با یک ظرف عسل امنیت شبکه خود را افزایش دهید

استقرار یک سامانه ظرف عسل (Honeypot) در شبکه داخلی یک سازمان اقدامی پیشگیرانه است که اجازه می‌دهد بلافاصله پس از شناسایی یک مزاحم و قبل از هرگونه اقدام خرابکارانه‌ای همچون آسیب‌رساندن به سامانه‌ها یا سرقت اطلاعات دسترسی مزاحم به سامانه‌ها را قطع کنید. ظرف‌های عسل، یکی از بهترین مکانیزم‌های دفاعی در برابر هکرها هستند که بیشتر شرکت‌های بزرگ ازجمله بانک‌های بین‌المللی برای به دام انداختن هکرها از آن استفاده می‌کنند.

مدیران مجرب، زمانی که ظرف عسل موفق می‌شود مزاحمی را جذب کند، بلافاصله دسترسی او به سامانه را قطع نمی‌کنند، بلکه صبر می‌کنند تا عکس‌العمل او و کارهایی را که برای نفوذ به شبکه انجام می‌دهد، مشاهده کرده و اگر هکر موفق شد رخنه ناشناخته‌ای در شالوده مکانیزم‌های امنیتی سازمان پیدا کند، آن رخنه را به سرعت برطرف می‌کنند.

ظرف عسل (Honeypot) چیست؟

تاکنون به این موضوع فکر کرده‌اید که چگونه یک هکر مکانیزم‌های دفاعی یک سیستم را درهم می‌شکند و به آن نفوذ می‌کند؟ سازمان‌ها چگونه این مسئله را به سرعت تشخیص داده و زمانی که هکر سعی در ورود به سیستم یا دسترسی به اطلاعات دارد، مانع از ادامه فعالیت او می‌شوند؟ استقرار یک ظرف عسل راه‌حلی برای مشاهده و انجام فعالیت‌هایی است که یک هکر انجام می‌دهد. ظرف عسل سامانه‌ای درون یک شبکه است که نقش یک تله را بازی کرده و برای فریب هکرها از آن استفاده می‌شود. تعاریف مختلفی برای یک ظرف عسل ارائه شده است. با این حال، همه تعاریف حول این محور قرار دارد که ظرف عسل، سروری است که برای شناسایی یک مزاحم پیکربندی شده و درون آن اطلاعاتی به ظاهر ارزشمند قرار گرفته است. در حقیقت، سرور فوق عملکردی شبیه یک آینه دارد که تنها تصویری از اطلاعات واقعی را با هدف به دام انداختن مهاجمان در اختیارشان قرار می‌دهد. در ظاهر این‌گونه به نظر می‌رسد که یک سرور عادی در حال انجام فعالیت‌های روزانه است، در حالی که تمامی داده‌ها و تراکنش‌های درون سرور جعلی هستند. ظرف عسل می‌تواند داخل یا خارج از دیوارآتش قرار گیرد. در حالت کلی سازمان‌ها از ظرف عسل یا تله عسل برای تشخیص تکنیک‌های هکری و رخنه‌هایی که درون یک سامانه واقعی قرار دارد، استفاده می‌کنند. از آنجا که ظرف عسل هیچ‌گونه سرویس قانونی و معتبری ارائه نمی‌کند، تمام فعالیت‌های انجام شده درون آن بدون احراز هویت انجام می‌شود. ظرف عسلی که پیکربندی درستی داشته باشد، ویژگی‌های یک سامانه واقعی را دارد که از آن جمله می‌توان به رابط گرافیکی، پیام‌های هشداردهنده ورود به سیستم و رکوردهای اطلاعاتی اشاره کرد. در حقیقت، اگر یک کاربر ساده باشید و یک ظرف عسل مقابل شما قرار دهند، به‌هیچ‌عنوان متوجه نخواهید شد که یک سامانه غیرواقعی پیش روی شما قرار گرفته است. چرا یک ظرف عسل باید چنین پیکربندی دقیقی داشته باشد؟ پاسخ روشن است، زیرا مزاحم نباید به راحتی یک ظرف عسل را تشخیص داده و

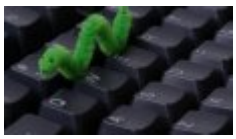
متوجه شود کارهایی که انجام می‌دهد، زیر نظر است.

مزایای به‌کارگیری ظرف عسل

برخی از سازمان‌ها با تحیر این پرسش را مطرح می‌کنند که چرا باید پول و زمان خود را صرف ساخت سامانه‌ای برای جذب هکرها کنند؟ در پاسخ به این سازمان‌ها باید بگوییم با توجه به مزایای متعدد یک ظرف عسل چرا تاکنون هیچ‌گونه تمهیداتی برای پیاده‌سازی یک چنین سامانه‌ای در نظر نگرفته‌اید؟
با ارزش‌ترین قابلیت یک ظرف عسل، اطلاعاتی است که دریافت کرده و هشداری است که به شکل بلادرنگ صادر می‌کند. داده‌های وارد و خارج‌شونده به ظرف عسل به کارکنان امنیتی اجازه می‌دهد، به جمع‌آوری اطلاعاتی اقدام کنند که در دسترس یک سامانه تشخیص نفوذ نیست. یک ظرف عسل می‌تواند در مدت زمان برقراری یک نشست (Session) و حتی زمانی که از الگوهای رمزگذاری برای برقراری ارتباط استفاده شده است، به شما درباره یک حمله هکری موسوم به کلیدهای فشرده که با هدف سرقت کلیدها ترتیب داده شده، اطلاعات مفیدی ارائه کند.
همچنین هرگونه تلاش برای دسترسی به سامانه می‌تواند با هشدار ظرف عسل موسوم به هشدار خاموش همراه باشد. یک سامانه تشخیص نفوذ برای شناسایی یک حمله به امضای منتشر شده در خلال یک حمله نیاز دارد، به همین دلیل، در برخی موارد به علت فقدان این امضا قادر نیست یک حمله را شناسایی کرده و شکست می‌خورد. در نقطه مقابل یک سامانه ظرف عسل می‌تواند نشانه‌های مشکوک مبتنی بر الگوهای رفتاری یک مهاجم را که در آسیب‌پذیری‌های روز صفر ریشه دارند و حتی جامعه امنیتی درباره این نشانه‌ها هیچ‌گونه اطلاعاتی ندارد، شناسایی کند. این نشانه‌ها در اغلب موارد با بهره‌گیری از آسیب‌پذیری‌های روز صفر باعث فاش شدن هویت یک هکر می‌شوند.

داده‌های جمع‌آوری‌شده توسط ظرف عسل‌ها می‌توانند برای تقویت سایر فناوری‌های امنیتی شبکه استفاده شوند. شما می‌توانید گزارش‌هایی را که یک ظرف عسل تولید کرده با سایر گزارش‌های دریافتی از سامانه‌های مختلف همچون گزارش‌های سامانه تشخیص نفوذ و گزارش‌های دیوارآتش ترکیب کرده و تصویری جامع از فعالیت‌های مشکوکی که درون سازمان در حال انجام است، به دست آورید. این ترکیب منحصر به فرد به شما اجازه می‌دهد، تعداد هشدارهای کاذب مثبت را تعدیل کرده و هرگونه تهدیدی هرچند کوچک را به درستی تشخیص دهید.
یکی دیگر از مزایای بالقوه یک ظرف عسل به زمانی باز می‌گردد که هکرها موفق شده‌اند به سیستم وارد شوند. در این زمان ظرف عسل قادر است حمله هکرها را عقیم کرده و مانع از آن شود تا هکرها با خرابی سیستم باعث از کار افتادن شبکه یک سازمان شوند. هرچه هکرها زمان بیشتری صرف یک ظرف عسل کنند، به همان نسبت زمان کمتری را صرف حمله به شبکه و سیستم واقعی می‌کنند.

مطلب پیشنهادی



مشابه‌ای برای انگل‌های دنیای واقعی
کرم اینترنتی چیست و چه خطراتی با خود به همراه دارد

طراحی و عملیاتی کردن یک ظرف عسل (Honeypot)

ظرف عسل با سیستم‌عامل‌ها و سرویس‌های مختلفی قابل استفاده است. امروزه، ظرف‌های عسل به دو گروه، ظرف عسل با رویکرد تعاملی بالا و ظرف عسل با رویکرد تعاملی پایین در دسترس قرار دارند. ظرف‌های عسل بر مبنای سرویس‌ها یا سطح تعاملی که با هکرها دارند، در یکی از این دو گروه قرار می‌گیرند. البته برخی از کارشناسان گروه سومی نیز تعریف می‌کنند؛ ظرف‌های عسلی که یک رویکرد تعاملی متعادل با هکرها را پیشنهاد می‌دهند. ظرف‌های عسلی که رویکرد تعاملی سطح بالا را ارائه می‌کنند می‌توانند یک سیستم کاملا حرفه‌ای را

طراحی کنند که اجازه می‌دهد هکرها به ساده‌ترین شکل با آن در ارتباط باشند. در نقطه مقابل یک ظرف عسل با حداقل قابلیت‌های تعاملی قادر است برخی از عملکردهای خاص یک سیستم را شبیه‌سازی کند. درست است که ظرف‌های عسل کمتر تعاملی قابلیت‌های محدودی ارائه می‌کنند، اما باز هم برای کسب اطلاعات مفید هستند. تجربه شخصی من نشان داده، ظرف‌های عسلی که سطح بالایی از تعامل دوطرفه با هکرها را ارائه می‌کنند، مفیدتر هستند، زیرا می‌توانند به‌طور کامل یک محیط تولیدی را (منظور شبکه یک سازمان یا خط تولید کارخانه‌ای است که با اینترنت ارتباط مستقیمی دارد) شبیه‌سازی کنند. با این حال، پیاده‌سازی، استقرار و پیکربندی چنین ظرف‌های عسلی به زمان زیاد و البته دانش فنی مناسب نیاز دارد. مهم‌ترین اصل در پیاده‌سازی یک ظرف عسل به پیکربندی درست آن برای ارائه هشدارها باز می‌گردد. باید گزارش‌های مربوط به همه دستگاه‌ها و گزارش‌های تولید شده از سوی ظرف‌های عسل را جمع‌آوری کرده، گزارش‌ها را برای یک سرور مرکزی ارسال کنید تا کارمند بخش امنیت آن‌ها را بایگانی کند تا هر زمان نشانه‌ای دال بر ورود یک هکر به محیط شناسایی شد، با مراجعه به بایگانی مکان‌های احتمالی که هکر ممکن است به سراغ آن‌ها برود، در کوتاه‌ترین زمان شناسایی شود. این رویکرد به کارمندان بخش امنیت اجازه می‌دهد از نزدیک فعالیت‌های هکر را ردیابی کرده و اطمینان حاصل کنند که محیط در سلامت کامل قرار دارد. توجه داشته باشید، هدف ما از نصب یک ظرف عسل این نیست که به محض رویت یک حمله هکری به سرعت آی‌پی هکر را مسدود کرده و مانع دسترسی او به سیستم شویم، بلکه هدف این است که اطلاعات بیشتری در ارتباط با چگونگی کار هکرها به دست آورده و آسیب‌پذیری‌های مستتر در شبکه را شناسایی کنیم.
عامل مهم دیگری که باعث موفقیت یک سامانه ظرف عسل می‌شود، جذابیت احتمالی آن برای یک هکر است. یک ظرف عسل قرار نیست به پیشرفته‌ترین مکانیزم‌های امنیتی تجهیز شده باشد، بلکه باید پورت‌های بازی برای پاسخ‌گویی به حس کنجکاوی هکر در آن قرار گرفته باشد تا هکر بتواند با استفاده از یک نرم‌افزار پویشگر پورت‌ها، یک پورت باز را شناسایی کرده و به سامانه وارد شود. در ادامه درون سامانه باید حساب‌های کاربری، فایل‌های سیستمی مختلف و گذرواژه‌های جعلی و ضعیفی قرار گرفته باشند تا هکر بتواند با کمی تلاش به آن‌ها دسترسی پیدا کند. این‌کار مهاجم را تشویق می‌کند، به جای آن‌که به سراغ محیط اصلی برود، وقت خود را صرف یک محیط ساختگی کند.
مهاجمان معمولا قبل از آن‌که به سراغ محیط‌هایی بروند که دفاع مستحکمی دارد، ترجیح می‌دهند ابتدا به محیط‌ها و مکان‌های ضعیف‌تر و آسیب‌پذیرتر حمله کنند. این‌کار به کارمندان بخش امنیت اجازه می‌دهد نکات آموزنده‌ای یاد گرفته و یاد بگیرند که چگونه هکرها از کنترل‌های استاندارد عبور می‌کنند و چه تهمیداتی برای ایمن‌سازی نقاط ضعیف باید لحاظ شود.
شما می‌توانید ظرف عسل را به دو شکل فیزیکی یا مجازی مستقر کنید. در بیشتر موارد، بهتر است که یک ظرف عسل مجازی را استفاده کنید، زیرا گسترش‌پذیری و سهولت استفاده را به همراه دارد. می‌توانید هزاران ظرف عسل را تنها درون یک ماشین فیزیکی در اختیار داشته باشید، علاوه بر این ظرف‌های عسل مجازی معمولا ارزان‌تر بوده و به راحتی در دسترس قرار دارند.

ظرف عسل و تهدیدات داخلی شبکه

ظرف‌های عسل می‌توانند از یک سازمان در برابر تهدیدات داخلی محافظت کنند. بر اساس گزارش واحد اطلاعات امنیت سایبری مستقر در شرکت آی‌بی‌ام، نزدیک به 60 درصد از تمام حملات به شبکه‌های یک سازمان توسط نیروهای خودی انجام می‌شود. یک ظرف عسل باید درون شبکه داخلی سازمان مستقر شود و تنها تعداد معدودی از کارکنان درباره آن اطلاع داشته باشند. استقرار داخلی بر استقرار خارجی به ویژه زمانی که تعداد حملات از جانب کارمندان داخلی زیاد است، ارجحیت دارد، زیرا هکرها ترجیح می‌دهند، سرورهای کنترل و فرماندهی را برای برقراری ارتباط با سرورهای مخرب خود درون شبکه داخلی یک سازمان مستقر کنند. به این شکل هر زمان حمله هکری شناسایی شود، متخصصان امنیتی موفق به شناسایی سروری می‌شوند که درون خود سازمان قرار داشته است و به این شکل شناسایی موقعیت مکانی هکرها راحت‌تر می‌شود.

یک ابزار کاربردی متن‌باز

Honeyd یک ابزار منبع‌باز برای ساخت یک ظرف عسل است. Honeyd یک سرویس‌دهنده است که می‌تواند برای ساخت بسیاری از میزبان‌های مجازی استفاده شود. شما می‌توانید هر میزبان را به صورت متفاوتی پیکربندی کرده و سرویس‌های مختلفی را روی آن‌ها اجرا کنید. این میزبان‌ها می‌توانند پیکربندی شوند تا سیستم‌عامل‌های مختلفی را اجرا کنند. همچنین می‌توانید سرورهای واقعی HTTP و سرورهای FTP را راه‌اندازی کرده و برنامه‌های لینوکسی را روی آن اجرا کنید. ابزار فوق به شما اجازه می‌دهد تا توپولوژی‌های مختلف شبکه را شبیه‌سازی کنید.

شبکه‌ها و مزارع عسل

شبکه‌ای متشکل از ظرف‌های عسل و مزارع عسل، هر دو اصطلاح به مجموعه‌ای از ظرف‌های عسل اشاره دارند. مزارع عسل بیشتر به سمت‌وسوی تمرکزگرایی تمایل دارند. سازمان‌ها برای رفع معایب ظرف‌های عسل سنتی و برطرف‌کردن یکسری کاستی‌های سنتی این سامانه‌ها از رویکرد اشتراک مساعی استفاده می‌کنند. به‌عنوان مثال، ظرف‌های عسل اغلب برای محافظت از گره‌های هر ظرف عسل ترافیک خروجی را محدود می‌کنند تا مانع از بروز حمله به این گره‌ها شوند. اما محدودیت فوق باعث می‌شود تا یک هکر به راحتی بتواند ظرف‌های عسل را شناسایی کند. به همین دلیل، از مزارع عسل برای هدایت ترافیک شبکه به سمت هر ظرف عسل منحصر به فرد استفاده می‌شود. شکل1 نحوه هدایت ترافیک خروجی از ظرف عسل را به سمت گره‌ای در یک مزرعه عسل نشان می‌دهد.

کلام پایانی

ظرف‌های عسل عمدتا توسط محققان استفاده می‌شود تا به شکل دقیق‌تری تاکتیک‌ها و تکنیک‌های مهاجمان را مطالعه و بررسی کنند. اما همان‌گونه که پیش‌تر توضیح دادم، ظرف‌های عسل می‌توانند برای دفاع از شبکه کمک فراوانی به متخصصان کنند. مزایای استفاده از ظرف‌های عسل به مراتب بیشتر از هزینه‌هایی است که سازمان‌ها برای مراقبت از اطلاعات حساس خود صرف می‌کنند، در نتیجه زمان آن فرارسیده تا سازمان‌های بیشتری از ظرف‌های عسل به عنوان یک راه پیشگیرانه برای حفاظت از شبکه خود استفاده کنند

تاریخ انتشار:

08 شهریور 1398

نشانی منبع:
https://www.shabakeh-mag.com/security/15989/%D8%A8%D8%A7-%DB%8C%DA%A9-%D8%B8%D8%B1%D9%81-%D8%B9%D8%B3%D9%84-%D8%A7%D9%85%D9%86%DB%8C%D8%AA-%D8%B4%D8%A8%DA%A9%D9%87-%D8%AE%D9%88%D8%AF-%D8%B1%D8%A7-%D8%A7%D9%81%D8%B2%D8%A7%DB%8C%D8%B4-%D8%AF%D9%87%DB%8C%D8%AF