کنترل های امنیتی حیاتی CIS از دیدگاه SANS

با توجه به توضیحات ارائه شده و اهمیت استفاده و پیاده سازی این ۲۰ کنترل امنیتی، موسسه SANS نیز یک دوره اختصاصی برای این منظورم با نام SANS SEC 566 تحت عنوان SANS Critical Security Controlsرا تدوین نموده است که به شما کمک می کند تا تکنیک های خاص و اثبات شده و ابزارهای مورد نیاز برای اجرای و ممیزی کنترل های امنیتی بحرانی را که توسط مرکز امنیت اینترنت (CIS) مستند شده است، در شرکت یا سازمان خود استفاده نمایید.

با گسترش تهدیدات، امنیت سازمان نیز باید بهبود یابند .برای فعال کردن سازمان خود در بالای این سناریوی تهدید در حال تغییر، یک دوره جامع) همان دوره (SANS SEC 566 در مورد چگونگی اجرای کنترل های امنیتی بحرانیCIS20 ، یک رویکرد اولویت بندی شده و مبتنی بر ریسک برای امنیت طراحی کرده است. این کنترل های امنیتی بهترین روش برای جلوگیری از حملات شناخته شده و کاهش آسیب ناشی از حملات موفقیت آمیز توسط متخصصان بخش خصوصی و دولتی از سراسر جهان است. آنها توسط وزارت امنیت داخلی ایالات متحده آمریکا، دولت های ایالتی، دانشگاه ها و بسیاری از شرکت های خصوصی پذیرفته شده اند.

کنترل های امنیتی حیاتی CIS از دیدگاه SANS

در واقع کنترل ها دستورالعمل های خاصی هستند که CISO ها (افسران ارشد امنیت اطلاعات)، CIO ها (مدیر ارشد فناوری اطلاعات)، IG ها (بازرسان ارشد)، سرپرست سیستم ها و پرسنل امنیت اطلاعات می توانند از آنها برای مدیریت و سنجش اثربخشی دفاع خود استفاده کنند. آنها برای تکمیل استانداردهای موجود، چارچوب ها و برنامه های انطباق با اولویت قرار دادن مهمترین تهدید و بالاترین میزان دفاع از پرداخت، ضمن ارائه یک مبنای مشترک برای اقدام در برابر خطراتی که همه ما با آن روبرو هستیم.

کنترل بحرانی ۱: موجودی دستگاه های مجاز و غیرمجاز

هر وقت دستگاه جدیدی روی شبکه نصب می شود، ریسک مواجهه شبکه با آسیب پذیری های ناشناخته یا مختل کردن عملکرد شبکه وجود دارد. کدهای مخرب می توانند از سخت افزار جدیدی که در زمان نصب پیکربندی و patch نشده و با استفاده از بروزرسانی های مناسب امنیتی در زمان نصب استفاده کنند. مهاجمان نیز می توانند از این سیستم های آسیب پذیر قبل از اینکه آنها را harden کنند جهت نصب backdoor ها استفاده کنند. در کنترل بحرانی ۱ بصورت اتوماتیک، کلیه تجهیزات دارای یک سیستم کنترل موجودی دقیق و به روز هستند. هر دستگاهی که در دیتابیس نباشد باید از اتصال آن به شبکه ممانعت شود. بعضی از سازمان ها با استفاده از محصولات تجاری enterprise در مقیاس بزرگ یا با استفاده از Solution های رایگان برای ردیابی و جابجایی شبکه بصورت دوره ای، asset inventory یا لیست دارایی های خود را حفظ و نگهداری می کنند. جهت ارزیابی اجرای کنترل ۱ به صورت دوره ای، تیم ارزیابی سیستم های تست harden شده را به حداقل ۱۰ مکان یا location در شبکه وصل می کند. این شامل مجموعه ای از زیرشبکه ها یا subnet های مرتبط با DMZ ها، workstation ها و server ها خواهد بود.

کنترل بحرانی ۲: موجودی نرم افزار مجاز و غیرمجاز

یک سازمان بدون توانایی موجودی و کنترل برنامه های نصب شده کامپیوترهای خود، سیستم های خود را در برابر حمله آسیب پذیرتر می کند. علاوه بر این، ماشین های کنترل شده ضعیف احتمالاً نرم افزاری را که برای اهداف تجاری بی ضرر است، در معرض نقص امنیتی بالقوه می دهند. سیستم های تسخیر شده به یک نقطه مهم برای مهاجمین برای جمع آوری اطلاعات حساس تبدیل می شوند. برای مقابله با این تهدید بالقوه، یک سازمان باید یک شبکه را اسکن کند و برنامه های شناخته شده یا پاسخ دهنده را شناسایی کند. نرم افزارهای تجاری و asset inventory به طور گسترده ای در دسترس هستند. بهترین ابزارها یک inventory از صدها مورد از برنامه های متداول را تهیه می کنند و اطلاعات مربوط به سطح patch هر برنامه نصب شده را به دست می آورند. این اطمینان حاصل می شود که آخرین نسخه از نرم افزار نصب شده و از اسامی برنامه های استاندارد مانند موارد موجود در مشخصات Common Platform Enumeration (CPE) استفاده می کند. علاوه بر بررسی های

کنترل های امنیتی حیاتی CIS از دیدگاه SANS

inventory، ابزارهایی که whitelistها (اجازه یا allow) و blacklistها (منع یا deny) را اجرا می کنند، در بسیاری از مجموعه های امنیتی مدرن در نقطه پایانی گنجانده شده اند. جهت ارزیابی پیاده سازی کنترل ۲ به صورت دوره ای، تیم باید یک برنامه تست نرم افزار خوب را که در لیست نرم افزارهای مجاز در ۱۰ سیستم موجود در شبکه درج نشده است، منتقل کند. سپس تیم باید تأیید کند که نرم افزار block شده و قادر به اجرای آن نیست.

کنترل بحرانی ۳: تنظیمات ایمن برای سخت افزار و نرم افزار در Laptopها، Workstationهای و Server ها

کنترل بحرانی ۳ به "جمع آوری، پایش و تحلیل لاگ های سیستم ها" می پردازد. شما می بایست نسبت به جمع آوری، مدیریت و تحلیل لاگ های سیستم های شبکه به منظور کشف، درک و یا بازیابی وضعیت سازمان به قبل از حملات امنیتی اقدام نمایید. توجه داشته باشید که، پیکربندی های پیش فرض نرم افزارها معمولاً جهت سهولت کاربری و سهولت استفاده و امنیت انجام نمی شوند و برخی سیستم ها را در حالت پیش فرض خود غیرقابل استفاده می کنند. مهاجمان سعی می کنند با استفاده از انواع مختلف بدافزارها، از هر دو سرویس قابل دسترسی به شبکه و نرم افزار مشتری بهره برداری (exploit) کنند. شرکت های بدون توانایی موجودی (یا inventory) و کنترل نصب و راه اندازی شده، سیستم های خود را آسیب پذیرتر می کنند. سازمان ها با پیاده سازی این کنترل توسط توسعه یکسری از imageها و سرورهای ذخیره سازی امن برای میزبانی از این imageهای استاندارد، می بایست این کنترل را پیاده سازی نمایند. از ابزارهای مدیریت پیکربندی می توان برای اندازه گیری تنظیمات نرم افزار نصب شده و جستجوی انحراف از تنظیمات image استاندارد استفاده شده توسط سازمان استفاده کرد. جهت ارزیابی اجرای کنترل ۳ به صورت دوره ای، یک تیم ارزیابی باید یک سیستم تست مناسب (یک سیستم که حاوی imageی باشد که harden نشده یا harden image رسمی، اما شامل سرویس های اضافی، پورت ها و تغییر فایل های پیکربندی است) بر روی شبکه قرار دهد. سپس تیم ارزیابی باید تأیید کند که سیستم ها در مورد تغییرات نرم افزار، هشدار یا ایمیلی را ایجاد می کنند.

کنترل بحرانی ۴: ارزیابی مستمر آسیب پذیری ها و اصلاح آنها

به زودی پس از کشف و گزارش آسیب پذیری های جدید توسط محققان امنیتی یا فروشندگان، مهاجمین از exploit code ها استفاده کرده و آنها را در برابر اهداف مورد نظر خود راه اندازی می کنند. هرگونه تأخیر قابل توجه در یافتن یا رفع نرم افزارهای دارای آسیب پذیری های مهم، فرصت کافی را برای مهاجمین بطور پیوسته فراهم می کند تا از بین بروند و کنترل ماشین های آسیب پذیر را به دست آورند. تعداد زیادی از ابزارهای اسکن

کنترل های امنیتی حیاتی CIS از دیدگاه SANS

آسیب پذیری برای ارزیابی پیکربندی امنیتی سیستم ها در دسترس هستند. ابزارهای اسکن آسیب پذیری، نتایج اسکن فعلی را با اسکن های قبلی مقایسه می کنند تا تعیین کنند که چگونه آسیب پذیری های محیط با گذشت زمان تغییر کرده اند. تمام ماشین های مشخص شده توسط asset inventory یا سیستم موجودی دارایی باید برای یافتن آسیب پذیری ها اسکن شوند. جهت ارزیابی عملکرد کنترل ۴ به صورت دوره ای، تیم ارزیابی باید تأیید کند که ابزارهای اسکن، اسکن های خود را به صورت هفتگی یا روزانه با موفقیت انجام داده اند.

کنترل بحرانی ۵: استفاده کنترل شده از Administrative Privilege ها

متداول ترین روشی که مهاجمان برای نفوذ به یک شرکت هدف از آن استفاده می کنند، از طریق سوء استفاده شخصی ازAdministrative Privilege است. یک مهاجم می تواند به راحتی یک کاربر workstation را متقاعد کند که attachment یک ایمیل مخرب را باز کند، یک فایل را از یک سایت مخرب دانلود و باز کند، یا از یک سایت بازدید کرده که به طور خودکار محتوای مخرب را دانلود کند. اگر کاربر به عنوان administrator وارد سیستم شود و به آن login کند، در این حالت مهاجم دسترسی کامل به سیستم دارد. ویژگی های داخلی و built-in شده در سیستم عامل می تواند لیستی از اکانت ها را با دسترسی super-user، به صورت محلی بر روی سیستم های شخصی و domain controller ها بصورت کلی استخراج (extract) کند. این اکانت ها باید بسیار دقیق رصد و ردیابی شوند. برای ارزیابی اجرای کنترل ۵ به صورت دوره ای، یک تیم ارزیابی باید تأیید کنند که خط مشی رمز عبور یا password policy سازمان اجرا شده است و اکانت های administrator با دقت کنترل می شوند. تیم ارزیابی این کار را با ایجاد یک حساب کاربری تستی، موقت، غیرفعال (disable) و محدود بر روی ۱۰ سیستم مختلف انجام می دهد. سپس سعی می کند رمز عبور یا password را بر روی حساب کاربری مزبور تا حدی که خط مشی رمز عبور سازمان را برآورده نکرده، تغییر دهند.

کنترل بحرانی ۶: نگهداری، نظارت و تجزیه و تحلیل Audit Log ها

در بعضی مواقع، Audit Logها تنها شواهدی از حمله موفقیت آمیز را نشان می دهند. بسیاری از سازمان ها سوابق حسابرسی یا audit recordها را برای اهداف انطباق نگه می دارند، اما بندرت آنها را مرور می کنند. وقتی Audit Logها بررسی نشود، سازمان ها نمی دانند سیستم هایشان به خطر افتاده است. مهاجمان به این امر اعتماد دارند. اکثر سیستم عامل های رایگان و تجاری، سرویس های شبکه و تکنولوژی های فایروال قابلیت های login به سیستم را ارائه می دهند. بنابراین قابلیت login به سیستم باید فعال شود و logها را به سرورهای centralized logging (سرورهایی که پروسه login کردن را متمرکز می کنند مثل SSO) ارسال کنید. سیستم باید قادر به ثبت تمام وقایع در شبکه باشد و ورود به سیستم باید از هر دو طریق شبکه و سیستم های

host-based معتبر و امکان پذیر باشد. برای ارزیابی اجرای کنترل ۶ به صورت دوره ای، یک تیم ارزیابی باید گزارش های امنیتی تجهیزات مختلف شبکه، سرورها و هاست ها را بررسی کند.

کنترل بحرانی ۷: محافظت از Email و Web Browser

مرورگرهای وب و سرویس گیرندگان ایمیل به دلیل پیچیدگی و انعطاف پذیری فنی بالا و تعامل مستقیم آنها با کاربران و در درون سیستم ها و وب سایت های دیگر، نقاط ورود و حمله بسیار رایج هستند. محتوا را می توان برای جلب توجه کاربران کلاهبردار یا اصطلاحاً spoof userها در انجام اقداماتی که خطر و ریسک را بسیار افزایش می دهند و اجازه ورود کد مخرب، از دست دادن داده های ارزشمند و سایر حملات را فراهم می آورد. سازمان ها باید از سطح حمله یا اصطلاحاً attack surface و فرصت حمله مهاجمین برای دستکاری رفتار انسان از طریق تعامل با مرورگرهای وب و سیستم های ایمیل استفاده کنند.

کنترل بحرانی ۸: دفاع از بدافزار

نرم افزارهای مخرب یک جنبه جدایی ناپذیر و خطرناک از تهدیدات اینترنت هستند. این کاربران و سازمان ها از طریق مرور وب، پیوست های ایمیل ها، دستگاه های تلفن همراه و سایر vectorها (منظور مکانیزم حمله ای که یک هکر برای نفوذ و هک کردن پیش می گیرد) هدف قرار می دهد. کد مخرب ممکن است محتوای سیستم را دستکاری کند، داده های حساس را ضبط کند و به سایر سیستم ها گسترش یابد. برای اطمینان از به روز بودن signatureهای آنتی ویروس، سازمان ها از اتوماسیون یا automation استفاده می کنند. آنها از ویژگی های built-in شده مدیریتی enterprise endpoint security suiteها استفاده می کنند تا تأیید کنند که ویژگی های آنتی ویروس، ضد جاسوس افزار یا anti-spyware و سیستم های تشخیص نفوذ از نوع host-based (یا HIDSها) در هر سیستم مدیریت شده فعال هستند. آنها همچنین بصورت روزانه ارزیابی های خودکار را انجام می دهند و نتایج را بررسی می کنند تا سیستم هایی را پیدا کنند که چنین محافظت هایی را غیرفعال کرده یا آخرین تعاریف بدافزار را ندارند (منظور featureهای امنیتی که off کرده اند مثل غیرفعال کردن قابلیت های windows defender در سیستم عامل های ویندوزی). این سیستم باید هرگونه نرم افزاری مخرب را که نصب شده، سعی در نصب، اجرای یا تلاش برای اجرای آن بر روی یک سیستم رایانه ای دارد، شناسایی کند. برای ارزیابی پیاده سازی کنترل ۸ به صورت دوره ای، تیم ارزیابی باید یک برنامه تست نرم افزار را که مناسب به نظر برسد مورد استفاده قرار داده، با فرض اینکه بدافزاری بر روی یک سیستم است و مطمئن شود که بدافزار مزبور به درستی کشف و اصلاح (منظور فاز Remediate) شده است. (در مقاله ای جداگانه به تشریح انواع فازهای بررسی بدافزارها و اسکن آنها خواهم پرداخت). اما بطور کلی می بایست اشاره نمایم که فاز Remediate در واقعی فازی پس از انجام پروسه اسکن آسیب پذیری ها توسط یک اسکنر است که زمانیکه یک آسیب پذیری را بر روی سیستم

هدف خود یافتید می بایست از طریق رهنمودهای ارائه شده توسط اسکنر خود اقدام به برطرف کردن آن نمایید (به عنوان مثال نصب hotfixها، security patchها و... بر روی سیستم هدف. معمولاً اسکنرهای آسیب پذیری معروف همچون: Nessus، Nexpose، OpenVAS، Acunetix، GIL LanGuard و... چنین Remediationهایی را ارائه می دهند). (در صورت تمایل جهت کسب اطلاعات بیشتر در این خصوص می توانید به فصل Vulnerability Assessment یا ارزیابی آسیب پذیری از کتاب مرجع آموزش CEH Master، تألیف مهندس میثم ناظمی، از انتشارات ناقوس مراجعه نمایید).

شکل ۳ – فازهای مختلف یک پروسه اسکن آسیب پذیری

کنترل بحرانی ۹: محدودیت و کنترل پورت های شبکه، پروتکل ها و سرویس ها

معمولاً مهاجمان سرویس های شبکه از راه دور (منظور remote serviceها) را که در معرض بهره برداری و exploit قرار دارند، جستجو می کنند. بسیاری از packageهای نرم افزاری بطور خودکار سرویس هایی را نصب می کنند و آنها را به عنوان بخشی از نصب بسته نرم افزاری اصلی در حالت on (فعال) قرار می دهند. هنگامی که این اتفاق می افتد، نرم افزار به ندرت به کاربر اطلاع می دهد که سرویس ها فعال شده اند. شما می توانید از ابزارهای Port Scanning جهت تعیین اینکه کدام سرویس ها در شبکه برای طیف وسیعی از سیستم های هدف در حالت listening هستند، استفاده می شود. علاوه بر تعیین اینکه کدام پورت ها باز هستند، می توان از اسکنرهای پورت برای پیکربندی و شناسایی نسخه پروتکل و سرویسی که در حال listening در هر پورت باز کشف شده استفاده نمود. این سیستم باید قادر به شناسایی پورت های جدید شبکه که در حالت listening غیر مجاز شبکه متصل هستند، باشد. جهت ارزیابی پیاده سازی کنترل ۹ به صورت دوره ای، تیم ارزیابی باید سرویس های تست harden شده را با listenerهای شبکه در ۱۰ مکان در شبکه، از جمله انتخاب زیرشبکه های مرتبط با DMZ، workstationها و سرورها نصب کند.

کنترل های امنیتی حیاتی CIS از دیدگاه SANS

کنترل بحرانی ۱۰: قابلیت بازیابی اطلاعات

زمانیکه مهاجمین ماشین ها را تسخیر می کنند، آنها اغلب در پیکربندی ها و نرم افزارها تغییرات قابل توجهی ایجاد می کنند. بعضی اوقات، مهاجمین همچنین تغییراتی ظریف در داده های ذخیره شده در تجهیزات تسخیر شده ایجاد می کنند و به طور بالقوه می توانند اثر سازمانی را با اطلاعات آلوده به خطر اندازند. در هر ۳ ماه یکبار، یک تیم تست برای بازگرداندن و restore آنها در یک بستر تست، می توانند نمونه تصادفی از backup سیستم را ارزیابی کنند. سیستم های بازیابی شده باید تأیید شوند تا اطمینان حاصل شود که سیستم عامل، برنامه و داده های restore شده از backup همگی دست نخورده و کاربردی هستند.

کنترل بحرانی ۱۱: تنظیمات امن برای دستگاه های شبکه مانند فایروال ها، روترها و سوئیچ ها

مهاجمان با جستجوی سوراخ های الکترونیکی یا اصطلاحاً electronic holeها در فایروال ها، روترها و سوئیچ ها به خط دفاعی آنها نفوذ می کنند. پس از بهره برداری یا exploit کردن این دستگاه های شبکه، مهاجمان می توانند به شبکه های هدف دسترسی پیدا کنند، ترافیک را در آن شبکه هدایت کرده (به یک سیستم مخرب که به عنوان یک سیستم مورد اعتماد در حال جابجایی است) و در هنگام انتقال، اطلاعات را رهگیری و تغییر دهند. سازمان ها می توانند از ابزارهای تجاری استفاده کنند که مجموعه قوانین تجهیزات فیلترینگ شبکه را ارزیابی کنند، که تعیین می کند آیا آنها سازگار بوده یا در تضاد هستند و یک بررسی خودکار از فیلترهای شبکه را ارائه می دهند. علاوه بر این، این ابزارهای تجاری errorها در مجموعه قوانین یا rule setها جستجو می کنند. این ابزارها باید هر بار اجرا شوند تا تغییرات مهمی را در مجموعه قوانین فایروال ها، ACLهای روتر یا سایر فناوری های فیلترینگ، ایجاد کنند. برای ارزیابی عملکرد کنترل ۱۱ به صورت دوره ای، یک تیم ارزیابی باید در هر نوع تجهیز متصل به شبکه تغییری ایجاد کند. حداقل، روترها، سوئیچ ها و فایروال ها باید تست شوند. در صورت وجود، IPS، IDS و سایر دستگاه های شبکه باید درج شوند.

کنترل بحرانی ۱۲: دفاع مرزی یا Boundary Defense

با حمله به سیستم های بر روی اینترنت (که روی اینترنت publish شده اند)، مهاجمین می توانند یک نقطه رله یا اصطلاحاً Relay Point برای خود ایجاد کنند تا به شبکه ها یا سیستم های داخلی دیگر نفوذ نمایند. از ابزارهای خودکار می توان جهت سوء استفاده از نقاط ورود آسیب پذیر به شبکه استفاده کرد. برای کنترل جریان ترافیک از طریق مرزهای شبکه و جستجوی حملات و شواهدی از ماشین های به خطر افتاده، باید از دفاع مرزی چند لایه استفاده کرد. این مرزها باید از فایروال ها، proxyها، شبکه های DMZ و سیستم های IPS مبتنی بر

شبکه و سیستم های IDS تشکیل شود. سازمان ها باید با راه اندازی ابزارهای اسکن آسیب پذیری، مرتباً این حسگرها را تست و آزمایش کنند. این ابزارها تأیید می کنند که ترافیک اسکنر باعث ایجاد یک هشدار مناسب می شود. بسته های capture شده از سنسورهای IDS باید هر روز با استفاده از یک اسکریپت خودکار مورد بررسی قرار گیرند تا اطمینان حاصل شود میزان ورود به سیستم در پارامترهای مورد انتظار قرار گرفته است، به درستی قالب بندی شده و خراب (منظور corrupt) نشده اند. برای ارزیابی اجرای کنترل ۱۲ به صورت دوره ای، یک تیم ارزیابی باید تجهیزات مرزی را تست و آزمایش کند. این کار با ارسال بسته هایی از خارج از یک شبکه trust انجام می شود که تضمین می کند فقط بسته های مجاز یا authorized packetها از طریق تجهیزات مرزی اجازه عبور دارند (allow) و همه بسته های دیگر باید drop شوند.

کنترل بحرانی ۱۳: حفاظت از داده ها یا Data Protection

از بین رفتن داده های محافظت شده و حساس یک تهدید جدی برای عملیات تجاری و بالقوه امنیت ملی است. در حالی که برخی از داده ها به دلیل سرقت یا جاسوسی به بیرون درز پیدا می کنند (اصطلاً leak می شوند) یا از بین می روند (اصطلاحاً lost می شوند)، بخش عمده ای از این مشکلات ناشی از درک ضعیف داده های نادرست نشأت می گیرد. این موارد شامل فقدان معماری سیاست مؤثر و خطای کاربر نیست، اما محدود به آنها هم نیست. عبارت "جلوگیری از، از دست دادن داده" یا Data Loss Prevention یا به اختصار DLP به یک رویکرد جامع شامل افراد، فرآیندها و سیستم هایی که اطلاعات در حال استفاده را شناسایی، نظارت و محافظت می کنند اطلاق می شود (به عنوان مثال، endpoint actionها)، داده های در حال حرکت (به عنوان مثال، network actionها) و داده ها در حالت استراحت (به عنوان مثال، داده های ذخیره شده یا data storage) از طریق deep content inspection و با یک چارچوب مدیریت متمرکز یا centralized management framework صورت می گیرد. امروزه Solutionهای تجاری DLP جهت جستجوی تلاش برای تبادل و کشف سایر فعالیت های مشکوک مرتبط با یک شبکه محافظت شده دارای اطلاعات حساس در دسترس هستند. این سیستم باید قادر به شناسایی داده های غیرمجاز باشد که سیستم های سازمان را از طریق انتقال فایل در شبکه یا removable mediaها (مثل Flash Memoryها و...) از سیستم خارج می کند. جهت ارزیابی پیاده سازی کنترل ۱۳ به صورت دوره ای، تیم ارزیابی باید تلاش کند تا مجموعه داده های تست شده (که باعث سیستم های DLP می شوند اما شامل اطلاعات حساس نیستند) را از طریق انتقال فایل ها در شبکه و از طریق removable mediaها قابل جابجایی به خارج از محیط قابل اعتماد و trust شبکه منتقل کند. به عنوان مثال می توان از ابزارهای OpenDLP، MyDLP و ماژول های DLP بر روی UTMهایی همچون FortiGate در این بخش اشاره نمود.

کنترل های امنیتی حیاتی CIS از دیدگاه SANS

کنترل بحرانی ۱۴: دسترسی کنترل شده مبتنی بر نیاز به دانستن

برخی سازمان ها داده های حساس را از اطلاعات حساس و کمتر در دسترس عموم در یک شبکه داخلی با دقت شناسایی و جدا نمی کنند. تا جاییکه در بسیاری از محیط ها، کاربران داخلی به کلیه یا بیشتر اطلاعات موجود در شبکه دسترسی دارند. هنگامی که مهاجمان به چنین شبکه ای نفوذ می کنند، می توانند با مقاومت کمی اطلاعات مهم را پیدا کرده و از آنها جدا کنند. این کنترل اغلب با استفاده از جداسازی داخلی administrator accountها از اکانت های غیر مدیریتی اجرا می شود. این سیستم باید بتواند تمام تلاش های کاربران جهت دسترسی به فایل ها را بدون privilegeهای مناسب تشخیص دهد و باید یک alert یا email برای پرسنل اداری ایجاد نماید. این موضوع شامل اطلاعات مربوط به سیستم های محلی یا فایل های قابل دسترسی به اشتراک گذاشته شده شبکه است. جهت ارزیابی اجرای کنترل ۱۴ بصورت دوره ای، تیم ارزیابی باید یکسری اکانت های تستی با دسترسی محدود ایجاد کرده و تأیید کند که اکانت قادر به دستیابی به اطلاعات کنترل شده نیست.

کنترل بحرانی ۱۵: کنترل دستگاه بیسیم

مهاجمانی که از پارکینگ های مجاور و از طریق ارتباطات بیسیم به یک سازمان دسترسی پیدا می کنند، سرقت های داده های اصلی را آغاز کرده اند. این موضوع به مهاجمان اجازه می دهد یک سازمان دور بزنند تا دسترسی طولانی مدت را در داخل یک هدف (منظور سیستم قربانی) حفظ کنند. سازمان ها نیز برای جلوگیری از این مورد، از اسکنرهای بیسیم تجاری و ابزارهای کشف و تشخیص همچون Wireless IDSها تجاری استفاده می کنند. سیستم باید قادر باشد دستگاه های بیسیم غیرمجاز یا پیکربندی های غیرمجاز را هنگام دسترسی در محدوده سیستم های سازمان یا به شبکه های آن شناسایی کند. برای ارزیابی اجرای کنترل ۱۵ بصورت دوره ای، کارکنان تیم ارزیابی باید اقدام به پیکربندی امن و harden کردن تجهیزات غیرمجاز وایرلس، کلاینت های وایرلس و همچنین Access Pointهای وایرلسی در شبکه سازمان نمایند. همچنین باید تلاش کنند تا آنها را به شبکه های بیسیم سازمان متصل نمایند. این نقاط دسترسی باید به موقع شناسایی و اصلاح شوند. به عنوان مثال می تواند به ابزار Kismet به عنوان یک ابزار Open Source و رایگان که عنوان یک Wireless IDS عمل می‌کند در این بخش اشاره نمود.

کنترل بحرانی ۱۶: کنترل و مانیتور اکانت

مهاجمان غالباً از طریق اکانت های کاربری غیرفعال، حساب کاربران مشروع را جعل می کنند. این روش برای network watcherها تشخیص رفتار مهاجمین را دشوار می کند. اگرچه اکثر سیستم عامل ها دارای امکاناتی برای logging information در مورد استفاده از اکانت هستند، اما این ویژگی ها گاهی به صورت پیش فرض

کنترل های امنیتی حیاتی CIS از دیدگاه SANS

غیرفعال هستند. پرسنل امنیتی می توانند سیستم ها را برای ضبط اطلاعات دقیق تر در مورد دسترسی به اکانت پیکربندی کرده و از اسکریپت های یا ابزارهای تجزیه و تحلیل log که معمولاً به صورت third-party ارائه می شوند جهت تجزیه و تحلیل این اطلاعات استفاده کنند. این ابزارها باید قادر به شناسایی اکانت های کاربری غیرمجاز موجود بر روی سیستم ها باشند. برای ارزیابی پیاده سازی کنترل ۱۶ به صورت دوره ای، تیم ارزیابی باید تأیید کند که لیست اکانت های lock شده، اکانت های غیرفعال، اکانت های دارای رمزهای عبورهایی هستند که از حداکثر طول عمرشان گذشته (منظور مدت زما قانون password policy برای ها گذشته) و اکانت های دارای رمزهای عبور که هرگز منقضی نمی شوند، بصورت روزانه با موفقیت تکمیل شده اند.

کنترل بحرانی ۱۷: ارزیابی مهارت های امنیتی و آموزش مناسب برای پر کردن شکاف ها

سازمانی که امید به یافتن و پاسخ دادن به حملات بطور مؤثر را دارد، به کارکنان و پیمانکاران خود متکی است تا بتواند گپ ها و شکاف ها را پیدا کرده و آنها را پر کند. یک برنامه ارزیابی مهارت های امنیتی درست و حسابی می تواند اطلاعات قابل توجهی را در مورد محل های بهبود آگاهی امنیتی در اختیار تصمیم گیرندگان قرار دهد. همچنین می تواند به تعیین تخصیص مناسب منابع محدود برای بهبود روش های امنیتی کمک کند. نکته اصلی برای ارتقاء مهارت ها، اندازه گیری یا measurement است نه با امتحانات صدور گواهینامه بلکه با ارزیابی هایی که هم به کارمند و هم کارفرما نشان می دهد که دانش کافی است و چه شکاف هایی وجود دارد. پس از شناسایی شکاف ها، از آن دسته از کارمندان که دانش لازم را دارند می توان برای به عنوان mentor و مربی کارمندانی که این دانش را ندارند، استفاده نمود. این سازمان همچنین می توانند برنامه های آموزشی ایجاد کنند تا مستقیماً آمادگی کارمندان را حفظ نمایند.

کنترل بحرانی ۱۸: امنیت نرم افزار کاربردی یا Application Software Security

سازمان های جنایی غالباً به هر دو نرم افزار کاربردی مبتنی بر وب و غیر مبتنی بر آسیب پذیری حمله می کنند. در واقع، این یک اولویت اصلی برای مجرمان است. نرم افزار کاربردی از سه طریق در برابر خطر از راه دور آسیب پذیر است:

۱. به درستی اندازه و سایز ورودی کاربر را بررسی نمی کند.
۲. با فیلتر کردن توالی کاراکترهای مخرب به طور بالقوه نمی توان ورودی کاربر پالایش نشده (یا sanitize user input) را از بین برد. (اشاره به ورود کاراکترهای غیرمجاز توسط هکر در حملاتی همچون SQL Injection دارد).
۳. اینکه متغیرها به صورت مناسب initialize و clear نمی شوند.

کنترل های امنیتی حیاتی CIS از دیدگاه SANS

جهت جلوگیری از حملات، نرم افزارهای کاربردی داخلی و third-party باید با دقت مورد تست قرار گیرند تا نقص امنیتی در آنها کشف شود. ابزارهای تست Source Code، ابزارهای اسکن امنیتی Web Application و ابزارهای تست object codeها در تأمین امنیت نرم افزار کاربردی بسیار مفید هستند. ابزار مفید دیگر، تست نفوذ امنیتی نرم افزار دستی توسط آزمایش کنندگانی است که دانش برنامه نویسی گسترده و تخصص تست نفوذ را دارند. این سیستم باید قادر به شناسایی و مسدود کردن یک حمله نرم افزاری در سطح برنامه باشد و باید یک alert ایجاد کند یا ایمیلی را برای کارمندان اداری سازمان بفرستد. برای ارزیابی عملکرد کنترل ۱۸ به صورت ماهانه، یک تیم ارزیابی باید از یک اسکنر آسیب پذیری Web Application استفاده کند تا نقص امنیتی نرم افزار را تست کند. از جمله این اسکنرهای آسیب پذیری می توان به اسکنرهایی همچون: Acunetix، Nexpose، Nessus، OpenVAS، GFI LanGuard، N-Stalker، Nikto و... اشاره نمود. در صورت تمایل جهت کسب اطلاعات بیشتر و تمرین عملی با این اسکنرها را می توانید به کتاب مرجع آموزش CEH Master، تألیف مهندس میثم ناظمی از انتشارات ناقوس مراجعه فرمایید.

کنترل بحرانی ۱۹: مدیریت و پاسخگویی به حوادث یا Incident Response

بدون داشتن یک برنامه Incident Response یا پاسخگویی به حوادث، یک سازمان ممکن است در وهله اول کشف یک حمله را انجام ندهد. حتی اگر حمله تشخیص داده شود، ممکن است سازمان از رویه های مناسب پیروی کند تا خسارت وارد شده با حضور مهاجم را ریشه کن کند و به روشی مطمئن بهبود یابد. بنابراین، ممکن است مهاجم تأثیر به مراتب بالاتری در سازمان هدف داشته باشد و باعث صدمه بیشتر، آلوده شدن سیستم های بیشتر و احتمالاً داده های حساس تر شود. پس از تعریف روش های دقیق پاسخ به حادثه، تیم پاسخگویی به حوادث یا تیم IR باید دوره ای در دوره های آموزشی سناریو-محور شرکت کنند. این دوره ها شمل محدودیت نیستند و از طریق انجام یکسری سناریوهای حمله که با تهدیدات و آسیب پذیری هایی که سازمان با آن روبرو است، تنظیم شده اند.

کنترل بحرانی ۲۰: تست های نفوذ و تمرینات تیم قرمز

مهاجمان از طریق مهندسی اجتماعی یا social engineering و با سوء استفاده از نرم افزارها و سخت افزارهای آسیب پذیر، به شبکه ها و سیستم ها نفوذ می کنند. آزمایش نفوذ شامل تقلید از اقدامات مهاجمان رایانه ای و exploit کردن آنها برای تعیین نوع دسترسی یک مهاجم می تواند باشد. هر سازمان باید scope و دامنه روشن و واضحی از قواعد درگیری را برای تست نفوذ و آنالیز تیم قرمز تعریف کند. دامنه چنین پروژه هایی باید حداقل شامل سیستم هایی با بالاترین ارزش اطلاعات و قابلیت پردازش تولید باشد.

کنترل های امنیتی حیاتی CIS از دیدگاه SANS

www.kaliboys.com