قسمت دوم (پایانی)

اقدامات امنیت سایبری در سامانه‌های کنترل صنعتی

برگردان
مهندس علیرضا قره‌خانلو
سرپرست برق و ابزاردقیق و کنترل و مخابرات پروژه‌ی میترینگ پالایشگاه‌های فازهای ۱ تا ۵ و ۹ و ۱۰

واژه‌های کلیدی: امنیت سایبری، راهکارهای اجرایی.

این گزارش اطلاع‌رسانی[1] یا به اصطلاح مقاله‌ی سفید، دوازده توصیه‌ای را شرح می‌دهد که می‌تواند به کاربران سامانه‌های کنترل اتوماسیون صنعتی کمک کند تا نقاط ضعف مورد بهره‌کشی و سوءاستفاده[2] را کاهش دهند و در برابر داده‌دزدی و حملات سایبری مقابله کنند. اطلاعات ارایه شده در این مقاله از منابع متنوعی شامل مطالب سازمان‌های ICS-CERT[3]، FBI[4] و IT-ISAC[5] تهیه و تولید شده است.

1. Whitepaper
2. Exploitation
3. Industrial Control Systems Cyber Emergency Response Team
4. Federal Bureau of Investigation
5. Information Technology-Information Sharing and Analysis Center

۵. بخش‌بندی شبکه را پایه‌ریزی کنید و از دیواره‌های آتش استفاده نمایید

دسترسی به نواحی شبکه را با جداسازی کامل آن‌ها یا با پیاده‌سازی دیواره‌ی آتش محدود نمایید

تکه‌تکه‌کردن شبکه مستلزم طبقه‌بندی و گروه‌بندی ادوات IT، داده و افراد در گروه‌های ویژه و سپس محدودکردن دسترسی به این گروه‌ها می‌باشد. با جانمایی و چینش مناسب منابع در نواحی مختلف شبکه، خطری روی یک تجهیز یا یک بخش، کل سامانه‌ی شما را به مخاطره نخواهد انداخت. در غیراین‌صورت، تهدیدگران سایبری قادر خواهند بود تا از هر درزی به درون سامانه‌ی سازمان‌تان یعنی ضعیف‌ترین حلقه از زنجیره، رخنه کنند تا راهی به‌درون پیدا کنند و به‌سرعت در کل شبکه بچرخند و به تجهیزات و داده‌های حساس دسترسی پیدا کنند. فناوری «اینترنت اشیاء[1]» در حال حاضر ادوات بیشتری را به سامانه‌ها و وب (شبکه‌ی باز عمومی) وصل می‌کند که شامل ادوات زیادی می‌شود که پیش‌تر به اینترنت متصل نبوده‌اند، نظیر دوربین‌های مدار بسته‌ی ویدیویی و سامانه‌های گرمایش و هواساز و سرمایش[2]. افزودن ادوات متصل بیشتر، اهمیت بخش‌بندی شبکه‌ها را بالاتر می برد.

دسترسی به نواحی شبکه را با جداسازی سراسری آن‌ها از یکدیگر محدود کنید که این در مورد ICSها بهترین روش است؛ و یا این که با پیاده‌سازی دیواره‌های آتش این کار را انجام دهید. یک دیواره‌ی آتش برنامه‌ای نرم‌افزاری یا تجهیزی سخت‌افزاری است که تردد (ترافیک) ورودی و خروجی میان بخش‌های مختلف یک شبکه یا اتصال شبکه‌ی مورد نظر با اینترنت را فیلتر (سَرَند) می‌کند. برای نقاطی که به اینترنت وصل می‌شوند، یک دیواره‌ی آتش می‌تواند جهت فیلترکردن اطلاعات ورودی و خروجی عمل کند. تعداد مسیرهای ورودی و داخلی شبکه‌ها را کاهش دهید و مقررات امنیتی[3] روی مسیرهایی که از قبل وجود دارند، پیاده کنید تا کار را برای تهدیدگران جهت رخنه به درون سامانه‌تان و دستیابی به سایر نواحی پرزحمت‌تر کنید.

ایجاد مرزبندی‌ها و بخش‌بندی‌های شبکه، سازمان شما را جهت اعمال کنترل‌های توأمان ردیابی و محافظتی در درون زیرساخت‌تان توانمند می‌سازد. قابلیت پایش، محدودسازی و مدیریت جریان‌های ارتباطی، روشی عملی جهت مرزبندی تردد شبکه (به ویژه ترددهای عبوری از مرزهای یک شبکه) و همچنین جهت شناسایی رفتارهای غیرعادی و مستعد آلودگی فراهم می‌آورد. مرزها و بخش‌ها فرصت‌هایی را فراهم می آورد تا حرکت از یک تجهیز به تجهیز دیگر در ناحیه‌ی مشخص یا حرکت میان نواحی رهگیری شود. در ضمن، شما قادرید، همان‌گونه‌که هکرها (مهاجمین) در تلاش هستند تا بهترین نقاط نفوذ به شبکه‌ی شما را تخمین بزنند، ردپاها و آمار شبکه را رصد کنید.

1. IoT: Internet of Things; IIoT: Industrial Internet of Things
2. HVAC: Heating, Ventilating and Air Conditioning
3. Security Protocol

۶. کنترل دسترسی مبتنی بر نقش بنا کنید و رویدادنگاری (ثبت وقایع) سامانه‌ای را پیاده کنید

مجوزهای کارکنان را از طریق کنترل دسترسی مبتنی بر سمت محدود نمایید و رویدادنگاری را جهت پایش فعالیت سامانه نیز در نظر بگیرید

این نوع کنترل دسترسی امکان دستیابی یا عدم‌دستیابی به منابع شبکه را بر پایه‌ی کارکردهای شغلی ایجاد می‌نماید. این نوع کنترل توانایی فردی کاربرها یا مهاجمین را جهت دستیابی به فایل‌ها یا قسمت‌هایی از سامانه که نباید به آن دسترسی داشته باشند، محدود می‌کند. برای مثال، بهره‌بردارهای سامانه‌ی اسکادا به احتمال زیاد نیاز ندارند به اکثر فایل‌های مدیریتی[۴] یا به بخش حسابداری دسترسی داشته باشند. مجوزهایی مبتنی بر سطح دسترسی هر کارکرد شغلی که نیاز به انجام وظایف خود دارد، صادر کنید. با بخش منابع انسانی جهت پیاده‌سازی رویه‌های اجرایی اصولی جهت حذف دسترسی‌های شبکه متعلق به کارکنان و پیمانکاران اسبق همکاری کنید. اعمال کنترل شدید دسترسی مبتنی بر نقش، امکان ممیزی بهتر را ممکن می‌سازد و خطرات را با کاهش امتیازبخشی و ویژه‌سازی و استثنا قایل‌شدن برای گروه خاصی، به حداقل می‌رساند.

بکار بستن یک قابلیت رویدادنگاری به شما امکان می‌دهد تا فعالیت سامانه را بپایید. این امر شما را توانمند می‌سازد تا منابعی از مواردی را در سامانه بیابید که ممکن است مربوط به فعالیت‌های یک کارمند یا یک بیگانه باشد. در ضمن، پایش تردد شبکه به سازمان شما کمک می‌کند تا ارزیابی کنید که آیا یک کاربر، فعالیت‌های غیرمجاز انجام می‌دهد یا این که یک بیگانه در سامانه رخنه کرده است؛ به‌گونه‌ای‌که فرصت‌هایی جهت ورود به موقع، پیش از بروز مشکلات برای شما و سازمان شما فراهم آورد[۵].

۷. گذرواژه‌های قدرتمندی را الزام کنید و امنیت گذرواژه را نیز به آن اضافه کنید

گذرواژه‌های بلندمدت‌تر و قدرتمندتر را اجباری کنید و احراز هویت چندعاملی را نیز به کار بندید

استفاده از گذرواژه‌های قوی را جهت حفظ امنیت سامانه‌ها و اطلاعات خود الزام کنید. کاربرها را وادار کنید تا برای حساب‌های کاربری مختلف، گذرواژه‌های متفاوتی ایجاد کنند. نفوذگرها و دزدان سایبری می‌توانند نرم‌افزارهای پیش‌ساخته‌ی حاضر و آماده‌ای را به‌کار گیرند تا میلیون‌ها ترکیب حروف و اعداد و علائم را جهت اقدام به ورود غیرمجاز که به آن «حمله‌ی جست‌وجوی فراگیر[۶]» می‌گویند، با روش آزمون و خطای روشمند امتحان کنند. گذرواژه ها باید دستکم ۸ کاراکتر (رقم) داشته باشند، اما گذرواژه‌های طولانی‌تر به خاطر تعداد

4. Administration

۵. برای جزییات بیشتر به منبع زیر مراجعه نمایید:
https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B

6. Brute Force Attack

ارقام بیشتر برای حدس و گمان‌زدن، قوی‌تر هستند. از کاربرها بخواهید تا حروف بزرگ و کوچک، اعداد و رقم‌های ویژه از جمله علائم را نیز در آن بگنجانند.

هنگامی‌که نرم‌افزار جدیدی نصب می‌شود، به‌ویژه برای حساب‌های کاربری متصدی (با اختیار تام) و ادوات سامانه‌ی کنترل و پس از آن به‌طور مرتب، گذرواژه‌های پیش‌فرض را تغییر دهید. جوانب امنیتی گذرواژه را از جمله قفل‌شدن حساب که درصورت تکرار بیش از حد گذرواژه‌های اشتباه فعال می‌شود، اضافه کنید. گزینه‌ی «احراز هویت چندعاملی[7]» را در نظر بگیرید، به گونه‌ای که کاربرها وادار شوند تا هویت‌شان را در هر اقدام به ورود، مورد راستی‌آزمایی قرار دهند. کاربرها رمزی را روی ابزار شخصی خود (مثلاً گوشی همراه هوشمند) دریافت می‌کنند که شماره‌ی آن را قبلاً به سامانه داده باشند؛ سازوکار آن به گونه‌ای پیش‌بینی شده است که تا رمز ارسالی را وارد نکنند، قادر به ورود نخواهند شد[8].

۸. خط‌مشی‌هایی را روی ادوات همراه ایجاد کنید و آن‌ها را الزام نمایید

خاطر آسوده دارید که ادوات همراه در محل کار شما به سادگی نتواند در معرض فعالیت‌های خرابکارانه قرار گیرد.

رواج لپ‌تاپ، تبلت، گوشی‌های همراه هوشمند و سایر ادوات همراه در محل کار، چالش‌های شدید امنیتی را پیش می‌کشد. ادوات همراه امکان قرار گرفتن در معرض نرم‌افزارها و شبکه‌های نفوذی و خراب‌کارها را فراهم می‌آورد. این بحث همان معضل فرهنگی تازه‌ای است که در محیط‌های کاری رواج یافته است، یعنی اصطلاح «ابزار خود را بیاورید[9]» به عنوان یک پدیده‌ی مصرف‌گرایی و خودابزاری از دیدگاه جامعه‌شناختی.

حائز اهمیت است که سیاست‌ها و خط‌مشی‌هایی را درمورد بکارگیری وسایل شخصی در دفتر کار خود و روی شبکه‌های‌تان بسط دهید. این تمهیدات باید به‌شدت برای تمامی کارکنان و پیمانکاران اعمال گردد. ادوات می‌باید با گذرواژه محافظت شوند تا اطمینان خاطر حاصل شود که تنها کاربرهای مجاز می‌توانند وارد سامانه شوند. این امر از دسترسی کاربران غیرمجاز به شبکه‌ها و پرونده‌های محدودشده حتی با استفاده از دستگاه یک کاربر دیگر، اما مجاز، جلوگیری به‌عمل می‌آورد. کاربرها باید درباره‌ی استفاده از ادواتی که به آن‌ها تعلق ندارد، اجتناب کنند و یا جوانب احتیاط را در نظر بگیرند، چراکه ممکن است آن ادوات به‌درستی محافظت نشده باشند یا با خط‌مشی پیاده‌شده‌ی سازمان سازگار نباشند. این ادوات حتی ممکن است آلوده شده باشند و استفاده از آن‌ها ممکن است اطلاعات و شبکه‌های سازمان شما را در معرض خطر قرار دهند[10].

گوش به زنگ باشید

بهترین اقدامات جهت کمک به حفظ ادوات به منظور کار کردن در اوج ایمنی و آرامش

۹. اطلاع‌رسانی از آسیب‌پذیری‌ها را حفظ کنید و تکه‌نویسی (پچ) و به‌روزنویسی را پیاده کنید

یک سامانه‌ی پایش بنا کنید تا مطمئن شوید که همیشه آخرین پچ‌ها و به‌روزنویسی‌ها به‌کار گرفته‌اید

بیشتر سازندگان و تأمین‌کنندگان سرسختانه کار می‌کنند تا تکه‌نویسی‌هایی را جهت آخرین آسیب‌پذیری‌های شناسایی شده تولید کنند. حتی پس از این که تکه‌نویسی‌ها و به‌روزنویسی‌ها به بازار عرضه شد، بسیاری از سامانه‌ها رخنه‌پذیر باقی می‌مانند، چراکه سازمان‌ها یا از آن بی‌خبرند یا نمی‌خواهند از تکه‌نویسی‌ها و به‌روزنویسی‌ها که نقش چفت‌وبَست را بازی می‌کنند، استفاده کنند.

در ضمن، تکه‌نویسی مؤثر می‌تواند جلوی تعداد زیادی از حملات را بگیرد؛ با در نظر گرفتن این‌که ۱۰ رخنه‌ی اول سایبری برای ۸۵ درصد از ترافیک‌های نفوذیافته، ناشی از عدم به‌روزرسانی و به‌هنگام‌سازی اعلام شده است.

در گزارش پژوهش‌های داده‌دزدی[11] مربوط به سال ۲۰۱۶، وریزون[12] دریافت که در اکثر صنایع، ۷۵ درصد حوادث و شکاف‌های داده‌دزدی توسط تنها سه نمونه انجام شده است. برای نرم‌افزارهای کاربردی، این سه نمونه جاسوسی به ترتیب سایبری، جرم‌افزار[13] و منع خدمات (ازکاراندازی)[14] هستند.

وریزون توصیه کرد که درک اجزای سازنده‌ی یک حمله (مثلاً زنجیره را بشکن[15]) می‌تواند سازمان‌ها را یاری کند تا سپرهای دفاعی بنا کنند و هرگونه رخنه‌ای را ردیابی نمایند.

جهت حفاظت از سازمان‌تان در برابر این حملات فرصت‌طلبانه، ساختاری از پایش و اعمال تکه‌نویسی‌ها و به‌روزنویسی‌های سامانه پی‌ریزی کنید. به‌روزنویسی‌ها طراحی شده‌اند تا نقاط ضربه‌پذیر و شکننده‌ی شناخته‌شده را بپوشانند؛ بنابراین قویاً برای هرگونه ادوات متصل به اینترنت تجویز می‌شوند[16].

۱۰. تدابیری را برای نقاط ضعف و نفوذپذیر قابل تشخیص تدارک ببنید و پیاده نمایید

ثبت وقایع از دیواره‌های آتش، کشف نفوذ و حسگرهای پیش‌گیری و کارگزارها یا خدمات‌رسان‌های شبکه[17] را برای هرگونه نفوذی رصد کنید

برخلاف این‌که بسیاری از تمهیدات بازدارنده و پیشگیرانه توسط سازمان‌ها اعمال می‌شود، هنوز بسیاری از آن‌ها با نقاط ضعف‌هایی دست‌وپنجه نرم می‌کنند. در واقع، بسیاری از خبره‌های امنیت سایبری اشاره داشته‌اند که مواجهه با یک حفره در واقع سخن از «اگر» نیست، بلکه بیشتر سخن از «چه‌هنگام»

7. Multi-factor Authentication
۸. برای جزییات بیشتر به منبع زیر مراجعه نمایید:
https://www.us-cert.gov/ncas/tips/ST04-002
9. Multi-factor Authentication

۱۰. برای جزییات بیشتر به منبع زیر مراجعه نمایید:
https://www.us-cert.gov/ncas/tips/ST05-017

11. Data Breach
12. Verizon
13. Crimeware
14. DoS: Denial of Service
15. Kill Chain
۱۶. برای جزییات بیشتر به منبع زیر مراجعه نمایید:
https://www.waterisac.org/system/files/2002__Library/Patch%20Management%20Recommended%20Practice.pdf
17. Server

است. هنگامی‌که شکافی در معرض قرار می‌گیرد، سازمان‌هایی که دست به اقدام می‌زنند، آن‌هایی هستند که به‌سرعت موضوع را شناسایی می‌کنند و طرحی به‌جا جهت پاسخگویی در آستین خود از پیش پرورانده‌اند. تدارک ابزارها و امکاناتی نظیر سامانه‌های تشخیص نفوذ[18] (IDS) و سامانه‌های بازدارنده‌ی نفوذ[19] (IPS)، نرم‌افزار ضدویروس و رویدادنگاری‌ها می‌توانند کمک نمایند تا منافذ در اولین مراحل‌شان کشف شوند. اکثر IDSها و IPSها امضاهایی را (به عنوان الگوهای رفتاری شناخته‌شده) جهت ردیابی درگاه‌خوانی[20] (بخشی از عمل نفوذ در لایه‌ی TCP[21])، بدافزار و سایر ارتباطات غیرطبیعی شبکه به‌کار می‌برند. ویروس‌های جدید روزانه کشف می‌شوند و برنامه‌های ضدویروس همواره طوری بازنویسی می‌شوند تا آخرین امضاهای تهدید را به‌طور خودکار دربرگیرند. با این حال، شما نمی‌باید تنها روی نرم‌افزار ضدویروس برای شناسایی آلودگی‌ها حساب کنید. شما باید رویدادنگاری‌ها از دیواره‌های آتش، کشف نفوذ و حسگرهای بازدارنده‌ی نفوذ و کارگزارها (سرورها) را برای مشاهده‌ی علائم آلودگی‌های احتمالی، مورد سرکشی و وارسی مدون و منظم قرار دهید[22].

۱۱. یک طرح واکنش حوادث امنیت سایبری تهیه کنید

طرح واکنش حوادث شما باید از مشارکت میان همه‌ی سهامداران و ذی‌نفعان که بالقوه از یک حادثه‌ی امنیت سایبری متحمل خسارات می‌شوند، حاصل شده باشد

طرح‌های اقدام در برابر حوادث، یک بخش حیاتی از کسب آمادگی و ایجاد مقاومت به شکل یک اقدام اضطراری و فوری است. یک طرح اثربخش اقدام حوادث امنیت سایبری، صدمات و لطمات را کاهش خواهد داد، اطمینان خاطر سهامداران و مشتریان را افزایش می‌دهد و زمان و هزینه‌ی بازیابی را به‌حداقل خواهد رساند. طرح شما باید شامل تمهیداتی برای دستیابی به بدافزار ویرانگر در یک محیط ICS باشد. در این شرایط، شما باید جهت جداسازی محیط های ICS خود از طریق قطع ارتباط با شبکه‌های غیر ICS آماده باشید. شما باید قادر باشید که در صورت لزوم به حالت بهره‌برداری دستی تغییر وضعیت دهید. به عنوان نمونه، اگر شرایط شبکه روی پایش و نظارت سامانه‌ی اسکادا تأثیر بگذارد و بهره‌بردار دید خود را از فرآیند از دست دهد، بدافزار قدرت آن را دارد که ادوات کنترلی را از فعالیت طبیعی خودکار خارج کند. این طرح، بیش از آن که توسط یک واحد تکی تدوین شود، باید برآمد و برساختی از مشارکت میان تمامی بخش‌هایی تلقی شود که در یک حادثه‌ی امنیت سایبری سهیم هستند. این امر پاسخی همکارانه و یکدست را تضمین می‌کند که تمامی منابع سازمان شما را تا گسترده‌ترین سطح ممکن ارتقاء می‌دهد.

برای قابلیت پاسخگویی ارتقایافته‌تر در وقوع یک حادثه‌ی امنیت سایبری، شما باید تشکیل یک «تیم پاسخ رویداد امنیت رایانه‌ای[23]» را مد نظر قرار دهید.

این تکلیف تا زمانی که طرح نوشته نشود، ادا نشده است. بسیار حیاتی‌ست که طرح‌ها روال‌مندانه بازبینی و به‌روز شوند تا این اطمینان را بدهند که در صورت نیاز شکل نهایی مناسبی به خود گرفته‌اند. جهت درک حقیقی از طرح پاسخ رخداد امنیت سایبری، سازمان شما باید تمرینات منظم و مدونی را انجام دهد. این امر تضمین می‌کند که کلیه‌ی افراد درگیر، رویه‌هایی را در صورت وقوع یک خرابکاری جدی یا داده‌دزدی اساسی با بکارگیری یک پاسخ کارا و اثربخش به‌درستی درک کرده‌اند[24].

18. IDS: Intrusion Detection System
19. IPS: Intrusion Prevention System
20. Port Scanning
21. Transmission Control Protocol
۲۲. برای جزییات بیشتر به منبع زیر مراجعه نمایید:
https://www.cisecurity.org/controls/maintenance-monitoring-and-analysis-of-audit-logs/

23. CSIRT: Computer Security Incident Response Team
۲۴. برای جزییات بیشتر به منبع زیر مراجعه نمایید:
https://ics-cert.us-cert.gov/sites/default/files/FactSheets/ICS-CERT_FactSheet_Cyber_Incident_Analysis_S508C.pdf

۱۲. نسخه‌های جاری انباره‌ی داده را برای بازیابی سریع‌تر داده‌ها پشتیبان‌گیری کنید و بایگانی نمایید

ساده‌ترین راه بازگرداندن و احیاء یک دستگاه آلوده‌شده با بدافزار، بازیابی آن از یک نسخه‌ی ذخیره‌شده‌ی پشتیبان است

نسخه‌های ذخیره [۲۵] مؤثرترین راه یگانه جهت بازیابی از یک حمله‌ی بدافزاری می‌باشد. اطمینان خاطر حاصل کنید که هر سامانه دستِ‌کم به‌صورت هفتگی و حتی شاید هفته‌ای چند بار برای ذخیره‌سازی اطلاعات حساس سامانه پشتیبان‌گیری می‌شوند. جهت توانمندسازی شما برای بازگرداندن سریع یک سامانه با نسخه‌ی پشتیبان، مطمئن شوید که تمامی نرم‌افزارها و داده‌های حیاتی روی هر دستگاه طبق رویه‌ی پشتیبان‌گیری دربرگرفته شده باشند و به همه رسیدگی شده باشد. مطمئن شوید که در طول زمان، پشتیبان‌هایی چندگانه به تعدد گرفته‌اید، طوری‌که در صورت وقوع یک آلودگی بدافزاری شما قادر باشید از نسخه‌ای که پیش از آلودگی اصلی گرفته شده است، عمل بازگردانی را انجام دهید؛ نه از یک نسخه‌ی آلوده.

تأیید و تصدیق نمایید که خط‌مشی‌ها و سیاست‌های پشتیبان‌گیری شما با آیین‌نامه‌ها و مقررات و ملزومات اداری سازمان شما سازگار و منطبق هستند[۲۶].

25. Backup

۲۶. برای جزییات بیشتر به منبع زیر مراجعه نمایید:
https://www.cisecurity.org/controls/data-recovery-capability/

مراجع

منبع اصلی:
Schneider Electric Whitepaper Document B0852AB_A: “Cybersecurity Best Practices”

مراجع انگلیسی منبع اصلی:
Booz Allen Hamilton Industrial Cybersecurity Threat Briefing for 2016
https://www.slideshare.net/BoozAllen/booz-allen-industrial-cybersecurity-threat-briefing
Center for Internet Security (CIS) Top 20 Critical Security Controls
https://www.cisecurity.org/cybersecurity-best-practices/
FBI Cyber Crime
https://www.fbi.gov/investigate/cyber
Guide to Industrial Control Systems (ICS) Security
https://www.nist.gov/publications/guide-industrial-control-systems-ics-security
Industrial Control Systems Cyber Emergency Response Team
https://ics-cert.us-cert.gov/
The State of Malware Detection and Prevention
http://go.cyphort.com/Ponemon-Report-Page.html
Virtual Private Networking: An Overview
https://msdn.microsoft.com/en-us/library/bb742566.aspx
WaterISAC Water Security Network
https://www.waterisac.org