۵ مورد از بهترین روش‌های پیشگیری از حملات سایبری برای کسب و کارهای کوچک با شبیه‌سازی "حملات و نشت اطلاعات"

پیشگیری از حمله سایبری برای کسب و کارهای کوچک موردی است که امنیت سایبری آن‌ها باید بسیار جدی گرفته شود. اکنون مهاجمین به دلیل ضعف‌های امنیتی موجود در این بخش، به طور جدی در حال انجام حملات سایبری هدفمند هستند. در واقع، در آخرین گزارشات ۴۳ درصد از حملات سایبری مربوط به شرکت‌های کوچکتر است.

متأسفانه، در شرایط کنونی شرکت‌هایی که مورد حملات سایبری قرار می‌گیرند، ضرر و زیان‌های مختلف را در ابعاد گوناگون تجربه می‌کنند. حملات سایبری می‌تواند باعث خرابی، بدنامی و از دست رفتن درآمد شود که این موارد، از دسته مواردی هستند که کسب و کارهای کوچک از آن‌ها دوری می‌کنند. البته پیشگیری از حملات سایبری نیز یک بخش چالش برانگیز برای آن‌ها است.

خوشبختانه اگر صاحب کسب و کار کوچک باشید، بدانید که می‌توانید امنیت خود را بهبود بخشید. ارائه‌دهندگان

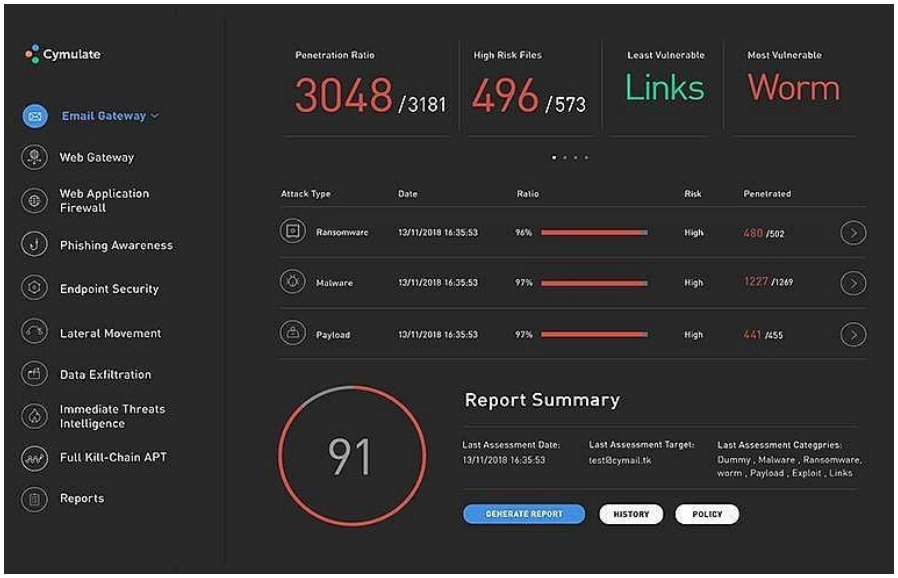
راه‌حل‌های امنیتی، ابزارهایی را برای کسب و کارهای کوچک و ارزان‌تر ارائه می‌دهند.

امروزه امکان عضویت در سرویس‌های ضدبدافزار و فایروال cloud-based وجود دارد که می‌توانند حفاظتی مشابه با آنچه که شرکت‌های بزرگ از آن لذت می‌برند را فراهم کنند.

گذشته از این راه‌حل‌های متداول، اقدامات پیشرفته‌تری مانند شبیه‌سازی نشت اطلاعات و حمله (BAS) در حال حاضر برای کسب و کار کوچک قابل دسترسی است. BAS می‌تواند با ارزیابی راه‌حل‌های امنیتی شما و تمام پیشگیری‌هایی که از حملات سایبری کرده‌اید، به شما کمک کند.

پلتفرم BAS Cymulate به شما امکان می‌دهد با راه‌اندازی حملات شبیه‌سازی شده علیه آن، تمهیدات امنیتی خود را برای آسیب‌پذیری‌های احتمالی بررسی کنید.

ارزیابی‌های مختلف اگر بتوانند فایروال را برای نقص‌های احتمالی در پیکربندی و حتی راه‌حل‌های امنیتی نقطه پایانی را بررسی کنند، به راحتی نقاط ضعف را تشخیص خواهند داد. در زیر تصویری از Cymulate نشان داده شده است.



این ابزار حتی می‌تواند حملات فیشینگ را شبیه‌سازی کرده تا ببیند کاربران تا چه حد احتمالاً در برابر حملات مهندسی اجتماعی آموزش دیده‌اند. با دانستن این مشکلات می‌توانید

تنظیمات یا تغییرات لازم را برای برطرف کردن نقص‌ها انجام دهید.

بنا بر آمارهای موجود در حوزه کسب و کارهای کوچک، باید توجه کرد که تهدیداتدر حوزه امنیت سایبری واقعی و جدی هستند و بعید نیست هکرها در حال حاضر شرکت شما را مورد هدف قرار داده باشند. به همین دلیل، شما باید اقدامات سختگیرانه امنیتی را اجرا کنید که بتواند حتی تهدیدات پیچیده را خنثی کند.

در این گزارش، پنج مرحله وجود دارد که می‌توان برای اطمینان از محافظت از اطلاعات شرکت، از آنها استفاده کرد:

۱- تعیین یک سطح پایه از نیازهای امنیتی

۲- سرمایه‌گذاری بر روی راه‌حل‌های امنیتی کارا

۳- پیاده‌سازی دقیق کنترل سطوح مختلف دسترسی

۴- تهیه نسخه پشتیبان از برنامه‌ها و به‌روزرسانی مداوم نرم افزارها

۵- آموزش کارمندان

۱ - تعیین یک سطح پایه از نیازهای امنیتی

صاحبان کسب و کار برای جلوگیری از حملات سایبری مربوط به کسب و کارهای کوچک، با مجموعه‌ای از راه‌حل‌ها طرف هستند که ممکن است گاهی استفاده از کدام یک از آن موارد گمراه کننده باشد.

برای شما مهم است که ابتدا درک کنید که نیازهای تجاری شما به چه صورت است، بنابراین می‌دانید برای پشتیبانی از این نیازها به چه نوع زیرساخت‌های فناوری اطلاعات نیاز دارید. این را باید دانست که بدون توجه به نیازهای خود، اگر هم حتی بالاترین هزینه‌ها در حوزه فناوری اطلاعات و امنیت انجام شود، بدیهی است منابع با ارزش خود را به آسانی هدر داده اید.

ابتدا باید درک کنید که چه حوزه‌هایی از کسب و کارتان باید توسط فناوری پشتیبانی شود. به این ترتیب، شما قادر خواهید

بود نرم افزار و سخت افزارهای مورد نیاز خود را شناسایی کنید. علاوه بر این، می‌دانید که داده‌ها و منابع مربوط به شرکت به چه صورت مورد استفاده خواهند بود.

باید دانست که آیا از سرور داخلی یا فضای ذخیره‌سازی ابری استفاده می‌کنید؟ با بررسی نیازها و داشتن تصوری از ساختار کلی شرکت خود در این حوزه، می‌توان مشخص کرد که چه راه‌حل‌های امنیتی برای محافظت از هر یک از این مؤلفه‌ها مورد نیاز است.

اگر شبکه اداری کوچک شما فقط دارای سه ایستگاه کاری باشد، دستیابی به راه‌حل‌های امنیتی ارائه شده برای شرکت‌های بزرگ مانند پلتفرم‌های مدیریت IT یا حتی security information and event management (SIEM) می‌تواند برای شرکت شما زیاده‌روی و هدر رفت هزینه باشد.

اگر بدون بررسی نیازها و بسترهای خود از راه‌حل‌ها و ابزارهایی استفاده کرده و هزینه‌هایی را انجام دهید، به احتمال فراوان قادر به بازگشت سرمایه خود نخواهید بود.

برای انتخاب راه‌حل‌ها، صرف نظر از مقیاس شرکت از نظر تعداد کارمندان و بسترها، بررسی وضعیت دفاعی شرکت بسیار مهم است. اینجا است که BAS مفید است. برای پیشگیری از حملات سایبری، Cymulate می‌تواند یک حسابرسی جامع از تمام نقاط بسترها و مؤلفه‌های آسیب‌پذیری را انجام دهد.

۲ – سرمایه‌گذاری بر روی راه‌حل‌های امنیتی کارا

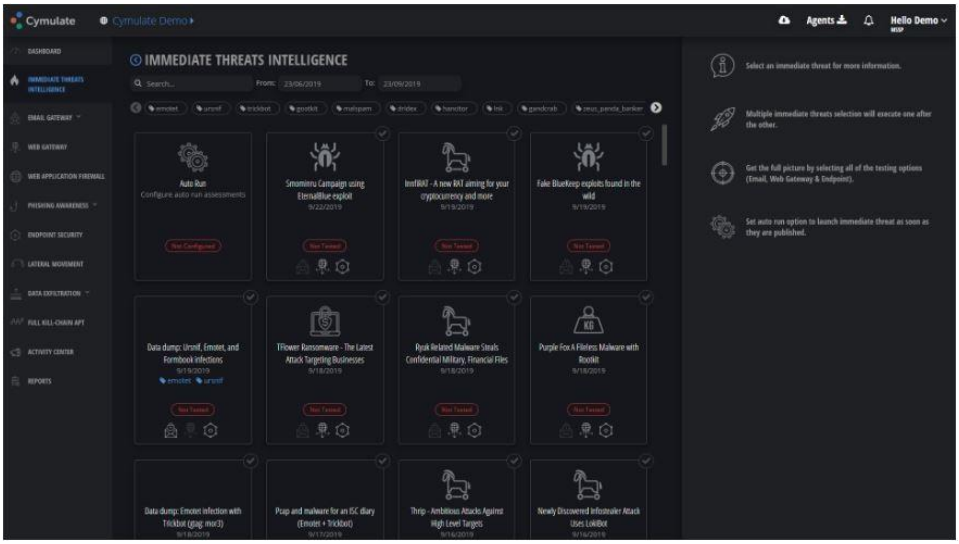
سرمایه‌گذاری در ابزارهای امنیتی کارا گامی مهم است که بتوان امنیت سایبری را تا حد زیادی برقرار ساخت. استفاده از ابزارها برای محافظت از سیستم‌های کارمندان مانند انتی‌ویروس، ضد بدافزار و ابزارهای امنیتی شبکه مانند فایروال از جمله راه‌حل‌هایی است که باید در شرکت پیاده کرد.

ممکن است نیاز شما فراتر از ابزارهای رایگان باشد و میبایستی راه‌حل‌های بهتری که بتواند تهدیدهای پیشرفته را شناسایی و با آن‌ها مقابله کند، مورد استفاده قرار دهید و بر روی این موارد باید سرمایه‌گذاری کنید.

خوشبختانه، اکنون بسیاری از سرویس‌ها برای سازمان‌ها از طریق سرویس‌های ابری موجود است که می‌توان به راحتی از آنها استفاده کرد. حتی برای استفاده از بسیاری از ویژگی‌ها نیاز به دانش بالا نیست و می‌توان به راحتی از این سرویس‌ها استفاده کرد.

همچنین باید بتوان اثربخشی این ابزارها را ارزیابی و بررسی کرد. پلتفرم BAS می‌تواند به طور مرتب و مداوم عملکرد اقدامات امنیتی شما را بررسی کند.

Cymulate به شما امکان می‌دهد تا ارزیابی‌ها را به صورت خودکار انجام دهید تا ببینید آیا به طور مثال انتی‌ویروس یا فایروال شما تهدیدها و حملات را شناسایی کرده‌اند و یا نه. در نتیجه یک پروفایل ارزیابی تهدید سایبری را ایجاد خواهند کرد. در زیر عکسی از این پروفایل نشان داده شده است.



۳- پیاده‌سازی دقیق کنترل سطوح مختلف دسترسی

هکرها برای دستیابی به سیستم‌ها و حساب‌های آنلاین از روش‌های مختلفی استفاده می‌کنند. از بین تکنیک‌های متداول مورد استفاده آن‌ها برای نفوذ، انجام حمله brute force مواردی است که از تعداد زیادی نام کاربری و رمز عبور استفاده می‌کنند تا اطلاعات یک حساب کاربری موجود را پیدا کنند. هکرها معمولاً دارای بانک اطلاعاتی گسترده از رمزهای عبور معمول هستند، بنابراین اگر یکی از حساب‌ها در شرکت شما از رمزهای

عبور ساده استفاده کرده که در لیست آن‌هاست موجود باشد، دسترسی به آن حساب به راحتی انجام می‌شود.

در صورت استفاده از رمزهای عبور که ترکیبی از حروف، عدد و نمادها باشد، حملات brute force که در حقیقت آزمایش و خطای تمامی احتمالات موجود است، دارای شانس موفقیت کمتری خواهد بود. در این بخش تعریف سیاست‌هایی برای انتخاب رمز عبور می‌تواند مفید باشد.

همچنین فعال کردن تأیید هویت دو عاملی(two-factor authentication) یکی از روش‌های جلوگیری از نفوذ است که می‌تواند یک لایه دیگر برای محافظت از حساب را اضافه کند. همچنین یک راه‌حل دیگر، استفاده از رمزعبور یک بارمصرف (OTP) برای کارت‌های بانکی و حساب‌های کاربری، تا حد زیادی می‌تواند مانع هکرها شود حتی در صورتی که قبلاً نام کاربری و رمز عبور را به دست آورده باشند.

همچنین ممانعت از استفاده از رمز عبورهای تکراری برای حساب‌های مختلف شخصی و شرکتی نیز مهم است. کاربرانی که از همان رمز عبور برای حساب‌های شخصی و شرکتی خود استفاده می‌کنند، هم شرکت شما و هم خود را در معرض خطر قرار می‌دهند.

در شرکت می‌توان برای ایجاد و مدیریت رمزهای عبور قوی و منحصر به فرد برای هر حساب، از یک password manager استفاده کردد. به این ترتیب، شما همچنین می‌توانید افرادی را که به حساب‌های خاص، داده‌ها و زیرساخت‌های حساس شما دسترسی دارند، کنترل کنید.

۴ -تهیه نسخه پشتیبان از برنامه‌ها و به‌روزرسانی مداوم نرم‌افزارها

باید توجه داشت که حتی با وجود راه‌حل‌های امنیتی کارا، باید در مورد نشت اطلاعات محتاط بود. برخی از هکرها، نه تنها داده‌های کاربران را سرقت می‌کنند بلکه نسخه‌های کاربران را نیز از بین می‌برند. برای جلوگیری از پاک شدن کامل اطلاعات، برنامه‌ریزی برای تهیه نسخه پشتیبان بسیار مهم است.

همچنین می‌توان از یک راه‌حل امن ذخیره‌سازی مانند فضای ابری استفاده کرد که نسخه‌ای پشتیبان از اسناد را ذخیره کنند. بیشتر راه‌حل‌ها به شما این امکان را می‌دهند تا داده‌های خود را در صورت حذف شدن به دلیل حملات بدافزاری، بازیابی کنید.

در صورت استفاده از نرم‌افزارهای مختلف، میبایست به‌صورت مداوم آنها را به‌روز کرد، که این امر می‌تواند از حمله‌هایی که از آسیب‌پذیری‌هایی که به موجب عدم به‌روزرسانی نرم‌افزارها ایجاد می‌شود، بهره‌برداری می‌کنند، جلوگیری کرد.

بنابراین، برای جلوگیری از حملات سایبری و نفوذ، اعلان‌های به‌روزرسانی را نادیده نگیرید. اکثر برنامه‌ها اکنون دارای یک ویژگی به‌روزرسانی خودکار هستند. همچنین می‌توانید برای نرم‌افزارهایی که نیاز به به‌روزرسانی دستی دارند، یک یادآوری در سطح شرکت برای کارمندان ارسال کنید.

۵- آموزش کارمندان

حملات مهندسی اجتماعی مانند فیشینگ همچنان از جمله روش‌های رایج هکرها برای دستیابی به سیستم‌ها است. طبق آخرین آمارها، در حقیقت ۵۷ درصد از کسب و کارهای کوچک که مورد حمله قرار گرفته‌اند، قربانی فیشینگ و مهندسی اجتماعی هستند. شما باید اطمینان حاصل کنید که کارمندان شما به راحتی قربانی این کلاهبرداری‌ها نمی‌شوند.

Cymulate را می‌توان برای انجام حملات فیشینگ شبیه‌سازی شده، مانند سیستم شبیه به ایمیل واقعی، پیکربندی کرد. این پلتفرم، ایمیل‌های فیشینگ شبیه‌سازی شده به صورت الگوهای قالب‌بندی شده و کاملاً هوشمندانه، ارسال می‌کنند تا بتوانند توانایی کارمندان خود را برای تشخیص دقیق‌تر ایمیل‌های جعلی ارزیابی کنند.

این ارزیابی‌ها می‌توانند تشخیص دهند چه حساب‌های کاربری خاصی، هدف چنین حملاتی قرار می‌گیرند. به این ترتیب، می‌توان نقاط ضعف سازمان را شناسایی کرده و درخصوص این موارد به کارمندان خود آموزش داد.

انجام آموزش امنیت سایبری باید بخشی از برنامه‌ریزی‌های شما برای شرکت باشد. از طریق آموزش می‌توان تا حد بسیاری از حملات جلوگیری کرد.

آموزش منظم همچنین به کارکنان شما کمک می‌کند تا یک ذهنیت گسترده‌تر از اهمیت و اولویت امنیت داشته باشند. آن‌ها می‌دانند که چگونه می‌توانند ابزارهای امنیتی را بطور مؤثر مدیریت کرده، حملات فیشینگ را کشف کنند و فعالیت‌های مشکوک را در یک شبکه تشخیص دهند.

کار از محکم کاری عیب نمیکند (امنیت بهتر از تأسف)

بیشتر کسب و کارهای کوچک توان مقابله در برابر حملات و نشت اطلاعات بزرگ را ندارند. بنابراین، ایجاد یک بستر امنیتی قوی و برقراری تمهیداتی که اشاره شد، می‌تواند پلتفرمی را برای مقابله با تهدیدات مدرن امنیتی ایجاد کرده و باید توجه داشت که این امر یکی از اولویت‌های اصلی شرکت باشد.

با رعایت این مراحل، اگرچه هیچگاه نمی‌توان امنیت کامل را برقرار کرد اما می‌توان امنیت سایبری شما را تا حد زیادی بالا برده و احتمال هک شدن را کاهش داد. درنهایت، رعایت نکات گفته شده می‌تواند به شما در حفاظت از داده‌های حساس کمک کند تا شرکت‌ها و کسب و کارهای کوچک را از آسیب‌ها نجات دهد.

منبع:

https://gbhackers.com/cyber-attack-prevention/