PSC2009
24th International Power System Conference
09-F-DTC-0117
بیست و چهارمین
کنفرانس بین‌المللی برق

امنیت اطلاعات در سیستم‌های اسکادا

فرهاد غفارزاده، مجتبی طباطبائیان
پژوهشگاه نیرو
ایران
fghaffarzadeh@nri.ac.ir , mtabatabaeian@nri.ac.ir

واژه‌های کلیدی: SCADA، امنیت اطلاعات، سیستم‌های کنترل صنعتی، حملات سایبر، آسیب‌پذیری، کشف نفوذ، پیشگیری از نفوذ

چکیده

امنیت اطلاعات همواره یک عامل کلیدی در قابلیت اعتماد و حفظ پایداری صنعت برق بوده است. همزمان با افزایش توسعه سیستم‌های EMS[1]/SCADA[2]، تعداد شرکت‌های بازار رشد یافته و توسعه‌های پیچیده‌تری از این سیستم‌ها براساس تکنولوژی اطلاعات مطرح گردید که این عامل آنها را در برابر ریسک‌های امنیت اطلاعات بیشتر از پیش آسیب‌پذیر نمود. با توجه به الزام لحاظ نمودن امنیت اطلاعات برای سیستم‌های موجود در کوتاه مدت و هم‌چنین با درنظر گرفتن حملات سایبر و گسترش روزافزون فن‌آوری اطلاعات در سیستم‌های جدید و مبتنی بر اینترنت در درازمدت، پرداختن به موضوع امنیت اطلاعات و ارائه راه حل، امری ضروری و اجتناب‌ناپذیر می‌نماید. در این مقاله مروری بر ریسک‌های امنیت اطلاعات صورت گرفته و در ادامه به پیامدهای حملات اطلاعاتی، مکانیزم‌های دفاعی و پیشگیری و نیز مراحل حفاظت اطلاعات در سیستم‌های اسکادا اشاره می‌شود. هدف از این مقاله بیان نمودن دلایل اهمیت امنیت در این سیستم‌ها، تحلیل آسیب‌پذیری‌های اساسی و بیان توصیه‌هایی برای پیاده‌سازی و اجرای امنیت در آنها می‌باشد.

۱ـ مقدمه

امروزه سیستم‌های اسکادا به طور گسترده و همه جانبه‌ای در اتوماسیون صنعتی و کنترل فرآیندهای خاص مورد استفاده قرار می‌گیرند و بطور ویژه برای خودکار کردن سیستم‌هایی نظیر کنترل تبادلات انرژی، مدیریت شبکه برق و پردازش تلفات طراحی شده‌اند. اغلب سیستم‌های کنترل که امروزه

[1]- Energy Management System
[2]- Supervisory Control And Data Acquisition

استفاده می‌شوند، در سالهای گذشته و پیش از آنکه شبکه‌های مختلف، کامپیوترهای شخصی و اینترنت یک بخش مشترک و جدایی ناپذیر از پروسه‌های تجاری و اقتصادی باشند، توسعه یافته و پیاده‌سازی شده‌اند. این سیستم‌ها برای برآورده ساختن نیازهایی مانند افزایش بازده، قابلیت اطمینان، ایمنی و انعطاف‌پذیری طراحی شده و از نظر فیزیکی نسبت به خارج از شبکه کنترل ایزوله هستند. سیستم‌های موجود بر پایه سخت‌افزار، نرم‌افزار و پروتکل‌های ارتباطی که دارای قابلیت تشخیص و اصلاح خطا هستند، استوار می‌باشند ولی قابلیت ارتباطات امن که امروزه برای اتصال سیستم‌ها و شبکه‌های مختلف موردنیاز می‌باشد را دارا نمی‌باشند [7].

نسل‌های پیشین سیستم‌های کنترل صنعتی (ICS)[1] به طور عام، و اسکادا به عنوان نمونه‌ای از این گونه سیستم‌ها به طور خاص، با هدف بالا بردن قابلیت‌های اعتماد، نگهداری و دسترسی یا به عبارتی RMA[2] طراحی شده‌اند و در آنها نیاز به امنیت اطلاعات و برقراری ارتباطات ایمن با یکدیگر پیش‌بینی نشده بود. در حال حاضر آسیب‌پذیری سیستم‌های کنترل و اسکادا عمدتاً از نوع فیزیکی نبوده و بیشتر به موضوع امنیت اطلاعات ارتباط دارد. امروزه یک سیستم و شبکه ایمن می‌بایست در برابر حملات تخریب اطلاعات محافظت شده و الزاماتی نظیر محرمانگی[3]، تمامیت[4]، قابلیت دسترسی، انکارناپذیری[5]، پاسخ‌گویی[6]، احراز هویت[7] و قابلیت اطمینان[8] اطلاعات و سرویس‌ها را برآورده نماید [2]، [4] و [10].

۲ـ تاریخچه ایمنی

توسعه سیستم‌های کنترل صنعتی با تغییر و تحولات میکروپروسسورها، کامپیوترهای شخصی، تکنولوژی‌های شبکه در طی سالهای ۱۹۸۰ و ۱۹۹۰ و تکنولوژی‌های مبتنی بر اینترنت در طراحی سیستم‌های ICS بعد از دهه ۱۹۹۰ همزمان گردید. این تغییرات سیستم‌های ICS را در معرض انواع تهدیدهای جدید قرار داده و امکان حمله به آنها را افزایش داد [2].

از ۱۱ سپتامبر ۲۰۰۱، تهدید حمله‌های تروریستی به عنوان یک تهدید بزرگ برای بسیاری از منابع اقتصادی آمریکا پدیدار گردید. اغلب فعالیت‌های اجتماعی و اقتصادی براساس منابع انرژی، سرویس‌های ارتباطی، حمل و نقل و غیره بنا شده است. یک حمله به این زیرساختارها، اثرات ویرانگری بر اقتصاد و زندگی مردم خواهد داشت. بعد از واقعه ۱۱ سپتامبر، تلاش‌های زیادی برای حفاظت ایمن و مطمئن از عملکرد زیرساختارهای برق، گاز، مخابرات، حمل و نقل و موسسات مالی انجام شده است [4].

موسسه CIN/SI[9] با موسسه تحقیقاتی EPRI[10] و سازمان دفاع آمریکا (DoD)[11] کنسرسیومی ایجاد کردند تا جهت بررسی اثر زنجیره‌ای وابستگی زیرساختارهای ذکر شده، ابزارها و تکنیکهای جدیدی را توسعه دهند. استاندارد طراحی بازار به وسیله کمیته تنظیم انرژی فدرال (FERC)[12] تهیه شده است که در برگیرنده استانداردهای امنیتی برای حوزه برق که توسط NERC[13] پیشنهاد شده است، نیز می‌باشد. گروه CIPAG[14] به عنوان هماهنگ کننده فعالیت‌های امنیتی NERC با تمرکز بر امنیت اطلاعات، فیزیکی و عملیاتی تشکیل شده است. آنها هم‌چنین با سازمان‌هایی نظیر DoE[15] و NIPC[16] همکاری می‌نمایند. PKI[17] نیز یک خط مشی امنیتی برای امنیت اطلاعات است که با اتصال خط مشی و تکنولوژی، یک محیط و بستر ایمن برای حوزه تجارت الکترونیکی به وجود می‌آورد.

[1]- Industrial Control Systems
[2]- Reliability, Maintainability and Availability
[3]- Confidentially
[4]- Integrity
[5]- Nonrepudiation
[6]- Responsibility
[7]- Authentication
[8]- Reliability

[9]- Complex Interactive Network/ System Initiative
[10]- Electric Power Research Institute
[11]- Department of Defense
[12]- Federal Energy Regulatory Commission
[13]- North American Electric Reliability Council
[14]- The Critical Infrastructure Protection Advisory Group
[15]- Us Department of Energy
[16]- National Infrastructure Protection Center
[17]- Public Key Infrastructure

۳ـ مقایسه سیستم‌های کنترل صنعتی و IT

سیستم‌های ICS مشابهت زیادی با سیستم‌های IT[1] دارند. هر چه بر میزان در دسترس بودن تجهیزاتی که از شبکه استفاده می‌کنند افزوده می‌شود، به احتمال وقوع رویدادها و آسیب‌پذیری‌های امنیت اطلاعات اضافه می‌گردد. همان‌گونه که سیستم‌های ICS با کاربردهای IT به جهت ایجاد ارتباط و قابلیت دسترسی‌های از راه دور سازگار می‌گردند، در طراحی و پیاده‌سازیهای آنها از کامپیوترهای صنعتی، سیستم عامل‌ها و پروتکل‌های شبکه نیز استفاده می‌گردد تا شروعی برای همانندسازی آنها با سیستم‌های IT شود. در این یکپارچه سازی از قابلیت‌های جدید IT پشتیبانی می‌شود اما این مسئله موجب ایزوله شدن کمتر آنها از دنیای بیرون می‌گردد و نیازهای بیشتری را در رابطه با امنیت این سیستم‌ها به وجود می‌آورد. راه حل‌های امنیتی که برای سیستم‌های IT طراحی می‌گردند، می‌بایست با جنبه‌های احتیاطی بیشتری برای موارد مشابه در محیط کنترل صنعتی به کار گرفته شوند. با توجه به ریسک‌ها و مشخصه‌های متفاوت سیستم‌های کنترل صنعتی از سیستم‌های پردازش اطلاعات IT، گاهی راه حل‌های جدیدی موردنیاز می‌باشد [2] و [5].

به خطر افتادن سلامتی و ایمنی انسانها، خرابی‌های جدی در محیط، مسائل مالی نظیر قطع تولید، ضربات منفی به اقتصاد جهانی و دستیابی و سوء استفاده از اطلاعات اختصاصی از جمله این ریسک‌ها هستند. دستیابی به ایمنی و راندمان گاهی اوقات با مسئله امنیت در طراحی و عملکرد سیستم‌های کنترل تلاقی نموده و اختلال ایجاد می‌نماید. در اینجا به چند ملاحظه خاص به هنگام در نظر گرفتن امنیت برای سیستم‌های کنترل صنعتی اشاره می‌شود:

۱. ICS ها عموماً نسبت به زمان حساس می‌باشند به طوری که تاخیر، بی‌ثباتی و بی‌نظمی در تحویل اطلاعات قابل پذیرش نمی‌باشد. در نقطه مقابل، سیستم‌های IT می‌بایست دارای توان عملیاتی بالا باشند ولی می‌توانند در برابر بعضی تاخیرها مقاومت نموده و آن را تحمل کنند.

۲. بسیاری از پردازش‌های ICS به طور مداوم عمل می‌نمایند و وجود هرگونه وقفه ناخواسته در آنها غیرقابل قبول می‌باشد. بنابراین استفاده از استراتژی‌های مرسوم حوزه IT نظیر راه‌اندازی مجدد[2] یک جزء، معمولاً راه حل قابل قبولی برای داشتن RMA بالا برای ICS نمی‌باشد.

۳. در یک سیستم ICS، ایمنی انسان و تحمل خطا جهت جلوگیری از خسارت‌های جانی و مالی از ملزومات و اهداف اولیه محسوب می‌گردد در حالی که در سیستم‌های IT، محرمانگی داده و حفظ یکپارچگی آن از ملزومات و اهداف اولیه می‌باشند.

٤. برای ICS ها، واحدهایی نظیر PLC ها، ایستگاه‌های عملیاتی، کنترلرهای توزیع شده(DCS)[3] و حفاظت از سرور مرکزی از اهمیت برخوردارند . در سیستم IT، تمرکز اولیه بر حفاظت از عملکرد تجهیزات IT چه به صورت متمرکز و چه به صورت توزیع شده، و هم‌چنین اطلاعات ذخیره شده بر روی آنها و اطلاعات انتقال یافته بین این تجهیزات می‌باشد.

۵. یک ICS می‌تواند فعل و انفعالات پیچیده‌ای با پردازش‌های فیزیکی و رویدادهای پیرامونی خود داشته باشد و هرگونه اخلال در عملکرد آن می‌تواند منجر به حوادث فیزیکی گردد. در یک سیستم IT معمولاً تعامل فیزیکی با محیط وجود ندارد.

٦. در سیستم‌های ICS، زمان پاسخ اتوماتیک و یا پاسخ سیستم به اقدام انسانی بسیار با اهمیت می‌باشد. به عنوان نمونه نیاز به تصدیق کلمه عبور و اجازه عمل بر روی یک واحد HMI[4] نبایستی مانع از عملکردهای ضروری ICS گردیده و در جریان پردازش وقفه‌ای ایجاد نماید. در سیستم IT، کنترل دسترسی می‌تواند بدون توجه به جریان داده پیاده‌سازی گردد.

۷. نسل‌های پیشین سیستم‌های عامل ICS و برنامه‌های کاربردی آن، معمولاً قابلیت موارد امنیتی IT نظیر رمز کردن، ثبت اشکالات و حفاظت توسط کلمه عبور را دارا نمی‌باشند. ارتقاء دادن سخت‌افزار و برنامه‌های کاربردی در یک شبکه سیستم کنترل عملیاتی بسیار مشکل بوده و به سادگی نمی‌توان قابلیت‌های امنیتی جدید را به آن اعمال نمود.

۸. پروتکل‌های ارتباطی استفاده شده در تجهیزات کنترلی با موارد مشابه در سیستم‌های IT متفاوت می‌باشند.

---

[1]- Information Technology

[2]- Rebooting

[3]- Distributed Control System

[4]- Human Machine Interface

۹. به روز کردن نرم‌افزارها بر روی یک ICS نمی‌تواند همیشه براساس یک منطق زمانی اجرا گردد چرا که بایستی برنامه کنترل صنعتی توسط فروشنده آن در محل نصب تست شده و با برنامه‌ریزی‌های از پیش تعریف شده برای قطعی‌های ICS، هماهنگ باشد در حالی که نرم‌افزارها بر روی سیستم‌های IT به سادگی و با اجرای بسته‌های اصلاحی امنیتی بروز می‌گردند.

۱۰. پشتیبانی تجهیزات ICS معمولاً از طریق یک فروشنده خاص صورت می‌گیرد که ممکن است هیچ تنوعی نداشته و توسط سایر فروشنده‌ها نیز پشتیبانی نشود. اما سیستم‌های IT می‌توانند از انواع پشتیبانی متنوع استفاده نمایند حتی اگر هیچ تجانسی هم با یکدیگر نداشته و از فن‌آوری‌های مختلف و متفاوت در آنها استفاده شده باشد.

۱۱. دوره عمر تکنولوژی برای ICS در حدود ۱۵ تا ۲۰ سال و گاهی اوقات بیشتر می‌باشد در حالیکه با توجه به تحولات سریع تکنولوژی دوره عمر اجزاء IT ۳ تا ۵ سال است.

۱۲. اجزاء سیستم‌های کنترل صنعتی می‌توانند در یک گستره جغرافیایی وسیع پراکنده باشند و دسترسی به آنها مشکل و پرهزینه می‌باشد در حالی که دسترسی به اجزاء IT معمولاً به صورت محلی بوده و دسترسی به آنها آسان است .

٤ـ پیامدهای حملات اطلاعاتی[1] یا سایبر

ارزیابی پیامدهای حملات اطلاعاتی در محیط صنعتی به سادگی برآورد مالی ناشی از یک واقعه نمی‌باشد. اگرچه خسارت‌های مستقیمی وجود دارد که به سادگی قابل ارزیابی و برآورد مالی است (همانند از دست رفتن تولید و یا تخریب واحد صنعتی) ولی پیامدهای دیگری نیزدارد که ممکن است کمتر قابل مشاهده باشند. برای اغلب کمپانی‌ها، ضربه وارده به اعتبار و آبروی آنها با اهمیت‌تر از هزینه‌های حاصل از قطع تولید می‌باشد. ضربه به سلامت و اعتبار نشان تجاری[2] یک کمپانی می‌تواند بسیار زیان بار باشد.

بررسی گزارش‌های وقایع به طور واضح نشان می‌دهد که اغلب پیامدهای حملات اطلاعاتی به واحدهای صنعتی منجر به از دست دادن نظارت و قابلیت کنترل و یا پردازش گردیده است. این مسئله افزودن واحدهای ایمنی و اضطراری به سیستم‌های موجود را الزام‌آور می‌کند. درگذشته، این واحدها از سیستم کنترل اصلی مستقل بودند. اتصال و تلفیق سیستم کنترل اصلی با واحد ایمنی، ریسک بالقوه ناکامی در کل سیستم را افزایش می‌دهد. در آینده می‌باید ریسک‌های حمله اطلاعاتی نه تنها در طراحی سیستم‌های کنترل بلکه در سیستم‌های ایمنی نیز در نظر گرفته شود بگونه‌ای که تداوم سرویس‌دهی و خدمات محقق گردیده و سیستم پس از بروز یک حمله یا وجود اشکال در کمترین زمان به شرایط طبیعی بازگردد [6].

یکی از روش‌های موثر در تامین امنیت اطلاعات، آگاه بودن یک مرجع تخصصی از حملات واقعی بر علیه کلیه سیستم‌های کنترل صنعتی و IT کشور، و متعاقب آن ارائه راه حل‌های جامع برای مقابله با آنها می‌باشد ولی متاسفانه اکثر سازمان‌ها به دلایل حیثیتی نسبت به ارائه گزارش‌های وقایع امنیتی رغبتی نشان نمی‌دهند. در حقیقت بیشتر سازمان‌ها وجود حتی یک ریسک در سیستم‌های صنعتی خود را انکار می‌نمایند.

در تحلیل امنیت صنعتی این مسئله پذیرفته شده است که ریسک‌های امنیتی که یک سازمان با آن مواجه می‌شود، تابعی از دو پارامتر احتمال حمله موفق بر علیه یک تجهیز و پی‌آمد حاصل از این حمله می‌باشد. دومین پارامتر (پیامد حمله) هنگامی که به طور مشخصی نمود کند، عموماً آسان‌ترین راه برای کشف بروز آن حمله *می‌باشد* [2].

٥ـ انواع حملات در شبکه های کنترل

برخی از حمله‌های امنیتی در شبکه‌ها عبارتند از:

الف) حمله از طریق استراق سمع : نفوذ غیرمجاز به ارتباطات شبکه و افشا کردن داده‌های مبادله شده.

ب) حمله سوء استفاده ورود[3]: دور زدن مکانیزم‌های کنترل دسترسی و تصدیق در سیستم و تخصیص دسترسی در سطحی بالاتر از حد مجاز به کاربر.

[1]- Cyber Attacks
[2]- Brand Image
[3]- Logon Abuse Attack

ج) حمله فریبکارانه[1]: استفاده از موجودیتی غیر مجاز مانند استفاده از یک IP جعلی برای نفوذ به سیستم.

د) حمله نفوذی[2]: دسترسی کاربران غیرمجاز به یک سیستم از طریق شبکه با استفاده از نقص‌های ایمنی آن.

ه) حمله سارقانه[3]: دسترسی غیرمجاز به منابع سیستم در پوشش ارتباطات درست و قانونی و یا سوء استفاده از آن. (نظیر مکانیزم اسب تراوا)

و) حمله انکار سرویس (DOS[4]) : اخلال در عملکرد شبکه و جلوگیری از سرویس‌دهی سرور به کاربران قانونی.

برخی از حمله‌ها به تکنولوژی‌های خاصی در شبکه مربوطند و برخی دیگر مستقل از تکنولوژی به کار رفته هستند. در این حمله‌ها ممکن است هدف، کشف توپولوژی و یا ارسال بسته‌های داده و یا هر دو باشد و موفقیت آنها به سیستم مسیریابی و پروتکل‌های آنها وابسته است. کنترل یک یا چند مسیریاب در شبکه‌ها توسط دشمن و جعل هویت آنها برای مسیریابی نادرست، استفاده از مسیریاب‌های خاص در مسیر ارسال جهت تخریب داده و ایجاد بسته‌هایی با آدرس جعلی، بالا بردن تصنعی بار ترافیک شبکه و کاهش راندمان آن و در نتیجه بروز انکار سرویس از جمله این حملات می باشند [2]، [3] و [9].

٦ـ مکانیزمهای دفاعی و پیشگیری

۱- به کارگیری دیواره آتش[5]: یکی از مرسوم‌ترین روش‌های محافظت در برابر حملات شبکه‌ای استفاده از دیواره‌های آتش می‌باشد. دیواره‌های آتش عمدتاً به عنوان مکانیزم‌های جلوگیری از تخریب عمل می‌نمایند و نقش اصلی آنها محافظت شبکه از نفوذ موجودیت‌های غیرمجاز خارجی است. دیواره‌های آتش، وسایل یا سیستم‌هایی هستند که جریان ترافیک را بین شبکه‌های به کار گرفته شده با وضعیتهای امنیتی گوناگون کنترل می‌نمایند. دیواره‌های آتش در محیط‌های شبکه‌ای بدون اتصالات اینترنتی نیز کاربرد دارند. با به کارگیری دیواره‌های آتش برای اتصال شبکه کنترل صنعتی به واحدهایی نظیر مدیریت و مالی، یک سازمان قادر خواهد بود که از دسترسی‌های غیرمجاز به سیستم‌های صنعتی و منابع حساس خود جلوگیری نماید [2] و [3].

از دیواره‌های آتش به طور فزاینده‌ای برای قرنطینه کردن زیر شبکه‌ها و یا میزبان‌های خاص که رفتار مشکوکی از خود بروز می‌دهند، استفاده می‌شوند. برای نمونه کرم‌هایی نظیر Slammer و یا CodeRed تعداد زیادی بسته داده را در مدت زمان کوتاهی به میزبان‌های مختلف ارسال می‌نمایند. برای این منظور در بیشتر روش‌های قرنطینه پیشرفته، میزبان تحت تاثیر قرار گرفته، در یک شبکه داخلی (LAN) مجازی قرار می گیرد و فقط اجازه دسترسی به وب سرور به آن داده می‌شود که دارای آخرین بسته‌های اصلاحی نرم‌افزارها برای چندین سیستم عامل مختلف باشد. سپس کاربر می‌تواند این بسته‌های اصلاحی را نصب نموده و سیستم را بدون وجود کرم و خطر آلودگی مجدد به آنها راه‌اندازی نماید [7] و [8].

دیواره های آتش انواع گوناگونی دارند که از آن جمله می توان به دیواره آتش اختصاصی[6]، دیواره آتش توزیع شده[7]، دیواره آتش لایه دوم و دیواره آتش سخت افزاری[8] اشاره نمود [3].

دیواره آتش اختصاصی، نرم‌افزارهایی را در سطح هسته اصلی سیستم عامل[9] برای مانیتور کردن و حائل شدن بین ارتباطات شبکه‌ای نصب می‌نماید و بدین وسیله فیلترینگ بسته‌های ارسالی را انجام می دهد. دیواره آتش اختصاصی تعدادی ضعف نیز دارد. به عنوان مثال این دیواره آتش تحت یک سیستم عامل همه منظوره اجرا می‌شود و نیاز به سرویس‌هایی دارد که در سطوح دسترسی بالاتر اجرا می‌شوند و چنانچه یک پردازش ویژه مورد هدف واقع شود، می‌تواند دیواره آتش را دچار اختلال نموده و یا از کار بیندازد.

در دیواره آتش توزیع شده یک خط مشی امنیتی به صورت مرکزی تعریف شده است اما بر روی هر نقطه پایانی شبکه همانند میزبان‌ها و مسیریاب‌ها توزیع شده است. سیستم، خط مشی مرکزی را به تمامی نقاط پایانی تسری می‌دهد که در شکل‌های مختلف می‌تواند صورت پذیرد. به عنوان مثال ممکن است این خط مشی مستقیماً به نقطه پایانی سیستم جهت اجرا اعمال شود، یا به صورت چارچوبی از اختیارات

[1]- Spoofing Attack
[2]- Intrusion Attack
[3]- Hijacking Attack
[4]- Denial-of-Service Attack
[5]- firewall

[6]- Personal Firewall
[7]- Distribution Firewall
[8]- Appliance Firewall
[9]- Kernel

کاربران تعریف شود تا به هنگام ارتباط با میزبان‌ها استفاده نمایند و یا به صورت ترکیبی از این دو حالت باشد.

دیواره‌های آتش لایه دوم نوعاً در لایه internetwork (IP) قرار گرفته و عمل می‌نمایند. آنها معمولاً جایگزین مسیریاب‌های سنتی می‌شوند که شبکه داخلی را با شبکه‌های غیرمطمئن خارجی مرتبط می‌سازند. شفافیت[1] دیواره آتش لایه ۲ برای میزبان‌های IP، این اجازه را می‌دهد که یک دیواره آتش بدون ایجاد مشکل و از هم گسیختگی عملیات شبکه، افزوده و نصب گردد. این خصوصیت از دیواره آتش لایه ۲ اجازه می‌دهد تا توسعه و پیاده‌سازی امنیت اضافی برای یک بخش خاص از شبکه داخلی به سادگی صورت پذیرد و برای حل مشکلات و کاهش حملات احتمالی کاربرد دارد. دیواره آتش سخت افزاری به یک سخت‌افزار خارجی نیاز دارد که برای حفاظت میزبان استفاده می‌شود. این نوع دیواره آتش عموماً همانند یک دیواره آتش سنتی عمل می‌نماید اما فقط برای حفاظت یک میزبان منفرد به کار می‌رود. این دیواره آتش دارای دو کارت واسط شبکه می‌باشد، یکی به کامپیوتری که حفاظت می‌شود و دیگری به بقیه شبکه متصل می‌گردد و ارتباط میزبان با دنیای خارج همواره از طریق این دیواره آتش انجام می‌شود. دیواره‌های آتش سخت افزاری به ویژه برای کمک به کاربران متحرک برای ایمن کردن لپ تاپهایشان موثر است [3] و [4].

۲- به کارگیری سیستم کشف و پیشگیری از نفوذ : مطالعه مکانیزم‌هایی که دیواره آتش آن را اجرا می‌نمایند، نشان می‌دهد که برای حفاظت در برابر برخی حمله‌ها ناتوان هستند. دیواره‌های آتش آنچه را که به شبکه وارد و یا از آن خارج می‌شود، کنترل می‌کنند ولی نمی‌توانند محتوای مبادلات را ببینند. بنابراین آنها نمی‌توانند هیچ کاری برای محافظت در برابر حمله‌هایی که از نقطه نظر مبادلات با شبکه مجاز می‌باشند، صورت دهند. برای این منظور مدیران اغلب آن را با یک سیستم کشف نفوذ (IDS)[2] جایگزین می‌کنند. از آنجایی که مدیران همیشه در دسترس نیستند و همین طور سرعت بعضی حمله‌ها به گونه‌ای است که هرگونه عکس‌العمل از طرف انسان غیرممکن می‌شود، دیواره‌های آتش مدرن به طور روزافزونی از اقدامهای متقابل اتوماتیک و تعریف شده استفاده می‌نمایند [3]. فعالیتهای کنترل دسترسی و کشف نفوذ با یکدیگر مرتبط بوده و این مسئله می‌تواند به دیواره‌های آتش اجازه دهد تا سریعاً به رفتار نادرست از طرف کاربران غیرقانونی عکس‌العمل نشان دهند. سیستم‌های جلوگیری از نفوذ (IPS)[3] مجاز هستند تا به کاربران ناشناخته و رفتارهای مجاز خارج از سیستم، اجازه تعامل با سیستم حفاظت شده را در حد محدودی بدهند. IPS وسیله‌ای است (سخت‌افزاری و یا نرم‌افزاری) که توانایی تشخیص حمله‌ها اعم از شناخته شده و یا نشده را داشته و جلوی حمله را سد می نماید. در عمل IPS هایی خوب هستند که توسط IDS ها کنترل شوند. یک مشکل عمومی در رابطه با IDS ها تعداد زیاد دفعاتی است که رفتارهای درست و قانونی را به عنوان رفتار مشکوک شناسایی می‌کنند. بنابراین متکی بودن به یک IDS منفرد به عنوان خط دفاعی، غیرمنطقی است [2] و [3].

۳- تفکیک شبکه‌های کنترل و اداری : در یک محیط کنترل صنعتی، دیوارهای آتش، اغلب بین شبکه کنترل و شبکه اداری قرار می‌گیرند. در صورت پیکربندی صحیح، آنها می‌توانند تا حدود زیادی از دسترسی‌های ناخواسته میان سیستم‌های کنترل، کامپیوترهای میزبان و کنترل کننده‌ها جلوگیری کرده و امنیت را بهبود بخشند. هم‌چنین آنها می‌توانند با حذف ترافیک غیرضروری در شبکه، پاسخگویی شبکه را کنترل نمایند و با طراحی، پیکربندی و نگهداری صحیح و اختصاص دیواره آتش سخت‌افزاری، امنیت ICS را افزایش دهند [2]، [1] و [7].

یک شبکه ICS می‌بایست به صورت منطقی از یک شبکه اداری جدا شود. برای این منظور می‌باید:

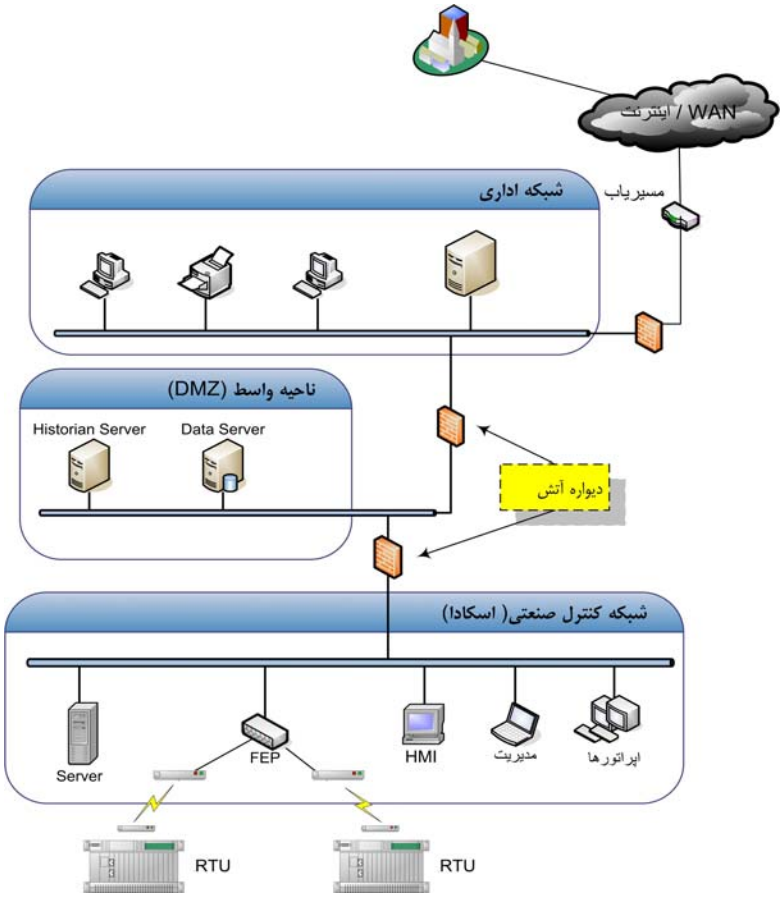
الف) نقاط دسترسی[4] بین شبکه ICS و شبکه اداری و هم‌چنین نقاط دسترسی افزونه[5] مشخص و مستند گردند.

ب) دیواره آتش بین شبکه‌های ICS و اداری طوری پیکربندی شود که ترافیک غیر مجاز را متوقف نماید. ج) دستورات دیواره آتش می‌باید امکان فیلتر کردن مبداء و مقصد، فیلتر کردن پورت‌های UDP[6]، TCP ، پروتکل کنترل اینترنت (ICMP[7]) و فیلتر کردن کد را داشته باشد.

---

[1]- Transparency
[2]- Intrusion Detection System

[3]- Intrusion Prevention System
[4]- Access Points
[5]- Redundant Access Points
[6]- User Datagram Protocol
[7]- Internet Control Message Protocol



شکل (۱) جداسازی شبکه‌ها با استفاده از DMZ

یک راه حل قابل دسترسی در برقراری ارتباط بین یک شبکه ICS و یک شبکه اداری، قرار دادن یک شبکه واسط میان آن دو می‌باشد که به ناحیه غیرنظامی یا DMZ[1] موسوم است. DMZ می‌باید به گونه‌ای به دیواره آتش متصل شود که یک ارتباط محدود بین شبکه اداری و DMZ و هم‌چنین شبکه کنترل صنعتی و DMZ به وجود آید. با قرار دادن اجزاء قابل دسترسی از شبکه اداری در DMZ، به وجود هیچ مسیر ارتباط مستقیمی از شبکه اداری به شبکه کنترل نیاز نبوده و کلیه مسیرها به DMZ ختم خواهند شد. اغلب دیواره‌های آتش می‌توانند اجازه استفاده از چند DMZ را بدهند و هم‌چنین می‌توانند مشخص نمایند که چه نوعی از ترافیک تبادل و ارسال شود.

چنانچه از یک سرور مدیریت بسته‌های اصلاحی نرم‌افزارها[2]، یک سرور آنتی ویروس و یا دیگر سرورهای امنیت برای شبکه کنترل استفاده شده باشد، می‌بایست به طور مستقیم در DMZ قرار گیرند. نخستین ریسک امنیتی در این نوع معماری این است که اگر یک کامپیوتر در DMZ هدف قرار گیرد، از آن می‌توان برای شکل دادن یک حمله بر علیه شبکه کنترل و از طریق برنامه‌های کاربردی مجاز واقع در DMZ استفاده نمود. امنیت بیشتر را می‌توان از طریق پیاده‌سازی تونل یا شبکه مجازی اختصاصی و امن (VPN)[3] بین شبکه کنترل و سایر شبکه‌ها ایجاد نمود [3].

استفاده از دیواره آتش با دو پورت ساده بین شبکه‌های کنترل و اداری، طرح پیشرفته استفاده از دیواره آتش و مسیریاب بین

[1]- Demilitarized Zone

[2]- Patch Management
[3]- Virtual Private Network

شبکه کنترل و شبکه اداری، استفاده از دیواره آتش بـه همـراه یـک DMZ بـین شـبکه‌هـای کنتـرل و اداری، اسـتفاده از دیواره‌های آتـش دوتـایی (زوج) بـین شـبکه اداری و شـبکه کنترل از جمله روش‌های تفکیک شبکه های کنترل و اداری و کاستن از شانس موفقیت یک حمله به شبکه کنترل می‌باشـند. شکل (۱) نحوه استفاده از دو دیواره آتش با DMZ بین شـبکه کنترل و شبکه اداری را نشان می دهد.

۷ـ روش‌های اجرایی حفاظت اطلاعات در سیسـتم‌هـای کنترل

با استفاده از استانداردهای امنیتی وضع شده برای صنعت برق و استانداردهای امنیـت اطلاعـات، روش‌هـایی اجرایـی بـرای حفاظت تجهیزات اطلاعاتی به دست می‌آید که بطور خلاصـه عبارتند از [2] و [4]:

۱. استفاده از روش‌های کلمه عبور موثر که به طور دوره‌ای الزام به تغییر داشته و به هنگام نصب یک تجهیز جدید، تغییر کلمه عبور پیش فرض الزامی باشد.
۲. تصدیق و بازرسی دروه‌ای کامپیوترها و حق دسترسی فیزیکی
۳. فاقد اعتبار نمودن کامپیوترهای غیرمجاز
٤. بستن یا غیرمجاز کردن پورت‌ها و سرویس‌های استفاده نشده شبکه
۵. ایجاد کانال‌های ارتباط تلفنی مطمئن جهت مودم‌ها
٦. استفاده از دیواره آتش
۷. استفاده از تجهیزات کشف و جلوگیری از نفوذ
۸. مدیریت بسته‌های امنیتی اصلاحی نرم‌افزارها
۹. نصب و به روز کردن نرم‌افزارهای ضد ویروس
۱۰. اطمینان از ایمن بودن تجهیزات مخابراتی و کانال‌های ارتباطی تجهیزات اطلاعاتی در محیط امن الکترونیکی
۱۱. ثبت و بررسی مداوم عملکرد اپراتورها، ورود به برنامه‌های کاربردی و نفوذهای کشف شده

۸ـ نتیجه‌گیری

ارتباط سیستم‌های اسکادای قـدیمی بـا اینترنـت، شـبکه‌هـای خطوط تلفن و استفاده هر چه بیشتر از شبکه‌های کامپیوتری و سیستم‌های بی‌سیم، بیانگر این حقیقت است که تروریست‌هـا، هکرها، کارکنان ناراضی و افراد هوشمند در نقاط مختلف دنیا می‌توانند به مراکز کنترل سیستم‌های قدرت دسترسـی یافتـه و به پارامترهای کلیدی و اقتصـادی کشـورها آسـیب رسـانده و خسارات جبران ناپذیری در بخش‌های مختلف ایجاد نمایند.

در این مقاله برخی نمونه‌ها، ایده‌ها و فعالیت‌های اصلی را که می‌باید در جهت کاستن ریسک تا رسـیدن بـه یـک وضـعیت مطلوب انجام داد، ارائه گردید.

کاهش تهدیدها در حوزه برق نیاز به یک تغییر اساسی در طرز فکر ما نسبت به سیستم، معماری آن، تحقیقات صورت گرفته در مدل کـردن شـبکه‌هـای پیچیـده داشـته و معمـاری آینـده سیستم‌ها مـی‌بایـد بـه سـوی زیرسـاختارهای مسـتحکم‌تـر و سازگارتر حرکت نماید به طوری که این زیرساختارها قادر به خود ترمیمی در پاسخ به تهدیدها، خرابی‌ها و سایر اختلال‌هـا باشند.

مراجع

[1] Edward Wilding, “Information Risk and Security”, Gower Pub., 2006.
[2] Keith Stouffer, Joe Falco, Karen Scarfone “Guide to Industrial Control Systems (ICS) Security” , NIST (National Institute of Standards and Technology) , September 2007
[3] Christos Douligeris , Dimitrios N.Serpanos, “Network Security”, IEEE Press pub., 2007.
[4] Ronald L.Krutz, “Securing SCADA Systems”, Wiley pub., 2006.
[5] Ramesh Subramanian, “Computer Security,Privacy,and Politics” , IRM Press pub., 2008
[6] “SCADA EMS DSM-A part of a corporate it systems,” L. Grasberg, L. O. Osterlund, IEEE/PES Conf. on Power Industry Computer Applications (PICA), Pg 141-147, 2001.
[7] Arjun Venkatraman, “SCADA System Security”
[8] Eric Byres, P. Eng , Justin Lowe , “The Myths and Facts behind Cyber Security Risks for Industrial Control Systems” , 2004
[9] ANSI/ISA 99-00-01, “Security for Industrial Automation and Control Systems” , American National Standard , October 2007
[10] ISO/IEC 18028-2, “Network Security Architecture”, ISO , 2006