وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

مرکز ماهر

گزارش آسیب پذیری روز صفر CVE-۲۰۲۰-۷۴۸۹ مشابه استاکس نت

اردیبهشت ماه ۱۳۹۹

مقدمه

امروزه سیستم های کنترل نظارتی و اکتساب داده، SCADA[1] تلقی می گردند. سیستم های اسکادا به منزله مغز کنترل و مانیتورینگ زیرساخت های حیاتی نظیر شبکه های انتقال و توزیع برق، پالایشگاه ها، شبکه های انتقال آب، کنترل ترافیک و ... می باشند. با توجه به نقش برجسته سیستم های اسکادا در کنترل و مانیتورینگ زیرساخت های حیاتی و صنایع مهم یک کشور، پرداختن به ایمن سازی آنها به یک اولویت ملی مهم تبدیل شده است چراکه :

سیستم های اسکادا با هدف حداکثر بازدهی و کارآیی مطلوب طراحی شده اند و به امنیت آنها توجه جدی نشده است، این درحالی است که نیاز اساسی امروز با توجه به واقعیت های موجود و افزایش آمار حملات و سو استفاده های اخیر در این سیستم ها می باشد.

در اغلب سیستم های اسکادا، به محیط عملیاتی بطور کامل اعتماد می شود و با فرض وجود یک محیط ایمن، فعالیت ها انجام می شود. ارتباط تنگاتنگ این سیستم ها با سایر سیستم های موجود در یک سازمان، ضرورت توجه به امنیت آنها را مضاعف کرده است.

امنیت سیستم های اسکادا مدتی است که نگرانی فزاینده ای داشته است. این فناوری برخی از اساسی ترین خدمات همچون نیروگاه های هسته ای و شبکه های برقی را کنترل می کند. در حالی که بسیاری از این پیاده سازی ها با پیچیدگی های منحصر به فرد محافظت می شوند ، مانیتورینگ شبانه روزی، آسیب پذیری ها و حملات مورد نظر آنها را نباید از نظر دور داشت.

شرح آسیب پذیری

محققان آسیب پذیری دیگری را در نرم افزار ساخته شده توسط اشنایدر الکتریک مشاهده کرده اند که شبیه به مورد سوء استفاده از بدافزار استاکس نت است.

استاکس نت، بدافزاری که یک دهه پیش توسط ایالات متحده و اسرائیل برای آسیب رساندن به برنامه هسته ای ایران بهکار رفته بود. این بدافزار برای هدف قرار دادن کنترلرهای منطقی قابل برنامه ریزی (PLCs) زیمنس (SIMATIC S۷-۳۰۰ و S۷-۴۰۰) طراحی شده بود. یکی از روشهای مورد استفاده ، تزریق DLL برای جایگزینی DLL است که توسط نرم افزار SCADA استفاده شده است بنابراین این بد افزار با جایگزین کردن فایل DLL مرتبط با نرم افزار برنامه نویسی کنترلر زیمنس STEP۷، با کد مخرب روی PLC ها قرار گرفت. با انجام این کار ، به مهاجمان اجازه می دهد تا هر دو روش کنترل و نظارت را رهگیری و دستکاری کند و سانتریفیوژها را مجبور کند صدمه ببینند که توسط اپراتور به آنها آسیب نرساند.

[1] Supervisory Control And Data Acquisition

در ماه مارس، Airbus Cybersecurance گزارش داد که آسیب پذیری مشابهی را در نرم افزار مهندسی EcoStruxure Control EneStruxure Control Schneider Electric، که قبلاً با عنوان Unity Pro شناخته می شد، شناسایی کرده است. این نقص که با عنوان CVE-۲۰۲۰-۷۴۷۵ ردیابی می شود، می تواند یکی از فایل های DLL مرتبط با نرم افزار مهندسی در Modicon M۳۴۰ و M۵۸۰ PLC را با کد مخرب مورد نظر مهاجم را جایگزین نماید و مورد سوء استفاده قرار دهد، که می تواند منجر به اختلال در روند و سایر آسیب ها شود.

محققان موسسه امنیت سایبری Trustwave روز پنجشنبه گزارش دادند که آنها نیز آسیب پذیری مشابهی را در نرم افزار اشنایدر، بخصوص(EcoStruxure Machine Expertقبلاً با نام SoMachine شناخته می شد) شناسایی کرده اند که به کاربران امکان می دهد پروژه هایی مشابه با Stuxnet را در مورد کنترلرهای Modicon M۲۲۱ توسعه دهند.

SoMachine Basic یک نرم افزار رایگان است که توسط Schneider Electric برای برنامه ریزی و کنترل کننده منطق قابل برنامه ریزی (PLC) M۲۲۱ تهیه شده است. تحقیقات نشان می دهد که SoMachine Basic در مقادیر حساس مورد استفاده در ارتباطات با PLC بررسی های کافی را انجام نمی دهد. از آسیب پذیری بالقوه می توان برای ارسال بسته های دستکاری شده به PLC استفاده کرد ، بدون آنکه نرم افزار از این دستکاری آگاه باشد

اشنایدر وصله هایی را برای هر دو آسیب پذیری منتشر کرده است، اما در مشاوره برای اولین حفره امنیتی خاطرنشان کرده است که محصولات سایر فروشندگان نیز می توانند در برابر این نوع حملات آسیب پذیر باشند.

کارل سیگلر، مدیر ارشد تحقیقات امنیتی در SpiderLabs Trustwave ، به SecurityWeek گفت که بهره برداری از CVE-۲۰۲۰-۷۴۸۹ نیاز به دسترسی به محیط میزبان نرم افزار SoMachine و PLC هدف دارد.

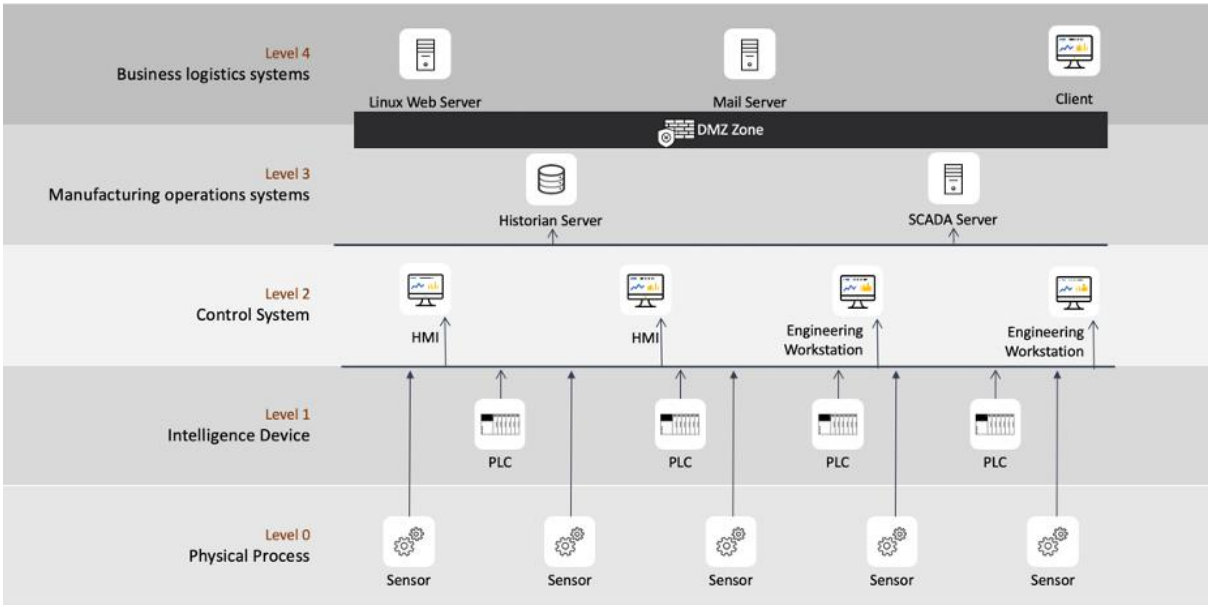
برای آسیب پذیری تزریقDLL (CVE-۲۰۲۰-۷۴۸۹) در نرم افزار SoMachine حمله کننده باید تزریق را با استفاده از کاربر محلی مجاز به اجرای نرم افزار انجام دهد و لزومی به دسترسی ادمین ندارد مگر اینکه در تنظیمات اجرای اینگونه پیکره بندی فقط در اختیار ادمین باشد که عموما این اتفاق نمی افتد و ما در استاکس نت دیده ایم که لزوماً مانعی برای بهره برداری نیست.

محققان Trustwave همچنین کشف جالبی را در رابطه با آسیب پذیری قدیمی مؤثر بر نرم افزار اشنایدر الکتریک انجام دادند. در سال ۲۰۱۷، آسیب پذیری CVE-۲۰۱۷-۶۰۳۴ گزارش شد.

در این آسیب پذیری هکرها قادر به شنود ، دستکاری و انتقال مجدد دستورات کنترلی بین نرم افزار مهندسی و PLC می باشد. تأثیر این حمله بدین گونه است که یک مهاجم مخرب قادر است PLC را از راه دور بدون احراز هویت با نرم افزار مهندسی شروع و متوقف کند. این مهاجم مخرب همچنین می تواند منطق منطق برنامه نویسی در PLC را بدون احراز هویت تغییر دهد. جزئیات این آسیب پذیری با مشخصه CVE-۲۰۱۷-۶۰۳۴ اطلاع رسانی شد.

جزییات آزمون نفوذپذیری

جهت آشنایی خواننده با ویژگی های اجزای موجود در شبکه سیستم های کنترل صنعتی، شکل یک شماتیک کلی را نشان می دهد. در سطح ۰ ، یک شبکه ICS دارای حسگرها و محرک هایی است که با فرآیندهای فیزیکی شبکه در تعامل هستند. به طور معمول به PLC ها در سطح ۱ یک واقع شده اند و برای دریافت و ارسال دستورات به سطح ۰. استفاده می شود. یک PLC معمولاً با چندین دستگاه سطح ۰ می تواند ارتباط داشته باشد. معمولاً یک نرم افزار مهندسی برای برنامه ریزی و کنترل PLC نصب می شود. نرم افزار مهندسی، منطق کنترل PLC ها را طراحی و تنظیم می کند. از دستگاهی که میزبان نرم افزار مهندسی است معمولاً به عنوان ایستگاه کاری مهندسی یاد می شود. در این گزارش ، نرم افزار مهندسی SoMachine Basic v۱,۶ است و PLC که با آن ارتباط برقرار می کند Schneider Electric M۲۲۱ است.



شکل ۱: شماتیک کلی سیستم های اسکادا

اجزای صنعتی در شبکه های ICS از پروتکل های ICS برای برقراری ارتباط با یکدیگر استفاده می کنند. پروتکل های ICS ممکن است اختصاصی برای فروشندگان باشد. در محیط این تحقیق ، SoMachine با استفاده از Modbus TCP / IP با PLC ارتباط برقرار می کند.

پروتکل Modbus

پروتکل Modbus یک پروتکل ارتباطی است که در ابتدا در سال ۱۹۷۹ توسط شرکت Modicon عرضه شد. البته بعدها شرکت اشنایدر الکتریک اقدام به خریداری این شرکت نمود. کاربرد اولیه این پروتکل استفاده در PLCها بود اما به¬تدریج به¬عنوان یک استاندارد ارتباطی پذیرفته شد و بسیاری از

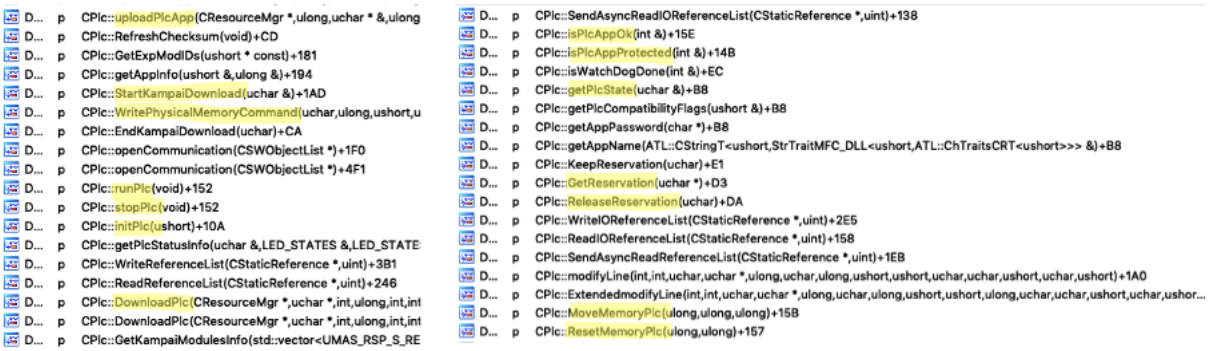
سازندگان تجهیزات اتوماسیون آن را پشتیبانی کردند. بدین ترتیب محصولات سازندگان مختلف به سهولت توسط این پروتکل با یکدیگر ارتباط برقرار کردند.

علل اصلی استفاده از پروتکل Modbus در شبکه¬های صنعتی عبارت‌اند از:

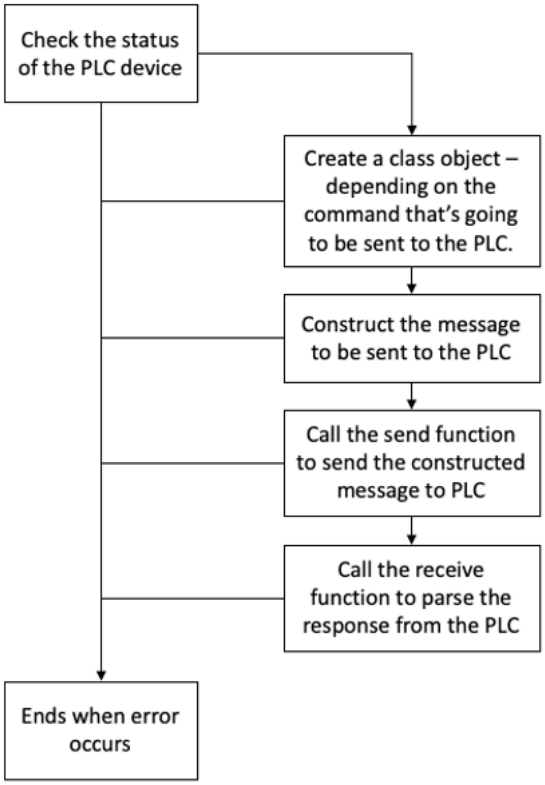
- با توجه به برنامه¬های کاربردی صنعتی توسعه‌یافته است.
- به‌صورت باز منتشر می¬شود و حق امتیاز خاصی ندارد.
- استقرار و نگهداری آسانی دارد.
- بیت¬ها یا کلمات در آن به‌صورت خام و بدون قرار دادن محدودیت¬ها¬یی از سوی فروشندگان منتقل می-شوند.

پروتکل Modbus بین تجهیزات مختلفی که در یک شبکه به هم متصل هستند ارتباط برقرار می¬کند. برای مثال سیستمی که درجه حرارت و رطوبت را اندازه¬گیری می¬کند و نتایج را برای کامپیوتر که جزء دیگری از شبکه است ارسال می¬کند. Modbus اغلب برای اتصال یک کامپیوتر نظارت با یک واحد ترمینال ازراه¬دور ((RTUدر اسکادا استفاده می¬شود.

در گزارش محققان Trustwave ، نحوه تجزیه و تحلیل از آسیب پذیری در مورد نحوه بارگذاری مقادیر و متغیرها در DLL، SoMachine Basic برای ایجاد بسته هایی که با PLC ارتباط برقرار می کنند ، توصیف شده است. این آسیب پذیری به طور بالقوه می تواند برای ارسال مداوم بسته های دستکاری شده و باعث از دست رفتن مانیتورینگ و کنترل PLC می شود. آنها دو DLL که توسط SoMachine Basic برای ساخت بسته های شبکه استفاده می شد شناسایی کرده و هر دو در IDA Pro بارگذاری کرده اند تا تمام عملکردهایی که دستورات کنترلی به PLC ارسال می شود شناسایی گردیده است. شکل ۲ برخی از توابع را برجسته می کند.

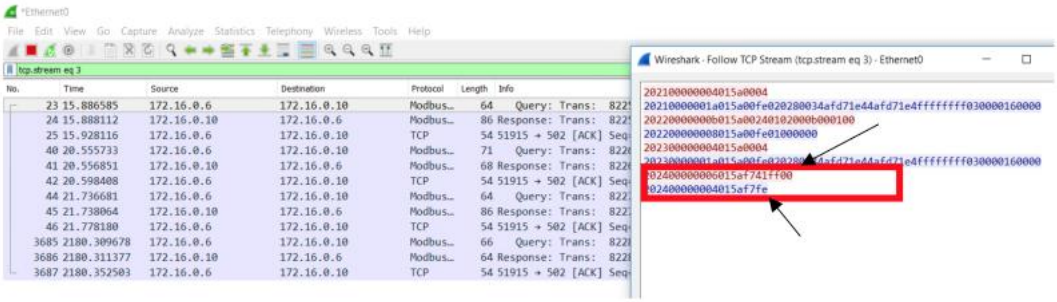


شکل ۲: استخراج دو DLL که دستورات کنترلی ارسال می کنند



شکل ۳: نحوه آنالیز توابع در DLL

محققان Trustwave پس ازمشاهده و کنترل بین توابع متوجه شدند که مقادیر کدگذاری شده هرگز بررسی و تأیید نشده اند. این یک مهاجم را قادر می سازد تا DLL را اصلاح کند ، مقادیر را تغییر داده و رفتارهای مورد نظر بسته ها را تغییر دهد. به عنوان نمونه در شکل زیر مهاجم مقادیر را در DLL تغییر داده و به PLC ارسال کرده است.



شکل۴: نحوه تغییر مقادیر توسط مهاجم در DLL

توصیه ها

معماری امنیتی سامانه‌های کنترل صنعتی

هنگام طراحی یک شبکه برای گسترش یک سامانه کنترل صنعتی عموما تفکیک کامل شبکه کنترل صنعتی از شبکه شرکتی IT توصیه می‌شود. طبیعت ترافیک این دو شبکه با یکدیگر کاملا متفاوت است: دسترسی

به اینترنت، پست الکترونیک و دسترسی از راه دور عموما در شبکه شرکتی مجاز شمرده است اما در شبکه صنعتی لزوما مجاز نمی‌باشند. ملاحظات عملی مانند هزینه راه‌اندازی سامانه‌های کنترل صنعتی و نگهداری یک زیرساخت شبکه همگن الزام کننده وجود ارتباط میان این دو شبکه است. این ارتباط یک ریسک امنیتی مهم بوده و بایستی توسط تجهیزات حافظت مرزی، تحت حفاظت قرار گیرد. چنانچه لازم است اتصالی میان دو شبکه وجود داشته باشد، توصیه می‌شود که این اتصال به‌صورت حداقلی بوده و از طریق تجهیزات دیواره آتش و DMZ صورت گیرد.

به طور کلی مراحل زیر وجود دارد:

- تجزیه و تفکیک شبکه
- محافظت مرزی[۲]
- دیواره‌های آتش
- شبکه کنترلی تفکیک‌شده منطقی
- جداسازی شبکه
- معماری دفاع در عمق توصیه‌شده
- سیاست‌های عمومی دیوار آتش برای سامانه‌های کنترل صنعتی
- قوانین توصیه‌شده دیواره آتش برای سرویس‌های خاص
- مسائل مختص دیواره آتش سامانه‌های کنترل صنعتی
- نقاط خرابی تکی
- افزونگی و تحمل‌پذیری خطا
- جلوگیری از حملات مرد میانی
- احراز هویت و صدور مجوز
- پایش، ثبت وقایع و ممیزی
- کشف حادثه، پاسخ و بازیابی سیستم

در ادامه و در بخش های مختلف تمامی مراحل شرح داده شده است.

تجزیه و تفکیک شبکه

لازم است تحلیل ریسک عملیاتی جهت تشخیص بخش‌های بحرانی هر شبکه سامانه کنترل صنعتی انجام شود تا به تشخیص اینکه چه بخش‌هایی از سامانه کنترل صنعتی نیازمند تفکیک است کمک کنند. تفکیک شبکه به‌معنای ناحیه‌بندی شبکه به شبکه‌های کوچکتر است. جداسازی[۳] و تفکیک[۴] (ناحیه‌بندی) شبکه از مؤثرترین مفاهیم معماری است که یک سازمان می‌تواند برای حفاظت از سامانه کنترل صنعتی خود به کار

[۲] Boundary Protection
[۳] Segregation
[۴] Segmentation

بگیرند. هدف تفکیک و جداسازی شبکه کاهش دسترسی به اطلاعات حساس برای سامانه‌ها و افرادی است که احتیاجی به این اطلاعات ندارند. محیط‌های کنترل صنعتی اغلب دارای چندین ناحیه و دامنه به خوبی تعریف شده نظیر شبکه محلی عملیاتی[۵]، شبکه محلی کنترل[۶] و ناحیه DMZ عملیاتی است و همچنین دارای دروازه‌هایی به شبکه‌های غیر سامانه کنترل صنعتی با دامنه‌های با اطمینان کم‌تر نظیر اینترنت و شبکه محلی خصوصی است.

برخی از فناوری ها و روش های تفکیک شبکه عبارت اند از:

- تفکیک شبکه از طریق اعمال رمزنگاری و یا اعمال بخش‌بندی حاصل از تجهیزات
- تفکیک فیزیکی شبکه به‌منظور ممانعت کامل از هرگونه تبادل ترافیک بین دامنه‌ها
- اعمال فیلترینگ ترافیک در لایه‌های شبکه‌ای متنوع با استفاده از فناوری‌های متنوع برای اعمال نیازمندی‌های امنیتی و محدوده‌ها

صرف نظر از فناوری انتخابی برای تفیک و جداسازی شبکه، چهار رویکرد متداول جهت پیاده‌سازی مفهوم دفاع در عمق جهت ارائه تفکیک و جداسازی مناسب شبکه در زیر آمده است:

- بکار بردن فناوری‌ها در لایه‌های متفاوت علاوه بر لایه شبکه
- استفاده از اصول حداقل دسترسی سطح بالا و نیاز به دانستن[۷]
- اطلاعات و زیرساخت[۸] مختلف بر اساس نیازمندی‌های امنیتی
- به‌کارگیری لیست سفید به جای لیست سیاه
- بهبود تحلیل فایل های log

جداسازی شبکه

برای افزایش امنیت می‌توان دو شبکه سامانه‌های کنترل صنعتی و شبکه خصوصی را بر اساس معماری‌های گوناگون از هم جدا نمود. در زیر معماری هایی برای این منظور ارائه شده است که بیشتر چگونگی قرار گیری دیوار آتش برای جداسازی دو شبکه نمایش می دهد.

- رایانه دو میزبانه[۹] یا کارت‌های واسطه شبکه دو میزبان
- دیواره آتش بین دو شبکه خصوصی و شبکه کنترل
- دیواره‌آتش و مسیریاب بین شبکه خصوصی و شبکه کنترل
- دیوار آتش با تعریف ناحیه DMZ بین شبکه خصوصی و شبکه کنترل
- دو دیواره آتش بین شبکه شرکتی و شبکه کنترل

---

[۵] Operational LAN
[۶] Control LAN
[۷] Need to know
[۸] Infrastructure
[۹] Dual Homed

امن‌ترین، قابل مدیریت‌ترین و مقیاس‌پذیرترین معماری جداسازی دو شبکه کنترل صنعتی و شبکه شرکتی بر اساس معماری با حداقل سه ناحیه و استفاده از حداقل یک ناحیه DMZ می باشد.

معماری دفاع در عمق توصیه شده

یک محصول، فناوری و یا راهکار امنیتی به‌تنهایی توانایی حفاظت از سامانه‌های کنترل صنعتی را ندارد. روش دفاع در عمق یک استراتژی چندلایه‌ای شامل دو یا چند ساز و کار امنیتی همپوشانی شده است. معماری دفاع در عمق شامل استفاده از دیوارهای آتش، ایجاد نواحی DMZ، قابلیت‌های تشخیص نفوذ، به همراه سیاست‌های امنیتی، برنامه‌های آموزشی، ساز و کارهای مدیریت بحران و امنیت فیزیکی بهینه می‌باشد.

مسائل مختص دیواره آتش سامانه‌های کنترل صنعتی

علاوه بر مسائل مربوط به دیواره‌های آتش و سامانه‌های کنترل صنعتی که تاکنون مورد بحث قرار گرفت، مشکلات دیگری نیز وجود دارد که می‌بایست با دقت بررسی شوند. یکی از حوزه های اصلی نگرانی استقرار تاریخ‌نگار داده می‌باشد.

تاریخ‌نگار داده

در سیستم‌های سه ناحیه‌ای، قرار دادن این سرویس‌دهنده‌ها در ناحیه DMZ رایج می‌باشد، اما در طراحی‌های دو ناحیه‌ای مشکل پیچیده‌تر خواهد شد. قرار دادن ناحیه تاریخ‌نگار در بخش خصوصی دیوار آتش، به‌معنای آن است که پروتکل‌های ناامنی مانند Modbus/TCP و یا DCOM از سوی دیواره آتش مجاز شناخته شده و گزارش تمامی تجهیزات کنترلی به تاریخ‌نگار در شبکه شرکتی نیز نمایش داده می‌شود. از سوی دیگر، قرار دادن تاریخ‌نگار در شبکه کنترل به‌معنای مجاز دانستن پروتکل‌های پرسش برانگیز دیگری مانند HTTP یا SQL از سوی دیواره آتش می‌باشد، درنتیجه سرویس‌دهنده توسط تمامی واحدهای شبکه کنترل قابل دسترسی می‌باشد.

در حالت کلی، بهترین راه‌حل اجتناب از سیستم‌های دو ناحیه‌ای (بدون DMZ) و استفاده از طراحی سه ناحیه‌ای می‌باشد تا به این ترتیب جمع‌کننده داده در شبکه کنترلی و تاریخ‌نگار در DMZ قرار داده شود.

تمام اتصالات به شبکه های SCADA شناسایی شوند.

انواع اتصالات زیر باید شناسایی و ارزیابی شوند:

- شبکه های محلی داخلی و گسترده، از جمله شبکه های تجاری
- اینترنت
- دستگاه های شبکه بی‌سیم، از جمله پیوندهای ماهواره‌ای[۱۰]
- اتصالات مودم یا dial-up

[۱۰] satellite uplinks

- اتصالات شرکای تجاری، فروشندگان یا آژانس های نظارتی

اتصالات غیرضروری به شبکه SCADA قطع شوند.

برای اطمینان بیشتر امنیت سیستم های SCADA، باید شبکه SCADA تا حد ممکن از سایر اتصالات شبکه جدا باشد. هرگونه اتصال به شبکه دیگر، خطرات امنیتی را افزایش می دهد، به ویژه اگر اتصال در بستر اینترنت باشد. جداسازی شبکه SCADA یک هدف اصلی برای تامین حفاظت مورد نیاز می باشد. از استراتژی هایی مانند DMZs[۱۱] استفاده کرد.

امن کردن شبکه های SCADA با حذف یا غیرفعال کردن سرویس های غیر ضروری

سرورهای کنترل SCADA که بر روی سیستم عامل هاس متن باز[۱۲] ساخته شده اند، از طریق خدمات شبکه پیش فرض، می توانند در معرض حمله قرار گیرند. در حد امکان، سرویس های بدون استفاده و دیمن های[۱۳] شبکه را حذف یا غیرفعال کنید تا خطر حمله مستقیم کاهش یابد. سرویس یا ویژگی را در یک شبکه SCADA مجاز نکنید، مگر اینکه ارزیابی دقیق ریسک از عواقب آن نشان دهد که مزایای استفاده از آن سرویس یا ویژگی به مراتب بالاتر از پتانسیل سوءاستفاده از آسیب پذیری آن باشد.

ایجاد یک استراتژی حفاظت از شبکه را براساس اصل دفاع در عمیق

یک اصل اساسی که باید جزئی از هر استراتژی حافظت از شبکه باشد، دفاع در عمق[۱۴] است. دفاع در عمق باید در مرحله طراحی فرآیند توسعه در نظر گرفته شود و باید در تمام تصمیم گیری های فنی مرتبط با شبکه مورد توجه قرار گیرد. از کنترلهای فنی و مدیریتی برای کاهش تهدیدات ناشی از خطرات شناسایی شده تا حد امکان در کلیه سطوح شبکه استفاده شود. علاوه بر این، هر لایه باید در برابر سایر سیستم ها در همان لایه، محافظت شوند. به عنوان مثال، برای محافظت در برابر تهدیدات درون سازمانی، کاربران باید به گونه ای محدود شوند که فقط به آن دسته از منابعی دسترسی داشته باشند که فقط برای انجام وظایف خود به آن ها نیاز دارند.

ایجاد فرآیندهای مدیریت پیکربندی مؤثر

یک فرآیند مدیریتی اساسی برای حفظ یک شبکه امن، مدیریت پیکربندی[۱۵] است. مدیریت پیکربندی نیاز به پوشش هر دو تنظیمات سخت افزار و تنظیمات نرم افزار دارد. تغییر در سخت افزار یا نرم افزار می تواند به راحتی آسیب پذیری هایی را ایجاد کند که امنیت شبکه را تضعیف می کند. فرآیندهایی برای ارزیابی و کنترل هر گونه تغییر، برای آنکه اطمینان حاصل شود که شبکه امن باقی خواهد ماند مورد نیاز است.

---

[۱۱] demilitarized zones
[۱۲] open-source
[۱۳] daemon
[۱۴] defense-in-depth
[۱۵] Configuration management

منبع

https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/۲۱_Steps_-_SCADA.pdf

دسترسی فیزیکی به فیلدباس و دستگاه ها کنترل شود.

دلیل	کنترل نقاط دسترسی فیزیکی می تواند، اجازه ورود به سیستم را دهد.
روش	مشخص شود که چه کسی به دسترسی به دستگاه ها نیاز دارد، چرا و به چه تعداد دفعات. سرورها را در مکان های دسترسی کنترل شده، نصب شوند (درصورت امکان در اتاق های IT). واحدهای مرکزی ایستگاه های کاری، دستگاه های شبکه صنعتی و PLC ها را در قفس های قفل شده قرار داده شوند.
دامنه	ایستگاه های کاری، سرورها، دستگاه ها و دستگاه های شبکه، PLC ها، سنسورها یا محرک ها، صفحه های نمایش لمسی
محدودیت ها	اندازه سیستم - حفاظت کلی سایت مجوز دسترسی را در مواقع اضطراری حفظ شود.
راه های مدیریت محدودیت ها	یک درب "تماس خشک[۱۶]"[۱۷] نصب شود تا هنگام باز شدن زنگ خطر در سیستم SCADA تولید شود.

تفکیک شبکه

دلیل	انتشار حملات و آسیب پذیری ها محدود می شوند.
روش	یک نقشه جریان ایجاد شود. شبکه ها را با استفاده از دستگاه های اختصاصی یا VLAN ها، جدا شوند. فیلتر جریان با استفاده از یک فایروال. ترافیک رد شده، ردیابی و تجزیه و تحلیل شود.
دامنه	شبکه SCADA، شبکه PLC، شبکه توسعه یافته و غیره.
محدودیت ها	محدودیت های زمان واقعی در شبکه های پردازش.
راه های مدیریت محدودیت ها	فیلترگذاری در upstream شبکه انجام شود. دسترسی فیزیکی به شبکه فرایند محدود و کنترل شده است.

مستندسازی

دلیل	مستندات کنترل می شوند تا نمایانگر دقیقی از ICS و جلوگیری از خطاهای عملیاتی باشند. انتشار اطلاعات را کنترل می شود تا فقط افرادی که به اطلاعات نیاز دارند، آن را دریافت کنند.
روش	یک سیاست مدیریت مستندات تعریف شود (فرآیند به روزرسانی، مدت زمان نگهداری، لیست توزیع، ذخیره و غیره). مستندات مربوط به یک سیستم اطلاعاتی نباید در خود سیستم نگه داشته شود.
دامنه	مستندات فنی مربوط به تاسیسات، نمودارهای معماری، موقعیت جغرافیایی، نقشه آدرس دهی، کتابچه راهنمای مدیر، دفترچه نگهداری، آنالیز عملکردی، تجزیه و تحلیل سیستم و غیره.
محدودیت ها	داشتن نسخه های چاپی اسناد و مدارک حاوی گذرواژه ها می تواند مفید باشد. کنترل این اسناد ممکن است پیچیده باشد و ممانعت از نسخه های چاپی لزوما امکان پذیر نیست.

[۱۶] dry contact

[۱۷] اتصال خشک اتصالی که جریان را قطع یا وصل نمی کند

راه های مدیریت محدودیت ها	کاربران را از خطرات مرتبط با مستندات آگاه شوند. گذاشتن اسناد در معرض دید، برای مثال روی میز یا صندوق عقب اتومبیل عمل خوبی نیست.

منبع

https://www.ssi.gouv.fr/uploads/۲۰۱۴/۰۱/Managing_Cybe_for_ICS_EN.pdf

تقسیم بندی شبکه

هدف از تقسیم بندی شبکه، تقسیم سیستم به قسمتهای امنیتی مجزا و پیاده سازی لایه های محافظت برای جداسازی قسمت های مهم سیستم با استفاده از دستگاه اجرای سیاست است.

پیاده سازی تقسیم شبکه، جدا کردن شبکه های تجاری از شبکه های سیستم‌های کنترل

ISA۹۹، شش سطح تقسیم بندی را شرح می دهد:

- سطح ۰ شبکه تجهیزات BUS
- سطح ۱ کنترلر LAN
- سطح ۲ نظارت HMI LAN
- سطح ۳ عملیاتDMZ
- سطح ۴ Enterprise LAN
- سطح ۵ DMZ اینترنت

منبع

https://www.publicsafety.gc.ca/cnt/rsrcs/cybr-ctr/۲۰۱۲/tr۱۲-۰۰۲-en.aspx