باسمه تعالی

عنوان مستند

مطالعه مستقل با تاکید بر خطرات پراهمیت امنیت سایبری SCADA / ICS

فهرست مطالب

۱ مقدمه

در سال های اخیر بسیاری از شرکت ها و سازمان های دولتی از سیستم های کنترل نظارت و گردآوری داده (SCADA) [۱] یا سیستم های کنترل صنعتی (ICS) [۲] استفاده کرده اند، اما این فناوری ها با چالش های امنیتی مهمی مواجه هستند. در تحقیقی که توسط Forrester Consulting به سفارش Fortinet انجام شد، تقریبا از هر ۱۰ سازمان مورد بررسی ۶ سازمان که از SCADA یا ICS استفاده می کنند در سال گذشته نفوذ به این سیستم ها را تجربه کرده اند و بسیاری از این سازمان ها با اجازه دادن به فناوری ها و شرکای دیگر، سطح بالایی از دسترسی به سیستم های خود را فراهم کرده اند. اکثر سازمان ها همچنین ارتباط بین سیستم های سنتی IT و SCADA / ICS خود را گزارش داده اند، و این پتانسیل موجود برای نفوذ به این سیستم های کنترلی را توسط هکرهای بیرونی نشان می دهد.

با وجود این خطرات، بسیاری از اپراتورها از بسیاری از ابزارهای امنیتی موجود برای محافظت از SCADA / ICS استفاده نمی کنند. تقریبا نیمی از کسانی که مورد بررسی قرار گرفته اند رمزگذاری ترافیک Secure Shell (SSH) یا Transport Layer Security (TLS) را برای SCADA / ICS خود بکار نبرده اند و بسیاری از کنترل دسترسی مبتنی بر وظیفه [۳] برای کارمندان استفاده نمی کنند.

در عین حال، بسیاری از سازمان هایی که از SCADA / ICS استفاده می کنند با اجازه دادن به یک میزبان از تکنولوژی های دیگر، از جمله سیستم موقعیت یاب جهانی(GPS)، سامانه شناسایی فرکانس رادیویی (RFID) و دستگاه های Wi-Fi، راه های حمله را باز نموده اند. در عین حال، ۹۷ درصد از کسانی که مورد بررسی قرار گرفتند، چالش های امنیتی را به دلیل همگرایی فن آوری اطلاعات سنتی (IT) و فناوری عملیاتی(OT) [۴] تایید کردند.

در حالی که خبر بد این است که SCADA / ICS با چندین تهدید مواجه هستند، خبر خوب این است که اپراتورها می توانند اقدامات بیشتری برای محافظت از سیستم خود با راه اندازی ابزارهای امنیتی اضافی انجام دهند.

---

[۱] supervisory control and data acquisition
[۲] industrial control systems
[۳] role-based access
[۴] operational technologies

۲ SCADA / ICS به عنوان اهداف مورد توجه

در سال های اخیر، بسیاری از سازمان ها پس از سازمان های آب و برق، SCADA / ICS را بکاربرده اند، زیرا آنها به دنبال جمع آوری اتوماتیک داده ها و کنترل اتوماتیک تجهیزات خود هستند. این فن آوری اهداف ارزشمندی را برای هکرها که به دنبال مختل نمودن فعالیت های کسب و کار(تجاری)، جمع آوری باج و یا حمله به زیرساخت های مهم کشور های رقیب می باشند، فراهم می کند. در مطالعه Forrester، ۵۶ درصد از سازمان هایی که از SCADA / ICS استفاده می کردند، یک نفوذ را در سال گذشته گزارش داده اند و تنها ۱۱ درصد آنها نفوذی نداشتند.

مهاجمان می توانند آسیب واقعی ایجاد کنند. در دسامبر ۲۰۱۵، چندین ناحیه اوکراین غربی به علت حمله به سیستم های کنترل صنعتی با قطعی برق مواجه شد. این تنها به اشخاص خارج از ایالات متحده محدود نمی‌شود. به عنوان مثال، در مارس ۲۰۱۶، هکرها به شبکه یک سازمان آب در آمریکا نفوذ کردند و برای مدت کوتاهی کنترل چندین کنترل کننده منطقی برنامه ریزی شده را که جریان مواد شیمیایی سمی مورد استفاده برای تصفیه آب را کنترل می کردند، کنترل نمودند.

بخش مهمی از مشکل، دسترسی اشخاص ثالث به SCADA / ICS است. بسیاری از سازمان ها اعتماد زیادی به فروشندگان فناوری و سایر سازمان های خارجی دارند و به آنها امکان دسترسی گسترده به سیستم های داخلی خود را می دهند. تقریبا از هر ۱۰ سازمان مورد بررسی توسط Forrester، ۶ سازمان دسترسی کامل یا سطح بالایی از دسترسی را برای سازمان های شریک و یا سازمان های دولتی فراهم آورده بودند. به طور خلاصه، اپراتورهای SCADA / ICS با خطرات جدی مواجه هستند و در راه بهبود وضعیت امنیتی با موانع متعددی مواجه هستند.

SCADA و ICS

ICS اغلب توسط سیستم های SCADA مدیریت می شود که برای اپراتورها یک رابط کاربری گرافیکی برای مشاهده وضعیت سیستم، دریافت هشدارها یا وارد کردن تنظیمات برای مدیریت فرآیندها را فراهم می کند.

۳ رشد سریع SCADA / ICS در تمامی جهات

بازار SCADA / ICS به سرعت در حال رشد است. تحقیقات بازار پیش بینی می کند بازار جهانی ICS، به تنهایی، از ۵۸ میلیارد دلار در سال ۲۰۱۴ به ۸۱ میلیارد دلار در سال ۲۰۲۱ افزایش خواهد یافت و رشد سالانه آن ۴/۹ درصد بین سال های ۲۰۱۵ تا ۲۰۲۱ خواهد بود. ICS به طور گسترده ای در تولید، بنادر ساحلی، در طرح های تصفیه آب، در خطوط لوله نفت، در شرکت های انرژی، و در ساخت سیستم های کنترل محیط زیست استفاده می شود. SCADA، که به عنوان رابط کاربری گرافیکی برای ICS عمل می کند، همزمان، با نرخ رشد سالیانه ۶/۶ درصد رشد می کند. خبر خوب این است که سازمان هایی که از SCADA / ICS استفاده می کنند تشخیص داده اند که با خطراتی مواجه هستند. بسیاری از آنها از تکنولوژی های مختلف و روش های امنیتی استفاده می کنند.

به عنوان مثال، مطالعه Forrester نشان داد ۷۰ درصد از سازمانهای مورد بررسی به طور مداوم ورود و ترافیک شبکه خود را تجزیه و تحلیل می کنند، ۲۴ درصد از آنها در حال حاضر، تجزیه و تحلیل امنیتی خود را گسترش داده اند. حدود دو سوم، از انواع روش های کنترل امنیت شبکه استفاده می کنند و ۶۲ درصد از روش های کنترل های امنیتی مبتنی بر بیومتریک مانند اثر انگشت یا تشخیص چهره استفاده می کنند.

انتظار می رود بازار ICS به سرعت رشد کند و به ۸۱ میلیارد دلار در سال ۲۰۲۱ برسد.

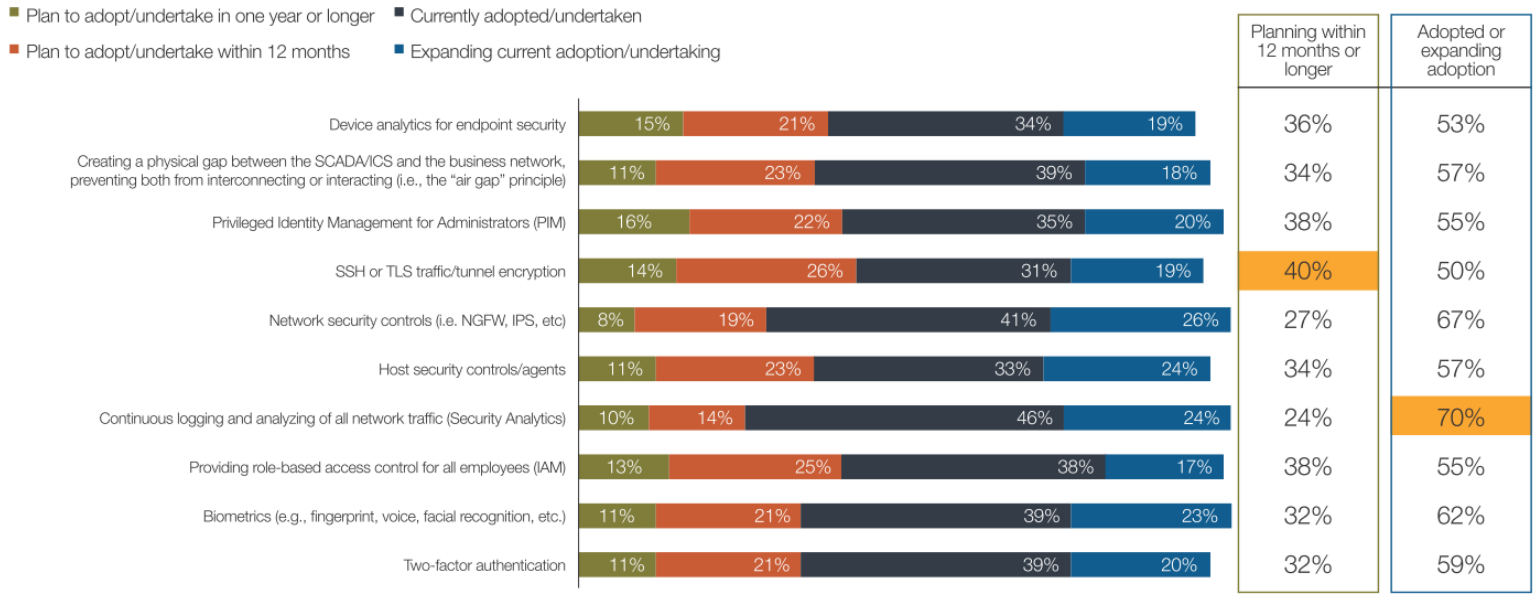
سطح حمله هر ساله افزایش می یابد.

انتظار می رود بازار SCADA سالانه ۶/۶ درصد رشد کند و به ۱۳/۴۳میلیارد دلار در سال ۲۰۲۲ برسد.

با وجود این ارقام، بسیاری از سازمان ها، تکنولوژی های امنیتی را که می توانند به محافظت از SCADA / ICS کمک کنند، بکار نگرفته اند. نیمی از آنهایی که مورد بررسی قرار گرفتند رمزگذاری ترافیک SSH یا TLS را بکارنگرفته اند، اگرچه بیش از نیمی از این تعداد برای اتخاذ یکی از این فن آوری ها در طول سال برنامه ریزی کرده اند.

اکثر سازمان های بزرگ در حال حاضر اقدامات متعددی را برای ایمن سازی SCADA / ICS خود دارند.

سوال (۱) - طرح های سازمان شما برای اتخاذ یا انجام اقدامات زیر جهت حفاظت از SCADA / ICS چیست؟



شکل (۱) نتایج تحلیل ترافیک صنعتی

اکثر اپراتورهای SCADA / ICS به طور مداوم ورود و ترافیک شبکه را تجزیه و تحلیل می کنند، در حالی که بیش از نیمی از انها از تجزیه و تحلیل دستگاهی برای امنیت پایدار استفاده می کنند.

علاوه بر این، ۴۵ درصد از پاسخ دهندگان از سیستم های مدیریت احراز هویت برای مدیران، استفاده نمی کنند این سیستم ها به سازمان اجازه می دهد تا حساب های سطح بالا را در محیط IT خود نظارت کنند. ۴۵ درصد دیگر از کنترل دسترسی مبتنی بر وظیفه برای کارکنان استفاده نمی کنند. با این حال، فقط یک درصد کوچک می گویند که هیچ برنامه ای برای اتخاذ این فناوری ندارند.

بسیاری از اپراتورهای SCADA / ICS ابزارهای امنیتی اولیه را نادیده می گیرند.

۴۵٪ از کنترل دسترسی مبتنی بر وظیفه استفاده نمی کنند.

این امر باعث تهدیدات داخلی می شود.

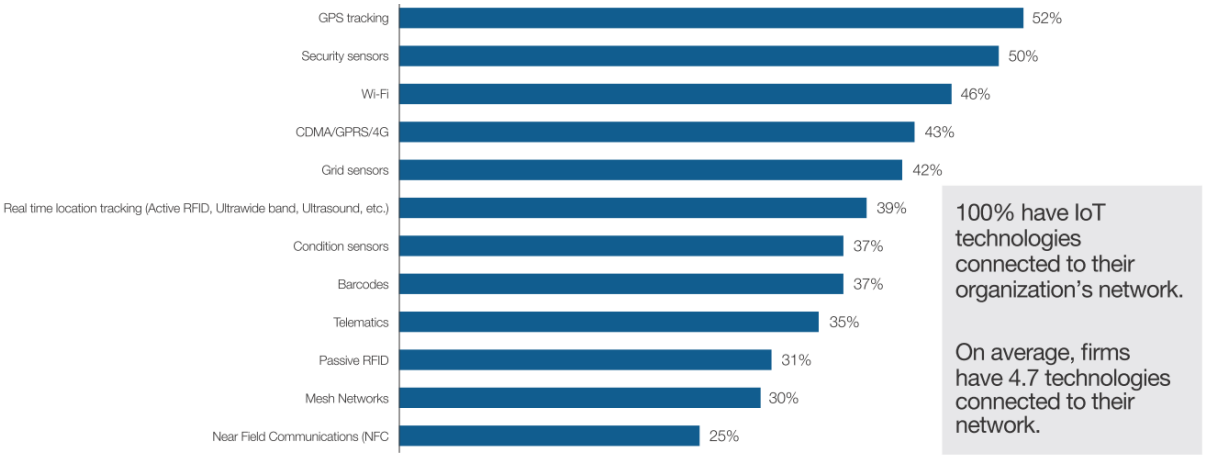
۴ چالش های امنیتی SCADA / ICS

به نظر می رسد سازمان های مبتنی بر تکنولوژی SCADA / ICS نگران استفاده از ابر[۵]، توسط فروشندگان این سیستم ها هستند. به ویژه، سازمانها نگران استفاده کارمندان از فناوریهای(دستگاه های) شخصی و ابری هستند که ممکن است به SCADA / ICS آنها متصل شوند.

حتی اگر سازمانها چندین خطر امنیتی را ببینند، ممکن است با برخی از اقدامات خود به مشکلات اضافه کنند. قابل توجه است که بسیاری از آنها اجازه می دهند تعداد زیادی از فن آوری های(دستگاه های) بی سیم و IoT به شبکه هایشان متصل شوند، که باعث آسیب پذیری های اضافی می شوند. هر شرکتی که توسط Forrester مورد بررسی قرار گرفت، دارای برخی از فن آوری های بی سیم یا IoT متصل به شبکه بود، که ممکن است شامل اتصالات به SCADA / ICS نیز باشند. به طور متوسط با وجود ۴/۷ دستگاه IoT متصل، خطر حتمی است.

در حال حاضر فناوری های(دستگاه های) IoT به شبکه متصل هستند.

سوال (۲)- کدام یک از فناوری های(دستگاه های) اینترنت اشیا (IoT) در حال حاضر به شبکه سازمان شما متصل است؟ (همه مواردی که بکار می روند انتخاب شود.)



شکل (۲) دستگاه های مورد استفاده در اتصال به SCADA/ICS

بیشتر کاربران SCADA / ICS دارای تعداد زیادی از دستگاه های متصل به شبکه های خود هستند.

[۵] cloud

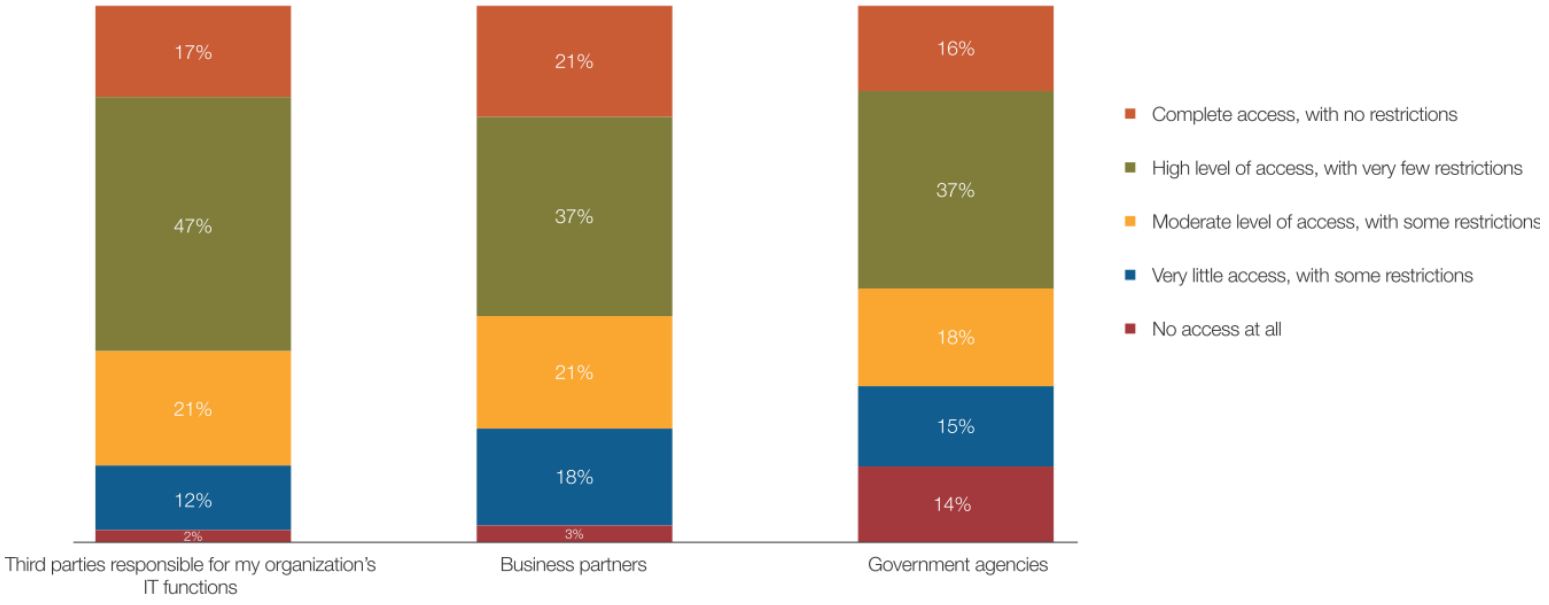
Wi-Fi مشکل بزرگی است. بیش از ۴۰ درصد از سازمان ها دارای دستگاه های Wi-Fi، دستگاه های تلفن همراه و سنسورهای تحت شبکه هستند. بسیاری از این اتصالات منجر به عوارضی برای سازمان هایی می شوند که تلاش می کنند تا همگرایی فناوری اطلاعات (IT) و فناوری های عملیاتی (OT) شان را مدیریت کنند - سخت افزار و نرم افزاری که SCADA و ICS را اجرا می کنند.

علاوه بر این، تقریبا سه چهارم دارای حداقل ارتباطات پایه بین IT و OT هستند، که خود نشانه خطر احتمالی هنگام حفاظت از آنها در برابر تهدیدات مخرب است.

نگرانی در مورد همگرایی IT و OT متفاوت است. حدود ۴ مورد در ۱۰ مورد نگران این هستند که آنها یا شرکای امنیتی شان فاقد تخصص لازم برای محافظت از IT و OT شان هستند. ۳۹ درصد دیگر نگران نشت اطلاعات حساس هستند و یک سوم نگران سوءاستفاده کنندگان درب های پشتی از دستگاه های متصل هستند. یکی دیگر از مشکلات بالقوه برای سازمان های استفاده کننده ازSCADA / ICS سطح دسترسی است که آنها به فن آوری و سایر شرکا داده اند. این دسترسی به هکرها راه دیگری برای حمله می دهد.

اکثر سازمان های بزرگ به بخش های خارجی اجازه دسترسی کامل و یا سطح بالا می دهند.

سوال (۳)- سطح دسترسی سایر سازمان ها به SCADA / ICS سازمان شما چقدر است ؟



شکل (۳) دسترسی سازمانها به سیستم های SCADA

بسیاری از کاربران SCADA / ICS به ارائه دهندگان فناوری و سایر شرکای کسب و کار اجازه دسترسی سطح بالا به سیستم های خود را می دهند.

به عنوان مثال، ۶۴ درصد از سازمان ها اجازه دسترسی کامل یا سطح بالا به SCADA / ICS خود را به فروشندگان فناوری اطلاعات شخص ثالث می دهند. اما مشکل با سطح اول روابط شروع نمی شود: تقریبا ۶۰ درصد به دیگر همکاران تجاری خود اجازه دسترسی کامل یا سطح بالا می دهند و بیش از ۵۰ درصد از آنها به سازمان های دولتی دسترسی مشابهی می دهند. هنگامی که به صنعت می آیید، تولید کنندگان بیشتر مایل به ارائه دسترسی کامل به سازمان های خارجی هستند.

به ریسک بالقوه این واقعیت را اضافه کنید که بسیاری از سازمانها امنیت SCADA / ICS خود را برون سپاری می کنند. بیشترین پروژه های SCADA / ICS که به فروشندگان فناوری اطلاعات برون سپاری می شود امنیت بی سیم، تشخیص نفوذ، کنترل دسترسی به شبکه و امنیت IoT است.

و برون سپاری به صورت ایزوله نیست: ۵۶ درصد از سازمانهایی که مورد بررسی قرار گرفتند، امنیت SCADA را به چندین فروشنده محول کردند. در بعضی موارد، استفاده از چندین فروشنده، مجموعه ای از وصله های امنیتی را ایجاد می کند که به خوبی با هم کار نمی کنند.

سازمان هایی که SCADA / ICS را اجرا می کنند، به شرکای خود اعتماد می کنند.

۶۴ درصد به فروشندگان فناوری اطلاعات شخص ثالث اجازه دسترسی کامل یا سطح بالا را می‌دهند.

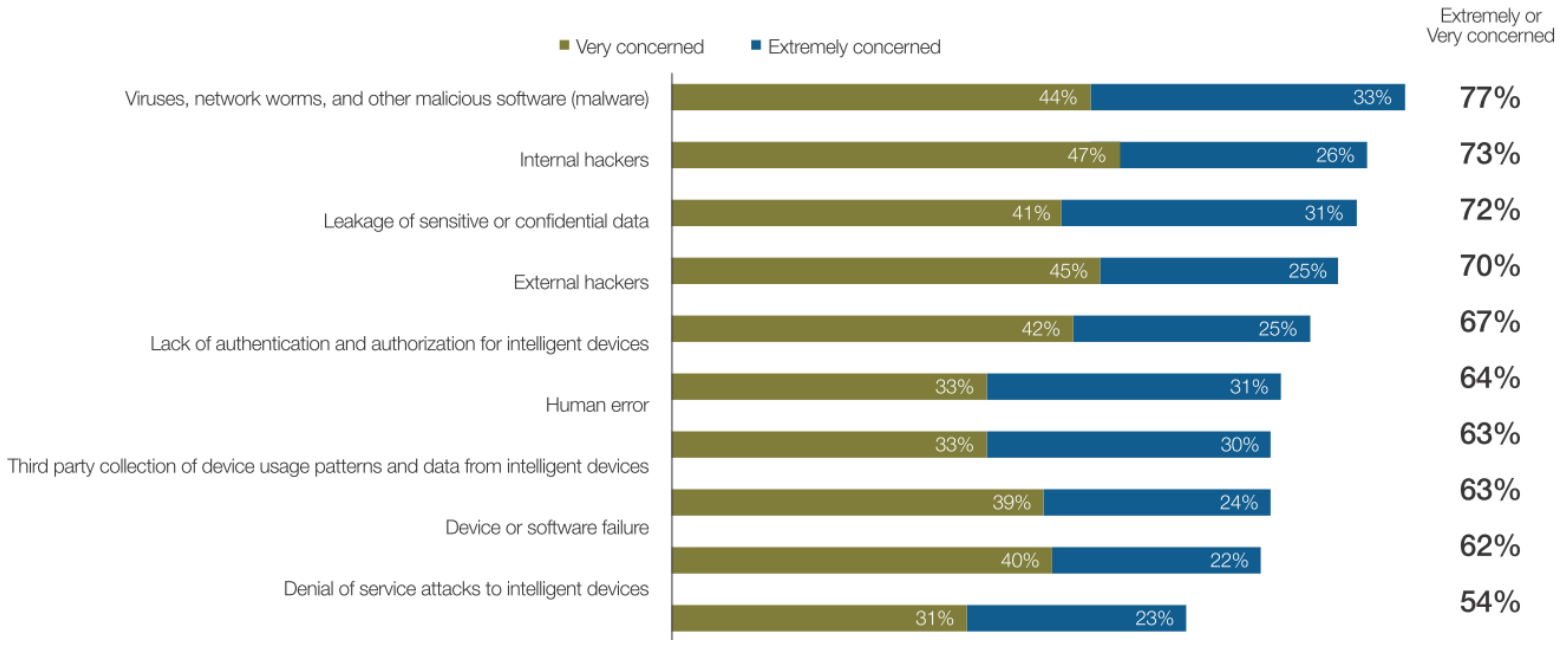
آسیب پذیری فروشنده IT شما، ممکن است آسیب پذیری شما باشد.

۵ تهدیدات SCADA و ICS

در ادامه پرسش در مورد سیاست های داخلی، مطالعه Forarester جدی ترین تهدیدات امنیتی سازمان هایی که از SCADA / ICS استفاده می کردند را مورد بررسی قرار داد. اپراتورها تهدیدهای چندگانه از چندین منبع را مشاهده می کنند، نرم افزارهای مخرب و نشت داخلی، نگرانی های امنیتی را بالا می برند. در اینجا، بیش از سه چهارم سازمان ها اذعان می کنند که در مورد نرم افزارهای مخرب خارجی بسیار نگران هستند. بیش از ۷ مورد از ۱۰ مورد بسیار نگران هکرهای داخلی، نشت اطلاعات حساس و هکرهای خارجی بودند. بیش از دو سوم نگران فقدان احراز هویت یا مجوز برای دستگاه های هوشمند هستند و تقریبا دو سوم نگران خطاهای انسانی و جمع آوری داده ها توسط شرکت های شخص ثالث هستند.

نگرانی های امنیتی دربرگیرنده گستره ای از ویروس ها و هکرها تا نشت اطلاعات و عدم وجود تایید هویت است.

سوال (۴)- میزان نگرانی خود را با موارد زیر در ارتباط با امنیت شبکه SCADA / ICS ارزیابی کنید.



شکل (۴) تهدیدات موجود در رابطه با امنیت شبکه SCADA / ICS

اپراتورهای SCADA / ICS در مورد نرم افزارهای مخرب، هکرهای داخلی و چندین تهدید دیگر صحبت می‌کنند.

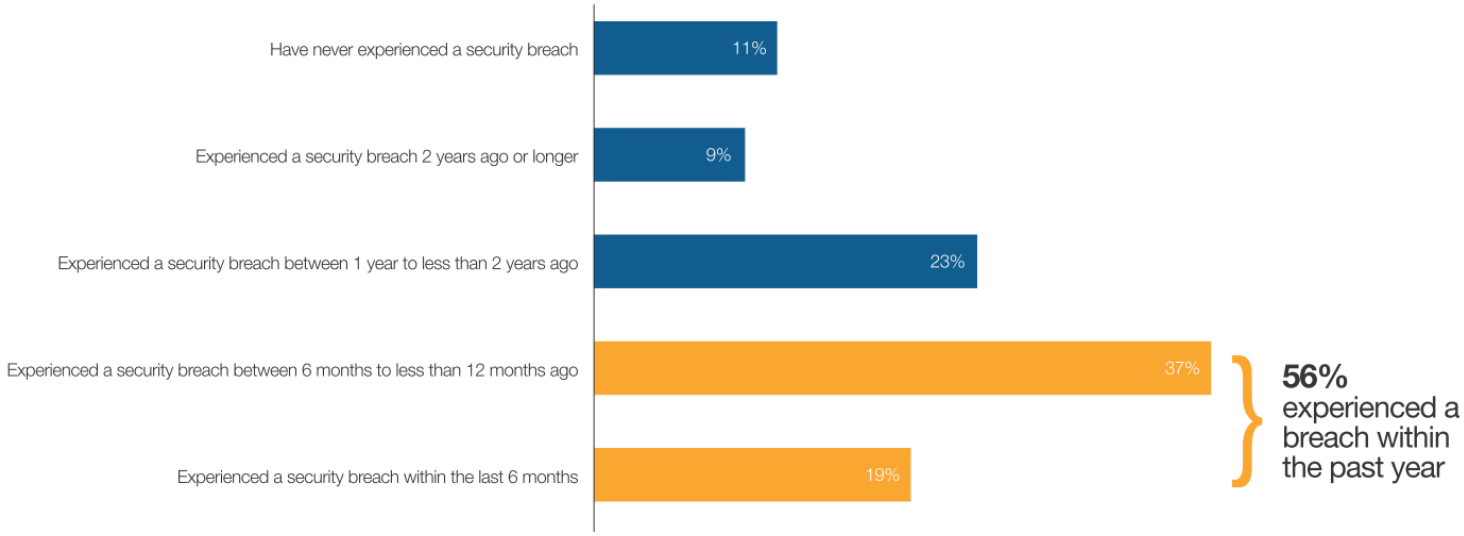
نگرانی ها در مورد نرم افزارهای مخرب و هکرهای داخلی از زمانی که مطالعه مشابه در سال ۲۰۱۶ انجام شد افزایش یافته است. در حالی که چشم انداز تهدید از آن زمان به طور قابل ملاحظه ای پیشرفت کرده است و سطح خطر بالاتری برای SCADA / ICS وجود دارد، اپراتورهای SCADA / ICS درک کردند که خطرات واقعی کاهش یافته اند. به عنوان مثال، خطای انسانی، جمع آوری داده توسط شخص ثالث و خطای دستگاه یا نرم افزار، برای آنها اهمیت کمتری دارند، اما این ممکن است به دلیل آن باشد که آنها شاهد خطرات امنیتی از منابع دیگر هستند.

۶ تأثیر تهدیدات

اگرچه بسیاری از سازمان ها اقدامات امنیتی متعددی را انجام می دهند، نفوذ در SCADA / ICS رایج است. به عنوان مثال، ۵۶ درصد از پاسخ دهندگان نفوذ به SCADA / ICS را در سال گذشته گزارش کردند، و ۳۲ درصد دیگر نیز نفوذ را زودتر تجربه کرده بودند. درصد کمی فقط هرگز نفوذی را مشاهده نکردند.

۵۶ درصد سازمانها نفوذ امنیتی به SCADA / ICS را در ۱۲ ماه گذشته تجربه کرده اند.

سوال (۵) تا آنجا که شما اطلاع دارید آیا SCADA / ICS سازمان شما، نفوذ امنیتی را تجربه کرده است ؟



شکل (۵) آثار میزان نفوذ به سامانه های SCADA / ICS

بیشترین کاربران SCADA / ICS یک نفوذ را در سال گذشته تجربه کرده اند.

نفوذ به SCADA / ICS پیامدهای جدی دارند. ۶۳ درصد از سازمان ها می گویند ایمنی کارکنان آنها به شدت تحت تاثیر نفوذ امنیتی به SCADA / ICS قرار گرفته است. ۵۸ درصد دیگر تاثیرات مهمی در ثبات مالی سازمان را گزارش می دهند و ۶۳ درصد آنها به یک مشکل بازدارنده اشاره کردند که مانع فعالیت در سطح رضایت بخش میشد.

نفوذ به SCADA / ICS رایج است.

۵۶ درصد از اپراتورهای SCADA / ICS یک نفوذ را در سال گذشته گزارش دادند.

نفوذ، امنیت کارمندان و ثبات مالی سازمان ها را به خطر می اندازد.

۷ توصیه هایی برای کاهش خطرات

بسیاری از سازمان ها گزینه های متعددی را برای کاهش خطرات SCADA / ICS مشاهده می کنند. تقریبا نیمی از شرکت ها، ارزیابی خطرات عملیاتی یا تجاری را به عنوان بهترین راه جهت بهبود وضعیت امنیتی خود در همگرایی سیستم های IT و OT می بینند. سایر رویکردهای رایج برای کاهش خطر شامل اجرای استانداردهای عمومی، افزایش تمرکز مدیریت دستگاه و مشاوره با سازمان های دولتی مانند Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) می باشد.

هنگامی که درباره انتخاب یک فروشنده امنیتی SCADA / ICS پرسیده شد، تقریبا بیش از نیمی از سازمان ها به مشاوران فناوری برای ارائه اطلاعات قابل اطمینان اعتماد می کنند. به عنوان مثال، فروشندگان و شرکای SCADA / ICS کمی بیش از ۵۰ درصد اعتماد را به دست می آورند.

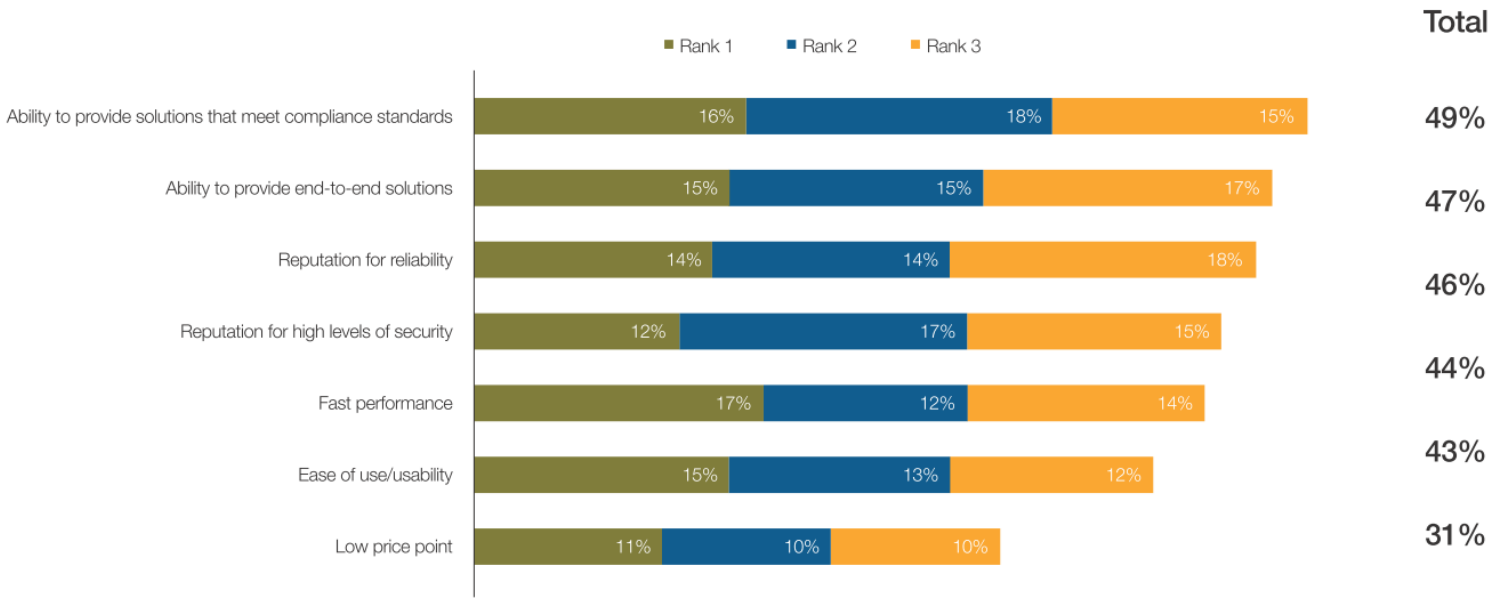
سازمان ها باید برای ارزیابی ارائه دهندگان امنیت و فن آوری، توانایی های آنها شامل موارد زیر را در نظر بگیرند:

- عملکرد سریع
- توانایی رعایت استانداردهای قابل انطباق
- جامع بودن، راه حل های (سراسری) end-to-end

اعتبار برای قابلیت اطمینان و امنیت بالا در بین سازمان ها دارای امتیاز بالا است. سازگاری با استانداردهای صنعت و امنیت، نگرانی عمده ای است که تقریبا نیمی توانایی رعایت استانداردهای قابل انطباق را به عنوان عامل اصلی در انتخاب راه حل های امنیتی می دانند. توانایی ارائه راه حل های end-to-end در لیست عوامل متمایزکننده، دوم است. جالب توجه است، تنها ۳ مورد از ۱۰ مورد قیمت کم را به عنوان یک عامل اصلی مطرح کردند.

هنگامی که یک فروشنده را انتخاب می کنید، رعایت استانداردهای قابل انطباق، ارائه راه حل های end-to-end، و قابلیت اطمینان بسیار مهم است.

سوال (۶) هنگامی که یک فروشنده امنیتی برای SCADA / ICS خود در نظر می گیرید، کدام یک از عوامل زیر، در صورت وجود، در انتخاب شما مهم هستند؟ (سه انتخاب اول را به ترتیب اهمیت مشخص کنید)



شکل (۶) پارامترهای انتخاب راه حل امن سازی برای سیستم های SCADA / ICS توسط پیمانکاران

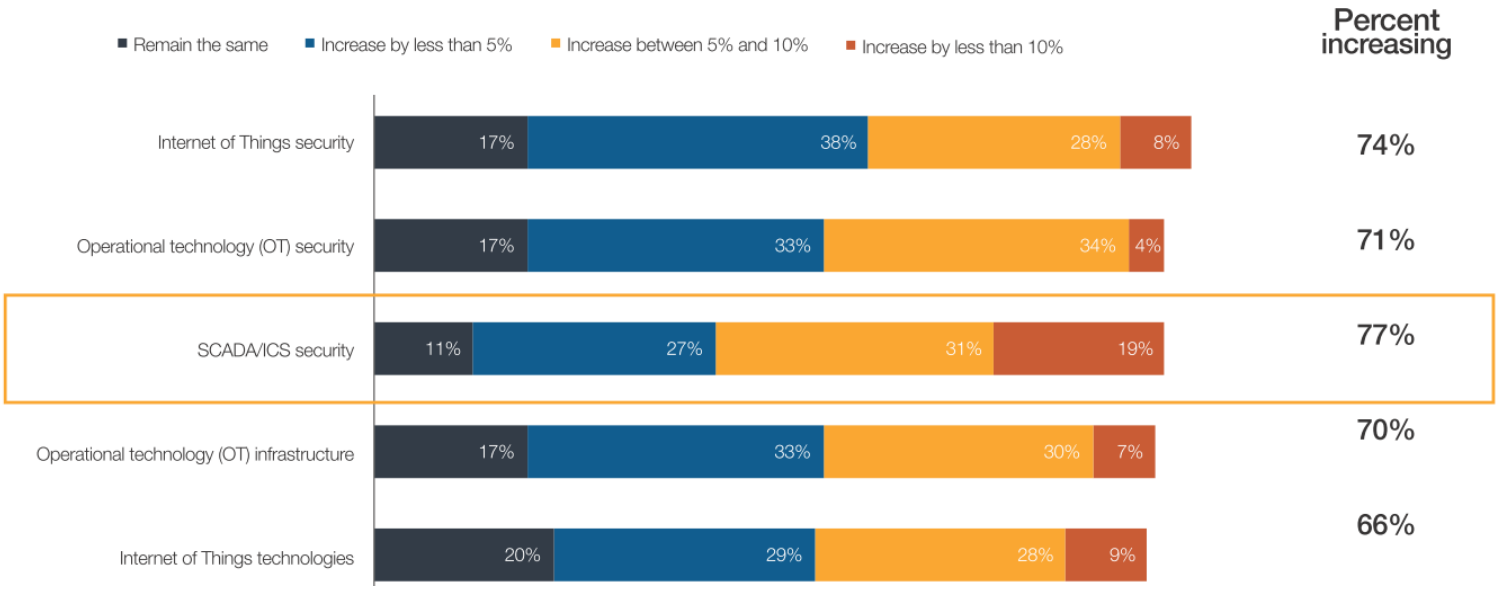
کاربران SCADA / ICS دارای چندین وظیفه برای تامین کنندگان امنیت، از جمله توانایی اجرای استانداردهای قابل انطباق و توانایی ارائه راه حل های end-to-end هستند.

۸ مسیر پیش رو

بسیاری از سازمان ها که از SCADA / ICS استفاده می کنند طرح هایی را برای افزایش هزینه کرد برای فناوری های امنیتی برای امسال برنامه ریزی نموده اند. کسانی که برنامه ریزی برای اضافه کردن به بودجه امنیتی خود ندارند از چرخه مسائل امنیتی جا می مانند. تقریبا سه چهارم سازمان ها برنامه های افزایش هزینه کرد امنیتی IOT را برنامه ریزی می کنند، و ۳۶ درصد از آنها هزینه کرد را ۵ درصد یا بیشتر افزایش می دهند. بیش از ۷ مورد از ۱۰ مورد برنامه ای برای افزایش هزینه کرد بیشتر در امنیت OT، و نزدیک به ۴ در ۱۰ مورد برنامه ای برای افزایش هزینه کرد حداقل ۵ درصد دارند. هر ۷ مورد از ۱۰ مورد، در سال جاری بیشتر به زیرساخت های OT خواهند پرداخت، ۳۷ درصد برنامه ریزی برای افزایش گردش مالی ۵ درصد یا بیشتر دارند. این سرمایه گذاری ها تعهد پیوسته و رو به افزایش به OT و استانداردهای امنیتی و نیاز به محافظت از این سیستم ها را نشان می دهد.

هزینه های امنیت SCADA / ICS بیشتر از هزینه برای دیگر حوزه ها افزایش می یابد.

سوال (۷) هنگامی که یک فروشنده امنیتی برای SCADA / ICS خود در نظر می گیرید، کدام یک از عوامل



زیر، در صورت وجود، در انتخاب شما مهم هستند؟ (سه انتخاب اول را به ترتیب اهمیت مشخص کنید)

شکل (۷) عوامل موثر در انتخاب پیمانکار امنیتی برای سامانه SCADA / ICS

بسیاری از اپراتورهای SCADA / ICS برای افزایش هزینه ها در امنیت در حوزه های مختلف در سال ۲۰۱۸ برنامه ریزی کرده اند.

در حالی در مورد اینکه برای چه اقدامات امنیتی پول صرف شود فکر می کنیم، اپراتورهای SCADA / ICS می توانند اقدامات مختلفی برای حفاظت از سیستم ها انجام دهند. از جمله:

- با جدا کردن فن آوری های بی سیم و IoT متصل از SCADA / ICS، شبکه را به بخش های جداگانه تقسیم کنید.
- امنیت زیرساخت های شبکه، از جمله سوئیچ ها، روتر ها و شبکه های بی سیم، از طریق فایروال ها و سایر ابزارهای طراحی شده برای محافظت از انها را تامین کنید.
- سیاست های هویت و مدیریت دسترسی را برای جلوگیری از دسترسی خارج از شبکه به شبکه و جلوگیری از دسترسی کارمندان به بخش های شبکه که نیازی به دسترسی به آن را ندارند اعمال کنید.
- از فایروال برنامه وب [۶] (WAF) برای اسکن و پچ برنامه های وب محافظت نشده استفاده کنید.
- سیستم حفاظت endpoint را برای عملکرد قابل اجرا در زمان حال، و مشاهده تهدیدات پیاده سازی کنید.

با توجه به توان بالقوه برای تاثیرگذاری بر ایمنی فیزیکی کارکنان یا مشتریان، ملاحظات امنیتی SCADA / ICS باید متفاوت از سیستم های سنتی IT باشد. خبر خوب این است که با در نظر گرفتن یک رویکرد چند لایه برای امنیت SCADA / ICS، سازمان ها می توانند به طور قابل توجهی پایه امنیت خود را بهبود بخشند و در نتیجه باعث کاهش خطرات آنها می شود.

[۶] web application firewall