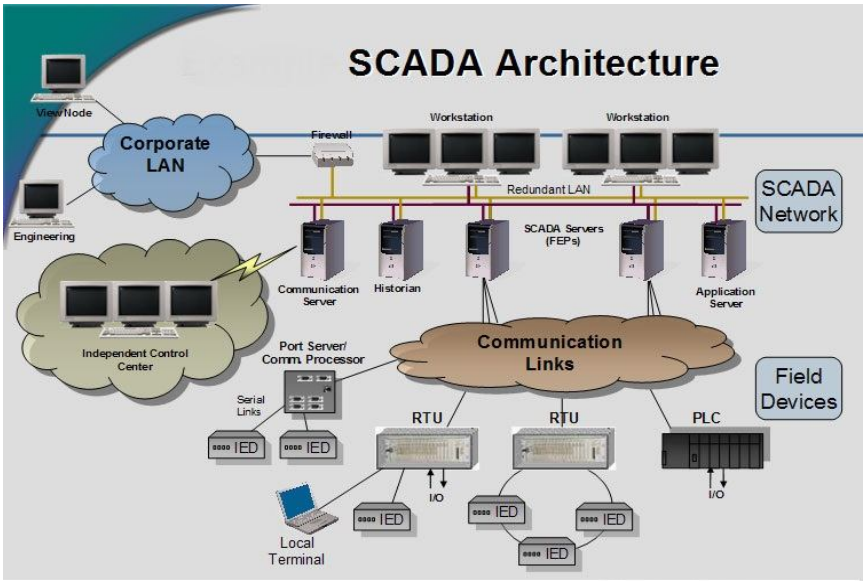
امنیت در سیستم‌های کنترل صنعتی و SCADA

امین علی‌بلندی

سیستم کنترل صنعتی آمده است تا سرعت، دقت تولید و بهره‌وری را در صنعت بهبود ببخشد. حتی فرایندهای ناممکن و بسیار پیچیده را تسهیل کند و امکان کنترل و مانیتورینگ از راه دور را فراهم سازد. روند رو به رشد تکنولوژیهای بکار رفته در سیستم‌های کنترل صنعتی، تغییرات مداوم، حرکت رو به جلو دانش فناوری‌اطلاعات و ظهور پدیده‌ها و امکانات جدید قابل استفاده در بخش‌های مختلف به خصوص بخش صنعت و نیز ارتباط تنگاتنگ صنعت و IT و از همه مهمتر مسایل سیاسی، پرداختن به مقوله امنیت را دوچندان می‌کند.

پیدایش SCADA

SCADA (Supervisory Control And Data Acquisition) به معنای کنترل نظارتی و دستیابی به اطلاعات است.



با گسترش سامانه‌های رایانه‌ای، استفاده از SCADA جهت نظارت بر شبکه‌ی برق، توسعه‌ی چشمگیری یافت. سامانه‌های مدیریت شبکه‌ی برق از اواخر دهه‌ی 1970 جهت تحلیل رفتار شبکه‌ی برق، نظارت بر قابلیت اطمینان سامانه و برنامه‌ریزی تولید نیروگاه‌ها به کار گرفته شدند.

تا اواسط دهه‌ی1990میلادی، عمدتاً شرکتهای برق کشورهای مختلف مبادرت به خرید و راه‌اندازی سامانه‌ی جامع اتوماسیون و دیسپاچینگ برق به صورت یک سامانه‌ی یکپارچه شامل پایانه‌های راه‌دور (RTU)، سامانه‌ی مخابراتی، تجهیزات مرکز کنترل، نرم‌افزار اسکادا و نرم‌افزارهای کاربردی قدرت برای شبکه های تولید و انتقال می‌کردند.

در واقع این سامانه‌ها صرفا کنترلی نیستند، بلکه بر سطح نظارتی نیز احاطه دارند و SCADA مجموعه‌ای نرم‌افزاری است که به همراه کنترل کننده‌های صنعتی نظیر PLCها و سایر ماژول‌های سخت‌افزاری عملیات کنترل نظارتی و داده‌برداری را در فرایندهای شیمیایی، حمل و نقل، نیروگاه‌های اتمی، سیستم‌های آبرسانی شهری، کنترل تولید و توزیع انرژی الکتریکی و در خطوط نفت و گاز و سایر فرایندهای گسترده و توزیع یافته استفاده می‌شود، حتی در شبکه‌های آبیاری و نیز به منظور جمع‌آوری اطلاعات، کنترل و نمایش وضعیت جایگاه‌های سوخت‌رسانی گاز طبیعی CNG کاربرد دارد و شامل فرایندهای زیر است :

- جمع‌آوری اطلاعات.
- انجام آنالیزها و کنترل‌های مورد نیاز.
- نشان دادن اطلاعات بر روی صفحات نمایش بهره‌برداران و گزارش‌گیری از آنها.

- ارسال اعمال کنترلی مورد نیاز به فرایند.

تهدیدات سامانه‌های کنترل صنعتی

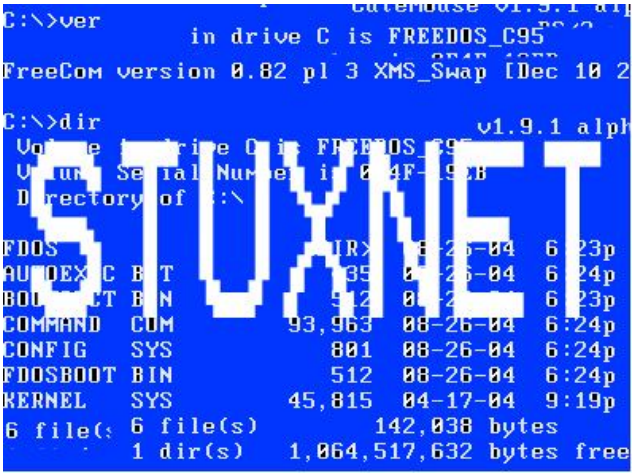
استفاده بیش از پیش سیستم‌های کنترل صنعتی و همچنین ساده انگاری مقوله امنیت در اینگونه سامانه‌ها و نیز بهره‌گیری از این سیستم در فضاهای مهم در همه کشورها باعث شده تا مهاجمین سایبری توجه زیادی به این مجموعه‌ها داشته باشند. کنترل‌کننده‌های منطقی برنامه‌پذیر(PLC)، سامانه‌های کنترل توزیع‌شده (DSC) و پروتکل‌های ارتباط در شبکه‌های سامانه‌های کنترل صنعتی و اسکادا عمدتاً با تمرکز بر قابلیت اطمینان و سادگی رفع مشکلاتشان طراحی شده‌اند و امنیت در آن‌ها کم‌تر مورد توجه بوده است و به راحتی در مقابل حملات سایبری آسیب‌پذیر هستند که نیاز به وصله شدن دارد. این محصولات عموماً دارای 1000 تا 5000 هزار خط کد سفت‌افزاری[1] هستند.

انگیزه مهاجمین :

واضح است که انگیزه‌ی مهاجمین تنها ایجاد اختلال و خسارت رساندن به زیرساخت‌های انرژی قربانیان نیست و آن‌ها به دنبال کسب اطلاعات و جزییات دقیق شبکه و تجهیزات قربانیان نیز می‌باشند، تا در فرصت‌های بعدی با پیچیده‌تر کردن مولفه‌های بدافزار، کنترل کامل سامانه‌های کنترل صنعتی و اسکادای قربانی را به‌دست بگیرند.

دستاوردهای مهاجمین در برخی حملاتی که صورت داده‌اند

- نفوذ به اطلاعات
- تغییر سرعت خنک‌کننده سی‌پی‌یو
- دسترسی به رابط کاربری ماشین و انسان (HMI)[2]
- تغییرات در Modbus[3]
- تغییر فشار پمپ
- تغییر در دمای خروجی
- تغییر در سامانه‌ی پمپ



حملات شناخته شده علیه اسکادا :

➢ **استاکس‌نت**

در سال 2010 (تیرماه 1389)، بدافزار استاکس‌نت که به عنوان اولین بدافزار در شروع حملات سایبری شناخته می‌شود با موفقیت توانست به شبکه‌های ایزوله یا air-gapped نفوذ کند و باعث اختلال در فرآیندهای صنعتی شود. این کرم مخرب، از روش‌های مختلفی برای انتشار استفاده می‌کرد، که معروف‌ترین روش آن از طریق USB بوده است.

وزیر ارتباطات ایران در آبان 1389 در این خصوص اعلام نمود که منشاء ورود این ویروس به ایران نه از طریق شبکه اینترنت بلکه از طریق حافظه‌های جانبی بوده که افرادی از خارج از کشور به ایران آورده و بدون بررسی لازم به کامپیوترهای در داخل ایران متصل کرده‌اند.

هدف

بنابر اظهارنظر کارشناسان سیمانتک، این بدافزار سیستم‌هایی را هدف قرار داده است که دارای یک مبدل فرکانس هستند که نوعی دستگاه برای کنترل سرعت موتور است. استاکس نت به دنبال این دستگاه‌ها بر روی سیستم قربانی می‌گردد و فرکانسی (بازه‌ای از 800 تا 1200 هرتز) را که دستگاه‌های مذکور با آن کار می‌کنند شناسایی می‌کند. دستگاه‌های صنعتی که از این مبدل استفاده می‌کنند بسیار محدود هستند و غالباً در تاسیسات غنی‌سازی اورانیوم استفاده می‌شوند. این بدافزار فرکانس‌های مبدل را ابتدا تا بیشتر از 1400 هرتز بالا می‌برد و سپس آن را تا کمتر از 2 هرتز پایین می‌آورد و سپس آن را فقط برای بالاتر از 1000 هرتز تنظیم می‌کند. در اصل، این بدافزار سرعتی را که موتور با آن کار می‌کند، به هم می‌ریزد. از این طریق کیفیت محصول پایین می‌آید و یا اینکه اصلاً تولید نمی‌شود، مثلاً تأسیسات غنی سازی نمی‌توانند به درستی اورانیوم را غنی سازی کند و همچنین منجر به خرابی موتور به صورت فیزیکی می‌شود.

- بدافزار **هاوکس**

بدافزار هاوکس نیز درست مانند کرم‌واره‌ی استاکس‌نت، به نحوی طراحی شده است که نرم‌افزارهای اسکادا و سامانه‌های کنترل صنعتی را هدف قرار دهد و این بدافزار قابلیت حمله به سدهای برق‌آبی، سایت نیروگاه‌های هسته‌ای و حتی حمله به تاسیسات برق یک کشور تنها با یک کلید را داراست. از این بدافزار در برخی از حملات سایبری علیه زیرساخت‌های انرژی اروپا مورد استفاده قرار گرفته شد.

مهاجمین از سه شیوه‌ی مهم (که دو روش اول نسبتاً مرسوم و روش سوم بسیار خلاقانه است) برای آلوده کردن قربانیان استفاده کرده‌اند:

- سوءاستفاده از آسیب‌پذیری‌های موجود در ماشین‌آلات و نرم‌افزارهای قربانیان.
- ارسال هرزنامه‌های همراه با بدافزار.
- نفوذ به وب‌گاه‌های منتشرکننده‌ی نرم‌افزار و سفت‌افزارهای کنترل صنعتی و اسکادا، تا قربانیان نسخه‌های آلوده را از وب‌گاه دانلود نمایند.

- **BlackEnergy**

از سال 2011 میلادی، بسیاری از شرکت هایی که از سامانه های کنترل صنعتی استفاده می کنند و به اینترنت متصل هستند، مورد حمله بدافزاری به نام Blackenergy قرار گرفته اند که با ایجاد یک درب مخفی (Backdoor) دسترسی غیرمجاز به سیستم ها و ماشین های صنعتی داشته‌اند. چندین شرکت صنعتی ، بدافزارBlackenergy را بر روی نرم‌افزار کاربردی HMI در سامانه های کنترل صنعتی متصل به اینترنت خود یافته و شناسایی کرده اند.

- **Regin**

و حالا رجین "Regin" که چندی نیست کشف شده است، نه دقیقا برای جاسوسی در سیستم‌های کنترل صنعتی بلکه با هدف پایش و جمع‌آوری اطلاعات در مراکز مخابراتی، ISPها،صنایع خطوط هوایی، بیمارستان هاو... به طور مخفیانه فعالیت کرده است.

هر چند تاریخ شروع فعالیت این بدافزار و بازه‌های مختلف زمانی آن دقیق مشخص نیست ولی مهم آن است که بدون اینکه ما متوجه شویم، این ویروس با یک روش فوق‌العاده پیچیده ارتباط با مرکز فرماندهی خود برقرار کرده و حتی می‌تواند از صفحه کامپیوتر قربانیان اسکرین‌شات تهیه کند، صفحه کلید را کنترل و حتی اطلاعات حذف شده را بازسازی نماید.

برخی کاستی‌های موجود در سیستم های کنترل صنعتی و SCADA که در نهایت منجر به آسیب‌پذیری می شود:

- بسیاری از پروتکل‌هایی که در سیستم‌های اسکادا و زیرمجموعه‌های آن استفاده میشود از رمزنگاری برای ارسال داده‌ها استفاده نمی‌کنند.
- آموزش‌ها و آگاهی‌های امنیتی در این زمینه محدود است.
- استفاده از ضد ویروسها در این سیستمها به دلیل الزام آنها بر بلادرنگ بودن بسیارسخت است.
- تست نفوذپذیری به صورت روتین انجام نمیشود و می‌بایست با دقت بسیار بالاصورت پذیرد.
- به روزکردن وصله‌های امنیتی روی این سیستمها باید با دقت بالا و معمولا با حضور تامیین کننده سیستم‌ها و فروشندگان مربوطه انجام شود.
- اطلاعات از دست رفته بازیابی نمی‌شوند و این امر می‌تواند منجر به وقایع بسیار خطرناک شود.
- نیاز به پاسخ‌دهی بلادرنگ دارد و تاخیر در این سیستمها قابل اصلاح نیست.

سیستمها همیشه باید پشتیبان داشته باشند زیرا باز ایستادن سیستمها از فعالیت میتواند خطرات جبران ناپذیری به همراه داشته باشد.

توصیه‌های Kyle Wilhoit (پژوهشگر امنیتی شرکت ترندمیکرو) برای ایمن نگاه داشتن سامانه :

- ✓ قفل کردن درگاه‌های USB
- ✓ اعمال احراز هویت دومرحله‌ای در همه سامانه‌ها.
- ✓ غیرفعال کردن دسترسی به اینترنت در منابع.
- ✓ همواره آخرین وصله‌ها را به تجهیزات و سامانه‌های اعمال گردد.
- ✓ استفاده از تقسیم‌بندی شبکه (مثلاً «WLAN » و «SCADA»).
- ✓ استفاده از SSL/TLs برای تمامی ارتباطات در سامانه‌های کنترل صنعتی مبتنی بر وب. (البته با در نظر گرفتن نکات مرتبط با آسیب پذیری جدید پروتکل SSLv3 به نام POODLE)
- ✓ افزایش امکانات گزارش‌گیری در این محیط‌ها.
- ✓ یک مدل تهدید برای سازمان خود توسعه دهید تا دریابید چه کسی و چرا به آن حمله می‌کند. (مانند استفاده از Honeypot[4])
- ✓ استفاده از حفاظت بلادرنگ.
- ✓ طبقه‌بندی داده و دارایی.
- ✓ کنترل دسترسی پیمان‌کار: شبکه‌های کنترل صنعتی از پیمان‌کاران راه دور استفاده می‌کنند؛ کنترل دستیابی آن‌ها به منابع بسیار مهم و ضروری است.

نتیجه :

بنا بر روند قبل از این و پیش رو، تهدیدات بسیار پیشرفته تر در این حوزه انتظار می‌رود. هرچند که بیشتر مواقع هکرها و مهاجمین سایبری یک پله جلوتر از ما هستند ولی شاید بالا بردن دانش امنیت حوزه IT و همچنین دقت بیشتر در این مقوله و تبعیت از فرهنگ پیشگیری بهتر از درمان، راهی به سوی پایین آوردن آسیب باشد.

منابع :

1. http://news.asis.io
2. KyleWilhoit (Trend Micro Forward-Looking- Threat Research Team)
3. https://www.owasp.org/index.php/OWASP_Scada_Security_Project
4. http://www.f-secure.com
5. http://threatpost.com
6. https://ics-cert.us-cert.gov/jsar/JSAR-12-241-01B
7. http://www.kaspersky.com/about/news/virus/2014/Regin

---

۱ - Firmware

۲ - HMI(Human-Machine Interface): نوعی نرم افزار است که یک صفحه رابط گرافیکی برای مدیریت و کنترل ماشین های صنعتی در اختیار کاربر می گذارد.

۳ - MODBUS یک پروتکل ارتباطی سریال است که برای استفاده در کنترل کننده‌های منطقی قابل برنامه‌ریزی (PLC) به کار می‌رود.

٤ - Honeypot یک منبع سامانه‌ی اطلاعاتی با اطلاعات کاذب است که برای مقابله با رخنه‌گران و کشف و جمع‌آوری فعالیت‌های غیرمجاز در شبکه‌های رایانه‌ای بر روی شبکه قرار می‌گیرد.