاملاً متفاوت از ریسک‌ها را از لحاظ آلوده شدن در بر داشته باشد. یک نفر ممکن است به‌عنوان کاربری استاندارد تنها به حقوق ویژه کاربر محدود شود و دیگری ممکن است دسترسی مدیریتی کاملی را به سیستم میزبان داشته باشد. اگر کاربر از حساب مدیر دامنه یا سایر حقوق ویژه استفاده کند، اکسپلویت می‌تواند مجوزهایی را به تمام محیط داشته باشد. این چیزی است که عامل تهدید به‌عنوان ثمره‌ای دست‌یافتنی مورد هدف قرار می‌دهد. اینکه چه کسی خارج از بهترین روش‌های امنیتی[1] کار خود را انجام می‌دهد و من چطور می‌توانم از آن‌ها بهره‌ببرم تا به محیط نفوذ کنم؟

با در نظر گرفتن این موضوع، آسیب‌پذیری‌ها می‌توانند اشکال و ابعاد مختلفی داشته باشند. می‌توانند سیستم‌های عامل، برنامه‌ها، برنامه‌های تحت وب، زیرساخت‌ها و غیره را هدف قرار دهند. همچنین می‌توانند پروتکل‌ها، ارتباطات و انتقال‌های بین منابع از شبکه‌های سیمی، وای‌فای تا فرکانس‌های رادیویی صوتی را نیز هدف قرار دهند. به‌هرحال تمام آسیب‌پذیری‌ها اکسپلویت ندارند. برخی‌ها اثباتی از مفاهیم هستند، برخی‌ها غیرقابل اطمینان بوده و برخی نیز به‌عنوان سلاحی مورد استفاده قرار می‌گیرند و حتی در ابزارهای تست نفوذ تجاری یا متن‌باز رایگان مورد استفاده قرار می‌گیرند. برخی از اکسپلویت‌ها در Dark Web به مجرمان سایبری فروخته می‌شوند و بقیه نیز به‌طور انحصاری به‌وسیله دولت‌ها مورد استفاده قرار می‌گیرند تا زمانی که وصله شوند و یا به‌صورت عمومی افشاء گردند (چه عمدی و چه غیر

[1]Security Best Practice

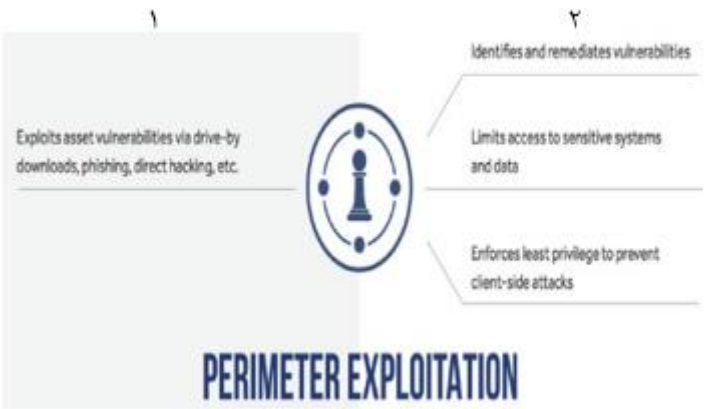
عمد). نکته آن است که آسیب‌پذیری‌ها می‌توانند در هر چیزی و هر زمانی وجود داشته باشند اما این نحوه بهره‌برداری از آن‌ها است که اهمیت دارد، همچنین امکان دارد آسیب‌پذیری خود به اکسپلویتی منجر شود که می‌تواند حقوق ویژه را تغییر دهد (ارتقاء مجوزهای یک کاربر به کاربری با سطح دیگر). تا به امروز، کمتر از ۱۰ درصد تمام آسیب‌پذیری‌های مایکروسافت که وصله شده‌اند، امکان ارتقاء حق ویژه را داشتند. صنعت امنیت چندین استاندارد برای ریسک‌ها، تهدیدات و موارد مرتبط با آسیب‌پذیری دارد. متداول‌ترین استانداردها به‌صورت زیر هستند:

- استاندارد CVE[۱]– استانداردی برای نام‌ها و توضیحات آسیب‌پذیری‌های امنیت اطلاعات؛
- استاندارد CVSS[۲]– سیستمی ریاضیاتی برای امتیازدهی به ریسک آسیب‌پذیری‌های اطلاعاتی؛
- استاندارد XCCDF[۳]–یک زبان مشخص برای نوشتن چک‌لیست‌های امنیتی، بنچ-مارک‌ها و انواع اسناد مربوطه؛
- استاندارد OVAL[۴]–انجمن امنیتی اطلاعات که تلاش دارد تا نحوه ارزیابی و گزارش وضعیت ماشینی سیستم‌های کامپیوتری را استانداردسازی نماید.
- استاندارد CCE[۵]–شاخص‌های یکتایی را برای مشکلات پیکربندی سیستم ارائه می‌کند تا همبستگی سریع و دقیق پیکربندی داده میان چندین منبع و ابزار اطلاعاتی را تسهیل نماید؛
- استاندارد CWE[۶]–زبان عامه از مباحثه را برای بررسی و یافتن دلایل آسیب‌پذیری‌های امنیتی نرم‌افزاری را که در کد پیدا شده است، ارائه می‌کند؛
- استاندارد CPE[۷]– طرح نام‌گذاری ساختار یافته برای سیستم‌ها، نرم‌افزارها و پکیج‌های فناوری اطلاعات؛

[1]Common Vulnerabilities and Exposure
[2]Common Vulnerability Scoring System
[3]The Extensible Configuration Checklist Description Format
[4]Open Vulnerability Assessment Language
[5]Common Configuration Enumeration
[6]Common Weakness Enumeration Specification
[7]Common Platform Enumeration

- استاندارد CCSS[1]– مجموعه‌ای از معیارهای مربوط به میزان و شدت مشکلات پیکربندی امنیتی نرم‌افزار است و استاندارد CCSS، شاخه‌ای از استاندارد CVSS است.

نتایج تمام این اطلاعات به افراد حرفه‌ای امنیت و تیم‌های مدیریتی اجازه می‌دهد تا ریسک‌های آسیب‌پذیری‌ها را مورد بحث قرار دهند و اولویت‌بندی نمایند. بدون وجود زبانی عام و ساختاری واحد میان فروشنده‌ها، شرکت‌ها و دولت‌ها، ارزیابی‌های آسیب‌پذیری‌های بین سازمان‌ها تقریباً بی‌معنی است. ریسک‌های حیاتی بسته به محیط شرکت‌ها می‌توانند برای یک شرکت وجود داشته و برای شرکتی دیگر وجود نداشته باشند. استانداردهایی مانند سیستم امتیازدهی به آسیب‌پذیری‌های عام (CVSS) به آن‌ها این امکان را می‌دهد تا به‌درستی امتیازبندی هر آسیب-پذیری را به تمام ذی‌نفعان اعلان کنند. نگاهی به شکل (۵-۲) داشته باشید که در آن اکسپلویت نفوذ به محیطی نشان داده شده است.



شکل (۵-۲). اکسپلویت محیط و ملاحظات

۱. آسیب‌پذیری‌های دارایی‌ها را از طریق دانلودهای ناخواسته به‌وسیله قربانی، حملات فیشینگ، هک مستقیم و غیره اکسپلویت می‌کند؛
۲. آسیب‌پذیری‌ها را شناسایی و رفع می‌کند؛ دسترسی به سیستم‌ها و داده‌های حساس را محدود می‌کند. حداقل حقوق ویژه را اجرا می‌کند تا مانع از حملات سمت مشتری شود. نفوذ با اکسپلویت کردن محیط

[1]Common Configuration Scoring System

پیکربندی‌ها

نقص‌های پیکربندی شکل دیگری از آسیب‌پذیری‌ها هستند، با این‌وجود نقص‌هایی هستند که به رفع آن‌ها نیازی نیست و باید آن‌ها را کاهش داد. تفاوت بین رفع و کاهش آن‌ها یک نکته کلیدی است. رفع آن به اجرای وصله نرم‌افزاری یا سخت‌افزاری اشاره دارد که برای تصحیح آسیب‌پذیری به کار می‌روند که اینکار مدیریت وصله نام دارد اما کاهش آن تنها تغییر در برخی سطوح از وضعیت موجود است که ریسک اکسپلویت شدن را تغییر داده یا کاهش می‌دهد. اینکار می‌تواند تغییری ساده در فایل، سیاست گروهی یا به‌روزرسانی گواهینامه‌ها باشد. در انتها باید بیان شود که این موارد تنها آسیب‌پذیری‌هایی مبتنی بر پیکربندی‌های ضعیف هستند و ممکن است به‌وسیله عامل تهدید به‌سادگی به‌عنوان هدف حمله‌ای دارای حق ویژه مورد استفاده قرار گیرند.

متداول‌ترین مشکلات پیکربندی برای حقوق ویژه شامل حساب‌هایی است که از راهکارهای امنیتی پیش‌فرض ضعیف استفاده می‌کنند. این موارد می‌تواند رمزهای عبور خالی یا پیش-فرضی باشند که به‌محض پیکربندی اولیه برای حساب‌های مدیر یا روت تنظیم می‌شوند یا مسیرهای ارتباطی ناامنی باشند که بعد از نصب اولیه قفل نشده‌اند و این امر ناشی از نبود تخصص یا درب‌های پشتی مستند نشده است. به‌هرحال نقص‌های پیکربندی تنها به تغییری برای برطرف شدن نیاز دارند و اگر این نقص به اندازه کافی شدید باشد، عامل تهدید می‌تواند حقوق ویژه‌ای را با کمترین تلاش به دست آورد.

اکسپلویت‌ها

اکسپلویت‌ها به آسیب‌پذیری نیاز دارند و بدون یک نقص قابل مستندسازی، اکسپلویتی نمی‌تواند وجود داشته باشد. ممکن است زمانی که اکسپلویت جدیدی منتشر می‌شود، به‌صورت دقیق متوجه آسیب‌پذیری نشویم لذا ممکن است متخصصان امنیتی به زمانی نیاز داشته باشند تا اکسپلویتی را مهندسی معکوس نمایند تا دریابند از چه آسیب‌پذیری استفاده می‌کند. انجام اینکار معمولاً به دانش فنی بالایی نیاز دارد و همان‌طور که در بخش آسیب‌پذیری‌ها اشاره شد، اکسپلویت‌ها نیز می‌توانند اشکال و ابعاد مختلفی را به خود بگیرند. می‌توان از آن‌ها برای نشر اطلاعات، نصب بدافزار و نظارت استفاده کرد و درنهایت هدف ایجاد رخنه‌ای پایدار و ناشناس در یک منبع هست. اکسپلویت‌ها با توجه به روش اجرایشان می‌توانند بسیار مخرب

باشند، اکسپلویتی که می‌تواند حقوق ویژه به دست بیارود، کد اجرا کند و بدون شناسایی کارش را انجام دهد، بسیار به آسیب‌پذیری‌ها وابسته است ولی در زمان اجرا به حق امتیازهایی که اکسپلویت دارد نیز وابسته می‌شود. به همین دلیل است که مدیریت آسیب‌پذیری، ارزیابی‌های ریسک، مدیریت وصله و حقوق ویژه بسیار اهمیت دارند. اکسپلویت‌ها تنها می‌توانند در محدوده منبعی که آلوده می‌کنند، اجرا شوند و درصورتی‌که به دلیل رفع نقص‌ها، آسیب‌پذیری وجود نداشته باشد، هیچ اکسپلویتی هم نمی‌تواند اجرا شود. اگر حقوق ویژه کاربر یا اپلیکیشن مربوط به آسیب‌پذیری، پایین باشد (کاربر استاندارد) و امکان اجرای اکسپلویت-های ارتقاءحقوق ویژه‌ای وجود نداشته باشد، حمله محدودخواهد شد. به‌هرحال توجه شود که: اکسپلویت حتی در سطح حق امتیازهای کاربر استاندارد می‌تواند سبب خرابکاری به شکل باج‌افزار یا دیگر حملات مخرب شود. خوشبختانه عمده آن‌ها را می‌توان تنها با کم کردن حق امتیازها و حداقل ساختن سطح حمله برای حملات با اهداف حقوق ویژه کاهش داد. اکسپلویت‌ها بهترین نتیجه را با بالاترین حقوق ویژه به دست می‌آورند؛ بنابراین کمینه‌سازی آن‌ها یکی از بهترین روش‌های امنیتی برای شکست اکسپلویت‌ها و محروم گذاشتن عامل تهدید از آلوده‌سازی یک سازمان است.

بدافزارها

بدافزارها که معمولاً شامل ویروس‌ها، جاسوس‌افزارها، تبلیغ‌افزارها، باج‌افزارها و غیره هستند، درواقع هر نوع نرم‌افزار نامطلوب و نامعتبری هستند که با قصد خرابکاری روی یک منبع طراحی شده‌اند. قصد اجرای آن‌ها می‌تواند از نظارت، نشر داده، اختلال، دستور و کنترل گرفتن تا باج‌خواهی باشد. بدافزارها می‌توانند وسیله فعالیت مجرمانه سایبری را برای یک عامل تهدید فراهم کنند. بدافزار مثل هر برنامه دیگر می‌تواند در هر مجوزی از کاربر استاندارد گرفته تا مدیر (روت) اجرا شود. بسته به ایجاد، قصد و حق امتیازهای آن، خساراتی که می‌تواند وارد کند ممکن است از آزاری کوچک تا تخریبی کامل باشد. بدافزار می‌تواند از طریق یک آسیب‌پذیری و ترکیب با اکسپلویت یا از طریق نرم‌افزارهای نصب‌کننده قانونی یا حتی مهندسی اجتماعی و حملات فیشینگ روی یک منبع نصب شود. جدای از مکانیزم اجرای بدافزار، انگیزه اصلی اجرای کدی نامعتبر روی یک منبع است و وقتی این کد اجرا شود، جنگی بین عاملان تهدید و شرکت‌های ضدبدافزار برای ممانعت از شناسایی بدافزار و حفظ عملکرد آن آغاز می‌شود. اینکار شامل تطبیق بدافزار برای ممانعت از شناسایی و همچنین

غیرفعال‌سازی راهکارهای دفاعی برای ادامه عملیات نفوذ است. بدافزار بسته به قصدی که دارد می‌تواند عملکردهایی مانند ثبت کلیدهای فشرده‌شده و پاس کردن هش(PtH) را انجام دهد. بدافزار تنها یک وسیله برای ادامه انتشار یک حمله پایدار است و درنهایت به مجوزهایی برای دستیابی به اطلاعات هدف به‌وسیله مهاجم نیاز دارد.

مهندسی اجتماعی

ممکن است شما در کودکی خاطرات تلخ و شیرینی را با فرزندانِ نزدیکان خود تجربه کرده باشید، با وجودی که این مسئله کمی احمقانه به نظر می‌رسد ولی بین ویژگی‌های هکی که تمام ما از طریق مهندسی اجتماعی تجربه می‌کنیم و خواسته‌های یک عامل تهدید برای دسترسی به حقوق ویژه، تفاوت آنچنانی وجود ندارد. انگیزه اصلی خویشاوندان ما آن بود تا از اعتماد ما بهره‌برده و از روی سرگرمی کاری را انجام دهند و بخندند. هرچقدر که این کارها ظالمانه‌تر بود ما درس‌های بیشتری از آن‌ها می‌گرفتیم تا در ادامه مانع از انجام آن‌ها شویم.

مهندسی اجتماعی نیز تفاوتی با این موضوع ندارد. ما اعتماد کورکورانه‌ای به ایمیل، تماس یا نامه دریافتی داریم چون باور داریم شخصی به لحاظ اجتماعی می‌خواهد با ما ارتباط برقرار کند. اگر پیام به‌گونه‌ای تنظیم شده باشد که ما به آن اعتماد کنیم، عامل تهدید اولین گام برای فریب ما را برداشته است. اگر ما به آشنایی‌هایی جعلی که از طرف برخی افراد ارائه می‌شود، حساب باز کنیم، ممکن است به قربانی مهندسی اجتماعی تبدیل شویم. با در نظر گرفتن تهدیدات پیشرفته در دنیای سایبری از باج‌افزار گرفته تا ضبط صدای ما در تماس تلفنی، خروجی می‌تواند بسیار بدتر از آزاری ساده باشد. باید نحوه عملکرد مهندسی اجتماعی را درک کنیم و ببینیم در مرحله اول چطور باید به‌صورت منطقی آن را شناسایی کنیم. از دید مهندسی اجتماعی، عاملان تهدید تلاش دارند تا روی رفتارهای کلیدی انسان سرمایه‌گذاری کنند تا به اهداف خود برسند. از جمله این رفتارها:

- اعتماد- اعتقاد بر اینکه مکاتبه در هر نوعی از سمت یک منبع موثق است؛
- زودباوری- اعتقاد بر اینکه محتوا، هرچند که عجیب و ساده باشد ولی واقعی است؛
- صمیمیت- محتوای هدف به بهترین نحو پاسخ شما را داده یا سبب خوشحالی شما شده است؛

- شکاکیت- محتوای مکاتبه با داشتن غلط املایی یا دستور زبان ضعیف و یا حتی به‌صورت جوابی از سوی یک ربات، باز هم هیچ نگرانی در شما ایجاد نمی‌کند؛
- کنجکاوی- تکنیک حمله شناسایی نشده است یا فرد روش حمله را به خاطر می‌آورد ولی واکنشی نشان نمی‌دهد.

اگر هر یک از این مشخصه‌ها را در نظر بگیریم، می‌توانیم به‌صورت مناسبی اعضاء تیم را آموزش دهیم تا در دام مهندسی اجتماعی نیفتند. دشواری کار در آن است که بر رفتارها و عادات انسان غلبه کنیم تا از مسیر آموزش‌ها منحرف نشوند. برای کسب این هدف، لطفاً تکنیک‌های آموزشی و خودآگاهی زیر را در نظر بگیرید تا مانع از به دام افتادن در حملات مهندسی اجتماعی شوید:

- اعضاء تیم برای درخواست‌های اطلاعات حساس تنها باید به افراد مورد اعتماد سازمان اطمینان کنند. برای تأیید درخواست تنها به قسمت «From» ایمیل دریافتی اکتفا نکنند و حتی Reply کردن به ایمیل‌های قبلی هم مورد تأیید نیست زیرا ممکن است آن حساب یا ایمیل آلوده شده باشد. بهترین گزینه آن است که از احراز هویت دو مرحله‌ای درس بگیریم و تلفن را برداشته و به بخشی که اطلاعات حساس را درخواست کرده، تماس بگیریم و آن درخواست را تأیید نماییم. به‌علاوه، تمام این موارد باید قبل از باز کردن هرگونه پیوست یا کلیک بر روی هر نوع لینکی انجام شوند چون در غیر این‌صورت، اگر ایمیل اهداف مخربی داشته باشد ممکن است قبل از هرگونه تأییدی آن فعالیت مخرب اجرا شود؛
- اگر درخواست از سمت منبعی ناشناس آمد ولی نسبتاً مورد اعتماد به نظر می‌رسید، برای مثال درخواست از سمت بانک یا شرکتی باشد که با آن تعامل دارید، تکنیک‌هایی ساده می‌توانند مانع فریب شما شوند. ابتدا تمام لینک‌های موجود در ایمیل را بررسی کنید و مطمئن شوید که شما را به آدرس مناسبی هدایت می‌کنند، تنها با رفتن و نگه داشتن موس بر روی لینک در اکثر کامپیوترها می‌توانید اینکار را انجام دهید. اگر درخواست به‌صورت تلفنی است، هرگز اطلاعات شخصی (اعم از رمزها و کدهای عبور) را ارائه ندهید. به خاطر داشته باشید که بانک‌ها و مؤسسات معتبر هرگز از شما درخواست رمزعبور در تماس تلفنی و ایمیل نمی‌کنند و تنها از مکاتبات رسمی استفاده می‌نمایند؛

- آموزش شناسایی اینکه مکاتبه‌ای از اصالت برخوردار است یا خیر، کمی دشوار است. مهندسی اجتماعی می‌تواند در اشکال مختلفی مانند حساب‌هایی با قابلیت پرداخت، نامه‌های عاشقانه، رزومه‌ها، درخواست‌های منابع انسانی و غیره ظاهر شود. درصورتی-که همه همکاران شما مکاتبه ای با محتوای مشابه دریافت کردند، آنگاه می‌توان گفت که احتمالاً به سازمان شما حملات فیشینگ هدفمند انجام شده است. بهترین گزینه آن است که در مرحله اول بررسی کنیم آیا این درخواست باید برای ما ارسال می‌شد یا خیر؟ کاری است که به‌طور معمول انجام می‌دهید و یا دریافت ایمیلی با این محتوا غیرمعمول است؟
- تشخیص مکاتبه‌ای مشکوک، راحت‌ترین راه برای شناسایی و مغموم گذاشتن تلاش‌های مهندسی اجتماعی است. اینکار به کمی بررسی کارآگاه‌گونه مکاتبه با نگاه به اشتباهات املایی، دستور زبان ضعیف، قالب نادرست یا صوت‌های رباتی در تماس نیاز دارد و اگر درخواست از منبعی است که با آن هیچ تعاملی ندارید باید حتماً آن را مورد بررسی قرار دهید. این موارد می‌تواند پیشنهادی رایگان از یک شرکت قایقرانی یا از سمت بانکی باشد که حسابی در آن ندارید. اگر دلیلی برای مشکوک شدن وجود دارد، بهترین کار این است که کمی احتیاط کنید: هیچ پیوست یا فایلی را باز نکنید، روی هیچ لینک یا پاسخی ایمیلی کلیک نکنید و مکاتبه را حذف کنید. اگر مکاتبه واقعی و اصل باشد، بخش مربوطه دوباره با شما تماس برقرار می‌کند؛
- کنجکاوی بدترین جرم از دید مهندسی اجتماعی است. چه می‌شد، چه خواهد شد و در واقع نباید اتفاقی برای من رخ دهد چون اعتقاد دارم به‌وسیله کامپیوتر خود و منابع امنیتی فناوری اطلاعات سازمان کاملاً محافظت‌شده هستم. این فرض اشتباهی است و حملات پیشرفته می‌توانند بهترین سیستم‌ها و راهکارهای امنیتی را دور بزنند و حتی از دستورات سیستم‌عامل برای هدایت حملات خود بهره‌ببرند. بهترین دفاع برای کنجکاوی یک شخص آن است که کاملاً خویشتن‌دار باشد. به تماس‌های ناشناس پاسخی ندهید و اگر هر یک از نشانه‌های بالا را دریافت کردید، پیوست‌ها را باز نکنید و باورتان این نباشد که هیچ اتفاقی برای شما رخ نخواهد داد (حتی برای

کسانی که از سیستم‌عامل مَک[1] استفاده می‌کنند). واقعیت آن است که کنجکاوی و ساده‌لوح بودن شما را به یک قربانی تبدیل می‌کند.

مهندسی اجتماعی مشکل بزرگی است و هیچ فناوری نیست که ۱۰۰٪ بتواند مؤثر باشد. فیلترهای هرزنامه می‌توانند ایمیل‌های مخرب را جدا سازند و راهکارهای ضد بدافزار می‌توانند بدافزارهای شناخته‌شده و مبتنی بر رفتار را بیابند ولی هیچ‌چیزی نمی‌تواند مسئله مهندسی اجتماعی انسان‌ها و تهدیدات داخل سازمانی را متوقف کند. بهترین دفاع در برابر حملات مهندسی اجتماعی آموزش کاربران است و اینکه بدانیم چطور این حملات از عادات و رفتارهای ما بهره‌می‌برند تا به هدف خود برسند. اگر ما بتوانیم نقص‌های خود را دریابیم و مطابق با آن واکنش نشان دهیم، می‌توانیم توانایی عامل تهدید در آلوده کردن منابع و دسترسی به حقوق ویژه درون سازمان را حداقل سازیم.

احراز هویت چند مرحله‌ای

با وجودی که ما به رمزهای عبور به‌عنوان شکل اصلی احراز هویت با اعتبارنامه‌ها تمرکز کردیم ولی تکنیک‌های دیگری می‌توانند مدل احراز هویت را تقویت نمایند. هر یک از آن‌ها مزایا و معایب خود را دارند اما درنهایت، احراز هویت حساب انجام می‌شود و حقوق ویژه آن تأیید می‌شوند. به‌عنوان راهکاری مهم برای امنیت و موردنیاز برای مقامات قانونی، این تکنیک‌های احراز هویت اضافی برای دسترسی امن به‌جای استفاده از یک اعتبارنامه نام کاربری و رمز عبور، ضروری هستند. این موارد یک لایه اضافی را ارائه می‌کنند که هک کردن آن را دشوار می‌سازند (اما آن را به امری غیرممکن بدل نمی‌کنند) و بنابراین همیشه به‌عنوان راهکاری برای امنیت اطلاعات حساس پیشنهاد می‌شوند. این مدل، احراز هویت چند مرحله‌ای نام دارد. فرضیه احراز هویت چند مرحله‌ای (که احراز هویت دو مرحله‌ای زیرمجموعه‌ای از آن است) ساده است. علاوه بر اعتبارنامه، نام کاربری و رمز عبور مرسوم، «کد عبور» یا سند اضافی دیگری برای اعتبارسنجی کاربر موردنیاز است. تحویل کد عبور و تصادفی بودن آن در یک فناوری نسبت به فناوری دیگر متفاوت است و این موارد از شرکتی به شرکتی دیگر نیز با هم فرق دارند. این موارد معمولاً شکلی از دانش (چیزی که منحصراً خود آن‌ها می‌دانند)، مالکیت

[1] MacOS

(چیزی که به‌صورت فیزیکی دارند و منحصر به آن‌ها است) و اصلیت (چیزی که وضعیت معین آن‌ها است) را شامل می‌شوند.

استفاده از چندین عامل احراز هویت برای اثبات هویت یک شخص است. فرض بر این اساس است که عامل تهدید غیرمجاز، به احتمال زیادی قادر نیست تمام فاکتورهای موردنیاز را برای دسترسی صحیحی که ناشی از یک متغیر احراز هویت اضافی است، ارائه کند. طی یک نشست، اگر حداقل یکی از مؤلفه‌ها دچار خطا شوند، هویت کاربر با قطعیت کافی (تطبیق ۲ معیار از ۳ مورد) تأیید نمی‌شود و دسترسی به منبعی که با احراز هویت چند مرحله‌ای حفاظت می‌شود، محدود باقی می‌ماند. عامل‌ها و مراحل یک مدل احراز هویت چند مرحله‌ای معمولاً شامل موارد زیر است:

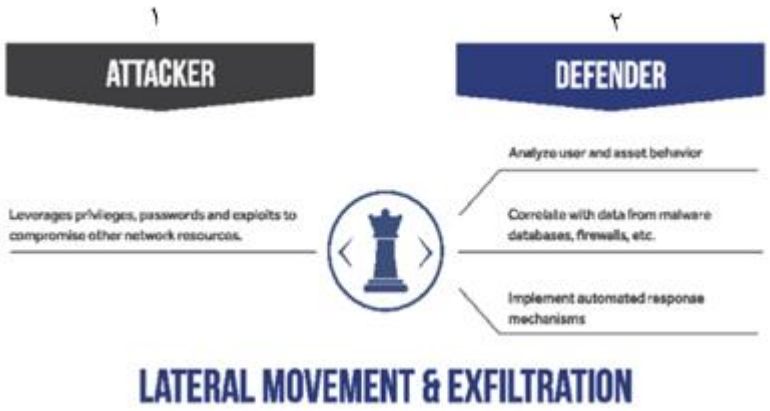
- یک دستگاه سخت‌افزاری یا نرم‌افزاری (مثل برنامه‌های موبایلی که کد عبور امنیتی را به‌طور منظم و به‌صورت تصادفی تولید می‌کند)؛
- کد امنیتی که تنها کاربر نهایی می‌داند، مثل PIN کدهاکه معمولاً به‌صورت ذهنی ذخیره می‌شوند؛
- مشخصه‌ای فیزیکی که می‌توان آن را به‌صورت دیجیتالی برای منحصربه‌فرد بودن مورد تحلیل قرار داد، مانند اثرانگشت، سرعت تایپ یا صدا. این موارد فناوری احراز هویت زیست‌سنجی نامیده می‌شوند.

شایان ذکر است که چند عاملی بودن، یک لایه خاص هویتی برای احراز هویت است ولی وقتی اعتبارسنجی انجام شود، حقوق ویژه اختصاصی به‌عنوان هدف حمله‌ای بالقوه، به میزان قابل-توجهی تغییر نمی‌کند. برای مثال اگر اعتبارنامه‌ها در یک مدل نام کاربری و رمز عبور مرسوم هک شود و افشاء گردد، عامل تهدید می‌تواند با احراز هویت به هر هدفی که به‌صورت محلی یا از راه دور آن‌ها را قبول می‌کند، نفوذ کند. برای احراز هویت چند عاملی، اگرچه به متغیر اضافی مثل حضور فیزیکی نیاز داریم ولی وقتی اعتبارسنجی تأیید شود، مسیریابی بعدی موقعیت اولیه شما همچنان امکان‌پذیر است. تفاوت تنها در نقطه شروع احراز هویت شما است و احراز هویت چند مرحله‌ای باید تمام شرایط امنیتی موردنیاز از یک نقطه ورودی را داشته باشد، درحالی‌که برای اعتبارنامه‌های قدیمی چنین نیست. هکر می‌تواند از اعتبارنامه‌های درون یک شبکه بهره‌ببرد تا از میزبانی به میزبانی دیگر منتقل شود. آن‌ها نمی‌توانند میزبان چند عاملی را برای احراز هویت مورد هدف قرار دهند مگر اینکه خود سیستم چند عاملی هک شود

و یا اینکه آن‌ها تمام موارد امنیتی موجود برای احراز هویت را داشته باشند. از این رو همیشه باید یک نقطه ورودی برای شروع نشست چند عاملی وجود داشته باشد و وقتی وارد شدیم اگر همچنان اقدامات بعدی ممکن بود از اعتبارنامه‌ها یا دیگر ابزارها استفاده کنیم.

حقوق ویژه محلی در برابر حقوق ویژه متمرکز

در فصول بعدی، رویکردهای مختلف برای گزینه‌های مدیریت هویت و حقوق ویژه قوی را مورد بحث قرار می‌دهیم که برای سازمان‌ها نیز در دسترس است. همان‌طور که اهداف حمله دارای حقوق ویژه دسترسی را به‌طور عمیق مورد بحث قرار دادیم، دیدیم که این هدف را می‌توان به بهترین حالت ممکن با یک طرح دسترسی و هویت قوی تأمین کرد که می‌تواند از سرویس‌های دایرکتوری در این امر بهره‌ببرد. به‌هرحال، با توجه به اینکه سازمان‌ها زیرساخت‌های هویتی را تحکیم و ساده می‌سازند، بایستی احتیاط به خرج دهند. اگر این موارد به‌درستی پیاده‌سازی وامن‌سازی نشوند، می‌توانند به بزرگ‌ترین نقطه ضعف حقوق ویژه بدل شوند. اگر یک حساب ممتاز هک شود، ریسک اقدامات بعدی (شکل (۵-۳)) برای دیگر منابع که بر این سرویس متکی هستند و به آن اعتماد دارند، امکان‌پذیر است.



شکل (۵-۳). اقدامات بعدی

۱. مهاجم: از حقوق ویژه، رمزهای عبور و اکسپلویت‌ها بهره می‌برد تا دیگر منابع شبکه را آلوده سازد. ۲. مدافع: رفتار کاربر و دارایی را تحلیل می‌کند. برای داده‌های پایگاه‌های داده بدافزار، دیوارهای آتش و غیره، همبستگی را ایجاد می‌کند. مکانیزم‌های پاسخ خودکار را پیاده می‌کند. اقدامات بعدی و برداشت اطلاعات

به‌هرحال، بدون یک طرح هویت و دسترسی مرکزی قدرتمند، احراز هویت نمی‌تواند بین لایه‌های سیستم‌عامل‌ها، برنامه‌ها، کاربران، فایل‌های سیستمی، داده‌ها و حتی شرکای سازمان وجود داشته باشد. این مشکل دوراهی قدیمی فناوری اطلاعات در ارائه توأم بهترین راهکارهای امنیتی و انجام راحت امور سازمان است. امنیتِ بسیار زیاد مانع انجام کارهای سازمان است و امنیت خیلی کم نیز زمینه را برای عامل تهدید در جهت انجام اقدامات مخرب در سازمان فراهم می‌کند. در انتها باید اشاره کرد که بهترین ملاحظات برای حقوق ویژه، متمرکز ساختن آن‌ها است. این کار کنترل‌های محدودی بر حقوق و مکانی مجزا برای مدیریت آن‌ها را ممکن می‌سازد. برای زیرساخت مدرن امروزی، این امر (متمرکز ساختن حقوق ویژه) بهترین راهکار امنیتی است که می‌توانیم پیاده کنیم.

فصل ۶

تهدیدهای داخلی و درون‌سازمانی

بیشتر متخصصین حوزه امنیت با تهدیدات داخلی زیادی دست و پنجه نرم می‌کنند. تهدیدات درون‌سازمانی موضوع جدیدی نیست، این روش حمله قدیمی تنها به سبب طبیعت، کمیت و حساسیت داده‌هایی که به‌صورت الکترونیکی دزدیده می‌شوند، عمومی‌تر شده است. سال‌ها پیش، این حملات به‌صورت مرتب رخ می‌دادند ولی پیامدهایی که امروزه دارند، متفاوت از پیامدهای آن‌ها در گذشته است البته این بدان معنا نیست که این حملات در آن زمان پذیرفته شده بودند. باید درباره ماهیت تهدید درون‌سازمانی واقع‌بین باشیم و بپذیریم که این تهدید برای صدها سال، اشکال مختلفی را تجربه کرده است.

بنابر تعریف، تهدید درون‌سازمانی، کاربرنما یا شخصی است که به‌عنوان عامل تهدید عمل می‌کند. این کاربرنماها جدای از تکنیک‌هایی که مورد استفاده قرار می‌دهند، رفتار آن‌ها به سود شرکت نیست و احتمالاً این افراد قوانین را زیر پا گذاشته و اطلاعاتی را که مجوز داشتن آن‌ها را ندارند، برداشت می‌کنند. مثالی از این نوع تهدید، لیست مشتریان است. این موضوع یک تهدید درون‌سازمانی است که امروزه نیز شیوع دارد. فروشنده یا مدیر اجرایی و غیره که قرار است شرکتی را ترک کند، ممکن است نسخه رونوشت یا چاپ‌شده‌ای از لیست مشتریان و سفارش‌ها داشته باشد و زمانی که با کارفرمایی جدید وارد کار شد، از آن به‌عنوان مزیتی رقابتی استفاده نماید؛ هرچند برای اثرگذاری باید حجم این اطلاعات بالا باشد. قرار دادن اطلاعات محرمانه بر روی کاغذهای پرینت‌شده نیز یک تهدید درون‌سازمانی است. واضح است که در گذشته هم این اطلاعات را در قفسه‌های عادی قرار نمی‌دادند ولی امروزه با رسانه‌های الکترونیکی و اینترنت، می‌توان آن حجم از داده را بدون اینکه شخصی متوجه آن شود، از

سازمان خارج نمود. دقت شود که آن قفسه اطلاعات حساس را می‌توان به‌راحتی بر روی یک فِلَش در جیب یک شخص جای داد؛ بنابراین ما برچسب‌هایی برای این نوع از تهدیدات داریم. تهدیدات درون‌سازمانی روزبه‌روز شایع‌تر می‌شوند و این موضوع همچنان متخصصین امنیت را درگیر خود نگه داشته است زیرا این موضوع یک تهدید قدیمی است ولی روش‌ها و حجم بالای داده‌ها، آن‌ها را به امری بدل کرده است که باید به دقت بررسی کرد و برای حفاظت از آن‌ها استراتژی جدیدی طرح‌ریزی نمود.

تهدیدات درون‌سازمانی به دلایل مختلفی رخ می‌دهند. این دلایل نشئت‌گرفته از شخصیت انسان‌ها است که به دنبال ضربه زدن یا به دست آوردن مزیتی علیه یک سازمان هستند. صرف‌نظر از قصد آن‌ها، این جنبه دیجیتالی از تهدیدات درون‌سازمانی است که لازم است بیشترین توجه به آن شود. انسان‌ها غیرمعمول‌ترین کارها را در وخیم‌ترین شرایط انجام می‌دهند ولی اگر اجازه کار به آن‌ها داده نشود، می‌توان ریسک‌های زیادی از تهدیدات امنیتی را کاهش داد. پیشنهاد می‌شود موارد زیر را برای سازمان خود در نظر بگیرید:

- چند نفر به حجم انبوهی از اطلاعات حساس دسترسی دارند؟ این به معنای استفاده از یک برنامه برای بازیابی یک سند نیست بلکه بدان معنا است که آن شخص دسترسی مستقیمی به پایگاه‌داده دارد و یا می‌تواند گزارشی را اجرا کند تا میزان زیادی از اطلاعات را در یک درخواست جستجو برداشت کند؟
- آیا تمام حساب‌ها مربوط به افراد معتبری هستند که هنوز کارمند شرکت هستندو یا با آن ارتباط دارند؟
- هر چند وقت یک‌بار رمزهای عبور حساب‌های حساس را تغییر می‌دهید؟
- آیا دسترسی با حق ویژه به سیستم‌ها یا داده‌های حساس را مورد نظارت قرار می‌دهید؟

درصورتی‌که به‌درستی به این سؤالات پاسخ دهیم به مسائل پیچیده‌ای خواهیم رسید. با این وجود، اگر به تهدیدات درون‌سازمانی اهمیت می‌دهید باید به آن‌ها پاسخ دهید. به این دلیل که:

- تنها مدیران باید به داده‌ها در حجم انبوه دسترسی داشته باشند. اینکار باعث می‌شود فردی در درون سازمان نتواند میزان زیادی از اطلاعات را استخراج کند و یا حساب مدیر اجرایی هک نشود و از آن علیه سازمان استفاده نگردد؛
- هرگز هیچ یک از کاربران نباید از حساب‌های مدیریتی برای کارهای روزانه مانند ایمیل استفاده نمایند. این امر شامل خود مدیران نیز می‌شود چون ممکن است حساب آن‌ها نیز هک شود. تمام کاربران باید مجوزهای کاربر استاندارد را داشته باشند؛
- تمام دسترسی‌ها به داده‌های حساس باید تنها برای کارکنان معتبر باشد. کارکنان قبلی، پیمانکاران نباید به کارهای بنیادی و روزانه دسترسی داشته باشند. این حساب‌ها بسته به سیاست‌های سازمان باید غیرفعال شده و یا حذف گردند؛
- کارکنان زیادی به سازمان‌ها می‌آیند و می‌روند. اگر رمزهای عبور همانی باقی بمانند که در زمان ترک آن‌ها تنظیم شده بود و فرد جدیدی استخدام شود، ریسک دسترسی به داده‌های حساس زیاد می‌شود چون کارکنان قبلی همچنان به‌صورت فنی رمزهای معین برای دسترسی به اطلاعات حساس شرکت را در اختیار دارند؛
- نظارت بر فعالیت‌های ویژه، کاری حیاتی است. این امر شامل پرونده‌ها، نظارت نشست، ضبط نمایشگر، ثبت کلیدهای فشرده‌شده و حتی نظارت بر اپلیکیشن است. چرا؟ اگر فردی در درون سازمان به سیستم حیاتی برای دزدیدن اطلاعات دسترسی داشته باشد، نظارت بر نشست می‌تواند دسترسی آن‌ها را مستند کند و اینکه چطور اطلاعات را استخراج کرده‌اند و چه زمانی این کار را انجام داده‌اند؟

اگر فکر می‌کنید که با دنبال کردن تمام این گام‌ها در برابر تهدیدات داخلی ایمن خواهید بود، اشتباه می‌کنید. این گام‌ها با این فرض است که عامل تهدید به‌طور مستقیم برای دزدیدن اطلاعات آمده است و یا فعالیت مخربی را انجام می‌دهد. تهدیدات داخلی می‌توانند از آسیب‌پذیری‌ها، پیکربندی‌های ضعیف، بدافزارها و اکسپلویت‌ها نیز بهره‌ببرند. عامل تهدید می‌تواند نرم‌افزار غیرمجاز دریافت داده‌ها را بر روی سیستمی نصب کند، از سیستمی بهره ببرد که وصله‌های امنیتی بر روی آن نصب نشده است و با استفاده از درب‌های پشتی به منابعی دسترسی داشته باشد تا انواع مشابهی از فعالیت‌های جمع‌آوری داده را اجرا نماید. تهدیدات داخل سازمانی مربوط به دزدیدن اطلاعات یا اختلال در کسب‌وکار سازمان است ولی بسته به

هوشمندی عامل تهدید، می‌تواند از ابزارهایی استفاده کند که به‌طور معمول با تهدیدات خارجی همراه هستند؛ بنابراین باید تهدیدات امنیتی را که به‌طور خاص از دو سمت وارد می‌شوند، در نظر بگیریم: حقوق ویژه اضافی (که در بالا بحث شد) و حفاظت امنیتی ضعیف (مدیریت آسیب‌پذیری و پیکربندی).

برای رسیدن به این منظور، تمام سازمان‌ها باید این وظایف را نیز به‌طور مرتب اجرا کنند تا سیستم‌های خود را محفوظ نگه دارند:

- مطمئن شدن از اینکه راهکارهای ضدویروسی و حفاظتی برای نقاط انتهایی نصب‌شده و در حال اجرا هستند و به‌روز باقی می‌مانند؛
- اجازه به ویندوز و برنامه‌های ثالث برای به‌روزرسانی خودکار یا اجرای راهکارهای مدیریت وصله برای نصب پَچ‌های امنیتی به‌صورت مرتب؛
- استفاده از یک راهکار ارزیابی یا مدیریت آسیب‌پذیری برای تعیین اینکه ریسک‌های موجود در کجای محیط سازمان قرار دارند و تصحیح آن‌ها به‌صورت مرتب؛
- پیاده‌سازی یک راهکار کنترل اپلیکیشن برای اینکه تنها به برنامه‌های معتبر اجازه اجرا شدن با حقوق ویژه را بدهیم تا ریسک حملات را کاهش دهیم؛
- در جایی که ممکن است کاربران را بر حسب سیستم‌ها و منابع تقسیم‌بندی کنیم تا ریسک‌های تهدیدات مستقیم را کاهش دهیم.

با وجودی که این موارد پایه‌ای به نظر می‌رسند ولی واقعیت آن است که اکثر سازمان‌ها حتی در پایه‌ای‌ترین موارد کارشان را خوب انجام نمی‌دهند. اگر آن‌ها این اقدامات امنیتی را انجام دهند، ریسک تهدیدات داخلی را می‌توان با دسترسی مدیریتی و به‌روز نگه داشتن منابع فناوری اطلاعات با آخرین وصله‌ها و راهکارهای دفاعی به حداقل رساند. تهدیدات داخلی قرار نیست از بین بروند. این تهدیدات صدها سال وجود داشته‌اند ولی وسایل و تکنیک‌های مورد استفاده آن‌ها تکامل یافته و به فناوری‌های مدرنی بدل شده‌اند. هدف همان است: از نشر داده‌ها جلوگیری شود و آگاه باشیم که هر عامل داخلی، چندین هدف و روش حمله برای رسیدن به اهداف خود دارد. به‌عنوان متخصصان امنیتی، باید ریسک‌ها را در ابتدای امر کاهش دهیم. کیف‌ها و حجم‌های کوچکی از مدارک نیز هنوز تهدیداتی داخلی هستند ولی به اندازه فلشی که حاوی تمام اطلاعات مشتریان پایگاه‌داده شماست، خطرناک نیستند. در انتها باید

ذکر شود که هر عامل داخلی همچنان به حقوق ویژه‌ای برای دزدیدن تمام این اطلاعات نیاز دارد.

فصل ۷

شکار تهدید

آیا در دوران کودکی و یا حتی در بزرگ‌سالی، بازی معمایی «Where's Waldo?» را انجام داده‌اید؟ اگر این بازی را انجام داده باشید، متوجه می‌شوید که این بخش چه ارتباطی با شکار تهدید دارد لذا برای کسانی که درباره این بازی چیزی نشنیده‌اند، بیان می‌کنیم که هدف این بازی آن است که عکسی از والدو (Waldo) را درون تصویری پر از تصاویر گرافیکی و افراد پیدا کنیم. پیدا کردن والدو سخت است و تشخیص آن در میان جمعیتی پر از تصاویر متفاوت در برخی اوقات بسیار ناامیدکننده می‌شود. در اینجا مسئله بازی صبر، هوش تصویری و بررسی مبتنی بر روشی درست در تصاویر مطرح است. برای سخت‌تر شدن، روش‌های جدید در این بازی، تصاویری دارد که در آن تقریباً تمام اشخاص والدو هستند. هدف در این نوع بازی آن است که فردی که والدو نیست را پیدا کنیم. این موضوع، نمونه تشابهی از خطاهایی شناسایی مثبتی است که هنگام اجرای شکار تهدید به وجود می‌آیند و به همین دلیل این تشابه بسیار مهم است.

پس برای متخصصان حرفه‌ای امنیت، شکار تهدید چیست؟ شکار تهدید، اقدامی برای امنیت اطلاعات پردازشی و جستجوی فرآیندمحور در میان شبکه‌ها، دارایی‌ها و زیرساخت‌ها جهت یافتن تهدیدات پیشرفته‌ای است که از دست راهکارهای امنیتی و دفاعی موجود فرار می‌کنند. دیوارهای آتش، راهکارهای جلوگیری از نفوذ و مدیریت داده‌های ثبتی برای تشخیص و حفاظت در برابر تهدیدات طراحی شده‌اند، حتی اگر که این تهدیدات کاملاً نوین و پیشرفته باشند. شکار تهدید لایه‌ای است برای اینکه ببینیم «چه تهدیداتی به‌صورت فعالانه در شبکه اجرا می‌شوند و من اطلاعی ندارم و چطور می‌توانم آن‌ها را پیدا کنم؟» این لایه محیطی را با

فرض اینکه تهدیدی در آن وجود دارد و در حال حاضر آلوده شده است، در نظر می‌گیرد. راهکاری ساده برای اکثر شرکت‌ها این است که داده‌ها را جمع‌آوری کرده، بررسی و ارائه نمایند. اینکار شامل عمیق‌تر شدن در فایل‌های ثبتی، بررسی دسترسی‌ها برای ورودهای ناموفق و پردازش رویدادهای جمع‌آوری‌شده اپلیکیشن‌ها باشد اما این چیزی نیست که درواقع شکار تهدید باشد. این گام‌ها صرفاً راهکارهای امنیتی هستند که در راهبردهای بیشتر استانداردهای قانونی از PCI گرفته تا NIST به‌منظور بررسی و مدیریت فایل‌های ثبتی وجود دارند. شکار تهدید می‌تواند فرآیند خودکار یا دستی کشف تهدیدات پنهان باشد، این فرآیند فرض می‌کند که تهدیدی وجود دارد و شما فقط باید آن را بیابید. فرآیند شکارتهدید شامل پردازش چندین منبع به‌طورهم‌زمان و جمع‌آوری اطلاعات با دانشی ذاتی از سیستم‌ها و زیرساخت‌هایی است که اطلاعات را تولید می‌کند. با وجودی که شاید این جواب، پاسخی ساده و مختصر به نظر برسد ولی این‌طور نیست. ابزارهای مدیریت سازمانی اطلاعات امنیتی[1] (SIEM) برای این طراحی شده‌اند تا این اطلاعات را در خود جمع‌آوری کرده و نگه دارند ولی تنها برچسب‌زنی محدودی از داده‌ها را بر حسب منبع و نوع آن ممکن می‌سازند تا عناصرسازمان را در آن‌ها اعمال کنیم. این موارد درست مانند دیگر فناوری‌ها در برابر اعمال عناصر انسانی شکست می‌خورند. برای کمک به این موضوع و درک مستقیم داده می‌توان این فرآیند را با استفاده از تحلیل‌های رفتاری یا یادگیری ماشینی به‌صورت خودکار انجام داد. برای موفقیت‌آمیز بودن شکار تهدید، متخصصان حرفه‌ای امنیتی باید با یک فرضیه شروع کنند. این فرضیه تهدیدی را فرض می‌کند و الگوها را ترسیم می‌کند و سپس به‌صورت دستی داده‌ها را مرور می‌کند تا به نتیجه‌ای برسد (اینکه تهدیدات به‌صورت فعالی در حال اجرا هستند). فرضیه‌های معمول به صورت زیر است:

- تحلیلی: می‌توان الگوها را در انجام تحلیل‌های خودکار با رتبه‌بندی‌های ریسک مشخص کرد و از آن‌ها درصورتی‌که یک رخداد با ریسک بالا شناسایی شد، استفاده کرد؛
- موقعیتی: اهداف با ارزش بالا مورد تحلیل قرار می‌گیرند که شامل داده‌ها، دارایی‌ها و کارکنان می‌شود و می‌توان با این تحلیل‌ها ناهنجاری‌ها را یافت؛

[1] Security Information Enterprise Managers

- هوشمندی: همبستگی الگوهای تهدید، بدافزارها و اطلاعات آسیب‌پذیری برای بیرون کشیدن نتیجه.

بنابراین برای موفقیت‌آمیز بودن شکار تهدید، باید الزامات زیر را محقق کنیم وگرنه داده‌ها و شکار ما ناقص می‌ماند:

- حساب‌های مدیریتی و ممتاز (دارای حق ویژه) به‌صورت مناسبی برای مدل‌سازی داده شناسایی شوند؛
- منابع اطلاعاتی را می‌توان با CVE، آدرس IP و نام میزبان[1] به‌طور قابل اطمینانی همبسته نمود. تغییرات ناشی از DHCP و حتی همگام‌سازی زمانی (پیاده‌سازی ضعیفNTP) می‌توانند نتایج شکار تهدید را بی‌معنی سازند. باید بتوانیم به وضوح و به‌طور آشکاری به اطلاعات اعتمادکنیم؛
- ابزارهای قدرتمندسازی مثل یکSIEM، تمام منابع داده‌های قابل اعمال برای شناسایی الگو را جمع‌آوری می‌کنند؛
- به‌صورت آزمایشی تهدیدات و رویدادهای نفوذ جدی در سازمان، اجرا شده و برای ساخت فرضیه مورد استفاده قرار می‌گیرند؛
- ابزارها برای ارزیابی‌های ریسک، تشخیص نفوذ و جلوگیری از حمله به‌روز هستند و به‌درستی کار می‌کنند، اگر این سیستم‌ها مشکل داشته باشند، صف اول دفاعی شما در خطر است؛
- مستندسازی مانند مستند کردن نقشه شبکه‌ها، توضیحات فرآیندهای سازمانی، مدیریت دارایی‌ها و غیره حیاتی هستند. شکار تهدید به عنصری انسانی برای جمع‌آوری اطلاعات تکیه دارد. بدون توانایی نگاشت تراکنش‌ها به گردش کاری الکترونیکی آن، فرضیه نسبت به اینکه تهدید چطور رخ داده و دائمی باقی خواهد ماند، ناتوان است.

شکار تهدید بیشتر شبیه به بازی «Where's Waldo?» است. شما می‌دانید که عامل تهدید وجود دارد، می‌دانید که به چه شکلی است ولی نمی‌توانید آن را پیدا کنید. با وجودی که شکار تهدید ممکن است نداند تهدید دقیقاً به چه شکلی است ولی فرض درستی است که آن تهدید

[1]Hostname

در حال انجام کاری نادرست است و یا قرار است در آینده خرابکاری انجام دهد. اگر شما بتوانید آن تهدید پنهان را بیابید، می‌توانید والدو را بیابید. به مسئله، معما و بازی با اهدافی روشن فکر کنید و از ابزارهای موجود خود بهره‌ببرید و تنها از یک گزارش یا هشدار نامعلوم استفاده نکنید. برای شکار تهدید باید عمیق شوید، از عینکی ذره‌بینی استفاده کنید و بر حس خود برای یافتن آن تهدید تکیه داشته باشید. داشتن بهترین روش‌های امنیتی برای آغاز، یک الزام حتمی برای موفقیت است چون هرکاری که شما برای شکار تهدید انجام می‌دهید، به خود آن تهدید بستگی دارد. همچنین ممکن است عاملان تهدید حرفه‌ای از ابزارهای امنیتی موجود در سازمان بر علیه شما بهره ببرند تا پنهان باقی بمانند. به همین دلیل باید راهکارهای امنیتی بسیار مستحکمی را قبل از حرکت به سمت شکار تهدید داشته باشید. جدای از آن، اگر عامل تهدید در محیط شما است و راهکارهای موجود نمی‌توانند آن را پیدا کنند، باید حقوق ویژه‌ای را بررسی کنید که آن‌ها برای پنهان شدن از آن استفاده می‌کنند.

فصل ۸

بازرسی و حفاظت داده محور

حفاظت از اطلاعات در گذشته نسبت به حال بسیار آسان‌تر بود به‌طوری‌که راهکارهای دفاعی به‌صورت مناسبی در سازمان قرار داشته و راه‌های دسترسی به داده‌های شما بسیار بود. این داده‌ها از دستگاه‌های IT و کنترل‌شده سازمانی و برنامه‌های آن‌ها ارسال می‌شد که بر روی سرورهای شما و در آرایه‌هایی از فضای ذخیره‌سازی قرار می‌گرفت.این داده‌ها با ایجاد مرزی بین داخل و بیرون از سازمان و همچنین اعتماد به افراد درون‌سازمانی حفاظت می‌شد ولی امروزه همه‌چیز به‌شدت تغییر کرده است. حال داده‌های بیشتری از برنامه‌ها، کاربران، دستگاه‌ها، خدمات ابری و سخت‌افزارهای متصل‌شده به آن‌ها جمع‌آوری می‌شود و رفته‌رفته میزانی از داده‌ها که تحت کنترل سازمان باشد، کاهش می‌یابد. انواع سازمان‌های جدید به دسترسی آسان از دنیای بیرون نیاز دارند. با ظهور فضای ابری، داده‌های شما، کاربران و برنامه‌ها ممکن است دیگر در درون سازمان نباشند. افرادی که به داده‌های شما دسترسی دارند رو به افزایش بوده و شامل واحدهای ثالثی است که به‌هیچ‌وجه برای سازمان شما کار نمی‌کنند. رویکرد مدیریت جزئیات دسترسی به این داده‌ها، DCAP (بازرسی و حفاظت داده محور[1]) نامیده می‌شود.

مدل‌های رایانشی سنتی (مدل ارتباطی سیستم‌های باز- ISO) اجازه دسترسی به تمام مؤلفه‌های روی یک سرور در یک ابر را می‌دهد و داده‌ها را بر اساس احراز هویت کاربر مهیا می‌کند. کاربر احراز هویت شده، بسته به حق امتیازها (آلوده‌شده، مجاز یا عامل تهدید) می‌تواند

[1]Data-Centric Audit and Protection

تمام این سلسله‌مراتب‌ها را طی کند و به فایل‌های سیستمی و پیکربندی پلتفرم دسترسی داشته باشد البته اگر حقوق ویژه او اجازه این امر را بدهند (به شکل (۸-۱) مراجعه کنید).

محدودیت‌ها و ممیزی‌ها تنها به‌وسیله لیست‌های کنترل دسترسی محلی و دسترسی مبتنی بر نقش در برنامه‌ها، پایگاه‌های داده و سیستم‌های عامل نظارت می‌شوند؛ بنابراین مدیر می‌تواند به هر فایل و حجمی از اطلاعات به دلیل نقش مدیریتی خود به‌سادگی دسترسی داشته باشد. کاربران مجوزدار در قسمت‌های مختلف ما بین یک کاربر استاندارد و مدیر ممکن است نیازمند دسترسی به یک اپلیکیشن باشند ولی دسترسی محدودی به فایل‌های سیستمی داشته باشند. این شیوه، مبنای معماری کلاینت-سرور یا حتی یک اپلیکیشن‌های تحت وب پیشرفته است.

شکل (۸-۱). مدل پُشته‌ای و سلسله‌مراتبی DCAP

- **کاربران**
- **اپلیکیشن‌ها**
- **پایگاه‌داده**
- **سیستم‌عامل**
- **فایل‌های سیستمی/ مدیرانVolume**
- **ماشین مجازی/ ابر / NAS / SAN / DAS**

متأسفانه کنترل‌های امنیتی سیستم‌عامل‌های یونیکس، لینوکس، سیستم‌عامل مَک و ویندوز، به حساب کاربری روت یا مدیر اجازه دسترسی به پایین و بالای پشته را می‌دهند و هیچ راهکاری برای محدود ساختن آن وجود ندارد. شاید شما بتوانید حق امتیازها را حذف کنید ولی به‌عنوان مدیر، همیشه می‌توانید آن‌ها را دوباره برگردانید. وقتی مهاجمی دسترسی روت یا مدیریتی را به دست آورد، کار تمام است. باید در نظر داشت وقتی شما دسترسی مدیر داشته باشید، همیشه راه‌هایی برای دور زدن مکانیزم‌های کنترل امنیتی وجود خواهد داشت. مدیریت دسترسی ویژه (PAM) می‌تواند دسترسی کاربر را کنترل کند ولی نمی‌تواند الزاماً فایل‌های سیستمی و یا فرآیندهای موجود را بدون داشتن حق مالکیت کنترل نماید. راهکارهای کنترل فایل‌های سیستمی و فرآیندها می‌توانند تقسیم‌بندی و رمزگذاری فایل‌ها و دایرکتوری‌ها (مثلDLP،DCAP و غیره) را فراهم آورند ولی نمی‌توانند در مرحله اول کاربر واقعی را که احراز هویت شده است، کنترل نمایند پس اگر کاربری که احراز هویت شده، مدیر باشد احتمالاً راهی برای دور زدن این فناوری‌ها پیدا خواهد کرد.

برای حل این مسئله، می‌توان از راهکار استفاده از مدیریت دسترسی‌های ممتاز بر روی پُشته بهره برد تا سیستم‌عامل و برنامه‌ها را مدیریت کرده و بر یکپارچگی فایل[1] نظارت کنند (FIM)، همچنین دیگر راهکارهای کنترلی را برای مسدودسازی استراتژیک تهدیداتی استفاده کنند که متعلق به مدل‌های رایانش قدیمی هستند.

اینکار شامل مدیریت حق امتیازها در تمامی لایه‌ها، از احراز هویت کاربر گرفته تا سیاست‌های FIM را شامل می‌شود که دسترسی‌ها را اعطا کرده و یا رد می‌کند(حتی اگر کاربر، روت یا مدیر باشد). برای این امر، راهکارها باید با هم هماهنگ بوده و مستقل از هم نباشند پس هرگونه دست‌کاری را می‌توان بین لایه‌ها همبسته نمود تا از هک شدن جلوگیری کرد؛ بنابراین وقتی مفاهیمDCAP به PAM اعمال می‌شوند، می‌توان کاربردهای زیر را محقق کرد:

- دسترسی کاربر از احراز هویت تا دسترسی به فایل، مدیریت شده و مورد نظارت قرار می‌گیرد؛
- برنامه‌ها با حداقل حقوق ویژه اجرا می‌شوند تا ریسک‌های ارتقاء حقوق ویژه کاهش یابد؛

[1]File Integrity Monitoring

- پایگاه‌های داده و برنامه‌ها، رمزهای عبور را با استفاده از اسکریپت‌ها و ابزارهای خودکار مدیریت می‌کنند تا تغییرات را اعمال کنند و دسترسی‌ها را محدود سازند؛
- دسترسی سیستم‌عامل به کاربران استاندارد، دستورات، وظایف و اسکریپت‌ها محدود می‌شود و قابلیت‌ها بر حسب نیاز به استفاده و با اعمال حقوق ویژه افزایش داده می‌شوند؛
- فایل‌های فردی مربوط به اسکریپت‌ها و دستورات به‌صورت مجزا در برابر دست‌کاری محافظت می‌شوند ولی به حقوق ویژه همان کاربر تخصیص داده شده یا از آن حذف می‌شوند؛
- دسترسی کاربر در یک زنجیره حمله را می‌توان در امتداد هر سطح افقی یک مدل رایانش قدیمی، مورد نظارت قرار داده و کاهش داد؛
- تنها کاربران مورد اعتماد و مجاز، به یک دارایی و داده‌های پشتیبان آن با استفاده از حقوق ویژه و فناوری نظارت بر یکپارچگی فایل سیستمی دسترسی دارند؛
- حذف حقوق ویژه کاربر از برنامه‌ها و فایل‌های سیستمی را می‌توان در یک محیط رایانشی مورد اعتماد پشتیبانی کرد.

بازرسی و حفاظت داده‌محور، تعمیمی از مدیریت دسترسی‌های ممتاز است. این روش، کنترل‌ها و سیاست‌های فنی را برای کاربرد حقوق ویژه در زیرلایه سیستم‌عامل به فایل سیستمی و پایین‌تر از لیست‌های کنترل دسترسی اعمال می‌کند. راهکارهای نظارت بر یکپارچگی فایل (FIM) که با مدیریت دسترسی ممتاز یکپارچه می‌شود، این ابزار را ارائه می‌کنند و رویکردی جامع را در جهت نظارت بر هر لایه‌ای که ممکن است توسط عامل تهدید برای استخراج اطلاعات استفاده نمایند، فراهم می‌سازد. اینکار حتی مسدودسازی حساب مدیر برای دسترسی به فایل‌ها و دایرکتوری‌ها را نیز شامل می‌شود و بر FIM به‌عنوان راهکاری امنیتی جهت اجرای این تقسیم‌بندی تکیه دارد.

فصل ۹

نظارت بر حقوق ویژه

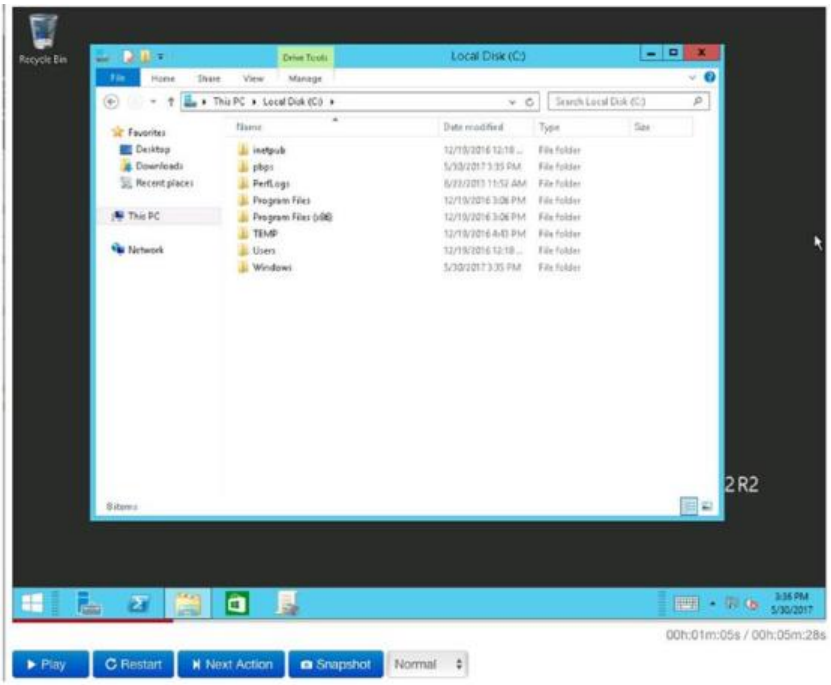
ریسک اصلی برای هر فعالیت دسترسی ممتاز خود آن فعالیت است. شما به‌عنوان مدیر یا روت باید این سؤال را بپرسید که: آیا یک فعالیت، یک اقدام اشتباه یا یک عامل تهدید با استفاده از اعتبارنامه‌های خود، رفتارهای ناهنجاری دارند؟ اگر شما نتوانید نظارتی بر اقدامات کاربر داشته باشید، ایرادات زیادی بر مدل سنتی امنیت برای بررسی این فعالیت وارد است و اینکه آیا هر نشست یا هر دستور و یا تمامی اطلاعاتی که دانلود شده و روی نمایشگر نشان داده می‌شوند، مورد تأیید است؟ بررسی تمام فعالیت‌ها امری دشواراست ولی به لطف فناوری و ابزارهای خودکارسازی موجود می‌توان این چالش مهم را حل نمود.

ضبط نشست

ضبط نشست عمل ثبت تمام فعالیت‌های قابل رؤیتی است که ممکن است طی یک نشست بر روی نمایشگر کاربر به نمایش درآید (شکل (۹-۱)). اینکار را می‌توان به‌صورت ضبط ویدیویی، ثبت متنی یا عکس‌برداری سریع از نمایشگر بر اساس تغییرات نمایشگر انجام داد. روش‌های معمول برای ضبط تضمین می‌نمایند که داده‌های ضبط‌شده به‌طور امن ذخیره‌سازی می‌شوند، امکان فهرست‌سازی آن‌ها وجود داشته و قابلیت‌های پیشرفته‌ای را برای جستجوی جزئیات و درک مفاهیم به‌وسیله یک مأمور رسیدگی و یا از طریق فرآیندی خودکار ارائه می‌کنند. ضبط نشست را می‌توان با استفاده از انواع فناوری‌ها پیاده‌سازی نمود:

- یک سیستم ضبط ویدیویی خطی که خروجی نمایشگر را پیش از نمایش ضبط می‌کند. معمولاً این فناوری با OCR (تشخیص نوری کاراکترها[1]) همراه می‌شود تا بتواند نمایشگر را برای یافتن واژه‌های کلیدی و متن کاوش نماید. این فناوری در سمت ویدیوی سرورها به سخت‌افزار نیاز دارد و معمولاً با فناوری‌های ابری و مجازی عملی (عملیاتی) نیست؛
- یک عامل کاربر نهایی یا افزونه مرورگری که نمایشگر یا نشست را بر اساس فعالیت ضبط می‌کند. این نتایج برای بررسی و پردازش در یک سرور مرکزی ذخیره‌سازی می‌شوند و یا به‌صورت بلادرنگ فرستاده می‌شوند. در این رویکرد، فناوری عامل باید به‌گونه‌ای تنظیم و اجرا شود تا اتصالات خارج از باند را برقرار نکند زیرا ممکن است سبب دور زدن فناوری‌های ضبط گردد؛
- یک فناوری پروکسی مبتنی بر پروتکل که عملیات ضبط نمایشگر یک نشست فعال از راه دور را بدون استفاده کردن از عاملی، فراهم سازد. این رویکرد از تقسیم‌بندی پشتیبانی کرده و به دسترسی جهت اتصال موفقیت‌آمیز نیاز دارد تا مسیریابی را از طریق پروکسی انجام دهد؛ بنابراین تمام لاگ‌ها به‌وسیله پروکسی ضبط می‌شوند و بر روی تجهیز کاربر نهایی ذخیره‌سازی نمی‌شوند، همچنین به تغییرات سخت‌افزاری نیازی ندارد.

[1]Optical Character Recognition



شکل (۹-۱). پخش دوباره یک نشست ضبط‌شده

جدای از رویکرد فناوری به کار گرفته‌شده، هدف همیشه یکسان است: بررسی فعالیت نشست ممتاز در قبال داده‌ها و سیستم‌های حساس. با وجودی که این رویکرد به‌تنهایی فعالیت عامل تهدید را متوقف نمی‌کند ولی فعالیت آن‌هایی را که خارج از محدوده‌های عملیاتی معمول هستند، مستند می‌سازد. ضبط فعالیت‌های ممتاز را می‌توان برای بررسی رخداد استفاده کرد و اگر به‌درستی پیکربندی شده باشد، می‌تواند در شناسایی یک تهدید کمک کند.

به‌علاوه اگر سیستم ضبط نشست به اندازه کافی پیشرفته باشد، خودکارسازی آن می‌تواند پاسخ پیشگیرانه‌ای را برای رفتارهای نامناسب در پی داشته باشد. برای مثال می‌توان دستورات پیشرفته‌ای را تنظیم کرد تا خروجی نمایشگر را رصد کند و در صورت شناسایی رفتار نامعمول، اقداماتی از قبیل ارسال هشدار، قفل نمودن، از بین بردن نشست یا غیرفعال نمودن حساب کاربری مربوطه را اجرا نماید. با وجودی که عملیاتی شدن این امر به تنظیماتی کامل و پیشرفته نیاز دارد ولی اگر عامل تهدید سعی داشته باشد تا حضوری مداوم را حفظ کند و یا

در حال اجرای دستورات خاصی باشد و یا اطلاعاتی را بارگیری نماید، این رویکرد کار را برای آن‌ها سخت‌تر می‌کند.

و در آخر اینکه وقتی بحث رسیدگی قانونی توسط مأمورین مطرح باشد، ضبط نشست‌ها، الزامات مستندسازی مربوط به فعالیت‌های ممتاز را برآورده می‌کند.

ثبت کلیدهای فشرده‌شده

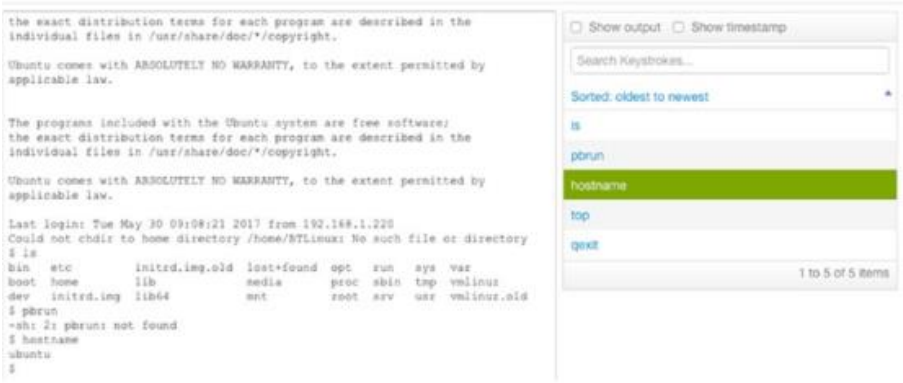
با وجودی که ضبط نشست، خود نمایشگر را به‌صورت گرافیکی و یا متنی مستند می‌کند ولی کلیدهای فشرده‌شده توسط کاربر در صفحه کلید را ضبط نمی‌کند: تنها کلیدهای فشرده-شده‌ای را داریم که روی نمایشگر نمایان شوند. میانبرها و دستورات صفحه کلید مثل کپی کردن (Ctrl+C) و غیره ممکن است اصلاً ضبط نشوند. بر اساس الگوهای ضبط نمایشگر که در بالا بیان شد، ثبت کلیدهای فشرده‌شده نیز به سه روش برای انجام این کار و دریافت ورودی‌های کاربر نیاز دارد:

- یک دستگاه فیزیکی مثل USB یا PS2 برای ثبت کلیدهای فشرده‌شده کاربر. این دستگاه‌ها می‌توانند اطلاعات را به‌صورت محلی ذخیره کنند و یا نرم‌افزار و شبکه‌ای داشته باشند تا اطلاعات دریافتی را بارگذاری[1] نمایند. هیچ راهکار فیزیکی برای ثبت کلیدهای فشرده‌شده صفحه کلیدهایی که از طریق بلوتوث یا دانگل همراه به سیستم متصل می‌شوند، وجود ندارد؛
- یک عامل کاربر نهایی که کلیدهای فشرده‌شده را ثبت می‌کند. این کار روشی رایج است ولی باید آن را جزء موارد مجاز به سیستم معرفی کرد و سیستم نباید آن را با بدافزاری (مانند کیلاگرها) اشتباه بگیرد که کار آن ثبت کلیدهای فشرده‌شده است. این رویکرد برای تمام فناوری‌های صفحه کلید سیمی و بی‌سیم مناسب است زیرا تمام داده‌های ورودی دستگاه را ثبت می‌کند؛
- فناوری‌های پروکسی که تفاوت بین پردازش نمایشگر و ورودی کاربر را ثبت می‌کند. این رویکرد به هیچ سخت‌افزار فیزیکی (خارج از پروکسی) نیاز ندارد و نیازی به هیچ عامل محلی برای ثبت کلیدهای فشرده‌شده ندارد. فناوری‌های پروکسی برای ثبت

[1] Upload

کلیدهای فشرده‌شده به شکل صفحه کلیدهای مجازی یا فناوری‌های ورودی صوتی نیز سازگاری دارند.

هدف اصلی ثبت کلیدهای فشرده‌شده آن است تا عامل تهدید را در مرحله وارد کردن دستور متوقف نماید. دستورات خاص برای اضافه کردن کاربر، بازیابی یک پایگاه‌داده یا نصب بدافزار به نسبت در تمام سیستم‌های عامل، برنامه‌ها و پایگاه‌های داده، صورت استانداردی دارند. اگر سیستم نظارت بر حقوق ویژه به‌درستی برای نظارت، هشدار یا از بین بردن یک نشست پیکربندی شده باشد و اگر این دستورات مشاهده و شناسایی شوند، احتمالاً می‌توان رخنه‌ای را قبل از نشر اطلاعات ارزشمند شناسایی نمود. عامل تهدید برای اینکه بتواند در حمله خود موفق باشد باید این دستورات را اجرا نماید. خود دستورات به حق امتیازهای سطح بالاتری نیاز دارند که از طریق روش‌های بیان‌شده قبلی استفاده می‌شوند؛ بنابراین اگر بتوانیم نشست‌های معتبر را شناسایی کنیم و تحت کنترل درآوریم و نمونه‌های بدافزاری را برچسب‌گذاری نماییم، ابزار دیگری برای کاهش استفاده از حقوق ویژه به‌عنوان اهداف حمله در اختیار داریم. نگاهی به شکل (۹-۲) داشته باشید.



شکل (۹-۲). فیلتر کردن خط دستور و جستجو در دستورات

نظارت بر اپلیکیشن

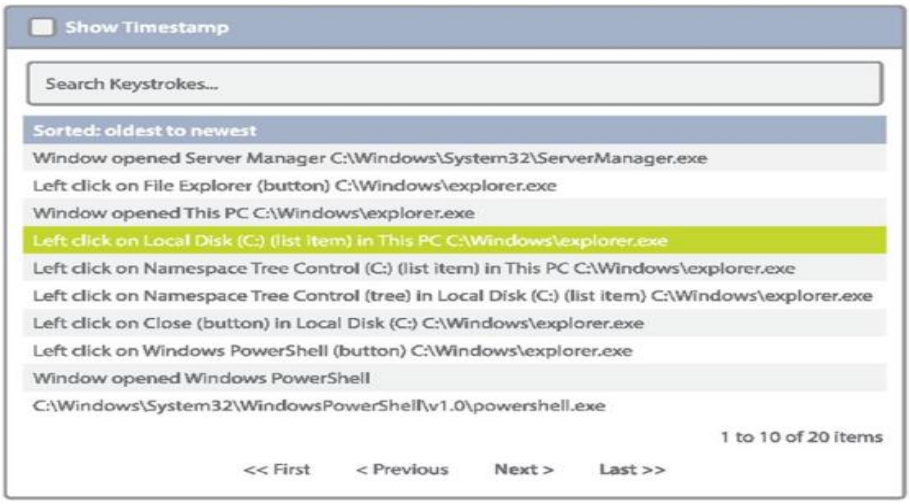
برنامه‌ها چالشی منحصربه‌فرد برای نظارت بر حقوق ویژه هستند. هر اپلیکیشن ذاتاً متفاوت از سایر اپلیکیشن‌ها است حتی اگر منوها و دکمه‌های مشترکی با آن‌ها داشته باشد و یا به موتورهای اجرایی ازجمله Oracle Java یا Adobe Flash و یا کدهای کامپایل‌شده به‌صورت

محلی وابسته باشند. ضبط نشست می‌تواند حرکت موس و ضبط نمایشگر را انجام دهد ولی برای دکمه‌ای خاص، بررسی نشست کار بسیار دشواری است و نیاز به استفاده از ابزارهایی دارند. برای مثال برخی از ثبت‌کننده‌های کلیدهای فشرده‌شده، نمی‌توانند کلیک‌های موسی را که خارج از مختصات محور x و محور y است، ثبت کند مگر اینکه نسبت به خود اپلیکیشن اطلاعی داشته باشد. به دلیل وجود این مشکلات، تنها راهکارهایی که برای نظارت بر اپلیکیشن عملی کاربرد دارند، استفاده از کدهای محلی به‌صورت یک عامل (عامل محو شونده موقت) و یا استفاده ازOCR (تشخیص نوری کاراکتر) هستند. به‌هرحال OCR به پردازش داده‌های ثبت-شده نیاز دارد که ممکن است با انواع قلم‌ها به مشکل برخورد نماید یا مسیر فایل‌ها را نبیند؛ بنابراین برای اعلام هشدار لحظه‌ای مناسب نیست پس تنها روش عملی برای نظارت بر اپلیکیشن مربوط به PAM استفاده از انواع فناوری‌های عاملی است.

عامل‌های نظارت بر اپلیکیشن، جدای از مکانیزم کاری که دارند (مداوم یا موقت)، عملیات برنامه اعم از فراخوان‌ها برای API، کلیک‌های موس و تغییرات نمایشگر را بر اساس تعامل کاربر مورد نظارت قرار می‌دهند. برای مثال در API ویندوز، نوار عنوان اپلیکیشن، نام دکمه‌ها و منوها تماماً نشان داده می‌شود. وقتی کاربر تعاملی با آن داشته باشد، می‌توان آن‌ها را ثبت کرد و به‌صورت زمانی آن‌ها را با ضبط نمایشگر و کلیدهای فشرده‌شده ذخیره‌سازی نمود. اینکار امکان انجام بررسی کاملی را جهت پیگیری یا تصدیق‌های قانونی و فعالیت‌های مخرب احتمالی ارائه می‌کند. برای درک بهتر، بازی «Where's Waldo?» برای شکار تهدید را به یاد آورید.

ابزارهایی که به عاملان تهدید اجازه می‌دهد تا به صورت گرافیکی داده‌ها را دست‌کاری نموده و به فعالیت مخرب ادامه دهد، مورد نظارت قرار می‌گیرد حتی اگر آن‌ها صرفا از رابط‌های گرافیکی برای حملات خود استفاده نمایند. دکمه‌ها و دیالوگ‌ها معمولاً به‌طور صریح برای عملیات حذف داده، دانلود یا ارسال درخواست جستجو در برنامه‌ها برچسب‌گذاری می‌شوند؛ بنابراین تکنیک‌های خودکارسازی مشابه با ثبت کلیدهای فشرده‌شده را می‌توان برای جستجوی واژه‌های کلیدی مورد استفاده قرار داد که شامل شاخص‌هایی از فعالیت‌های مخرب و غیرمجاز هستند. نتایج بررسی‌ها می‌تواند هشداری را به تیم‌های امنیتی ارسال کند یا با استفاده از همان فناوری‌های پروکسی یا عاملی، نشست را از بین ببرد. نظارت بر اپلیکیشن یک بخش حیاتی از خنثی‌سازی عامل تهدید است و این برنامه‌ها حتی در رابط کاربری هم

برای اجرای وظایف حساس نیاز به حقوق ویژه‌ای دارند. همچنین نظارت بر خود اپلیکیشن هنگام تعامل آن با کاربر و سیستم‌عامل، اجازه نظارت بر مؤلفه‌های رابط کاربری حساس هنگام فعالیت‌های نامناسب را می‌دهد. نگاهی به شکل (۹-۳) داشته باشید.



شکل (۹-۳). نظارت بر اپلیکیشن با استفاده از فناوری عاملی

فصل ۱۰

مدیریت دسترسی‌های ممتاز

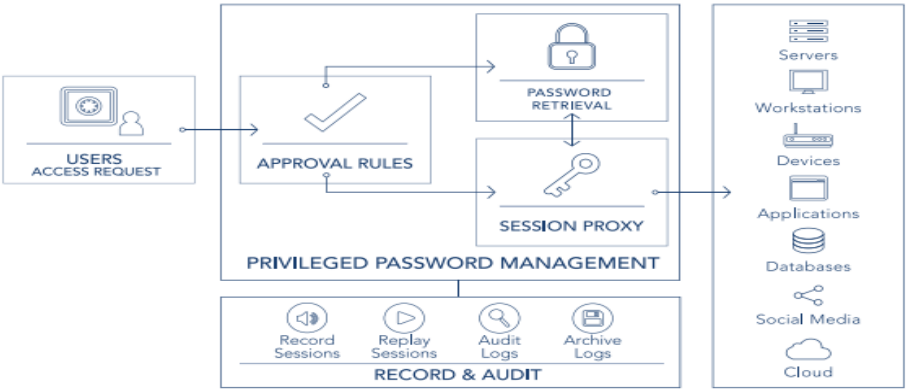
مدیریت دسترسی‌های ممتاز (PAM) تحت عناوینی مثل مدیریت حساب های ممتاز (PAM) و یا مدیریت هویت های ممتاز (PIM) نیز شناخته می‌شود. این موضوع زیر مجموعه‌ای از مدیریت دسترسی هویت (IAM) است که به‌وسیله تحلیلگران پیشروی این حوزه تعریف شده است.

هدف اصلیPAM آن است تا سازمان شما را از سوءاستفاده اتفاقی یا برنامه‌ریزی‌شده اعتبارنامه‌های ممتاز امن نگه دارد؛ سوءاستفاده‌هایی که پیش‌تر ریسک‌های آن را تبیین کردیم. این تهدیدات مخصوصاً زمانی آشکار می‌شود که سازمان شما به سبب رشد، پیدایش بازارهای جدید و دیگر ابتکارات توسعه‌ای کسب‌وکار تغییراتی را تجربه می‌کند. هر چه که سیستم‌های IT سازمان شما بزرگ‌تر و پیچیده‌تر شود، کاربران ممتاز بیشتری خواهید داشت. این کاربران شامل کارکنان، پیمانکاران و حتی کاربران دورکار یا کاربران خودکار می‌شود. باید در نظر داشت که این امر نیاز سازمان‌های کوچک به بهره‌گیری از PAM را کاهش نمی‌دهد بلکه نشان‌دهنده آن است که متخصصان حوزه امنیت، گستره زمانی دشوارتری از مشکلات را دارند همچنین باید راهکارهای کاهش این مشکلات را در مقیاس‌های بزرگ‌تری داشته باشند. هر سازمانی در معرض ریسک استفاده از حق امتیازها به عنوان اهداف حمله قرار دارد لذا همین حقیقت به‌تنهایی نیاز به PAM در هر جایی را نشان می‌دهد، اگرچه برای کاهش ریسک‌های مرتبط ممکن است به بخش‌هایی از آن نیاز باشد ولی امری بدیهی است که هرچه سازمانی بزرگ‌تر و پیچیده‌تر باشد، به‌منظور پیاده‌سازی کاربردهای PAM بیشتری نیاز داشته باشد.

یک استراتژی موفق PAM، یک شیوه بهینه‌سازی‌شده امن و کارآمد را ارائه می‌کند که برای احراز هویت و نظارت بر تمام کاربران ممتاز کاربرد دارد. اینکار قابلیت‌های زیر را برای سازمان شما به ارمغان می‌آورد:

- اعطاء حقوق ویژه به کاربران تنها برای منابعی که آن‌ها مجاز به دسترسی هستند؛
- اعطای دسترسی تنها در زمان مناسب و قطع دسترسی هنگامی که محدودیت زمانی تمام شده است؛
- حذف نیاز کاربران با حقوق ویژه برای داشتن یا نیاز به دانستن رمزهای عبور سیستم‌ها؛
- تضمین اینکه می‌توان تمام فعالیت‌های ممتاز را به یک حساب اختصاص داد و زمانی که حساب‌ها به اشتراک گذاشته می‌شوند، نگاشت فعالیت‌ها به هر هویت را اجرا نمود؛
- مدیریت مرکزی و سریع تمام منابع فیزیکی و مجازی، در محیط سازمان یا بر روی ابر که هر مجموعه ناهمگن از منابع با نیاز به دسترسی ممتاز را در خود جای می‌دهد؛
- ایجاد یک مسیر حسابرسی پایدار برای هر مصرف‌کننده دارای حقوق ویژه از طریق ثبت نشست، ثبت کلیدهای فشرده‌شده و نظارت بر اپلیکیشن؛
- تقویت سازمان‌ها برای پاسخ راحت و سریع به نفوذها به‌وسیله ثبت فعالیت‌های ممتاز که شاخص‌های آلودگی در آن‌ها مشاهده می‌شود.

وقتی شما این مزایای مدیریت دسترسی‌های ممتاز را در نظر بگیرید، قابلیت عامل تهدید برای کسب دسترسی ممتاز و انجام کارها به‌صورت ناشناس به میزان زیادی کاهش می‌یابد و استفاده از حقوق ویژه را به‌عنوان اهدافی برای حمله کاهش می‌دهد. شکل (۱۰-۱) گردش کار این فرآیند کلی را در زمان استفاده از مدیریت دسترسی‌های ممتاز به‌عنوان مؤلفه‌ای از PAM نشان می‌دهد.



شکل (۱۰-۱). دسترسی PAM برای مدیریت رمز عبور

چالش‌های PAM

برای اینکه به سراغ چالش‌های مدیریت حقوق ویژه برویم، باید از مشکلات اصلی و ذاتی عدم بهره‌مندی از استراتژی مدیریت دسترسی ممتاز آگاه باشیم:

- **نبود دید و آگاهی** از تمام حساب‌های ممتاز و اعتبارنامه‌ها در کل سازمان، چالشی یکپارچه را به وجود می‌آورد، مخصوصاً برای شرکت‌هایی که به فرآیندها و ابزارهای دستی متکی هستند. حساب‌های ممتاز که مدت زیادی است فراموش شده‌اند، در اغلب سازمان‌ها وجود دارند. ممکن است تیم‌های مختلفی در حال مدیریت مجموعه اعتبارنامه‌های خود باشند. البته اگر مدیریتی در کار باشد که ردیابی تمام رمزهای عبور را دشوار می‌کند و کسانی را که به آن‌ها دسترسی دارند و از آن‌ها استفاده می‌کنند، به حال خود رها می‌کنند.
- **نبود نظارت و حسابرسی بر اعتبارنامه‌های ممتاز:** حتی اگر واحد IT با موفقیت تمام اعتبارنامه‌های ممتاز را که در سازمان پراکنده است شناسایی کند، اینکار به معنای دانستن اینکه چه فعالیت‌های خاصی در طی یک نشست ممتاز صورت گرفته است، نیست (مثلاً دوره زمانی که طی آن حق امتیازهای اضافه‌ای به یک حساب، سرویس یا فرآیند اعطا می‌شود). دسترسی ممتاز به یک کاربری سرپرست نباید منجر به قدرت بدون قید و شرط آن کاربر شود. به‌علاوه، درPCI، HIPAA و دیگر قوانین، سازمان‌ها نه‌تنها باید امنیت و حفاظت داده‌ها را تأمین کنند بلکه باید بتوانند کارایی

این معیارها را ارائه نمایند. پس هم برای سازگاری با قوانین و هم به دلایل امنیتی، تیم فناوری اطلاعات به رؤیت‌پذیری فعالیت‌هایی نیاز دارد که طی نشست‌های ممتاز اجرا می‌شوند. به‌طور ایده‌آل، بخش فناوری اطلاعات باید این قابلیت را داشته باشد تا هنگام استفاده نامناسب از اعتبارنامه‌ها، کنترل آن نشست را در دست گیرد اما در جایی که صدها یا هزاران نشست ممتاز به‌صورت هم‌زمان در سازمان در حال اجرا هستند، چطور تیم IT سریعاً فعالیت مخرب را شناسایی کند و آن را متوقف سازد؟ با وجودی که برخی از برنامه‌ها و سرویس‌ها (مانند اکتیو دایرکتوری مایکروسافت) می‌تواند اقدامات کاربر را ثبت کنند و با وجودی که سرورهای ویندوزی رویدادهای ورود و لاگ‌های رخدادها را ثبت می‌کنند و می‌توانند برخی از ناهنجاری‌های رفتاری را آشکار سازند اما برای پوشش و نظارت کامل حساب‌های ممتاز نیاز به راهکاری ثالث است.

- **اشتراک حساب‌های ممتاز برای راحتی کار:** تیم‌های فناوری اطلاعات معمولاً حساب‌های روت، مدیر ویندوز و بسیاری از رمزهای عبور ممتاز را به اشتراک می‌گذارند؛ بنابراین می‌توانند در صوت نیاز وظایفشان را به‌صورت یکپارچه به اشتراک بگذارند. در هر صورت، وقتی چندین نفر رمز عبور یک حساب را با هم به اشتراک می‌گذارند، ممکن است ردیابی اقدامات انجام‌شده به‌وسیله یک حساب و نسبت دادن آن به یک فرد غیرممکن باشد که این امر، حسابرسی و مسئولیت‌پذیری را پیچیده می‌کند.
- **اعتبارنامه‌های تعبیه‌شده در کد برنامه:** اعتبارنامه‌های ممتاز برای تسهیل احراز هویت، دسترسی و ارتباطات اپلیکیشن به اپلیکیشن (A2A) و اپلیکیشن به پایگاه‌داده (A2D) ضروری هستند. برنامه‌ها، سیستم‌ها و دستگاه‌های اینترنت اشیاء معمولاً با اعتبارنامه‌های تعبیه‌شده و پیش‌فرض به فروش رسیده و نصب می‌شوند که به‌راحتی قابل حدس زدن هستند و تا زمانی که مدیریت نشوند، ریسک بزرگی آن‌ها را تهدید می‌کند. این اعتبارنامه‌های ممتاز معمولاً در متنی آشکار[1] و شاید درون اسکریپت، کد یا یک فایل، ذخیره‌سازی می‌شوند. متأسفانه هیچ راه دستی برای شناسایی یا مدیریت متمرکز رمزهای عبور ذخیره‌شده درون برنامه‌ها یا اسکریپت‌ها وجود ندارد.

[1] Clear text

ایمن‌سازی رمزهای عبور تعبیه‌شده به جداسازی رمز عبور از کد نیاز دارند به‌گونه‌ای که وقتی مورد استفاده نیست، در یک صندوق رمز عبور امن و متمرکز ذخیره‌سازی شود، برخلاف اینکه به‌صورت مرتب به شکل متنی آشکار در دسترس باشد.

- **کلیدهای**SSH: تیم‌های فناوری اطلاعات معمولاً برای خودکارسازی دسترسی امن به سرورها از کلیدهای SSH استفاده می‌کنند که نیاز به وارد کردن اعتبارنامه‌های لاگین را به‌صورت دستی دور می‌زنند. پراکندگی کلیدهای SSH ریسکی واقعی را برای هزاران سازمان ایجاد می‌کندکه ممکن است میلیون‌ها کلید SSH داشته باشند. این کلیدها مدت زیادی بدون استفاده و فراموش‌شده بودند ولی هنوز راه‌های مخفی برای هکرها جهت نفوذ به سرورهای حیاتی هستند. کلیدهای SSH کلیدهای استانداردی هستند که در محیط‌های یونیکس و لینوکس استفاده بیشتری دارند ولی در ویندوز هم کاربرد دارند. مدیرها از کلیدهای SSH برای مدیریت سیستم‌های عامل، شبکه‌ها، انتقال فایل‌ها، تونل‌زنی داده‌ها و غیره بهره می‌برند؛ مانند دیگر اعتبارنامه‌های ممتاز، کلیدهایSSH نیز به یک کاربر خاص تعلق ندارند و ممکن است چندین نفر کلید و عبارت عبور خصوصی برای ورود به یک سرور را به اشتراک بگذارند که کلید عمومی را نگه می‌دارد؛ مانند دیگر اعتبارنامه‌های ممتاز، وقتی سازمان‌ها به فرآیندهای دستی تکیه می‌کنند، تمایلی وجود دارد تا از یک عبارت عبور در بسیاری از کلیدهایSSH و یا از کلید SSH عمومی یکسانی استفاده گردد و این یعنی یک کلید هک‌شده را می‌توان برای نفوذ به چندین سرور استفاده نمود.
- **اعتبارنامه‌های ممتاز و ابر:** به‌طورکلی چالش‌های رؤیت‌پذیری و حسابرسی در محیط‌های ابری و مجازی تشدید می‌شوند. کنسول‌های مدیریت ابری و مجازی (مانندAWST، Office 365 و غیره) قابلیت‌های فوق کاربری وسیعی را ارائه می‌کنندکه کاربران را قادر می‌سازد تا سریعاً سرورها را در مقیاسی انبوه تدارک دیده، پیکربندی کرده و حذف نمایند. درون این کنسول‌ها، کاربران می‌توانند تنها با چند کلیک، ثبت‌نام کرده و هزاران ماشین مجازی را مدیریت کنند (که هر یک مجموعه حقوق ویژه و حساب‌های ممتاز خود را دارند)؛ بنابراین در نحوه پیاده‌سازی و مدیریت تمام این حساب‌ها و اعتبارنامه‌های ممتاز به مشکلاتی برمی‌خوریم .جدای از آن، پلتفرم‌های ابری معمولاً قابلیت حسابرسی فعالیت‌های کاربر را ندارند حتی برای

سازمان‌هایی که درجاتی از خودکارسازی را برای مدیریت رمز عبور اجرا کرده‌اند (چه به‌وسیله راهکارهای درون‌سازمانی و چه راهکارهای شرکت‌های ثالث)، اگر معماری آن برای محیط ابری در نظر گرفته نشده باشد، هیچ تضمینی وجود ندارد که راهکار مدیریتی قادر باشد تا به اندازه کافی و به‌صورت مناسب اعتبارنامه‌های ابری را مدیریت نماید.

- **حساب‌ها یا راهکارهای دسترسی از راه دور شرکت‌های ثالث:** در آخر، مسئله دیگر برای سازمان‌ها آن است که چطور دسترسی های ممتاز و مدیریت اعتبارنامه را برای کاربران ثالث مانند مشاوران یا دیگر شرکت‌ها که ممکن است فعالیت‌های متنوعی را انجام دهند، بسط دهند. شما چطور تضمین می‌کنید که احراز هویت ارائه‌شده از طریق دسترسی از راه دور به یک بخش ثالث، به‌طور مناسب مورد استفاده قرار می‌گیرد؟ چطور تضمین می‌کنید که سازمان ثالث اعتبارنامه‌ها را به اشتراک نمی‌گذارد یا مثلاً در دیگر روش‌های حفاظت رمز عبور در زمانی که کارمندی از شرکت جدا می‌شود، اعتبارنامه‌های ورود آن به‌درستی حذف می‌شوند؟

مدیریت رمز عبور

مدیریت رمز عبور عملکردی ساده است که به کاربر کمک می‌کند تا رمزهای عبور را ذخیره‌سازی و مدیریت نماید. راهکارهای ذخیره‌سازی رمز عبور (که معمولاً نرم‌افزارهای مدیریت رمز عبور، کیف‌ها یا صندوق‌های رمز عبور نام دارند) رمزهای عبور را به‌صورت رمزگذاری‌شده ذخیره‌سازی می‌کنند و برای این کار نیاز است تا کاربر یک رمز اصلی برای آن تعریف کند. این کار با این فرض است که راهکار برای مدیریت رمز عبور مستقیم کاربر نهایی طراحی شده است. رمز اصلی اجازه دسترسی به پایگاه‌داده رمز عبور جهت بازیابی و به دست آوردن سایر رمزهای عبور را در برنامه‌ها می‌دهد.

مدیریت رمز عبور با محوریت سازمانی این مفهوم را به سطح متفاوتی می‌برد. آن‌ها دسترسی مبتنی بر نقش را به ذخیره‌سازی و بازیابی رمزهای عبور اشتراکی اضافه می‌کنند که به‌صورت خودکار رمزهای عبور را تغییر می‌دهد و واسط کاربری برای دسترسی به رمز عبور برنامه‌ریزی-شده را ممکن می‌سازد و قابلیت‌های حسابرسی، رمزگذاری و ثبت را برای چندین کاربر و اپلیکیشن در سراسر سازمان فراهم می‌کند. این ویژگی‌ها همه موارد از ثبت نشست تا گزارش

تصدیق رمز عبور را پوشش می‌دهد. این قابلیت‌ها برای کاهش تهدیدات و همچنین برای نشان دادن سازگاری با قوانین ضروری است.

راهکارهای مدیریت رمز عبور را می‌توان در گستره وسیعی از اشکال مبتنی بر نیازهای سازمان پیاده‌سازی نمود. اینکار می‌تواند شامل نرم‌افزارها، ابزارها، نمونه‌های مجازی یا حتی میزبانی-شده در ابر باشد. جدای از فلسفه اجرای آن، هدف همچنان واحد است: امن‌سازی رمزهای عبور حساب‌های ممتاز و مهم‌تر از همه، اطمینان از اینکه نرم‌افزار مدیریت رمز عبور خودش به چالش و مسئله‌ای برای سازمان تبدیل نمی‌شود. برای مثال، رمزگشایی رمزعبور اصلی و دسترسی بدون محدودیت به پایگاه‌داده مدیریت‌کننده رمز عبور در هر زمانی مانند یافتن شاه‌کلیدی برای دسترسی به منابع تحت مدیریت آن سازمان است. سازمان‌ها می‌خواهند تا توازنی بین ریسک ذخیره‌سازی تمام رمزهای عبور حساس خود در یک مکان مقاوم در برابر خطا را در مقابل تهدیدات مربوط به دسترسی‌های ممتاز مدیریت‌نشده ایجاد کنند.

مدیریت حقوق ویژه حداقلی

مفهوم حقوق ویژه حداقلی، ریشه در امنیت سیستم‌های اصلی و بزرگ دارد. هر کاربری وقتی برای اولین بار معرفی می‌شود قطعاً هیچ حقوق ویژه‌ای برای انجام کاری در سازمان ندارد و در این حالت یک سیاست امنیتی کاملاً بسته در نظر گرفته می‌شود. از آنجایی‌که کاربر باید عملیاتی را انجام دهد، حقوق ویژه‌ای به حساب‌های آن ها اضافه می‌شود تا وظایف خاصی را انجام دهند. خوشبختانه این مجوزها حداقل‌های موردنیاز برای اجرای وظیفه‌ای خاص هستند و چیزی بیشتر از آن نیست که بتواند منجر به سوءاستفاده از حقوق ویژه شود.

جدای از یونیکس، لینوکس، ویندوز یا مک بودن پلتفرم، حقوق ویژه حداقلی در تمام پلتفرم‌ها به روشی یکسان عمل می‌کند. متأسفانه مدل پیش‌فرض برای سیستم‌عامل‌های ویندوز و مک متضاد هم هستند و در سیستم‌های ویندوزی کاربران اولیه به‌صورت پیش‌فرض، مدیر هستند که برای تسهیل حقوق ویژه حداقلی، به کاربران جدید یا موجود، حقوق ورود پایه (کاهش‌یافته) تخصیص می‌یابد و برنامه‌ها، وظایف و حتی عملکردهای سیستم‌عامل بر اساس نیاز اعطا می‌شوند. حساب پایه تخصیصی در این مدل به‌عنوان کاربر استاندارد در نظر گرفته می‌شود. حقوق پایه کاربر استاندارد امکان تعامل با سیستم‌عامل، برنامه‌های محدود را ممکن می‌سازد ولی هیچ تغییری را که بتواند تهدیدی برای محیط باشد، اجرا نمی‌کند. در این مدل برای

حساب‌هایی که برای اجرای وظایف، برنامه‌ها و پیکربندی‌ها، مجوزهای بالاتری نسبت به کاربر استاندارد نیاز دارند (که شامل مدیر و روت می‌شود) به‌طور سنتی به کاربران، حسابی ثانویه به‌عنوان مدیر اعطا می‌شود تا این وظایف را انجام دهند ولی اینکار ریسک حملات با اهداف حقوق ویژه را افزایش می‌دهد. در یک مدل حقوق ویژه حداقلی، حقوق ویژه اضافی حذف می‌شوند تا مانع از آن شوند که عامل تهدید از آن‌ها بهره‌ببرد.

خودکار سازی حقوق ویژه اپلیکیشن به اپلیکیشن

خودکارسازی اپلیکیشن به اپلیکیشن (A2A) از یک رابط برنامه‌نویسی اپلیکیشن (API) استفاده می‌کندکه اجازه می‌دهد اعتبارنامه‌های ذخیره‌سازی‌شده را به‌صورت خودکار از درون سازمان یا یک پیاده‌سازی مبتنی بر ابر مدیریت نماید. اگر شما یک توسعه‌دهنده اپلیکیشن‌های تجاری هستید یا برنامه‌های سفارشی برای سازمان خود تولید می‌کنید، مزیت اصلی انجام خودکارسازی این است که به برنامه‌ها اجازه می‌دهد تا بدون دخالت کاربر نهایی و یا نوشتن اعتبارنامه‌ها در کد برنامه‌ها اعم از نوشتن درون اسکریپت‌ها، درون کدهای کامپایل‌شده و یا درون یک فایل، احراز هویت را انجام دهند. اگر ابزارها، اعتبارنامه‌های ذخیره‌سازی‌شده را به‌صورت خودکار بازیابی کرده و به دست آورند، اعضاء تیم مانند مدیران پایگاه داده هرگز به حقوق یک مدیر نیاز ندارند. اپلیکیشن‌ها می‌توانند اتصالاتی به پایگاه داده برقرار کنند یا با دیگر برنامه‌ها ارتباط برقرار کرده و عملکردهای خود را با رمز عبور فعلی و همچنین بدون دخالت دستی اجرا کنند. سازمان‌ها و توسعه‌دهندگان اپلیکیشن‌ها از چندین مزیت در استفاده از یک API مدیریت دسترسی ممتاز، برای امن‌سازی اعتبارنامه‌ها در برابر عامل تهدید بهره‌می‌برند:

- **مدیریت امن اعتبارنامه:** توسعه‌دهندگان به‌جای ورود اعتبارنامه‌های استاتیک، از یک API مدیریت دسترسی ممتاز برای بازیابی و به دست آوردن آخرین اعتبارنامه‌ها برای کاربرها، اپلیکیشن‌ها، زیرساخت ها، محیط ابری یا پایگاه‌داده استفاده می‌کنند تا عمل احراز هویت را انجام دهند و سپس در پایان نشست اعتبارنامه‌ها را آزاد می‌کنند. این کار سبب چرخش خودکار و تصادفی رمز عبور می‌شود، کاربر نهایی هرگز با نام کاربری یا رمز عبور مواجه نمی‌شود. تمام احراز هویت به‌صورت پنهان درپشت صحنه و با حسابرسی کامل فعالیت‌ها در صورت نیاز انجام می‌شود.

- **دسترسی سریع و چابک توسعه‌دهنده:** چابکی و پاسخ‌دهی تیم فناوری اطلاعات، با عدم نیاز به نام کاربری و رمز عبور برای اتصال جهت ایجاد برنامه‌های سفارشی بهبود می‌یابد. کاربران نهایی مانند مدیران پایگاه‌داده، هرگز به اعتبارنامه‌های مدیر برای دسترسی به پایگاه‌داده نیاز پیدا نمی‌کنند زیرا ابزارها، اعتبارنامه‌های ذخیره‌سازی‌شده را به‌صورت خودکار بازیابی می‌کنند. ابزارهای مدیریتی برای سرویس‌ها، دسترسی‌های از راه دور و زیرساخت‌های اتومات، کاربر واردشده را شناسایی کرده و دارایی‌هایی را که بدان دسترسی دارند، مشخص می‌کنند و به‌صورت یکپارچه اعتبارنامه‌ها را به اپلیکیشن ارسال و عبور می‌دهند.
- **حفاظت در برابر حملات استفاده مجدد از رمز عبور:** از آنجایی‌که اعتبارنامه‌ها می‌توانند درون خود اپلیکیشن، به‌صورت مستقیم از API عبور داده شوند، تیم IT می‌تواند زمان اجرا را امن نگه دارد و مانع از تکنیک‌های هک مانند حملات پاس کردن هش (PtH) و ثبت کلیدهای فشرده‌شده شود و باعث می‌شود تا این رویکرد بسیار امن‌تر از فناوری مرسوم شناسایی یگانه (SSO) شود.

- **انعطاف‌پذیری در برنامه‌نویسی:** برای ایجاد این امکان برای توسعه‌دهنده‌ها جهت دسترسی به API و کمک به امن‌سازی برنامه‌های خود، شرکت‌های PAM نمونه‌هایی را پیشنهاد می‌دهند و گستره وسیعی از زبان‌های برنامه‌نویسی شامل C#، PowerShell، Ruby، Python، Java و Bash Shell را پشتیبانی می‌کنند.

نتیجه نهایی نیاز به رمزعبورهای استاتیک را از بین می‌برد و برنامه‌های در محیط ابری یا درون‌سازمانی را با آخرین رمزعبور (کلید) امن نگه می‌دارد. عملکردهای معمول API شامل موارد زیر است:

- بازیابی رمزعبور فعلی برای یک دارایی یا اپلیکیشن؛
- الزام به تغییر رمز عبور؛
- ثبت یک منبع برای مدیریت رمز عبور که شامل فناوری‌های مالکیت حساب (سیستم‌عامل، پایگاه‌داده، اپلیکیشن، منبع ابری، رسانه اجتماعی و غیره) می‌شود؛
- سیاست و معیاری خودکار برای مدیریت رمز عبور شامل بازیابی آن؛

- دسترسی به جزئیات نظارت نشست؛
- تعریف گروه‌هایی از کاربران و منابع برای مدیریت ساده‌تر.

مدیریت کلید SSH

بخشIT سازمان‌های پیشرفته که اغلب شامل چندین هزار سرور یونیکسی هستند و تنها تعداد انگشت‌شماری مدیر برای مدیریت این سرورها دارند، به کلیدهای SSH تکیه می‌کنند تا به آن‌ها برای انجام مؤثر این امور کمک کنند. کلیدها علاوه بر راحتی که ارائه می‌کنند ممکن است ریسک‌های امنیتی نیز داشته باشند که شبیه به ریسک‌های حساب‌های اشتراکی است:

۱. کلیدهای SSH وابسته به حساب‌های سرور یونیکس بوده و به فرد متصل نیستند. چطور می‌شود برای یک حسابرسی اثبات کرد که یک کاربر خاص با استفاده از کلیدهای SSH به یک سرور دسترسی داشته است؟
۲. جایگزینی و مدیریت کلیدهای SSH نیاز به کار عملی و دستی دارد. از آنجایی که این کلیدها روی سرورهای یونیکس استفاده شده و معمولاً تعداد کمی از مدیران یونیکس در سازمان‌ها وجود دارند، لذا ممکن است این کلیدها به‌سادگی تنظیم شده و فراموش شوند. در اینجا یک ریسک عملیاتی بزرگ وجود خواهد داشت مبنی بر اینکه هرچه کلید قدیمی‌تر باشد، بیشتر به اشتراک گذاشته شده است و احتمال دسترسی غیرمجاز و وجود رخنه بیشتر می‌شود؛
۳. درنتیجه ریسک بیان شده در شماره قبلی، به مدیریت و تغییر دستی کلیدهای SSH منجر می‌شود تا تیم‌های فناوری اطلاعات از عبارت عبور یکسانی برای کلیدهای SSH مختلف استفاده کنند. در نتیجه تیم‌هایIT ناخواسته امنیت سازمان خود را در معرض خطر قرار می‌دهند و اگر عبارت عبور به دست شخص نامعتبری برسد، عامل تهدید راهی برای نفوذ به سازمان شما خواهد داشت.

سازمان‌ها باید مانند رمز عبورها، چرخه عمر کلیدهای SSH اعم از ایجاد، اجرایی شدن، تغییر، توزیع، مدیریت و در آخر حذف کردن آن‌ها را به‌صورت خودکار انجام دهند.

پل زدن بین دایرکتوری‌ها[1]

برنامه‌ها و سیستم‌عامل‌ها می‌توانند مدل‌های امنیت دسترسی مبتنی بر نقش داشته باشند و یا درون سرویس‌های دایرکتوری مثل اکتیو دایرکتوری (AD) یا LDAP یکپارچه شوند. متأسفانه سیستم‌های عامل زیادی به‌صورت ذاتی احراز هویت متقابل دایرکتوری از پلتفرم‌های یونیکسی و لینوکسی به ویندوز مایکروسافت را دارا نیستند. این بدین معناست که حساب یک کاربر روی ویندوز را نمی‌توان برای احراز هویت در یونیکس و لینوکس به کار برد و اینکه برای احراز هویت باید یک حساب مستعار ایجاد کرد.

در مواجه با محیط‌های پیچیده، این امر می‌تواند به هزاران حساب بر روی تعداد زیادی سیستم منجر شود که همه آن‌ها احتمالاً از نام‌های مستعار نسبتاً متفاوتی برای یک کاربر استفاده می‌کنند. این امر باعث مشکلاتی در مدیریت آن‌ها، سردرگمی در رمزهای عبور و یک فاجعه حسابرسی برای نام‌های مستعار منتسب به یک کاربر انسانی و هویت واقعی آن‌ها است. راهکار این مسئله، پل زدن بین دایرکتوری‌ها است. این راهکار روشی پایه‌ای را برای سیستم‌عامل غیرویندوزی فراهم می‌کند تا کاربران را بر اساس حساب‌های ایجادی در اکتیو دایرکتوری احراز هویت نماید؛ بنابراین می‌توانند از همان حساب مورد استفاده برای ورود به ویندوز و با همان رمز عبور برای احراز هویت در سیستم‌های عامل یونیکس، لینوکس و مک استفاده کنند.

از دید مدیریتی، این مزایا برای شما وجود دارد:

- حسابی یگانه برای تمام کاربران با همان اعتبارنامه‌ها یا الزامات چند مرحله‌ای صرف‌نظر از پلتفرم آن‌ها؛
- کمینه‌سازی نیاز به حساب‌های مستعار، مدیریت آن‌ها و همبستگی حساب‌های کاربران؛
- گرفتن گزارشات ساده از هر کاربر در تمام پلتفرم‌ها؛
- کشف حساب و مدیریت ساده برای پلتفرم‌های غیرویندوزی از طریق اکتیو دایرکتوری.

پل زدن بین دایرکتوری‌ها مثل یک تابع پایه‌ای با مزایای بسیار است، این امر می‌تواند به کمینه‌سازی تهدیدات داخلی کمک کند زیرا تمام حساب‌های اضافی ایجادشده برای کاربران

[1]Directory Bridging

در سیستم‌های غیرویندوزی را به‌صورت ساده حذف می‌کند. با توجه به اینکه تمام نام‌های مستعار حذف شده‌اند، عامل تهدید راه‌های پنهان کمی داشته و آن‌ها مجبور هستند تا به حساب‌های در حال استفاده و احتمالاً تحت نظارت سازمان حمله کنند. وقتی این امر با تحلیل داده‌ها، تحلیل رفتار کاربر و راه‌های ثبت قدیمی همراه می‌شود، یافتن فعالیت‌های مخرب بسیار ساده‌تر می‌شود.

حسابرسی و گزارش

پروژه‌های مدیریت دسترسی ممتاز بدون توانایی حسابرسی تغییرات، گزارش رویدادها، یافته‌ها و همچنین بدون ارائه مسیری قابل اقدام از فعالیت‌ها، تنها در کاهش ریسک‌های اهداف حمله دارای حقوق ویژه موفق بوده است. با وجودی که این دستاورد نیز به‌نوبه خود بسیار حائز اهمیت است ولی هیچ اقدامی در مستندسازی موردنیاز حسابرسان قانونی یا تعیین اشتباهات سهوی و عمدی که می‌توانند به رخنه داده‌ها منجر شود، انجام نمی‌دهد.

بنابراین برای اینکه اجرای موفقیت‌آمیزی از PAM داشته باشیم، مؤلفه‌هایی را در نظر می‌گیریم که به مستندسازی تغییرات و فرآیندها در طول مسیر کمک می‌کنند. این موارد عبارت‌اند از:

- مستندسازی تغییرات در سرویس‌های دایرکتوری مانند اکتیو دایرکتوری که می‌تواند زمان اجرای آغازی PAM را تحت تأثیر قرار دهد؛
- نظارت بر یکپارچگی فایل (FIM) در تمام سیستم‌عامل‌ها برای شناسایی تغییرات غیرمجاز حقوق ویژه بر روی سیستم عامل و فایل‌های اپلیکیشنی حساس؛
- مستندسازی تغییرات در برنامه‌های کلیدی مانند مایکروسافت Exchange یا سرور SQL که می‌تواند به‌وسیله عامل تهدید برای نظارت یا نفوذ به داده‌ها مورد استفاده قرار گیرد؛
- نظارت بر رکوردهای ثبت‌شده رویدادها، برای رویدادهای حیاتی که می‌تواند سوءاستفاده‌های احتمالی از حقوق ویژه را نشان دهد؛
- نظارت بر تمام نشست‌های تعاملی، ثبت کلیدهای فشرده‌شده و نظارت بر اپلیکیشن.

وقتی این مفاهیم پیاده‌سازی شوند، نشان دادن مدیریت دسترسی‌های ممتاز به‌عنوان تابعی از انطباق‌پذیری نسبتاً ابتدایی می‌شود. خروجی گرفتن از گزارش‌ها، فیلتر کردن دستورات،

بازبینی نشست ممتاز و غیره، همه به مؤلفه‌هایی برای مستندسازی تبدیل می‌شود و مهم‌تر از همه ارائه امنیت موردنیاز برای جلوگیری از استفاده کردن از حقوق ویژه به‌عنوان اهداف حمله نیز است.

تحلیل تهدیدات حقوق ویژه

با وجودی که کاهش مجوزهای کاربرها و به‌کارگیری مفهوم حداقل حقوق ویژه در کاهش سطح حمله و تأثیر احتمالی یک نفوذ مفید هستند ولی باید در نظر داشت که این کاربران در برخی از نقاط برای اجرای وظایف معمول خود نیاز به دسترسی با حقوق بیشتری دارند. باید در نظر داشت که این حساب‌ها ریسک قابل‌توجهی را برای سازمان‌ها به همراه دارند و برای اجرای وظایف خاص و دسترسی به مجموعه داده‌های خاص، مجوزی دریافت می‌کنند. کنترل و حسابرسی دقیق این حساب‌ها خارج از گستره مدیریت شناسه‌های معمول است. چطور باید تشخیص داد که یک حساب تأییدشده از مجوزهای اعطایی خود سوءاستفاده می‌کند یا ممکن است این حساب احتمالا هک شده باشد؟ لذا نیاز است تا از پایه به بررسی این امر بپردازیم.

یکی از عجیب‌ترین کلمات در زبان انگلیسی، کلمه Datum به معنای مأخذ یا داده است. طبق تعریف این کلمه شکل مفرد کلمه Data به معنای داده‌ها است اما به‌ندرت در گفتگوها یا مستندات نوشته‌شده دیده می‌شود. به‌طورکلی این کلمه به نقطه مفردی از اطلاعات یا نقطه مبنای یک مقیاس یا عملیات اشاره دارد. وقتی‌که اطلاعات امنیتی یا اقدامات مربوط به رفع عیوب را مرور می‌کنیم، معمولاً به تک درایه ثبتی با نام داده‌ها یا همان Data اشاره می‌کنیم درحالی‌که درواقع شکل درست آن به‌صورت داده یا Datum است. شاید شما این عبارت را منسوخ‌شده در نظر بگیرد ولی وقتی بحث امنیت در میان باشد، ما در موارد زیادی تصمیمات حیاتی را بر روی داده می‌گیریم نه داده‌ها. در اینجا بحث‌ها بر سر تحلیل رفتار کاربر اهمیت پیدا می‌کند، باید در نظر داشت که نباید تصمیمی را صرفاً بر پایه رفتار یک کاربر در داده (Datum) بنا کنیم بلکه تجزیه‌وتحلیل رفتار کاربر نیاز به داده‌ها (Data) دارند. هر راهکار تحلیلی که توصیه‌ای را بر مبنای یک قطعه‌ای از اطلاعات ارائه می‌دهد، بیشتر شبیه به یک راهکار نظارت بر رویدادهای امنیتی است تا یک موتور تحلیلی. برای مثال، یک رویداد مبتنی بر زمان، تاریخ، کاربر و مکان، یک رویداد تحلیلی نیست بلکه فقط یک datum است. این اطلاعات با دیگر رویدادهای datum یکپارچه شده و پردازش می‌شوند ولی بااین‌حال هنوز هم

پردازش این رویدادهای یکپارچه‌شده تحلیلی نیست و در اصل این کار فقط ایجاد موتور یکپارچه‌ای است که چندین رویداد را از لحاظ منطقی مرور می‌کند؛ بنابراین در صورت داشتن رویدادهای تکی تنها در صورت استفاده از پردازش‌های یادگیری ماشین، تحلیل‌های خوشه‌ای، موتورهای همبسته‌سازی سازگار و غیره می‌توان گفت که یک کار تحلیلی انجام داده‌ایم. آگاهی از تحلیل و مدل جذب داده‌ها کلید فهم این موضوع است که متوجه شویم راهکار تحلیلی می‌تواند در شناسایی و حل ناهنجاری‌های امنیتی کمک‌کننده باشد یا خیر.

عامل تهدید سعی می‌کند تا هر ردی از اقدامات یا تحرکات خود را در سازمان پاک کرده و حذف نماید. نقطه اصلی استفاده از حقوق ویژه به‌عنوان اهداف حمله آن است تا هر زمانی را که عامل تهدید سعی دارد به حساب‌های ممتاز دسترسی داشته باشد، مستند کنیم. این کار مجموعه داده‌هایی از فعالیت‌های عاملان تهدید را بر اساس رفتارهای نامعمول آن‌ها تولید می‌کند و با استفاده از تحلیل داده‌ها توسط موتورهای خودکار سعی دارد تا عاملان تهدید را در هنگام نفوذ آن‌ها به یک محیط شناسایی کند. رویکرد و رویه فعلی در بازار، پیاده‌سازی تحلیل‌های پیشرفته رفتاری و تهدیدی، برای شناسایی رفتارهای مشکوک در این حساب‌ها است. به‌هرحال بسیاری از راهکارهایی که به تحلیل‌های تاریخچه‌ای قابل‌توجهی نیاز دارند، به دلیل رویکرد محرمانه‌ای که دارند و همچنین تنها تحلیل عناصر داده‌ای سطح بالا مانند رکوردهای ثبتی یا داده‌های ارسالی به SIEM، نمی‌توانند مورد اطمینان باشند. علاوه بر آن، این راهکارها بر روی شناسایی تمرکز دارند و نه مهار آن. این حوزه‌ای است که در آن قابلیت‌های PAM یکپارچه می‌تواند مزایای زیادی را ارائه کند. PAM یک راهکار سازمانی است که می‌تواند دسترسی‌های حساس را اعطا کرده و یا رد کند. PAM محدود به سیاست‌های دسترسی صفر یا صد نیست بلکه می‌تواند به‌صورت پویا، سیاست‌های دسترسی، عملیات تأیید برای سیستم‌های حساس، برنامه‌ها و داده‌ها را تنظیم کرده و تغییر دهد. این حوزه‌ای است که سازمان‌ها و متخصصان امنیتی باید به نظارت آن ادامه دهند. شرکت‌هایی مثل مکافی[1] استانداردهای جدیدی مثل OpenDXL را برای خودکارسازی پاسخ بر اساس هر رویداد همبسته توسعه داده‌اند و حلقه را بر اساس نتایج تحلیل تهدید به‌صورت خودکار می‌بندند.

[1] McAfee

فصل ۱۱

معماری مدیریت دسترسی‌های ممتاز (PAM)

مدیریت دسترسی‌های ممتاز (PAM)، مدیریت خودکار رمز عبور و نشست را فراهم می‌کند تا عملیات کنترل، حسابرسی، تغییر و ثبت امن دسترسی برای هر نوع حساب ممتاز را ارائه کند. این فناوری برای مدیریت حساب‌های اشتراکی مدیر محلی یا دامنه، حساب‌های شخصی کاربر، سرویس‌ها، سیستم‌عامل‌ها، دستگاه‌های شبکه، پایگاه داده (A2DB)، اپلیکیشن (A2A) و حتی کلیدهای SSH، ابر و رسانه اجتماعی طراحی شده است. با بهبود مسئولیت‌پذیری و کنترل رمزهای حساب‌های ممتاز، سازمان‌های IT می‌توانند تهدیدات حقوق ویژه را کمینه سازند و به اهداف مدنظرشان دست یابند.

به‌هرحال اجرای این فناوری علاوه بر کاربردهای ذکرشده به حضور منابع در سازمان، فضای مجازی یا فضای ابری وابسته است. به‌علاوه سازمان‌ها باید دسترسی‌پذیری بالا، بازیابی پس از فاجعه، راهکارهای Break Glass و مدت زمان موردنیاز برای بازیابی در مواقعی که خطایی در هر مؤلفه‌ای (از زیرساخت شبکه‌ها گرفته تا ارتباطات اینترنت) رخ می‌دهد، مدنظر قرار دهند؛ بنابراین پیکربندی‌های مختلفی را باید برای پشتیبانی از تجهیزات یک سایت یا سایت‌های مختلف در نظر داشت که ممکن است این سایت‌ها در مناطق جغرافیایی مختلفی پراکنده شده باشند. این موارد عبارت‌اند از:

- ✓ **اکتیو/ اکتیو**– که گاهاً هم اکتیو چندگانه نامیده می‌شود، این مورد به گره‌های چندگانه اجازه می‌دهد تا به‌طور هم‌زمان فعال باشند. هر گره به‌صورت مستقیم به پایگاه داده متصل می‌شود.

مزایا

- مقیاس‌پذیری نامحدود
- افزونگی مؤلفه‌ها
- رویدادهای هدفمند تغییر رمز عبور برای مکان‌های خاص

معایب

- نیاز به پایگاه داده خارجی؛
- پیکربندی‌های پایگاه داده‌های اضافی مانند SQL AlwaysOn می‌تواند هزینه‌بر باشد و به افراد خاصی برای مدیریت آن نیاز داشته باشد و راهکارهای پایگاه داده متن‌باز نیز ممکن است برای یک اپلیکیشن لایه I از این قسم مناسب نباشد؛
- این بر عهده مصرف‌کننده است که تضمین نماید پایگاه داده و سرورهای پشتیبان آن به‌صورت امن تنظیم شده باشند.

✓ **اکتیو/ پسیو**– برای اکتیو/ پسیو به نصب دو تجهیز نیاز داریم. پایگاه داده‌های داخلی تکثیر[1] می‌شوند و اگر که قرار باشد که دومی عملیات‌هایی را بر عهده بگیرد، اعلان-هایی از اولی به دومی ارسال می‌شود.

مزایا

- راه‌اندازی ساده
- دسترسی‌پذیری بالا، درون راهکار به کار گرفته می‌شود

معایب

- برای سوئیچینگ خودکار کاربران به ابزار اکتیو، به یک متعادل‌کننده بار خارجی نیاز است؛
- فرآیند غلبه بر خرابی[2] فوری نیست و ممکن است برای به راه افتادن به زمان نیاز داشته باشد؛

[1] Replicate
[2] Failover

- نسخه‌های یدکی امکان دارد پایگاه‌های داده‌ای داشته باشند که همگام نباشند یا در صورتی که مدت زمان زیادی از پشتیبان اولیه گذشته باشد، پیکربندی‌های مختلفی داشته باشند.
- ✓ **غلبه بر خرابی‌های ثالث**– برای مواردی که در آن تنها نصب یک تجهیز مطلوب است، فناوری مجازی‌سازی می‌تواند برای حفظ نصب به‌صورت مداوم و از طریق تکثیر در دسترس باشد، حتی اگر سرور فیزیکی در حال اجرا به هر دلیلی آفلاین شود.

مزایا

- دسترسی‌پذیری مقرون‌به‌صرفه با یک نمونه
- ارائه دسترسی‌پذیری بالا و عملکرد پیوسته در زمان از دسترس خارج شدن سرور میزبان

معایب

- برای راه‌اندازی و پیکربندی درست، مبتنی بر فناوری تکثیر مجازی است؛
- در صورت بروز خرابی نرم‌افزار، افزونگی ارائه نمی‌شود.

جدای از انتخاب مدل برای دسترسی‌پذیری PAM و تحمل در برابر خطا، آن مدل بایستی بسته به موقعیت اجرا تنظیم گردد. همچنین از این نظر که در سازمان نیازی به مدل هیبرید هست یا خیر نیز باید مورد بررسی قرار گیرد. این موارد برای مدیریت دسترسی‌های ممتاز به‌صورت اجرای درون‌سازمانی، ابری، زیرساخت به‌عنوان سرویس (IaaS) و نرم‌افزار به‌عنوان سرویس (SaaS) بیان می‌شوند. برای رسیدن به این هدف، مدل کامل مدیریت دسترسی‌های ممتاز ارائه‌شده در جدول (۱۱-۱) را در نظر بگیرید. این جدول به شما کمک می‌کند تا در سازمان مسیر پیاده‌سازی PAM را دریابید.

جدول (۱۱-۱) مدل کامل مدیریت دسترسی‌های ممتاز

مدل کامل حق ویژه دسترسی	سطح ۱ ناموجود	سطح ۲ موردی[1]	سطح ۳ استانداردشده	سطح ۴ مدیریت‌شده	سطح ۵ پیشرفته
حساب‌های اشتراکی	کنترل‌های محدود	کنترل‌ها و فرآیندهای دستی	کشف، فهرست‌سازی و استقرار خودکار	دسترسی و مدیریت نشست بدون رمز عبور	یکپارچگی هویت (IAM، SSO، AD-Bridge، حسابرسی و بازیابی AD)
	بدون مدیریت رمز عبور حساب مشترک	دنباله‌ای از اسناد که قابل اطمینان نیستند	مدیریت متمرکز رمز عبور با تأیید گردش کار و تغییر خودکار	دسترسی ممتاز با آگاهی از محیط و با استفاده از RBAC و MFA	پوشش پیشرفته (ابر، SaaS و اپلیکیشن‌ها)
	نبود مسئولیت‌پذیری		گزارش مصرف حساب ممتاز		HSM تحلیل رفتار کاربر
حساب‌های اپلیکیشن و سرویس	نامشخص و مدیریت‌نشده	مستند شده	مدیریت اپلیکیشن به اپلیکیشن هدفمند	مدیریت اپلیکیشن به اپلیکیشن متمرکز	DevOps یکپارچه‌شده
		نوشتن رمز در کد برنامه	رمزهای عبور نوشته‌شده در کد برنامه حذف شوند	بدون رمزهای عبور نوشته‌شده در کد برنامه	حجم بالا
		تغییر کم یا بدون تغییر	بازیابی با محور API		HA و ذخیره‌سازی پنهان برای افزونگی
نظارت فعال و شناسایی تهدید	بدون نظارت	فایل‌های ثبتی توزیع‌شده	کنترل‌های حسابرسی متمرکز	شناسایی و UBA پیشرفته تهدید	پاسخ فعال حق ویژه خودکار (رد، غیرفعال سازی، قرنطینه و هشدار)

[1] Adhoc

		نبود ردیابی از استفاده شخصی از حساب‌های اشتراکی	مسئولیت‌پذیری فردی در استفاده از حساب‌های اشتراکی	یکپارچه‌سازی SIEM	یکپارچه‌سازی IGA
			رؤیت‌پذیری عمیق با ثبت نشست‌ها و کلیدهای فشرده‌شده	نمایه‌سازی خودکار کلمات کلیدی و فعالیت‌ها	استقلال پلتفرم
مدیریت دقیق دسکتاپ	مدیریت‌نشده، کاربران دسترسی مدیر دارند	حذف برخی از حقوق مدیر	مدیریت متمرکز رمز عبور	دسترسی دقیق	سیاست دسترسی با آگاهی از محیط (ریسک کاربر، ریسک دارایی، اعتبارسنجی ITSM و MFA)
		ابزارهای دسکتاپ برای ارتقاء موردی	دسترسی محدود پروکسی مطابق با لیست سفید/ سیاه	نشست‌های کنترل‌شده سرور از راه دور	یکپارچه‌سازی IGA با جداسازی وظایف
			سرویس‌های اعتباری	FIM	استقلال دارایی دسکتاپ و سیاست کاربر
				کنترل اقدامات بعدی	
مدیریت دقیق سرور	مدیریت نشده، کاربران دسترسی روت دارند	ایزوله‌شده	مدیریت متمرکز رمز عبور	دسترسی دقیق	سیاست دسترسی با آگاهی از محیط (ریسک کاربر، ریسک دارایی، اعتبارسنجی ITSM و MFA)

		متن‌باز (SUDO)	دسترسی محدود پروکسی مطابق با لیست سفید/ سیاه	سپر دارای حق ویژه	یکپارچه‌سازی IGA با جداسازی وظایف
			وابسته به پلتفرم	نشست‌های کنترل‌شده سرور از راه دور	استقلال سیاست کاربر و دارایی سرور
				FIM	
				کنترل اقدامات بعدی	
مدیریت دقیق زیرساخت	مدیریت نشده، کاربران دسترسی روت دارند	ایزوله‌شده	مدیریت متمرکز رمز عبور	دسترسی دقیق	سیاست دسترسی با آگاهی از محیط (ریسک کاربر، ریسک دارایی، اعتبارسنجی ITSM، MFA)
		وابستگی به فروشنده	دسترسی محدود پروکسی مطابق با لیست سفید/ سیاه	نشست‌های کنترل‌شده سرور از راه دور	سیاست دسترسی با آگاهی از محیط (ریسک کاربر، ریسک دارایی، اعتبارسنجی ITSM و MFA)
				کنترل اقدامات بعدی	

درون محیطی

اجرای درون محیطی مدیریت دسترسی‌های ممتاز در محدوده‌های فایروال‌بندی شده شبکه سازمان عمل می‌کند ولی می‌تواند منابعی را که از مراکز داده به منابع ابری، اتصالی خارج از باند را نیز برقرار می‌کنند، مدیریت کند. این پیاده‌سازی می‌تواند شبکه‌ای فاقد دسترسی اینترنتی باشد اما باید یک مسیر شبکه‌ای به سیستم‌های هدف داشته باشد یا با استفاده از گره‌های مدیریت از راه دور، بتواند تغییرات رمز عبور را انجام دهد. این معماری بسیار شبیه به یک راهکار ایمیل درون‌سازمانی یا سیستم ضد ویروس با مدیریت متمرکز است. تفاوت اصلی آن است که مدیر PAM باید نام‌های میزبان را انتخاب کرده و مسیر خود را به هر جزء مدیریت‌شده برای تغییرات رمز عبور بیابد و هر گره باید بتواند سروری را برگزیند و مسیر شبکه‌ای را برای هر فناوری عاملی که ممکن است بخشی از مدل اجرایی PAM باشد، ارائه کند. اگر شبکه مشکلات پایداری با DNS، NTP، تکثیر AD، مسیریابی یا عملکرد داشته باشد، یکپارچه‌سازی هر مدل اجرایی PAM می‌تواند معضلی باشد؛ بنابراین شبکه‌ای با معماری صحیح و پایدار موردنیاز است چون PAM برای استقرار، مدیریت و تغییر رمزهای عبور به‌صورت مؤثر همراه با نظارت بر نشست، به زیرساخت متکی است. برای یک عامل تهدید، زیرساخت ضعیف مکانی عالی برای انجام کارهای موردنظر است. خطاهایی مربوط به DNS، تکثیر AD از طریق موارد ثبت‌شده با مدیریت ضعیف می‌تواند هویت آن‌ها را حتی با یک مدل اجرایی مدیریت دسترسی‌های ممتاز پنهان سازد. بازی والدو را در نظر بگیرد و اینکه اگر او می‌توانست پشت خطاهای زیرساختی پنهان شود که در حالت عادی نباید در یک سازمانی با عملکرد صحیح وجود داشته باشد.

ابر

مدل‌های اجرایی ابر برای مدیریت دسترسی‌های ممتاز می‌تواند شکل‌های مختلفی داشته باشد:

- مدیریت حقوق ویژه ابر به ابر شامل اپلیکیشن به اپلیکیشن (IaaS)
- ذخیره‌سازی و مدیریت حقوق ویژه مبتنی بر ابر برای کاربران (SaaS)
- مدیریت حقوق ویژه برای منابع درون محیطی (هیبرید)

اگر این یک سؤال چند گزینه‌ای بود، نوآوری‌های استراتژیک سازمان شما احتمالاً به بیش از یکی از این انتخاب‌ها نیاز داشت. در مدیریت دسترسی‌های ممتاز بسیار غیرمعمول است تا تنها در یک بخش از سازمان و بدون داشتن برنامه‌ای جهت گسترش فناوری در تمام سیستم‌های حساس و حساب‌های ممتاز استفاده شود. درحالی‌که ممکن است اجرای اولیه آن در محدوده کوچکی آغاز شود ولی بعد از مدتی امکان دارد برای داشتن قابلیت مدیریت از هر مکانی، نیازمند ابر باشد. این موضوع در زمان انتخاب مدیریت دسترسی‌های ممتاز درون محیطی، ابری و یا هیبریدی حیاتی است. برای رویکردهای هیبریدی این مورد می‌تواند ترکیبی از IaaS، SaaS یا درون محیطی یا به‌صورت ترکیبی با استفاده از گره‌های مدیریت از راه دور جهت مسیریابی و تجمیع داده‌ها به‌صورت امن باشد.

زیرساخت به‌عنوان سرویس (IaaS)

چه سازمان شما تصمیم بگیرد تنها با یک سرویس‌دهنده ابری کار کند و یا چندین شرکت ابری را انتخاب کند و یا اصلاً مقررات مبتنی بر محدودیت‌های جغرافیایی داشته باشد، محیط‌های ابری باید برنامه‌ها و کاربران را مانند هر فناوری اطلاعات دیگری احراز هویت نمایند. مدیریت دسترسی‌های ممتاز الزامات منحصربه‌فردی را در مقایسه با پیاده‌سازی درون محیطی دارد:

- معماری‌های با قابلیت دسترسی‌پذیری بالا می‌توانند نمونه‌های ابری اضافی را در زمان از دسترس خارج شدن ابر یا زیرساخت ارائه نمایند و دسترس‌پذیری را تضمین کنند؛
- قوانین و مقررات ممکن است به نمونه‌های مجزا اما تکراری نیاز داشته باشند و داده‌ها را بر اساس قوانین منطقه‌ای یا محلی فیلتر سازند؛
- سازمان‌ها ممکن است محدوده‌های IP عمومی و خصوصی داشته باشند تا خدمات موردنیاز را ارائه کنند و نیاز به تدارکات خاصی برای امن‌سازی آن‌ها باشد؛
- مدیریت آسیب‌پذیری ناشی از سرویس‌های عمومی به ارائه‌کننده بالاتری برای کاهش تهدیدات نیاز دارد؛
- دسترسی API نیاز به توجه خاصی برای دسترسی امن و محدودسازی افشاء دارد؛

- داده‌های مهم در ابر مانند رمزهای عبور، به روش‌های امنیتی اضافی مانند HSM برای حفاظت از اطلاعات پایگاه داده نیاز دارند.

برای سازمان‌هایی که به دنبال پیاده‌سازی راهکار PAM، تنها در ابر هستند چندین فناوری وجود دارد. معمول‌ترین آن‌ها استفاده از فناوری جعبه سیاه[1] مبتنی بر راهکارهای PAM به میزبانی ارائه‌دهندگان سرویس‌های ابری (آمازون AWS، Microsoft Azure ، ابر گوگل، ابر اوراکل یا سرویس‌دهنده‌های ثالث) است. برخی از فروشندگان PAM نیز راهکارهایی را ارائه می‌دهند که می‌توان آن‌ها را به‌عنوان یک پیاده‌سازی نرم‌افزاری در قالب سیستم‌عامل ابری معرفی کرد. این موارد بیشترین انعطاف‌پذیری را برای یک مشتری ارائه می‌کنند اما امنیت، مقاوم‌سازی و پیکربندی سیستم‌عامل بر عهده مشتری است و بر عهده ارائه‌دهنده ابر یا فروشنده PAM نیست. برای این نوع از پیاده‌سازی‌ها، ریسک‌ها بیشتر هستند زیرا ممکن است هرگونه نقص داخلی در محیط، باعث ایجاد یک مشکل امنیت سایبری شود ولی می‌توان آن را سفارشی‌سازی کرد تا الزامات منحصربه‌فردی را محقق نماید.

نرم‌افزار به‌عنوان سرویس (SaaS)

راهکارهای مدیریت دسترسی‌های ممتاز که به‌صورت یک راهکار SaaS اجرایی شده است، می‌توانند صرفاً در ابر اجرایی شوند و یا برای مسیریابی و تجمیع سیاست و رویدادها به گره‌های مدیریتی درون سازمان نیازمند باشند. این پیاده‌سازی‌ها به‌طور کامل و به‌وسیله فروشنده PAM مدیریت می‌شوند و منابع ابری را با دیگر کلاینت‌های PAM در مدل نصبی چند مستاجری[2] فروشنده به اشتراک می‌گذارند. درحالی‌که امروزه راهکارهای PAM بسیار کمی در ابر وجود دارند که از SaaS استفاده کنند ولی رویه‌ها نشان‌دهنده این است که سازمان‌ها به‌تدریج به ذخیره‌سازی رمزهای عبور، سیاست‌ها و ابزارهای مدیریتی PAM در ابر تمایل نشان می‌دهند. این روند با پیشروی فروشندگان منحصربه‌فرد و ارائه‌دهندگان خدمات مدیریت‌شده (MSP) ادامه می‌یابد که در حال ارائه خدمات مقرون‌به‌صرفه مبتنی بر پیشنهادهای تجاری PAM هستند و هزینه‌های کم یا حتی متمایل به صفر را برای کاربران نهایی در نظر می‌گیرند.

[1] Black Box
[2] Multi-Tenant

فصل ۱۲

Break Glass

Break Glass عبارتی است که در زمینه کامپیوتر استفاده می‌شود و مختص به زمانی است که موقعیتی اضطراری پیش می‌آید و روش‌های دسترسی متداول با شکست مواجه می‌شوند. در اصل این عبارت از شکستن شیشه در زمان شنیدن هشدار آتش‌سوزی الهام گرفته شده است. کنترل‌های دسترسی به یک اپلیکیشن یا دارایی را می‌توان در طی یک مورد اضطراری با استفاده از Break Glass دور زد. یک کاربر در صورت نیاز به دسترسی فوری، درخواست Break Glass را اجرا می‌کند یا اعتبارنامه‌ها را منتشر می‌نماید، حتی اگر کاربر مجاز به مدیریت آن سیستم نباشد. این روش به‌طور سفارشی برای حساب‌های سیستمی در سطح بالا مانند حساب‌های روت در یونیکس و لینوکس، SYS یا SA برای پایگاه داده یا مدیر (administrator) برای ویندوز (محلی یا دامنه) استفاده می‌شود. این حساب‌های ممتاز معمولاً به شخص خاصی اختصاص نمی‌یابد بلکه به‌جای آن Break Glass موارد استفاده خود را با کنترل‌های مختلف محدود می‌کند تا ریسک‌ها را کاهش داده و تنها وظایفی خاص را ممکن سازد اما واضح است که دسترسی کاربر به اعتبارنامه‌های Break Glass همچنان محدود است.

سناریوهای Break Glass می‌تواند به علت از دسترس خارج شدن شبکه، خطاهای اپلیکیشن یا بلایای طبیعی اجرا شود که این اتفاقات دسترسی عادی به راهکارهای PAM را با اختلال مواجه می‌کنند؛ بنابراین عامل‌هایی مانند منبع توان و قابلیت اتصال شبکه باید در هنگام طراحی سیاست‌های Break Glass مورد بررسی قرار گیرند، همچنین عامل تهدید ممکن است فرآیند Break Glass شما را یک هدف حمله برای خود قرار دهد چون شامل اعتبارنامه‌هایی جهت مدیریت سیستم‌ها است. دسترسی اعتبارنامه‌های مورد استفاده در Break Glass باید

به‌صورت سخت‌گیرانه‌ای مرتب مورد نظارت قرار گیرند. سناریوهای Break Glass معمولاً زمانی در نظر گرفته می‌شوند که مدیران فناوری اطلاعات در حال اجرای زیرساختی حیاتی برای دسترسی امن به سیستم هستند. در اینجا سه مورد متداول سناریوهای Break Glass قابل اعمال در اکثر سازمان‌ها را بیان می‌کنیم:

۱. الزام دسترسی فوری و مستقیم به سیستم‌های تحت مدیریت با استفاده از یک رمز عبور به‌عنوان عامل فعال‌ساز؛
۲. دسترسی خارج از فرآیندهای استاندارد به منابع به دلیل از دسترس خارج شدن سیستم‌های حیاتی یا در دسترس نبودن فرد تأییدکننده؛
۳. بازیابی رمزهای عبور یا موارد محرمانه از یک صندوق امن فیزیکی یا دیگر پشتیبان‌های آفلاین روی یک دستگاه فیزیکی مثل USB یا CD.

فرآیند Break Glass

هنگام طراحی و توسعه سیاست‌های Break Glass، ملاحظات و فرآیندهای بالقوه‌ای وجود دارند که باید آن‌ها را پیاده‌سازی نمود:

- برای کاربران تأییدشده Break Glass (جدید یا موجود)، ساختن حساب‌های کاربری ضروری را باید از پیش در نظر داشته باشیم که این حساب‌ها مدیریت شده و توزیع گردند تا بتوان آن‌ها را به‌سرعت در دسترس قرار داد، بااین‌حال محدودیت‌های مناسبی را هم در برابر عامل تهدید داشته باشند. حساب‌های Break Glass و روندهای توزیع باید مستند شده و به‌عنوان بخشی از پیاده‌سازی تست شوند و به‌دقت مدیریت شوند تا دسترسی را در زمان موردنیاز ارائه کنند. این موارد را می‌توان در برنامه مدیریت‌کننده رمز عبور یا یک مکان فیزیکی امن ذخیره‌سازی کرد و نسخه‌هایی کاغذی از آن‌ها را در ابزاری دیگر یا محیطی امن ذخیره نمود؛
- برای تطابق با الزامات حسابرسی، حتی اگر تأییدی دور زده شود، سیستم باید همچنان شخصی را که دسترسی داشته و اقداماتی را که انجام داده است، ثبت نماید. به‌علاوه، مدیران IT باید داده‌های ثبت‌شده را بازبینی نمایند تا تطابق آن‌ها با فرآیندهای مدیریت تغییر را در هنگام استفاده از فرآیند Break Glass تضمین نمایند؛

- فرآیندهای Break Glass که خارج از فناوری‌های مدیریت کننده رمز عبور پیاده‌سازی می‌شوند، برای مثال یک گاوصندوق فیزیکی و یا ذخیره‌سازی رمزهای عبور چاپ‌شده، باید به‌صورت مرتب به‌روزرسانی شوند و برای کنترل کارایی و تغییر به‌صورت دستی مورد آزمایش قرار گیرند. تنها کاربران انتخابی مورد اطمینان باید به کلیدهای گاوصندوق فیزیکی دسترسی داشته باشند و باید با آن‌ها مانند دیگر اطلاعات حساس درون سازمان رفتار کرد.

Break Glass با استفاده از یک نرم‌افزار مدیریت رمز عبور

تیم‌های فناوری اطلاعات سازمان‌ها اغلب از یک نرم‌افزار مدیریت رمز عبور به‌عنوان راهکاری برای Break Glass، در جهت ارائه دسترسی به محیط سازمان در مواقعی استفاده می‌کنند که فرآیندهای تبیین‌شده برای ورود یا احراز هویت با شکست مواجه می‌شوند. واحد IT ممکن است با LDAP، AD یا غیره احراز هویت کاربران را انجام دهد. درصورتی‌که کاربر بخواهد با استفاده از راهکار حقوق ویژه حداقلی یا sudo به حقوق ویژه مدیریتی محدودشده‌ای دست یابد ولی این روش با خطایی مواجه شود، آنگاه فرآیند Break Glass یک رمز عبور را به‌وسیله واحد IT برای یک حساب در محدوده پارامترهای تبیین‌شده (مانند چهارچوب زمانی، حقوق ویژه، گستره و غیره) فراهم می‌کند تا کاربر به اپلیکیشن یا سیستم موردنظر دسترسی پیدا کند.

در حالت عادی، کاربرانی که به رمزهای عبور ممتاز نیاز دارند به این ابزار برای بازیابی و به دست آوردن یک رمز عبور یا ایجاد نشست، دسترسی دارند به‌گونه‌ای که می‌توانند هر کاری یا عملیاتی را که به نقش آن‌ها اختصاص یافته است، اجرا نمایند. این امر نیازمند راهکار مدیریت رمز عبوری است که مجوزهایی برای مدیریت، تغییر و حفظ کامل رمز عبور کنونی داشته باشد. تکیه به کاربران نهایی برای به خاطر آوردن، تغییر و مستندسازی امن تمام رمزهای عبور، همیشه قابل اطمینان نبوده و ریسک بیشتری دارد.

هنگام استفاده از نرم‌افزار مدیریت رمز عبور، این کاربردهای Break Glass را در نظر بگیرید:

۱. شخصی که به رمز عبور مدیریت‌شده نیاز دارد ولی نمی‌تواند وارد شود:

الف. دسترسی کاربر را به نرم‌افزار مدیریت رمز عبور اصلاح کنید؛

ب. اعتبارنامه‌های مدیریت‌شده را مجدداً تنظیم کنید؛
ج. رمز عبور را برای کاربری که به نرم‌افزار مدیریت رمز عبور دسترسی دارد تنظیم مجدد کنید.

۲. خطای احراز هویت به نرم‌افزار مدیریت رمز عبور:

الف. قابلیت اتصال شبکه برای مسیرهای حیاتی را اصلاح کنید؛
ب. قابلیت اتصال نرم‌افزار مدیریت رمز عبور به سرویس‌های احراز هویت حیاتی را به حالت اول برگردانید؛
ج. سیستم احراز هویت را اصلاح کنید؛
د. نسخه‌ای چاپ‌شده از رمز عبورها را در یک مکان با امنیت بالا ذخیره کنید.

۳. نرم‌افزار مدیریت رمز عبور در دسترس نیست:

الف. قابلیت اتصال شبکه را اصلاح کنید؛
ب. از طریق گره مقاوم در برابر خطا به نرم‌افزار دسترسی پیدا کنید.

۴. رمزهای مدیریت‌شده فاقد اعتبار هستند:

الف. با استفاده از نرم‌افزار به‌صورت خودکار یک رمز عبور جدید را تولید کنید؛
ب. از ویژگی تاریخچه رمز عبور در نرم‌افزار مدیریت‌کننده رمز عبور استفاده کنید تا آخرین رمز عبور معتبری را که استفاده کردید، بیابید.

۵. مشکلات قابلیت اتصال:

الف. وقتی سرویس‌های حیاتی عمل نمی‌کنند، ممکن است به دسترسی از طریق iDrac، شبکه‌های مدیریتی و یا کِرَش کارت‌ها[1] نیاز باشد؛
ب. وقتی قابلیت اتصال شبکه اجازه دسترسی را نمی‌دهد، اتصال بعدی که در رنج تقسیم‌بندی نیست، می‌تواند دسترسی Break Glass را فراهم کند.

۶. فرآیندها و گردش کاری مانع دسترسی هستند:

الف. هیچ تأییدکننده‌ای در دوره زمانی موردنیاز موجود نیست؛
ب. دسترسی کاربر به خاطر مالکیت سیستم مانند نقش کارمند، پیمانکار یا فروشنده محدود شده است؛

[1] Crash Carts

ج. رویدادهای بحرانی نیاز به دسترسی بدون محدودیت و فوری دارند.

مدیریت نشست

برای مواردی که Break Glass نیستند، راهکار مدیریت رمز عبور سازمانی، قابلیت اتصال را به‌وسیله مدیر نشست جهت مستندسازی فعالیت اجرا کرده و تقسیم‌بندی را اعمال می‌نماید. با توجه به طراحی، هیچ راه جایگزینی برای اتصال به شبکه و سیستم هدف بدون دسترسی اولیه به مدیر نشست وجود ندارد. یک گزینه برای دسترسی به Break Glass آن است که کنترل‌های امنیتی را کنار بگذاریم تا دسترس‌پذیری را به حالت اول بازگردانیم اما مانند تمام تصمیم‌های مبتنی بر ریسک، بازبینی و مستندسازی ریسک‌ها و حرکت در مسیر سازمان اهمیت دارد. این امر برای تمام دسترسی‌های اعطایی خارج از فرآیندهای عادی صادق است. به‌عنوان یک جایگزین بالقوه، شبکه‌های مدیریتی کنترل‌کننده دسترسی iDarc یا سرورهای ترمینال ممکن است رویکردی امن‌تر و جایگزین را نسبت به کاهش کنترل‌های امنیتی در سناریو Break Glass ارائه کنند، مخصوصاً وقتی‌که آن رویداد احتمالاً مرتبط با امنیت است. دسترسی به شبکه‌های مدیریتی می‌تواند به‌صورت مستقل نظارت شود تا کنترل‌ها و تضمین‌های امنیتی مشابهی را ارائه کند. دسترسی به سناریوی Break Glass باید شامل دو راه زیر برای دسترسی به مدیر نشست در زمان رخداد قطع دسترسی باشد:

۱. کنترل دسترسی ثالث برای سیستم‌های مدیریت‌شده:

الف. باز کردن دسترسی جایگزین به درون شبکه سازمان با استفاده از اتصالات پشتیبان؛
ب. غیرفعال سازی دسترسی مدیریت نشست به سیستم‌های اصلی (پیشنهاد نمی‌شود).

۲. دسترسی مدیریت نشست در یک مرکز داده جایگزین:

الف. باز کردن مسیر شبکه در اطراف دستگاه مدیریت نشست (پیشنهاد نمی‌شود)؛
ب. دسترسی به دستگاه مدیریت نشست در یک مرکز داده جایگزین یا محیط بازیابی فاجعه؛
ج. انجام مدیریت نشست به‌صورت مستقل برای شبکه‌های مدیریتی به‌منظور ارائه دسترسی.

رمزهای عبور قدیمی

موقعیت‌های زیادی وجود دارند که در آن رمز عبور ذخیره‌شده در یک مدیریت‌کننده رمز عبور ممکن است به خاطر عدم وجود خطا در فناوری، قدیمی بوده و کهنه باشد. چنین مواردی می‌تواند ناشی از برگرداندن فایل‌های ایمیج از نسخه پشتیبان، برگرداندن نسخه‌های پشتیبان مجازی و یا حتی اجرای نمونه‌ای جدید یا سیستم مبتنی بر یک قالب پیش‌فرض باشد. در این موارد، مدیریت‌کننده رمز عبور Break Glass، رمزهای عبور مربوط به کاربر، سرویس یا حساب‌های داخلی را به‌صورت خودکار در تمام سازمان تغییر می‌دهد. درنتیجه هیچ‌کس رمز عبور صحیح را نمی‌داند و رمز عبور برای بازیابی دستی در جایی نوشته نمی‌شود. در زمان کارکرد عادی، مدیران رمز عبور، رمزهای عبور را به‌صورت تصادفی تغییر می‌دهند، سیستم‌های مدیریت‌شده را به‌روزرسانی می‌کنند و رمزهای عبور را ذخیره‌سازی کرده و مورد آزمایش قرار می‌دهند.

پس اگر این فرآیند با خطا مواجه شود چه اقدامی انجام می‌دهید؟ در اینجا پیشنهادهایی را ارائه می‌کنیم:

۱. اگر ابزار نمی‌تواند یک رمز عبور یا تعداد کمی از آن‌ها را تغییر دهد:

الف. قابلیت اتصال را اصلاح کنید و یا پیکربندی سیستم را به ابزاری جدید مجهز کنید تا تغییرات رمز عبور را بر اساس اهداف و به‌صورت منحصربه‌فرد انجام دهد؛
ب. رمز عبور را به‌صورت دستی با استفاده از حساب دیگری که حقوق ویژه دارد، تغییر دهید. اکثر ابزارهای مدیریت رمز عبور، حساب مختص خود را به‌منظور اجرای چنین وظایف عملیاتی دارند و معمولاً «حساب عملکردی[1]» نام دارند؛

۲. اگر ابزار نمی‌تواند هیچ رمز عبوری را تغییر دهد:

الف. قابلیت اتصال شبکه یا دسترسی به سیستم را اصلاح کنید؛
ب. مطمئن شوید که حساب عملکردی، حقوق ویژه مناسبی برای مدیریت از راه دور رمزهای عبور دارد.

۳. اگر رمز عبور یک حساب داخلی مشخص نیست:

[1] Functional Account

الف. رمز عبور حساب داخلی را با استفاده از حساب عملکردی به‌صورت تصادفی تعیین کنید؛
ب. سیستم را با استفاده از بوت[1] به حالت تک کاربره اصلاح کنید و رمز عبور را تغییر دهید.

۴. اگر رمز عبور یک حساب خدماتی مشخص نیست، یعنی آن سرویس دیگر نمی‌تواند آغاز به کار کند:

الف. رمز عبور سرویس را با استفاده از حساب عملکردی به‌صورت تصادفی تعیین کنید؛
ب. با استفاده از اعتبارنامه ذخیره‌شده، اتصالی را به سیستم ایجاد کنید و به‌صورت دستی رمز عبور حساب خدماتی را قبل از مدیریت‌کننده خودکار رمز عبور تنظیم کنید.

رمزهای عبور اپلیکیشن به اپلیکیشن

در چنین مواردی، مدیران یا توسعه‌دهندگان IT یک مدیریت‌کننده رمز عبور را برای جلوگیری از نوشتن رمزهای عبور در کد و درون فایل‌های پیکربندی، اسکریپت‌ها یا برنامه‌های کامپایل شده پیاده‌سازی می‌کنند. در عوض، اپلیکیشن، اسکریپت یا فایل پیکربندی از طریق یک رابط برنامه‌نویسی اپلیکیشن (API) به مدیریت‌کننده رمز عبور دسترسی پیدا می‌کند تا رمز عبور فعلی را که برای تکمیل عملیات پردازش نیاز دارند، به دست آورند. اپلیکیشن می‌تواند رمز عبور را برای استفاده پیوسته در حافظه پنهان ذخیره کند یا وقتی کار انجام شد آن را پاک کند. برای این کار، محیط باید امکان تغییر رمز عبور را هنگام اجرای اپلیکیشن بدهد. ادمین-های IT باید فرآیند تغییر و بازسازی رمزهای عبور در این چرخه را بدانند. در اینجا چند گام توصیه‌ای را بیان می‌کنیم:

۱. اگر وظایف خودکار با خطا مواجه شوند:

الف. راهکار مدیریت رمز عبور را اصلاح کنید؛
ب. مقاومت در برابر خطا را برای API فعال کنید؛

[1] Booting

ج. حافظه پنهان را به اسکریپت‌ها، فایل‌های پیکربندی یا اپلیکیشن‌ها اضافه کنید تا در برابر مشکلات شبکه‌ای، اتصالاتی و خطاهای مدیریت‌کننده‌های رمز عبور، مقاوم به خطا باشند؛

د. وظایف را به‌صورت دستی به‌روزرسانی کرده و دوباره ارسال کنید. مطمئن شوید که تمام وابستگی‌ها در نظر گرفته شده‌اند.

۲. اگر وظایف خودکار به کنترل تغییرات برای تغییر رمزهای عبور نیاز دارند:

الف. تغییرات رمز عبور را طی نگهداری ویندوز زمان‌بندی کنید؛

ب. برنامه‌هایی را توسعه دهید که در برابر خطا مقاوم هستند یا می‌توانند در صورت بروز هرگونه خطایی در API Query، به کار خود ادامه دهند.

فضای ذخیره‌ساز فیزیکی رمز عبور

برنامه‌های بازیابی شما باید شامل راهکار نهایی Break Glass نیز باشند تا بتوانند نسخه‌های فیزیکی رمزهای عبور را بازیابی کنند. ریسک‌های ذاتی در ذخیره‌سازهای فیزیکی رمز عبور ممتاز وجود دارند. به‌هرحال با کنترل‌های فیزیکی مناسب در جای خود به‌منظور ذخیره‌سازی امن اعتبارنامه‌ها، فضای ذخیره‌ساز فیزیکی می‌تواند به‌عنوان گزینه‌ای برای سناریوهای موارد اضطراری به کار برود. ملاحظات عبارت‌اند از:

- نسخه‌ای رونوشت از اعتبارنامه‌ها بگیرید و به‌صورت خودکار آن‌ها را در یک مکان امن چاپ کنید و یا آن‌ها را روی یک ابزار مورد اطمینان و قابل‌حمل ذخیره‌سازی نمایید. جدای از شکل کار که کاغذ باشد و یا از ابزارهای قابل‌حمل دیجیتال، مطمئن شوید که ذخیره‌ساز نهایی امنیت بالایی دارد؛
- اگر فرآیندهای شما این امکان را دارد، ابزار دیجیتال را قبل از نوشتن در یک درایو USB یا CD، با یک بسته رمزگذاری آفلاین رمزگذاری کنید. به یاد داشته باشید تا برای رمزگذاری آفلاین، در یک مکان امن نیز از رمز عبور پشتیبان بگیرید؛
- به‌طور کامل فرآیند ایجاد و ذخیره‌سازی رمزهای عبور Break Glass را مستند کنید. رمزهای عبور باید به‌طور مرتب تغییر یافته و دوباره ذخیره‌سازی شوند.

آگاهی از زمینه[1]

اعتبارنامه‌هایی که باید خارج از سازمان به آن‌ها دسترسی داشت، چالشی در رمزگذاری هستند و برای انجام آن باید زمینه را برای دسترسی فراهم کنید و تمام پارامترهای زمان اجرای درخواست باید برای ایجاد دسترسی مناسب مورد ارزیابی قرار گیرند. این کار باعث می‌شود تا ریسک نفوذ عامل تهدید خارجی که تلاش دارد این اعتبارنامه‌ها را هک کند، کاهش یابد.

- چه کسی سعی دارد وارد شود؟
- آن‌ها سعی دارند به چه سیستمی متصل شوند؟
- از کجا می‌خواهند وارد شوند؟
- در چه روزی از هفته هستیم؟
- در چه زمانی از روز قرار داریم؟

اعمال و فراهم کردن زمینه به شما این امکان را می‌دهد تا بهترین راهکارهای PAM را برای حفاظت بهتر از سازمان خود در برابر نفوذ به کار بگیرید. برای مثال، اگر حساب Break Glass شما تنها برای استفاده ضروری است، آن را تنها در ساعات خاصی در دسترس قرار دهید. اگر انتظار می‌رود که حساب باید توسط کارمندی در خانه و از راه دور در دسترس قرار گیرد، اطمینان حاصل کنید که اتصالات از طریق VPN صورت گیرد.

معماری

اگر هر مؤلفه یک فرآیند Break Glass یا سیستم مدیریت رمز عبور از دسترس خارج شود (فاجعه‌ای طبیعی یا خرابی)، چندین سطح از افزونگی[2] باعث می‌شود تا ریسک تلفات داده یا میزان در دسترس نبودن، کاهش یابد. معماری‌های اجرایی با دسترسی‌پذیری و انعطاف بالا تضمین می‌کنند که رمزهای عبور همیشه در دسترس هستند، حال چه همه رمزها تنها در یک مرکز داده وجود داشته باشد و یا در چندین مکان جغرافیایی و به‌صورت توزیع‌شده قرار گرفته باشد. این امر اولویت اول یک معماری و روش دفاعی مرسوم قبل از هرگونه استفاده از فرآیند Break Glass است. نسخه‌های فیزیکی اعتبارنامه‌ها نیز باید با در نظر گرفتن مکان‌های بازیابی فاجعه تهیه شوند.

[1] Context Aware
[2] Redundancy

و در آخر برای مواقع از دسترس خارج شدن کوتاه‌مدت زیرساخت‌های درون‌سازمانی، می‌توان رمزهای عبور را در محیط‌های ابری ذخیره‌سازی کرده و بازیابی نمود. این کار نیاز به پیکربندی اطلاعات دارد تا بتوان آن‌ها را در خارج از سازمان ذخیره یا تکثیر کرد و همچنین بایستی امن‌سازی‌های لازم در برابر تهدیدات خارجی صورت گیرد.

بازیابی Break Glass

بعد از رخداد مورد اضطراری برای بازیابی به عملکردهای طبیعی، باید رویدادهای امنیتی و عملیاتی را در نظر گرفت درحالی‌که ممکن است این مورد محرمانه به نظر برسد ولی هدف فرآیند Break Glass ارائه دسترسی در بدترین سناریوها است. اگر امر بازیابی به‌سرعت و بدون انجام بررسی، تأیید و کنترل تغییرات صورت گیرد، باید در نظر داشت که این کار می‌تواند فرآیند Break Glass را در حملات آینده به تهدیدی علیه سازمان تبدیل کند و یا به رویداد مشابه در آینده منجر خواهد شود؛ بنابراین موارد زیر را قبل از بازیابی سرویس‌های معمول در نظر بگیرید:

- چه رویدادی رخ داده که به فرآیند Break Glass نیاز داشته است؟
- می‌توان از این رویداد در آینده جلوگیری کرد؟
- آیا دسترسی به اعتبارنامه‌های Break Glass مناسب بود؟
- در کجای فرآیند Break Glass منابعی وجود دارد که پوشش داده نشده‌اند؟
- چه کسی از اجرای فرآیند Break Glass باخبر شده است؟
- آیا هیچ ریسک دیگری (از بین رفتن داده، نشر منابع و غیره) به‌وسیله فرآیند به وجود آمد؟

اگر بتوان به این سؤالات به‌صورت قانع‌کننده‌ای پاسخ داد، می‌توان سرویس‌ها را به عملکردهای عادی برگرداند. بعد از انجام این کار، جستارهای زیر را ادامه دهید:

- آیا فرآیند بازیابی خدمات درست بعد از رویداد مورد اضطراری بود؟ اگر این‌طور نیست، چطور می‌توان آن را بهبود بخشید و اصلاح کرد؟
- تمام اعتبارنامه‌های الکترونیکی و رمزهای عبور بعد از رویداد مورد اضطراری در چه قسمتی مجدد تنظیم می‌شوند؟

- آیا تمام فضای ذخیره‌سازی اعتبارنامه‌ها به حالت اولیه برگشتند و دستورالعمل‌ها برای فضای ذخیره‌سازی فیزیکی مجدد تنظیم شدند؟
- آیا تمام فعالیت نشست موارد اضطراری تأیید شده و برای فعالیت نامناسب حسابرسی شده‌اند؟

اگر سناریوهای Break Glass به‌صورت مرتب رخ دهند، در وهله اول کل فرآیند باید مورد ارزیابی قرار گیرد. این کار می‌تواند بررسی هر چیزی از سخت‌افزاری خراب و ناهنجاری‌های شبکه گرفته تا عدم دسترسی پرسنل کلیدی را در یک موقعیت حیاتی موردنیاز شامل شود. بازیابی سرویس‌های عادی باید همیشه شامل رویداد کلیدی Break Glass پس از رخداد باشد.

سناریوهای Break Glass را باید برای هر حساب ممتاز در نظر گرفت حتی اگر صاحب آن حساب فوت شده باشد. استفاده از فناوری به‌منظور پشتیبانی از خودش و دسترسی فیزیکی تضمین می‌کند که کنترل‌های پیشنهادی به مسئولیتی برای سازمان و یا شاه‌کلیدی برای عامل تهدید بدل نمی‌شوند.

فصل ۱۳

سیستم‌های کنترل صنعتی[1] (ICS)

سیستم‌های زیرساخت حیاتی که تأمین آب و انرژی، تولید، حمل‌ونقل و غیره را شامل می‌شوند، همگی برای نظارت و کنترل به سیستم‌های اطلاعاتی وابسته هستند. به‌طور مرسوم امنیت سیستم‌های کنترل صنعتی به‌شدت وابسته به ایزوله‌سازی شبکه است اما فرآیندهای مدیریتی، معیارهای کنترل هزینه و معماری سیستم‌های کنترل پیشرفته، منجر به افزایش یکپارچگی شبکه سازمان و محیط ICS شده است. با وجودی که این ارتباطات متقابل قابلیت کنترل، انعطاف‌پذیری و دید عملیاتی را افزایش می‌دهد ولی این کار می تواند ریسک‌هایی را که پیش‌تر در سیستم‌های کنترل صنعتی ایزوله‌شده امکان وقوع نداشتند، افزایش دهد. به‌هرحال در شبکه به‌هم‌متصل، سیستم کنترل صنعتی می‌تواند در معرض عاملان تهدیدی قرار گیرد که اینترنت و شبکه سازمان را اکسپلویت کرده و مورد نفوذ قرار می‌دهند و یا در معرض کارکنان داخلی که ممکن است از حقوق ویژه خود سوءاستفاده نمایند.

ICS-CERT (تیم پاسخ اضطراری سایبری سیستم‌های کنترل صنعتی[2]) هشدارهای ICS-CERT[3] را برای کمک به مالکان و اپراتورها جهت نظارت بر تهدیداتی ارائه کرده‌اند که می‌توانند سیستم‌های کنترل صنعتی را تحت تأثیر قرار دهند. برای حل این ریسک‌ها، ICS-CERT ما را تشویق می‌کند تا از راهکارهای امنیتی استفاده کنیم که از اصول دفاع در عمق[4]

---

[1] Industrial Control Systems

[2] Industrial Control Systems Cyber Emergency Response Team. (https://ics-cert.us-cert.gov/)

[3] (https://ics-cert.us-cert.gov/alerts)

[4] Defence-in-depth

استفاده می‌کند؛ دفاعی که شامل معیارهای دفاعی در عمق و حقوق ویژه مدیریتی جدول (۱-۱۳) است ولی تنها محدود به آن نیست.

جدول (۱۳-۱). ماتریس ریسک سیستم‌های کنترل صنعتی (ICS)

ریسک	توصیه ICS-CERT	مدیریت دسترسی‌های ممتاز (PAM)
رمزهای عبور امن	در هر جا که امکان دارد، حساب‌های سیستمی پیش‌فرض را حذف، غیرفعال و یا تغییر نام دهید.	پیاده‌سازی یک راهکار مدیریت رمز عبور سازمانی که از تغییر رمز عبور، مدیریت نشست فعال و مدیریت رمزهای عبور پشتیبانی می‌کند و ضبط نشست یک روش کارآمد برای حذف بسیاری از این چالش‌های معمول است.
مدیریت قدرتمند رمز عبور	ایجاد و پیاده‌سازی سیاست‌هایی که به استفاده از رمزهای عبور قدرتمند نیاز دارند.	پیاده‌سازی یک راهکار مدیریت نشست ممتاز و رمز عبور خودکار که کنترل دسترسی امن، حسابرسی، هشداردهی و ضبط را برای حساب ممتاز ارائه می‌کند.
کاهش ریسک‌های حملات جستجوی فراگیر	پیاده‌سازی سیاست‌های قفل کردن حساب برای کاهش ریسک تلاش‌های جستجوی فراگیر	PAM امنیت ICS و محیط‌های به‌هم‌متصل را قوی‌تر می‌کند: ۱. تضمین اینکه هیچ دستگاهی رمز عبور پیش‌فرض ندارد؛ ۲. تضمین اینکه هر دستگاه رمز عبور پیچیده و یکتا دارد؛ ۳. تغییر خودکار رمزهای عبور بر اساس عمر و مصرف آن‌ها؛ ۴. محدود کردن دسترسی و ارتباطات مدیریتی.
کمینه‌سازی میزان آشکار بودن شبکه	این اقدام شامل پیاده‌سازی دیوارهای آتش و تقسیم‌بندی شبکه است. این کار می‌تواند سطح حمله	پیاده‌سازی یک راهکار PAM که می‌تواند به‌صورت یک مدل کانتینر امن نیز اجرایی شود تا تضمین نماید تمام حساب‌های ممتاز (کارکنان، پیمانکاران و بخش‌های ثالث) دسترسی مستقیمی برای مدیریت این دستگاه‌ها ندارند. این مدل تضمین می‌نماید که تنها دستگاه‌های

	برای عاملان تهدید را کم و ریسک‌های اقدامات بعدی درون محیط آلوده را کم کند.	تأییدشده و مسیرهای شبکه محدودشده می‌توانند برای ارتباط با منابع امن مورد استفاده قرار گیرند که شامل کامپیوترهای HMI (رابط‌های انسان-ماشین[1]) سیستم کنترل می‌شود.
دسترسی امن از راه دور	این اقدام شامل اجرا و به‌روزرسانی مناسب راهکارهای دسترسی از راه دور مثل VPN، در صورت نیاز است.	ICS-CERT مشخص می‌کند که راهکارهای دسترسی از راه دور مثل یک VPN تنها به اندازه دستگاه‌های متصل امنیت دارد. راهکارهای PAM می‌توانند مثل جلیقه ضدگلوله‌ای برای زیرساخت دسترسی از راه دور شما و با کنترل کامل و دسترسی حسابرسی به حساب‌های ممتازی مثل حساب‌های مدیریتی مشترک، حساب‌های برنامه‌ها، حساب‌های مدیریتی محلی، حساب‌های خدماتی، حساب‌های پایگاه داده، حساب‌های ابری و رسانه اجتماعی، دستگاه‌ها و کلیدهای SSH را فراهم کنند.
شرکت‌های ثالث	نظارت بر ایجاد حساب‌های سطح مدیریتی به‌وسیله شرکت‌های ثالث	ایجاد مدیریت امن از راه دور: ۱. شرکت‌ها باید با استفاده از PAM و تجهیزات دسترسی از راه دور به منابع ICS دسترسی پیدا کنند؛ ۲. شرکت‌ها از طریق PAM احراز هویت می‌شوند و نشست به منابع مدیریت‌شده را درخواست می‌کنند که می‌تواند شامل یک سیستم دارای نرم‌افزار کنترلی ICS باشد. دقت شود که این نشست نه‌تنها می‌تواند به یک سیستم خاص محدود شود بلکه می‌تواند به یک اپلیکیشن سیستم کنترلی خاص نیز محدود گردد که کاهش بیشتری را در

[1] Human-Machine Interfaces

		ریسک‌های آلوده شدن و اقدامات بعدی داریم؛ ۳. شرکت از یک ابزار دسکتاپ بومی (ابزار MSTSC/PuTTY و غیره) یا یک نشست RDP/SSH استفاده می‌کند که از طریق PAM برای نظارت نشست پروکسی‌گذاری می‌شود؛ ۴. تمام فعالیت‌های شرکت ثبت شده و به‌صورت انتخابی برای تطابق با سیاست‌های امنیت و توافقی ضبط می‌شود.
مدیریت آسیب‌پذیری	اعمال وصله‌ها در محیط ICS در زمان ممکن برای کاهش آسیب‌پذیری‌های شناخته‌شده	فرآیند مدیریت آسیب‌پذیری می‌تواند به‌صورت کنش‌گرایی نقص‌های امنیتی را شناسایی کند، تأثیر کسب‌وکار را تحلیل نماید و برای انجام اصلاحات در زیرساخت شبکه، وب، موبایل، ابر، مجازی و IoT برنامه‌ریزی نماید: ۱. کشف زیرساخت شبکه، وب، موبایل، ابر، مجازی و IoT؛ ۲. پیکربندی نمایه دارایی‌ها و بررسی پتانسیل ریسک؛ ۳. مشخص کردن دقیق آسیب‌پذیری‌ها، بدافزارها و حملات؛ ۴. تحلیل پتانسیل تهدید، انجام اصلاحات و دیگر موارد؛ ۵. ایزوله‌سازی دارایی‌های با ریسک بالا از طریق تحلیل‌های پیشرفته تهدید؛ ۶. اصلاح آسیب‌پذیری‌ها شامل رمزهای عبور پیش‌فرض و ضعیف؛ ۷. گزارش آسیب‌پذیری‌ها؛ ۸. حفاظت از دستگاه‌های تأییدشده و تأییدنشده از حملات.

شناسایی تهدید	ICS-CERT توصیه می‌کند که سازمان‌ها فعالیت‌های مشکوک را نظارت کنند و یافته‌های خود را به ICS-CERT برای پشتیبانی پاسخ به حوادث و همبستگی با دیگر حوادث مشابه گزارش دهند.	تحلیل رفتار کاربر و ریسک‌های فناوری اطلاعات، متخصصان امنیت را قادر می‌سازد تا رخنه‌های احتمالی و علت رخدادها را شناسایی کنند. مدیریت رویدادهای امنیت اطلاعاتی (SIEM) و راهکارهای تحلیل تهدید می‌توانند مبناهایی را برای رفتار عادی تعیین کنند، تغییرات را مشاهده نمایند و از طریق گام‌های زیر، ناهنجاری‌ها را شناسایی کنند: ۱. داده‌های کاربران و دارایی‌ها را جمع‌آوری کنند تا به‌صورت متمرکز درآورند و رفتارها را ردیابی نمایند؛ ۲. دارایی‌ها، کاربران و فعالیت‌های متنوع تهدید را به‌منظور آشکارسازی ریسک‌های حیاتی با هم همبسته نمایند؛ ۳. رفتارهای عادی در تغییرات دارایی‌ها و کاربران را تبیین کنند تا تهدیدات پیش رو را مشخص نمایند؛ ۴. کاربران و دارایی‌هایی را که رفتارهای انحرافی نشان می‌دهند، ایزوله نمایند؛ ۵. گزارش‌هایی را برای اطلاع‌رسانی و یکپارچه‌سازی تصمیمات امنیتی تولید نمایند. هر شناسایی تهدیدی که به‌وسیله یک سازمان اجرا شده است باید تمام داده‌های امنیتی موجود را در نظر بگیرد و نتایج را همبسته نماید. شناسایی تهدید نباید تنها روی رویداد و مبدأ آن متکی باشد.

درحالی‌که ICS یک هدف خاصی را به‌وسیله فناوری PAM بیان می‌کند ولی مزایای آن برای هر نوع پیاده‌سازی کاملاً مشخص است:

- کشف تمام دستگاه‌های مدیریت‌شده و مدیریت‌نشده در سازمان و زیرساخت‌های یکپارچه ICS شما؛
- کشف خودکار و فهرست نمودن حساب‌های ممتاز موجود تحت استفاده شرکت‌های ثالث؛
- ارائه کنترل مرکزی به‌وسیله ذخیره‌سازی امن رمزهای عبور و کلیدهای SSH در یک پایگاه داده امن؛
- کاهش ریسک اعتبارنامه‌های گم‌شده یا دزدیده‌شده شرکت به‌وسیله تغییر سیستماتیک رمزهای عبور برای تمام سیستم‌های مدیریت‌شده؛
- پیاده‌سازی کانتینرهای[1] امن شرکت به‌منظور ایزوله نمودن ICS و دستگاه‌ها برای کاهش ریسک‌های بدافزارها و حملات؛
- ارائه تأییدیه‌ای که هیچ رمز عبور پیش‌فرضی روی هیچ یک از سیستم‌ها یا دستگاه‌های مدیریت‌شده وجود ندارد؛
- تغییر خودکار رمز عبور هر دستگاه بر اساس عمر یا بعد از هر بار برقرار شدن نشست از راه دور از بیرون سازمان؛
- ارائه گردش کار کاملی برای دسترسی به دستگاه‌ها شامل یک فرآیند تأیید برای زمانی که نیاز به دسترسی از راه دور در آن شرکت وجود دارد؛
- ثبت تمام نشست‌ها یا فقط نشست‌های انتخاب‌شده از راه دور با قابلیت playback آن‌ها به‌منظور مستندسازی و بازبینی اتفاقاتی که هنگام دسترسی به دستگاه رخ داده است؛
- ارائه گزارش دقیق از تمام اعتبارنامه‌های مورد استفاده و درخواست‌شده در زمانی که فعالیتی از راه دور رخ داده است.

[1] Containers

فصل ۱۴

اینترنت اشیاء (IoT)

اینترنت اشیاء مجموعه‌ای منحصربه‌فرد از تهدیدات مبتنی بر حقوق ویژه و اهداف حمله را برای عامل تهدید معرفی می‌کند. بنا به تعریف، این تجهیزات، دستگاه‌های تک منظوره‌ای با سیستم‌عامل‌های تعبیه‌شده جهت اجرای عملکردهای خاص هستند که ویژگی‌های آن‌ها محدود بوده و قابلیت شبکه شدن را دارا هستند. این دستگاه‌ها شامل هر چیزی از دوربین‌های مبتنی بر شبکه و ضبط‌کننده‌های دیجیتالی ویدیو گرفته تا دستیاران شخصی دیجیتال را شامل می‌شود. همچنین آن‌ها را می‌توان برای استفاده تجاری مانند قفل‌های زیست‌سنج درب‌ها تا کاربردهای خانگی مانند ترموستات‌ها به کار برد. درحالی‌که این نوع از دستگاه‌ها، سالیان زیادی است که وجود دارند ولی اخیراً از آن‌ها استفاده گسترده‌تری می‌شود و مهم‌تر اینکه از آن‌ها به‌عنوان ریسک‌های امنیتی و اهداف حمله دارای حقوق ویژه استفاده می‌شود؛ بنابراین هرچه دستگاه‌های اینترنت اشیاء متداول‌تر شوند، نیاز به تضمین این امر داریم که آن‌ها برای عملکردهای سازمان ریسک امنیتی را ایجاد نمی‌کنند. متأسفانه اثبات شده است که بسیاری از این دستگاه‌ها امنیت لازم را در طراحی نداشته و نقص‌های برطرف‌نشده‌ای درون خود دارند که می‌توان از آن‌ها برای هک کردن سازمان با چیزی به‌سادگی اعتبارنامه‌ای پیش‌فرض استفاده نمود. این امر فرصتی طلایی برای عامل تهدید است. برای هر طرح اجرایی اینترنت اشیاء باید این پنج توصیه را در نظر بگیرید تا ریسک‌های امنیتی را کاهش دهید و تهدیدات با اهداف حقوق ویژه را از اطلاعات حساس سازمان دور نگه دارید:

۱. شبکه‌ها را تقسیم‌بندی کنید.

با استفاده کردن از قابلیت‌های پایه در مسیریاب‌های مدرن شبکه و سوئیچ‌ها، تمام دستگاه‌های اینترنت اشیاء باید با استفاده از شبکه‌های بی‌سیم و شبکه‌های VLAN جدا، شبکه شوند. همیشه باید تمام ارتباطات از شبکه‌های اینترنت اشیاء به سرورهای حیاتی، پایگاه‌های داده و مکان‌هایی که نباید به‌صورت مستقیم با این دستگاه‌ها ارتباط داشته باشند، مسدود شوند. این کار کمک می‌کند تا تضمین نماییم که آیا دستگاه اینترنت اشیاء هک شده است یا نه و نمی‌توان از آن به‌طور مستقیم برای دزدیدن اطلاعات حیاتی بهره برد. در صورت امکان باید تمام ارتباطات شبکه اینترنت اشیاء به اینترنت و دیگر شبکه‌های مورد اطمینان را مورد نظارت قرار داد تا هرگونه رفتار ناهنجار را شناسایی کرد.

۲. تمام رمزهای عبور را تغییر دهید.

تقریباً تمام دستگاه‌های اینترنت اشیاء به‌منظور پیکربندی اولیه، با رمزهای عبور پیش‌فرض فروخته می‌شوند. در فصل‌های قبل بدین مسئله اشاره کردیم که این امر چقدر می‌تواند خطرناک باشد. کاربران نهایی باید تمام نام‌های کاربری و رمزهای عبور روی این دستگاه‌ها را به رمزهای عبور پیچیده و نام‌های کاربری خاص و یکتایی تغییر دهند و تغییر رمزهای عبور در دوره‌های زمانی متناوب را مدنظر قرار دهند. در اینجا راهکار مدیریت رمز عبور می‌تواند در کاهش هرگونه تهدیدی کمک کند و رمزهای عبور را بر روی هر دستگاهی منحصربه‌فرد نگه دارد تا مانع از استفاده دوباره رمز عبور شود.

۳. به‌روزرسانی ثابت‌افزار[1]

مطمئن شوید که از آخرین نسخه ثابت‌افزار و وصله‌های امنیتی بر روی دستگاه‌های اینترنت اشیاء خود استفاده می‌کنید تا هرگونه تهدید در حال ظهور و آسیب‌پذیری‌های شناسایی-شده‌ای را که می‌توانند علیه دستگاه‌ها مورد استفاده قرار گیرند، از بین ببرید.

۴. دستگاه‌های IOT را مستقیماً به اینترنت متصل نکنید.

هرگز دستگاه‌های اینترنت اشیاء را به‌صورت مستقیم و با آدرس‌های IP عمومی به اینترنت متصل نکنید چراکه حتماً در آینده هک خواهند شد و یا در معرض حملات DDOS قرار می‌گیرند. دستگاه‌های اینترنت اشیاء مبتنی بر فناوری‌های شبکه‌ای ساده‌ای هستند و به اندازه

[1] Firmware

کافی مقاوم نیستند تا تمام ترافیک احتمالی IP را که شامل کدهای مخرب در شبکه است، خنثی سازند.

۵. با کاوش کردن مانع از فعالیت فناوری‌های تأییدنشده در قسمت Shadow IT شوید.

Shadow IT ، واژه دیگری برای دستگاه‌های جعلی و دارایی‌های بدون ضمانت معین است. اطمینان حاصل کنید که تمام دستگاه‌های IoT موجود در شبکه شما تأییدشده باشند و گام‌های بالا را دنبال کنند. Shadow IT مبتنی بر اینترنت اشیاء می‌تواند به‌سادگی بسیاری از سیاست‌های امنیتی شما را نقض کند و برای شما یک تهدید امنیتی تلقی شود. ابزارهای استاندارد کاوش شبکه می‌توانند این دستگاه‌های سرخود را بیابند و کمک کنند تا آن‌ها را تحت مدیریتی مناسب قرار دهید. برای هر سازمانی که قصد دارد از دستگاه‌های اینترنت اشیاء در شبکه سازمانی استفاده کند، نکاتی وجود دارد که با رعایت نمودن آن‌ها می‌توان امنیت را تضمین کرد. سعی کنید این موارد را در سیاست‌های امنیتی سازمان خود به کار گیرید.

۱- توافق‌نامه سطح خدمات برای آسیب‌پذیری را تقاضا کنید

از تولیدکننده بخواهید تا توافق‌نامه سطح خدمات را برای وصله کردن آسیب‌پذیری‌های حیاتی در هنگام شناسایی آن‌ها ارائه کند. این کار به شما کمک می‌کند تا تضمین نمایید که دستگاه‌های اینترنت اشیاء انتخابی در سازمان مطابق با آخرین تنظیمات و تغییرات به‌روزرسانی امنیتی می‌شوند. به‌علاوه، اطمینان حاصل کنید که این سؤالات در هنگام RFP یا فرآیند خرید، درخواست شده باشد تا تضمین نمایید فروشنده از بلوغ کافی برای مدیریت ریسک‌ها برخوردار است.

۲- بر اساس زمان‌بندی منظم به‌روزرسانی‌های امنیتی را انجام دهید

فرآیند را مستند کنید و تضمین نمایید تمام دستگاه‌های اینترنت اشیاء می‌توانند در صورت یافتن نقص و بدون اختلالی گسترده به سازمان، وصله شوند.

۳- دسترسی مبتنی بر نقش را اجرا کنید

هر مدل امنیتی ارائه‌شده در این دستگاه‌ها به اندازه کافی انعطاف‌پذیر است تا درون یک دایرکتوری سرویس یا یک سرور رادیوس (RADIUS) یکپارچه شود. به‌عنوان هدفی بلندمدت، تمام دسترسی‌های اختصاص‌یافته به این دستگاه‌ها بایست به‌صورت متمرکز مدیریت شده و

به‌طور مناسبی درون راهکارهای مدیریت هویت و دسترسی (IAM) موجود سازماندهی شوند. اگر به هر دلیلی نتوان این اقدامات را انجام داد، ممکن است این کارها ریسک جدیدی که نشئت‌گرفته از حساب‌های آزاد است، ارائه کند و هدفی ساده برای عامل تهدید باشد. درنهایت اگر دستگاه‌های مدیریت‌شده، هیچ مدل مبتنی بر نقشی نداشته باشند و یا مدیریت آن‌ها بر حسب شرایط موجود به دلایل امنیتی شدنی نباشد، راهکار حداقل حقوق ویژه را برای اینترنت اشیاء و دستگاه‌های شبکه به‌عنوان راهکاری جایگزین مدنظر قرار دهید. دستگاه‌های اینترنت اشیاء تنها بخش دیگری از فناوری هستند که منابعی راحت و یکپارچه را برای سازمان‌ها ممکن می‌سازند. آن‌ها در مقایسه با سرورها و یا دسکتاپ‌ها بالغ نیستند و همه‌چیز از اعتبارنامه‌های پیش‌فرض تا درب‌های پشتی، ریسک حقوق ویژه‌ای را برای یک سازمان به دنبال دارند. هرچه که تجهیزات IoT از بلوغ کمتری برخوردار باشند، باید دقت بیشتری در مورد آن‌ها به خرج داد. این تجهیزات به کنترل، اعمال محدودیت و نظارت بیشتری نیاز دارند.

فصل ۱۵

فضای ابری

تاریخچه رمزهای عبور به دوران ارتش روم باز می‌گردد. آن‌ها اطلاعاتی را روی چوب‌ها حک می‌کردند و از سربازانی با گاردهای ویژه محافظتی برای جابجایی آن‌ها استفاده می‌نمودند. این اسرار هک‌شده بر روی چوب‌ها، منابعی مشترک بودند. امروزه متداول‌ترین فضای ذخیره‌سازی رمز عبور مغز افراد است و بدین‌صورت به شکل فیزیکی مستند نشده و به اشتراک گذاشته نمی‌شود. ما رمز عبور را به یک سیستم یا برنامه تخصیص می‌دهیم، در هنگام لزوم آن را به یاد می‌آوریم و هر زمانی که آن را تغییر دادیم دوباره آن را به خاطر می‌سپاریم. مغز ما پر از رمزهای عبوری است که اغلب آن‌ها را فراموش می‌کنیم و در صورت نیاز برای اشتراک‌گذاری باید آن‌ها را ناچاراً روی یک برگه یادداشت و یا در فایلی درون کامپیوتر ذخیره کنیم و یا حتی ممکن است آن‌ها را با ایمیل ارسال نماییم (که خود این امر راهکار بسیار ضعیفی است). این روش‌های ناامن اشتراک‌گذاری رمزهای عبور سبب شده است که اغلب خبرگذاری‌ها در صفحه اول خود اخبار نشر داده‌های حساس سازمان‌های مختلف را قرار دهند. نمی‌توان از انسان‌ها انتظار داشت که هر وقت نیاز شد، رمزهای عبور را به‌صورت شفاهی یا نوشتاری به اشتراک بگذارند، باید در نظر داشت حتی ارسال رمزها با استفاده از ایمیل یا پیامک به یک همکار معتبر نیز امن نیست؛ بنابراین به روشی بهتر برای مستندسازی رمزهای عبور نیاز است که بسیار امن باشد، مستندات با دسترسی توزیع‌شده باشد و اشتراک‌گذاری و همکاری با کمترین ریسک انجام گیرد و مهم نباشد که دسترسی در کجا و به واسطه چه ابزاری صورت می‌گیرد. فضای ابری برای چنین موقعیتی که رمزهای عبور باید در بیرون سازمان در دسترس باشند و

یا به اشتراک گذاشته شوند (که البته این امر ترجیح داده نمی‌شود) ایده‌آل هستند و فناوری-های درون محیط سازمان در تحقق این الزامات ناتوان هستند.

متخصصین فناوری، فضای ابری را به دلیل ویژگی‌های زیادی که برای اشتراک‌گذاری، ذخیره‌سازی و امن‌سازی اطلاعات در بیرون از سازمان دارد، برای این کار انتخاب کرده‌اند. بسته به حساسیت اطلاعات، به گام‌های بیشتری برای تضمین امنیت اطلاعات در برابر روش‌های جدید حملات نیاز است. برای مدیریت دسترسی‌های ممتاز و ذخیره‌سازی رمز عبور در ابر، کاربردهای اصلی زیادی برای استقرارهای مبتنی بر ابر وجود دارند:

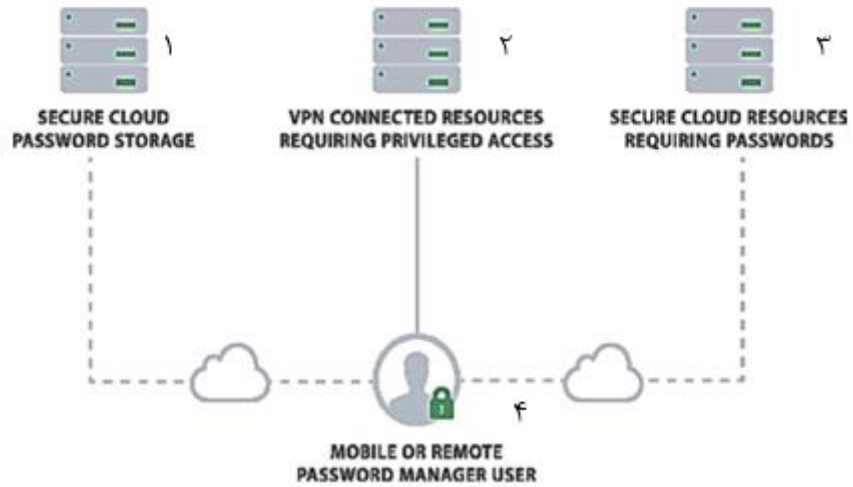
- نیروی کار سیار: توانایی اعضای تیم از راه دور برای دسترسی به رمزهای عبور فعلی و دریافت کردن سیاست‌ها و قوانین؛
- پشتیبانی IT توزیع‌شده یا برون‌سپاری: توانایی اعضاء تیم IT برون‌سپاری شده، پیمانکار یا تیم از راه دور برای دسترسی به اعتبارنامه‌ها و آغاز نشست‌هایی با استفاده از روش‌های context-aware برای منابعی که در قبال آن مسئول هستند؛
- همکاری IT: اعضاء تیم معمولاً باید رمزهای عبور را برای دارایی‌ها و برنامه‌ها جهت انجام وظایف و نگهداری، به اشتراک بگذارند. یک مرکز ذخیره‌سازی رمز عبور برای ذخیره کردن کلمه‌های عبور، امکان همکاری و مشارکت را بدون ریسک ذخیره‌سازی رمزهای اشتباه یا جعلی در مستندات قابل‌دسترسی فراهم می‌کند؛
- Break Glass: ذخیره‌سازی مستقل از فناوری رمزهای عبور برای سیستم‌ها و برنامه-های کلیدی در صورت بحران یا رخدادهای اضطراری است؛
- مدل‌های ابری: مسئولیت‌های سازمانی برای امن‌سازی اعتبارنامه‌های ابری بسته به مدل‌های ابری انتخاب‌شده (SaaS، Pass یا SaaS) تغییر می‌کند.

نیروی کار سیار

سازمان‌های زیادی هستند که امروزه درصدی از نیروی کار آن‌ها با استفاده از موبایل یا از راه دور کار می‌کنند. این نیروی کار می‌تواند از بخش فروش، پشتیبانی، مدیران اجرایی و غیره گرفته تا بخش توسعه را شامل شوند. این نیروهای کار از راه دور از طریق فناوری‌های مختلف، منابع را با کارکنان حضوری سازمان با استفاده از شبکه‌های خصوصی مجازی (VPN) یا خدمات ابری به اشتراک می‌گذارند. برای برخی از آن‌ها، نیاز به دسترسی به سیستم‌هایی وجود

دارد که اعتبارنامه‌های اشتراکی یا منحصربه‌فرد دارند و به سبب حساسیتی که دارند نباید آن‌ها را با ایمیل یا هیچ ابزار دیگری مستند نمود. در اینجاست که استفاده از ابر برای ذخیره‌سازی رمزهای عبور می‌تواند به سبب دسترسی سراسری که ایجاد می‌کند به امنیت و بهره‌وری کمک نماید.

در شکل (۱۵-۱)، یک کاربر مطمئن (یک فرد) به فضای ذخیره‌سازی ابری دسترسی می‌یابد تا رمز عبوری را بدون توجه به موقعیت و قابلیت اتصال خود بازیابی نماید. سپس از طریق VPN متصل شده و به دیگر منابع ابری دسترسی یابد یا حتی سیستم خودش در سازمان را مدیریت کند. باید توجه داشت هرگز نباید این رمزهای عبور مورد سرقت قرار گیرند و باید سیاست‌هایی را برای تغییر رمز عبور و پیچیدگی آن‌ها دنبال کرد. راهکارهای مدیریت خودکار رمز عبور می‌توانند برای دسترسی به این الزامات کمک‌کننده باشند.



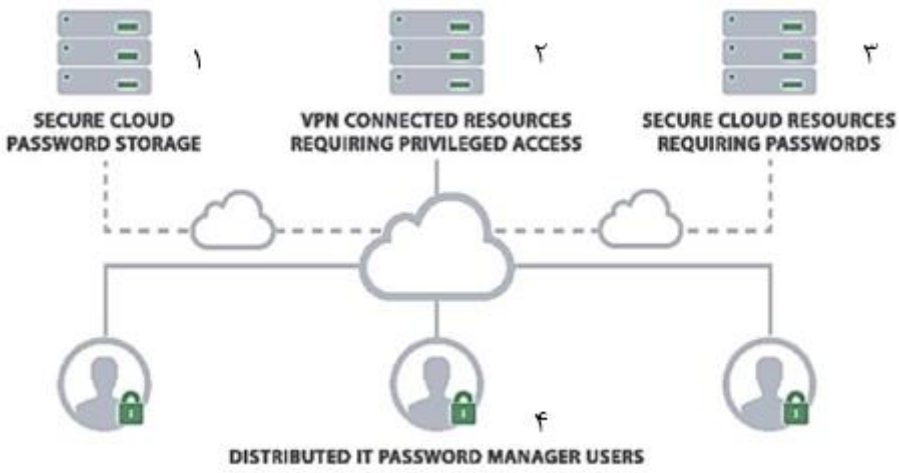
شکل (۱۵-۱). دسترسی موبایل تک کاربره به مدیریت‌کننده رمز عبور

۱. فضای ذخیره‌ساز ابری امن رمز عبور؛
۲. منابع متصل با VPN که به دسترسی ممتاز نیاز دارند؛
۳. منابع ابری امنی که به رمزهای عبور نیاز دارند؛
۴. موبایل یا کاربر مدیریت‌کننده رمز عبور از راه دور.

فناوری اطلاعات توزیع‌شده

سازمان‌ها برای مدیریت سیستم‌ها، برنامه‌ها و فناوری‌های مختلف به متخصصان فراوانی ازجمله پیمانکاران و کارکنان از راه دور گرفته تا فروشنده‌ها نیاز دارند. آن‌ها به فناوری‌هایی دسترسی دارند که امکان پشتیبانی از سازمان را از مکان‌ها و ناحیه‌های زمانی مختلف و انواع دستگاه‌ها فراهم می‌کند. وقتی امکان پیاده‌سازی مدیریت خودکار رمز عبور وجود نداشته باشد، ذخیره کردن امن آخرین رمزهای عبور در فضای ابری باعث ایجاد سازمانی فنی می‌گردد که دسترسی به سیستم‌های موردنیاز و تکمیل کارهایشان را دارند.

در شکل (۱۵-۲)، منابع از راه دور به روش‌های مختلفی (VPN، تبلت‌ها، تلفن‌های سلولی و غیره) به فضای ابری متصل شده‌اند. آن‌ها بر اساس وظیفه‌ای که دارند، رمز عبور را به دست آورده و برای تکمیل مأموریت خود به منبعی متصل می‌شوند. تغییر مرتب این رمزهای عبور بر عهده بخش‌های فناوری اطلاعات و مرکز امنیت سازمان است و آن‌ها را ترغیب می‌کند که این شکل از همکاری در مقیاس‌های محدودی مورد استفاده قرار گیرد. برای تعداد زیادی از کاربران، با دسترسی‌های مکرر و داشتن سیستم‌های مدیریت‌شده نیز می‌توان همچنان از این الگو بهره برد اما تغییر رمز عبور و همگام بودن با فضای ابری باید به‌صورت خودکار انجام شود.



شکل (۱۵-۲). دسترسی توزیع‌شده IT به مدیریت‌کننده‌های رمز عبور

۱. فضای ذخیره‌ساز ابری امن رمز عبور؛
۲. منابع متصل با VPN که به دسترسی ممتاز نیاز دارند؛

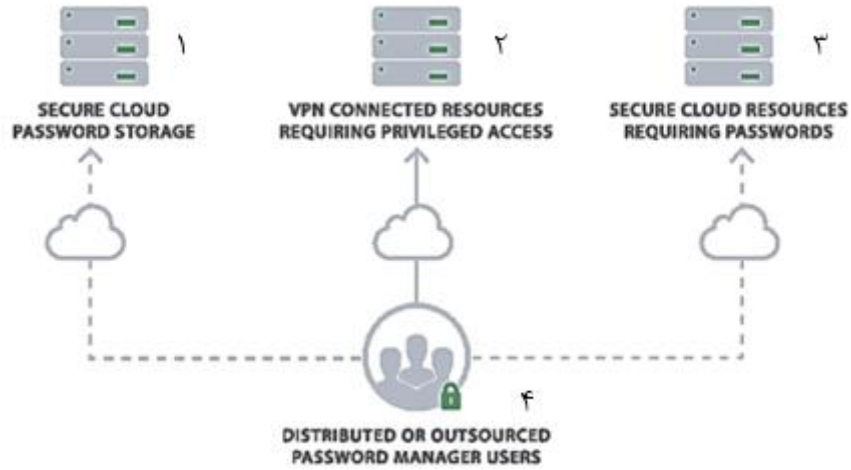
۳. منابع ابری امنی که به رمزهای عبور نیاز دارند؛
۴. کاربران مدیریت‌کننده رمز عبور توزیع شده.

همکاری فناوری اطلاعات

فناوری‌های جدید برای آماده‌سازی، پیکربندی و نگهداری معمولاً به همکاری بین تیم‌های IT نیاز دارند. یک حساب که از حقوق ویژه استفاده می‌کند در برابر حسابی دیگر باید داده‌های ثبتی و تنظیمات مشابهی را نشان دهد اما برای مؤلفه‌های مختلف از وب‌سرور و میان‌افزار[1] گرفته تا پایگاه داده به حساب‌های مختلفی نیاز است. برای همکاری موفقیت‌آمیز تیم‌ها، گاهاً برای عملکرد یک فناوری و اجرای تعمیرات و نگهداری به دسترسی از جنبه دیگری نیاز داریم.

در شکل (۱۵-۳) تیم‌های فناوری اطلاعات با هم همکاری می کنند و برای انجام وظایف، اجازه دسترسی به رمزهای عبور به دیگر تیم‌ها داده شده است. رمزهای عبور در مدیریت‌کننده رمز عبور مبتنی بر فضای ابری ذخیره می‌شوند و تمام اعضاء تیم برای به دست آوردن اعتبارنامه‌هایی که برای انجام مأموریت خود بدان نیاز دارند، مورد اعتماد هستند. درحالی‌که این دسترسی به تیم‌ها اجازه می‌دهد تا از حقوق ویژه مرتبط با دیگر نقش‌ها استفاده نمایند ولی سازمان باید این ریسک را بپذیرد و تمام دسترسی‌های بعدی را مورد نظارت قرار دهد. به‌علاوه، مدیریت خودکار رمز عبور و ضبط نشست می‌تواند دسترسی بعدی را مستند سازد اما به‌جای اینکه از این فناوری‌ها استفاده شود، باید از بهترین راهکارها برای پیچیدگی و تغییر رمز عبور استفاده شود. در آخر، فهرست کاربران مورد اعتماد باید به‌منظور حفظ تفکیک وظایف و ناچاراً ریسک اشتراک رمزهای عبور (که البته هرگز توصیه نمی‌شود اما در واقعیت همچنان اتفاق می‌افتد) محدود گردد.

[1] Middleware

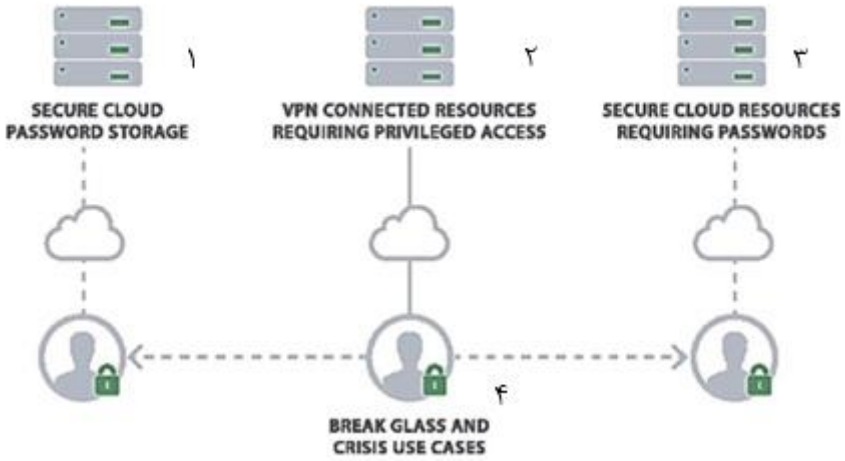


شکل (۱۵-۳). همکاری با استفاده از یک مدیریت‌کننده رمز عبور

۱. فضای ذخیره‌ساز ابری امن رمز عبور؛
۲. منابع متصل با VPN که به دسترسی ممتاز نیاز دارند؛
۳. منابع ابری امنی که به رمزهای عبور نیاز دارند؛
۴. کاربران توزیع‌شده یا برون‌سپاری شده مدیریت‌کننده رمز عبور.

Break Glass

در مواقع بحرانی، دسترسی به سیستم‌ها برای نگهداری، ارتقاء و یا به دلیل یک رویداد امنیتی می‌تواند بین خروج از دسترسی طولانی‌مدت و نشر داده‌ها تعیین‌کننده باشد. رمزهای عبور حیاتی ممکن است به خاطر در دسترس نبودن کارمند و به دلیل قفل شدن حساب کاربری او در دسترس نباشد. به‌طور معمول، سازمان‌ها کاربردهای Break Glass را به‌وسیله مستندسازی رمزهای عبور ضروری بر روی کاغذ، ذخیره‌سازی در جایی امن و یا قرار دادن آن روی ابزاری ایمن که قابل حمل بوده و با قابلیت قفل شدن اجرا می‌کردند. در سناریوهای Break Glass، فرض بر این است که شخصی به فضای فیزیکی امن و یا رمز عبور برای رمزگشایی فایل‌های امن دسترسی دارد. ذخیره‌سازی این رمزهای عبور ضروری و حیاتی بر روی ابر کار را ساده‌تر کرده و می‌تواند خطراتی ازجمله بلایای طبیعی را نیز مدیریت نماید.



شکل (۱۵-۴). Break Glass و مدیریت‌کننده رمز عبور مبتنی بر فضای ابری

۱. فضای ذخیره‌ساز ابری امن رمز عبور؛
۲. منابع متصل با VPN که به دسترسی ممتاز نیاز دارند؛
۳. منابع ابری امنی که به رمزهای عبور نیاز دارند؛
۴. کاربردهای Break Glass و مواقع بحرانی.

در شکل (۱۵-۴)، کارمندان فناوری اطلاعاتی که به دسترسی مدیریت‌کننده رمز عبور مبتنی بر ابر اعتماد کرده‌اند و می‌تواند رمزهای عبور Break Glass را بازیابی نماید، در صورت نیاز آن‌ها را دوباره توزیع کند و از طریق هر واسطه‌ای که برای تکمیل وظیفه‌ای نیاز است، به منابع کلیدی دسترسی یابند. بعد از هر بار استفاده از Break Glass، تمام رمزهای عبور مورد دسترسی باید دوباره تنظیم گردیده و به مدیریت کننده رمز عبور ارسال شوند. راهکارهای خودکار می‌توانند این کار را به‌صورت خودکار و بر اساس زمان‌بندی تعریف‌شده انجام دهند تا مصرف درست از آن‌ها و امنیتش را تضمین نمایند. برای جزئیات بیشتر درباره مدیریت دسترسی‌های ممتاز و سناریوهای Break Glass می‌توانید به فصل ۱۲ مراجعه کنید که به این موضوع می‌پردازد.

لازم است تا یادآور شویم، هر زمانی که اطلاعات حساسی در فضای ابری ذخیره می‌شود، امنیت این اطلاعات و اپلیکیشن میزبان به مسئله مهمی در تبادل نظرهای امنیتی تبدیل می‌شود. اگر رخنه‌ای برای یک حساب منحصربه‌فرد و یا برای کل سیستم رخ دهد، نتایج

احتمالی آن می‌تواند ویرانگر باشد. تیم‌ها و عملیات امنیتی در هنگام بررسی فضای ابری به‌عنوان بستر مدیریت دسترسی‌های ممتاز باید همیشه تهدیدات، سطح ریسک، نشر و اطلاعات شخصی قابل‌شناسایی و ذخیره‌شده را ارزیابی نمایند تا تعیین کنند مزایای آن بیشتر از ریسک باشد. بر اساس این اطلاعات، انتخاب پلتفرم ابری مناسب برای مدیریت دسترسی ممتاز، گام منطقی بعدی در این روند است.

مدل‌های فضای ابری

رشد استفاده از محیط‌های ابری برای پردازش، ذخیره‌سازی و یا میزبانی و توسعه اپلیکیشن، راه‌های جدیدی را برای هکرها و یا افراد درون‌سازمانی بداندیش باز کرده است تا به‌صورت نامناسبی به داده‌های حساس دسترسی پیدا کنند و سازمان‌ها را مختل نمایند. با ادامه رشد پرشتاب فضای ابری، سازمان‌ها باید دسترسی به این محیط‌ها را امن‌سازی نمایند تا ریسک‌های امنیتی آن‌ها را کاهش داده و درعین‌حال هزینه و بازدهی میزبانی از برنامه‌ها و سرویس‌های بیشتر را در ابر محقق نمایند.

مانند هر دارایی دیگر درون‌سازمانی، محیط‌های ابری مدیریت‌نشده نیز می‌توانند شکاف امنیتی قابل‌توجهی را ایجاد کنند که می‌تواند شبکه‌ها را با رخنه‌های امنیتی، از دست رفتن داده، سرقت مالکیت معنوی و معضلات سازگاری با قوانین مواجه کند. اولین گام برای کنترل دارایی‌های ابری، یافتن و تهیه فهرستی است که می‌تواند به تمام خدمات ابری بسط پیدا کند.

مدل‌های اجرایی مبتنی بر ابر برای مدیریت دسترسی‌های ممتاز می‌تواند به اشکال مختلف باشد:

- مدل ابر به ابر برای مدیریت حقوق ویژه شامل اپلیکیشن به اپلیکیشن (IaaS)؛
- ذخیره‌سازی و مدیریت حقوق ویژه مبتنی بر ابر برای کاربران (SaaS)؛
- پلتفرم مبتنی بر ابر به‌عنوان سرویسی برای اجرای راهکار مخصوص خودتان (PaaS)؛
- مدیریت حقوق ویژه برای منابع درون‌سازمانی (هیبرید).

اگر این موضوع، سؤالی بود که امکان انتخاب چندین گزینه را داشت، احتمالاً ابتکارات استراتژیک سازمان شما به بیش از یکی از این طبقه‌بندی‌ها نیاز داشت. بسیار غیرمعمول است که PAM تنها در یک قسمت از سازمان و بدون بهره بردن از برنامه‌هایی جهت گسترش

فناوری به تمام سیستم‌های حساس و حساب‌های ممتاز، استفاده شود. درحالی‌که ممکن است مدل‌های اجرایی اولیه با بخش کوچکی شروع شود ولی فضای ابری باید برای همه جا استفاده شود. در هنگام انتخاب PAM، درون‌محیطی بودن، فضای ابری و یا رویکرد هیبرید برای ما مهم خواهد شد. برای رویکردهای هیبرید می‌تواند ترکیبی از IaaS، SaaS و یا درون‌محیطی و یا ترکیبی باشد که از گره‌های مدیریتی از راه دور برای مسیریابی و تجمیع داده‌ها به‌صورت امن استفاده می‌کند.

زیرساخت به‌عنوان سرویس (IaaS)

زیرساخت به‌عنوان سرویس (IaaS) به تحویل ظرفیت رایانشی و زیرساختی به‌عنوان سرویس اشاره دارد. در این مدل، شرکتی دیگر زیرساخت‌های مرکز داده و سخت‌افزاری را فراهم می‌کند و به مشتری‌ها اجازه می‌دهد تا از زیرساخت‌ها و سخت افزارها استفاده کنند. مثال‌هایی از زیرساخت‌های IaaS شامل آمازون AWS، مایکروسافت آزور و پلتفرم ابری گوگل است. هر یک از این پلتفرم‌ها، مدل مجوزهای خود را برای ارائه دسترسی منتخب به کاربران و گروه‌ها دارند. این مجوزها معمولاً در نقش‌های از قبل ساخته‌شده و یا سفارشی تعریف‌شده‌ای با هم پیوند می‌خورند که دسترسی لازم را فراهم می‌کنند. با قابلیت‌ها و تأثیرات کسب‌وکاری که این امر دارد، اگر این حساب‌ها آلوده شوند، امنیت و کنترل مناسب این دارایی‌ها جزء اولویت-دارترین مواردی است که باید درون برنامه امنیتی چندلایه‌ای سازمان، ازجمله در لایه دسترسی ممتاز در نظر گرفت.

چه سازمان شما بخواهد درون یک ارائه‌دهنده فضای ابری کار کند و یا چندین شرکت را انتخاب نماید و یا بر اساس مقررات و یا مدل کسب‌وکاری، محدودیت‌های جغرافیایی داشته باشد، بایستی محیط‌های ابری برنامه‌ها و کاربران را مانند هر استقرار دیگری در IT، احراز هویت نماید. مدیریت دسترسی‌های ممتاز ابر به ابر در مقایسه با پیاده‌سازی‌های درون‌سازمانی، الزامات منحصربه‌فردی دارد:

- معماری‌های با دسترسی‌پذیری بالا می‌توانند نمونه‌های ابری اضافی را به‌منظور ارائه دسترس‌پذیری بهتر در ابر یا زیرساخت را تضمین نمایند؛
- ممکن است مقررات به نمونه‌های جدا از هم ولی تکثیریافته نیاز داشته باشد و داده‌ها را بر اساس منطقه یا قوانین محلی فیلتر نماید؛

- ممکن است سازمان‌ها به محدوده‌های IP عمومی و خصوصی برای ارائه خدمات و تدارکات اختصاصی موردنیاز جهت امن‌سازی آن‌ها، نیاز داشته باشند؛
- مدیریت آسیب‌پذیری‌های ناشی از سرویس‌های عمومی ممکن است نیاز به هماهنگی با ارائه‌دهنده فضای ابری را جهت کاهش این تهدیدات داشته باشد؛
- دسترسی API به توجه ویژه‌ای برای دسترسی امن و محدودسازی آن نیاز دارد؛
- داده‌های حساس در ابر مانند رمزهای عبور به امنیت پایگاه داده اضافی مثل HSM برای حفاظت از اطلاعات نیاز دارند.

برای سازمان‌هایی که به دنبال آن هستند تا PAM را تنها روی ابر اجرایی کنند، فناوری‌های زیادی برای پیاده‌سازی این راهکار وجود دارد که معمول‌ترین آن‌ها استفاده از فناوری جعبه سیاه مبتنی بر راهکارهای PAM است که در فضای ابری میزبانی شده است. این موارد امکان ارائه مدل‌های اجرایی PAM امن‌شده مبتنی بر انواعی از مدل‌های صدور مجوز و هزینه‌های زمان اجرای ابر را ممکن می‌سازند. برخی از شرکت‌های PAM راهکارهایی را پیشنهاد می‌دهند که می‌توان آن‌ها را به‌عنوان یک پیاده‌سازی نرم‌افزاری در قالب سیستم‌عامل ابری معرفی کرد. این موارد منعطف‌ترین نمونه برای مشتری را به ارمغان می‌آورد ولی امنیت، مقاوم‌سازی و پیکربندی سیستم‌عامل جزء مسئولیت‌های مشتری است و سرویس‌دهنده‌های فضای ابری یا شرکت‌های ارائه‌دهنده PAM این کار را انجام نمی‌دهند. در این نوع از پیاده‌سازی‌ها، ریسک‌ها بیشتر است ولی می‌توان آن را برای تحقق موارد موردنیاز، کاملاً سفارشی‌سازی نمود.

نرم‌افزار به‌عنوان سرویس (SaaS)

نرم‌افزار به‌عنوان سرویس (SaaS) مدل تحویلی است که در آن سرویس به‌صورت مرکزی در ارائه‌دهنده میزبانی می‌شود و بر اساس حق اشتراک به مشتریان، مجوز استفاده صادر می‌شود. سازمان‌ها و کاربران نهایی معمولاً با این سرویس‌ها و از طریق یک صفحه وب یا APIهای برنامه‌نویسی تعامل دارند. این کار به شما اجازه می‌دهد تا بخش کوچکی از اپلیکیشن را بدون هزینه و پیچیدگی ساخت سرورها و نگهداری نرم‌افزار مورد استفاده قرار دهید. مثال‌هایی از راهکارهای SaaS سازمانی شامل SalesForce، Workday، Facebook و LinkedIn است. در یک مدل SaaS، مسئولیت امنیت هسته سازمان با خود اپلیکیشن است. این مورد شامل کسی است که می‌تواند به اپلیکیشن دسترسی داشته باشد، احراز هویتی است که موردنیاز است و

چیزی است که کاربران پس از دسترسی باید داشته باشند. هر اپلیکیشن ممکن است مدل دسترسی خود را داشته باشد که سطوح تدارکات موجود آن بر اساس شرکت ارائه‌دهنده متفاوت باشد. برنامه‌های SaaS ممکن است سرویس‌های کسب‌وکاری سنتی داشته باشند و یا ممکن است مدل‌های مجوز دقیقی برای ارائه انعطاف‌پذیری و مجوزها به گروه‌های خاصی از کاربران بر اساس وظایف و یا کاربردها تدارک دیده باشند. همچنین ممکن است این برنامه‌ها، ویژگی‌های نظارتی درون‌سازمانی مانند جداسازی وظایف و حسابرسی دقیقی داشته باشند که سازمان را قادر می‌سازد تا دسترسی به ویژگی‌ها و داده‌های حساس را کنترل کرده و بررسی نماید. دیگر برنامه‌های SaaS مانند Facebook، LinkedIn و یا Twitter که به‌طور معمول متمرکز بر مصرف‌کننده بوده‌اند، جزئیات کمتری را در مدل‌های مجوزدهی خود دارند. در برخی موارد، کاربران حساب سازمانی مشترکی را برای مدیریت سیستم‌های سازمان به اشتراک می‌گذارند درحالی‌که ممکن است این برنامه‌های SaaS، سطح یکسانی از اطلاعات حساس مثل فهرست مشتریان یا داده‌های مالی را نداشته باشند ولی این حساب‌ها ریسک قابل‌توجهی را برای یک سازمان به همراه دارند. از معضلات آن می‌توان به آسیب‌رسانی اشاره کرد، مثلاً اگر کاربر مدیر به مرخصی رفته باشد، به‌روزرسانی‌ها متوقف خواهند شد. مشکل دیگر می‌تواند اختلال باشد مثلاً اگر هکری از یک حساب هک‌شده برای ارسال نوشته یا توییتی نامناسب استفاده کند، می‌تواند بر شهرت و اعتبار شرکت اثرگذار باشد. در هر دو مورد، مدیریت مناسب و کنترل این حساب‌ها باید در هنگام طراحی یک برنامه امنیتی کلی، مدنظر قرار گیرد.

علاوه بر این، برای امن‌سازی و کنترل دسترسی به برنامه‌های ابری، این لایه امنیتی دارای حق ویژه جدید را نیز می‌توان میزبانی کرد. راهکارهای مدیریت دسترسی‌های ممتاز که به صورت راهکار SaaS اجرا می‌شوند، می‌توانند صرفاً در ابر عمل کرده و یا به گره‌های مدیریتی درون-سازمانی نیاز دارند تا مسیریابی و تجمیع سیاست‌ها و رویدادها را انجام دهند. این مدل‌های پیاده‌سازی کاملاً توسط شرکت‌های ارائه‌دهنده PAM و یا محیط‌های ابر خصوصی کاربر نهایی مدیریت می‌شود و یا با استفاده از منابع ابری مشترک با دیگر مشتریان PAM در تجهیزات چند مستأجری فروشنده عمل می‌کند. این مدل را می‌توان به‌وسیله شرکت ارائه‌دهنده PAM و یا یک MSP میزبانی کرد.

پلتفرم به‌عنوان سرویس (PaaS)

پلتفرم به‌عنوان سرویس گروهی از رایانش ابری است که سطح اضافی از آسان‌سازی و خودکارسازی کارها را ارائه می‌کند. این خدمات ابری پلتفرمی را ارائه می‌کنند که به مشتریان اجازه می‌دهد تا برنامه‌ها را بدون پیچیدگی ساخت، نگهداری زیرساخت و یا چهارچوب خودکار آن، توسعه داده، اجرا نموده و مدیریت نمایند. مثال‌هایی از شرکت‌های PaaS شامل پلتفرم Oracle Cloud، Cloud Foundry و RedHat OpenShift است. معمولاً پلتفرم‌های PaaS برای طراحی و میزبانی از برنامه‌ها و خدمات حیاتی یک سازمان استفاده می‌شوند و لازم است که امنیت آن را از پایه بسازیم. مؤلفه‌ای از این طراحی باید شامل کنترل و حسابرسی دسترسی‌های ممتاز باشد.

برای محافظت از این مدل‌های ابری، راهکارهای مدیریت حقوق ویژه ممکن است برای کنترل انواعی از فعالیت‌ها اعم از فعالیت‌های زیر اجرایی شوند:

۱. فناوری‌های مبتنی بر عامل بر روی ماشین‌های مجازی در حال اجرا درون IaaS ای که در سیستم‌عامل یا لایه پوششی استقرار یافته‌اند، قرار می‌گیرند تا با ایجاد مدل دسترسی ممتاز و ارائه ثبت فعالیت لحظه‌ای دقیق از تمام فعالیت‌های ممتاز مورد استفاده قرار گیرند. نقش‌های دارای حقوق ویژه می‌توانند شامل مدیران سرور، توسعه‌دهندگان، مدیران پایگاه داده و غیره باشند؛
۲. عملکردهای مدیریت رمز عبور جهت استقرار، مدیریت و خودکارسازی امن حساب‌های ممتاز در تمام سیستم‌عامل‌ها و لایه‌های سرویس ارائه‌شده توسط ماشین‌های مجازی در حال اجرا درون محیط IaaS است. نقش‌های ممتاز می‌توانند شامل مدیران سرور، حساب‌های موجود در سرویس‌ها و اسکریپت‌های مربوط به برنامه‌ها باشند؛
۳. عملکردهای مدیریت رمز عبور جهت استقرار، مدیریت و خودکارسازی امن حساب‌های ممتاز در لایه مدیریتی PaaS است. نقش‌های دارای حقوق ویژه می‌توانند شامل مدیران ابر Azure، مدیران مرکز داده و غیره باشند؛
۴. مدیریت و ضبط نشست برای تمام فعالیت‌های ممتاز در لایه مدیریتی PaaS؛
۵. عملکردهای مدیریت رمز عبور و نشست جهت مدیریت، خودکارسازی و حسابرسی امن فعالیت‌های مربوط به حساب‌های ممتاز در تمام برنامه‌های SaaS سازمان.

فصل ۱۶

دستگاه‌های موبایل

دستگاه‌های موبایل، هدف حمله منحصربه‌فردی برای عاملان تهدید هستند. این دستگاه‌ها، دارای حساب و اعتبارنامه هستند ولی دسترسی مبتنی بر نقش ندارند و در حالت کلی تنها دو نوع مجوز در آن‌ها وجود دارد: کاربر و روت. به‌علاوه، معمولاً بر روی دستگاه‌های موبایل تنها یک حساب وجود داشته و سیستم‌عامل تدارکاتی برای حساب کاربری بیشتر را به‌عنوان بخشی از طراحی‌اش ارائه نمی‌کند.

برای اینکه حمله موفقیت‌آمیزی رخ دهد، عامل تهدید باید سیستم‌عامل یا برنامه‌ها را با استفاده از بدافزارها یا اکسپلویت‌ها هک کند. این مورد احتمالاً شامل نرم‌افزار مخربی است که می‌تواند به‌طور نامناسبی روی یک ارائه‌دهنده قانونی برنامه‌ها میزبانی شده باشد. هدف هکر بهره‌گیری از دستگاه‌ها است تا اقدامات زیر را انجام دهد:

- خروج اطلاعات از دستگاهی که به‌صورت شخصی قابل‌شناسایی بود و یا برای سازمان حساس به شمار می‌رفت؛
- فعال‌سازی نظارت از طریق GPS، دوربین و یا صوت؛
- بهره‌گیری از دستگاه برای استفاده از اقدامات بعدی به‌منظور حمله به دارایی‌ها و تجهیزات سازمانی، عمومی و یا رومینگ[1]؛
- ایجاد حضور دائمی برای حملات جدید یا دیگر حملات دائمی پیشرفته.

[1] Roaming

نکته قابل ذکر در اینجا آن است که هدف عامل تهدید بدون توجه به دارایی‌های قدیمی سازمان یا دستگاه‌های اینترنت اشیاء همیشه یکسان است. وقتی عامل تهدید دسترسی ممتازی را به دست آورد، هدف حمله آن یکسان خواهد بود درصورتی‌که عملیات دفاع برای تجهیزات موبایلی کاملاً متفاوت است زیرا هیچ دسترسی مبتنی بر نقش در آن‌ها وجود نداشته و برخی از دستگاه‌های موبایل حتی از راهکارهای ضد بدافزار سنتی نیز پشتیبانی نمی‌کنند مانند iOS اپل؛ بنابراین بهترین راهکار دفاعی آن است تا مدل‌های امنیتی که اجازه استفاده از آن‌ها را داریم، به کار ببریم:

- برای سازمان‌هایی که از دستگاه‌های موبایل در مدل «دستگاه خود را بیاورید[1] (BYOD)» یا از مدل دستگاه‌های عرضه‌شده سازمانی استفاده می‌کنند، پیشنهاد می‌شود از یک مدیریت‌کننده دستگاه موبایل[2] (MDM) به‌منظور ارائه تقسیم‌بندی برنامه‌ها و داده‌ها استفاده کنند. این کار به سازمان اجازه می‌دهد تا سیاست‌های استفاده قابل‌قبولی را اجرا کند و حتی برنامه‌های مخرب احتمالی را که می‌توانند دستگاه را آلوده نمایند، پاک کند؛
- برای دستگاه‌های غیر اپلی، راهکارهای امنیتی فراوانی وجود دارند که می‌توانند بدافزارها، مجوزهای نامناسب و حتی پیکربندی‌های ضعیف (مثلDebugging USB) را شناسایی کنند که ممکن است برای آلوده‌سازی دستگاه به کار روند. بسیاری از این عامل‌ها در بازارهای اپلیکیشن یافت می‌شوند ولی به وسیله راهکارهای MDM و شرکت‌های ضد ویروس مرسوم نیز پشتیبانی می‌شوند. توصیه می‌شود که از آن‌ها برای شناسایی ریسک‌ها و کاهش هرگونه تهدیدات خاص مربوطه به آن دستگاه موبایل استفاده شود؛
- در صورت امکان دستگاه‌های موبایل نباید هرگز دسترسی مستقیمی به مرکز داده و سیستم‌های حساس سازمان داشته باشند. اتصال آن‌ها همیشه باید از طریق پروکسی یا از طریق یک میزبان واسط برای دسترسی به منابع صورت گیرد. دسکتاپ‌های مجازی و اپلیکیشن‌های از راه دور برای تقسیم‌بندی دستگاه‌های موبایل جهت دسترسی محدود، اجرای احراز هویت چند مرحله‌ای و جلوگیری از اقدامات بعدی

[1] Bring Your Own Device
[2] Mobile Device Manager

هکر ایده‌آل هستند. این کار می‌تواند شامل استفاده از مدیریت‌کننده‌های رمز عبور برای ایجاد اتصالات اضافی و نظارت بر نشست‌ها باشد تا بتوان دریافت که آیا تمام دسترسی‌های رومینگ مناسب و مجاز هستند یا خیر.

دستگاه‌های موبایل ابزاری برای اتصال دائمی افراد را در جهان فراهم کرده‌اند. این دستگاه‌ها برای یک عامل تهدید، راهی را برای نفوذ به محیط سازمان ایجاد می‌کنند، حتی اگر این دستگاه‌ها درون دفتر کار نباشند. به دست آوردن دسترسی ممتاز، نیاز ضروری نیست؛ همچنین این دستگاه‌ها مدل‌های امنیتی مقاوم همچون منابع مرسوم IT را ندارند؛ اما بهره‌مندی از دستگاه موبایل برای دسترسی به یک نقطه در محیط می‌تواند به اندازه کافی برای یک اکسپلویت یا بدافزار به‌منظور تحمیل خسارتی به اندازه روت خوب باشد.

پس عامل تهدید چطور می‌تواند دسترسی‌های موردنیاز را برای انجام این جرایم به دست آورد؟ این امر خیلی راحت‌تر از آن است که فکر می‌کنید و مدل‌های امنیتی برای دستگاه‌های موبایلی نیز پر از نقص‌های مفتضحانه‌ای هستند، برای مثال سناریوهای احتمالی زیر را در نظر بگیرید:

- نصب نرم‌افزار جدید از یک ارائه‌دهنده نرم‌افزار معتبر (مانند گوگل پلی) که می‌تواند حاوی بدافزار باشد. شرکت‌ها تنها می‌توانند غربالگری برنامه‌ها را انجام دهند و بدافزارهای تکراری را شناسایی کنند ولی برخی از بدافزارها قابلیت دور زدن سیستم‌های شناسایی بدافزارها را داشته و می‌توانند منتشر شوند؛
- زیست‌سنج‌ها برای اعتبارسنجی و احراز هویت، همچنین جهت دسترسی دستگاه به اعتبارنامه‌های اپلیکیشن مورد استفاده قرار می‌گیرند. زیست‌سنج‌ها نه‌تنها دسترسی به دستگاه‌ها را ارائه می‌کنند بلکه برای برنامه‌هایی مثل برنامه‌های بانکداری، از همان مکانیزم برای دسترسی به اطلاعات مالی بهره می‌برند. زیست‌سنج‌ها به‌تنهایی به‌عنوان اعتبارنامه ایده بدی هستند زیرا اگر شکل الکترونیکی آن‌ها هک شود هرگز نمی‌توان آن‌ها را تغییر داد. زیست‌سنج‌ها را باید با احراز هویت چند مرحله‌ای به صورت مکمل استفاده کرد چون اعتبارنامه‌های مبنا را همیشه می‌توان تغییر داد درحالی‌که زیست‌سنج‌ها تنها هویت شما را به‌صورت الکترونیکی اثبات می‌کنند. متأسفانه تولیدکنندگان دستگاه موبایل زیادی وارد این عرصه شده‌اند و با تبدیل این

روش به‌عنوان تنها راه شناسایی موردنیاز برای دسترسی به دستگاه حین عملیات‌های عادی، best practice ها را منظور نکرده‌اند. این کار به نوعی قمار بر روی ماژول امنیتی زیست‌سنج آن‌ها است و زمان اثبات خواهد کرد که آیا این طراحی‌ها به اندازه کافی برای متوقف ساختن تهدیدات مدرن کافی هستند یا خیر؛

- دستگاه‌های موبایل (جدای از شارژ Qi) به یک اتصال سیمی برای شارژ مجدد به‌صورت روزانه نیاز دارند. همچنین این دستگاه‌ها سیستم‌های ارتباطی دوطرفه زیادی مثل NFC، بلوتوث و وای‌فای دارند. مشکل امنیتی که وجود دارد این است که کنترل‌های بسیار کمی در مورد اکسپلویت شدن از راه دور این مسیرهای ارتباطی وجود دارد. این موارد شامل شارژرهای USB نیز می‌شود که شامل بدافزاری به‌منظور انجام حملات «man in the middle» است که می‌تواند ارتباطات وای‌فای را شنود و هک کند. این‌ها تنها نقص‌های امنیتی هستند که در ذات دستگاه‌های موبایل است و جدای از قفل کردن آن‌ها ریسک بالا را بر روی منابع معتبر شناخته‌شده ارائه می‌کنند. به‌طور پیش‌فرض، این دستگاه‌ها مستعد آسیب دیدن هستند؛
- تنها برای دستگاه‌های اندرویدی، پراکندگی سیستم‌عامل‌ها و نرم‌افزارها، چالش‌های امنیتی منحصربه‌فردی را برای هر دستگاه به همراه دارد. گستره مشکلات فراتر از محدودیت‌های این بخش است و در موارد زیادی، نقصی بر روی یک دستگاه اندرویدی ممکن است بر روی دستگاه دیگری وجود نداشته باشد و حتی ممکن است تولیدکننده تصمیم به رفع آن نقص نگیرد. در سازمان‌ها، اجازه دادن به استفاده از دستگاه‌های اندرویدی مطابق با مدل‌های BYOD یا دستگاه‌های عرضه‌شده توسط خود سازمان، باید حداقل موارد امنیتی شرکت‌ها را مدنظر قرار دهند. تمام تولیدکنندگان، سطح توافق خدمات[1] (SLA) یکسانی را برای تأمین وصله‌ها به کار نمی‌برند و برخی نیز با ایجاد درب‌های پشتی که برای دستگاه‌های خود و با هدف به‌روزرسانی‌ها و نظارت به کار می‌برند، شناخته می‌شوند که ممکن است هیچ یک از آن‌ها برای سازمان‌هایی با عملیات حساس مورد قبول نباشد.

[1] Service Level Agreement

با وجود این نقص‌ها، فناوری‌هایی برای کاهش این ریسک‌ها و اعمال بهترین روش‌های امنیتی وجود دارد. برای مثال:

- با استفاده از فناوری MDM یا بهترین راهکارهای امنیتی، دستگاه‌های BYOD را به شبکه‌های مورد اعتماد محدود کرده و قفل کنید و از شارژر USB نامعتبر استفاده نکنید؛
- در مواردی که می‌توانید پشتیبانی کنید و یا مواردی که نمی‌توانید پشتیبانی کنید، تصمیم‌گیری کنید. داشتن لیست محدودی از تولیدکنندگان و نسخه سیستم‌عامل‌ها به کاهش ریسک‌ها، مخصوصاً از سوی تهدیدات خارجی کمک خواهد کرد.

فصل ۱۷

باج‌افزارها

بگذارید در همین ابتدای امر مسئله‌ای را مشخص کنیم: هیچ راهکار قطعی که بتواند به‌صورت ۱۰۰٪ ریسک باج‌افزارها را کاهش داده و حذف نماید، وجود ندارد. برخی از فناوری‌ها ادعا می‌کنند که صدها نمونه را تست کرده‌اند و اینکه ابزار آن‌ها می‌تواند ۱۰۰٪ نمونه‌ها را شناسایی و متوقف سازد. متأسفانه این حرف دروغ است. چرا؟ اگر هر شرکتی راهکاری داشت که می‌توانست این مشکل را کاملاً حل کند، باج‌افزار به چیزی که در حال حاضر وجود دارد، تبدیل نمی‌شد.

راهکارهای کنترل اپلیکیشن، محصولات حفاظت نقاط انتهایی (کاربران) و حتی راهکارهای حداقل حقوق ویژه درجات مختلفی از موفقیت را در کاهش باج‌افزارها دارند ولی هیچ‌کدام ۱۰۰٪ موفق نیستند. چرا؟ باج‌افزارهای پیشرفته می‌توانند در صورت موجود بودن از حقوق ویژه بهره ببرند، همیشه فایل‌های اجرایی جداگانه‌ای را راه‌اندازی نمی‌کنند و گاهاً دستگاه‌هایی مثل تلویزیون‌های هوشمند را هدف قرار می‌دهند. برای مثال ما باج‌افزاری را دیدیم که از ماکروهای[1] مایکروسافت آفیس برای پخش تهدیدات استفاده می‌کرد و حتی نسخه‌هایی که از Jscript تعبیه‌شده در یک سند برای اجرای فعالیت‌های مخرب بهره می‌بردند. همچنین باج‌افزارهایی مثل WannaCry را دیدیم که از اکسپلویت‌های سیستم‌عامل‌های ویندوزی جدید و قدیمی بهره می‌برند تا سازمان‌ها را آلوده کنند. با ادامه بلوغ و پیشرفت باج‌افزار به‌عنوان بزرگ‌ترین تهدید امنیت سایبری این دهه، اهداف حمله در حال رشد هستند. باج افزارها

[1] Macros

می‌توانند از یک آسیب‌پذیری قابل اکسپلویت وارد سازمان شوند، به‌صورت اسکریپت‌های پاورشل باشند و یا به‌عنوان یک ماکرو یا اسکریپت در یک فایل یا وب‌سایت تعبیه شده باشند یا به‌صورت فایل‌های اجرایی باشند. چیزی که آن‌ها را خطرناک‌تر می‌کند آن است که حملات زیادی، روش‌های مختلف را با هم ترکیب کرده و از یک سرور کنترل و دستور برای نگهداری کلیدهای نامتقارن رمزنگاری استفاده می‌کنند. باج‌افزارهای مدرن ممکن است تنها یک اسب تروآ[1] برای دیگر تهدیدات پیشرفته‌ای باشند که برای منحرف کردن فکر تیم‌های امنیتی IT به کار می‌روند. به همین دلیل است که متوقف کردن باج‌افزارها بسیار سخت است و هیچ فناوری به‌طور ۱۰۰٪ مؤثر نیست.

اقداماتی جهت کاهش تهدید وجود دارد که شما می‌توانید با مدیریت کردن دسترسی‌های ممتاز انجام دهید. متأسفانه، هیچ چیزی هرگز مانع از آن نمی‌شود که کاربران روی لینک‌های فیشینگ کلیک نکنند و یا هنگام اجرا کردن یک فایل ناشناخته، ماکروها را انتخاب ننمایند. به‌هرحال، در اینجا ما سیاست‌هایی را بیان می‌کنیم که پیاده‌سازی آن‌ها آسان بوده و از بیشتر اشتباهات کاربران جلوگیری می‌کند. در صورت اجرای صحیح این سیاست‌ها می‌توان مانع از اجرای دراپِرها[2] و استفاده از برنامه‌های آسیب‌پذیر علیه دارایی‌های سازمان شد.

- کنترل اپلیکیشن برای مسدودسازی فایل‌های اجرایی غیر قابل اطمینان- راهکارهای مدیریت دسترسی‌های ممتاز (PAM)، امکان کنترل اپلیکیشن و قابلیت اجرای قواعد و سیاست‌ها برای بهتر کردن برنامه‌ها را به وجود می‌آورد. این کار مانع از اجرای هرگونه اپلیکیشنی غیر معتبر می‌شود، جدای از اینکه منبع آن برنامه از کجاست و دارای امضاء دیجیتالی مناسبی است یا خیر و یا اینکه برنامه سعی دارد تا فرآیند مخربی را به‌عنوان یک دراپر آغاز نماید یا خیر؛
- متوقف کردن دراپرها- متأسفانه برنامه‌های مورد اعتماد می‌توانند دیگر برنامه‌ها را اجرا نمایند تا عملیات مورد نظر خود را انجام دهند. این برنامه‌ها شامل مرورگرها، برنامه‌های ایمیل و حتی برنامه‌های پی‌دی‌اِف‌خوان است. بخش ثابت مسئله آن است که این فایل‌های اجرایی تقریباً همیشه از دایرکتوری‌های فایل موقت[3] اجرا می‌شوند.

[1] Trojan Horse
[2] Droppers
[3] Temporary file

با استفاده از مدیریت دسترسی‌های ممتاز (PAM) جهت مدیریت یکپارچگی فایل، مدیران می‌توانند فایل‌های اجرایی دراپر را که در این دایرکتوری‌ها ظاهر می‌شوند و الزامات حداقلی معتبر بودن را محقق نمی‌کنند، ردیابی کرده، هشدار داده و مسدود سازند؛

- برنامه‌های آسیب‌پذیر- راهکارهای مدیریت دسترسی‌های ممتاز معمولاً دارای موتور ارزیابی فایل یا فناوری‌های دیگری برای اندازه‌گیری ریسک یک اپلیکیشن قبل از اجرای آن هستند. این مؤلفه امکان ارزیابی لحظه‌ای امنیت یک اپلیکیشن را برای بررسی از نظر بدافزار بودن، داشتن آسیب‌پذیری‌ها، مجوزها و حریم خصوصی امکان-پذیر می‌کند. برای رسیدن به این هدف می‌توان سیاست‌هایی را برای رد (یا اعلان) اجرای برنامه‌های ریسکی ایجاد کرد که می‌توانند در حمله باج‌افزار مورد استفاده قرار گیرند. این کار کمک می‌کند تا تضمین نماییم توافقات سطح خدمات برای حفاظت امنیت سایبری محقق شده‌اند و سیستمی باقی نمانده است که بتواند ریسک غیرقابل‌قبولی را داشته باشد.

درسی که از باج‌افزار می‌گیریم، همان حقوق ویژه به‌عنوان اهداف حمله هستند. ریسک باج‌افزار را می‌توان به‌وسیله استفاده از همان فناوری مدیریت حساب‌های ممتاز حداقل کرد. با وجودی که این رویکرد ۱۰۰٪ مؤثر نیست ولی هنگامی‌که سازمان‌ها این رویکرد را در پیش بگیرند، در همان مرحله اول با ندادن مجوزهای موردنیاز به باج‌افزار برای اجرا شدن، مانع از اجرای آن‌ها شوید.

فصل ۱۸

عملیات توسعه‌ای امن (SDevOps)[1]

هرچه سازمان‌ها با به‌کارگیری روش‌های توسعه چابک پیش می‌روند که در آن‌ها به یکپارچه‌سازی گسترده و خودکارسازی میان ابزارهای عملیاتی نیاز دارند، درمی‌یابند که مدیریت مؤثر و ایمن اعتبارنامه‌های موردنیاز برای پشتیبانی از فرآیندهای انتها-به-انتها[2] دشوارتر می‌شود. یک فرآیند DevOps معمول برای خودکارسازی، مدیریت و اجرای کدهای ساخته‌شده، ممکن است شامل موارد زیر باشد:

- حساب‌های خدماتی که خدمات مختلفی را اجرا می‌کنند (TFS، Builds، SQL)؛
- وظایف زمان‌بندی‌شده و خودکار (اسکریپت‌های سفارشی، Git و GitHub، Jenkins، Puppet و دیگر موارد)؛
- خدمات ثالث (SMTP، خدمات ابری، SNTP و غیره)؛
- گواهی‌هایی برای وب‌سایت‌های SSL، امضاء خودکار کد و دیگر فرآیندهایی که پوشش‌های امنیتی دارند.

تمام این فناوری‌هایی که توسعه و اجرای اپلیکیشن را درون فرآیند ساده‌تری یکپارچه کرده و خودکار می‌نمایند، به اعتبارنامه‌ها نیاز دارند و هیچ هویتی ندارند چون به‌صورت خودکار انجام می‌شوند. در برخی موارد، این اعتبارنامه‌ها را می‌توان در اسکریپت‌ها، کدها و فایل‌های پیکربندی ذخیره‌سازی کرده و به اشتراک گذاشت. ریسک ذخیره‌سازی، اشتراک‌گذاری و

[1] Secured Development Operations (DevOps)
[2] End-to-End

اعتبارنامه‌های با تغییرات کم که مورد استفاده برای خودکارسازی فرآیندهای DevOps هستند، آن‌ها را در معرض آسیب و هک شدن قرار می‌دهد، مخصوصاً اگر به‌صورت متنی آشکار باشند. برای کاهش این ریسک‌ها، سازمان‌ها باید به دنبال گسترش برنامه‌های دسترسی ممتاز باشند و فازهایی را پیاده‌سازی کنند که شامل موارد زیر است:

۱. حذف اعتبارنامه‌های نوشته‌شده در کد (کامپایل شده)، اسکریپت‌ها و حساب‌های خدماتی. اغلب شرکت‌های مدیریت رمز عبور سازمانی، حساب خدماتی و APIهای رمز عبوری را شامل می‌شوند که می‌تواند برای حل این موارد پیاده‌سازی شود؛
۲. یک میزبان واسط و تجهیزاتی را برای نشست‌های مدیریت‌شده پیاده‌سازی کنید تا بتوانید توسعه‌دهندگانی را که به سرورهای تولید دسترسی دارند، کنترل کنید. روش‌های DevOps اغلب به وارد کردن کد، کامپایل و یکپارچه‌سازی گردش‌های کاری پس از کامپایل نیاز دارند. هدف آن است که توسعه‌دهندگان را امن نگه داریم و به‌راحتی جریان‌های کاری حیاتی را اجرا کنیم ولی دسترسی مستقیمی به خود سیستم‌ها نداشته باشیم. پیاده‌سازی یک میزبان واسط یا راهکار مدیریت نشست با کنترل اتصالات امن در محیط اجرای یکپارچه و پیوسته، این کار را به‌وسیله مدیران، وظایف خودکار یا توسط توسعه‌دهندگان ممکن می‌سازد؛
۳. پیاده‌سازی مفهوم حداقل حقوق ویژه در سراسر محیط اپلیکیشن. آیا توسعه-دهندگان، ابزارها یا فرآیندهای توسعه به دسترسی روت یا مدیر به سیستم‌ها و پایگاه‌های داده پشتیبان محیط اپلیکیشن نیاز دارند؟ فرآیندهایی که توسعه داده شوند نباید به دسترسی‌های روت یا مدیر نیاز داشته باشند. پیاده‌سازی حقوق ویژه حداقلی تضمین می‌کند که توسعه‌دهنده‌ها و فرآیندها تنها حقوق ویژه‌ای دارند که برای پشتیبانی گردش کار آن‌ها در فرآیند DevOps انتها به انتها نیاز است. به‌علاوه، افزودن حق ویژه حداقلی به ضبط نشست و ثبت کلیدهای فشرده‌شده نیز به شناسایی فعالیت‌های آلوده حساب و ریسک‌های مربوط به سوءاستفاده حقوق ویژه کمک می‌کند؛
۴. طراحان برای کمتر کردن پیچیدگی‌های مربوط به ایجاد و مدیریت حساب‌های محلی در تمام سیستم‌های غیر ویندوزی یک محیط ابری پویا، باید روش‌هایی را مورد تحقیق و بررسی قرار دهند تا حساب‌ها را تحکیم کرده و متمرکز نمایند.

و در آخر اینکه سازمان‌ها باید راهکارهایی را برای حفافظت کُنشی کانتینرها و میکرو سرویس‌هایی که به برنامه‌های سازمان در ارتباط هستند، مورد آزمایش قرار دهند. وقتی سازمان‌ها برنامه‌های قدیمی خود را به فضای ابری تبدیل می‌کنند و مفاهیم جدید شامل کانتینرها را می‌پذیرند، باید بررسی کنند که چطور پایه‌های امنیتی را به بلوغ برسانند و ریسک‌های مربوط به این محیط‌های پویا را حداقل نمایند. علاوه بر اسکن کردن آسیب‌پذیری-ها و بررسی نمودن یکپارچگی، برای داشتن بهبودهای پیوسته تنها به کانتینرهای تأییدشده‌ای نیاز است که در محیط در حال اجرا هستند، پس سازمان‌ها باید حقوق حداقلی، نظارت دسترسی، تقسیم‌بندی و تهیه لیست سفیدی از فایل‌ها و سرویس‌ها را نیز در سطح کانتینر ارزیابی نمایند تا از میزبان‌ها و دیگر کانتینرهایی که ممکن است در حال اجرا در محیط باشند، محافظت کنند. انتقال تمام برنامه‌ها و کدهای منبع شما به ابر بسیار سخت و مشکل است. بسیاری از کنترل‌ها که متخصصان امنیتی به‌صورت صریح می‌پذیرند، رویکردهای جایگزینی دارند و نباید از آن‌ها صرف‌نظر شود. برای DevOps، امنیت موضوعی کلیدی است و مدیریت حقوق ویژه برای حفاظت از فرآیند خودکار ضروری است!

فصل ۱۹

سازگاری با قوانین

عاملان تهدید اهمیتی به قانون، مقررات، توافقات و راهکارهای امنیتی نمی‌دهند. درواقع آن‌ها امیدوار هستند که سازمان شما درباره بسیاری از این مشخصه‌ها و چهارچوب‌ها سهل‌انگاری کرده باشد تا بتوانند از آن‌ها برای اقدامات مخرب خود بهره ببرند. درحالی‌که پیروی و سازگاری با قوانین به این دلیل طراحی شده است تا راهبردهای لازم را برای اجرای قانون در صنایع و دولت‌ها ارائه کند ولی به‌هرحال ابزارهای موردنیاز برای امن ماندن را ارائه نمی‌کنند و پیروی از آن‌ها به معنای امن بودن نیست. آن‌ها این راهبردها را برای حرکت به‌سوی امنیت سایبری سالم اجرا کرده‌اند ولی پیاده‌سازی آن‌ها بدون در نظر گرفتن فرآیندهای مناسب، افراد، آموزش‌های لازم و پشتکار سبب می‌شود که شما مستعد نفوذ و هک شدن باشید؛ بنابراین در هنگام مرور قوانین، موارد زیر را در نظر بگیرید:

- چگونه مقررات را بر مبنای اطلاعات حساس، قراردادها، صنعت و جغرافیا به سازمانتان اعمال کنید؟
- چه هم‌پوشانی بین آن‌ها وجود دارد و چه فرآیندهایی می‌توانند الزامات مختلف را محقق سازند؟
- اطمینان حاصل کنید که سخت‌گیرانه‌ترین استراتژی‌ها را برای سازمان خود به کار می‌گیرید.
- تحقیق و ارزیابی نقشی حیاتی دارند. تنها اعمال قواعد به سیستم‌های حساس جهت داشتن امنیتی مناسب، کافی نیست لذا تلاش‌ها و هزینه‌های لازم را جهت افزایش

محدوده و کاهش ریسک‌ها در تمام سیستم‌های متصل به سازمان مورد بررسی قرار دهید که از نظر قانونی می‌تواند محدوده موردنیاز را تحت تأثیر قرار دهد.

بنابراین در نظر داشته باشید که پیروی از الزامات قوانین و مقررات موارد حداقلی از اقداماتی است که سازمان شما باید در پیش بگیرد. اگر شما این حداقل‌ها را محقق نکنید و یا در الزامات شکافی وجود داشته باشد، شما راحت‌ترین گزینه برای عامل تهدید هستید و البته کُندترین فرد در بین گروهی که خرسی به دنبال آن‌ها است!

صنعت کارت پرداخت[1] (PCI)

استاندارد امنیت اطلاعات در صنعت کارت پرداخت (PCI DSS) که ابتدا در سال ۲۰۰۴ توسعه داده شد و نسخه کنونی آن به شماره 3.2 است، یک استاندارد امنیت اطلاعاتی برای سازمان هایی است که کارت‌های اعتباری مثل Visa، MasterCard، American Express و بقیه را قبول می‌کنند.

استاندارد PCI:

- جهت کاهش تقلب در کارت های اعتباری و افزایش کنترل داده‌های دارندگان کارت ایجاد شد؛
- به استانداردی عملی جهت حفاظت دسترسی به اطلاعات قابل‌شناسایی شخصی[2] (PII) مخصوصاً در صنعت خرده‌فروشی تبدیل شد؛
- در اختیار صادرکنندگان کارت است؛
- به‌وسیله شورای استانداردهای امنیتی صنعت کارت پرداخت (PCI SSC) مدیریت می‌شود.

سازمان‌ها برای اثبات پیروی خود از PCI DSS با چالش‌های زیادی روبرو می‌شوند. بزرگ‌ترین سازمان‌ها در چالش با ارزیابی‌هایی هستند که به‌صورت سالانه توسط یک ارزیاب امنیتی واجد شرایط[3] (QSA) انجام می‌شود که این شخص گزارشی از پیروی و انطباق[4] (ROC) آن سازمان

[1] Payment Card Industry
[2] Personally Identifiable Information
[3] Qualified Security Assessor
[4] Report on Compliance

با PCI DSS تهیه می‌کند. اگرچه انطباق با PCI DSS برای قانون فدرال در ایالات‌متحده موردنیاز نیست ولی قوانین برخی ایالات‌ها یا به‌صورت مستقیم به PCI DSS اشاره کرده‌اند و یا نمونه‌هایی معادل را تهیه نموده‌اند. اگر سازمانی رخنه امنیتی داشته باشد و از PCI پیروی نکرده باشد، صادرکنندگان کارت می‌توانند جریمه‌های مالی قابل‌توجهی را برای آن شرکت تحمیل کنند. بهترین راهکار برای PCI DSS آن است که به‌صورت پیوسته فرآیندها را به‌منظور تضمین تطابق با مقررات بهبود دهیم و پیروی و انطباق را به‌صورت یک مرحله در زمان اجرای پروژه نبینیم. به‌طور طبیعی، این کار می‌تواند منابع عظیمی را مصرف کرده و به‌کارگیری تیم‌های امنیتی زیادی را طلب کند.

مأموریت اصلی به‌عنوان بخشی از فرآیند، حفاظت از داده‌های دارنده کارت‌ها و امنیت تراکنش‌های انجام‌شده با این اطلاعات است. مدیریت دسترسی‌های ممتاز می‌تواند در تمام الزامات ۱۲ گانه‌ای که برای تطابق با PCI DSS است، در اشکال مختلفی اعم از دسترسی محدود تا فیلتر کردن خط دستور، کمک‌کننده باشد. شکل (۱۹-۱) دیاگرام سطح بالای الزامات PCI DSS را نشان می‌دهد. بر اساس این الزامات، مشاهده نحوه تأثیر PAM روی حقوق ویژه در هنگام استفاده از دیوارهای آتش به‌منظور محدود کردن دسترسی به داده‌های دارنده کارت، آسان است.

استاندارد امنیت داده PCI- مرور استانداردهای سطح بالا	
شبکه و سیستمی امن ساخته و امنیت آن را حفظ کنید	۱. یک پیکربندی دیوار آتش را برای حفاظت داده‌های دارنده کارت نصب کرده و آن را حفظ کنید؛ ۲. از پیش‌فرض‌های تأمین‌شده به‌وسیله فروشنده برای رمزهای عبور سیستم و دیگر پارامترهای امنیتی استفاده نکنید.
از داده‌های دارنده کار محافظت کنید	۳. از داده‌های ذخیره‌شده دارنده کارت محافظت کنید؛ ۴. داده‌های انتقالی دارنده کارت را در شبکه‌های باز و عمومی رمزگذاری کنید.
برنامه‌ای برای مدیریت آسیب‌پذیری داشته باشید	۵. از تمام سیستم‌ها در برابر بدافزار محافظت کنید و به‌صورت مرتب نرم‌افزارها و برنامه‌های ضدویروس را به‌روزرسانی کنید؛ ۶. سیستم‌ها و برنامه‌ها را به‌صورت امن توسعه داده و امنیت آن‌ها را حفظ کنید.
معیارهای کنترل دسترسی قدرتمندی را پیاده‌سازی کنید	۷. دسترسی به داده‌های دارنده کارت را محدود کنید؛ ۸. دسترسی به مؤلفه‌های سیستم را شناسایی کرده و احراز هویت نمایید؛ ۹. دسترسی فیزیکی به داده‌های دارنده کارت را محدود کنید.
شبکه‌ها را مرتباً تست کرده و نظارت کنید	۱۰. تمام دسترسی‌ها به منابع شبکه و داده‌های دارنده کارت را ردیابی کرده و نظارت کنید؛ ۱۱. سیستم‌ها و فرآیندهای امنیتی را به‌صورت مرتب تست کنید.
سیاست امنیت اطلاعاتی داشته باشید	۱۲. سیاستی داشته باشید که امنیت اطلاعات را برای تمام پرسنل در نظر بگیرد.

شکل (۱۹-۱). الزامات PCI DSS، سطح بالا

HIPAA

قانون انتقال و پاسخگویی الکترونیک بیمه سلامت[1] (HIPAA) که در سال ۱۹۶۶ به‌وسیله کنگره ایالات‌متحده به شکل قانون در آمد، تدارکاتی را برای حفاظت از پوشش بیمه سلامت برای کارگران و خانواده‌هایشان هنگامی‌که شغل خود را تغییر داده یا آن را از دست می‌دهند،

[1] Health Insurance Portability and Accountability Act

ارائه می‌کند و به ایجاد استانداردهای ملی برای تراکنش‌های الکترونیکی بهداشت و شناسه‌های ملی برای ارائه‌دهندگان، برنامه‌های بیمه سلامت و کارکنان نیاز دارد.

HIPAA به استانداردی عملی برای حفاظت از حریم خصوصی و امنیت اطلاعات سلامت شخصی در صنعت بهداشت و بر اساس مأموریت‌های اولیه آن بدل شد. قانون امنیت در HIPAA به‌طور اختصاصی به اطلاعات سلامت الکترونیکی حفاظت‌شده[1] (EPHI) می‌پردازد.

این قانون سه نوع حفاظت امنیتی را برای پیروی کردن بیان می‌کند:

- حفاظت‌های مدیریتی- سیاست‌ها و روندهای طراحی‌شده برای نشان دادن صریح نحوه موافقت و تطابق آن واحد با قانون؛
- حفاظت‌های فیزیکی- کنترل دسترسی فیزیکی به‌منظور حفاظت در برابر دسترسی نامناسب به داده‌های محافظت‌شده؛
- حفاظت‌های فنی- کنترل دسترسی به سیستم‌های کامپیوتری و فعال‌سازی واحدهای تحت پوشش به‌منظور حفاظت از ارتباطات شامل PHI (اطلاعات حفاظت-شده سلامت[2]) ارسالی از طریق ابزارهای الکترونیکی روی شبکه‌های باز برای جلوگیری از قطع ارتباط به‌وسیله هر شخص دیگری غیر از گیرنده موردنظر.

بر اساس این سه حفاظت، واضح است که اطلاعات سلامت بیمار باید در برابر عامل تهدید حفاظت شود. با وجودی که یک داده ثبتی سلامت می‌تواند هدفی برای این کار مخصوصاً برای داده‌های مرتبط با شخصی مشهور و یا مهم باشد اما داده‌های عظیم ارزش بیشتری برای وب تاریک[3] و مجرمان سایبری خرابکار دارد. دسترسی به مقدار زیادی از داده‌ها به دسترسی با حقوق ویژه نیاز دارد؛ بنابراین HIPAA به مدیریت دسترسی‌های ممتاز نیاز دارد و در این صورت ممکن است از مشکلات مشابهی مربوط به استفاده از حقوق ویژه به‌عنوان هدفی برای حمله رنج ببرد. جدول (۱۹-۱) بخش‌هایی از HIPAA را نشان می‌دهد که به‌وسیله PAM حل شده است:

[1] Electronic Protected Health Information
[2] Protected Health Information
[3] Dark Web

جدول (۱۹-۱). الزامات HIPAA که می‌توان آن‌ها را با PAM حل کرد

استاندارد HIPAA	مرجع
فرآیند مدیریت امنیت	164.308(a)(1)
مسئولیت امنیتی تخصیص‌یافته	164.308(a)(2)
امنیت نیروی کار	164.308(a)(3)
مدیریت دسترسی اطلاعات	164.308(a)(4)
آگاهی و آموزش امنیت	164.308(a)(5)
رویه‌های حوادث امنیت	164.308(a)(6)
برنامه‌های احتمالی	164.308(a)(7)
ارزیابی	164.308(a)(8)
قراردادهای مرتبط با کسب وکار و دیگر تمهیدات	164.308(b)(1)
کنترل‌های دسترسی به تجهیزات	164.310(a)(1)
استفاده از محل کار	164.310(b)
امنیت محل کار	164.310(c)
کنترل‌های دستگاه و رسانه	164.310(d)(1)
کنترل دسترسی	164.312(a)(1)
کنترل‌های حسابرسی	164.312(b)
یکپارچگی	164.312(c)(1)
احراز هویت شخص و واحد	164.312(d)
امنیت انتقال	164.312(e)(1)
قراردادهای مرتبط با کسب‌وکار و دیگر تمهیدات	164.314(a)(1)
الزامات برای برنامه‌های سلامت گروه	164.314(b)(1)
سیاست‌ها و رویه‌ها	164.316(a)
مستندسازی	164.316(b)(1)

SOX

در ماه جولای سال ۲۰۱۲، کنگره ایالات‌متحده قانون Sarbanes-Oxley (SOX) را تصویب کرد، قانونی که در ابتدا برای بازیابی اعتماد سرمایه‌گذار در ادامه ورشکستگی‌های عمومی طراحی شد که مدیران عامل، کمیته‌های حسابرسی و حسابرسان مستقل را تحت رسیدگی

سنگینی قرار داد. قانون به تمام شرکت‌هایی که به‌صورت عمومی ثبت شده‌اند و تحت صلاحیت کمیته امنیت و تبادل[1] (SEC) قرار دارند، اعمال می‌شود. داده‌ها و مستندات مالی مبحث اصلی این مسئله قانونی است و در بخش ۴۰۴ قانون SOX اشاره دارد که: ارزیابی کنترل‌های داخلی، مدیریت دسترسی‌های ممتاز و آسیب‌پذیری را به‌عنوان یک الزام کسب‌وکاری تعریف می‌کند. این کار به یک سازمان کمک می‌کند تا جریان تراکنش‌ها و جنبه‌های IT آن را درک کند و نقاطی را که ممکن است در آن‌ها بی‌نظمی وجود داشته باشد، تعیین نماید و سپس کنترل‌های طراحی‌شده برای جلوگیری یا شناسایی تقلب و کلاه‌برداری را مورد بررسی و ارزیابی قرار دهد. مورد آخر به‌طور واضح حقوق ویژه را به‌عنوان هدفی برای حمله و نظارت بر نشست‌ها در کانون شناسایی و جلوگیری از کلاه‌برداری و تقلب قرار می‌دهد.

GLBA

قانون گرام-لیچ-بلایلی[2] (GLBA) برای تضمین حفاظت از داده‌های ثبتی و اطلاعات مشتری، تصویب شده است. برای تحقق قوانین GLBA، مؤسسات مالی باید ارزیابی‌های ریسک امنیتی را اجرا کنند؛ راهکارهای امنیتی را توسعه داده و پیاده‌سازی نمایند که این امر به‌طور مؤثری رخدادها را شناسایی کرده، از موارد مشکوک جلوگیری می‌نماید و اجازه پاسخ به‌موقع به رخدادها را می‌دهد، همچنین اجازه می‌دهد تا حسابرسی و نظارت بر محیط امنیتی خود را انجام دهند. GLBA همانند قانون SOX، یک بخش کامل مبحث مدیریت ریسک را پوشش می‌دهد. بخش‌های اصلی قسمت ۵۰۸ مرتبط با حقوق ویژه به‌عنوان هدفی برای حمله شامل موارد زیر است:

- بند الف: افشای اطلاعات شخصی غیرعمومی- ساخت کامل [مدیریت ریسک] در هر دپارتمانی که اطلاعات غیرعمومی را مدیریت می‌کند؛
- بند ب: دسترسی جعلی به اطلاعات مالی- وقتی حملات مهندسی اجتماعی رخ می‌دهد، فردی سعی دارد تا به اطلاعات شخصی غیرعمومی به‌صورت غیرمجاز دسترسی پیدا کند.

[1] Security and Exchange Commision
[2] Gramm-Leach-Bliley Act

NIST

نشریه ۵۳-۸۰۰ اختصاصی NIST، کنترل‌های امنیتی و حریم خصوصی را برای سیستم‌ها و سازمان‌های اطلاعاتی فدرال، توسط نیروی کار مشترک متشکل از نمایندگان NIST، دپارتمان دفاع، جامعه اطلاعاتی و کمیته امنیت ملی توسعه داد و این مشارکت بین سازمانی در سال ۲۰۰۹ شکل گرفت. این راهبرد با تدارک مجموعه‌ای کامل از کنترل‌های امنیتی ضروری جهت تقویت سیستم‌های اطلاعاتی و همچنین محیط‌هایی که در آن‌ها فعالیت می‌کنند، رویکرد جامعی را برای مدیریت ریسک و امنیت اطلاعات ارائه می‌کند. سیستم‌های به‌دست‌آمده در مواجهه با تهدیدات و حملات سایبری، انعطاف‌پذیری بیشتری دارند.

NIST SP 800-53 یک استراتژی «Build It Righ» را با کنترل‌های امنیتی مختلف جهت نظارت مستمر مشخص می‌کند و سعی دارد تا مدیران ارشد سازمان‌های اطلاعاتی را در اتخاذ تصمیمات ریسکی لحظه‌ای مرتبط با مأموریت‌های حیاتی‌شان یاری کند. کنترل و نظارت دسترسی ممتاز برای کاهش ریسک‌های ناشی از تهدیدات داخلی، جلوگیری از نفوذ به داده‌ها و تحقق تطابق با الزامات، بسیار مهم است. بر همین اساس مدیران امنیت و IT باید بین حفاظت از داده‌های حیاتی سازمان جهت تضمین تداوم کسب‌وکار و یا ارائه امکان کارکرد با بهره‌وری بالا برای مدیران و کاربران، مسیر مشخصی را تبیین کنند. ابزارهای ناهمگون و متفرقه‌ای که در بخش‌های ایزوله، اجرا و مدیریت می‌شوند، باعث می‌شوند که شکاف‌هایی در دسترسی‌های ممتاز ایجاد شود. این مدل قدیمی هزینه بالا و همچنین مدیریت سختی داشته و به زمان زیادی برای نشان دادن کاهش ریسک نیاز دارد.

NIST این معضل را تشخیص داده و با اجرای تفکیک بین وظایف، کنترل تغییر و حسابرسی نشست‌های ممتاز، عمل فرمالیزه را انجام می‌دهد. این موضوع به‌صورت مشخص نحوه مدیریت دسترسی توسط سازمان را مشخص می‌کند. متأسفانه اندازه و محدوده نگاشت دقیق PAM به NIST SP 800-83 بسیار گسترده است. اگر سازمان شما الزامات NIST را دارد، لطفاً از مشاورهای خارجی بهره بگیرید (و یا اگر منابع آن را دارید از متخصصان داخلی استفاده کنید) تا الزامات کسب‌وکاری خود را با قراردادهای دقیق مشخص کنید. محدوده حتی ممکن است شامل زنجیره تأمین سازمان شما شود و البته به غیر از حسابرسی‌های مبتنی بر قرارداد، کاملاً خارج از کنترل شما باشد.

ISO

سازمان بین‌المللی استانداردسازی[1] (ISO) راهبردها و اصول کلی را برای آغاز، پیاده‌سازی، نگهداری و بهبود مدیریت امنیت اطلاعات در یک سازمان تبیین کرده است. اهدافی که در ISO 27002:2013(E) مشخص شده است، راهبردی کلی را برای اهداف معمول موردقبول از مدیریت امنیت اطلاعات ارائه می‌کند.

اهداف کنترلی و کنترل‌ها در ISO 27002 با قصد پیاده‌سازی جهت تحقق الزامات مشخص‌شده به‌وسیله یک ارزیاب ریسک تبیین شده‌اند. ISO 27002 می‌تواند به‌عنوان یک راهبرد عملی برای توسعه استانداردهای امنیت سازمانی و راهکارهای مدیریت امنیت عمل کند و به ایجاد اعتماد در فعالیت‌های سازمانی کمک نماید.

برای سازمان‌هایی که ISO 27002 را به کار گرفته‌اند، اینکه تمام راهکارهای موجود و جدید امنیتی در قالب این چهارچوب باشند، اهمیت دارد. استاندارد شامل ۱۴ ماده برای کنترل امنیت است که در مجموع شامل ۳۵ گروه امنیتی اصلی و ۱۱۴ کنترل است. هدف هر سازمانی، چه دستیابی به تطابق قانونی باشد و چه به‌کارگیری بهترین راهکارهای امنیت، این کنترل‌ها قابل اعمال و اجرا در اکثر سازمان‌ها و شرکت‌ها هستند. این ماده استانداردها به‌طور مستقیم به مدیریت دسترسی‌های ممتاز و نظارت نشست ممتاز ترجمه می‌شوند. جدول (۱۹-۲) گروه‌ها و کنترل‌های تأثیرپذیر از ISO 27002 و PAM را نشان می‌دهد.

[1] International Organization for Standardization

جدول (۱۹-۲). نگاشت PAM برای ISO 27002:2013(E)

۶ سازمان امنیت اطلاعات
۶ – ۱ سازمان داخلی
۶ – ۱ – ۱ نقش‌ها و مسئولیت‌های امنیت اطلاعات
۶ – ۱ – ۲ تفکیک وظایف
۶ – ۱ – ۵ امنیت اطلاعات در مدیریت پروژه
۶ – ۲ دستگاه‌های قابل حمل و دورکاری
۶ – ۲ – ۲ دورکاری
۸ مدیریت دارایی‌ها
۸ – ۱ مسئولیت دارایی‌ها
۸ – ۱ – ۳ استفاده پسندیده از دارایی‌ها
۸ – ۲ طبقه‌بندی اطلاعات
۸ – ۲ – ۳ اداره دارایی‌ها
۹ کنترل دسترسی
۹ – ۱ الزامات کسب‌وکار برای کنترل دسترسی
۹ – ۱ – ۱ خط‌مشی کنترل دسترسی
۹ – ۱ – ۲ دسترسی به شبکه‌ها و سرویس‌های شبکه
۹ – ۲ مدیریت دسترسی کاربر
۹ – ۲ – ۱ ثبت و حذف کاربر
۹ – ۲ – ۲ تأمین مجوز دسترسی کاربر
۹ – ۲ – ۳ مدیریت حق دسترسی ویژه
۹ – ۲ – ۴ مدیریت اطلاعات محرمانه احراز هویت کاربران
۹ – ۲ – ۵ بازنگری حقوق دسترسی کاربر
۹ – ۳ مسئولیت‌های کاربر
۹ – ۳ – ۱ استفاده از اطلاعات محرمانه احراز هویت
۹ – ۴ کنترل دسترسی سیستم‌ها و برنامه‌ها
۹ – ۴ – ۱ محدودیت دسترسی به اطلاعات
۹ – ۴ – ۲ رویه‌های ورود امن
۹ – ۴ – ۳ سیستم مدیریت کلمه عبور
۹ – ۴ – ۴ استفاده از برنامه‌های کمکی ویژه
۹ – ۴ – ۵ کنترل دسترسی به کد منبع برنامه

۱۰ رمزنگاری

۱۰ – ۱ کنترل‌های رمزنگاری

۱۰ – ۱ – ۲ مدیریت کلید

۱۲ امنیت عملیات

۱۲ – ۱ رویه‌های عملیاتی و مسئولیت‌ها

۱۲ – ۱ – ۲ مدیریت تغییر

۱۲ – ۴ واقعه‌نگاری و پایش

۱۲ – ۴ – ۱ ثبت رویداد

۱۲ – ۴ – ۲ حفاظت از اطلاعات ثبت‌شده رویدادها

۱۲ – ۴ – ۳ ثبت رویدادهای مدیر و اپراتور سیستم

۱۲ – ۵ کنترل نرم‌افزارهای عملیاتی

۱۲ – ۵ – ۱ نصب نرم‌افزار بر روی سیستم‌های عملیاتی

۱۲ – ۷ ملاحظات ممیزی سیستم‌های اطلاعاتی

۱۲ – ۷ – ۱ کنترل‌های ممیزی سیستم‌های اطلاعاتی

۱۳ امنیت ارتباطات

۱۳ – ۱ مدیریت امنیت شبکه

۱۳ – ۱ – ۱ کنترل‌های شبکه

۱۳ – ۱ – ۲ امنیت سرویس‌های شبکه

۱۳ – ۱ – ۳ تقسیم‌بندی شبکه‌ها

۱۳ – ۲ انتقال اطلاعات

۱۳ – ۲ – ۱ خط‌مشی‌ها و رویه‌های انتقال اطلاعات

۱۴ اکتساب، توسعه و نگهداری از سیستم

۱۴ – ۱ الزامات امنیتی سیستم‌های اطلاعاتی

۱۴ – ۱ – ۱ تحلیل و تعیین الزامات امنیت اطلاعات

۱۴ – ۲ امنیت در فرآیندهای توسعه و پشتیبانی

۱۴ – ۲ – ۱ خط‌مشی‌های توسعه امن

۱۴ – ۲ – ۶ محیط توسعه امن

۱۴ – ۳ داده‌های آزمون

۱۴ – ۳ – ۱ حفاظت از داده‌های آزمون

۱۶ مدیریت رخدادهای امنیت اطلاعات

۱۶ – ۱ مدیریت و بهبود رخدادهای امنیت اطلاعات

۱۶ – ۱ – ۱ مسئولیت‌ها و رویه‌ها

۱۶ – ۱ – ۲ گزارش‌دهی رویدادهای امنیت اطلاعات

۱۶ – ۱ – ۳ گزارش‌دهی نقاط ضعف امنیت اطلاعات

۱۶ – ۱ – ۴ ارزیابی و تصمیم‌گیری درباره رویدادهای امنیت اطلاعات

۱۶ – ۱ – ۷ جمع‌آوری شواهد

۱۷ جوانب امنیت اطلاعات در مدیریت تداوم کسب‌وکار

۱۷ – ۱ تداوم امنیت اطلاعات

۱۷ – ۱ – ۱ طرح‌ریزی تداوم امنیت اطلاعات

۱۷ – ۱ – ۲ پیاده‌سازی تداوم امنیت اطلاعات

۱۷ – ۱ – ۳ بررسی، بازنگری و ارزیابی تداوم امنیت اطلاعات

۱۷ – ۲ افزونگی‌ها

۱۷ – ۲ – ۱ دسترسی‌پذیری امکانات پردازش اطلاعات

۱۸ انطباق

۱۸ – ۱ انطباق با الزامات قانونی و قراردادی

۱۸ – ۱ – ۲ حقوق مالکیت معنوی

۱۸ – ۱ – ۳ حفاظت از سوابق

۱۸ – ۲ بازنگری‌های امنیت اطلاعات

۱۸ – ۲ – ۱ بازنگری مستقل امنیت اطلاعات

۱۸ – ۲ – ۲ انطباق با خط‌مشی‌ها و استانداردهای امنیتی

۱۸ – ۲ – ۳ بازنگری انطباق فنی

best practice های امنیتی در همه مقررات و چهارچوب‌ها بکار رفته‌اند. ISO 27002 نیز از این قاعده مستثنی نیست به‌طور مثال وقتی نظارت و مدیریت حقوق ویژه و نشست‌ها بخش پایه‌ای از مدیریت اهداف حمله دارای حقوق ویژه و خنثی کردن عاملان تهدید هستند. نگاشت این کنترل‌ها به مدل اجرایی مدیریت دسترسی‌های ممتاز شما را در محفوظ نگه داشتن بیشتر اهداف حمله‌ای که آن‌ها را مورد بحث قرار دادیم، کمک می‌کند.

ASD

مدیریت سیگنال‌های استرالیا[1] (ASD) لیستی از استراتژی‌ها را برای کاهش نفوذهای سایبری هدف‌دار توسعه داده است. استراتژی‌های کاهشی توصیه‌شده از سوی ASD، حاصل تجربه گسترده آن‌ها در عملیات امنیت سایبری شامل اجرای ارزیابی‌های آسیب‌پذیری و تست نفوذ، پاسخ به نفوذهای سایبری جدی و غیره است و برای سازمان‌های دولتی استرالیا در سال ۲۰۱۴ توسعه داده شده است.

در سال ۲۰۱۷، ASD چهار توصیه برتر را برای تشکیل هشت‌گانه ضروری، با افزودن چهار توصیه دیگر گسترش داد. طبیعت پویای امنیت سایبری به یک اصلاح برای حل آخرین تهدیدات مثل باج‌افزارها نیاز داشت. شرکت‌ها و دولت‌ها به ایجاد تغییرات اساسی که غالباً هر چند سال رخ می‌دهد، عادت کرده‌اند ولی به‌ندرت توصیه‌هایی تبیین می‌شوند که برای مدیریت تهدیداتی خاص بسیار دقیق باشند. این هشت توصیه ضروری به‌صورت زیر هستند:

چهار توصیه برتر مدیریت سیگنال‌های استرالیا (توصیه‌های اصلی تبیین‌شده در سال ۲۰۱۴)

۱. تهیه لیست سفید از برنامه‌های دارای مجوز/ مورد اعتماد به‌منظور جلوگیری از اجرای برنامه‌های مخرب یا تأییدنشده است که شامل فایل‌های اجرایی، اسکریپت‌ها و نصب-کننده‌ها[2] است؛

۲. وصله کردن برنامه‌ها- مثل برنامه‌های جاوا، نمایشگرهای PDF، FLASH، مرورگر وب و مایکروسافت آفیس. آسیب‌پذیری‌های با ریسک بالا در سیستم‌ها را در طی دو روز وصله کنید، آخرین نسخه اپلیکیشن‌ها استفاده شود؛

۳. وصله کردن آسیب‌پذیری‌های سیستم‌عامل. آسیب‌پذیری‌های با ریسک بالا در سیستم‌عامل‌ها را در طی دو روز وصله‌سازی کنید، استفاده از آخرین نسخه مناسب سیستم عامل و پرهیز از استفاده از ویندوز ایکس‌پی؛

[1] Australian Signals Directorate
[2] Installers

۴. محدود کردن حقوق ویژه مدیریتی به سیستم‌عامل‌ها و برنامه‌ها بر اساس وظایف کاربر. چنین کاربرانی باید از یک حساب بدون حقوق ویژه برای ایمیل و جستجو در وب استفاده کنند.

[توصیه‌های] هشت‌گانه ضروری (اصلاح‌شده در سال ۲۰۱۷)

الف. غیرفعال کردن ماکروهای غیرقابل‌اعتماد مایکروسافت آفیس، بدین منظور که بدافزاری نتواند کارهای روتین غیرمعتبری را اجرا کند؛

ب. مسدودسازی مرورگر وب از دسترسی به اَدوبی فِلَش، تبلیغات وب و کدهای نامطمئن جاوا در اینترنت. در صورت امکان، حذف تمام افزونه‌های غیر ضروری مرورگر؛

ج. احراز هویت چند مرحله‌ای برای تمام سیستم‌ها در صورت امکان تا دسترسی مهاجم به یک سیستم یا اطلاعات را سخت‌تر کنیم؛

د. پشتیبان‌گیری روزانه از داده‌های مهم به‌صورت امن و آفلاین به‌منظور اینکه حتی در صورت به خطر افتادن داده‌ها، نسخه‌های حفاظت‌شده برای بازیابی در دسترس باشند.

بر اساس روش‌های عامل تهدید برای دسترسی به حقوق ویژه، این توصیه‌ها کاملاً در راستای تهدیداتی هستند که به‌وسیله مدیریت دسترسی‌های ممتاز حل شده‌اند. اهداف حمله دارای حق ویژه در چهار توصیه برتر قرار داده شده است و یک رویکرد کاهشی را بیان می‌کند که باید در سطح سراسری برای متوقف ساختن تهدیدات پیشرفته مورد استفاده قرار گیرد.

MAS

مؤسسه مالی سنگاپور[1] (MAS) در سال ۱۹۷۱ تأسیس شد تا بر عملکردهای مختلف مرتبط با مؤسسات مالی و بانکی نظارت کند. طی این سال‌ها، راهبردهای آن‌ها برای مدیریت فناوری‌های در حال ظهور و چشم‌انداز در حال تکامل تهدیدات، مورد بازبینی قرار گرفته است. در ماه ژوئن سال ۲۰۱۳، MAS مجموعه جدیدی از راهبردها را برای بانکداری اینترنتی و مدیریت ریسک فناوری[2] (IBTRM) ایجاد کرده است. این الحاقیه الزامات خاصی را برای

[1] Monetary Authority of Singapore
[2] Internet Banking and Technology Risk Management

مدیریت ریسک فناوری (TRM) حکم می‌کند و شامل مجموعه‌ای از راهبردها (راهبردهای TRM) نیز می‌شود و در کنار آن اطلاعیه‌هایی (اطلاعیه‌های TRM) برای غلط‌های موجود در نحوه نگارش نیز وجود دارد.

راهبردهای TRM بیانیه‌هایی از بهترین‌های موجود است که انتظار می‌رود تا مؤسسات مالی آن‌ها را به کار گیرند. این راهبرد از نظر قانونی لازم‌الاجرا نیست ولی در حسابرسی‌های ریسک مؤسسات مالی به‌وسیله MAS مورد استفاده قرار می‌گیرد. حقوق ویژه به‌عنوان اهدافی برای حمله چهار مورد از این بخش‌ها را که مرتبط با حفاظت از حقوق ویژه در برابر عامل تهدید است، به کار می‌گیرند:

- بخش ۴: چهارچوب ریسک فناوری؛
- بخش ۶: اکتساب و توسعه سیستم‌های اطلاعاتی؛
- بخش ۹: مدیریت امنیت زیرساخت عملیاتی؛
- بخش ۱۱: کنترل دسترسی.

GDPR

مقررات حفاظت از اطلاعات عمومی[1] (GDPR) در سالیان اخیر یکی از مهم‌ترین جنبش‌ها در حوزه حفاظت از داده‌ها است. این مقررات در ۲۸ آوریل سال ۲۰۱۶ وارد قوانین اتحادیه اروپا (EU) شد و در ۲۵ ماه مِی سال ۲۰۱۸ اجرایی شد. به‌طور خلاصه، GDPR کنترل‌هایی را در مورد نحوه ذخیره‌سازی و پردازش داده‌های شخصی شهروندان اروپا تعریف می‌کند که مستقل از محل قرارگیری، مالکیت و عملکرد سازمان است. هر کسی که داده‌های شخصی یک شهروند از اتحادیه اروپا را ذخیره‌سازی و یا پردازش می‌نماید باید طبق مقررات GDPR پیش برود، در غیر این صورت هنگام حسابرسی و یا رخنه‌ای در داده‌ها با جریمه‌های قابل‌توجهی روبرو می‌شوند. این جریمه‌ها می‌توانند تا ۴٪ از گردش مالی کلی سازمان و یا ۱۰ میلیون یورو باشد. با این سطح از تأثیرگذاری، ضروری است که تمام سازمان‌ها تعهدات خود تحت GDPR را درک کرده و معیارهای مناسبی را برای تضمین اینکه با این مقررات سازگار هستند، به کار گیرند که نشان دهند کنترل‌های مناسبی برای حفاظت اطلاعات دارند.

[1] General Data Protection Regulation

GDPR برای ساده‌سازی الزامات کنونی طراحی شده است و بار جدید سنگینی را بر سازمان‌ها تحمیل نمی‌کند. درواقع، GDPR توانسته ۲۸ پیاده‌سازی متفاوت از دستورالعمل حفاظت از داده‌های قبلی (95/46/EC) را در قالب یک واحد جمع کرده تا ثبات، کنترل نسخه استاندارد و گزارشی را در پی داشته باشد. شایان ذکر است که این مقررات به سازمان‌های اجرای قانونی که ممکن است به تبادل این اطلاعات به‌عنوان بخشی از یک تحقیق و بازجویی نیاز داشته باشند، اعمال نمی‌شود.

برای رسیدن به این هدف، راهکارهای PAM که مبتنی بر بهترین روش‌های امنیتی برای دسترسی‌های ممتاز هستند، می‌توانند به سازمان‌ها کمک کنند تا با توسعه مبنای امنیت سایبری قوی اما ساده به GDPR دست یابند. این کار با حل ابهام حریم خصوصی و از طریق ویژگی‌های استاندارد PAM انجام می‌شود:

- مدیریت رمز عبور ممتاز می‌تواند به کنترل شخصی که به سیستم‌عامل‌ها، برنامه‌ها، پایگاه‌های داده، زیرساخت و منابع ابری دسترسی دارد، کمک نماید و گزارش تصدیقی از فعالیت نشست برای کاربرانی که به داده‌ها و منابع حساس دسترسی دارند، ارائه می‌دهد؛
- مدیریت حقوق ویژه در سرورها می‌تواند دسترسی‌های ممتاز به برنامه‌ها و دستورات را مدیریت کند. آن‌هایی که نیاز به دسترسی روت و sudo داشته و امکان دارد سبب افشای داده‌های حساس کاربر گردد، حذف می‌کند.

SWIFT

چهارچوب شماره ۱ از کنترل‌های امنیت مشتری SWIFT در ۳۱ ماه مارس از سال ۲۰۱۷ منتشر شد که مجموعه‌ای از کنترل‌های امنیتی پیشنهادی و اجباری را برای سازمان‌های مالی شرکت‌کننده در SWIFT تشریح می‌نماید. این چهارچوب به سه هدف تقسیم‌بندی می‌شود:

- امن‌سازی محیط
  - محدودسازی دسترسی اینترنت
  - حفاظت از سیستم‌های حیاتی از محیط کلی IT (اقدامات بعدی)
  - کاهش سطح حمله و آسیب‌پذیری‌ها
  - امن‌سازی فیزیکی محیط

- شناختن و محدودسازی دسترسی
  - جلوگیری از به خطر افتادن اعتبارنامه‌ها
  - مدیریت هویت‌ها و جداسازی حقوق ویژه (PAM)
- شناسایی و پاسخ
  - شناسایی فعالیت‌های غیرعادی در سیستم‌ها یا رکوردهای تراکنش‌ها
  - برنامه‌ریزی برای پاسخ‌دهی به حوادث و اشتراک‌گذاری اطلاعات

SWIFT نیاز دارد تا کاربران انطباق با کنترل‌های امنیتی اجباری را خودشان تصدیق نمایند (این کار برای کنترل‌های پیشنهادی، اختیاری است) و مهلت آن در ابتدای ماه ژانویه سال ۲۰۱۸ بود تا اظهارات خودشان را ارائه کنند. PAM کنترل‌های اجباری زیر را تحت پوشش قرار می‌دهد:

۱ – ۱ کنترل حساب ممتاز سیستم‌عامل

۲ – ۱ امنیت جریان داده‌های داخلی

۲ – ۲ به‌روزرسانی‌های امنیتی

۲ – ۳ مقاوم‌سازی سیستم

۲ – ۶ محرمانگی و یکپارچگی نشست یک اپراتور

۲ – ۸ برون‌سپاری یک فعالیت حیاتی

۴ – ۱ خط‌مشی رمز عبور

۴ – ۲ احراز هویت چند مرحله‌ای

۵ – ۱ کنترل دسترسی منطقی

۵ – ۴ فضای ذخیره‌سازی فیزیکی و منطقی رمز عبور

۶ – ۲ یکپارچگی نرم‌افزار

۶ – ۴ واقعه‌نگاری و پایش

سازمان‌ها می‌توانند انطباق و الزامات امنیتی را با توجه به تعریف ارائه‌شده در چهارچوب کنترل‌های امنیتی مشتری SWIFT به وسیله پیاده‌سازی راهکارهای PAM حل کنند. دقت داشته باشید که اگر سازمان شما در حال حاضر چهارچوب امنیت سایبری NIST، ISO 27002 و یا PCI DSS را اتخاذ کرده است، SWIFT نگاشت‌هایی را به دیگر چهارچوب‌ها به‌منظور تسریع در تأیید انطباق ارائه می‌دهد و تلاش‌ها را برای گزارش ارزیابی، دو برابر نمی‌کند.

فصل ۲۰

نمونه کاربردهای مدیریت دسترسی‌های ممتاز (PAM)

عامل تهدید سعی دارد تا با بهره‌گیری از نقاط ضعف فرآیندها و ناتوانی سازمان‌ها در ایجاد بهترین روش‌های امنیتی و یا حتی دنبال کردن فرآیندها، کار خود را انجام دهد. برای رسیدن به این هدف، مدیریت دسترسی‌های ممتاز می‌تواند مانع عامل تهدید شود، حتی اگر از بهترین راهکارهای امنیتی استفاده شده باشد. برای به موفقیت رساندن آن، این سه مشکل بزرگ را که هر سازمانی با آن مواجه است و راهکارهای حل آن‌ها را در نظر بگیرید:

۱. کارکنان و دیگر افراد درون سازمان دسترسی‌هایی غیرضروری دارند: کارکنان، شرکت‌ها و دیگر افراد درون‌سازمانی اغلب دسترسی‌های زیادی به سیستم‌ها و داده‌ها دارند و ممکن است این دسترسی‌ها تحت نظارت نیز نباشند؛
۲. اعتبارنامه‌ها به اشتراک گذاشته شده و مدیریت نمی‌شوند: رمزهای عبور ایجاد شده و به اشتراک گذاشته می‌شوند ولی بر اساس نظام یا مسئولیت‌پذیری، حسابرسی، نظارت و حتی مدیریت نمی‌شوند؛
۳. تجهیزات فناوری اطلاعات (IT) بدون بررسی ارتباطاتی را برقرار می‌کنند: دسکتاپ‌ها، لپ‌تاپ‌ها، سرورها و برنامه‌ها ارتباطاتی برقرار کرده و مسیرهایی را به دارایی‌ها و داده‌های حساس باز می‌کنند.

حتی با در نظر گرفتن بهترین راهکارهای امنیتی، این سه مشکل می‌تواند خود را در تمامی قسمت‌ها نشان دهد. کاربردهای بیان‌شده در جدول (۲۰-۱) را برای حل این سه مسئله با کاربردهایی از PAM که می‌تواند آن‌ها را برای هر سازمانی حل کند، در نظر بگیرید.

جدول (۲۰-۱). کاربردهای PAM

عنوان			
چالش	نیاز	راه‌حل	مزیت
وظایفی که به اعتبارنامه‌های مدیریتی نیاز دارند			
برخی برنامه‌ها برای عملکرد خود نیاز به اعتبارنامه‌هایی با حقوق ویژه دارند. سیاست‌های امنیتی، اعتبارنامه‌های مدیریتی یا روت را به کاربران به‌منظور تکمیل وظایفشان ارائه نمی‌دهد.	کاربران باید برنامه‌هایی را اجرا کنند که به حقوق ویژه‌ای بالاتر از یک کاربر استاندارد نیاز دارند.	پیاده‌سازی یک راهکار حقوق ویژه حداقلی برای تغییر حقوق ویژه اپلیکیشن یا اعمال اعتبارنامه‌های ممتاز به اپلیکیشن	کاربران می‌توانند وظایف مورد نظر خود را اجرا کنند و سیاست‌های امنیتی با عدم ارائه اعتبارنامه‌های ممتاز رعایت می‌شوند.
اعتبارنامه‌های محلی، رمزهای عبور قدیمی دارند			
حساب‌های محلی رمزهای عبور قدیمی دارند که دوباره استفاده شده، شناخته شده‌اند و یا هرگز روی سرورها، دسکتاپ‌ها، لپ‌تاپ‌ها و تبلت‌ها تغییر نکرده‌اند.	بهترین راهکارهای امنیتی و سازگاری با قوانین به مدیریت رمزهای عبور دارای حقوق ویژه نیاز دارد و این امر رمزهای عبور دوباره استفاده‌شده، شناخته‌شده و مدیریت‌نشده را کاهش می‌دهد.	استفاده از یک راهکار مدیریت رمز عبور یا فناوری عامل، روشی را برای شناسایی اعتبارنامه‌هایی که جهت ورود کاربران و سرویس‌ها مورد استفاده قرار گرفته نشان می‌دهد و آن‌ها را تحت مدیریت قرار می‌دهد.	از مدیریت اعتبارنامه‌ها با بهره بردن از بهترین روش‌های امنیتی اطمینان حاصل می‌کند و حتی تضمین می‌دهد که دستگاه‌های قابل‌حمل را می‌توان در برابر استفاده دوباره رمز عبور و مشکل رمزهای قدیمی محافظت کرد.

همبستگی و مقاوم‌سازی نام‌های مستعار حساب‌ها			
سازمان‌ها نام‌های مستعار محلی و سرویس‌های دایرکتوری زیادی را با شناسه های یکسانی دارند که امر شناسایی را دشوار می‌کند.	سازمان‌ها و مقررات به شناسایی قابل اطمینان فعالیت‌های کاربر نیاز دارند. با نام‌های مستعار مجزا، این نگاشت به کار دشواری بدل می‌شود.	استفاده از یک فناوری پل زدن بین دایرکتوری‌ها برای تمام محیط‌های یونیکس، لینوکس و مَک جهت متمرکز ساختن احراز هویت از طریق اکتیو دایرکتوری	تضمین می‌کند که حساب دایرکتوری یک هویت فعال، همان حساب دارای اختیار برای تمام پلتفرم‌ها است و نام‌های مستعار محلی را حذف می‌کند.
همبستگی برنامه‌های آسیب‌پذیر و استفاده از آن‌ها			
برنامه‌های تحلیل تهدید و مدیریت آسیب‌پذیری فاقد همبستگی برنامه-های آسیب‌پذیر و استفاده آن‌ها در دنیای واقعیت هستند.	سازمان‌ها آسیب‌پذیری‌ها را بر اساس رفتار کاربر و استفاده از اپلیکیشن اولویت‌بندی کنند.	استفاده از اپلیکیشن را با جزئیات دقیق ردیابی کنید و نتایج را برای شناخت آسیب‌پذیری‌ها ترسیم نمایید.	کنترل برنامه‌ها از طریق قرار دادن آن‌ها در لیست‌های سفید، سیاه و خاکستری بر اساس آسیب‌پذیری‌ها، عمر و ریسک.
حذف حقوق ویژه مدیریتی کاربر نهایی			
بهترین راهکارهای امنیتی، انطباق-پذیری با مقررات و کاهش تهدیدها همگی به مدیریت حقوق ویژه نیاز دارند.	حقوق مدیریتی را از تمام کاربران نهایی حذف کنید درحالی‌که عملکرد و بهره‌وری کاربرها دچار تأثیر نشود.	یک راهکار حداقل حقوق ویژه را پیاده‌سازی کنید که می‌تواند وظایف برنامه‌ها و سیستم‌های عامل را برای حقوق ویژه، بدون ارائه اعتبارنامه‌های مدیریتی به کاربر نهایی مورد هدف قرار دهد.	کاهش ریسک به‌وسیله پرهیز از بالا بردن حقوق مبنا، کاهش بدافزار از طریق حذف حقوق ویژه، هزینه کلی کمتر برای مالک، انطباق‌پذیری با مقررات و حساب‌های مدیریتی کمتر.

حذف حقوق مدیریتی سرور			
بهترین راهکارهای امنیتی، انطباق-پذیری با مقررات و کاهش تهدیدها، همگی به مدیریت حقوق ویژه و نظارت فعالیت نشست در زمان دسترسی به سرورها نیاز دارد.	حذف حقوق مدیریتی یا روت از مدیران درحالی‌که برای آن‌ها امکان حفظ بهره‌وری در سرورها، بر اساس سیستم‌های عامل داده می‌شود.	پیاده‌سازی یک راهکار حقوق ویژه حداقلی که می‌تواند برنامه‌ها، پایگاه داده‌ها و وظایف سیستم‌عامل‌ها را برای حقوق ویژه بدون ارائه اعتبارنامه-های واقعی برای حساب‌های محلی و مدیریتی دامنه، مورد هدف قرار دهد.	کاهش ریسک به‌وسیله اجرای کنترل تغییر، کاهش بدافزار از طریق حذف حقوق ویژه، انطباق‌پذیری با مقررات و مدیریت کامل نشست.
حذف رمزهای عبور اپلیکیشن به اپلیکیشن			
برنامه‌ها، سرویس‌ها و پایگاه‌های داده به اعتبارنامه‌ها یا گواهی‌هایی برای عملکرد صحیح نیاز دارند چون فرآیندهای آن‌ها برای منابع محلی یا از راه دور احراز هویت می‌شود.	قابلیت حذف رمز عبورهای قدیمی و استاتیک درون برنامه‌ها و جایگزینی آن‌ها با فراخوانی توسط API یا جایگزینی‌های برنامه‌نویسی‌شده	پیاده‌سازی یک راهکار مدیریت کلمه عبور با قابلیت جایگزینی رمزهای عبور در برنامه‌ها یا عوض کردن فراخوانی‌های API در برنامه‌ها به-منظور حذف رمزهای عبور یا گواهی‌های تعریف‌شده توسط کاربر یا نوشته‌شده در کد برنامه‌ها.	رمزهای عبور یا گواهی‌های استفاده-شده بین برنامه‌ها، دیگر درون کد برنامه نیستند و قدیمی نمی‌شوند و می‌توان آن را با یک مدیریت کننده رمز عبور، مدیریت کرد.

گردش کاری کنترل تغییر، به تأییدات نیاز دارد			
کنترل تغییر به حقوق ویژه مدیریتی یا روت نیاز دارد که تأیید از سوی اعضاء تیم قبل از اجرا را ضروری می‌نماید.	راه‌اندازی گردش کاری که با اعضاء تیم ارتباط برقرار می‌کند، به تأییدیه یا رد یا دسترسی ممتاز به میزبان نیاز دارد تا وظایف ممتاز تحت نظارت کنترل تغییر را تکمیل نماید.	پیاده‌سازی یک مدیریت رمز عبور یا راهکار حقوق ویژه حداقلی که موتور گردش کاری (به‌صورت داخلی یا سازگار با راهکارهای ثالث) دارد تا بتواند وقتی تأییدیه دریافت شد، دسترسی را ردیابی کرده، گزارش داده و ارائه کند.	مدیریت تغییر، بهترین روش‌های امنیتی و تأیید گردش کاری و الزامات را می‌توان برای دسترسی ممتاز محقق کرد.
کاهش تهدیدات برای دسترسی به زیرساخت			
زیرساخت‌هایی که مبتنی بر سرور نیستند، مثل مسیریاب‌ها، سوئیچ‌ها، دیوارهای آتش، بالانسِرهای بار، دوربین‌ها، سیستم‌های امنیتی، iDracها و غیره، معمولاً رمز عبور یکسانی در چندین دستگاه دارند (استفاده دوباره از رمز عبور) یا رمزهای عبور قدیمی دارند که منجر به ریسک و افشای بی‌دلیل آن‌ها می‌شود.	ارائه یک مکانیزم برای مدیریت رمزهای عبور زیرساخت، تضمین اینکه همه منحصربه‌فرد هستند و تغییر (مدیریت) خودکار آن‌ها به‌صورت دوره‌ای برای اطمینان از اینکه قدیمی نمی‌شوند.	پیاده‌سازی یک راهکار مدیریت رمز عبور که قادر است تا دستگاه‌های زیرساختی را کشف کرده و دسته‌بندی نماید و رمزهای عبور را به‌صورت دوره‌ای برای هر حساب مدیریت‌شده، مدیریت کند (تغییر دهد).	کاهش ریسک و اجرای بهترین راهکار امنیتی برای داشتن رمزهای عبور یکتا برای هر دستگاه و تغییر خودکار رمزهای عبور به‌منظور جلوگیری از نشر یا افشا شدن رمزهایی که قدیمی هستند.

ورود خودکار بدون افشاء اعتبارنامه			
ارائه دسترسی به یک منبع بدون افشاء اعتبارنامه‌ها. اتفاقی که قرار است پس از منتشر شدن یک رمز عبور رخ دهد را چطور کنترل کنیم؟	قابلیت ورود به یک منبع (اپلیکیشن، سیستم‌عامل، پایگاه داده و غیره) بدون افشاء اعتبارنامه‌ها و فراهم آوردن فرصت خرابکاری برای کاربر یا تهدید داخلی با کپی یا استفاده دوباره از اعتبارنامه‌ها.	پیاده‌سازی یک راهکار مدیریت رمز عبور و یا حقوق ویژه حداقلی که می‌تواند به‌صورت خودکار اعتبارنامه‌ها را برای احراز هویت و بدون نشان دادن آن‌ها به کاربر نهایی ارسال کند.	کاربران به‌صورت خودکار وارد می‌شوند و می‌توان نشست را برای فعالیت‌های مخرب احتمالی مورد نظارت قرار داد.
مستندسازی فعالیت‌های ممتاز برای حسابرسی و درست بودن فعالیت‌ها			
تعیین اینکه کاربر طی یک نشست چه کاری انجام داده و هشدار دادن در صورت بروز هرگونه فعالیت نامناسب مخصوصاً هنگام استفاده از حساب‌های مدیریتی یا اشتراکی.	راهکاری که بتواند ویدیو ضبط کند، کلیدهای فشرده‌شده را ثبت کند و فعالیت‌های اپلیکیشن را به‌صورت گزارش و ایندکس‌شده جهت بازبینی توسط تیم‌ها و حسابرسان امنیتی ارائه دهد.	پیاده‌سازی یک فناوری که بتواند این قابلیت را (ضبط نشست، ثبت کلیدها و فعالیت اپلیکیشن) در هنگام برقراری یک نشست یا استفاده از فناوری‌های پروکسی یا عامل ارائه کند. نتایج را باید در یک پایگاه داده ذخیره نمود، رمزگذاری کرد و به‌گونه‌ای محافظت کرد که در صورت نیاز بتوان از آن‌ها در مراجع قانونی بهره برد.	فعالیت نشست را می‌توان برای وجود اشتباهات، فعالیت خرابکارانه، آموزش و یا حتی تحت تعقیب قرار دادن نفوذ مورد بازبینی قرار داد.

ارائه یک واسط دسترسی به منابع ابری			
محدود کردن ریسک افشای ارتباط با منابع ابری به‌وسیله محدودسازی دسترسی‌های ممتاز به منابع و موقعیت‌های مکانی مورد اعتماد.	پیاده‌سازی فرآیندهای امنیتی و فناوری‌هایی که بتوانند دسترسی ممتاز به منابع ابری را کنترل کنند و تضمین نمایند این منابع از راه دور و به‌وسیله عاملان تهدید آلوده نمی‌شوند.	پیاده‌سازی یک سرویس واسط دسترسی ابری یا نشست پروکسی از راه دور که می‌تواند اتصالات از سمت کاربران، اعتبارنامه‌ها و موقعیت‌ها را مدیریت کند.	این کار لایه‌ای از امنیت را برای سازمان‌ها ایجاد می‌کند تا به‌طور مناسبی به منابع ابری دسترسی پیدا کرده و آن‌ها را کنترل کنیم درحالی‌که احتمال قابلیت اتصال بعدی را محدود می‌کنیم.
مدیریت ریسک دسترسی واحد ثالث			
تضمین اینکه دسترسی پیمانکار، شرکا و واحدهای ثالث مورد اعتماد به منابع شرکت، ابر و یا دیگر منابع به‌درستی به‌وسیله کارکنانِ غیر، حتی به‌صورت موقت، مورد استفاده قرار می‌گیرد.	ارائه موقعیت و زمان و تاریخ دسترسی به منابع. مستندسازی تمام فعالیت‌ها برای حسابرسی و تعقیب قانونی.	پیاده‌سازی یک راهکار مدیریت رمز عبور که دسترسی کارکنان غیر را با دقت کنترل کرده و مورد نظارت قرار می‌دهد.	محدودسازی دسترسی کارکنان غیر و کاهش ریسک‌های نشست‌های آزاد، دزدیده شدن اعتبارنامه‌ها و اقدامات بعدی به‌وسیله پرسنل غیرمعتبر.

Break Glass			
ارائه دسترسی خارج از روال معمول به سیستم‌ها در زمان رخداد بحران. نکته: این مبحث با جزئیات در بخش قبلی پوشش داده شد.	دسترسی ممتاز را می‌توان طی رویدادهای بحرانی اعطا کرد.	پیاده‌سازی یک سیستم مدیریت رمز عبور که قادر است تا اعتبارنامه‌های اضطراری (Break Glass) را در صورت رخداد بحران ارائه دهد و تمام فعالیت‌ها و مصارف را با دقت مناسب مستند سازد.	تضمین می‌نماید که موقعیت‌های بحرانی را می‌توان به‌سرعت حل کرد حتی اگر پرسنل کلیدی در دسترس نباشند و یا فاجعه‌ای رخ داده باشد.
حداقل‌سازی افشای داده‌ها			
کنترل دسترسی به داده‌های حساس وقتی به کاربران و مدیران حقوق ویژه‌ای برای دسترسی به سیستم، اپلیکیشن یا پایگاه داده اعطا شده است.	ارائه واسطی برای نظارت دستورات، داده‌های نمایش داده‌شده و قطع دسترسی برای فعالیت مخربی که ممکن است سبب افشای داده‌های حساس شود.	پیاده‌سازی یک مدیریت‌کننده رمز عبور و راهکار حقوق ویژه حداقلی که می‌تواند فیلترسازی خط دستور را انجام دهد، فعالیت را هشدار دهد و در داده‌های نمایش داده‌شده به دنبال مواردی بگردد که ممکن است نشانه‌ای از افشای داده‌ها باشد.	می‌توان درصورتی‌که داده‌های منابع حساس قابل‌رؤیت باشند، کاربران و مدیران را از اعمال دستورات حساس منع کرد و به تیم‌ها هشدار داد.

دسترسی دقیق مبتنی بر نقش			
سیستم‌عامل‌ها و برنامه‌ها ممکن است دارای کنترل‌های دقیق مجوز جهت محدودسازی دسترسی‌های نامناسب، نباشند.	در صورت امکان، محدودسازی دستورات، فرآیندها، برنامه‌ها و عملکردهای سیستم‌عامل حتی زمانی که کاربر با حقوق ویژه کار می‌کند.	پیاده‌سازی یک فناوری که می‌تواند دستورات، فرآیندها، اسکریپت‌ها و برنامه‌ها را مورد نظارت قرار دهد و اگر در حال اجرای کار غیرعادی بودند، اقدامی مثل ورود آن‌ها به لیست سیاه را انجام دهد.	نتایج سطح حمله را برای عملیات‌هایی که ممکن است ذاتاً دسترسی مبتنی بر نقش داخلی نداشته باشند، حداقل می‌نماید.
حساب‌های آزاد			
کاربران ممتاز (تهدیدات داخلی) ممکن است قابلیت آن را داشته باشند تا حساب‌های محلی، دامنه و یا اپلیکیشنی آزاد را برخلاف سیاست‌ها و راهکارهای امنیتی شرکت ایجاد کنند.	جلوگیری از دسترسی غیرعادی و فعالیت مخرب احتمالی با جلوگیری از ایجاد حساب‌های آزاد	پیاده‌سازی یک فناوری که می‌تواند ایجاد حساب‌های محلی، دامنه و اپلیکیشنی را مورد نظارت قرار دهد و حتی بر اساس برخی از سیاست‌ها در همان ابتدا مانع از ایجاد این‌گونه حساب‌ها شود.	کاهش ریسک با کنترل ایجاد حساب تنها به‌وسیله فرآیندهای مورد اطمینان سازمان

حساب‌های خدماتی			
حساب‌های خدماتی، دسترسی ممتاز به سیستم محلی دارند و در برخی موارد مثل حساب‌های دامنه ویندوز به منابع غیر سیستمی دسترسی دارند. با توجه به پیچیدگی مدیریت این اعتبارنامه‌ها و تأثیر احتمالی روی عملیات‌ها، اغلب با رمزهای عبور بدون تاریخ انقضاء و با تغییر کم پیکربندی می‌شوند.	روشی خودکار برای کشف، تغییر و شروع دوباره رمزهای عبور حساب‌های خدماتی توزیع‌شده با حداقل‌سازی تأثیر روی برنامه‌ها و فرآیندهای وابسته به هم.	پیاده‌سازی یک مدیریت‌کننده رمز عبور که می‌تواند عملیات کشف، مدیریت رمز عبور و شروع مجدد متمرکز حساب‌های خدماتی را در کل سازمان انجام دهد.	رمزهای ذخیره‌شده دیگر در کد برنامه نیستند و می‌توان آن‌ها را به‌صورت دوره‌ای عوض کرد و درعین‌حال زمان عدم دسترسی اپلیکیشن و خدمات مربوطه را کاهش داد. این‌کار ریسک‌های مربوط به دسترسی به‌صورت درب پشتی کارمندان و پیمانکاران را کاهش می‌دهد و ریسک‌های مربوط به بسیاری از تکنیک‌های هَک رمز عبور را کم می‌کند.

کنترل دسترسی‌پذیری یک دسترسی			
کنترل پویای دسترسی یک کاربرد خاص نیست ولی می‌توان آن را برای ارائه امنیت بیشتر در هر یک از سناریوهای قبلی پیاده کرد. سازمان‌هایی که می‌خواهند زمان دسترسی کاربر به منابع و سیستم-های خاص را کنترل کنند، می‌توانند محدودسازی را با مدل‌های دسترسی بومی انجام دهند. برای مثال، شرکت‌های ثالث نباید بعد از ساعات کاری سازمان به سیستم‌ها و رمزهای عبور آن‌ها دسترسی داشته باشند.	موضوع این است که سازمان‌های زیادی از واحدهای داخلی و خارجی تشکیل شده‌اند که باید به‌صورت مرتب به شبکه دسترسی داشته باشند. مشکلی که از این بابت وجود دارد این است که: چطور می‌توانید مطمئن شوید اعتبارنامه‌های مورد استفاده برای دسترسی به‌درستی مدیریت می‌شوند؟ همان‌طور که دیدیم، هکرها از اعتبارنامه‌های خارجی شرکت بهره می‌برند تا راهی به درون شرکت بیابند. جدای از آن، قدرت امنیتی سازمان شما به اندازه ضعیف‌ترین لینک خارجی شماست. سازمان‌ها باید بتوانند مدل دسترسی انعطاف‌پذیرتر و پویایی را در بالای ساختارهای دسترسی بومی سیستم‌ها و برنامه‌ها داشته باشند.	پیاده‌سازی یک راهکار مدیریت رمز عبور و یا مدیریت نشست که ساختارهای سیاست دسترسی پویا را ارائه می‌کند. مدل‌های دسترسی دینامیک تمام پارامترها را در لحظه درخواست دسترسی بررسی می‌کنند تا مطمئن شوند بر اساس آن دسترسی بهترین تصمیم گرفته می‌شود. معیارهای ارزیابی می‌تواند شامل موارد زیر باشد: چه کسانی سعی دارند وارد شوند؟ سعی دارند به چه سیستم‌هایی دسترسی داشته باشند؟ از کجا وارد می‌شوند؟ درخواست چه سطحی از دسترسی را دارند؟ چه روزی از هفته هستیم؟ در چه زمانی از روز قرار داریم؟	ترکیب بهترین روش‌های امنیتی و مدیریت دسترسی‌های ویژه می‌تواند ریسک‌ها را کاهش داده و به حفاظت سازمان در برابر نفوذ کمک کند. برای مثال، اگر بدانیم که حساب break glass تنها برای استفاده اضطراری است، باید آن را تنها برای چند ساعت در دسترس قرار دهیم. همچنین اگر به-طور طبیعی انتظار داریم که حساب باید از طریق کارمندی که در خانه است در دسترس قرار گیرد، باید مطمئن شویم که این درخواست از طریق اتصال VPN می‌آید.

ردیابی حادثه			
سیستم‌های مدیریت و تیکت‌دهی از راه دور فاقد رؤیت‌پذیری نسبت به حوادث هستند.	توانایی منابع معتبر جهت کنترل تغییرات و ردیابی حوادث برای آگاهی داشتن و تأیید دسترسی‌ها و تغییرات غیرعادی	پیاده‌سازی یک راهکار دسترسی ممتاز که فعالیت‌ها را با تیکت‌دهی، هِلپ-دِسک و دیگر راهکارهای مرکز تماس جهت گردش کار و مستندسازی، یکپارچه می‌کند.	هر کدام از دسترسی‌ها با تیکت‌ها مستند شده و درنهایت یک فرآیند مستندشده برای دسترسی‌ها را می‌توان آرشیو نمود.

فصل ۲۱

ملاحظات اجرایی

وقتی شما وارد پروژه سازمانی می‌شوید، باید هزینه‌ها، مزایا، بازگشت سرمایه، ریسک‌ها، تهدیدات و گردش کاری (برخی از آن‌ها) را مدنظر قرار دهید. در هنگام اجرای یک راهکار PAM، باید این مفهوم را در نظر گرفت که ممکن است این کار بر کل سازمان تأثیر بگذارد. این یعنی نه تنها مدیران تحت تأثیر قرار می‌گیرند، بلکه ممکن است کاربران نهایی، از پیمانکاران و مدیران اجرایی گرفته تا کارکنان موقت نیز حقوق مدیریتی را از دست بدهند (گرچه امیدوارم در سازمان شما به کارکنان موقت حقوق مدیریتی داده نشود ولی متأسفانه چنین چیزی اتفاق می‌افتد). تصمیم‌گیری درباره اینکه باید از کجا شروع کرد، چگونه اجرا نمود، نحوه آموزش به چه شکل باشد و خروجی‌های قابل اندازه‌گیری چیست، چالش‌هایی هستند که باید در مرحله اول مرتفع شوند. اگر این چالش‌ها را حل نکنیم، سیاست‌های داخلی، مقاومت کاربران و shadow IT ممکن است به‌طورکلی و در همان ابتدا دلایل به‌کارگیری PAM را مردود بدانند. این فصل برخی از ملاحظات مربوط به اجرای این موارد را پوشش می‌دهد که تمام مدیران اجرایی، متخصصان امنیت و تیم‌های عملیاتی باید مدنظر قرار داده، درباره آن‌ها بحث کنند و طی اجرا آن‌ها را حل نمایند.

اولویت‌بندی ریسک

نداشتن آگاهی و دید از تمام حساب‌های ممتاز و اعتبارنامه‌ها در یک سازمان، چالشی عظیمی را ایجاد می‌کند، مخصوصاً در شرکت‌هایی که به فرآیندها و ابزارهای دستی تکیه دارند. حساب‌های ممتازی که مدت زیادی است که فراموش شده و به حال خود رها شده‌اند، در اکثر

سازمان‌ها و در دسکتاپ‌ها، سرورها، هایپروایزورها، پلتفرم‌های ابری، فضاهای ابری، تجهیزات شبکه، برنامه‌ها، دستگاه‌های IoT، برنامه‌های SaaS و غیره پراکنده‌اند. تیم‌های مختلف ممکن است به‌صورت مجزا اعتبارنامه‌های خود را مدیریت کنند البته اگر مدیریتی در کار باشد که این کار عملیات ردیابی تمام رمزهای عبور را دشوار می‌کند و هر کسی را که از آن‌ها استفاده کرده و به آن‌ها دسترسی دارد، به حال خود رها می‌کند.

با توجه به ازدیاد حقوق ویژه که در سراسر سازمان پراکنده شده‌اند، شما کار را از کجا شروع می‌کنید؟ در برخی موارد، سازمان‌ها از کاربران نهایی شروع می‌کنند و دسکتاپ‌ها را مدنظر قرار می‌دهند و حقوق مدیریتی را حذف می‌کنند تا تهدیداتی مانند باج‌افزارها را کاهش دهند. در موارد دیگری، سازمان‌ها با حفاظت از سرورهای یونیکسی و لینوکسی آغاز می‌کنند که برنامه‌های حیاتی سازمان مانند سیستم‌های بازرگانی یا بانکی را پشتیبانی می‌نمایند. در برخی موارد نیز آن‌ها باید به نظارت شرکت‌های ثالث به‌عنوان الزامی برای انطباق‌پذیری با مقررات روی بیاورند. احتمالاً آن‌ها زمان کوتاهی دارند و باید روی زیرمجموعه‌ای از دارایی‌ها تمرکز کرده تا به یک حسابرسی مثل امن‌سازی و مدیریت صحیح دارایی‌های متصل به بخش شبکه امن PCI پاسخ دهند. مهم نیست که شما از سرورها، دسکتاپ‌ها، تجهیزات شبکه و یا دیگر دستگاه‌ها آغاز کنید چون درنهایت تصمیم شما تابعی از ریسک‌ها، پیچیدگی‌ها و هزینه خواهد بود. از خود بپرسید که بزرگ‌ترین مشکل در کجای سازمان قرار دارد، راه‌حل آن چیست و آیا می‌توان موفق شد؟ وقتی شما ریسک و مشکل را پیدا کردید، یا با بزرگ‌ترین مشکل موجود کار را آغاز می‌کنید و یا در دسترس‌ترین هدف را انتخاب کرده تا موفقیت را اثبات کنید و تجربه‌ای را به دست آورید.

بررسی اعتبارنامه های ممتاز

حتی اگر تیم IT به‌طور موفقیت‌آمیزی تمام اعتبارنامه‌های ممتاز را در سراسر سازمان شناسایی کند، باز هم به‌طورکلی بدین معنا نیست که ما تمام فعالیت‌های خاص انجام‌شده طی یک نشست ممتاز را می‌دانیم (مثلاً دوره زمانی که طی آن حقوق ویژه ارتقاءیافته به یک حساب، سرویس یا فرآیندی اعطا می‌شود). دادن دسترسی ممتاز به یک حساب فراتر از کاربر استاندارد نباید به معنای اعطاء اختیارات نامحدود به آن کاربر باشد. به‌علاوه، PCI، HIPAA و دیگر مقررات، سازمان‌ها را ملزم می‌کنند تا نه‌تنها داده‌ها را امن نگه داشته و از آن‌ها محافظت

نمایند بلکه باید بتوانند کارایی این معیارها را نیز اثبات کنند. پس هم به دلیل سازگاری با قانون و هم به دلایل امنیتی، تیم IT به رؤیت‌پذیری از فعالیت‌های انجام‌شده طی یک نشست ممتاز نیاز دارد.

به‌طور ایده‌آل، IT باید این قابلیت را نیز داشته باشد که در صورت استفاده نامناسب از اعتبارنامه‌ها، کنترل یک نشست را در دست بگیرد اما با وجود صدها نشست ممتاز در سازمان که به‌طور هم‌زمان در حال اجرا هستند، IT چطور باید فعالیت‌های مخرب را به‌سرعت مشخص کرده و متوقف سازد؟ با وجودی که برخی از برنامه‌ها و سرویس‌ها (مثل اکتیو دایرکتوری) می‌توانند فعالیت‌های کاربر را ثبت کنند و با وجودی که سرورهای ویندوز از داده‌های ورود موجود در داده‌های ثبتی بهره می‌برند و می‌توانند برخی از رفتارهای نامعمول را شناسایی کنند ولی برای پوشش کامل استفاده از حساب‌های ممتاز، به یک راهکار ثالث نیاز دارد. باید کاربردهای موردنیاز برای ردیابی نظارت و قابلیت را در هنگام طراحی مدل اجرایی و گردش کاری در نظر گرفت.

اشتراک گذاری حساب

تیم‌های IT معمولاً رمزهای عبور حساب‌های روت، مدیر ویندوز و بسیاری دیگر از حساب‌های ممتاز را به اشتراک می‌گذارند تا بتوانند در صورت نیاز، کارها و وظایفشان را مشترکاً انجام دهند اما به‌هرحال، با دسترسی چندین فرد به یک رمز عبور به‌صورت اشتراکی، ممکن است ردیابی فعالیت‌های انجام‌گرفته به‌وسیله آن حساب و نسبت دادن آن به یک شخص از آن افراد غیرممکن باشد که در نتیجه مسئولیت‌پذیری و عملیات حسابرسی را دشوار می‌کند. برای داشتن مدل اجرایی موفق، باید بررسی کرد که هر از چند مدتی این مشکل رخ می‌دهد و به چه صورت و در کجا برای حل این مشکل باید از PAM استفاده کرد.

اعتبارنامه‌های تعبیه‌شده

اعتبارنامه‌های ممتاز برای تسهیل عملیات احراز هویت در ارتباطات و دسترسی اپلیکیشن به اپلیکیشن (A2A) و اپلیکیشن به پایگاه داده (A2D) ضروری هستند. برنامه‌ها، سیستم‌ها و دستگاه‌های IoT معمولاً با اعتبارنامه‌های تعبیه‌شده پیش‌فرض فروخته شده و اجرا می‌شوند که این اعتبارنامه‌ها قابل حدس زدن بوده و ریسکی مهم را در بر دارند، مگر اینکه تحت

مدیریت قرار گیرند. این اعتبارنامه‌های ممتاز معمولاً به‌صورت متنی آشکار و احتمالاً درون اسکریپت، کد و یا یک فایلی ذخیره‌سازی می‌شوند. متأسفانه هیچ روش دستی برای شناسایی یا مدیریت متمرکز رمزهای عبور ذخیره‌شده در برنامه‌ها و اسکریپت‌ها وجود ندارد. امن‌سازی رمزهای عبور تعبیه‌شده به جداسازی رمز عبور از کد احتیاج دارد به‌گونه‌ای که وقتی مورد استفاده نیست، به‌طور امن و در یک مکان امن ذخیره‌سازی شود و به‌صورت متنی آشکار ذخیره نگردد. برای داشتن مدل اجرایی موفق، شناسایی تمام اعتبارنامه‌های تعبیه‌شده کلیدی است، همچنین نحوه کنترل شما برای تحمل خطا پس از حذف اعتبارنامه‌های تعبیه‌شده از نظر راهکار PAM A2A مهم و کلیدی است.

کلیدهای SSH

تیم‌های IT معمولاً برای انجام خودکار دسترسی به سرورها از کلیدهای SSH استفاده می‌کنند که نیاز به وارد کردن اعتبارنامه‌ها به‌صورت دستی را از بین می‌برد. پراکندگی کلیدهای SSH ریسکی برای هزاران سازمان است که ممکن است بیش از میلیون‌ها کلید SSH داشته باشند و مدت‌هاست فراموش شده‌اند ولی به‌صورت درب‌های پشتی برای هکرها جهت نفوذ به سرورهای حیاتی هستند پس باید این سؤال مطرح شود که این کلیدها در کجای سازمان قرار دارند، چگونه مدیریت می‌شوند و هنگامی‌که منقضی شدند باید چکار کرد؟ درواقع PAM می‌تواند کلیدهای SSH را مدیریت کند به‌گونه‌ای که سازمان‌ها هرگز وارد چنین موقعیت‌هایی نشوند.

اعتبارنامه‌های ممتاز در فضای ابری

به‌طورکلی چالش‌های رؤیت‌پذیری و قابلیت حسابرسی در محیط‌های ابری و مجازی بیشتر می‌شوند. کنسول‌های مدیریت فضای ابری و مجازی‌سازی (مثل AWS، Office 365، Azure و غیره) قابلیت‌هایی فراتر از کاربر معمولی را ارائه می‌کنند که به کاربران اجازه می‌دهد تا به‌سرعت سرورها را در مقیاسی انبوه تدارک دیده، پیکربندی کرده و حذف نمایند. در این کنسول‌ها، کاربران می‌توانند ثبت‌نام کنند و هزاران ماشین مجازی را (که هر یک از آن‌ها حساب‌های ممتاز خود را دارند) با تنها چند کلیک مدیریت کنند. مشکلی که پیش می‌آید آن است که چطور باید تمام حساب‌ها و اعتبارنامه‌های ممتاز ایجادشده را استقرار داده و مدیریت کنیم. جدای از آن، پلتفرم‌های ابری عمدتاً قابلیت ذاتی برای حسابرسی فعالیت‌های کاربر را

ندارند. حتی برای سازمان‌هایی که درجه‌ای از اتوماسیون را برای مدیریت رمز عبور خود پیاده‌سازی کرده‌اند (چه درون سازمان و چه با راهکارهای ثالث)، اگر در معماری‌شان فضای ابری را در نظر نگرفته باشند، هیچ تضمینی وجود ندارد که راهکار مدیریت رمز عبور قادر باشد تا اعتبارنامه‌های فضای ابری را به‌صورت مناسبی مدیریت کند. برای داشتن یک مدل اجرایی موفق، باید این سؤال مطرح شود که سازمان شما از چه تعداد منابع ابری استفاده می‌کند، چه کسانی دسترسی‌های حق ویژه دارند و این دسترسی‌ها چطور نگهداری و نظارت می‌شوند.

برنامه‌ها

برنامه‌های قدیمی معمولاً باید اعتبارنامه‌های منابع را خارج از اپلیکیشن ذخیره‌سازی می‌کردند. مثال‌هایی از آن پایگاه‌های داده از راه دور، برنامه‌های اشتراک فایل و یا سرورهای LDAP است. تضمین اینکه توسعه‌دهندگان به‌طور امن این اعتبارنامه‌ها را ذخیره‌سازی کنند، همیشه به‌عنوان یک چالش مطرح بوده است. متأسفانه، توسعه‌دهندگان طی سال‌های اخیر تعداد زیادی از برنامه‌هایی را توسعه داده‌اند که این اعتبارنامه‌ها را به‌صورت متنی ساده درون فایل‌های پیکربندی اپلیکیشن ذخیره می‌کنند. با ورود رایانش ابری، SaaS و IaaS که طی ۵ سال گذشته ارائه شده‌اند، برنامه‌ها به‌طور فزاینده‌ای در حال تعامل با پلتفرم‌های مختلف هستند و فقط با یک منبع خارجی ارتباط ندارند. پس اینکه فایل‌های پیکربندی، اعتبارنامه‌ها و کلیدهای API زیادی برای پلتفرم‌های مختلف داشته باشند، امری بدیهی است. اغلب کلیدهای API به‌عنوان بخش حساسی از اطلاعات دیده نمی‌شوند، درصورتی‌که توسعه-دهندگان باید این اطلاعات را حساس بدانند. سند این موضوع برنامه‌هایی هستند که در آن‌ها ذخیره امن اعتبارنامه‌ها در پایگاه‌ها داده انجام می‌شود ولی کلیدهای API برای منابع ابری به‌صورت متنی ساده رها می‌شوند. اغلب اتفاق افتاده است که توسعه‌دهندگان، کدهای با کلیدهای API را در GitHub قرار دهند و یا به‌صورت اتفاقی کلیدهای API را هنگام پست کردن کد منبع در StackOverflow، افشا کرده باشند؟ این نوع بی‌دقتی‌ها بسیار زیاد بوده است.

در هنگام سرمایه‌گذاری در فضای ابری همانند منابع قبلی باید توسعه‌دهندگان را به سمت دستیابی به بالاترین اهداف برای برنامه‌ها سوق دهیم ولی کمترین میزان حقوق ویژه را داشته باشیم. پایبند بودن به این فلسفه در اکثر APIهای عمومی مشکل است. با استفاده از نام

کاربری و رمزهای عبور، معمولاً امکان ایجاد دسترسی‌های مبتنی بر نقش دارای حقوق ویژه محدود، وجود دارد. توسعه‌دهندگان باید بدانند که کلیدهای API معمولاً دسترسی برنامه‌ها به تمام سازمان را ممکن می‌سازند و این موضوع در تضاد با اصل حداقل حقوق ویژه است. SendGrid یکی از استثنائات این موضوع است و کاری را انجام می‌دهد تا کنترل دقیقی را برای محدود کردن عملکردی داشته باشیم که کلید API اجازه استفاده از آن را دارد. برای مثال، توسعه‌دهنده می‌تواند با استفاده از CPM کلید API مربوط به SendGrid را پیکربندی نماید تا تنها از API تحویل ایمیل استفاده کند. حوزه‌های عملیاتی حساس مانند API رابط مدیریتی، نمی‌تواند به‌وسیله CPM مصرف شوند. در صورت افشا کلیدهای API، این کار باعث محدود شدن افشا حساب SendGrid می‌شود. با ادامه مهاجرت سازمان‌ها به سمت فضاهای ابری و حمایت از کدنویسی امن، امنیت پلتفرم‌های فروشنده‌ها و امنیت APIها نیز به بلوغ خود ادامه می‌دهند. مدیریت دسترسی‌های ممتاز تضمین می‌کنند که حقوق ویژه به‌صورت صفر و یکی عمل نکرده و هر دسترسی اپلیکیشن برنامه‌ریزی‌شده‌ای نیز یک مدل حق ویژه مشخص و معینی دارد.

حساب‌های فروشنده‌ها و دسترسی از راه دور

و در آخر، مسئله دیگری که برای سازمان‌ها وجود دارد آن است که چطور بهترین راهکارهای مدیریت دسترسی و اعتبارنامه‌های ممتاز را به کاربران ثالثی مثل مشاوران یا دیگر فروشنده‌هایی که ممکن است انواعی از فعالیت‌ها را انجام دهند، بسط داده و گسترش دهند. شما چطور اطمینان حاصل می‌کنید که احراز هویت ارائه‌شده از طریق دسترسی از راه دور یا به یک واحد ثالث به‌صورت مناسبی مورد استفاده قرار می‌گیرد؟ چطور تضمین می‌کنید که سازمان‌های ثالث، اعتبارنامه‌ها را به اشتراک نمی‌گذارند و یا اصلاً در نگهداری از رمزهای عبور قوی عمل می‌کنند، مثلاً وقتی کارمندی از شرکتی جدا می‌شود، آیا در حذف اعتبارنامه‌های او سهل‌انگاری می‌شود؟

فصل ۲۲

پیاده‌سازی مدیریت حساب‌های ممتاز

سازمان‌ها دریافته‌اند که امن‌سازی مناسب و کنترل اعتبارنامه‌های ممتاز جزء یکی از بهترین روش‌های دفاعی در برابر حملات از سوی هکرهای خارجی و همچنین تهدیدات درونی است. برای داشتن بهترین نتایج، راهکار مدیریت حقوق ویژه باید از حقوق ویژه در تمام مراحل زنجیره کشتار سایبری[1] و به‌وسیله پیاده‌سازی لایه‌های جامعی از کنترل‌ها و تحلیل‌ها، محافظت کند. اهداف کلی به‌صورت زیر هستند:

- کاهش سطح حمله با اعمال محدودیت در استفاده از حساب‌های ممتاز با کنترل دسترسی به حساب‌های اشتراکی ممتاز در سراسر سازمان؛
- نظارت بر کاربر، نشست و فعالیت ممتاز به‌منظور یافتن دسترسی‌های نامعتبر و یا تغییرات در فایل‌ها و دایرکتوری‌های کلیدی؛
- تحلیل دارایی و رفتار کاربر جهت شناسایی کردن فعالیت‌های مشکوک و مخرب از سمت افراد درون‌سازمانی و یا حساب‌های آلوده‌شده.

برای تطبیق حداکثری در سراسر سازمان، راهکار مدیریت دسترسی‌های ممتاز باید بدون محدود کردن عملکرد یا اضافه کردن عملیات‌ها، از حقوق ویژه محافظت کند.

پیاده‌سازی یک راهکار مدیریت دسترسی ممتاز انتها به انتها باید از یک فرآیند تعریف‌شده به‌منظور کمینه‌سازی هزینه‌ها پیروی کند و سرعت به نتیجه رسیدن را نیز افزایش دهد. برای مدیریت دسترسی‌های ممتاز استفاده از یک رویکرد ۱۲ مرحله‌ای ساده در مدیریت ریسک‌ها

[1] Cyber Kill Chain

کمک‌کننده خواهد بود و نتایج قابل پیش‌بینی و قابل استنادی را ارائه خواهد کرد. نتایج این فرآیند در اجرای این ۱۲ گام است و به شما کمک می‌کند تا کنترل و مسئولیت‌پذیری بیشتری را بر روی حساب‌ها، دارایی‌ها، کاربران و سیستم‌های دارای حقوق ویژه داشته باشید.

در فرآیند انتخاب و اجرای راهکار مدیریت دسترسی‌های ممتاز، این الزامات سازمانی را در نظر داشته باشید چون به شما کمک می‌کنند تا هزینه‌ها و ریسک‌ها را در سازمان خود کاهش دهید:

- کمینه‌سازی کل هزینه مالکیت؛
- ارائه رویه سریع برای رسیدن به ارزش[1]؛
- ارائه اطلاعاتی مناسب برای اتخاذ بهترین تصمیمات مبتنی بر ریسک.

دقت داشته باشید که این گام‌ها تنها یک راهنما هستند و الزامی نیست که آن‌ها را به ترتیب دنبال کنید.

گام ۱: بهبود مسئولیت‌پذیری برای رمزهای عبور ممتاز

منطقی‌ترین نقطه برای شروع دستیابی به کنترل بیشتر بر حقوق ویژه به‌وسیله بهبود مسئولیت‌پذیری در رمزهای عبور است. عدم مدیریت مؤثر حساب‌های اشتراکی مسئله‌ای است که مقیاس و ریسک‌های قابل‌توجهی دارد. تنها کافی است به رخنه‌های اطلاعاتی اخیر نگاه کنید و این موضوع را مشاهده کنید. سیستم‌های خاصی وجود دارند که رمزهای عبور تعبیه-شده یا نوشته‌شده در کد را دارند و باعث سوءاستفاده از این رمزهای عبور می‌شوند. رمزهای عبور علاوه بر پشتیبانی از تعامل با انسان، برای دسترسی‌های اپلیکیشن به اپلیکیشن و یا اپلیکیشن به پایگاه داده موردنیاز هستند. رمزهای عبور معمولاً به‌صورت استاتیک هستند و باید تمهیداتی برای آن‌ها در نظر گرفته شود. تغییر دستی رمز عبور زمان‌بر و غیر قابل اطمینان بوده و عملیات حسابرسی و گزارش‌دهی دسترسی‌ها را پیچیده‌تر می‌کند و مستعد خطا است؛ بنابراین سازمان‌ها چطور باید مسئولیت‌پذیری حساب‌های اشتراکی ممتاز را تضمین کنند تا بدون تأثیرگذاری بر عملکرد، انطباق‌پذیری با الزامات امنیتی را محقق نمایند؟

[1] Time to Value

پاسخ انجام خودکار این کار است- انجام خودکار مدیریت رمز عبور و نشست؛ ارائه کنترل دسترسی امن؛ حسابرسی، اعلام هشدار و ضبط کردن برای هر حساب ممتاز، از حساب‌های اشتراکی محلی و مدیریتی دامنه گرفته تا حساب شخصی کاربر (در صورت وجود دو حساب کاربری) تا حساب‌های سیستم‌عامل‌ها، تجهیزات شبکه، کلیدهای API، پایگاه داده (A2DB) و اپلیکیشن (A2A) و حتی کلیدهای SSH. با بهبود مسئولیت‌پذیری و کنترل روی دسترسی ممتاز، سازمان‌های IT می‌توانند ریسک‌های امنیتی را کاهش دهند و به اهداف تعیین‌شده دست یابند. با در نظر گرفتن این هدف، این ۱۰ توصیه را برای هر راهکار مدیریت دسترسی-های ممتاز در نظر داشته باشید:

۱. اسکن، شناسایی و نمایه‌سازی کامل شبکه به‌صورت خودکار؛
۲. ساخت مجموعه مجوزهای پویا مطابق با داده‌های به‌دست‌آمده از اسکن؛
۳. تغییر خودکار کلیدهای SSH و تعویض رمزهای عبور طبق زمان‌بندی تعریف‌شده؛
۴. کنترل دسترسی، گردش کاری و حسابرسی دقیق؛
۵. رابط کاربری زیبا و یکپارچه برای کاربران نهایی با قابلیت تطبیق سریع؛
۶. گزینه‌های مبتنی بر گردش کار و break glass برای درخواست دسترسی.
۷. مدیریت توأم رمز عبور و نشست در یک راهکار به‌گونه‌ای که نیازی به دو رابط مختلف یا نیاز به تغییر به‌صورت جدا از هم نباشد؛
۸. از ابزارها و برنامه‌های بومی به‌جای ابزارهای ثالث برای مدیریت نشست استفاده کنید تا ریسک‌های همراه با آن را وارد سازمان نکنید؛
۹. از یک فضای ذخیره‌سازی داده و تحلیل تهدید یکپارچه در سراسر سیستم حقوق ویژه بهره ببرید؛
۱۰. گزینه‌های انعطاف‌پذیر برای اجرا: تجهیزات سخت‌افزاری؛ تجهیزات مجازی، فضای ابری یا نرم‌افزار برای حداکثر پوشش.

با این الزامات، سازمان‌ها می‌توانند تمام حساب‌ها را در سازمان خود پیدا کنند، آن‌ها را تحت مدیریت خود درآورند و درخواست‌های حسابرسی را توجیه کرده و گزارش نمایند که تمامی حساب‌ها تحت مدیریت هستند.

گام ۲: پیاده‌سازی حقوق ویژه حداقلی در دسکتاپ ها

وقتی حساب‌ها و دارایی‌ها پیدا و مشخص شدند و به‌طور پیوسته تحت مدیریت قرار گرفتند، گام بعدی برای تکمیل مدیریت دسترسی‌های ممتاز، پیاده‌سازی حداقل حق ویژه در ماشین‌های کاربر نهایی است. به‌عنوان یک راهکار عالی، سازمان‌ها باید ریسک دسکتاپ‌ها را قبل از سرورها (مثل ویندوز، یونیکس یا لینوکس که در گام ۴ مشخص شده است) کاهش دهند چون نقاط انتهایی معمولاً آخرین موقعیتی است که باید امنیت آن تأمین شود. ممکن است برخی سازمان‌ها بخواهند این ترتیب را برعکس کنند، پس بر اساس محیط‌ها و ریسک‌های خاص کسب‌وکار ممکن است اولویت‌بندی برای این گام‌ها برای تطابق با سطح ریسک و هدف سازمان تغییر کند. به‌عبارت‌دیگر، ترتیب این سه گام می‌تواند تغییر کند اما تقریباً همیشه گام ۱ مهم‌ترین است و بیشترین ریسک هدف حمله به حقوق ویژه را در بر دارد.

فرآیند محدودسازی یا فعال‌سازی حقوق ویژه کاربر نهایی احتمالاً می‌تواند برای تیم IT زمان‌بر و پیچیده باشد اما این کار باید برای پشتیبانی از حسابرسی‌ها و قوانین لازم‌الاجرا انجام گیرد. وقتی سازمان‌ها برنامه‌های دسکتاپ استانداردشده‌ای داشته باشند، این فرآیند به نسبت ساده‌تر می‌شود. اگرچه نباید به کاربران حقوق ویژه مدیر محلی یا کاربری قوی را اعطا کرد ولی گاهاً برنامه‌هایی خاص برای اجرا به حقوق ویژه ارتقاءیافته نیاز دارند. سازمان‌های IT چطور باید ریسک کاربران ممتاز را کاهش دهند و بدون محدود کردن عملکرد آن‌ها یا افزایش بار کاریشان، ریسک سازمان را در برابر اکسپلویت شدن یا عدم تطابق با مقررات کاهش دهند؟

پاسخ تنها اجرای دسترسی دارای حداقل حقوق ویژه برای برنامه‌های مبتنی بر قواعد، جهت ارتقاء حقوق ویژه اپلیکیشن بدون ارتقاء حقوق ویژه کاربر است. با حذف حقوق ویژه مدیریتی در دسکتاپ کاربران، تیم IT اجرای سیاست‌های حداقل حقوق را ساده‌تر کرده، کنترل دسترسی اپلیکشین را حفظ می‌کند و فعالیت‌های ممتاز را ثبت می‌کند و بدین‌صورت شکاف‌های امنیتی را پوشش داده، بازدهی عملیاتی را بهبود بخشیده و با سرعت بیشتری به اهداف خود می‌رسد.

بنابراین ۱۰ قابلیت برتر دسکتاپ‌های دارای حداقل حقوق ویژه باید شامل موارد زیر باشد:

۱. تغییر حالت پیش‌فرض تمام کاربران به حقوق ویژه استاندارد در عین حفظ امکان ارتقاء حقوق ویژه برای برنامه‌ها و وظایفی خاص بدون استفاده از اعتبارنامه‌های مدیریتی؛
۲. اجرای محدودیت در نصب نرم‌افزارها و تغییرات در پیکربندی سیستم‌عامل؛
۳. حذف نیاز به داشتن دو حساب کاربری از سوی کاربر نهایی؛
۴. اتخاذ تصمیمات مشخص حداقل حقوق ویژه برای برنامه‌ها بر اساس آسیب‌پذیری‌ها، ریسک‌ها، اعتبار و سازگاری آن اپلیکیشن با قواعد؛
۵. تطبیق برنامه‌ها با قواعد به‌صورت خودکار بر اساس سیاست‌های مبتنی بر دارایی؛
۶. گزارش دسترسی ممتاز به فایل‌های سیستمی برای تمام کاربران و مستندسازی تغییرات سیستم در زمان نشست‌های ممتاز؛
۷. نظارت بر نشست و ثبت کلیدهای فشرده‌شده برای دسترسی‌های ممتاز؛
۸. ارائه یک تکنیک برای استفاده از حقوق ویژه دامنه یا محلی واقعی در صورت نیاز، شامل احراز هویت چند مرحله‌ای؛
۹. یکپارچه‌سازی با دیگر راهکارهای دارای حقوق ویژه جهت دستیابی به مدیریت جامع بر دسترسی‌های ممتاز؛
۱۰. بهره‌مندی از یک فضای ذخیره‌ساز و تحلیل داده یکپارچه در چشم‌انداز حقوق ویژه. با این راهکار، مشتری‌ها این قابلیت را دارند که به‌صورت مؤثری حقوق مدیر محلی را حذف کنند و تصمیمات ارتقاء اپلیکیشن را به‌صورت هوشمند برای تهدیدات حقوق ویژه در دنیای واقعی بگیرند.

گام ۳: بهره‌مندی از سطوح ریسک اپلیکیشن

حالا که اعتبارنامه‌های اشتراکی تحت مدیریت هستند و کاربران نهایی حقوق ویژه‌ای دارند تا با آن‌ها کارهای خود را انجام دهند، سازمان‌ها می‌توانند به سمت شناخت بهتر ریسک‌ها حرکت کنند تا تصمیمات ارتقاء حقوق ویژه آگاهانه‌تری را اتخاذ نمایند اما چالش آن است که بیشتر راهکارهای ارزیابی ریسک، کمک اندکی به متخصصان امنیتی در ارائه اطلاعات آسیب‌پذیری‌ها، حملات، بدافزارها و اطلاعات ریسک‌های موجود در سازمان می‌کنند. تیم امنیتی که با انبوهی از داده‌ها و گزارش‌های استاتیک مواجه است، باید به‌صورت دستی تهدیدات واقعی را تعیین کند و نحوه رویارویی با آن‌ها را مشخص نماید.

بنابراین در نظر داشته باشید که سیستم مدیریت آسیب‌پذیری‌ها و برنامه‌های ارزیابی ریسک خود را جهت گنجاندن کنترل دسترسی‌های ممتاز و کنترل اپلیکیشن گسترش دهید. اگر تیم‌ها اجرای برنامه‌ای را بر اساس نبود وصله‌های امنیتی، یا بدافزار بودن و دیگر تهدیدات دنیای واقعی، خطرناک تشخیص دهند، باید سیاست‌های مدیریت دسترسی حقوق ویژه را برای جبران این ریسک به کار گیرند. این کار در فرآیند کنترل اپلیکیشن بر مبنای اعتبار نیز به همین شکل است. این امر نه‌تنها استفاده از اکسپلویت‌ها به‌عنوان هدفی برای حمله را متوقف می‌سازد بلکه تهدیدات اجتماعی همراه با آن را نیز که می‌توانند از آسیب‌پذیری‌های درون سازمان بهره ببرند، متوقف می‌سازد.

گام ۴: پیاده‌سازی حقوق ویژه حداقلی در سرورها

در محیط‌های فناوری اطلاعات کنونی، برنامه‌های حیاتی لایه اول سازمان، اهدافی جذاب برای عاملان تهدید هستند. این برنامه‌ها شامل داده‌های حساس و اپلیکیشن‌هایی بوده که عاملان تهدید دنبال آن‌ها هستند. دسترسی به اعتبارنامه‌های ممتاز مربوط به این منابع می‌تواند دسترسی به داده‌های تجارت الکترونیک، سیستم‌های ERP مدیریت‌کننده داده‌های کاربران، اطلاعات مشتریان و داده‌های حساس مالی را فراهم کند. داشتن رمزهای عبور روت، وضعیت کاربر ارتقاءیافته یا دیگر حقوق ویژه اضافی برای کاربران به‌منظور انجام کارها مهم است اما متأسفانه این کار ریسک‌های امنیتی قابل‌توجهی را ناشی از سوءاستفاده عمدی، تصادفی یا غیرمستقیم از این حقوق ویژه اشتراکی بیان می‌کنند، مخصوصاً وقتی این حقوق ویژه به سیستم‌های لایه اولی دسترسی دارند که کسب‌وکار سازمان را تحت تأثیر قرار می‌دهند، مانند آن‌هایی که بر روی سرورهای لینوکسی و یونیکسی قرار دارند و پیش‌تر به آن اشاره کردیم. پاسخ‌های مرسوم به این مشکل شامل موارد زیر است:

- ناکارآمد و ناقص هستند (مانند گزینه‌های ذاتی سیستم‌عامل) که فاقد قابلیت سپردن احراز هویت به جایگزین، بدون افشای رمزهای عبور هستند؛
- به اندازه کافی امن نیستند (مانند حساب‌های متن‌باز Sudo یا مدیر محلی) تا ریسک و مسئله انطباق‌پذیری با مقررات را حل کنند و همچنین فاقد توانایی در ضبط نشست‌ها و کلیدهای فشرده‌شده برای حسابرسی‌ها هستند؛

- فعالیت‌های درون اسکریپت‌ها و برنامه‌های ثالث را به حساب نمی‌آورند که در نتیجه میانبری به برنامه‌های تأیید نشده می‌شوند؛
- اگر که در سراسر سازمان در حال استفاده باشند، مسیر حرکت کارآمدی را از حساب‌های اشتراکی و sudo نمی‌دهند.

بنابراین، سازمان‌های IT چگونه باید کسانی را که به حساب‌های روت دسترسی دارند محدود کنند تا ریسک آلوده شدن را بدون محدودسازی عملکردشان کاهش دهند؟

سازمان‌ها باید بتوانند به‌صورت مؤثر حقوق ویژه سرور و احراز هویت را بدون افشای رمزهای عبور برای حساب‌های روت، مدیران محلی یا دامنه یا دیگر حساب‌ها اختصاص دهند. ضبط تمام نشست‌های ممتاز برای حسابرسی‌ها، شامل اطلاعات کلیدهای فشرده‌شده، در دستیابی به الزامات کنترل دسترسی ممتاز بدون تکیه بر ابزارهای بومی کمک‌کننده است.

۱۰ قابلیت برتر مدیریت حقوق ویژه شامل موارد زیر است:

۱. پشتیبانی از ماژول احراز هویت قابل اتصال[1] به‌منظور استفاده از سیستم‌های احراز هویت با استاندارد صنعتی؛
۲. کنترل و حسابرسی پیشرفته روی دستورات در سطح سیستم؛
۳. خط‌مشی انعطاف‌پذیر و قدرتمند به‌منظور ارائه مسیر مهاجرت از ابزارهای بومی؛
۴. پشتیبانی گسترده از پلتفرم‌های ویندوز، یونیکس و لینوکس؛
۵. ضبط و فهرست کردن تمام نشست‌ها جهت کشف سریع در طی عملیات حسابرسی؛
۶. شفافیت مجوزهای واسطها که بهره‌وری و قانونمند عمل کردن کاربر را تضمین نماید؛
۷. مدیریت تغییرات مربوط به تنظیمات و پیکربندی سیاست‌ها که امکان حسابرسی کامل از کسانی که چیزی را تغییر داده‌اند یا کنترل نسخه و غیره را فراهم می‌کند؛
۸. استفاده از API با نام REST برای یکپارچه‌سازی راحت‌تر با محصولات ثالث؛
۹. یکپارچه‌سازی تمام سیاست‌ها، نقش‌ها و داده‌های ثبتی از طریق یک کنسول تحت وب؛

[1] Pluggable Authentication Module (PAM)

۱۰. بهره‌گیری از یک فضای ذخیره‌سازی و تحلیل تهدید یکپارچه در چشم‌انداز حقوق ویژه.

گام ۵: تجهیزات شبکه

معمول‌ترین نام‌های کاربری و رمزهای عبور برای دستگاه‌های شبکه ضرورتاً پیش‌فرض‌هایی نیستند که همراه با دستگاه ارائه می‌شوند، اگرچه در حال حاضر ما از این ریسک آگاه هستیم و بیشتر ادمین‌ها (مدیران) آن‌ها را تغییر می‌دهند. متأسفانه در برخی از محیط‌ها، می‌توان رمز عبور آن‌ها را حدس زد یا با استفاده از حملات جستجوی فراگیر رمزهای عبور آن‌ها را پیدا کرد. به‌علاوه، دومین نقص حقوق ویژه معمول استفاده از رمزهای عبور یکسان در تمام زیرساخت (استفاده دوباره از رمز عبور) است و حتی اگر شما مدیریت شبکه را برون‌سپاری کرده باشید، به‌ندرت رمز عبورهای تجهیزات به‌صورت دسته‌جمعی عوض می‌شوند، البته اگر تعویضی صورت گیرد. این مسئله می‌تواند به انواعی از فعالیت‌های مخرب منجر شود که شامل آخرین آسیب‌پذیری‌هایی باشند که می‌توانند بوت‌استرپ لودر[1] دستگاه‌ها را با بخشی از بدافزاری سفارشی جایگزین نمایند.

ریسک‌ها می‌توانند از نبود مدیریت حساب بر روی دستگاه‌های شبکه نشئت بگیرند، به‌طور مثال:

- رمزهای عبور پیش‌فرض یا متداولی که به‌درستی پیکربندی نشده‌اند؛
- استفاده از اعتبارنامه‌های مشترک در چندین دستگاه برای سادگی مدیریت؛
- استفاده طولانی‌مدت از رمز عبورها به دلیل ترس از تعویض آن‌ها یا نبود قابلیت‌های مدیریتی؛
- حساب‌های آلوده یا افراد داخلی که تغییراتی را انجام می‌دهند تا اجازه نفوذ به داده‌ها را ایجاد کنند؛
- دستگاه‌ها و زیرساخت‌های برون‌سپاری‌شده که پرسنل، قراردادها و ابزار در آن تغییر می‌کند؛
- افشاء اعتبارنامه‌ها برای افراد غیرمسئول.

[1] Bootstrap Loader

هر یک از این موارد می‌تواند منجر به افزایش ریسک در زیرساخت شما شود. همچنین، سازمان‌ها باید هنگام برنامه‌ریزی برای مدیریت حساب‌های ممتاز خود، با به حساب آوردن این دستگاه‌ها، فراتر از دسکتاپ‌ها و سرورها را ببینند. همچنین سازمان‌ها با راهکارهای حقوق ویژه جدیدتر می‌توانند پا را فراتر از مدل‌های احراز هویت صفر و یکی «دسترسی» یا «عدم دسترسی» بگذارند، مدل‌هایی که در بیشتر دستگاه‌های شبکه مورد استفاده قرار می‌گیرند. سازمان‌ها در حال حاضر به دروازه‌های پروکسی دسترسی دارند که می‌تواند اقداماتی اعم از قرار دادن در لیست سفید و سیاه، نظارت کردن نشست، اعلان هشدار فعال و غیره را انجام دهد.

گام ۶: مراکز داده مجازی و ابری

مراکز داده در حال رشد مجازی و محیط‌های ابری برای پردازش، ذخیره‌سازی یا میزبانی اپلیکیشن‌ها و توسعه آن‌ها، مسیر جدیدی را برای هکرها یا افراد بداندیش درون‌سازمانی باز کرده است تا به داده‌های حساس دسترسی پیدا کنند و سازمان‌ها را با اختلال مواجه سازند. با وجود این ریسک‌ها، شتاب استفاده از فضاهای ابری رو به رشد است. به همین ترتیب، سازمان‌ها باید دسترسی به این محیط‌ها را امن کنند تا ریسک‌های امنیتی را کاهش داده و درعین‌حال هزینه‌های میزبانی برنامه‌ها و خدمات در فضای ابری را جوابگو باشند.

مانند دسکتاپ‌ها و سرورهای مرسوم، محیط‌های مجازی یا ابری مدیریت‌نشده می‌توانند شکاف امنیتی قابل‌توجهی را ایجاد کنند که شبکه‌ها را در معرض رخنه‌های امنیتی یا از دست دادن داده‌ها، دزدی مالکیت معنوی و مشکلاتی در انطباق‌پذیری با مقررات قرار می‌دهد. گام اول در کنترل این دارایی‌ها، کشف آن‌ها است، تکنیک‌های زیادی برای کشف دارایی‌ها در محیط‌های مجازی و ابری وجود دارند که عبارت‌اند از:

- اجرای اسکن و شناسایی استاندارد شبکه از یک ماشین میزبان با دسترسی به محیط مجازی؛
- جستجوی هایپروایزور یا پلتفرم مدیریت فضای ابری به‌منظور بازیابی فهرست دارایی‌های محیط مجازی یا پیکربندی یک اعلان فعال برای به‌روزرسانی‌های این فهرست؛

- استفاده از عاملانی که روی کتابخانه مبنا از قبل نصب شده‌اند و یا آن‌هایی که در طی فرآیند عادی تدارک سرور نصب شده‌اند؛
- جستجوی یک راهکار مدیریت دارایی ثالث.

وقتی نمونه‌های فضای ابری پیدا شد، باید آن‌ها را مدیریت کرد تا خطر افشاء آن‌ها محدود شود. از دید یک مدیریت دارای حق ویژه، گزینه‌ها برای امن‌سازی این دارایی‌ها همانند دسکتاپ‌ها و سرورها است:

- استفاده از یک راهکار مدیریت رمز عبور برای مدیریت کلمه‌های عبور در تمام ماشین‌های مجازی به‌صورت خودکار؛
- استفاده از یک راهکار مدیریت نشست به‌منظور کنترل و نظارت دسترسی ماشین‌های مجازی؛
- استفاده از قابلیت‌های بومی جایگزین O\S جهت کاهش حقوق ویژه مربوط به کاربران در حال تعامل با سیستم؛
- استفاده از عامل مدیریت حقوق ویژه با معماری حقوق ویژه حداقلی جهت کاهش افشاء حساب‌های مدیر، روت و حساب‌های توسعه‌دهنده دارای حق ویژه.

حالا که ماشین‌های مجازی تحت کنترل هستند، در رابطه با خود هایپروایزور و پلتفرم مدیریت ابری چه کاری می‌توان انجام داد؟ در اینجا هم فعالیت‌های نامناسب و مخرب در این سطح مدیریتی، می‌تواند تأثیر عمده‌ای روی کسب‌وکار سازمان داشته باشد. این‌ها شامل مدیران محیط‌های VMWare، Microsoft Hyper-V، Amazon AWS و Microsoft Azure است. برای مقابله با این تهدید، سازمان‌ها چندین گزینه دارند:

- استفاده از یک راهکار مدیریت رمز عبور جهت مدیریت خودکار رمزهای عبور در تمام پلتفرم‌های هایپروایزور و مدیریت ابری؛
- استفاده از یک راهکار مدیریت نشست به‌منظور کنترل و نظارت تمام فعالیت‌های مدیریت فضای ابری؛
- استفاده از قابلیت‌های بومی یا ثالث هایپروایزور و یا سرویس‌دهنده مدیریت ابری جهت کاهش حقوق ویژه مربوط به کاربرانی که با سیستم تعامل دارند.

گام ۷: دستگاه‌های اینترنت اشیاء

با وجود پیچیدگی حملات نرم‌افزاری و رشد گسترده آن، حفاظت از محیط‌های آن‌ها برای سازمان‌ها بسیار چالش‌برانگیز شده است. اخیراً نسل جدیدی از حملات منع سرویس[1] ظهور کرده‌اند که ریسک قابل‌توجهی را برای سازمان‌ها و همچنین دولت‌ها دارند. تعریف اینترنت اشیاء مثل بسیار از عبارت‌ها در IT، تفاسیر زیادی دارد. معمولاً ما دستگاه‌های اینترنت اشیاء را مثل DVR، CCTV، میکروفون، وِب‌کَم، اتوماسیون خانگی و غیره می‌بینیم اما در واقعیت، این عبارت می‌تواند به معنای هر چیز متصل به اینترنت شامل تجهیزات کنفرانس ویدیویی، پرینترهای شبکه و غیره نیز باشد.

برخی از آسیب‌پذیری مهم در دستگاه‌های اینترنت اشیاء وجود دارند اعم از استفاده از رمزهای عبور نوشته‌شده در کد تجهیزات، رمز عبورهای ضعیف و پیش‌فرض آن‌ها است. حتی وقتی مدیران رمزهای عبور پیش‌فرض را تغییر می‌دهند، بیشتر اعتبارنامه‌ها را می‌توان از طریق حملات جستجوی فراگیر حدس زد، مخصوصاً وقتی رمزهای عبور ضعیف یا اشتراکی در زیرساخت اینترنت اشیاء مورد استفاده قرار گرفته باشد.

گام ۸: عملیات توسعه‌ای (DevOps)

DevOps ترکیبی از مخفف کلمات توسعه (Development) نرم‌افزار و عملیات‌های (Operations) فناوری اطلاعات است. این عبارت تعریفی برای ارتباط و همکاری بین توسعه-دهندگان نرم‌افزار و دپارتمان‌های فناوری اطلاعات است و هدف DevOps توسعه برنامه‌های نرم‌افزاری معمولی نیست بلکه بر روی انجام خودکار و برنامه‌ریزی‌شده مدیریت زیرساخت تمرکز دارد که می‌تواند شامل ارائه نرم‌افزار، مدیریت لحظه‌ای و یا اتوماسیون جهت اجرا کردن سریع منابع و مدیریت عملیات‌های مرتبط با آن‌ها باشد.

توسعه‌دهندگان برنامه‌های تجاری، یا برنامه‌نویسانی که برنامه‌های DevOps سفارشی برای سازمان تولید می‌کنند، باید در نظر داشته باشند که این کار چقدر برای آن‌ها و کاربرانشان و یا سایر برنامه‌ها مفید است و دیگر نیازی نیست تا در زمان اتصال، نام کاربری یا رمز عبور را وارد کنند. اگر ابزارها اعتبارنامه‌ها را به‌صورت خودکار ذخیره کنند و یا راهکار مدیریت را برای

[1] Denial of Service (DOS)

اثبات احراز هویت اعمال نمایند، کاربران نهایی مثل مدیران پایگاه داده هرگز به حقوق مدیریتی برای دسترسی به پایگاه داده نیاز ندارند. ابزارهای مدیریتی برای سرویس‌ها، دسترسی از راه دور و زیرساخت به‌صورت خودکار برای کاربری که در سیستم وارد شده است، دارایی که از آن استفاده می‌کند را شناسایی کرده و به‌صورت بی‌نقصی اعتبارنامه‌ها را درخواست داده و عبور می‌دهد. راهکارهای مدیریت دسترسی‌های ممتاز برای مدیریت رمز عبور این قابلیت را به واقعیتی عملی تبدیل می‌کند که از رابط برنامه‌نویسی اپلیکیشن (API) استفاده کرده تا درخواست‌های اعتبارنامه و رمز عبور را تنظیم نموده، بازیابی کرده و پردازش نماید. برخی از مزایای این رویکرد برای DevOps عبارت‌اند از:

- برنامه‌های امن- APIهای مدیریت دسترسی‌های ممتاز برای ارائه امنیت بهتر در تمام برنامه‌هایی که طراحی شده است، جهت انجام کارهای عادی به یک کاربر یا اپلیکیشن برای وارد کردن اعتبارنامه‌های استاتیک نیاز دارند. توسعه‌دهندگان می‌توانند یک PAM API را فراخوانی کرده و آخرین اعتبارنامه‌ها را برای کاربر، اپلیکیشن، زیرساخت، فضای ابری و یا پایگاه داده بازیابی نموده تا احراز هویت انجام دهند و به محض پایان نشست، اعتبارنامه‌ها را از بین ببرند. این عملکرد می‌تواند عامل آغاز تغییر خودکار و تصادفی رمز عبور یا دیگر فرآیندهای خودکار به‌منظور تحقق اهداف سازمانی باشد. کاربران هرگز آخرین اعتبارنامه‌های مربوط به منبع یا برنامه‌ای را نمی‌بینند.
- کاهش هدف حمله- استفاده از PAM API زمان اجرای برنامه‌ها را امن‌سازی می‌کند و مانع از تکنیک‌های حمله‌ای مانند پاس کردن هش (PtH) می‌شود. این رویکرد بسیار امن‌تر از شناسایی یگانه (SSO) است چون رمز عبور پیوسته به ازای هر نشست، کاربر یا دیگر معیارها تغییر می‌کند حتی اگر رمز عبورها به اشتراک گذاشته شوند.
- ساده‌سازی توسعه‌دهنده- این رویکرد باعث بهبود پاسخگویی و چابکی تیم IT می‌شود به‌طوری‌که دیگر نیاز به ورود یک نام کاربری و رمز عبور برای برقراری اتصال و ایجاد برنامه‌های سفارشی ندارند. اگر ابزارها اعتبارنامه‌ها را به‌صورت خودکار بازیابی نمایند، کاربران نهایی مثل ادمین (مدیران) پایگاه داده هرگز به حقوق مدیریتی برای دسترسی به پایگاه داده نیاز ندارند.

گام ۹: یکپارچه‌سازی مدیریت

واضح است که تیم IT و متخصصان امنیتی، دارای اطلاعات زیادی در مورد حقوق ویژه، آسیب‌پذیری‌ها و حملات هستند. متأسفانه تهدیدات پیشرفته مقاوم[1] (APTs) اغلب ناشناس باقی می‌مانند چون راهکارهای تحلیلی امنیتی مرسوم نمی‌توانند داده‌های پراکنده را برای تعیین ریسک‌های پنهان همبسته سازند. رویدادهای ایزوله‌شده به‌صورت موارد خاص، فیلتر شده و یا به‌صورت گم‌شده در دریایی از داده‌ها نوشته شده‌اند. عامل تهدید به گشت زدن در شبکه ادامه می‌دهد و خسارات ادامه یافته و چند برابر می‌شود. تیم‌های عملیاتی امنیت و IT چطور محل ورود تهدیدات را تشخیص دهند، آن‌ها را اولویت‌بندی کنند و ریسک‌های آن‌ها را به‌سرعت کاهش دهند؟

تحلیل داده‌ها تیم‌ها را قادر می‌سازد تا نفوذ به داده‌هایی را که به‌طور معمول توسط دیگر راهکارهای تحلیل امنیت مشخص نشده‌اند، شناسایی کنند. این راهکارها، به‌طور دقیق کاربران و دارایی‌های با ریسک بالا را به‌وسیله همبسته کردن حقوق ویژه سطح پایین، آسیب‌پذیری‌ها و داده‌های تهدید به‌دست‌آمده از انواع راهکارهای ثالث، مشخص می‌کنند؛

بنابراین هر راهکار مدیریت یکپارچه و تحلیل داده باید این ۱۰ قابلیت برتر را شامل شود:

۱. همبسته‌سازی داده‌های سطح پایین به‌دست‌آمده از انواع راهکارهای ثالث جهت یافتن تهدیدهای حیاتی؛
۲. همبسته‌سازی فعالیت‌های سیستمی بر اساس داده‌های ریسکی اپلیکیشن‌ها و بدافزارها؛
۳. گزارش‌دهی تست‌ها، تحلیل تهدیدها، انطباق‌پذیری با مقررات، سناریوهایی «اگر ...، آن وقت چه‌کار کنیم؟»، الزامات منابع و موارد دیگر؛
۴. مشاهده، مرتب و فیلتر کردن داده‌های قبلی برای داشتن دیدگاه‌هایی چندگانه؛
۵. مکان‌یابی شبکه (محلی و از راه دور)، وب، موبایل، ابر و دارایی‌های مجازی و همچنین حساب‌های دارای حقوق ویژه؛
۶. نمایه‌سازی IP، DNS، OS، آدرس مَک، کاربران، حساب‌ها، عمر رمزهای عبور، پورت‌ها، سرویس‌ها، نرم‌افزار، فرآیندها، سخت‌افزار، رویدادها و موارد دیگر؛

[1] Advanced Persistent Threats

۷. انجام گروه‌بندی، ارزیابی و گزارش دارایی‌ها با توجه به محدوده IP، روش نام‌گذاری، سیستم‌عامل، دامنه، برنامه‌ها، عملکرد کسب‌وکار، اکتیو دایرکتوری و موارد دیگر؛
۸. وارد کردن داده‌ها از اکتیو دایرکتوری، LDAP، IAM یا تنظیم مجوزهای سفارشی؛
۹. گردش کاری، ارسال تیکت و اعلان برای هماهنگی تیم‌های IT و امنیتی؛
۱۰. اشتراک داده‌ها با SIEM، GRC، NMS و راهکارهای هِلپ‌دِسک.

با یکپارچه‌سازی مدیریت دسترسی‌های ممتاز و دیگر راهکارهای مدیریت تهدید، تیم‌های IT و امنیت دیدی یکتا و مفهومی دارند که بتوانند با استفاده از آن ریسک کاربر و دارایی‌ها را تشخیص داده و آن‌ها را برطرف سازند.

گام ۱۰: یکپارچه‌سازی حساب های ممتاز

گام ۴ را به خاطر آورید. وقتی شما کنترل بیشتری روی دسترسی‌های ممتاز در سرورها دارید، گام منطقی بعدی آن است که آن سیستم‌ها را تحت مدیریت، سیاست و شناسایی یگانه (SSO) با ثبات درآورید. یونیکس، لینوکس و مَک از قبل سیستم‌هایی مدیریت‌شده و مستقل بوده‌اند، هر کدام بخشی مجزا با کاربران، گروه‌ها، سیاست‌های کنترل دسترسی، فایل‌های پیکربندی و رمزهای عبور منحصربه‌فرد خود را دارند. باید در نظر داشت که مدیریت یک محیط ناهمگن که متشکل از تمام این بخش‌ها است، به‌علاوه محیط‌های مایکروسافت ویندوز و فضای ابری، منجر به بی‌ثباتی مدیریتی برای تیم IT می‌شود، همچنین باعث پیچیدگی غیرضروری برای کاربران نهایی و پراکندگی حساب‌های نام مستعار می‌شود. این موارد تهدیداتی شناخته‌شده و حوزه‌های مورد علاقه برای عامل تهدید هستند.

بنابراین، سازمان‌های IT چطور به پیکربندی سیاست‌ها جهت دستیابی به الزامات قانونی، همچنین تجربه‌ای ساده‌تر برای کاربران و مدیران و ریسک کمتر برای یک سیستم با مدیریت نامناسب، دست یابند؟

راهکار ایده‌آل آن است که احراز هویت برای یونیکس، لینوکس و مَک را با گسترش احراز هویت کربروس[1] اکتیو دایرکتوری مایکروسافت و قابلیت‌های شناسایی یگانه (SSO) به این پلتفرم‌ها، متمرکز سازیم. با گسترش سیاست گروهی به این پلتفرم‌های غیر ویندوزی، شما به

[1] Kerberos

مدیریت پیکربندی متمرکزی دست می‌یابید که ریسک و پیچیدگی مدیریت یک محیط ناهمگن را کاهش داده و پراکندگی حساب‌های نام مستعار را متوقف می‌سازد.

۵ قابلیت برتر پل زدن در اکتیو دایرکتوری باید شامل موارد زیر باشد:

۱. بدون نیاز به اصلاح طرح اکتیو دایرکتوری برای اضافه شدن سیستم‌های لینوکس، یونیکس و یا مَک به شبکه. اینکار با تکامل فناوری، پایداری را به ارمغان می‌آورد؛
۲. ارائه یک چهارچوب قابل اتصال با یک رابط مشابه با کنسول مدیریت مایکروسافت روی لینوکس و مَک و پشتیبانی کامل برای اپلیکیشن مدیریت‌کننده گروه‌کاری[1] اپل که امکان مدیریت بی‌نقص و کنترل تنظیمات سیستم مَک را ممکن می‌سازد؛
۳. شناسایی یکتا (SSO) برای هر اپلیکیشن سازمان که از کربروس یا LDAP پشتیبانی می‌کند؛
۴. ارائه یک مجموعه ابزار مشابه مجزا برای مدیریت سیستم‌های ویندوزی و یونیکسی (مثل کاربران و کامپیوترهای اکتیو دایرکتوری، ADUC)؛
۵. ایجاد این امکان برای کاربران جهت استفاده از اعتبارنامه‌های اکتیو دایرکتوری خود، در دسترسی به سیستم‌عامل‌های یونیکس، لینوکس و مَک، همچنین هماهنگ کردن انواع فایل‌های رمز عبور، NIS و فضاهای ذخیره‌سازی LDAP درون اکتیو دایرکتوری و حذف نیاز به مدیریت مجزای حساب‌های کاربران.

این مفاهیم، مدیریت و سیاست پیکربندی ساده سیستم‌های غیر ویندوزی را ممکن می‌کند و به بهبود امنیت و تجربه کاربری کمک می‌نماید. این رویکرد به سازمان شما کمک می‌کند تا با کاهش تعداد ورودها (و تماس‌های مربوط به هِلپ‌دِسک)، همچنین کاهش تعداد مختلف سیستم‌ها، پیکربندی‌ها و سیاست‌های نیازمند مدیریت، کارآمدتر شود. پس با کمتر شدن حساب‌ها به حسابرسی‌های کمتری نیاز داشته و سطح ریسک برای عامل تهدید کمتر می‌شود.

گام ۱۱: حسابرسی و بازیابی

وقتی شما سیستم‌های غیر ویندوزی خود را با اکتیو دایرکتوری یکپارچه کردید، گام بعدی آن است تا فعالیت‌های کاربر را حسابرسی کنید تا دیدی بیشتر از تغییرات AD به دست آورید

[1] Workgroup Manager

که می‌تواند کل سازمان را تحت تأثیر قرار دهد اما سعی بر اینکه تمام تغییرات ایجادشده، به‌صورت دستی در اکتیو دایرکتوری صورت گیرد یک فرآیند بسیار زمان‌بر و پیچیده با تأخیرهایی در کشف و حل تغییرات است که احتمالاً به اختلال در کسب‌وکار سازمان منجر می‌شود.

وقتی شما دیگر فناوری‌های مایکروسافت را به‌صورت ترکیبی به کار می‌گیرید، درک «چه کسی، چه چیزی، چه زمانی و چه جایی» از تغییرات در کل زیرساخت ویندوز، پیچیده‌تر نیز می‌شود.

بنابراین سازمان‌های IT چطور این تغییرات را بهتر درک کنند و این قابلیت را داشته باشند که در صورت نیاز، آن‌ها را برگردانند و در فاز اول حقوق درستی را در سراسر یک زیرساخت ویندوزی پیچیده ایجاد کنند به‌گونه‌ای که آن‌ها بتوانند به‌صورت مؤثر از کسب‌وکار سازمان محافظت نمایند؟

سازمان‌ها به حسابرسی متمرکز و لحظه‌ای تغییرات در اکتیو دایرکتوری، سرورهای فایل، تبادلات و SQL نیاز دارند و همچنین در صورت نیاز اقدام به بازیابی اکتیو دایرکتوری در زیرساخت‌های ویندوزی سازمان کنند. سازمان‌ها از طریق مدیریتی ساده می‌توانند این ریسک‌های مربوط به تغییرات ناخواسته انجام‌شده توسط عاملان تهدید، افراد درون‌سازمانی و غیره را کاهش دهند و همچنین فعالیت کاربر را بهتر درک کرده تا بتوانند الزامات را محقق کنند.

برای اجرای این وظایف قانونی ضروری، این سه قابلیت برتر حسابرسی و حفاظت را در نظر بگیرید:

۱. حسابرسی و شناسایی «چه چیزی، چه کسی، چه جایی و چه زمانی» تغییراتی که انجام شده‌اند؛
۲. ارائه مکانیزمی برای پشتیبان‌گیری از اکتیو دایرکتوری و بازیابی آن. برگرداندن یک تغییر مجوز تصادفی (به‌وسیله عامل تهدید) می‌تواند شکاف‌های پیش‌بینی‌نشده‌ای در امنیت سازمان را هموار سازد؛
۳. حسابرسی و گزارش در چندین دامنه ویندوزی و سرورهای مورد اعتماد.

با این قابلیت، شما یک حسابرسی دقیق و لحظه‌ای از محیط‌های AD به دست می‌آورید و این قابلیت را دارید تا تغییرات ناخواسته را در صورت بروز تهدید یا اشتباه بازگردانید. اگر شما می‌دانید که یک عامل تهدید به خودش حقوق ویژه‌ای اعطا کرده است، دوست دارید شما هم آن را بدانید؟ حسابرسی و بازیابی حقوق ویژه در AD یک گام ساده به‌منظور تعیین و کاهش این ریسک است.

گام ۱۲: به‌کارگیری پُشته هویت[1]

مدیریت هویت و دسترسی (IAM) نقشی حیاتی در استراتژی امنیت IT یک سازمان دارد. با رشد سازمان‌ها، تعداد برنامه‌ها، سرورها و پایگاه‌های داده نیز رشد می‌کند. دسترسی به منابع سازمان معمولاً از طریق راهکارهای IAM مدیریت می‌شود که قابلیت‌هایی مانند شناسایی یگانه (sso)، تدارک بستر، مدیریت کاربر، کنترل دسترسی و نظارت را انجام می‌دهد اما امن‌سازی داده‌های حساس یک سازمان و برنامه‌های آن به چیزی بیشتر نیاز دارد. کاربران ارائه‌شده، جدای از حقوق ویژه، اگر فعالیتی که انجام می‌دهند به‌درستی نظارت نشود و مستند نگردد، می‌تواند سازمان را در معرض خطر قرار دهد. راهکارهای مدیریت هویت و دسترسی به تیم‌های IT کمک می‌کنند که سؤال «چه کسی به چه چیزی دسترسی دارد؟» را پاسخ دهند اما برای دستیابی به رؤیت‌پذیری کامل از کاربر، راهکارهای مدیریت دسترسی‌های ممتاز باقی سؤالات را پاسخ خواهد داد: آیا این دسترسی مناسب و به‌جا است؟ و آیا این دسترسی استفاده درستی انجام می‌دهد؟ این یعنی، PAM باید رؤیت‌پذیری و حسابرسی عمیق‌تری از دسترسی و استفاده از حساب‌های ممتاز ارائه دهد. اکثر اوقات، راهکارهای IAM کاربران را به سیستم یا گروهی از برنامه‌ها متصل می‌کنند اما جزئیاتی از اینکه چه چیزی به اعضاء آن گروه ارائه می‌شود یا دسترسی به جزئیات ثبت نشست و کلیدهای فشرده‌شده طی نشست دارای حقوق ویژه ارائه نمی‌کنند. همین‌طور، PAM رؤیت‌پذیری راهکار IAM را برای افزایش کنترل‌های امنیتی و حسابرسی گسترش می‌دهد.

[1] Identity Stack

فصل ۲۳

نکات کلیدی

حقوق ویژه به‌عنوان اهدافی برای حمله، در دسترس‌ترین هدف برای عاملان تهدید در دنیای دیجیتال امروزی هستند. درحالی‌که معماری و امن‌سازی یک محیط همچنان به نسبت پیچیده است ولی این ۲۰ توصیه مهم می‌تواند به هر متخصص امنیتی کمک کند تا به اهداف خود دست یابد و ریسک‌های موجود برای سازمان را حداقل سازد:

۱. از حساب‌های استاندارد برای کاربران استفاده کنید- اجرای اینکه تمام کاربران یک حساب استاندارد داشته باشند. مدیران در تمام پلتفرم‌ها باید با حساب‌های استاندارد خود وارد شوند. آن‌ها فقط باید زمانی که به اجرای وظایف مدیریتی نیاز است با حقوق مدیریتی وارد شوند؛

۲. هرگز رمزهای عبور را به اشتراک نگذارید- ریسک‌های مربوط به یک رمز عبور به اشتراک گذاشته‌شده با همکار یا پیمانکار، تنها ریسک سوءاستفاده از رمز عبور را بالا می‌برد؛

۳. هرگز از رمز عبورهای یکسان استفاده نکنید- اگر منبعی آلوده شود، تمام منابع دیگر که از آن رمز عبور یکسان استفاده می‌کنند، در خطر هستند؛

۴. هرگز رمزها را به شکل متنی آشکار ذخیره نکنید- رمزهای عبور باید سری نگهداری شوند. رمزها هرگز نباید به‌صورت متن ساده ذخیره شوند و این ربطی به نحوه ذخیره‌سازی ندارد؛

۵. رمزهای عبور را ایمن نگه دارید- اگر لازم است که رمزهای عبور مستند شوند، باید در یک فایل رمزگذاری‌شده و فایل سیستمی ایمن قرار گیرند و در صورت نیاز در یک مکان فیزیکی امن نگهداری شوند؛
۶. تعداد نام‌های مستعار را حداقل سازید-قابل ردیابی افراد و غیر قابل هک کردن آن‌ها کلید شناسایی استفاده از حقوق ویژه به‌عنوان هدفی برای حمله است؛
۷. تعداد حساب‌های مدیریتی را حداقل کنید- هرچه تعداد کاربران ممتاز کمتر باشد، سطح ریسک کمتر است و به نظارت و حسابرسی کمتری برای فعالیت‌های ممتاز نیاز است؛
۸. رمزهای عبور را مرتباً عوض کنید- رمزهای عبور را باید بعد از هر بار استفاده برای یک فعالیت ممتاز و یا بر اساس زمان‌بندی منظم برای حساب‌های استاندارد تغییر داد. این کار مانع از قدیمی شدن آن‌ها می‌شود؛
۹. مطمئن شوید رمزهای عبور کاملاً پیچیده هستند- رمزهای دارای حقوق ویژه نباید توسط انسان قابل خواندن باشند. این کار سبب می‌شود نتوانند به‌راحتی آن را کپی کرده یا با زبان بیان کنند. هر رمز عبوری باید مطابق با سیاست‌های پیچیدگی کلمه عبور انتخاب شود؛
۱۰. احراز هویت چند مرحله‌ای را ضروری کنید- احراز هویت چند مرحله‌ای را برای دسترسی به سیستم‌های داخلی، برنامه‌ها و داده‌ها پیاده‌سازی کنید. باید در نظر داشت که محدودسازی زیاد می‌تواند برای کاربران عذاب‌آور باشد. به دنبال راهکارهایی بگردید که می‌توانند دسترسی را نیز بر اساس ریسک مربوط به محیط یا فعالیت محدود سازند. برای مثال اگر شخصی بخواهد اپلیکیشن حساسی را بعد از ساعتی برای اولین بار اجرا کند و یا سعی داشته باشد تا دستور حساسی را روی سرور یونیکسی اجرا کند که فاقد وصله‌های حیاتی است، امنیت را راه‌اندازی کنید و احراز هویت چند مرحله‌ای را آغاز کنید؛
۱۱. کنترل اپلیکیشن را پیاده‌سازی کنید (اضافه کردن برنامه‌ها به لیست سفید، سیاه و خاکستری)- سیاستی را پیاده‌سازی کنید که به برنامه‌های خوب شناخته‌شده امکان اجرا دهد و تمام برنامه‌های دیگر و تلاش‌های آن‌ها برای اجرا شدن را ثبت کند. در صورت امکان، اجرای برنامه‌های کاربر نهایی که آسیب‌پذیری‌های امنیتی شناخته‌شده حیاتی را دارند، محدود کنید.

۱۲. اصل حقوق ویژه حداقلی را اجرا کنید- اگر کاربری نیازی به دسترسی به سیستم‌ها، برنامه‌ها و یا داده‌ها ندارد، آن را حذف کنید. حقوق مدیریتی روی دسکتاپ‌ها برای تمام کاربران را حذف کنید (حداقل حقوق ویژه را با نظارت بر یکپارچگی فایل در نظر بگیرید تا استفاده مناسب از سیستم‌ها را تضمین نموده و فعالیت‌های حساب‌های آلوده را به‌صورت مؤثرتری شناسایی کنید).

۱۳. مدیریت رمز عبور را به‌صورت خودکار انجام دهید- درخواست‌ها برای رمزهای عبور مدیریتی را کنترل کرده و حسابرسی نمایید. استفاده از رمزهای عبور یکتا برای تمام سیستم‌ها و حساب‌های ممتاز را ضروری کنید؛

۱۴. پا را از رمزهای عبور فراتر بگذارید- رمزهای عبور نوشته‌شده در کد برنامه در حساب‌های خدماتی و اسکریپت‌ها را حذف کنید. ابزارهای مدیریت کلید SSH را پیاده‌سازی کنید؛

۱۵. از کنترل‌های مبتنی بر محیط و نقش و دسترسی تطبیقی استفاده کنید- در برخی اوقات، افراد برای انجام کارشان نیاز به دسترسی دارند اما شما باید بر اساس زمان و موقعیتی که آن‌ها دسترسی می‌خواهند، مسدودسازی را انجام دهید. دسترسی بر اساس عناصری مثل زمانی از روز مناسب است اما محدودسازی دسترسی به‌صورت پویا و بر اساس ریسک (مثلاً آیا تیکتی برای دسترسی وجود دارد، آیا این دسترسی طبق الگوهای دسترسی عادی است، آیا اخیراً هشدارهایی از لایه‌های شناسایی تهدید دریافت شده و غیره) حفاظت بیشتری را ایجاد می‌کند؛

۱۶. نظارت بر تمام فعالیت‌های مربوط به نشست‌های ممتاز- هرگونه از فعالیت ممتاز با داده‌های مهم باید ضبط شود، کلیدها ثبت گردیده و اپلیکیشن مورد نظارت قرار گیرد تا برای بررسی مناسب بودن فعالیت مورد بازبینی قرار گیرد؛

۱۷. تعهدات حسابرسان و انطباق‌پذیری با مقررات را درک کنید- متخصصان امنیت تمام این عملکردها را برای امن‌سازی سازمان انجام می‌دهند. آن‌ها نباید این کار را نسنجیده انجام دهند، درک اینکه چه چیزی نیاز است و بهترین راه برای تحقق موارد اجباری، باعث می‌شود تا همه امن باقی بمانند و درنهایت حسابرسان راضی باشند؛

۱۸. نظارت پیشرفته تهدیدها و رفتارها را پیاده‌سازی کنید- جایی در سازمان، حساب‌هایی هستند که به داده‌ها دسترسی دارند. نظارت پایه‌ای امنیتی و شناسایی پیشرفته تهدید (شامل نظارت بر رفتار کاربر) را پیاده‌سازی کنید تا دقیق‌تر و سریع‌تر فعالیت‌های

حساب‌های آلوده‌شده و همچنین سرءاستفاده و استفاده اشتباه افراد درون سازمان را شناسایی کنید؛

۱۹. شبکه خود را تقسیم‌بندی کنید- دارایی‌ها شامل برنامه‌ها و سرورهای منبع را درون واحدهای منطقی گروه‌بندی کنید که هیچ‌کدام به دیگری trust نباشند. تقسیم‌بندی شبکه، دسترسی که هکرها باید از سیستم‌های داخلی شما داشته باشند، کاهش می‌دهد. برای دسترسی‌هایی که نیاز دارند از نواحی trust عبور کنند، سروری امن را با احراز هویت چندمرحله‌ای، اعتبارسنجی دسترسی و نظارت بر نشست اجرا کنید. هر جا که ممکن بود، پا را فراتر از استانداردهای تقسیم‌بندی شبکه بگذارید. تقسیم‌بندی را بر اساس زمینه کاربر و حقوق ویژه و منابع، برنامه‌ها و داده‌هایی که آن‌ها بدان دسترسی دارند، انجام دهید. این کار تحت عنوان ریزتقسیم‌بندی مطرح است؛

۲۰. اگر خوشحال نیستید باید شغل دیگری بیابید- اگر متخصص امنیتی خوشحال نباشد، کارش را به‌درستی انجام نمی‌دهد. تمام نکته‌های بیان‌شده در معرض خطر قرار می‌گیرند و درنتیجه سازمان در معرض خطر قرار می‌گیرد. متخصصان امنیت باید از کارشان راضی باشند، از محیط راضی باشند و به‌طور مرتب با چالش‌ها دست و پنجه نرم کنند. امنیت همیشه در حال تغییر است، خوشحال نبودن سبب می‌شود آخرین تهدیدات به سراغ شما بیایند. عامل تهدید اهمیتی نمی‌دهد که شما خوشحال هستید یا نه، آن‌ها تنها می‌خواهند به حساب‌های مدیریتی شما دست یابند؛ بنابراین باید شخصی باشد که همیشه به این موارد اهمیت داده و به آن‌ها پاسخ دهد.

فصل ۲۴: نتیجه‌گیری

پیش‌بینی‌های زیر در رابطه با تکامل PAM در آینده وجود دارد.

PAM یک لایه امنیتی است

مدیریت حساب‌های ممتاز چرخه عمر امنی را برای اعتبارنامه‌های ممتاز ممکن می‌سازد تا احراز هویت ایمن کاربران و برنامه‌ها به منابع را با استفاده از لایه‌های اضافی مانند فرآیندها، کنترل ها و حسابرسی تسهیل نماید. امروزه اکثر سازمان‌ها در جایی از زنجیره بین فرآیندهای دستی و خودکار در رویکرد مدیریت دسترسی‌های ممتاز قرار دارند. با وجود اینکه همچنان آگاهی و اطلاعات از PAM در حال رشد است، این رویکرد لایه امنیتی مبنایی است که باید درون تمام برنامه‌های امنیتی سازمان به کار گرفته شود. با بلوغ بازار، PAM به چیزی معمول بدل خواهد شد و یکپارچگی نزدیکی با چرخه عمر مدیریت هویت و دسترسی (IAM) پیدا خواهد کرد.

ساده‌سازی PAM

شرکت‌های PAM با توجه به خواسته مشتریان جهت ساده‌سازی PAM، به کار خود برای گسترش و ساده‌سازی اینترفیس‌های یکپارچه کنونی ادامه می‌دهند. سازمان‌های زیادی به دنبال آن هستند تا مجموعه ابزارهای مورد استفاده برای مدیریت امنیت داخلی سازمان خود را ساده‌سازی نمایند. سازمان‌های زیادی راهکارهای PAM را برای حل یافته‌های خاصی از حسابرسی‌ها یا چالش‌ها خریده‌اند اما این کار منجر به تکه‌های جدا از هم محصولات، کنسول‌ها و فرآیندهای فنی شده است که به‌درستی مدیریت نمی‌شوند. تحلیلگران پیشرو هر یک از این‌ها را به‌عنوان مؤلفه‌هایی از یک استراتژی موفق PAM می‌بینند که باید به‌صورت پیشنهادی یکپارچه بوده و به شکل مجموعه محصولاتی مجزا نباشند.

سازگاری به‌عنوان یک محرک

به‌طور مرسوم، سازمان‌های زیادی مدل‌های اجرایی PAM را روی زیرمجموعه کوچکی از حیاتی‌ترین سرورها و برنامه‌ها متمرکز کرده‌اند. با حرکتی رو به جلو، سازمان‌ها به گسترش استفاده از PAM جهت تطابق با مقررات، تقویت امنیت و ساده‌سازی عملیات ادامه می‌دهند. سازمان‌ها PAM را به‌عنوان لایه امنیتی مبنا می‌شناسند و به کار برای تضمین پوشش کامل آن بر همه چیز (یونیکس، لینوکس، مَک، ویندوز، مجازی، ابری، زیرساخت حیاتی، برنامه‌ها، SaaS، اینترنت اشیاء و فرآیندهای DevOps) ادامه می‌دهند. با ادامه رویه سازمان‌ها در سرمایه‌گذاری‌های استراتژیک کسب‌وکاری که روی فناوری‌های خاص تکیه دارد، اینکه از چنین فناوری‌هایی در برابر افراد مخرب درون‌سازمانی و تهدیدات خارجی محافظت کنیم، حیاتی است.

سیاست پویا

سازمان‌ها با استفاده از PAM، استراتژیک‌تر می‌شوند. با وجود اینکه داده‌های PAM محتوای ارزشمندی را ارائه می‌کنند که می‌تواند در سیستم‌های امنیتی و شناسایی مورد استفاده قرار گیرد اما اضافه کردن زمینه‌های بیشتر در ماژول‌های سیاست‌ها، به مقاوم‌سازی بیشتر سیاست دارای حق ویژه بر اساس محیط و دیگر فاکتورهای ریسکی کمک می‌کند. سیاست‌ها، تطبیقی و پویا خواهند شد و به‌صورت خودکار بر اساس زمینه تغییر می‌کنند تا تهدیدات مدرن را در بر گیرند.

تحلیل‌های پیشگیرانه

با آغاز به کار PAM در تحکیم و همبسته کردن اطلاعات، حجم رویدادها و داده‌های ثبتی نشست ها و غیره افزایش می‌یابد. با وجودی که همبسته‌سازی گزارش‌ها در پلتفرم‌های مختلف و ماژول‌های PAM کمک‌کننده است اما به تحلیل‌های پیچیده‌تر و خودکارسازی نیاز است تا سازمان‌ها بتوانند همیشه پیشرو باقی بمانند تا بتوانند استفاده نادرست و سوءاستفاده از حقوق ویژه را تشخیص دهند. برنامه‌های امنیتی PAM بلوغ می‌یابند و تحلیل‌های رفتاری و پیش-بینی‌کننده را برای شناسایی ناهنجاری‌ها و تولید هشدارها و گزارش‌ها به‌صورت خودکار

پیاده‌سازی می‌کنند. عاملان تهدید روزبه‌روز در حال پیشرفت هستند و راهکارهای PAM نیز برای مبارزه با این تهدیدات ساکن نمانده و تکامل می‌یابند.

درنتیجه، PAM در آینده فقط محدود به هویت‌ها، حساب‌ها، اعتبارنامه‌ها و رمزهای عبور باقی نمی‌ماند. PAM به رشد و تکامل خود ادامه داده تا بیشتر شبیه به سیستمی برای جلوگیری از نفوذ یا تقلب گردد و فقط ابزار مدیریت‌کننده حقوق ویژه و رمزهای عبور نباشد. سهل-الوصول‌ترین هدف و کم‌سرعت‌ترین شخص در بین افرادی که از دست یک خرس فرار می‌کنند، همان کسی است که این استراتژی‌ها را به کار نگرفته است و احتمالاً به محیط او نفوذ می‌شود.

Building Effective Cyber-Defense Strategies to Protect Organizations

Morey J. Haber, Brad Hibbert

مدیریت دسترسی های ممتاز (PAM) در ارتباط با مدیریت حقوق ویژه، شناسایی تکنیک ها و روش های مورد استفاده هکرها و عاملان تهدید، افزایش توانایی سازمان در شناسایی فعالیت های هکرها و تهدیدات داخلی است. همچنین در این کتاب تلاش می شود تا اقدامات دفاعی که سازمان ها باید برای محافظت در مقابل تهدیدات دسترسی های ممتاز در نظر بگیرند ارایه شود، در این کتاب فراخواهیم گرفت.

- چگونه هویت ها، اعتبارنامه ها، رمزهای عبور و اکسپلویت ها می توانند در طی یک حمله باعث ارتقا سطح دسترسی شوند
- پیاده سازی راهکارهای دفاعی و حسابرسی برای کاهش تهدیدات و ریسک ها
- درک و یادگیری یک برنامه ۱۲ مرحله ای برای پیاده سازی مدیریت دسترسی های ممتاز
- در نظر گرفتن ریسک ها، حسابرسی، مقررات و راهکارهای نظارتی در استقرار و محدوده مدیریت دسترسی های ممتاز

این کتاب برای چه کسانی است:

- برای متخصصین حوزه امنیت اطلاعات
- برای حسابرسان امنیت اطلاعات
- برای مدیران فناوری اطلاعات که به دنبال درک و حل تهدیدات مرتبط با دسترسی های ممتاز هستند.

ISBN: 978-600-995-725-5

ارشدان