۷ گام به منظور جلوگیری و محدود کردن تأثیر باج‌افزارها

بر اساس گزارش‌ها و آمارهای مراکز امنیتی، از سازمان‌های دولتی تا شرکت‌های کوچک و بزرگ، حملات باج‌افزاری را در سال ۲۰۱۹ تجربه کرده‌اند. در سال ۲۰۲۰ این تلنگر برای همه کاربران است که بتوان مانع از حملات موفق باج‌افزارها شد. اساس کار باج‌افزارها این است که دسترسی به یک سیستم، دستگاه یا فایل را تا زمانی که باج خواسته شده پرداخت نشود، برقرار نخواهد شد. این کار را با رمزنگاری فایل‌ها ، تهدید به پاک کردن فایل‌ها یا مسدود کردن دسترسی سیستم انجام می‌شود. این حملات در مواردی مانند بیمارستان‌ها، مراکز اضطراری و سایر زیرساخت‌های مهم می‌تواند بسیار خطرناک و بحرانی باشد.

دفاع در برابر باج‌افزار در سازمان‌ها و شرکت‌ها نیاز به یک رویکرد جامع دارد که کل افراد را درگیر خواهد کرد. در ادامه هفت گام معرفی می‌شود که سازمان‌ها با استفاده از این روش‌ها می‌توانند حملات را متوقف کرده و یا اثرات حملات باج‌افزاری را محدود کنند. هر کدام از این هفت گام با بهترین سیاست‌های امنیتی مرکز CIS Securityمنطبق بوده و برای هر موضوع از طریق این مرجع می‌توان اطلاعات بیشتری را کسب کرد.

۱. دقت به عملیات پشتیبان‌گیری

مرکزMS-ISAC توصیه می‌کند که تهیه نسخه پشتیبان از داده‌های مهم، مؤثرترین روش مقابله با آلودگی باج‌افزار است. با این حال، مواردی را باید در نظر داشته باشید. فایل‌های پشتیبان شما باید به طور مناسب

محافظت شود و به‌صورت آفلاین یا خارج از همان سیستم ذخیره شود تا توسط مهاجمین مورد هدف قرار نگیرد. استفاده از سرویس‌های ابری می‌تواند به شما در مقابله با آلودگی به باج افزارها کمک کند، زیرا نسخه‌های قبلی فایل‌ها را حفظ می‌کنند که به کاربر امکان می‌دهد به نسخه غیررمزنگاری شده، دستیابی داشته باشد. حتماً نسخه‌های پشتیبان بصورت مداوم برای اطمینان از مؤثر بودنشان، تست شوند. در صورت رخداد حمله، قبل از عملیات بازگردانی با استفاده از نسخه پشتیبان، مطمئن شوید که این نسخه نیز آلوده نشده باشد.

در CIS Control 10 که در لینک منبع قرار داده شده است جزئیات بیشتری در مورد نحوه تهیه یک برنامه گرفتن نسخه پشتیبان و بازیابی اطلاعات ارائه شده است.

۲. تدوین سازوکار و سیاست‌هایی در خصوص رخدادها

ایجاد یک سازوکار برای مقابله و پاسخ به رخدادها ضروری به نظر می‌رسد تا تیم فناوری اطلاعات وامنیت سایبری شما بداند که باید در حین یک رخداد باج‌افزاری چه کاری انجام باید دهد. این طرح شامل نقش‌ها و ارتباطات تعریف شده‌ای است که باید در حین حمله به اشتراک گذاشته شود. همچنین باید لیستی از مخاطبین مانند ذی‌نفعان یا مشتریان و یا کاربران که باید به آن‌ها اطلاع داده شود، در لیست درج شود. آیا سیاست‌هایی مانند "ایمیل مشکوک" دارید؟ اگر نه، میبایستی سیاستی همانند این مورد باید برای کل شرکت در نظر بگیرید. در نظر گفتن این سیاست به کارمندان آموزش می‌دهد که در صورت دریافت ایمیلی که از آن‌ها اطمینان ندارند، چه کاری باید انجام دهند مانند عدم دریافت پیوست ایمیل و ارسال آن ایمیل مشکوک به تیم امنیت سایبریشرکت یا سازمان.

در CIS Control 19 که در لینک منبع قرار داده شده است جزئیات بیشتری در مورد مقابله، پاسخ و مدیریت رخدادها بیان شده است.

۳. بازنگری درخصوص پورت‌ها

بسیاری از انواع باج‌افزارها از پورت 3389 (RDP) و پورت 445 (SMB) استفاده می‌کنند. باید در نظر گرفت که آیا سازمان یا شرکت شما نیاز دارد که این پورت‌ها را باز کند یا خیر، و چه فیترها و محدودیت‌هایی برای ارتباطات باید در نظر گرفته شود. حتماً این تنظیمات را هم برای محیط داخلی و هم در فضای ابری بررسی کرده و به ارائه‌دهنده خدمات ابری خود توصیه‌هایی برای غیرفعال کردن سرویس‌هایی مانند RDP که مورد استفاده نیستند، انجام شود.

در CIS Control 9 و CIS Control12 که در لینک منبع قرار داده شده است جزئیات بیشتری در مورد روش‌های مختلفی که شرکت یا سازمان شما می‌تواند پورت‌ها، پروتکل‌ها و سرویس‌های شبکه را کنترل کند، بیان شده است.

۴. امن‌سازی Endpoint ها

باید اطمینان حاصل کرد که سیستم‌های مورد استفاده در شرکت یا سازمان با امنیت بالا پیکربندی شده‌اند. تنظیمات پیکربندی امن می‌تواند به محدود کردن سطح تهدید سازمان و بستن شکاف‌های امنیتی کمک کرده و معمولا داشتن تنظیمات پیش‌فرض امنیت را تضمین نمی‌کنند. در سایت CISecurity بخش به نام CIS Benchmark وجود دارد که معیارها و راهنمایی‌هایی برای سنجش و امن‌سازی ارائه می‌کند و یک انتخاب عالی و بدون هزینه برای سازمان‌هایی است که به دنبال پیکربندی امن برای سیستم‌های خود هستند.

در CIS Control 5 که در لینک منبع قرار داده شده است جزئیات بیشتری در مورد پیکربندی امن سیستم‌ها بیان شده است.

۵. توجه به به‌روزرسانی سیستم‌ها

باید اطمینان حاصل کرد که همه سیستم‌عامل‌ها، برنامه‌ها و نرم‌افزارهای سازمان به‌طور مداوم به‌روزرسانی می‌شوند. انجام عملیات به‌روزرسانی باعث می‌شود نقص‌ها و شکاف‌های امنیتی موجود، که مهاجمین به دنبال سوءاستفاده از آن‌ها هستند، رفع گردد. در صورت امکان، تنظیم به‌روزرسانی‌های خودکار فعال گردد تا به‌صورت خودکار آخرین به‌روزرسانی‌ها و وصله‌های امنیتی اعمال گردد.

در CIS Control 3 که در لینک منبع قرار داده شده است جزئیات بیشتری در مورد به‌روزرسانی‌ها و اعمال وصله‌های امنیتی بیان شده است.

۶. توجه به آموزش و آگاهی‌رسانی به تیم کاری

یکی از مهمترین جنبه‌ها برای مقابله با حملات باج‌افزاری در سازمان‌ها و شرکت‌ها توجه به امر آموزش است. به طور مثال یکی از راه‌های آلودگی سیستم، باز کردن ایمیل‌های مخرب و دریافت پیوست‌های آن‌ها است که تمامی کارکنان سازمان و شرکت‌ها این نوع ایمیل‌ها را دریافت می‌کنند و میبایستی آموزش مناسب در این

حوزه به افراد برای جلوگیری از آلوده شدن سیستم‌ها داده شود، پس به این نتیجه می‌رسیم که همه افراد در حفاظت از سازمان نقش دارند.

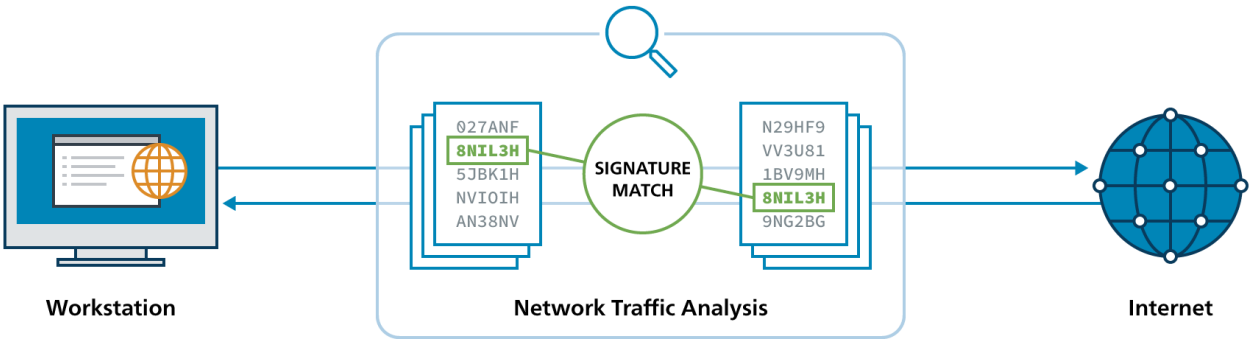
در CIS Control 17 که در لینک منبع قرار داده شده است جزئیات بیشتری در مورد آگاهی‌رسانی و آموزش‌های امنیتی به کارکنان بیان شده است.

۷. پیاده‌سازی IDS

یک سیستم تشخیص نفوذ (IDS) با مقایسه ترافیک شبکه با امضاهایی که فعالیت‌های مخرب شناخته شده را داشته‌اند، به کشف فعالیت مخرب می‌پردازند. یک IDS مقاوم و قوی اغلب بانک اطلاعاتی امضاهای خود را به روز می‌کند و در صورت شناسایی فعالیت‌های مخرب احتمالی، به سرعت به سازمان شما هشدار لازم را می‌دهد.

در CIS Control 6 و CIS Control 12 که در لینک منبع قرار داده شده است جزئیات بیشتری در مورد مانیتورینگ، نگهداری، تجزیه و تحلیل لاگ‌ها و ترافیک توسط IDS بیان شده است.

در زیر این سازوکار نشان داده شده است.



در نهایت نکته بسیار مهم در هنگام رخ دادن حملات باج‌افزاری این است که مدیران فناوری اطلاعات و تیم امنیت سایبری سازمان یا شرکت به سرعت از حمله اطلاع پیدا کرده و بررسی انجام شود. بر اساس داده‌های Crowdstrike، ۱۰ دقیقه طول می‌کشد تا یک سازمان با تیم قدرتمند امنیت سیابری یک نفوذ را بررسی کند با این حال، تنها ۱۰٪ سازمان‌ها قادر به رعایت این معیار هستند!!!

منابع:

- https://www.cisecurity.org/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware/
- https://www.cisecurity.org/controls/data-recovery-capability/
- https://www.cisecurity.org/controls/incident-response-and-management/
- https://www.cisecurity.org/controls/limitation-and-control-of-network-ports-protocols-and-services/
- https://www.cisecurity.org/controls/boundary-defense/
- https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/
- https://www.cisecurity.org/controls/continuous-vulnerability-management/
- https://www.cisecurity.org/controls/implement-a-security-awareness-and-training-program/
- https://www.cisecurity.org/controls/maintenance-monitoring-and-analysis-of-audit-logs/