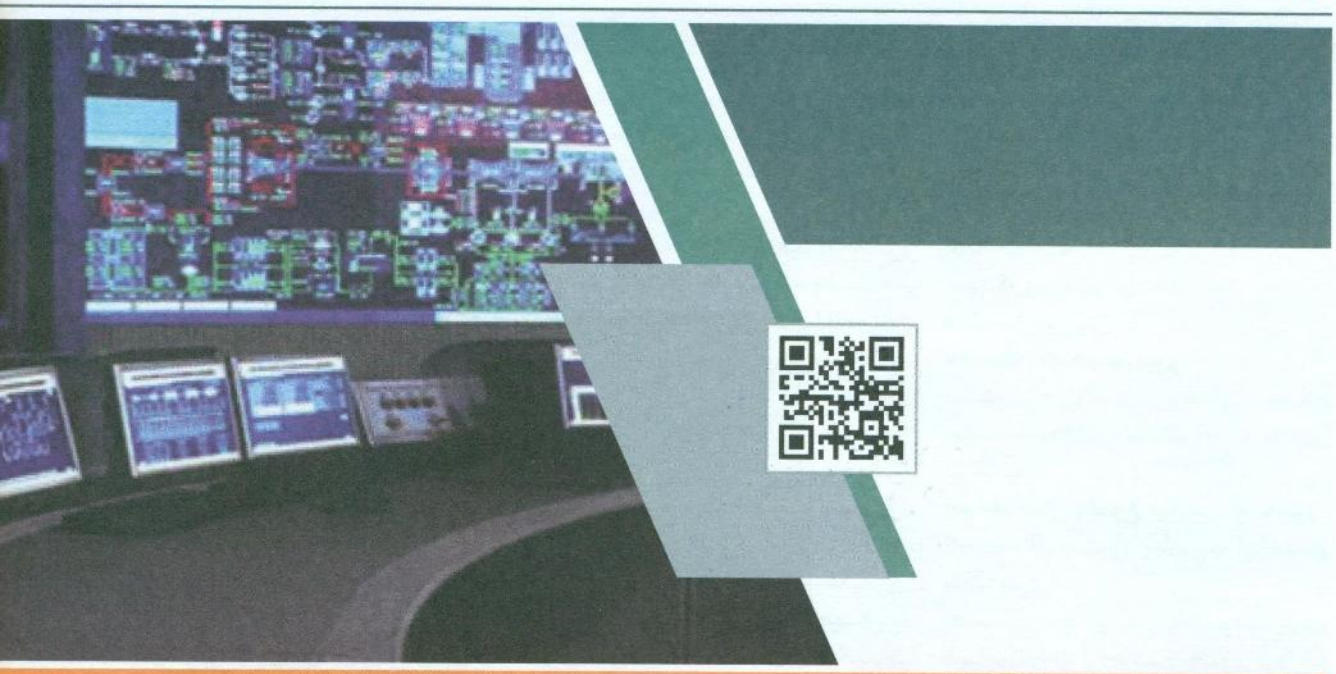
محمد مهدی واعظی نژاد



پدافند سایبری سیستم‌های کنترل صنعتی

تهدیدها و آسیب‌پذیری‌ها در سیستم‌های کنترل صنعتی به سرعت در حال افزایش است. در ۱۰ سال گذشته تعداد تهدیدها، آسیب‌پذیری‌ها و حمله‌های سایبری صنعتی افزایش چشمگیری داشته است. با ظهور فناوری‌های تولید انبوه و اتصال بین سیستم‌های کنترل صنعتی و IT، دسترس‌پذیری سیستم‌های کنترل صنعتی افزایش یافته و آنها را در برابر تهدیدها به شدت آسیب‌پذیرتر کرده است. حملات سایبری اخیر علیه زیرساخت‌های حیاتی، به شدت از نظر پیچیدگی پیشرفته‌تر شده‌اند. این تهدیدها نیازمند این هستند که به خوبی و بدون شک با آنها مقابله شود و سامانه‌های پیشگیری از نفوذ هم تقویت شوند یعنی قبل از رخداد حمله نیز باید سامانه‌های دفاعی فعالیت‌های تأثیرگذار داشته باشند.

پیشرفت‌های روزافزون در سیستم‌های کنترل صنعتی و تجهیزات مورد استفاده در آنها نه تنها باعث بالابردن کارایی و بهبود عملکرد سیستم و فرایندهای صنعتی شده است، بلکه کنترل بسیاری از فرایندهای ناممکن و یا پیچیده را تسهیل کرده و امکان کنترل و پایش از راه‌دور را فراهم ساخته است. با وجود پیشرفت‌های بسیار زیادی که در ساختار و عملکرد سیستم‌های صنعتی وجود داشته است، این سیستم‌ها از دیدگاه سایبری دارای ضعف‌های بسیاری هستند و همین امر باعث شده است که سیستم‌های کنترل صنعتی، مورد تهدید و حملات سایبری زیادی قرار بگیرند. حرکت به سمت هوشمندکردن سیستم‌های کنترل صنعتی که ورود گسترده سیستم‌های اطلاعاتی، ارتباطی و رایانه‌ای به سیستم‌های کنترل صنعتی را دربر داشته است، چالش‌های پدافندی جدیدی را نیز در حوزه سایبری برای این سیستم‌ها ایجاد کرده است.

امروزه حملات‌سایبری علیه زیرساخت‌های حیاتی، به شدت از نظر پیچیدگی پیشرفته‌تر شده‌اند. شبکه‌های صنعتی، ستون فقرات یک کشور به حساب می‌آیند، زیرا این سیستم‌ها در حساس‌ترین بخش‌های صنعت استفاده می‌شوند که شامل منابع اقتصادی، انرژی و پتروشیمی هستند. نفوذ به این سیستم‌ها تنها به بخش کوچکی ضربه نمی‌زند بلکه یک کشور را دچار بحران می‌کند. بنابراین چنین درجه‌ای از حساسیت، مستلزم توجه ویژه‌ای به این شبکه‌ها در مقابل حملات سایبری و نفوذگران است.

شبکه‌های صنعتی در اصل از ابتدا فقط برای محیط‌هایی ساخته

شدند که حتی تصور نمی‌شد روزی بتوانند انگیزه نفوذگران برای حمله را جلب کنند. بنابراین تفاوت‌های زیادی در امن‌سازی ICS1 و IT2 وجود دارد که مهم‌ترین این تفاوت‌ها در اولویت‌بندی اهداف پدافندی است. برخلاف سیستم‌های IT، اهداف پدافندی ICS به صورت زیر اولویت‌بندی می‌شوند:

۱ دسترس‌پذیری
۲ جامعیت
۳ محرمانگی

اما در سیستم‌های IT، اهداف پدافندی به ترتیب محرمانگی، جامعیت و دسترس‌پذیری دارای اولویت بالاتری هستند. این بدان معنا است که در سیستم‌های کنترل صنعتی، اولویت در بحث ایمنی در ویژگی دسترس‌پذیری است. در حالی که در سیستم‌های حوزه IT این ویژگی از کمترین اولویت برخوردار است. این امر به لحاظ ارتباط سیستم‌های کنترلی با زیرساخت‌های صنعتی از جمله صنایع آب، برق، نفت، گاز، پتروشیمی، نیروگاهی و الزام دسترسی بدون تأخیر افراد مجاز به این سیستم‌ها است. در جدول شماره ۱، تفاوت‌های دیگر سیستم‌های ICS با سیستم‌های IT آورده شده است [۱ و ۲].

جدول ۱: تفاوت سیستم‌های IT و ICS

سیستم‌های فناوری اطلاعات	سیستم‌های کنترل صنعتی
در صورت از دست دادن داده و یا بروز وقفه‌های ناخواسته می‌توان سیستم را دوباره راه‌اندازی کرد و یا با استفاده از فایل‌های پشتیبان، به حالت اولیه برگرداند.	از دست دادن داده و یا بروز وقفه، قابل تحمل نیست و ممکن است نتایج مهلکی را به دنبال داشته باشد.
از پروتکل‌های ارتباطی استاندارد برای شبکه‌های سیمی و بی‌سیم استفاده می‌شود.	پروتکل‌های ارتباطی استاندارد و اختصاصی برای آنها وجود دارد (DNP3، ModBus). انواع دستگاه‌های ارتباطی شامل سیمی و غیرسیمی (ماهواره و رادیو) در آنها استفاده می‌شود. این شبکه‌ها پیچیده هستند و در برخی مواقع نیاز به مهندسین کنترل حرفه‌ای دارند.
با تأخیر ناخواسته می‌توان کنار آمد.	تأخیر زیاد قابل تحمل نیست.
درصورت بروز مشکلات حاد برای سیستم، با راه‌اندازی دوباره آن می‌توان مشکل ناخواسته را به نوعی حل کرد.	تأخیر زیاد قابل تحمل نیست.
درصورت بروز مشکلات حاد برای سیستم با راه‌اندازی دوباره آن می‌توان مشکل ناخواسته را به نوعی حل کرد.	از کار افتادن سیستم حتی برای لحظاتی اندک می‌تواند فاجعه‌آمیز باشد.
از نرم افزارهای ضدویروس استفاده زیاد می‌شود.	بکارگیری نرم افزارهای ضدویروس در بیشتر موارد مشکل است، چرا که تأخیر قابل تحمل نیست.
ارایه دوره‌های آموزشی به منظور افزایش سطح آگاهی کاربران در خصوص مسایل امنیتی، بسیار متداول است.	ارائه دوره‌های آموزشی به منظور افزایش سطح آگاهی کاربران در خصوص مسائل امنیتی کم است.
از رمزنگاری استفاده می‌شود.	تعداد بسیار زیادی از سیستم‌های کنترل صنعتی، داده و پیام‌های کنترلی را به صورت غیررمز شده ارسال می‌کنند.
آزمون نفوذپذیری، به صورت ادواری انجام می‌شود.	آزمون نفوذپذیری، به صورت ادواری در شبکه کنترلی انجام نمی‌شود و زمانی هم که این کار انجام می‌شود باید این کار با دقت صورت پذیرد تا باعث بروز اختلال نشود.
پیاده‌سازی وصله‌های* نرم افزارها به صورت ادواری انجام می‌شود (منظم/زمان‌بندی شده).	پیاده‌سازی وصله‌های نرم افزاری می‌بایست با دقت صورت پذیرد و معمولاً مستلزم هماهنگی با شرکت فروشنده تجهیزات سیستم کنترل صنعتی است (کند و مختص فروشنده).
ممیزی امنیت اطلاعات لازم است و معمولاً به صورت ادواری انجام می‌شود.	ممیزی امنیت اطلاعات به طور ادواری انجام نمی‌شود.
برون‌سپاری رایج و به طور گسترده استفاده می‌شود.	برون‌سپاری به ندرت استفاده می‌شود.

در جدول ۲، اهمیت حفاظت انواع اطلاعات کلیدی با توجه اهداف پدافندی در سیستم‌های کنترل صنعتی مشخص شده است [۳ و ۴].

جدول ۳: اهمیت ویژگی‌های پدافندی برای داده‌ها، فرمان‌ها و نرم‌افزارها در سیستم‌های کنترل صنعتی

	اطلاعات با ارزش[۲]	فرمان‌های کنترلی	داده‌های اندازه‌گیری شده	نرم‌افزار
محرمانگی	پایین	پایین	متوسط	پایین
جامعیت	بالا	بالا	بالا	بالا
دسترس‌پذیری	بالا	بالا	پایین	

پدافند در شبکه‌های صنعتی از ۳ بعد قابل بررسی است:

- آسیب‌پذیری‌های ذاتی که در محصولات ICS وجود دارد.
- آسیب‌پذیری‌هایی که در طول ذخیره‌سازی، پیکربندی و نگهداری ICS حاصل می‌شود.
- نبود یک حفاظت مناسب به خاطر معماری و طراحی ضعیف شبکه.

برای مثال بدافزار Havex که در سال ۲۰۱۴ شناسایی شد، مهاجم پس از هک کردن وب سایت‌های تولیدکنندگان سیستم‌های کنترل صنعتی و نیز آلوده کردن نرم افزارهای قانونی قابل دانلود در وب سایت‌ها می‌پردازد.

F-Secure سه شرکت فروشنده نرم‌افزارهای ICS که به این بدافزار آلوده شده‌اند را شناسایی ولی نام آنها را بیان نکرده اما اظهار داشت که دو شرکت از آنها توسعه‌دهنده نرم افزار مدیریت از راه دور ICS بودند و سومی تولیدکننده دوربین‌های صنعتی با دقت بالا و نرم‌افزارهای مرتبط با آن است. به گفته این شرکت پدافندی، فروشندگان در آلمان، سوئیس و بلژیک هستند. این حمله جز دسته اول قرار می‌گیرد.

چالش‌ها و تهدیدهای سیستم‌های کنترل صنعتی

چالش‌های پدافندی سیستم‌های کنترل صنعتی را می‌توان به سه دسته تقسیم کرد:

۱ چالش جمع آوری داده

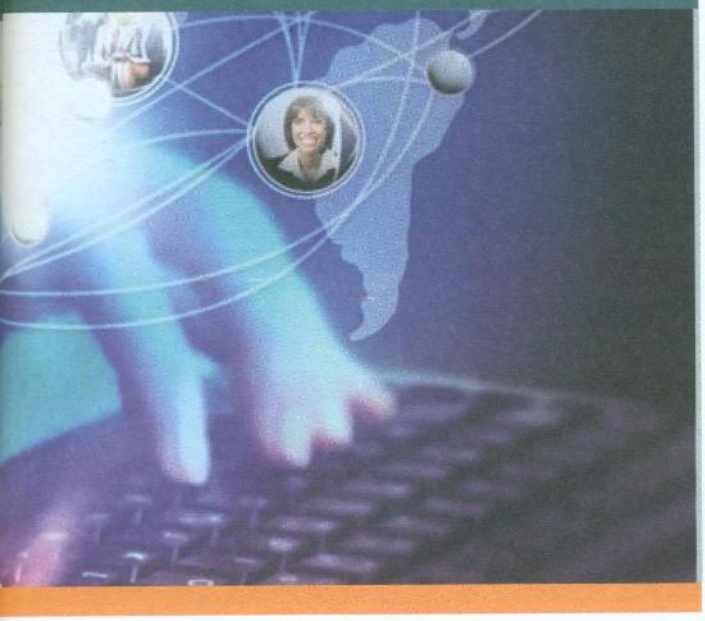
- سازوکارهای سیاهه‌برداری نامناسب
- نوسانات بالای داده‌ها
- هسته‌های سفارشی سیستم عامل
- گستردگی داده‌ها در سطوح پایین‌تر
- نیروی محاسباتی پایین

۲ چالش تحلیل داده

- ابزارهای تحلیل رخداد
- همبستگی و تحلیل داده

۳ چالش‌های عملیاتی

- عدم وجود مطالعات علمی-تخصصی
- چرخه عمر متفاوت زیرساخت‌ها
- نبود یک معماری مرجع برای ICS



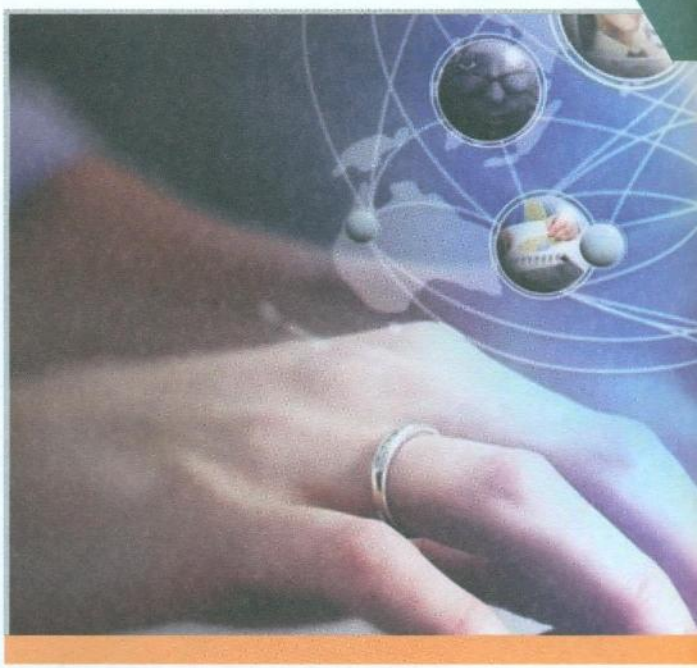
- نبود طرح‌ها و ابتکارات ویژه برای پدافند ICS
- نبود مدیریت یکپارچه برای پدافند ICS
- **چالش‌های فنی پدافند ICS:** اندازه، شبکه شخص سوم و حفظ حریم خصوصی مشتری

عامل‌های تهدید برای شبکه‌های صنعتی به ۸ دسته تقسیم می‌شوند:

- **شرکت‌ها:** این نوع تهدیدات مربوط به شرکت‌ها و سازمان‌هایی می‌شود که در راستای رقابت، از تاکتیک‌های حمله استفاده می‌کنند.
- **جنایی‌سایبری:** هدف این نوع تهدیدات، سود اقتصادی است و در ۳ سطح محلی، ملی و بین‌المللی سازماندهی می‌شوند.
- **کارکنان:** این نوع تهدید، مربوط به کارکنان، پیمانکاران و کارکنان عملیاتی یک شرکت می‌شود.
- **هکرهایی که اهداف سیاسی و اجتماعی دارند:** هدف آنها بیشتر وب‌سایت‌ها، شرکت‌ها، عامل‌های هوشمند و نهادهای نظامی است.
- **دولت‌ها:** این تهدید، استفاده از قابلیت‌های سایبری علیه دشمن است.
- **حوادث طبیعی:** این تهدیدات، آسیب‌های فیزیکی را به دنبال دارد. و حوادث مانند رعد و برق، زلزله، سیل، آتش‌سوزی را شامل می‌شود.
- **تروریست:** انگیزه آنها ممکن است سیاسی و مذهبی باشد. هدف تروریست‌های سایبری اغلب زیرساخت‌های حیاتی (سلامت عمومی، تولید انرژی، مخابرات و غیره) است.
- **جنگجویان سایبری:** گروهی از شهروندان علیه گروهی دیگر به خاطر تعصبات مذهبی، سیاسی یا ملی جنگ سایبری راه می‌اندازند [۵ و ۶].

جدول ۳ نشان می‌دهد این گروه از عوامل، در تهدیدات در نظر گرفته شده برای دارایی‌های سیستم‌های کنترل صنعتی دخیل هستند.

جدول ۳: عوامل دخیل در تهدیدات سیستم‌های کنترل صنعتی



	شرکت	جنایی سایبری	کارکنان	هکرها	دولت‌ها	حوادث طبیعی	تروریست‌ها	جنگجویان سایبری
حملات فیزیکی					✓		✓	
اسب‌های غیرعمدی			✓					
نقص‌ها/خرابی‌ها		✓	✓	✓	✓			
استراق سمع/ رهگیری/ حک	✓	✓	✓	✓	✓		✓	✓
قانونی			✓					
خسارت و از دست دادن دارایی	✓	✓	✓	✓	✓		✓	✓
فاجعه						✓	✓	

معماری امن سیستم‌های کنترل صنعتی

مدل پدافند سایبری سیستم‌های کنترل صنعتی علاوه بر این که باید نقص‌هایی که در پیاده‌سازی کنترل‌های پدافندی وجود دارد و حوزه‌های پدافندی که ممکن است در آنها غافل بمانند را پوشش دهد، دربرگیرنده تمامی جوانب پدافندی این سیستم‌های کنترلی بوده و مبتنی بر استانداردها و بهروش های پدافندی باشد. به طور معمول، راهکار جامع پدافندی این سیستم‌ها باید براساس استراتژی دفاع در عمق۴ و با تمرکز بر امن‌سازی لایه‌ای بنا نهاده شود تا بتواند در برابر بیشتر حملات و تهدیدات از مقاومت لازم برخوردار باشد.

لایه‌های پدافندی که در این معماری در نظر گرفته می‌شوند باید بیانگر سلسه مراتبی از تجهیزات و تسهیلات گروه‌بندی شده شبکه‌های صنعتی بوده و توسط ابعاد پدافندی حفاظت شوند. در بیشتر موارد، این لایه‌های پدافندی بهتر است جهت تدارک راه‌حل‌های مبتنی بر شبکه، بر روی هم بنا شوند. مؤلفه‌های پدافند در این رویکرد لایه‌ای نیز ترکیبی از خط‌مشی‌ها، طراحی، مدیریت و فناوری خواهند بود.

معماری مرجع پدافندی سیستم‌های کنترل صنعتی باید یک نمای انتها به انتها، با رویکرد بالا به پایین و جامع پدافندی که تمام اجزا، خدمت‌ها و برنامه‌های کاربردی را به منظور پیش‌بینی، کشف و برطرف‌سازی سریع آسیب‌پذیری‌های پدافندی در این سیستم‌های کنترلی دربر می گیرد را شامل شود.

توصیه می شود در این معماری، مجموعه پیچیده خصیصه‌های پدافندی انتها به انتهای شبکه صنعتی، به‌طور منطقی به مؤلفه‌های معماری مجزا تقسیم شده و این جداسازی، امکان ارائه یک رویکرد نظام‌مند به پدافند انتها به انتها را در شبکه‌های صنعتی فراهم کند. به نحوی که از آن بتوان در برنامه‌ریزی برای راه‌حل‌های پدافندی و نیز ارزیابی و شناسایی پدافند این شبکه‌ها استفاده کرد.

این معماری لایه‌ای، در نهایت، با فرض این واقعیت که هر لایه، دارای آسیب‌پذیری‌های پدافندی مختص به خود و متفاوتی است می تواند مناسب‌ترین روش مقابله با حملات بالقوه، برای هر یک از لایه‌های پدافندی خاص را پیشنهاد می‌کند.

مراجع

[۱] مؤسسه استاندارد و تحقیقات صنعتی ایران، «فناوری اطلاعات- فنون پدافندی- پدافند شبکه فناوری اطلاعات (معماری پدافندی شبکه)»، شماره استاندارد ۲-۱۱۲۱۰، ۱۳۸۷

[2] E.Zwan," Security of Industrial Control Systems What to Look For", ISACA JOURNAL VOLUME 4, 2010

[3] Frankel, David S., Model Driven Architecture: Applying MDA to Enterprise Computing, OMG Press, Wiley Publishing, 2003.

[4] A.Dhanjal,P.Eng,N.Kurada,B.Venkatesh,"Evolving Perimeter Information Security Models in Smart Grids and Utilities", ISACA JOURNAL Volume 4, 2013

[5] enisa, " Protecting Industrial Control Systems Recommendations for Europe and Member States", 2011

[6] CPNI, "Good Practice Guide Process Control and SCADA Secuity GUIDE 2. Implemnet Secure Architecture". October 2008.

زیرنویس‌ها

1. Industrial Control System
2. Information Technology
3. Patches
4. Defense in Depth