به نام خداوند یکتا

مرکز ماهر

نام گزارش:

بررسی آسیب پذیری های امنیتی سامانه های اسکادا و راهکارهای امن سازی آنها

فهرست مطالب

عنوان | شماره صفحه

۱. مقدمه ای بر امنیت اسکادا

۱-۱- مقدمه:

امروزه سیستم های کنترل نظارتی و اکتساب داده، اسکادا (**S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition) 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 امن 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.

متاسفانه در اغلب سیستم های اسکادا، به محیط عملیاتی بطور کامل اعتماد می شود و با فرض وجود یک محیط امن، 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.

سیستم های کنترل نظارتی از معماری سیستم مجزا شده به سمت معماری مبتنی بر شبکه حرکت کرده اند. سخت افزار و نرم افزار استفاده شده در سیستم ها از طراحی و پیاده سازی کاملا" سفارشی به سمت استانداردهای سخت افزاری و پلت فرم های نرم افزاری سوق پیدا کرده اند.

مهم ترین قسمت یک زیر ساخت حیاتی، سیستم شبکه آن می باشد. کار این سیستم جمع آوری بلادرنگ اطلاعات وضعیت سیستم و مخابره کردن اطلاعات سیستم های موجود در نقشه در قالب یک رابط تصویری قابل فهم به مسئول سیستم می باشد. نمونه هایی از این سیستم های زیر ساخت حیاتی را بسته به اندازه ی آن سیستم ها بزرگ مثل شبکه توزیع و انتقال برق هوشمند یا کوچک مثل واحد اندازه گیری فاز در یک شبکه منتقل کننده برق؛ یا یک PLC که کنترل کننده ی یک سیستم بخار یا سرما در نیروگاه برق می باشد. یکی دیگر از مهم ترین قسمت های سیستم های حیاتی سیستم کنترل مرکزی آن می باشد.

در این گزارش ابتدا سیستم های اسکادا معرفی شده، سپس به آسیب پذیری های عمده این سیستم ها اشاره خواهد شد. در بخش های آتی، راه حل هایی که در خصوص امنیت شبکه، پایگاه داده، سیستم عامل و نرم افزارها وجود دارد عنوان می گردد. در بخش جمع بندی راهکارها بیان خواهند شد.

۱-۲- اجزاء سامانه اسکادا

واسط انسان و ماشین (HMI) :

دستگاهی است که نحوه پردازش داده را به یک اپراتور انسانی نشان میدهد و از این طریق، اپراتور انسانی عملکرد ماشین را نظارت و کنترل میکند.

واحدهای پایانه دوردست[۱](RTU):

این واحدها به سنسورها متصل شده، سیگنالهای سنسور را به داده های دودویی تبدیل کرده، و داده های دودویی را به سیستم نظارتی ارسال می کنند.

کنترلر منطقی قابل برنامه نویسی یا PLC[۲]ها :

که مانند مغز متفکر این سیستمها هستند و کارهای اساسی را انجام میدهند. کنترلرها با پرادزش ورودیهای مختلف در مورد نحوه کنترل خروجی ها تصمیم گیری می کنند. آنها اقتصادی تر، تطبیق پذیر و انعطاف پذیر بوده و دارای قابلیت پیکربندی بهتری نسبت به "RTU" های (**پایانه دوردست**) با هدف خاص هستند.

زیرساخت ارتباطاتی :سیستمهای ناظر را به واحدهای پایانه راه دور متصل می سازد.

۱-۳- جایگاه سامانه اسکادا

سیستم های اسکادا به منظور ارائه کردن اطلاعات به صورت بلادرنگ به یک اپراتور انسانی طراحی شده اند و می توانند اطلاعات حالت جاری فرآیندهای فیزیکی و همچنین توانایی تغییر ایجاد کردن در فرآیند از راه دور را به اپراتور ارائه کنند. سیستم های اسکادا در یک سیستم کنترلی توزیع شده معمولا چندین سیستم تعاملی را کنترل می کنند که مسئولیت یک فرآیند محلی را بر عهده دارند.

اما کنترل کننده برنامه پذیر منطقی یا **PLC** یک سیستم نهفته مبتنی بر کامپیوتر است که می تواند تجهیزات صنعتی یا فرآیند ها صنعتی را کنترل کند، و می تواند جریان های اجرایی فرآیندها را نیز می تواند مرتب

---

۱ Remote Terminal Unit

۲ Programmable Logic Controllers

کند. PLCها به همراه اسکادا ؛ جهت اجرای عملیات سرپرستی شده توسط اپراتور اسکادا مورد استفاده قرار می گیرد.

اولین سیستم های کنترل صنعتی مربوط به ۱۹۷۷ هستند که نمی توانستند به یک شبکه خارجی متصل شوند، اما با این حال توانایی متصل شدن به یک شبکه محلی با یک محیط کنترلی بسته را دارند، اما سیستم های کنترل صنعتی فعلی با استفاده از پروتکل TCP/IP به صورت بلادرنگ و اجرا شدن روی اینترنت پشتیبانی می کنند.

۱-۴- مروری بر نا امنی در اسکاداها

امروزه اسکادا همه جا حضور دارد. مردم به دلیل شفافیت و فراگیر بودن آن در زندگی روزانه خود، متوجه آن نمیشوند. اسکادا معمولا توسط برخی شرکت ها و یا کارکنان دولت دور از دسترس مردم،تحت نظارت است. و شامل:

- برقی که به خانه شما وارد می شود
- پمپ های آب که آب را به خانه شما پمپ می کند
- چراغ راهنما
- حمل و نقل عمومی
- تهویه مطبوع در ساختمانی که شما در آن مشغول کار هستید
- تلفن همراهی که استفاده می کنید
- گاز طبیعی که به خانه شما وارد می شود

بسیاری از افرادی که در مورد این سیستم ها اطلاعاتی دارند، یا در صنعت مربوطه مشغول کار هستند یا بر سیستم آنها نظارت می کنند. بنابراین، هنگامی که این سیستم ها توسط هکر ها مورد حمله قرار می گیرند، مردم نوع تاثیر آنها را درک نمی کنند، آنها فقط یک بار درباره آن خبری خوانده و فراموش می کنند.

کارشناسان امنیتی ادعا می کنند که بسیاری از اسکادا ها آسیب پذیر هستند. اغلب احراز هویت در سیستم های اسکادا وجود ندارد. سیستم های اسکادا قدیمی هرگز به روز نشده، و تنها پس از چندین سال جایگزین می شوند. سیستم های جدید در هر ماه وصله امنیتی (اصلاح، رفع آسیب پذیری و مشکل) می شدند. شرکت های در حال استفاده از اسکادا اتصال آن به اینترنت را تکذیب کرده، در حالی که آنها به اینترنت متصل بودند. اسکادا های ساخته نشده برای اتصال به اینترنت، در صورت اتصال آسیب پذیر بودند. نفوذ به اسکادا توسط کارکنان ناراضی آسان بود و حتی از اتصال آنها به اینترنت نیز خطر بیشتری داشت. آزمون های نفوذ کردن، برای تخمین امنیت اسکادا ها، به طور گسترده ای در دسترس هستند و برای انجام آزمایش توسط محققان مورد استفاده قرار می گرفتند. مدیر سیستم و مدیران در شرکت های مختلف اغلب دروغ گفته یا در مورد امنیت آسیب پذیری های

سیستم خود را اطلاعی نداشتند. نقاط دسترسی بی سیم، به عنوان یک مشکل بزرگ، به اثبات رسیده بودند. اگر در یک شرکت دسترسی کافی به شبکه شرکت فراهم نبود، کارکنان اغلب روتر بی سیم خود را به شبکه، بدون حفاظت رمز عبور، متصل می کردند. برخی از شرکت ها شبکه های مختلف، یکی برای آزمایشگاه ها و دیگری برای کارکنان در اختیار داشتند. آنها درک نمی کردند که هر دو شبکه اغلب با هم در چندین نقطه متصل می شد. شرکت هایی با بخش IT اغلب متوجه عدم مطابقت نمودار شبکه خود با پیکربندی واقعی شبکه نمی شدند. کارمندان اجازه اتصال لپ تاپ خود را به صورت فیزیکی و یا از طریق درایوهای USB به شبکه اسکادا، که در نهایت باعث گسترش ویروس ها می شد، داشتند. برخی از سیستم های اسکادا که در تولید نفت و گاز دخالت داشتند کاملا بدون حفاظت بودند. شرکت های بزرگ با وب سایت هیچ جدایی شبکه بین شبکه خصوصی و وب سایت خود را نداشتند. آزمون نفوذ قادر به حمله از طریق وب سایت به سرور خصوصی این شرکت، با استفاده از شبکه آسیب پذیری اصلاح نشده بود. شبکه های خصوصی به سادگی با کلمه عبور به طور پیش فرض راه اندازی شده بودند، چرا که مشتری هرگز زحمت تغییر آن را به خود نداده بود.

اگرچه این سیستم های اسکادا آسیب پذیر به خوبی شناخته شده نیست، اما آنها را به راحتی با نگاه در اینترنت می توان یافت. اسکادا هایی که به صورت الکترونیکی امن هستند گاهی اوقات از نظر فیزیکی نا امن می باشند. برخی ایستگاه های کاری جداگانه، حتی اتصال بی سیم ناامن به اسکادا داشتند. سدها نیز سیستم اسکادا ناامن داشتند، که در آن یک مزاحم (هکر) در واقع می توانست با رهاسازی آب از سد، باعث سیل در مناطق مسکونی شود. مزاحم می تواند سیستم های دیگر سد را نیز مختل کند. آسیب پذیری به اینجا ختم نمی شود. حتی اگر دستکاری تشخیص داده شد بود، اغلب هیچ راهی برای پیگیری کردن این که از کجا آمده وجود نداشت. هیچ احراز هویت کاربری در سیستم وجود نداشت، همه از یک حساب کاربری استفاده می کردند. سیستم های ردیابی اغلب خاموش بودند و یا هرگز فعال نمی شدند. بسیاری از آزمایش های نفوذ انجام شده، توسط محققان دشوار نبودند. محققان دریافتند که بسیاری از سیاست های امنیتی، اجرا نشده بود. کارکنان اغلب در هنگام کار با سیستم از پروتکل پیروی نکرده و یا به سادگی نمی دانستند که سیاست های امنیتی وجود دارد. آنها همچنین دریافتند که این حوادث جدا از هم نیست، اقدام امنیتی یا به طور کامل وجود نداشت و یا فاقد یک راه یا دیگری بود.

همانطور که قبلا ذکر شد، سیستم های اسکادا برای کنترل و نظارت کردن بر روی فرآیند های صنعتی مورد استفاده قرار می گیرند, به عنوان مثال سیستم های اسکادا در انتقال برق، جریان نفت و گاز در لوله ها یا چاه ها، توزیع آب، مدیریت مواد زائد، سیستم های حمل و نقل، چراغ های کنترل ترافیک و دیگر سیستم های اساسی جامع مدرن استفاده می شوند.

یک حمله تایید شده در سال ۲۰۱۵ به خطوط انتقال برق اوکراین اتفاق افتاد که ۵۷ ایستگاه برق در غرب اوکراین را به خاموشی فرو برد. در اولین بررسی نتیجه را دخالت در سیستم نظارت یکی از شرکت های آسیب

دیده نسبت دادند که بعداً معلوم شد که در نتیجه حمله ی هکر به سیستم های کنترل صنعتی انجام شده است و در نهایت در ۴ ژانویه ۲۰۱۶ توسط CERT –UA تایید شد. این یک حمله ی پیچیده و با طراحی خیلی خوب بود، و در ۳ مرحله انجام شد: در گام اول آلوده کردن سیستم ها از طریق email کردن یک فایل word آلوده به ماکروهای مخرب. در گام دوم جلوگیری از حذف و بازیابی فایل ها به وسیله پاک کردن فایل های سیستمی از روی سیستم کنترل. پس از آن به وسیله ی تماس های تلفنی جعلی به مرکز سرویس های مشتریان شرکت های مختلف تولید قدرت (برق)، در نتیجه شرکت ها را برای بررسی و پیدا کردن دلیل اصلی مشکل به تاخیر می انداختند. بدافزار استفاده شده در این حمله به خانواده بدافزار های BlackEnergy مرتبط می باشد.

دو تهدید مجزا برای یک سیستم کنترل زیرساخت مدرن وجود دارد که آنها را در اینجا بررسی خواهیم کرد:

اولین نوع تهدید برای سیستم های زیرساخت، دسترسی به برنامه های کنترلی بدون احراز هویت است؛ مانند دسترسی گرفتن انسان به سیستم های زیرساخت کنترلی یا تغییر در فرآیند کنترل توسط نفوذ یک ویروس و دیگر تهدیدات که مبتنی بر نرم افزار است. دومین نوع تهدید برای سیستم های زیر ساخت دسترسی گرفتن به بسته های شبکه ابزار میزبانی اسکادا است. در بیشتر حالات، مکانیزم های امنیتی ابتدایی، مثل Modbus یا هیچ نوع مکانیزم امنیتی در پروتکل های کنترل بسته سیستم های اسکادا وجود ندارد .اما با این تفاصیر، هر کسی که بتواند بسته ای به دستگاه های اسکادا یا هر سخت افزار صنعتی ارسال کند می تواند به سادگی کنترل شود.(از پروتکل های بی سیم یا پروتکل های صنعتی از قبیل Modbus یا DNP3 یا TCP/IP)

بعضی افراد در این تصور هستند که وجود یک شبکه VPN این امنیت را برایشان ایجاد می کند اما غافل از اینکه هر کس که به سوئیچ هایی که به دستگاه اسکادا وصل است و دسترسی فیزیکی داشته باشد،می تواند بدون احراز هویت به سیستم وصل شود. راه حل پیشنهادی استفاده از احراز هویت نقطه پایانی به نقطه پایانی (EndPoint To EndPoint Authentication) حل می شود و راه حل دوم استفاده از رمزنگاری است.

حمله به سیستم های اسکادا برای سلامتی انسان ها نیز تهدید محسوب می شود زیرا همان طور که مطلع هستید هدف حمله سیستم های زیرساخت های حیاتی یک کشور می باشد، به عنوان نمونه به آزمایشی که به نام انفجار سرخ شفق (Aurora Explosion) به درخواست DHS یا سازمان امنیت داخلی آمریکا صورت گرفت اشاره می کنیم آزمایش این حمله، در ماه مارس توسط آزمایشگاه ملی اوهایو برای DHS و در طی آن یک ضعف امنیتی که در برنامه نویسی سیستم های اسکادا کنترل الکتریکی آب و کارخانه های شیمایی در آمریکا موجود بود، اکسپلویت شد. مقصود از این آزمایش نمایش دادن حملات راه دور توسط هکر ها به منظور ایجاد تخریب در سیستم های صنعتی بود. اتاق ژنراتور در آزمایشگاه ملی اوهیاو که توسط یک متخصص امنیت(جهت آزمایش واقعی)مورد دسترسی قرار گرفته بود .یک میلیون دلار قیمت دستگاه مورد نفوذ قرار گرفته است.

برای محافظت سیستم های اسکادا؛ در سال ۲۰۰۷ یک جامعه ی بین المللی اتوماسیون اقدام به ایجاد دستور العمل های امنیتی در قالب یک کارگروه به نام WG4 کرد.

در مقاله ای به نام اسکادا security and terrorism : we're not crying wolf به حمله ای به یک نیروگاه برق با استفاده از ضعف امنیتی RPC DCOM اشاره می کند. با استفاده از RPC برنامه های موجود بر روی یک کامپیوتر قادر به اجرای روتین هایی در کامپیوتر دوم از طریق ارسال داده و بازیابی نتایج می باشند. با توجه به جایگاه عملیاتی RPC، استفاده از آن بسیار متداول بوده و درموارد متعددی از آن بمنظور ارائه سرویس های توزیع شده شبکه نظیر مدیریت از راه دور، اشتراک فایل NFS و NIS استفاده می گردد. وجود ضعف های امنیتی متعدد در RPC باعث بهره برداری مهاجمان بمنظور انجام حملات مختلفی شده است.دراکثر موارد، سرویس های RPC با مجوزهای بیش از حد معمول، اجراء می گردند. بدین ترتیب یک مهاجم غیر مجاز قادر به استفاده از سیستم های آسیب پذیر در جهت اهداف خود خواهد بود.اکثر حملات از نوع DoS در سال ۱۹۹۹ و اوایل سال ۲۰۰۰ در ارتباط با سیستم هائی بود که دارای ضعف امنیـتی و نقطه آسیب پذیر RPC بودند. مثلا" حملات گسترده و موفقیت آمیز در رابطه با سیستم های نظامی امریکا، بدلیل نقطه آسیب پذیر RPC کشف شده در صدها دستگاه کامپیوتر مربوط به وزارت دفاع امریکا بوده است. اخیرا" نیز وجود یک ضعف امنیتی DCOM RPC در ویندوز، باعث انتشار گسترده یک کرم در سطح اینترنت گردید.

تمامی نسخه های یونیکس و لینوکس که بر روی آنان سرویس های RPC نصب شده است در معرض این آسیب می باشند. سرویس های RPC، عموما" از طریق حملات سریز بافر، مورد سوء استفاده قرار می گیرند. علت این امر، عدم انجام بررسی لازم و کافی در خصوص خطاها و یا اعتبار داده های ورودی توسط برنامه های RPC است. نقاط آسیب پذیر سریز بافر، این امکان را برای یک مهاجم فراهم می نماید که داده غیر قابل پیش بینی را (اغلب بصورت کد مخرب) به درون حافظه برنامه ارسال نماید. با توجه به ضعف موجود در رابطه با بررسی خطاء و صحت داده، داده ارسالی مکان هائی حساس و کلیدی که مورد استفاده پردازنده می باشند را بازنویسی می نماید.در یک تهاجم موفقیت آمیز سریز، کد مخرب ارسالی، در ادامه توسط سیستم عامل اجراء می گردد. با توجه به اینکه تعداد زیادی از سرویس های RPC، با مجوزهای بیش از حد معمول، اجراء می گردند، استفاده موفقیت آمیز از نقاط آسیب پذیر فوق می تواند امکان دستـیابی غیر مجاز و از راه دور را به سیستم فراهم می نماید.

در بعضی مواقع معرفی و بررسی کردن این مشکلات و خطا ها خود دلیلی برای ایجاد مشکل و حمله خواهد شد زیرا راه های حمله و نقاط ضعف، ایده ای جدید به هکر ها خواهد داد مثل اتفاقی که در روشن سازی مشکل سیستم هایی که Modbus بر روی آنها فعال بود افتاد و توسط شخصی به نام Daniel Grzelak درمورد انجام فازینگ بر روی دستگاه های Modbus از قبیل تغییر دادن کدهای توابع و Transaction ID در پروتکل Modbus استفاده می کرد.

۲. آسیب پذیری امنیتی اسکادا

اکثر نمونه های نصب شده از سیستم های اسکادا هم اینک از پروتکل هایی استفاده می نمایند که ذاتا" غیرامن هستتند و یا توسط تولید کنندگان محصولات اسکادا به خوبی پیاده سازی نشده اند. این وضعیت سیستم های اسکادا را غیرامن می سازد. برای مثال ممکن است، با بکارگیری یک برنامه ساده پویش پورت در یک شبکه اسکادا، تمامی شبکه دچارمشکل شود چراکه نحوه برخورد با خطاء به خوبی پیاده سازی نشده است. اولین مرحله، در شناخت خطرات مرتبط با اسکادا در دنیای دیجیتال و اتوماسیون امروز، پذیرش این واقعیت است که سیستم های اسکادا به منظور کار در یک محیط بسته طراحی شده اند. با این که اغلب سازمان ها ادعا می نمایند که سیستم اسکادا آنها به شبکه آنها متصل نمی باشد، تخمین زده می شود که بین ۸۰ تا ۹۰ درصد سیستم های اسکادا در برخی کشورهای صنعتی به شبکه های بزرگ سازمان مربوط به خود متصل هستند. همین وضعیت باعث شده است که مهاجمان بتوانند حملات خود را متوجه سیستم های اسکادا نمایند. ضعف های سطح بالا که امروزه در سیستم های اسکادا یافت می شود شامل موارد ذیل است: الف) نیاز به هیچگونه تاییدیه ندارند ب) نیاز به هیچگونه مجوزی برای انجام کار ندارند. ج) از رمزنگاری استفاده نمی نمایند. د) به صورت مناسبی با خطا و اتفاقات غیرقابل پیش بینی برخورد نمی نمایند.

سیستم های کنترل ازداخل وخارج ازشبکه سیستم کنترل، در برابر حمله سایبری آسیب پذیرند. برای درک آسیب پذیری های مرتبط باسیستم های کنترل باید نوع ارتباط وعملیات مرتبط باسیستم کنترل را دانست. همچنین باید متوجه بود که چطور مهاجمان ازآسیب پذیری های سیستم درجهت منافع خوداستفاده می‌کنند.

- ✓ درک آسیب پذیری سایبری سیستم کنترل
- ✓ دسترسی به سیستم کنترل LAN[1]
  - معماری رایج شبکه
  - دسترسی به RTU ها به روش dial-up
  - پشتیبانی فروشنده
  - ادوات کنترل ارتباط IT[2]
  - VPNs[1] سازمانی

[1] Local Area *Network*
[2] Information Technology

- لینک های پایگاه داده
- ضعف تنظیمات فایروال ها
- یکسان سازی لینک های ابزارهای نظیر

✓ کشف فرآیند

✓ کنترل فرآیند

- ارسال دستورات بطور مستقیم به تجهیزات اکتساب داده
- Export کردن صفحه HMI[۲]
- تغییر پایگاه داده
- حمله های مردی در میان [۳]

۲-۱- سیستم عامل های اسکادا

سیستم عامل های اسکادا یا از اصول کلی سیستمهای DCS پیروی می کند.گرچه هردو سیستم بر پایه یک هدف بنا شده اند. تفاوتهای عمده ای نیز باهم دارند از جمله این تفاوتها می توان به نوع کاربرد و کارآیی این سیستمها اشاره کرد.سیستم اسکادا همانطور که از نام آن پیداست یک سیستم کنترل کامل نیست بلکه جهت ارائه مدیریت نظارت و بررسی برکنترل و جمع آوری اطلاعات طراحی شده و اهداف اولیه و طراحی و تولید آن عبارتند از مونیتورینگ، مدیریت در تصمیم گیری در کنترل و اعلام اخطار و آلارم در مواقع مورد نیاز از طریق یک مرکز واحد می باشد.

هسته اصلی این سیستم بسته های نرم افزاری حرفه ای هستند که برروی سخت افزار ها استاندارد و مشخصی از قبیل PLC ها ویا RTU((Remote Terminal Units)قرار گرفته اند.

سیستم اسکاداعلاوه بر کاربرد در فرایندهای صنعتی مانند تولید و توزیع برق (به شیوه های مرسوم یا هسته ای)،ساخت فولاد، صنایع شیمیایی،صنایع آب،گاز و نفت در بعضی از امکانات آزمایشی مانند فوزیون هسته ایی نیز کاربرد دارد.اندازه اینچنین تاسیساتی از ۱۰۰۰تا چندین ده هزار کانال I/O می باشد. و با کمک شبکه ها و سیستمهای مخابراتی منطقه وسیعی را تحت بازرسی ونظارت قرار می دهد.

---

۱ Virtual Private Network

2 Human-Machin Interface

3 Man-in-the-Middle

سیستمهای اسکادا بر روی سیستم عاملهایDOS ،VMSوUNIX قابل اجرا هستند در سالهای اخیر همه سیستم های اسکادابه سمت سیستم عامل NT و بعضی هم بسمتLinux گرایش پیدا کرده اند.

- **معماری سیستم عامل**

نرم افزار های سیستم اسکادا بر پایه تکنولوژیهای Multitasking و Real Time استوار شده است وسیستم بانک اطلاعاتی آن نیز(RTDB(Real-Time Data Bus ،نام دارد که برروی یک یا چند Serverهمزمان پیاده سازی و اجرا می شود Serverسیستم وظیفه پاسخگویی به اعمال مشخص مانند : polling controllers،alarm checking،calculation، (logging and archiving)را بر عهده دارند.

در عین حال امکان تخصیص یک Server به اعمال خاصی مانندAlarm checking،datalogger، historian وجود دارد.

ارتباط بین field و client از طریق روشهای polling انجام می شود. بدین ترتیب که Data Server پارامتر مورد نظر خود را از کنترلر در خواست کرده وآنرا می خواند، کنترلر نیز در این زمان پارامتر مورد نظر را بهServer ، ارسال می کند.سرعت polling برای پارامترهای مختلف، متفاوت است.

مرکز کنترل اسکادا، به لحاظ اهمیت فرایند تحت کنترل، بصورت Redundant پیاده سازی می گردد. بدین صورت که جهت افزایش تحمل پذیری سیستم، به ازای هر جزء یا برخی از اجزای کلیدی، اعم از سخت افزار یا نرم افزار، یک یا چند جزء Stand by اضافه می گردد و در صورت بروز خطا در جزء اصلی، قسمتStand by ، ادامه فعالیت را به عهده می گیرد سیستمهای Stand by به سه دسته تقسیم می شوند:

به عبارت دیگر در صورت بروز برخی حوادث نا خواسته، کار سیستم، مختل نمی گردد. بلکه با درجه کمتری از کارایی (Graceful Degradation)استفاده می شود.

Alarm Handing:

هر اتفاقی که باعث تغییر وضعیت یکی از اجزا تحت کنترل گردد یک رویداد نامیده می شود رویدادهایی که نیاز به اعلام به اپراتور و عکس العمل وی را داشته باشد آلارم نامیده می شود. آلارم علاوه بر ثبت در فایل،

منجر به ایجاد فعالیتهای دیگر نظیر چاپ بر روی چاپگر، ایجاد آژیر صوتی و چشمک زدن شی مورد نظر و... می گردد.

Alarm handing اعمال مربوط به درک وضعیت اضطراری و تولید سیگنال آلارم را برعهده داردکه در یک Data Server انجام می گیرد.

آلارمها از نظر منطقی بصورت متمرکز اداره می شوند، اطلاعات فقط در یک محل وجود دارند و همه کاربران وضعیت های مشابه می بینند، و چندین آلارم بر اساس سطوح اولویت و اهمیت پشتیبانی می شوند.

Logging/Archiving

Logging/Archiving به جمع آوری اطلاعات مربوط به سطوح دسترسی کاربران در زمانهای مشخص به منابع سیستم می پردازند و این اطلاعات را به شکل یک فایل Archive نگهداری می کنند.ثبت رویداد ها می تواند به عنوان ذخیره میان مدت داده روی دیسک صورت گیرد در حالیکه نگهداری و بایگانی اطلاعات در بلند مدت روی دیسک ذخیره می شود.

ایجاد گزارش اسکادا با استفاده از SQL گزارشهایی را برای Archive،RTDBیا Logsفراهم می کند.با وجود اینکه درج جدولهای EXCELدر گزارش ا مکانپذیر است اما قابلیت "cut and paste" بطور کلی فراهم نشده است. امکانات موجودقادر به ایجاد،چاپ و آرشیو (بایگانی) گزارش ها به طور اتوماتیک هستند.

۲-۲- آسیب پذیری های متداول بر روی سیستم عامل های صنعتی

- **Backdoor**

درب پشتی (به انگلیسی (Backdoor :به راهی گفته می‌شود که بتوان از آن بدون اجازه به قسمت/قسمت‌های مشخصی از یک سامانه مانند رایانه، دیوار آتش، یا افزاره‌های دیگر دست پیدا کرد. درهای پشتی ممکن است از قبل در سامانه وجود داشته باشند یا اینکه فرد نفوذگر با فریب کاربر، او را نسبت به نصب در پشتی ترغیب کند (مانند ارسال پیوست‌های آلوده در رایانامه). درهای پشتی را به سه دسته فعال، غیرفعال و حمله بنیان تقسیم می‌کنند .

- درهای پشتی‌ای که منتظر رسیدن دستورات از طریق درگاه‌ها می‌شوند را غیرفعال می‌نامند.
- درهای پشتی فعال خودشان آغازگر ارتباط با میزبان‌های دیگر هستند .

- درهای پشتی حمله‌بنیان به درهایی گفته می‌شود که با استفاده از حمله‌ای مبتنی بر کدهای مخرب به دسترسی‌های لازم می‌رسند.

○ حمله Zero Day Attack

نوعی از خرابکاری است که عمدتاً با استفاده از ضعف های موجود در سیستم عامل ها و نرم افزارهای کاربردی اتفاق می افتد. علت نام گذاری به "حمله صفر" این است که حملات در زمان صفر قبل از آگاهی توسعه دهندگان نرم افزارها اتفاق می افتد. در واقع زمان صفر، فرصتی برای حمله کنندگان از زمان افشاء شدن یک حفره امنیتی در نرم افزارها تا زمان صدور اولین patch بروز رسانی توسط توسعه دهنده برای رفع این مشکل است. بیشتر کسانی که این حملات را سازماندهی میکنند گروه های برنامه نویسی نسبتاً پیشرفته و بزرگی هستند که با مطلع بودن از اشکلات و حفره های امنیتی در کدهای موجود در نرم افزار،که حتی توسعه دهندگان و کاربران، از آنها آگاهی ندارند سوء استفاده و اقدام به خرابکاری میکنند.

این زمان بسیار مهم است. ازاینرو که سرعت بروز رسانی توسعه دهندگان نرم افزارها و رفع اشکالات سیستم هایشان ممکن است کند بوده و در این فاصله، افرادی سود جو اقدام به حمله از طریق این ضعف ها نمایند. حتی این کندی در بروز رسانی، بعضاً در نرم افزارهایی که از بزرگترین سازندگان و توسعه دهندگان دنیا نظیر مایکروسافت و گوگل هستند نیز دیده می شود. در بسیاری از موارد، توسعه دهندگان نرم افزار بلافاصله متوجه مشکلات سیستم خود میشوند، ولی بدلایلی از قبیل; زمان، هزینه و کم اهمیت بودن مشکل، توسعه نسخه جدید را به تعویق می اندازند. گاهاً توسعه دهندگان صبر میکنند که تعداد زیادتری از مشکلات کشف شده و سپس در یک نسخه واحد مرتفع شوند. در صورتی که این احمال میتواند بسیار پر خطر باشد و امنیت و اطلاعات بسیاری از استفاده کنندگان آن نرم افزارها را به خطر بیاندازد.

حملات ZeroDay عمدتاً برای رساندن بیشترین آسیب در یک روز طراحی میشوند. آنها از یک پنجره و قسمت که عمدتاً به Vulnerability Window یا پنجره آسیب پذیری است شروع میکنند و کم کم به تمامی نقاط گسترش پیدا میکنند. این حملات میتوانند از یک دوره کوتاه تا چندین سال در تناوب باشند.

○ بمب منطقی

قطعه‌ای کد است که عمداً دریک سیستم نرم‌افزاری درج شده‌است که به هنگام وقوع شرایط مشخص عملیات مخربی را اجرا می‌نماید. به عنوان مثال، یک برنامه نویس ممکن است قطعه‌ای کد را که شروع به حذف فایل‌ها می‌کند را پنهان کند. نرم‌افزاری است که ذاتاً مخرب است مانند ویروس‌ها و کرم‌ها، و اغلب

شامل بمب‌های منطقی که (payload) معینی را در یک زمان از پیش تعریف شده و یا شرایط معین دیگرری که به وقوع بپیوندد اجرا می‌کند. این تکنیک می‌تواند برای یک ویروس یا کرم برای رسیدن به شتاب و گسترش پیش از شناسایی استفاده می‌شود. بسیاری از ویروس‌ها، به سیستم‌های میزبان خود در تاریخ‌های مشخص حمله می‌کنند، مانند جمعه ۱۳ام ماه آوریل. تروجان‌ها نیز که اغلب به نام "بمب زمانی" نامیده می‌شوند هم در تاریخ خاصی فعال می‌شوند. به منظور به اجرا درآوردن یک بمب منطقی،(payload) باید به طور ناخواسته و ناشناخته برای کاربر نرم‌افزار در نظر گرفته شود. به عنوان مثال، برنامه‌های آزمایشی با کد که قابلیت‌های خاصی از آنها پس از زمان تعیین شده غیر فعال می‌شوند به عنوان بمب‌های منطقی درنظر گرفته نمی‌شوند.

نمونه: در سال ۱۹۸۲ درخط لوله ترانس سیبری حادثه‌ای رخ داده‌است که علت آن بمب منطقی گزارش شده‌است. کارگزار شرکت (KGB)ادعا کرده بود که برنامه‌های سیستم کنترل و نرم‌افزار آن از یک شرکت کانادایی که برای استفاده در خط لوله سیبری بوده دزدیده شده‌است. سیا (CIA) ظاهراً اسناد محرمانه موجود در پرونده تودیع آنان را به دست آورده و دریافته بود که این شرکت با استفاده از یک بمب منطقی در این برنامه اهداف خرابکارانه‌ای داشتند. در نهایت آن به "غیر هسته‌ای ترین انفجار و آتش که تا به حال از فضا دیده می‌شود " منجر شد.

۳. راه حل های پیشنهادی

همانگونه که مشخص گردید توجه به مسائل امنیتی در حوزه اسکادا بسیار مهم است. در این گزارش به برخی از مسائل مهم تر در حوزه نفوذ در سیستم های اسکادا توجه گردید. با توجه به طبقه بندی امنیتی سیستم های اسکادا می توان در مکان های که نصب سیستم های خارجی مشکل اساسی برای کشور ایجاد نخواهد کرد پکیج‌های سخت افزاری- نرم افزای برای جلوگیری از نفوذ در این سامانه ها تهیه کرد در حالیکه برای مکان های بسیار حساس استفاده از سیستم های اسکادای بومی تنها راه حل برای این مورد است.

۳-۱- بهبود اسکادا های موجود

اسکادا های قدیمی نباید به دلیل قدیمی بودن، به سادگی ناامن تلقی شوند. اسکادا را می تواند تا حدی به روز رسانی کرد تا به نرم افزار های امنیتی بین مانیتور کارمند و ماشین آلات، مجهز شود. خروجی بسیاری از ماشین آلات می تواند به طور مستقیم به یک کنترلر تعبیه شده با نرم افزار های امنیتی که اطلاعات امن را به مانیتور کارمند می فرستد، هدایت شود. دستگاه های فیزیکی باید پس از آن، قفل شده تا دسترسی فیزیکی مزاحم به سیستم دشوار باشد.

۳-۱- اعمال سیاست های امنیتی

بسیاری از سیستم های اسکادا به سادگی می توانند امن تر شوند اگر شرکت،کارکنان IT صلاحیت دار که به طور منظم شبکه اسکادا را چک می کنند، داشته باشد. ابزار آنلاین برای بررسی آسیب پذیری ها وجود دارد و هیچ بهانه ای برای انجام ندادن این کار وجود ندارد. مدیریت این شرکت ها به وضوح باید گام بردارد و کارکنان خود را موظف به پیروی از پروتکل در هنگام کار کردن با سیستم های اسکادا خود نماید. از آنجا که سیستم های اسکادا، در حال حاضر اغلب از شبکه های کامپیوتری متداول استفاده می کنند، هیچ مشکلی برای امن کردن شبکه های اسکادا همانند شبکه های کامپیوتری نباید وجود داشته باشد. فروشندگان نیز می تواند با مراحلی مانند نیاز به تغییر رمز عبور اجباری و تنظیم مجدد آن هنگامی که مشتریان محصول خود را خرید می کنند، به امن کردن سیستم، کمک کنند. شرکت ها می تواند کارکنان خود را از متصل کردن درایوهای USB از یک کامپیوتر به کامپیوتر دیگر، برای جلوگیری از انتشار ویروس منع کنند. سیستم اسکادا همچنین باید حساب های تمام

کارکنان را پیگیری و نگهداری کند و همه کارکنان باید حساب کاربری خود را داشته باشند. بدیهی است که شبکه‌های خصوصی باید خصوصی بمانند و یک کامپیوتر نباید قابلیت دسترسی به شبکه های متعدد در یک شرکت را داشته باشد. در نهایت، حساب کاربری کارمندان سابق باید برای جلوگیری از اقدامات تلافی جویانه، بلافاصله از سیستم حذف شود.

۳-۲- سیاست های امنیتی پویا از طریق روش اکتشافی

برای جلوگیری از رخنه های امنیتی، حتی در سیستم های جدیدتر امن، شبکه اسکادا را می توان با درک محیط اطراف آن تنظیم(سفارشی) کرد. اگر سیستم اسکادا در یک محیط تولید گاز طبیعی مستقر شده باشد، یک کامپیوتر می تواند به ردیابی تمامی سنسورها اقدام کرده و از هر یک از دستورات که ثبات سیستم را به خطر اندازد، جلوگیری کند. به عنوان مثال، یک کامپیوتر نظارت بر دریچه ها و مخازن مختلف و ارتباط بین دریچه و فشار مخزن را بررسی می کند. اگر یک کارمند اقدام به وارد کردن هر دستوری که می تواند یک شکست را آغاز کند نمود، کامپیوتری که کنترل مقادیر را به طور مستقیم بر عهده دارد، باید دستور را رد کند. پس از آن دستور نامعتبر باید در یک پایگاه داده مرکزی ثبت شود.

پایگاه داده متمرکز باید سیاست کاربری چند سطحی داشته باشد که کارکنان را به سطوح دسترسی مختلف تقسیم کند. دسترسی سطح پایین یا می تواند تغییرات جزئی در سیستم های غیر حساس اعمال کند یا فقط خواندنی است. دسترسی بیشتر به سطوح بالاتر و بالاتر داده می شود. جزئیات دسترسی، به محیطی که سیستم در آن مستقر شده بستگی دارد. پایگاه داده نیز دستورات اجرا شده کارمند را نگه می دارد و یک تاریخچه از آن را برای مشاهده توسط مدیران تولید می کند. پایگاه داده، خود نیز اجازه یا رد تغییرات به سیستم را بسته به رفتارهای گذشته کارمند، می دهد. اگر کارمندی توانایی (دسترسی) یک تغییر معتبر به سیستم را ندارد، مدیر می تواند آن را با دسترسی بالاتر تایید کند. این امر نیز می تواند ثبت شود و در روند دستورات کارمند قرار داده شود. اگر این نوع از تغییر در سیستم اغلب به دفعات اتفاق افتد، پس از آن سیاست امنیتی تغییر خواهد کرد تا اجازه دهد که کارمند دسترسی دائمی به تغییر سیستم، بدون نیاز به تایید صریح مدیر در هر زمان را داشته باشد.

این سیستم از ارسال دستورات مهلک توسط مزاحمان جلوگیری می کند چرا که حتی اگر مزاحم به کامپیوتر دسترسی پیدا کرد، کامپیوتر به خودی خود دستور را رد می کند. اگر مزاحم به جعل مجوز یک کارمند قادر بود، پایگاه داده اکتشافی، دستور عجیب و غریب را پیدا کرده و آن را رد خواهد کرد.

۳-۳- اعمال کنترل دسترسی در اسکادا

از آنجا که یکی از نقاط ضعف اساسی سیستم های صنعتی نبود سیاست ها مشخص در تعیین و پیاده سازی سطوح مختلف دسترسی است در این قسمت مروری بر روش های تعیین این سطوح می کنیم.

اصطلاح کنترل دسترسی به کنترل بیشتر بر روی دسترسی به منابع سیستم اشاره دارد یعنی فرض را بر این می گذاریم که هویت کاربر مورد تایید قرار گرفته است و اکنون چگونگی نحوه دسترسی کاربر به منابع باید کنترل گردد.

در محیط رقابتی امروز، تامین امنیت داده ها و تعیین نحوه دسترسی به آنها بصورت حداقل لازم (leat privilege)،یکی از مباحث لازم و ضروری می باشد، به همین منظور راهکارها و مدل های متفاوتی ارائه شده است.

انواع مدل های کنترل دسترسی

- کنترل دسترسی اجباری(Mandatory Access Control-MAC)
- کنترل دسترسی اختیاری(Discretionary Access Control-DAC)
- کنترل دسترسی مبتنی بر نقش(Role Based Access Control-RBAC)

اما توجه داشته باشید یک مدیر، طراح و یا تحلیلگر همیشه بر اساس نیازها و قابلیت های تعریف شده برای محیط کاری خود، مدلی را انتخاب می نماید.

○ کنترل دسترسی اجباری(Mandatory Access Control-MAC)

در این مدل اشیاء تشکیل دهنده هر کدام از منابع سیستم کاملا مشخص می گردند و به هر شی برچسب امنیتی اختصاص داده می شود. هر کدام از این برچسب ها شامل اطلاعات زیر می باشند که بصورت هارد کد در برنامه مشخص می شوند:

طبقه بندی اطلاعات بصورت بسیار سری، محرمانه و.(classification) ..

تعیین گروه هایی که می توانند به این شی دسترسی داشته باشند مثلا مدیران، مسئول پروژه و. .. (categoriess) به طور مشابه کاربران سیستم هم دسته بندی می شوند یعنی مشخص می گردد هر کاربر در چه طبقه ای از اطلاعات و در چه گروهی قرار دارد.بدین ترتیب هر زمان کاربری بخواهد به یک شی

دسترسی داشته باشد، برچسب امنیتی شی را با مشخصات کاربری، مورد مطابقت قرار می دهند و نتیجه آن وضعیت دسترسی کاربر را مشخص می نماید. توجه داشته باشید که حتی اگر کاربری در طبقه اطلاعات سری قرار گیرد اما در گروهی باشد که در گاتالوگ شی نیامده است، مجوز دسترسی به او داده نمی شود. البته کاربری که در بالاترین سطح دسترسی قرار دارد، مجوز دسترسی به اطلاعات سطوح پایین تر از خود را هم دارد. یعنی رابطه سطوح بصورت سلسه مراتبی می باشد.

در این روش امنیت تا حد بالایی لحاظ می شود اما کم هزینه هم نیست، چرا که اولا باید دقت زیادی صرف مشخص نمودن تمامی اشیاء سیستم و طبقه بندی آنها شود و ثانیا بعد از پیاده سازی، تمامی درخواست ها مبنی بر بروزرسانی کردن اشیاء و برچسب های آنها و یا تغییر موقعیت یک کاربر و سطح دسترسی آن، به مرکز مدیریتی ارسال می گردد که برای محیط های بزرگ و پویا بسیار وقت گیر خواهد. یکی دیگر از محدودیت های این مدل این است که کاربران نمی توانند داده های خود را به اشتراک بگذارند چرا که همه دسترسی ها از قبل و بصورت ایستا مشخص شده اند.

- **کنترل دسترسی اختیاری(Discretionary Access Control-DAC)**

برخلاف کنترل دسترسی اجباری که در آن دسترسی به منابع توسط سیستم عامل و تحت کنترل مدیر سیستم صورت می گیرد، مدل کنترل دسترسی اختیاری به هرکاربر این اجازه را می دهد که نحوه دسترسی به داده های خود را تحت کنترل داشته باشد.

در این مدل دیگر از برچسب امنیتی استفاده نمی شود بلکه برای هر شی یک لیست کنترل دسترسی) (Access Control List، تعریف می گردد که شامل فهرستی از کاربران و گروه هایی که به کاربر اجازه دسترسی می دهند و سطح دسترسی برای هر گروه، می باشد.. یکی از مزایای این روش امکان به اشتراک گذاشتن دیتاها است، مثلا کاربر A می تواند اجازه فقط خواندن را در مورد فایل خود، به کاربر B بدهد.

در این مدل تعریف لیست کنترل دسترسی می تواند بصورت متمرکز و یا توزیع شده باشد. در روش متمرکز، تنها مدیر سیستم می تواند لیست دسترسی ها را بروز رسانی نماید اما در مدل توزیع شده چنانچه مدیر مجوز تعریف و بروزرسانی لیست را به کاربری بدهد، او هم می تواند این تغییرات را اعمال نماید.

این روش برای سازمان های بزرگ و پویا به دلیل قابلیت انعطاف پذیری و صرفه جویی در وقت، مناسب می باشد،البته از لحاظ امنیتی در سطح پایین تری نسبت بهmac ، قرار دارد چرا که ممکن است حق دسترسی ای به کاربری داده شود در حالیکه مورد نیاز او نمی باشد.

- **کنترل دسترسی مبتنی بر نقش(Role Based Access Control-RBAC)**

با توجه به اینکه این مدل قابلیت استفاده در محیط های صنعتی را دارد بیشتر به آن پرداخته می شود.

با توجه به عدم انعطاف پذیری مدل کنترل دسترسی اجباری و کنترل دسترسی اختیاری، مفهوم امنیتی نسبتا جدیدی با عنوان کنترل دسترسی مبتنی بر نقش توسط موسسه ملی استاندارد و فناوری (NIST) مطرح گردید.

در روش کنترل دسترسی مبتنی بر نقش، حق دسترسی ها بستگی به عملیاتی دارد که کاربران در سازمان می توانند انجام دهند. در این مدل مجوز ها به نقش های تعریف شده اختصاص داده می شوند و سپس نقش هر کاربر در سازمان مشخص می گردد. به عنوان مثال کاربر حسابدار یک شرکت، نقش حسابداری به او انتصاب داده می شود از این طریق کاربر می تواند از مجوزهای تعیین شده برای نقش حسابدار، استفاده نماید.بدین ترتیب اگر شرکت دارای چند حسابدار هم باشد، همه آنها دقیقا حق دسترسی های یکسانی خواهند داشت. کنترل کاربران در این مدل به سادگی امکان پذیر است، چرا که می توان به کاربران تنها با انتصاب نقش جدید و یا انتقال به نقش دیگر، حق دسترسی های جدید داد. از طرفی با اختصاص دادن یک مجوز جدید به یک نقش و یا گرفتن مجوزی از یک نقش، تمامی کاربرانی که آن نقش به آنها انتصاب داده شده است، موقعیت جدیدی در مورد حق دسترسی ها پیدا می کنند.

اجزاء تشکیل دهنده این مدل عبارتند از:

شی : (object) موجودیتی که حاوی اطلاعاتی باشد که نیاز به تعیین دسترسی (محافظت) دارند.

عمل : (operationn) مجموعه عملیاتی که میتوان بر روی یک آبجکت انجام پذیرد و نیاز به تعیین دسترسی (محافظت) دارد.

مجوز: (permission) بررسی امکان انجام عمل بر روی یک آبجکت و دادن اجازه انجام آن.

نقش / جایگاه : (rolee) بیانگر موقعیت شغلی در قالب چهارچوب سازمانی است و توضیحی در رابطه با اختیارات و مسئولیت ها در این موقعیت.

کاربر : (user) شخصی است که مجاز به استفاده از قسمت¬هایی از نرم¬افزار می¬باشد. این شخص به جز انسان می تواندیک قطعه نرم افزاری هم باشد.

جلسه : (session) مشخص می¬کند که کاربر با کدام(یک یا چند) از نقشهای خود در حال فعالیت در سیستم می باشد. هر کاربر می تواند دارای چندین session باشد وی هر session تنها به یک کاربر اختصاص داده می شود.

تفکیک وظایف : تفکیک وظایف برای جلوگیری از ایجاد تضاد بین قوانین حاکم در یک سازمان، است. ایجاد تضاد بین قوانین تعریف شده، ممکن است در اثر انتصاب چند مسئولیت به یک نفر و یا فعال شدن یک نفر با چند نقش بصورت همزمان، بوجود آید. تفکیک وظایف به دو صورت امکان پذیر می باشد:

ایستا :(SSD) چنانچه مسئولیت های a و b هر کدام عملیاتی را انجام دهند که انتصاب آنها به یک نفر سبب شود قوانین امنیتی سازمان خدچه دار شود، با انتصاب مسئولیت a به یک نقش دیگر نمی توان مسئولیت b را به او اختصاص داد و بالعکس.

پویا :(DSD)چنانچه نقش های a و b هرکدام دارای مسئولیت هایی باشند که انجام دادن آنها بصورت همزمان سبب شود قوانین امنیتی سازمان خدچه دار شود، می توان هر دو نقش را به یک کاربر اختصاص داد اما در صورتیکه کاربر با نقش a فعال بود، دیگر نمی تواند بصورت همزمان و با یک session با نقش b هم فعال باشد.

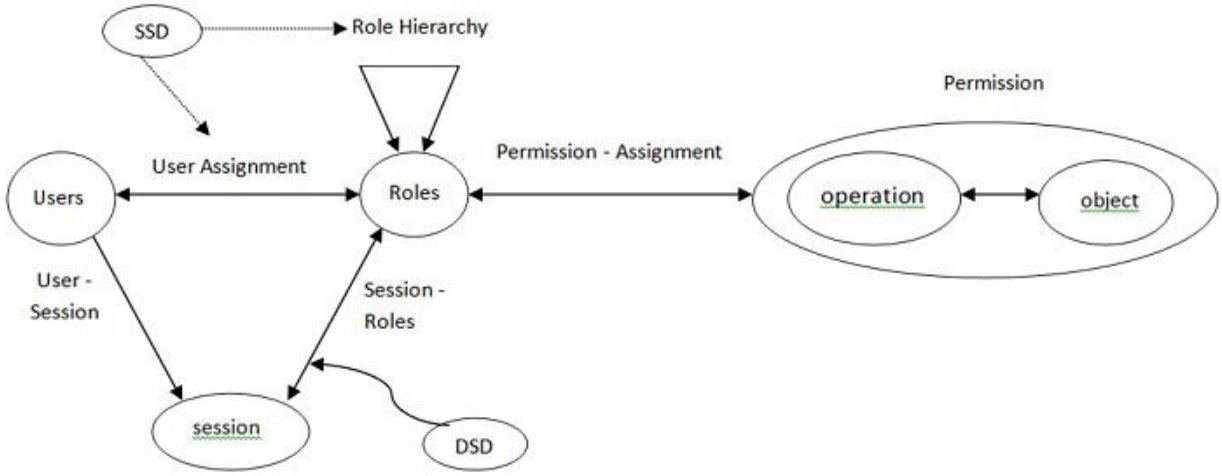
قوانین پایه ای حاکم بر سیستم مبتنی بر نقش:

Role assignment : یک کاربر در صورتی مجوز انجام عملی را در سیستم دارد که نقشی (role)به آن انتصاب داده شده باشد.

Role authorization : نقشی که کاربر با آن فعالی می شود، باید حتما مورد تایید سیستم قرار گیرد. این قانون به همراه قانون اول، تضمین می نماید که هر کاربر تنها می تواند در نقش هایی فعال شود که مجوز آنها را دارد .

Permission authorization : یک کاربر تنها می تواند حق دسترسی هایی را داشته باشد که برای نقشی که با آن فعال است، تایید شده باشد. این قانون به همراه دو قانون قبلی، تضمین می نماید که کاربران تنها می توانند حق دسترسی هایی را داشته باشند که برای آنها مجاز است.

نمای کلی از RBAC بصورت زیر می باشد:



۳-۴- ارتقاء امنیت در شبکه اسکادا

از جمله راهکارهای ارائه شده جهت کاهش امکان نفوذ و حملات به سیستم های کنترل صنعتی عبارتند از:

۱. شناسایی تمامی اتصالات به شبکه اسکادا

ارزیابی ضرورت وجود هر اتصال به شبکه اسکادا، آنالیز تهدیدات مرتبط با آنان و نحوه حفاظت هر یک از شبکه ها

- ✓ انواع اتصالات شبکه ای:
- شبکه های محلی و WAN شامل شبکه سازمانی
- اینترنت
- دستگاه های شبکه بی سیم شامل لینک های ماهواره ای
- اتصالات مودم و یا Dial up
- اتصالات به شرکاء تجاری، فروشندگان و یا نهادهای نظارتی

۲. قطع اتصالات غیرضروری به شبکه اسکادا

حتی المقدور سعی شود شبکه اسکادا از سایر شبکه ها مجزاء گردد. هر اتصال به شبکه دیگر می تواند تهدیدات امنیتی مختص به خود را به دنبال داشته باشد خصوصا" اگر اتصال ایجاد شده دریچه ای رو به اینترنت نیز گشوده باشد.

ایزوله کردن شبکه اسکادا یکی از اهداف اولیه در جهت تامین یک سطح حفاظتی قابل قبول است.

۳. ارزیابی و تقویت امنیت هر اتصال باقیمانده به شبکه اسکادا

اجرای تست نفوذ و آنالیز نقاط آسیب پذیر هر یک از اتصالات باقیمانده به شبکه اسکادا.

تحلیل نتایج حاصل از تست نفوذ به همراه فرآیند های مدیریت تهدیدات به منظور پیاده سازی یک استراتژی حفاظتی مستحکم

پیاده سازی فایروال، سیستم های تشخیص اختلال و سایر ابزارهای موجود در هر نقطه تماس شبکه اسکادا با سایر شبکه ها

پیکربندی قوانین فایروال بگونه ای که امکان دستیابی به شبکه اسکادا مدیریت یافته باشد.

۴. حذف و یا غیرفعال سازی سرویس های غیرضروری بر روی شبکه اسکادا

سیستم عامل موجود بر روی سرویس دهندگان کنترلی اسکادا (تجاری و یا کد باز) می تواند جذابیت های خاصی را برای مهاجمان از طریق سرویس های شبکه ای پیش فرض ایجاد نماید

حتی المقدور سعی گردد سرویس های استفاده نشده حذف و یا غیرفعال گردند (خصوصا" در مواردی که شبکه اسکادا با سایر شبکه ها مرتبط می گردد)

مطالعه و بکارگیری توصیه های امنیتی در خصوص امن سازی سیستم عامل

مشاوره با ارایه دهندگان اسکادا در زمان حذف و یا غیرفعال کردن یک سرویس و شناسایی امن ترین پیکربندی

۵. عدم استناد به پروتکل های اختصاصی جهت حفاظت سیستم

برخی سیستم های اسکادا از پروتکل های اختصاصی و منحصربفرد برای ارتباط با دستگاه های اندازه گیری، پردازنده های محلی و سرویس دهندگان استفاده می نمایند.

اغلب استناد به امن سازی سیستم های اسکادا، محدود به امن سازی این پروتکل ها می گردد. واقعیت این است که مبهم بودن این پروتکل ها صرفا" می تواند امنیت اندکی را به ارمغان آورد.

هرگز به پروتکل های اختصاصی و یا پیکربندی پیش فرض استناد نگردد.

از ارایه دهندگان سیستم های اسکادا تقاضاء نمایید سیستم را فاقد هرگونه back door و یا اینترفیس های مازاد (نظیر اینترفیس ارایه هنده به سیستم شما) تحویل دهد. ارایه دهنده، مسئولیت امن بودن سیستم را می بایست بپذیرد.

۶. پیاده سازی ویژگی های امنیتی ارایه شده توسط تولید کنندگان دستگاه ها و سیستم ها

اکثر سیستم های قدیمی اسکادا (اکثر سیستم هایی که هم اینک از آنها استفاده می شود)، دارای هیچگونه ویژگی امنیتی نمی باشند. مالکین سیستم های اسکادا می بایست به فروشندگان اصرار ورزند که ویژگی های امنیتی را به شکل وصله و یا بسته های ارتقاء ارایه نمایند.

وصله، یک به‌روزرسانی برای یک برنامه یا سامانه‌ی آسیب‌پذیر است. یکی از راه‌های معمول برای حفظ امنیت رایانه و دستگاه‌های همراه، نصب به موقع آخرین وصله‌های ارائه شده توسط تولیدکنندگان نرم‌افزارها است. برخی تولیدکنندگان وصله‌های خود را به صورت بسته‌های ماهانه و یا فصلی ارائه می‌کنند. در نتیجه اعمال نکردن وصله‌ها، حتی به مدت چند هفته، می‌تواند آن را آسیب‌پذیر بسازد.

تعدادی از سیستم های جدید اسکادا با برخی ویژگی های پایه امنیتی ارایه می گردند ولی اغلب این ویژگی ها به منظور نصب آسان، غیرفعال می گردند. هر دستگاه اسکادا را بررسی نمایید تا مشخص گردد که آیا دستگاه دارای ویژگی های امنیتی می باشد.

تنظیمات پیش فرض هر دستگاه بگونه ای انجام شده است که بیشترین قابلیت استفاده و کم ترین امنیت را داشته باشند. تمامی ویژگی های امنیتی موجود در هر دستگاه می بایست با حداکثر سطح امنیتی تنظیم گردد.

۷. ایجاد یک کنترل قدرتمند بر روی هر رسانه ای که به عنوان یک در پشتی درون شبکه اسکادا رفتار می نماید

جایی که backdoor و یا اتصالات ارایه دهندگان سیستم های اسکادا وجود دارد، می بایست از یک سیستم تایید هویت مستحکم برای حصول اطمینان از یک ارتباط امن استفاده گردد.

معمولا" از مودم، ارتباطات بی سیم و یا خطوط اختصاصی برای برقراری ارتباط و انجام خدمات پشتیبانی استفاده می گردد. این وضعیت می تواند یک نقطه آسیب پذیر با پتانسیل بسیار بالا را درون یک شبکه

اسکادا ایجاد نماید. به منظور کاهش این گونه تهدیدات، دستیابی ورودی را غیرفعال نمایید و آن را با یک نوع خاص از سیستم callback جایگزین نمایید.

۸. پیاده سازی سیستم های تشخیص اختلال داخلی و خارجی و مانیتورینگ شبانه روزی وقایع

به منظور پاسخ گویی موثر به حملات، لازم است یک استراتژی تشخیص اختلال که شامل هشدار به مدیران شبکه در خصوص فعالیت های مخرب از منابع داخلی و یا خارجی است، پیاده سازی گردد. سیستم تشخیص اختلال لازم است به صورت شبانه روزی باشد و به سیستم های اطلاع رسانی نظیر پیام کوتاه و یا pager نیز مرتبط گردد. رویه های پاسخ به وقایع می بایست پیش بینی گردد تا در صورت بروز حملات بتوان پاسخ لازم را در کوتاهترین زمان داد.

۹. ممیزی فنی دستگاه ها و شبکه اسکادا و هر شبکه متصل شده به منظور شناسایی اثرات امنیتی

به منظور ممیزی فنی می توان از مجموعه ای از ابزارهای کدباز و یا تجاری به منظور شناسایی نقاط آسیب پذیر، سطح patching، سرویس های فعال دستگاه ها و شبکه اسکادا استفاده کرد.

استفاده از این ابزارها مشکل مسائل سیستماتیک را حل نخواهد کرد ولی می تواند باعث حذف " مسیرهایی با حداقل مقاومت " گردد که یک مهاجم می تواند از آنها در جهت منافع خود بهره برداری نماید.

آنالیز نقاط آسیب پذیر شناسایی شده و انجام اقدامات ضروری در جهت برطرف کردن آنها

تست مجدد سیستم ها پس از انجام اصلاحات جهت حصول اطمینان از رفع مشکل نقاط آسیب پذیر

۱۰. ممیزی امنیت فیزیکی و ارزیابی تمامی سایت های راه دور متصل شده به شبکه اسکادا به منظور بررسی وضعیت امنیتی آنها

هر نقطه ای که دارای یک اتصال به شبکه اسکادا می باشد، می تواند یک هدف باشد خصوصا" سایت های راه دورشناسایی و ارزیابی هر گونه منبع اطلاعاتی شامل تلفن، شبکه کامپیوتری راه دور، کابل های فیبرنوری، لینک های رادیویی، ترمینال های کامپیوتری، دستگاه های نقطه تماس شبکه های بی سیم

۱۱. استفاده از نیروهای متخصص جهت شناسایی و بررسی حملات احتمالی

ایجاد یک گروه به منظور شناسایی حملات احتمالی و بررسی نقاط آسیب پذیر سیستم

استفاده از مجموعه ای از نیروهای کارشناس که در خصوص امنیت اطلاعات، سیستم های اسکادا، سیستم های فیزیکی و کنترل های امنیتی دارای بینش لازم می باشند.

بررسی ریسک نفوذ و اثربخشی کدهای مخرب و در اختیار قرار دادن نتایج مطالعات انجام یافته توسط گروه فوق به گروه مدیریت تهدیدات به منظور اتخاذ استراتژی لازم جهت مقابله با تهدیدات

۱۲. تعریف شفاف وظایف، مسئولیت ها، ممیزی ها، مدیریت ها و کاربران

کارکنان سازمان لازم است شناخت مناسبی نسبت به نقش خود در خصوص امن سازی اطلاعات داشته باشند. این کار از طریق تعریف دقیق و شفاف وظایف و مسئولیت ها صورت می پذیرد.

به کارکنان کلیدی سازمان می بایست مجوز لازم جهت انجام وظایف خود خصوصا" در موارد ممیزی داده شود.

یک ساختار سازمانی در خصوص امن سازی زیرساخت فناوری اطلاعات در سازمان ایجاد گردد.

۱۳. مستندسازی معماری شبکه و شناسایی سیستم هائی که دارای وظایف حیاتی هستند و یا شامل اطلاعات حساسی می باشند که نیازمند یک سطح اضافه از حفاظت می باشند.

۱۴. ایجاد فرآیند مدیریت خطرات (مستمر و سخت)

۱۵. ایجاد یک استراتژی حفاظت شبکه بر اساس اصول دفاع در عمق

۱۶. تدوین یک برنامه جامع امنیتی در سازمان شامل رویه ها، سیاست های امنیتی، مسئولیت ها و...

۱۷. مدیریت پیکربندی تجهیزات سخت افزاری و نرم افزاری

۱۸. انجام ارزیابی امنیتی بطور ادواری

۱۹. ایجاد یک برنامه جامع جهت برخورد مناسب با شرایط بحرانی (برگرداندن سریع سیستم ها به سرویس ها، عدم حذف و یا از دست دادن داده و...)

۲۰. ایجاد سیاست ها، آموزش، افزایش دانش و آگاهی کارکنان در خصوص امنیت

۳-۵- استفاده از RTU های امن بومی

همانطور که اشاره گردید ارائه سامانه اسکادای بومی توسط نیروهای متخصص این مرکز، به دلیل طراحی داخلی و دسترسی به تک تک بیت های ارسالی و لایه های امنیتی در بخش سخت افزار و نرم افزار سیستم تا حد بسیار زیادی آسیب های مربوط به عدم دسترسی به لایه های سطح پایین و لایه های امنیتی را کاهش می دهد. این مرکز به دنبال ارائه راهکارهای عملی تست های نفوذ نرم افزاری و سخت افزاری برای سیستم اسکادا می باشد و هم اکنون نیروهای متخصص در بخش IT، کنترل و الکترونیک در حال بررسی و انجام مطالعات اولیه بر این موضوع می باشند.

پیشنهادهای ارائه شده بر روی سخت افزارهای اسکادا:

از آنجا کهPLC های موجود قابلیت‌های بسیار محدود پردازشی دارند و سیستم عامل خاص در این مورد طراحی شده است، امکان نصب نرم‌افزارهای نظارتی جانبی روی آنها وجود ندارد، لذا برای امن‌سازی آنها مجبور به تعویض یا استفاده یک سخت‌افزار جانبی است که یک حائل امنیتی میان کامپیوترهای شبکه صنعتی و PLC خواهد شد. روش های مذکور توسط مرکز ماهر قابل اجرا است.

این مرکز با تجربه در طراحی سیستم اسکادا و RTU در زمینه شرکت آب و فاضلاب، شبکه برق داشته به طراحی و ساخت RTU برای دستگاه ها صنعتی دست زده است. این RTUبا برنامه ریزی خاص هر سازمان بستگی به نیازهای امنیتی و شبکه های صنعتی آن طراحی می شود. ویژگی های این RTU عبارتند از

- ✓ امکان ارتباط با انواع سنسورهای جریانی، ولتاژی و مقاومتی
- ✓ دارای انواع ورودی ها و خروجی دیجیتال
- ✓ امکان برنامه نویسی و هوشمند سازی
- ✓ دارای پورت های ارتباطی از جمله LAN، USB
- ✓ امکان ارتباط با شبکه وایرلس از جمله RF از جمله با پروتکل حفاظتی خاص

- ✓ امکان کنترل با لایه های امنیتی از جمله ارسال رمزهای یک بار مصرف
- ✓ ارتباط و عیب یابی توسط RTU های دیگر
- ✓ پشتیبانی از پروتکل های MODBUS ,-DNP3 ,

از جمله قابلیت های مهم این دستگاه نسبت به RTU مشابه استفاده از شبکه RF کد شده که قابل شناسایی توسط دستگاه معمولی نیست و به دلیل اینکه فقط با RTU مورد نظر قابل شناسایی هستند توسط سیستم های دیگر قابل رمزگشایی و ارتباط نخواهند بود که امنیت بسیار افزایش داده است. این دستگاه با انواع پروتکل های استاندارد از جمله DNP و فیلدباس و مدباس که بتواند با دستگاه ارتباط برقرار کند دارا است.

در بخش نرم افزاری این سامانه، تمامی داده های دستگاه ها واطلاعات دریافتی در دیتا بیس سرور ذخیره می‌شود و در مواقع نیاز توسط نرم افزار قابل دستیابی می‌باشند. نرم افزار تخصصی در حال طراحی توسط این مرکز، با لحاظ کردن نکات امنیتی هر گونه عملیات نمایش، کنترل، گزاش گیری، جمع آوری وذخیره سازی اطلاعات، را انجام خواهد داد. ویژگی های فوق نه فقط در مرکز کنترل بلکه در هر مکانی از طریق اینترانت و اینترنت، میسر خواهد شد.

پایانه دور دست(RTU):

توانایی ارتباط با نرم افزار مرتبط از طریق USB، پورت Ethernet و RS ۲۳۲، توانایی به روز رسانی اطلاعات در هر لحظه، قابلیت اتصال دستگاه ارسال پیامک و یا ارسال اطلاعات از طریق بستر GPRS به محض رخداد اتفاقی خاص، مجهزبه UPS انلاین جهت کنترل بی وقفه و هشدار قطعی برق از طریق GPRS , SMS

فرستنده گیرنده برد بلند:

فرستنده-گیرنده های رادیویی برد بلند (۴۰-۱۰ کیلومتر)، بدون نیاز به اتصال به برق شهر و تغذیه از طریق صفحات خورشیدی، ارسال و دریافت اطلاعات طبق پروتکلهای استاندارد RTU، قابلیت ارسال اطلاعات از طریق بستر RF

البته موارد فوق که

۳-۶- استفاده از فایروال صنعتی و پروتکل wrapper ها:

در این روش یک دستگاه قبل از PLC قرار می گیرد و تمام بسته‌های ارتباطی کـه PLC بـه کامپیوترهـای دیگر می‌فرستد یا می‌گیرد از این سخت‌افزار عبور می‌کند. به همین دلیل هرگونه حمله از طریق شبکه روی PLCتوسط این محصول قابل شناسایی و جلوگیری خواهد بود. توجه داشته باشید که کامپیوترهای محـیط صنعتی که حتی حاوی برنامه‌های کاربردی PLC نباشند هم می‌توانند بـه PLC حملـه کننـد و بـا ارسـال بسته‌های ساده، عملکرد PLC را دچار اختلال نمایند. برای مثال در برخی موارد ارسال رگباری بسته بسوی PLCیا ارسال بسته‌های غلط می‌تواند باعث توقف کار آن و یا حتی در برخی موارد باعث پاک شدن حافظـه موقت آن شود. لذا استفاده از فایروال صنعتی می‌تواند در شناسایی و جلوگیری از چنین حملاتی موثر باشد.

فایروال صنعتی بومی توانایی ارتباط با انواع پروتکل ارتبـاطی در PLC نظیـر DNP، MODBUS، را دارد و توانایی ارتباط با انواع PLC و HMI های و رایانه ها را دارا است.

در این فایروال به دلیل طراحی پروتکل های ارتباطی توسط برنامه نویسان از قابلیت اطمینان بالا جهت رفـع خطاهای امنیتی است و علاوه بر این امکان طراحی پروتکل خاص کـه از نظـر کـاربران ناشـناخته باشـد بـر امنیت شبکه صنعتی می افزاید و شبکه را از قابلیت نفوذ کم می کند. به دلیل استفاده از پروتکل های خاص امکان نفوذ ویروس ها و کرم های شبکه در شبکه امکان پذیر نخواهد بود.

علاوه بر این با انتخاب الگوریتم ها و رمزهای یک بار مصرف توسط RTU امکان کشف رمزها و دسترسی بـه کنترل های PLC وجود نخواهد داشت. در این فایروال از ماژول سیم کـارت جهـت ارتبـاط بـا نـرم افـزار و ارسال رمزها استفاده می شود.

ارتباط با شبکه صنعتی هم بصورت بی سیم و با سیم انجام می شود. ارتباط با سـیم در ایـن شـبکه هـا مـی تواند از طریق شبکه LAN یا سیم کشی مخصوص انجام شود. ارتباط بی سیم توسط فرستنده، گیرنـده RF یا ماژول سیم کارت انجام می شود. ارتباط RF با پروتکل خاص بصورت کدشده و با بردهای بالا منتشر شـده و امکان کدگشایی توسط فایروال ها یا RTU ها مرکز انجام می پذیرد. این نوع ارتباط با پروتکل هـا خـاص امنیت بسیار بالایی دارد و با سرعت بالایی و بدون امکان سخت افـزاری دیگـر همچـون روتـر یـا سـوئیچ بـا سیستم دیگر ارتباط برقرار می کند و به علت کاهش ترافیک شبکه باعـث سـرعت بخشـیدن در قسـمت هـا دیگر می شود. این ارتباط در حالت محلی و در فاصله های چندین کیلومتری بسیار مناسب است.

در فایروال صنعتی طراحی شده تمام اطلاعات با الگوریتم ها خاصی رمزگشایی خواهد شد و تمامی فـرامین و دستوارات مناسب قابل اجرا خواهند بود.

نرم افزارهای طراحی شده با رابط گرافیگی مناسب و ذخیره اطلاعات در دیتابیس سرور امکان گزارش گیـری از PLC و دستگاه صنعتی ها امکان پذیر می کند. نرم افزار سرور الگوریتم هـا امنیتـی اطلاعـات دریافـت و

ذخیره می کند. این نرم افزار بر روی سرور نصب می شود و ارتباط بین فایروال ها، RTU ها و رایانه های مرتبط با آنها کنترل می نماید و از حملات احتمالی بر روی PLC ها و دستگاه های صنعتی جلوگیری می کند.

نرم افزار کنترل و مانیتورینگ امکان نمایش وضعیت با تمام جزییات دستگاه ها صنعتی را دارد و تمام اطلاعات در بازه مشخص و کوتاه مدت بروز خواهند شد. در این طراحی با رابط گرافیگی مناسب از تمام خطاها و ایرادها دستگاه ها مشخص شده و در صورت لزوم فرامین مناسب از طریق سیستم یا توسط کاربر انجام خواهد شد. این نرم افزار با پروتکل خاص در لایه ها فیزیکی و برنامه با نرم افزار سرور ارتباط برقرار می کند و پروتکل های ارتیاطی همواره با نرم افزار سرویس بروز شده و امکان یافتن کدها و الگوریتم ها آن وجود ندارد. نرم افزار سرویس در صورت یافتن خطا و ایرادی در شبکه ارتباط را خاتمه داده و امکان نفوذ را از بین می برد.

علاوه بر این امکان در نرم افزار امکان تهیه رمزهای یک بار مصرف در نظر گرفته شده که توسط پیامک از فایروال های این مرکز ارسال می شود که بدون این کد امکان کنترل توسط افراد دیگر گرفته خواهد شد و یک سیستم امن را در نظر گرفته خواهد شد.

۳-۷- آزمون نفوذ پذیری

این راهکار مستقل از دو راهکار قبل می باشد چرا که آزمون تست نفوذ در هر حال اجرا می گردد آن هم به صورت دوره ای و متناوب. هدف از اجرای تست نفوذ، آنالیز نقاط آسیب پذیر در اسکادا می باشد. تحلیل نتایج حاصل از تست نفوذ به همراه فرآیند های مدیریت تهدیدات، به منظور پیاده سازی یک استراتژی حفاظتی مستحکم استفاده خواهد شد.

در حالت معمول دو نوع آزمایش نفوذپذیری در دنیای امنیت و اطلاعات وجود دارد که تمامی متخصصین امنیت، آنها را با نام های آزمایش نفوذپذیری جعبه سیاه (Black Box) و جعبه سفید (White Box) می شناسند. در امنیت سیستم های صنعتی، هنگامی از آزمایش نفوذپذیری جعبه سیاه استفاده می شود که شخص مهاجم یا متخصص امنیت و اطلاعات، به منظور تجزیه و تحلیل حفره های امنیتی هدف، هیچ اطلاعاتی در مورد ساختار درونی یا دیگر جنبه های هدف نداشته باشد. به همین دلیل، از آنجایی که اکثریت مهاجمین از ساختار درونی هدف خود اطلاعات کافی ندارند از این روش)آزمایش نفوذپذیری جعبه سیاه(برای حمله به سیستم های زیر ساخت استفاده می کنند. با این حال ما می توانیم با استفاده از این نوع آزمایش، سناریو های حمله در دنیای واقعی را شبیه سازی کرده و بر علیه آنها سیستم های دفاعی مستحکمی تدبیر کنیم.

واژه آزمایش نفوذپذیری جعبه سفید هنگامی استفاده مـی شـود کـه شـخص مهـاجم یـا متخصـص امنیـت اطلاعاتی از قبیل دیاگرام شبکه، کد منبع، ساختار معماری و... به منظور کشف ضعف های امنیتی به شـخص آزمایش کننده ارائه شده باشد. این آسیب پذیری ها به عنوان یک مبنا در تعیـین اثربخشـی امنیتـی از یـک محصول استفاده می شود. معمولا این روش با اجازه شرکت سازنده محصول به متخصصین صورت می گیـرد، چونکه آنها باید اطلاعاتی را به منظور آزمایش امنیت محصول خود به متخصصین ارائه بدهند. اما نوع دیگری از آزمایش نفوذ هم وجود دارد که Gray Box Penetration Testing یا آزمایش نفوذ جعبه خاکسـتری نامیده می شود، این روش ترکیبی از دو روش مذکور)جعبه سیاه و جعبه سفید(است. در این آزمایش ما هـم از روش Gray Box استفاده خواهیم کرد، چونکـه بـرای انجـام مقاصـد خـود نیـاز بـه اطلاعـاتی از قبیـل مشخصات حساب کاربری Root داریم.

برای آزمایش نفوذپذیری بر روی PLCهای مورد استفاده در صنعت گام به گام تلاش در پیدا کـردن ضـعف امنیتی بر روی آنها خواهیم کرد.

البته توجه داشته باشید که موارد فوق باید توسط ابزارهای خاصی انجام شود که باعث بروز مشـکل در اجـزاء سامانه اسکادا نگردد، چراکه استفاده از ابزارهای معمول در تست نفوذ شبکه هـای کـامپیوتری ممکـن اسـت باعث خرابی اسکادا گردند. برای این منظور برخی شرکتهای محصولهای ویژه ای طراحی نموده اند.

۳-۸- آموزش های امنیت سایبری برای کارکنان

بسیاری از حملات سایبری به شبکه ها و سازمان ها با سوء استفاده از افراد داخل مجموعه صورت می گیرد. این امر می تواند عمدی و یا به صورت غیر عمد و از روی نا آگاهی باشد. لذا توصیه می شود کلیه پرسنل مرتبط با کنترل صنعتی و شبکه داخلی در یک کارگاه آموزشی امنیت شبکه شرکت کنند. داشتن آگاهی لازم توسط پرسنل از بسیاری از رفتار های پر خطر جلوگیری می کند. رفتار های پر خطر به رفتارهایی گفته می شود که در ظاهر امن به نظرمی رسند ولی در باطن می تواند راه نفوذ به شبکه را باز کند.

- **باور های غلط**

گاها در اثر نا آگاهی باور های غلطی در افراد یک مجموعه شکل می گیرد که منجر به انجام رفتارهای پر خطر می شود. به عنوان مثال به سه مورد از باورهای غلط در مجموعه پتروشیمی پارس در زیر اشاره می شود.

- **پورت USB**

باور بر اینکه در صورت بسته بودن پورت USB راه نفوذ به کامپیوتر بسته است باور غلطی است. چرا که بستن پورت USB به طریق نرم افزاری بوده و می توان از آنها عبور کرد به خصوص اگر شرکت سازنده بخواهد چنین کاری بکند بسیار ساده خواهد بود. پس لازم است طریقه صحیح مسدود کردن پورت های کامپیوتر آموزش داده شود.

- **ارتباط یک طرفه شبکه**

باور بر اینکه ارتباط شبکه می تواند یک طرفه باشد دومین باور غلطی است که در بین کارکنان دیده شده است. مثلا کارکنان بر این باورند که کامپیوتری که برای گرفتن گزارش به شبکه متصل شده است نمی تواند اثری روی سیستم داشته باشد و فقط یک گزارش گیر است این در صورتی است که این ارتباط دو طرفه است و در صورتی که هکر ها به این کامپیوتر دسترسی پیدا کنند می توانند در کار سیستم اخلال ایجاد کنند. این در حالی است که این باور غلط باعث شده که این کامپیوتر به شبکه محلی متصل شود و امنیت خاصی هم برای آن در نظر گرفته نشده است. از این رو لازم است این کامپیوتر از شبکه محلی ایزوله شود و یا تدابیر امنیتی جهت دسترسی به آن در نظر گرفته شود و همچنین اتصال آن به شبکه صنعتی تحت نظارت قوی قرار گیرد.

- **گرفتن گزارش توسط CD**

گرفتن گزارش توسط CD راه حل خوبی بوده است. ولی این به شرطی است که از خام بودن سی دی ها مطمئن باشیم. در واقع ممکن است CD های آلوده در بین CD های خام قرار گرفته باشند و با توجه به اینکه کامپیوتر های صنعتی دارای آنتی ویروس مناسب نیستند، سیستم های اصلی به سرعت آلوده می شوند. لذا پیشنهاد می شود یک کامپیوتر میانه و کاملا ایزوله و دارای آنتی ویروس ساخت داخل کشور برای تست آلوده نبودن CD استفاده شود و یا با قرار دادن یک سیستم میانه مسیر ارتباط یک طرفه شود.

موارد ذکر شده تنها نمونه های بسیار ساده از باورهای نادرست است که می تواند به سیستم آسیب برساند. از این رو دیدن آموزش صحیح و کامل پرسنل بسیار ضروری است. کارگاه آموزشی می تواند توسط متخصصان مرکز ماهر برگزار شود.