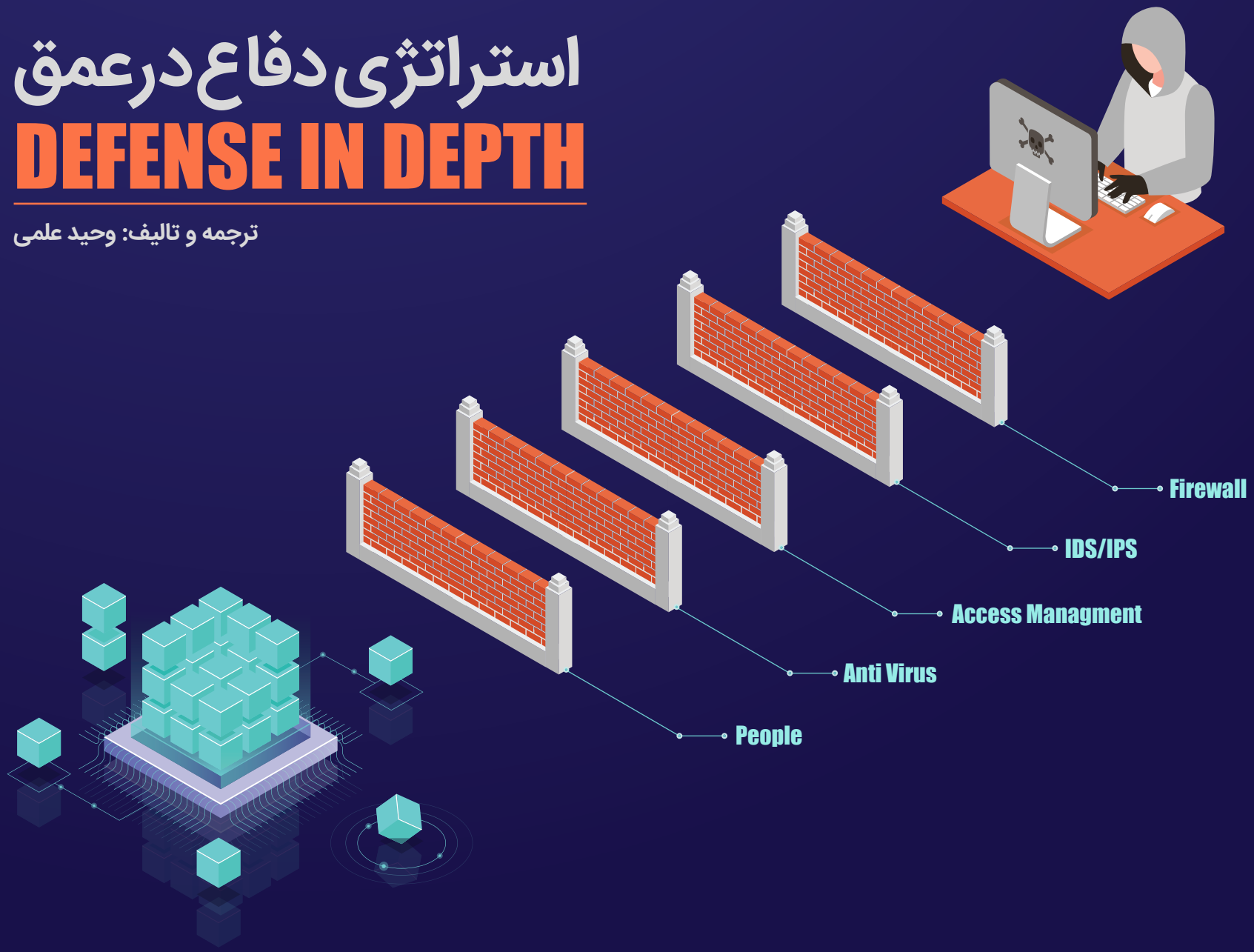
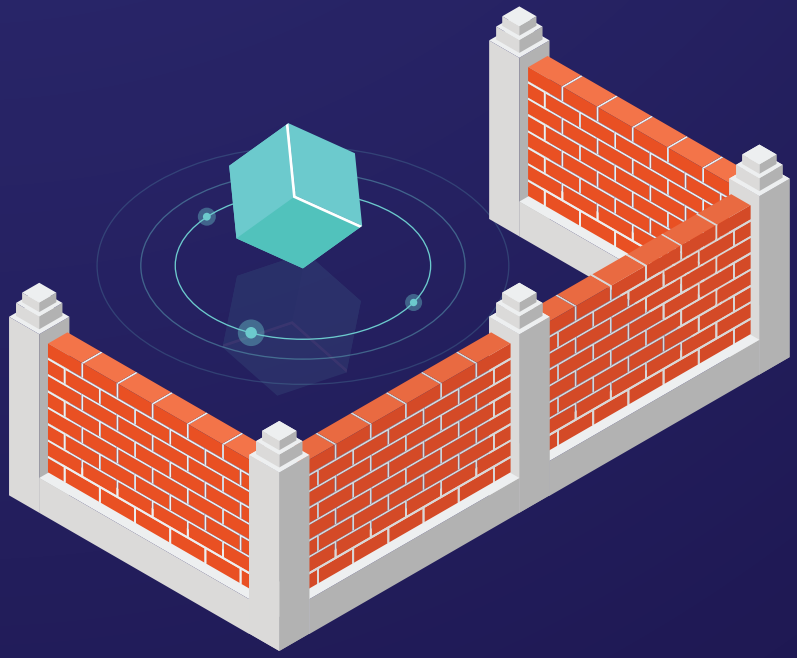
استراتژی دفاع در عمق
DEFENSE IN DEPTH

ترجمه و تالیف: وحید علمی



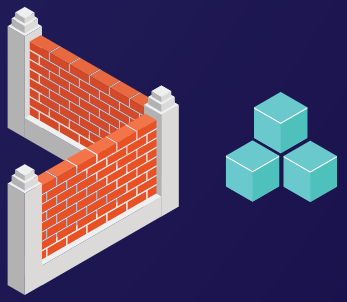
DEFENSE IN DEPTH



استراتژی دفاع در عمق یا Defense in Depth که به اختصار DiD نامیده می‌شود، مفهوم محافظت از شبکه رایانه‌ای با مجموعه‌ای از مکانیزم‌های دفاعی است، به گونه‌ای که اگر یک مکانیزم نتواند حمله را مسدود کند، مکانیزم دیگری برای خنثی کردن حمله آماده می‌باشد. در حقیقت هدف از این استراتژی این است که با ایجاد لایه‌های دفاعی، حملات مهاجمین سایبری مسدود شوند. در حقیقت استراتژی دفاع در عمق، استفاده هماهنگ از اقدامات متقابل امنیتی چندگانه به منظور دفاع از تمامیت دارایی‌های اطلاعات در یک شرکت در برابر مهاجمان سایبری است. این استراتژی مبتنی بر اصل نظامی است که شکستن یک سیستم دفاعی پیچیده و چند لایه برای دشمن، دشوارتر از نفوذ به یک سد واحد است. استراتژی دفاع در عمق، احتمال موفقیت هکرهای مخرب را به حداقل می‌رساند. یک استراتری دفاع در عمقی که به خوبی طراحی و مستقر شده است، می‌تواند به مدیران سیستم و پرسنل امنیتی کمک کند تا مهاجمانی که قصد به خطر انداختن یک رایانه، سرور، شبکه اختصاصی یا ISP دارند را شناسایی کنند. اگر هکر دسترسی به یک سیستم را داشته باشد، استراتژی دفاع در عمق اثرات منفی را به حداقل می‌رساند و به مدیران و مهندسان زمان می‌دهد تا اقدامات متقابل جدید یا به روز شده را برای جلوگیری از اتفاق مجدد به‌کار گیرند. مؤلفه‌های دفاع در عمق شامل نرم افزار آنتی ویروس، فایروال‌ها، برنامه‌های ضد جاسوسی، رمزهای عبور سلسله مراتبی، سیستم‌های تشخیص و جلوگیری از نفوذ و تأیید بیومتریک و همچنین ایجاد سیستم‌های مدیریت دسترسی چند مرحله‌ای است. علاوه بر اقدامات متقابل ذکر شده، حفاظت فیزیکی سایت‌های تجاری به همراه آموزش جامع و مداوم پرسنل، باعث افزایش امنیت داده‌های حیاتی در برابر نفوذ، سرقت یا تخریب می‌شود.

DEFENSE IN DEPTH

از آنجایی که مهاجمان سایبری بسیاری با طیف گسترده‌ای از روش‌های حمله و همچنین مقاصد مختلف وجود دارند، هیچ روش واحدی برای محافظت موفقیت آمیز از یک شبکه رایآن‌های وجود ندارد. استفاده از استراتژی دفاع در عمق باعث کاهش خطرات ناشی از حملات موفق آمیز و احتمالاً پرهزینه، به شبکه می‌شود. در این مقاله، سه سناریوی متداول برای حملات شبکه، روش‌های احتمالی حمله و اقدامات متقابل برای محافظت از شبکه در برابر حملات بررسی خواهند شد. سناریو اول حمله توسط یک جوجه هکر!! یا همان «اسکریپت‌کیدی» از اینترنت است، سناریو دوم حمله توسط یک هکر ماهر است و سناریو نهایی از طریق یک کاربر داخلی و قابل اعتماد است که به شبکه دسترسی دارد. در این مقاله هدف پاسخ به سوالاتی همچون «هکرها چه کسانی هستند» یا «از چه روش‌هایی استفاده می‌کنند» و یا «از چه روش‌هایی برای محافظت در برابر آن‌ها می‌توان استفاده کرد»، نیست. این موضوعات نیاز به نوشتن کتاب‌هایی با حجم‌های زیاد دارند و بسیار فراتر از حد و هدف این مقاله است. این مقاله سعی دارد با استفاده از تعدادی مثال ساده برای نشان دادن لزوم اجرای استراتژی دفاع در عمق، شما را با فواید پیاده سازی آن آشنا کند.



سناریو اول:
اسکریپت‌کیدی

اسکریپت‌کیدی کسی است که به دنبال انجام حمله آسان و تقلیدی است. این دسته هیچ موقع اطلاعات خاص را مورد حمله قرار نمی‌دهند، همچنین سازمان‌های خاص از برنامه این دسته خارج هستند. هدف آن‌ها این است که ساده‌ترین روش برای دستیابی به کاربری root را پیدا کنند. آن‌ها این کار را با تمرکز روی تعداد کمی از اکسپلویت‌ها انجام می‌دهند و سپس به جست و جوی کل اینترنت برای پیدا کردن اکسپلویت می‌پردازند. دیر یا زود آن‌ها اهداف آسیب پذیر را بدون داشتن هدف خاصی پیدا می‌کنند. با وجود عدم دانش فنی، اسکریپت‌کیدی‌ها بسیار خطرناک هستند زیرا اهمیتی نمی‌دهند به چه کسی حمله می‌کنند و می‌توانند بر توانایی‌های فنی دیگران سرمایه گذاری کنند. فرد می‌تواند به سایتی مانند www.exploit-db.com مراجعه کند که دارای لیستی از اکسپلویت‌ها، بحث در مورد اکسپلویت‌ها، اطلاعاتی درباره نحوه شناسایی سیستم‌های آسیب پذیر و کدهایی برای شروع حمله است. این موارد در واقع همه آن چیزی است که برای شروع حمله لازم است.

بهترین راه دفاع در برابر اسکریپت‌کیدی‌ها، دفاع محیطی است. به‌عنوان مثال یک فایروال ترافیک ورودی و خروجی را در یک شبکه نظارت و مدیریت می‌کند و برای ایجاد یک دفاع محیطی ضروری است. با اینکه فایروال‌ها بسیار موثر هستند، اما نمی‌توان به آن‌ها، به‌عنوان تنها راه تامین امنیت شبکه اعتماد کرد. بنابر تحقیقات موسسه SANS تکیه بیش از حد برروی فایروال یکی از هفت اشتباه رایج مدیریتی است که امنیت شبکه را به خطر می‌اندازد. سیستم‌های تشخیص نفوذ مبتنی بر شبکه (NIDS) و سیستم‌های جلوگیری از نفوذ (IPS) لایه دیگری از دفاع محیطی را فراهم می‌کنند. Stephen Northcutt در کتاب خود که با عنوان کتابچه راهنمای نفوذ شبکه منتشر شده است و یک کتابچه راهنمای تجزیه و تحلیل می‌باشد، می‌گوید:

«هنگامی که یک نابینا، می‌تواند ببیند. این همان چیزی است که یک سیستم تشخیص نفوذ برای سازمان انجام می‌دهد: کمک می‌کند تا یک سازمان از حالت نابینا به حالت بینایی برود و این مورد قطعاً اتفاق خوبی است».

سیستم‌های تشخیص نفوذ مبتنی بر شبکه، به منظور شناسایی اسکن‌ها یا الگوهای ترافیکی که نشان دهنده حمله است، بر ترافیک شبکه نظارت می‌کنند. این سیستم‌ها می‌توانند امضاهای حملات که از قبل تعریف شده‌اند یا رفتارهای غیرعادی را که نشان دهنده حمله به سمت شبکه است، تشخیص دهند. سیستم‌های تشخیص نفوذ مبتنی برشبکه می‌توانند حملاتی را شناسایی کنند که قبل از آن غیرقابل شناسایی و مشاهده بودند. گاهی اوقات اقدامات متداول مانند تعامل با فایروال، به‌منظور متوقف کردن ترافیک خاص، هشداری را به یک مدیر، از یک مشکل خاص ارسال می‌کند و می‌تواند به شناسایی آسیب پذیری که در این رویداد انجام شده است، کمک کند.

با وجود همه این روش‌های دفاع محیطی، گاهی ممکن است یک اسکریپت‌کیدی بتواند به شبکه نفوذ کرده و دسترسی بگیرد. شاید برایتان جالب باشد بدانید که برخی از مخرب‌ترین حوادث امنیتی تا به امروز، حملات تصادفی بوده‌اند که توسط اسکریپت‌کیدی‌ها صورت گرفته است. از آنجا که راه‌هایی برای دور زدن لایه‌های دفاعی مانند فایروال‌ها وجود دارد، نیاز است که سیستم‌های فردی نیز محافظت شوند. با اطمینان از اینکه سیستم‌ها تمام وصله‌های امنیتی که وندورها ارائه می‌دهند را نصب کرده‌اند، سیستم‌ها را هاردن کنید، همچنین از نرم افزار آنتی ویروس بر روی سیستم‌ها استفاده کرده و سرویس‌های غیرضروری و بدون استفاده را غیرفعال کنید. پروژه Honeynet بینش زیر را در مقاله «دشمن خود را بشناس» ارائه می‌دهد.

«اسکریپت‌کیدی‌ها به دنبال راه نفوذ آسان هستند، آن‌ها به دنبال استفاده از اسکپلویت‌های متداول به منظور انجام نفوذ خود می‌باشند. اطمینان حاصل کنید که سیستم‌ها و شبکه‌های شما در برابر این سوءاستفاده‌ها آسیب پذیر نیستند ...»

یکی از مهمترین نکات این است که مدیران شبکه‌ها باید از اخبار جدید در مورد انتشار آسیب پذیری‌های جدید و همچنین انتشار وصله‌های امنیتی آگاه باشند. امروزه وبسایت‌ها و منابع بسیاری به این منظور وجود دارد که مدیران می‌توانند از آن‌ها استفاده کنند.

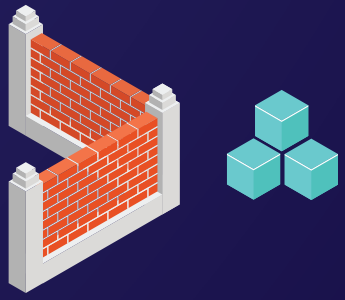
نکته دیگری که باید ذکر شود این است که اسکریپت کیدی‌ها ممکن است از روش‌های مهندسی اجتماعی نیز استفاده کنند. مهندس اجتماعی یک روش متداول برای حمله و دور زدن فایروال به حساب می‌آید. با توجه به تحقیقات انجام شده، بیشترین درصد انجام حملات مهندسی اجتماعی از طریق ایمیل انجام می‌شود. مهمترین خط دفاع در برابر این نوع حملات، آموزش کاربران است. Tom Peltier در مقاله خود با عنوان «برنامه آگاهی از امنیت» جامعه کاربران را برای فرآیند امنیت شبکه بسیار مهم می‌داند. او نوشته است:

«در صورت عدم وجود فرآیندی برای اطمینان از اینکه کارمندان از حقوق و مسئولیت‌های خود آگاه هستند، یک معماری امنیتی قوی چندان موثر و کارا نخواهد بود. اغلب اوقات، متخصصان امنیتی برنامه امنیتی «بی نقصی» را اجرا می‌کنند، درحالی که فاکتور مهم آگاهی کاربران را درنظر نمی‌گیرند.»

جامعه کاربران شبکه باید از تهدیدات مربوط به امنیت شبکه آگاه باشد. به‌عنوان مثال آن‌ها باید خطرات باز کردن پیوست‌های ایمیل، ارسال اطلاعات حساس از طریق شبکه و ... را به‌خوبی درک کرده و بدانند.

یکی دیگر از تهدیدات مربوط به امنیت شبکه که اسکریپت‌ها انجام می‌دهند، حملات تکذیب سرویس (DoS) است. حمله DoS حمله‌ای به منابع شبکه برای جلوگیری از دستیابی کاربران به آنچه نیاز دارند است. به عنوان مثال، حمله smurf از روترهایی که به درستی پیکربندی نشده‌اند، به منظور استفاده کامل از پهنای باند، استفاده می‌کنند، بنابراین کاربران مجاز نمی‌توانند به منابع شبکه دسترسی پیدا کنند. حملات Syn flood از ضعف داخلی TCP/IP برای اتصال منابع سیستم استفاده می‌کند تا کاربران نتوانند به هاست خاصی دسترسی پیدا کنند. تعداد بیشماری حملات دیگر وجود دارد که می‌توانند حساب‌های کاربر را قفل کنند، درایوهای دیسک را پر کنند، خرابی CPU را به بار آورند و موارد دیگر.

اسکریپت‌کیدی‌ها اغلب زمانی که نمی‌توانند کاری را انجام دهند، به حملات DoS روی می‌آورند. بسیاری از حملات DoS توسط یک محیط قوی و سیستم‌های پیکربندی شده قابل پیشگیری هستند، اما بعضی از این حملات قابل متوقف کردن نیستند و منجر به قطع سرویس‌دهی می‌شوند.



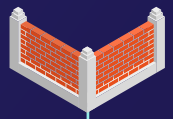
سناریو دوم:
مهاجم ماهر

حملات مهاجمانی که مهارت بالایی دارند، با فرکانس کمتری اتفاق می‌افتد اما بیشتر اوقات موفقیت آمیز است.
کوین میتنیک یکی از ماهرترین مهاجمان در مجلس سنا به این صورت شهادت داد:
«من با موفقیت تمام سیستم‌هایی را که برای دستیابی غیرمجاز هدف قرار داده‌ام، به خطر انداخته‌ام. من در برخی از بزرگترین شرکت‌های جهان به سیستم‌های رایانهای غیرمجاز دسترسی پیدا کرده‌ام و با موفقیت در برخی از مقاوم‌ترین سیستم‌های رایانه‌ای که تاکنون توسعه یافته، نفوذ کرده‌ام.»
مهاجمان ماهر با تحقیق در مورد شرکتی که می‌خواهند مورد حمله قرار دهند، با استفاده از روش‌های اضافی حمله، به‌طور معمول موفق‌تر عمل می‌کنند و با همان ابزارهای موردنظر اسکریپت‌کیدی‌ها، تهاجمی‌تر عمل می‌کنند. استفاده از دیواره‌های آتشی که به درستی تنظیم شده‌اند، ایمن کردن سیستم‌ها به‌صورت جداگانه، به‌کارگیری سیستم‌های تشخیص و جلوگیری از نفوذ و نرم افزارهای آنتی ویروس از اهمیت زیادی برخوردار هستند، اما روش‌های اضافی نیز باید مورد استفاده قرار گیرند.
دستیابی اطلاعات در مورد شبکه‌ها می‌تواند به راحتی در دسترس باشد و به همین علت هکرها به راحتی می‌توانند اطلاعات را در مورد سازمان‌ها جمع آوری کنند. اما حتی ماهرترین مهاجمان نیز غالباً روزها را صرف تحقیق در مورد اهداف خود می‌کنند، و طی این تحقیق لیستی از راه‌های نفوذ را آماده می‌کنند. پس از شناسایی آسیب پذیری، احتمالاً بهره برداری از آسیب پذیری در مدت زمان بسیار کمی اتفاق می‌افتد.
مهاجمان ماهر شرکت‌ها را بررسی می‌کنند و شبکه شرکت‌ها را به منظور کشف نقطه ورود به شبکه، بررسی و تست می‌کنند. این نقاط ورودی ممکن است از اینترنت، یک بستر اینترانت مشترک، یک اکسترانت و یا حتی درب جلوی ساختمان شرکت باشد. با شناسایی همه نقاط ورودی، مهاجم برای دستیابی به شبکه بهترین راهی که موجب دسترسی به شبکه می‌شود را تعیین می‌کند.

مهاجم ماهر از اطلاعات شرکت برای اکسپلویت موفقیت آمیز در حملات مهندسی اجتماعی استفاده خواهد کرد. به‌عنوان مثال، این مهاجمان ممکن است از طریق موقعیت شغلی یک هلپ‌دسک با مدیرعامل شرکت تماس بگیرند و خواستار تغییر رمز عبور وی یا ارسال یک تروجان از طریق ایمیل به یک کارمند باشند. این نوع حملات بسیار موفق خواهند بود زیرا مهاجمان با دسترسی به نام‌های مدیران و همچنین دسترسی به ایمیل‌ها، می‌توانند بسیاری از حملات مهندسی اجتماعی را انجام دهند، و از این طریق چون ایمیل از سمت یک مدیر به کارمندان بخش‌ها صادر می‌شود، مورد تایید خواهد بود. موضوعی که بازهم باید یادآوری شود این است که تنها راه مقابله با این نوع حملات، آموزش افراد شاغل در سازمان است.

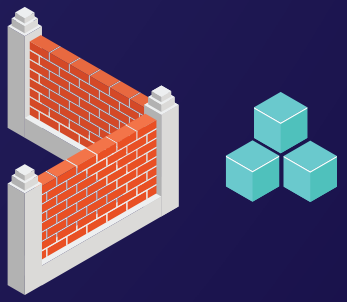
به منظور مقابله با حملات مهندسی اجتماعی، شرکت‌ها باید آگاهی همه کارمندان را تا جایی افزایش دهند که هرگونه درخواست غیرمعمول برای اطلاعات، به عنوان تهدید تلقی شود. موضوع مهمی که باید در سازمان‌ها نهادینه شود این است که تنها مدیران سیستم‌ها و امنیت، مسئول برقراری امنیت شبکه نیستند. همه افراد از نگهبانان گرفته تا کارمندان اجرایی باید آموزش ببینند تا تهدیداتی را که می‌توان به ظاهر اهمیتی ندارند، متوجه شده و گزارش دهند.

از آنجا که ممکن است یک مهاجم ماهر به سادگی از در ورودی یک مرکز عبور کند، امنیت فیزیکی نیز باید مورد توجه قرار گیرد. مهاجم ممکن است لپ تاپ یا سی‌دی یا دیسک‌های فلاپی را حمل کرده و تروجان یا نرم افزار اسنیفر خود را بر روی شبکه، نصب کند. به همین منظور است که باید امنیت فیزیکی در روند افزایش سطح امنیت سازمان مورد توجه قرار گیرد و از روش‌های متنوع به منظور ارتقاء این سطح از امنیت، استفاده شود.



****

گذرواژه‌های قوی برای یک شبکه امن ضروری است. یک مهاجم ماهر اغلب به راحتی رمزهای عبور را حدس می‌زند. اریک کول، در کتاب هکرهای هوشیار، اظهار داشته است که:
«هشتاد درصد از فروشندگانی که با آن‌ها ارتباط برقرار کردم دارای گذرواژه بسیار آسان بودند که به راحتی قابل حدس بود».
مهاجمی که قادر به دسترسی به فایل رمزعبور است نیز از یک نرم افزار کرک رمزعبور استفاده می‌کند. اریک کول در کتاب هکرهای هوشیار، به این نکته اشاره می‌کند:
«همه گذرواژه‌ها قابل کرک کردن هستند، این فقط یک موضوع زمان‌بر است. مدت زمان لازم برای کرک گذرواژه‌ها بسته به قدرت پردازنده رایانه‌ها متغیر است. گذرواژه‌ای که سالیان پیش چندین ماه طول می‌کشید تا شکسته شود، امروزه کمتر از ۱ روز شکسته می‌شود.»
استفاده از رمزعبورهای قوی، امکان شکستن و یا حدس آن‌ها توسط مهاجمان را دشوارتر می‌کند. نکته‌ای که در مورد انتخاب رمزعبور باید مورد توجه قرار گیرد این است که رمزعبورها نباید کلمات یا اسامی فرهنگ لغتی باشند. آن‌ها همچنین نباید با کلمات یا اسامی که به شخص خاصی اشاره می‌کنند، همراه باشند. رمزعبور قوی ترکیبی از حروف بزرگ و کوچک، کاراکترهای خاص (مانند !@#$%) و اعداد خواهد بود. همچنین این رمزهای عبور باید طوری باشند که کاربر بتواند بدون نوشتن بر روی مانیتور یا کاغذ، آن‌ها را به خاطر بسپارد.
استراتژی‌های بهتری به منظور تایید اعتبار کاربر نسبت به کلمه عبور وجود دارد. به‌عنوان مثال، رمزعبورهای یکبار مصرف که توسط نرم افزار یا سخت افزار می‌توانند برای یک دوره زمانی خاص استفاده شوند. روش‌های مختلفی برای اجرای این کار وجود دارد، اما یک راه این است که کاربر یک توکن خاص داشته باشد که هر دقیقه یک رمز عبور جدید تولید کند. این گذرواژه یکبار مصرف همراه با یک رمزعبور دائمی، یکی از مطمئن‌ترین روش‌های احراز هویت می‌باشد. روش احراز هویت بیومتریک یک نمونه دیگری می‌باشد که ایمنی بیشتری نسبت به روش قبلی دارد. دستگاه‌های بیومتریک از شناسه‌های بیولوژیکی مانند اثرانگشت یا اسکن شبکیه چشم به منظور شناسایی و تایید کاربر استفاده می‌کنند.



سناریو سوم:
کاربر داخلی

مهاجمی که قوی‌ترین موقعیت را برای آغاز یک حمله دارد، کاربر داخلی قابل اعتماد است.Stephen Northcutt در مصاحبه خود با مجله Information Security گفته است:
«کاربران داخلی یا به اصطلاح خودی‌ها، بدون شک بزرگترین تهدید برای امنیت هستند. آن‌ها می‌دانند اطلاعات مهم و حیاتی در کجا هستند. آن‌ها فرایندهای داخلی را می‌شناسند و به آن واقف هستند. آن‌ها از قبل به شبکه وارد شده‌اند و اگر به دنبال مورد باشند، مانع زیادی برای جلوگیری از آن‌ها وجود ندارد.»
به منظور جلوگیری از مهاجمان و کابران داخلی، باید اقدامات اضافی انجام شود. پالیسی‌ها و رویه‌ها، غربالگری کارمندان، تفکیک وظایف و اجرای سیاست حداقل دسترسی، روش‌های مهمی برای ایمن سازی شبکه از مهاجمینی است که مورد اعتماد سازمان هستند. سیاست‌های امنیتی و رویه‌های مرتبط برای یک شبکه امن، ضروری است. سیاست‌ها و رویه‌ها باعث افزایش آگاهی کاربران شبکه می‌شود، بنابراین آن‌ها می‌دانند که آیا از یک خط قرمز عبور کرده‌اند و یا کاری را انجام می‌دهند که لازم نیست. سیاست‌ها و رویه‌ها همچنین انتظارات مدیریت را برای همه افراد درگیر در پروسه امنیتی روشن می‌سازد.
غربالگری کارمندان می‌تواند از بررسی مراجع قضایی به منظور بررسی سوءپیشینه تا بررسی سوابق رانندگی و .. باشد. بدیهی است که سطح غربالگری که انجام می‌شود باید مربوط به بزرگی ریسکی باشد که درصورت خیانت شخص به شرکت، به تجارت و کسب و کار و همچنین اعتبار شرکت وارد می‌شود. در همه موارد باید مفهوم و سیاست حداقل دسترسی اجرا شود. این بدان معنی است که هیچ کس نباید به چیزی که به صراحت نیازی به انجام کار خود ندارد، دسترسی داشته باشد. به زبان ساده‌تر هرشخص باید حداقل دسترسی را به منظور انجام وظایف خود داشته باشد به‌طوری که خللی در روند کاری شخص نیز وارد نشود.

تفکیک وظایف برای انجام یک کار معین نیاز به اقدام حداقل دو نفر دارد. این امر نیاز به تبانی را ایجاد می‌کند و فرصتی برای نقض امنیت سیستم برای فرد را از بین می‌برد. به عنوان مثال، کلیدهای رمزنگاری که در حالت ایمن باید نگهداری شوند، می‌توانند به دو دسته تقسیم شوند که یک نفر دارای قسمت اول کلید باشد و یک نفر دیگر که بخش دوم آن را نگه داشته است. مثال دیگر در جایی است که یک شخص می‌تواند چک را چاپ کند در حالی که شخص دیگری قادر به امضای آن‌ها است. در هر صورت، هیچ یک از افراد نمی‌توانند بدون کمک یک همکار دیگر، از یک موقعیت استفاده کنند.

چرخش وظایف نیز روش دیگری است که سازمان‌ها می‌توانند از آن‌ها استفاده کنند. این روش، وظایف را با محدودیت زمانی در اختیار اشخاص قرار می‌دهد. این روش ممکن است برای برخی از مشاغل دارای مشکلات جانبی زیادی باشد، اما ممکن است برای سایرین موثر واقع شود. این روش باعث می‌شود فرد به‌علت اینکه امکان دارد نفر بعدی متوجه اقدامات خرابکارانه او شود، از انجام رفتارهای مخرب پرهیز کند.

یک سیستم که به خطر افتاده است

درصورت عدم موفقیت اقدامات مورد بحث، ممکن است مهاجمان، صرف نظر از اینکه اسکریپت‌کیدی است یا یک مهاجم ماهر یا یک کاربر مورد اعتماد داخلی، به سیستم و درنتیجه به شبکه دسترسی بگیرند و تمام اقدامات موجود شکست بخورند. به‌دست آوردن کنترل یک دستگاه بر روی شبکه شرکت، اولین قدم برای یک مهاجم برای به دست آوردن کنترل کل شبکه است. هیچ فایروال، سیاست، رویه و یا فرایندهای امنیت فیزیکی در جهان نمی‌تواند جلوی آسیب‌های ناشی از حملات را بگیرد. موضوعی که وجود دارد این است که سیستم نیاز به هاردنینگ دارد. سیستم‌های تشخیص و جلوگیری از نفوذ باید بر روی شبکه مستقر شوند، اقدامات کنترل دسترسی باید به‌صورت مدوام و قدرتمند در حال اجرا باشند، باید نرم افزارهای آنتی ویروس را با تعاریف جاری بر روی شبکه مستقر کرده و کاربران و مجریان سیستم‌ها باید در جست و جوی فعالیت‌های غیرمعمول باشند. همچنین نباید از موضوع آموزش کاربران در شبکه غافل شد. اما با این حال، این موارد کافی نیست، برای محافظت از شبکه باید لایه‌های دفاعی بیشتری را به‌کار گرفت. مهاجمی که دسترسی آزاد به شبکه دارد ممکن است اطلاعات بیشتری را جمع آوری کند. به‌عنوان مثال، ممکن است مهاجمان برای اطلاعات یا کلمه عبورهای موجود در شبکه، شبکه را اسکن و بررسی کنند و یا ممکن است مهاجم دستگاه‌های مشکوک را از نظر وجود آسیب پذیری بررسی بیشتری انجام دهد. مهاجمی که به شبکه دسترسی پیدا کرده، مسلماً نفوذ چشمگیری پیدا کرده است، اما هنوز اقدامات لازم برای محافظت از شبکه وجود دارد که می‌توانید آن‌ها را لحاظ کنید. به‌عنوان مثال می‌توان با اعمال تنظیمات امنیتی از حملاتی مانند Sniffing و یا Hijacking بر روی بستر شبکه جلوگیری کرد و یا با اجرای یک روش تأیید صحت و انتقال از قبیل Kerberos، می‌توان از سرقت رمزهای عبور و داده‌ها در شبکه جلوگیری کرد. گرفتن بکاپ نیز یک لایه دفاعی مهم است که در صورت نفوذ به سیستم‌ها، می‌توان از آن استفاده کرد. اگر همه لایه‌های دفاعی که ذکر شد، کافی نبوده و یک سیستم به خطر بیافتد، به احتمال زیاد نیاز به بازسازی و بازیابی سیستم به‌وجود می‌آید. باید توجه داشت که بدون داشتن یک استراتژی پشتیبان گیری مناسب، داده‌ها از بین می‌روند.

نتیجه گیری

مهمترین نکته‌ای که وجود دارد این است که هیچ یک از اقدامات امنیتی واحد نمی‌تواند به اندازه کافی از شبکه محافظت کند. روش‌های بسیار زیادی وجود دارد که یک مهاجم برای نفوذ به شبکه و دور زدن مکانیزم‌های امنیتی، می‌تواند از آن‌ها استفاده کند. اسکریپت‌کیدی‌ها، مهاجمان ماهر و یا کاربران قابل اعتماد، روش‌های متداولی دارند که هرکدام مشکلات منحصر به فردی را در یک شبکه امن ایجاد می‌کنند. به‌عنوان مثال، فایروال هیچگونه محافظتی در برابر تهدیدات کاربران قابل اعتماد داخلی ندارد اما به عنوان یک مانع مهم در برابر مهاجمین خارجی می‌تواند مورد استفاده قرار گیرد. به همین ترتیب، سیاست‌ها و رویه‌ها، به منظور جلوگیری از مهاجمان خارجی نیستند بلکه به منظور محافظت از شبکه در برابر کاربران داخلی قابل اعتماد نیز خواهند بود.

با این حال می‌توان تا حدودی امیدوار بود که استقرار استراتژی دفاع در عمق، مهاجمان را تا حدودی دل‌سرد کند. فایروال‌ها، سیستم‌های تشخیص و جلوگیری از نفوذ، کاربران آموزش دیده، سیاست‌ها و رویه‌ها، رمزهای عبور قوی و امنیت فیزیکی مناسب، نمونه‌هایی از مواردی هستند که به یک برنامه امنیتی، کمک می‌کنند. هریک از این مکانیزم‌ها به خودی خود دارای ارزش‌هایی هستند اما هنگامی که باهم پیاده سازی می‌شوند بخشی از یک برنامه امنیتی کلی بسیار با ارزش‌تر را تشکیل می‌دهند.