تاریخ دریافت: ۱۳۹۷/۰٤/۲۱
تاریخ پذیرش: ۱۳۹۷/۰۷/۲۰

فصلنامه دانش امنیتی
سال دوم * شماره هفتم* پاییز ۱۳۹۷

ضرورت مرکز عملیات امنیت برای زیرساخت صنعتی با تمرکز بر سامانه‌های SCADA

محمد شفیعی‌نیا[۱]

چکیده

ضرورت مرکز عملیات امنیت سایبری[۲] در حوزه فناوری اطلاعات اثبات‌شده و مزایای آن نمایان است. با توجه به همگرایی صنعت با حوزه سایبری و اتصال سامانه‌های صنعتی به اینترنت به‌صورت مستقیم و غیرمستقیم، مخاطرات حوزه سایبری به صنعت نیز منتقل‌شده است. در این مقاله با بررسی حملات بارز در حوزه صنعتی جمهوری اسلامی ایران، معماری انتزاعی از مرکز عملیات امنیت و مراکز پاسخگویی به رخدادهای رایانه‌ای (CERT) برای زیرساخت‌های حیاتی کشور پیشنهادشده است.

واژگان کلیدی

مرکز عملیات امنیت، مرکز پاسخگویی به رخدادهای رایانه‌ای، دفاع سایبری

---

۱. کارشناس ارشد فناوری اطلاعات گرایش امنیت اطلاعات دانشگاه تهران: shafienia@ut.ac.ir

۲. Cyber Security Operation Center

مقدمه

امنیت سایبری حوزه صنعتی به‌خصوص سامانه‌های نظارت مدیریتی و اخذ داده (SCADA[1]) از اهمیت روزافزونی برخوردار است. شبکه‌های اسکادا حیاتی تلقی می‌شود؛ زیرا زیرساخت‌های صنعتی، اقتصادی، نظامی و... یک کشور را کنترل و هدایت می‌کند (The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 2010). شبکه حمل‌ونقل، شبکه‌های انتقال انرژی، شبکه‌های مخابراتی و ارتباطی و بسیاری از زیرساخت‌های حساس یک ملت می‌توانند مصداق دامنه نفوذ شبکه‌های اسکادا باشند.

به‌رغم تلاش‌ها و فعالیت‌ها برای ایمن‌سازی و محافظت از این سامانه‌ها، هنوز مخاطرات سایبری جدی آن‌ها را تهدید می‌کند. راهبرد مدون و جامع برای رسیدن به سطح قابل قبولی از امنیت در این حوزه یکی از نیازهای جمهوری اسلامی ایران است.

با بهره‌گیری از تجارب حوزه فناوری اطلاعات (IT) و تعمیم آن‌ها به حوزه صنعتی، می‌توان راهکارهای مسکن و پیشگیرانه به دست آورد؛ اما هنوز خلأ راهبردی مختص این حوزه حس می‌شود. در این مقاله، پس از مرور فعالیت‌ها و پژوهش‌های صورت گرفته در این حوزه، راه‌حلی برگرفته از حوزه IT را برای حوزه صنعتی ارائه می‌کنیم. مرکز عملیات امنیت[2] امری اثبات‌شده در IT است و ضرورت آن آشکار است. ازاین‌رو با بهره‌گیری از تجارب پیاده‌سازی این راه‌حل در حوزه IT، آن را برای حوزه صنعتی سفارش و به‌عنوان یک راهکار دفاعی در فضای سایبری پیشنهاد می‌کنیم. در پایان معماری انتزاعی از SOC- و CERT[3] اختصاصی برای شبکه‌های اسکادا ارائه می‌دهیم.

هدف تحقیق پیش رو ارائه معماری انتزاعی از مرکز عملیات امنیت در فضای سایبری زیرساخت‌های حیاتی جمهوری اسلامی ایران است. تأکید بر ارائه راهبردهای بومی در این تحقیق بنا به دلایل متعددی انجام‌گرفته است که یکی از مهم‌ترین دلایل، اهمیت موضوع تحقیق از ابعاد امنیتی و عدم امکان استفاده از مدل‌های غیربومی و ضرورت طراحی مدل داخلی است. درنتیجه، در تحقیق حاضر از روش کیفی با رویکرد داده‌بنیاد[4] استفاده می‌شود.

---

1. Supervisory Control and Data Acquisition
2. Security Operation Center
3. Computer Emergency Response Team
۴. رویکرد داده بنیاد (Grounded Theory)، یک روش پژوهشی استقرایی و اکتشافی است که به محقق در حوزه‌های موضوعی گوناگون امکان می‌دهد تا به‌جای اتکا به نظریه‌های موجود، خود به تدوین نظریه اقدام کند

پارادایم روش تحقیق کیفی پس از دوران طولانی استیلای روش تحقیق کمی تا قرن بیستم به‌عنوان یک آلترناتیو در برابر این روش در سال ۱۹۸۰ مطرح شد.

روش کیفی مبتنی بر گردآوری داده‌های کیفی است. این روش استقرایی است و محقق پس از تحلیل داده‌های جمع‌آوری‌شده، درنهایت فرضیه‌ها و نظریه‌های مستدل را از اطلاعات جمع‌آوری‌شده ارائه می‌دهد. این روش بسترسیال، پویا و اقتضایی را برای محقق فراهم می‌کند و جنبه اکتشافی، تشریحی و تبیینی دارد. روش تحقیق کیفی لنز منعطفی را در اختیار محقق برای بررسی موضوع موردمطالعه قرار می‌دهد، به‌گونه‌ای که عمق و گستره موضوع به‌راحتی قابل‌بررسی است. در این رویکرد پژوهشی تلاش می‌شود به‌طور موقت پیش‌فرض‌های موجود در عرصه دانش مدنظر نادیده انگاشته و موضوع بدون پیش‌فرض‌های ارائه‌شده در دانش مطرح، بررسی شود. یکی دیگر از ویژگی‌های این روش، مطالعه پدیده در محیط طبیعی و شرایط آن است. اطلاعات کیفی از طریق مصاحبه عمیق، مشاهده از نوع مشارکتی، یادداشت‌های میدانی و سؤال‌های بسته و باز و غیره جمع‌آوری می‌شود و محقق ابزار اصلی جمع‌آوری داده است.

راهبری زیرساخت حیاتی توسط شبکه‌های اسکادا

شبکه نظارت مدیریتی و اخذ داده (SCADA) شامل رایانه‌ها و برنامه‌های کاربردی است که عملیات‌های کلیدی را برای فراهم کردن سرویس‌های ضروری یک چرخه صنعتی انجام می‌دهند. این چرخه‌های صنعتی بعضاً زیرساخت‌های حیاتی یک کشور را تشکیل می‌دهند؛ بنابراین همواره مورد تهدید و سوءاستفاده هستند. به‌طورکلی اسکادا به سامانه‌های کنترل صنعتی (ICS) که فرآیندهای صنعتی را پایش و راهبری می‌کند، اطلاق می‌شود (Cyber Security Concerns of Supervisory Control and Data Acquisition Systems, 2010). فرآیندهای دفاعی و نظامی نیز از این موضوع مستثنی نیست که ازجمله آن‌ها می‌توان به سامانه‌های مخابراتی، شبکه‌های راداری و سونار، شبکه‌های توزیع انرژی و برق اشاره کرد.

نظر به همگرایی روزافزون فناوری اطلاعات و صنعت، مخاطرات سایبری به بخش

(Tashakory & Teddli, 2003).

صنعت نیز تسری یافته و نیازمند پیشگیری و درمان است.

توسعه سامانه‌های اسکادا در سه نسل دسته‌بندی می‌شود:

نسل اول: یکپارچه (غیر توزیع‌شده)؛

نسل دوم: سامانه‌های توزیع‌شده؛

نسل سوم: شبکه‌های اسکادا.

با توجه به اینکه ایران یک کشور درحال‌توسعه است و براساس میانگین طول عمر سی‌ساله سامانه‌های اسکادا در کشور، در حال حاضر ایران در حال گذار از نسل دوم به نسل سوم است، بنابراین تمرکز ما در این مقاله بر نسل سوم یعنی شبکه‌های اسکادا و مخاطرات سایبری و به‌تبع آن ارائه راه‌حل است.

در بخش بعدی پس از مروری کوتاه بر فعالیت‌های پیشین، به آسیب‌پذیری‌های این شبکه‌ها اشاره و جدول جامعی دراین‌ارتباط ارائه می‌شود. استنتاج صورت گرفته از مطالعات پیشین و جدول جامع، ما را به سمت طراحی سامانه مدیریت امنیت اطلاعات (ISMS[1]) سفارشی‌شده برای شبکه‌های صنعتی سوق می‌دهد (افروز، ۱۳۹۰: ۱۳).

سابقه تحقیقات و پژوهش‌ها

بررسی جامعی از مقالات و فعالیت‌های پیشین مرتبط صورت گرفته که شرح آن در پیوست ۱ آمده است. در بیان نتیجهٔ پیشینهٔ تحقیقات می‌توان گفت مطالعه پیشینه تحقیقات، دانشِ عمومیِ پژوهشگر را در خصوص موضوع این مقاله بسط و گسترش داد. باآنکه مطالعه پیشینهٔ تحقیق زمینه دانش‌افزایی پژوهشگر را فراهم آورده، اما در هیچ‌یک از موارد درباره سامانه‌های صنعتی، به‌خصوص شبکه‌های اسکادا، مطالعه‌ای با نگرش انتزاعی ــ عملیاتی صورت نگرفته و همچنین به تهدیدهای سایبری در زیرساخت‌های صنعتی حیاتی کمتر توجه شده است.

1. Information Security Management System

ضرورت دفاع سایبری در حوزه صنعتی

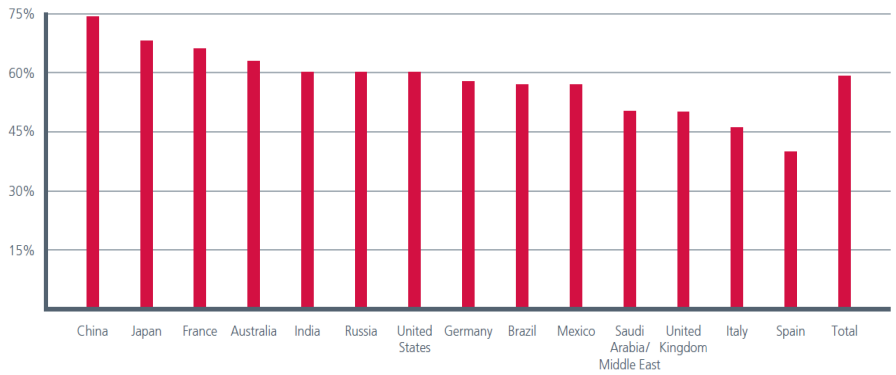
نگاهی به سه حمله بزرگ سایبری اخیر به کشورمان که توسط بدافزارهای استاکس نت، دوکو و فلیم (شعله) انجام گرفت، نشان می‌دهد ابزارهای به‌کاررفته در این حملات به‌مرور تکمیل‌شده‌اند و هر بار بر درجه تخریب آن‌ها افزوده‌شده است. برای پی بردن به اهمیت این تحقیق به برخی تأثیرات حملات سایبری روی تولید، توزیع و مصرف انرژی در دنیا اشاره می‌شود.

تولیدکنندگان انرژی در دنیا: ۸۵ درصد نفوذ در شبکه و ۸۰ درصد قطع خدمات به‌موجب حملات سایبری را تجربه کرده‌اند.

توزیع‌کنندگان انرژی در دنیا: ۵۶ درصد شبکه هوشمند را به اینترنت متصل کردند، ۴۰ درصد بدافزار استاکس نت را تجربه کردند و ۲۵ درصد قربانی حمله سایبری بوده‌اند (Centre for Strategic & International Studies Report, April 19, 2011).

مصرف‌کنندگان انرژی در دنیا: ۳۱ درصد در انتظار وقوع یک حمله بزرگ سایبری هستند که مصرف‌کنندگان (The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, 2010) انرژی را تحت تأثیر قرار می‌دهد (The Economist Mag, 2010: 9-10).

شکل ۱ بیانگر درصد حملات سایبری صورت گرفته علیه زیرساخت‌های حیاتی کشورهای یادشده است:



شکل ۱ ــ درصد حملات سایبری صورت گرفته علیه زیرساخت‌های حیاتی

(Critical Infrastructure in the Age of Cyber War, CSIS, McAfee, 2011**)**

اگرچه به‌کارگیری راهکارهای امنیتی نظیر استفاده از ضد بدافزارها، فایروال‌ها، سامانه‌های تشخیص نفوذ و سامانه‌های کنترل دسترسی و احراز هویت تا حدی می‌تواند شبکه را از حالت انفعالی و بدون نظارت نجات دهد و به تأمین امنیت آن کمک کند، ولی باید به این نکته مهم توجه کرد که به‌کارگیری این تجهیزات امنیتی خود باعث تولید حجم عظیمی از رخدادهای امنیتی در قالب‌های متفاوت می‌شود و به‌خصوص در شبکه‌های زیرساختی با ترافیک بالا این امر چشم‌گیرتر خواهد بود. این حجم بالای داده‌های امنیتی تولیدشده باعث سردرگمی و سلب امکان مدیریت و استفاده از آن‌ها می‌شود. همچنین به اذعان متواتر مراجع امنیتی، ابزارهای دفاعی و هشداردهنده که به‌صورت ایزوله و جزیره‌ای نسبت به یکدیگر فعالیت می‌کنند، نمی‌توانند کارایی قابل قبولی را در سطح کلان به وجود آورند (Valdes, A. Cheung, S. 2009; Rrushi, J. Kang, K. 2009; Gao, W. Morris, T. Reaves, B. Richey, D. 2010). رفتارشناسی سه حمله یادشده نیز بر این موضوع صحه می‌گذارد و ضرورت وجود یک راهکار متمرکز برای رصد، همبستگی سنجی و تحلیل رخدادهای امنیتی در حوزه‌های صنعتی و شبکه‌های اسکادا را نمایان می‌کند (Symantec - w32_stuxnet_dossier, 2011).

با توجه به جدول جامع چالش‌ها و مشکلات امنیتی شبکه‌های اسکادا که استخراج‌شده از بررسی مقالات مرتبط با این حوزه بوده است (جدول ۱)، می‌توان به این نکته اشاره کرد که سامانه‌های اسکادا خدمات، سیاست‌ها و بازبینی‌های دوره‌ای، پچها و وصله‌های امنیتی روتین را که سیستم‌های IT برای برنامه‌ریزی و به‌روزرسانی دریافت می‌کنند، ندارند. درنتیجه در طول زمان سیستم‌های اسکادا ممکن است آسیب‌پذیر شوند. یکی از وظایف مهم مرکز عملیات امنیت، مدیریت مستمر و مؤثر وصله‌های نرم‌افزاری و همچنین پیکربندی وضعیت فعلی همه سامانه‌هاست.

از حیث ضرورت قانونی این پژوهش، تحقق اهداف سند چشم‌انداز و رسیدن به‌جایگاه تعریف‌شده مستلزم توسعه فناوری اطلاعات است و برای تحقق این توسعه، تأمین امنیت فضای سایبری و اتخاذ تدابیر شایسته در برابر حملات ضروری است. حال چنانچه راهبرد و راهکار مشخصی برای دفاع از فضای سایبری کشور در حوزه زیرساخت‌های صنعتی وجود نداشته باشد، نه‌تنها ادامه فعالیت‌های زیرساخت‌های

حیاتی کشور با تهدید مواجه می‌شود، بلکه تحقق اهداف و آرمان‌های سند چشم‌انداز نیز در معرض مخاطره قرار می‌گیرد (ایزدی، ۱۳۹۰: ۲۳).

ضرورت انجام این پژوهش با توجه به تأکیدات اسناد بالادستی روشن می‌شود؛ بنابراین، ضرورت دارد باملاحظه این اسناد و هماهنگی میان آن‌ها با تدوین برنامه‌ها، راهبردها و راهکارهای مناسب، شرایط اجرای آن‌ها فراهم شود. ضرورت توجه به مخاطرات فضای سایبر، تهدیدهای زیرساخت‌های حیاتی، پدافند غیرعامل و... در قالب‌های گوناگون در اسناد زیر اشاره و به آن‌ها اهتمام ورزیده شده است:

ـ سیاست‌های کلی برنامه پنجم توسعه ـ احکام فناوری اطلاعات و ارتباطات؛

ـ سند چشم‌انداز بیست‌ساله جمهوری اسلامی ایران در افق ۱۴۰۴ هجری شمسی؛

ـ نقشه جامع علمی کشور؛

ـ سند راهبردی فضای تولید و تبادل اطلاعات.

مخاطرات و تهدیدهای شبکه‌های اسکادا

همگرایی-IT و صنعت موجب تسری مخاطرات حوزه سایبری به حوزه صنعت شده است. هم‌اکنون مشابه تکنولوژی‌های IT که نقاط آسیب‌پذیری[1] آن‌ها به‌صورت روزانه کشف و گزارش می‌شود، در شبکه‌های اسکادا نیز نقاط آسیب‌پذیری وجود دارد و بعضاً گزارش می‌شود. هرگونه بهره‌برداری سوء[2] از این نقاط آسیب‌پذیر ممکن است موجب خسارات جبران‌ناپذیری شود؛ بنابراین به‌عنوان یک راهکار دفاعی (غیرعامل)، شناخت و رفع این آسیب‌پذیری‌ها مهم ارزیابی می‌شود (دنینگ، ۱۳۸۶: ۶۷)

آسیب‌پذیری‌های شبکه‌های اسکادا را می‌توان به سه گروه دسته‌بندی کرد:

الف) آسیب‌پذیری‌های روال‌ها و سیاست‌ها؛[3]

ب) آسیب‌پذیری‌های سکوها و چارچوب‌ها؛[4]

ج) آسیب‌پذیری‌های شبکه.[1]

1. Vulnerabilities
2. Exploit
3. Policies & Procedures
4. Platforms & Frameworks

در ادامه به تشریح موارد مذکور می‌پردازیم.

۱. آسیب‌پذیری‌های روال‌ها و سیاست‌ها

روال‌های امنیتی نقش حیاتی در امنیت یک سازمان بازی می‌کنند. سیاست‌های مؤثر و کارا می‌توانند ریسک سازمان‌ها و تهدیدهای بالقوه را به‌شدت کاهش دهند. نقصان در سیاست‌ها و روال‌ها باعث بروز آسیب‌پذیری‌ها می‌شود و عدم به‌روزرسانی و بازنگری از علل اصلی این امر در کشور ماست. کمبود سیاست‌های اختصاصی و سفارشی برای شبکه‌های اسکادا کاملاً محرز است. برای مثال به‌کارگیری درایوهای USB Flash- در شرکت‌های کامپیوتری روالی مجاز به شمار می‌آید، اما همین روال در حوزه صنعتی روالی خطرناک و غیرمجاز است (غزنوی، ۱۳۹۱).

همچنین عدم ممیزی دوره‌ای این سیاست‌ها و روال‌ها، چرخه صنعتی را با افزایش نقاط آسیب‌پذیر و به‌تبع آن افزایش ریسک مواجه می‌کند.

۲. آسیب‌پذیری‌های سکوها و چارچوب‌ها

جنبه دیگر به وجودآورنده نقاط آسیب‌پذیر به علت عدم پیکربندی سکوها و چارچوب‌های نرم‌افزاری و سخت‌افزاری به‌کاررفته در شبکه‌های اسکاداست (Vale, Morais, Faria, Khodr, Ferreira, Kadar, 2011). پیکربندی نادرست، خرابی‌های سخت‌افزاری،[2] کمبود ابزارهای کنترل دسترسی، اجرای سرویس‌های غیرضروری، حفاظت کم در مقابل بدافزارها و... از مواردی است که در این گروه دسته‌بندی می‌شوند.

۳. آسیب‌پذیری‌های شبکه

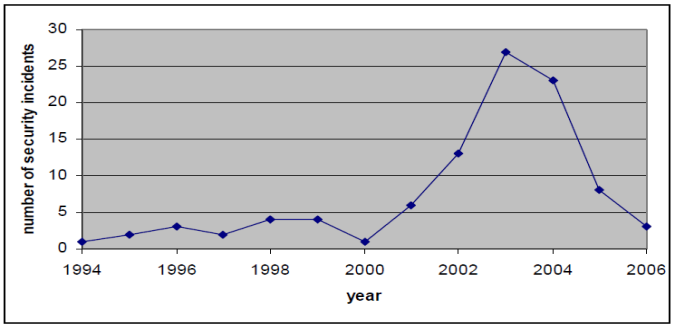
آسیب‌پذیری‌های این گروه مشابه گروه ب است، با این تفاوت که وابستگی آن به ابزارآلات شبکه است. معماری و توپولوژی‌های ضعیف شبکه، قواعد ناصحیح دیوارهای آتش و DMZ ها،[3] پایش نامناسب ترافیک شبکه، اتکای بیش‌ازحد به سامانه‌های

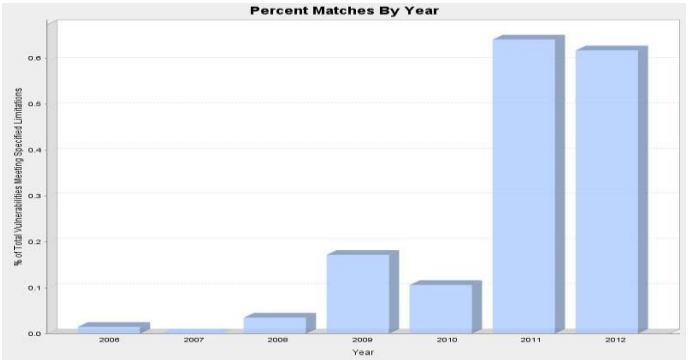
1. Network
2. Hardware Failure
3. Demilitarized Zone

تشخیص نفوذ ایزوله، پیکربندی نادرست مسیریاب‌ها و... از مواردی است که می‌توان اشاره کرد.

به راهکار مناسبی برای شناسایی، بهبود و رفع نقاط آسیب‌پذیر موارد یادشده در شبکه‌های اسکادا نیاز است. نگاهی به‌ضرورت و جایگاه سامانه مدیریت امنیت اطلاعات در حوزه فناوری اطلاعات، مخاطرات و ادله فوق ما را به سمت پیشنهاد ISMS سفارشی‌شده برای شبکه‌های صنعتی سوق می‌دهد. خوشبختانه نزدیکی و همگرایی IT و حوزه صنعتی باعث آسان شدن به‌کارگیری فرآیندها و استانداردهای ISMS با تغییرات جزئی خواهد شد؛ بنابراین به‌عنوان یک نیاز برای کار تحقیقاتی آتی، بومی‌سازی و سفارشی‌سازی سامانه مدیریت امنیت اطلاعات برای شبکه‌های اسکادا امری اجتناب‌ناپذیر و سودمند است.

برای تبیین هرچه بیشتر مخاطرات و شدت تهدیدها، گزارش‌های جمع‌آوری‌شده مراکز معتبر جهانی مبنی بر رخدادها و حوادث شبکه‌های اسکادا و حملات متواتر ارائه می‌شود:



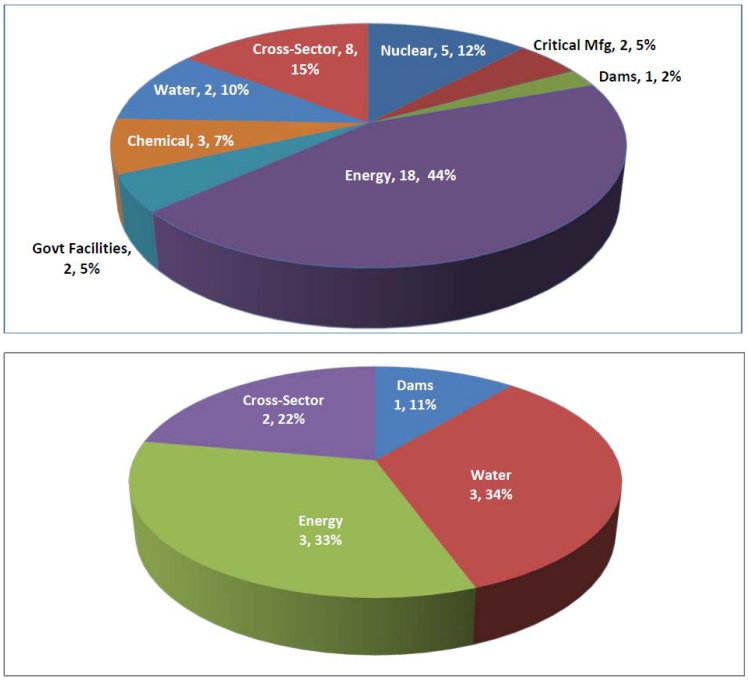


شکل ۲ و ۳ ــ رشد رخدادهای پروتکل‌های صنعتی

(ICS-CERT Incident Response Summary Report, USA, 2009–2011)

بررسی تمامی رخدادهای امنیتی گزارش‌شده به ICS-CERT (تنها CERT صنعتی جهان) از سال ۲۰۰۹ تا ۲۰۱۱ مفاهیم و زوایای مهمی را برای ما روشن می‌سازد. مطالعه تطبیقی بین حملات به کنترل‌کننده‌های صنعتی (ICS)، روند فزاینده مخاطرات این حوزه را نمایان می‌سازد و لزوم تدبیر راهکارهای دفاعی فعال و غیرفعال (پدافند غیرعامل) را بیش‌ازپیش یادآور می‌شود.

اشکال زیر نشان‌دهنده رخدادهای سایبری در حوزه زیرساخت‌های صنعتی به تفکیک نوع صنعت است:



شکل ۴ و ۵ ــ رخدادهای سایبری در حوزه زیرساخت‌های صنعتی به تفکیک نوع صنعت

(USA, April 19, 2011 Centre for Strategic & International Studies Report,**)**

۴۱ گزارش رخداد سایبری در سال ۲۰۱۰ دریافت شده که هشت مورد آن را خود تیم واکنش به رخدادهای رایانه‌ای (CERT) کشف و شناسایی کرده است. همچنین

گزارش حملات سایبری ارائه‌شده توسط NIAC[1] در پیوست آورده شده است.

مرور مقالات و پژوهش‌ها درباره شبکه‌های اسکادا طی دو سال اخیر منتج به استخراج جدول جامعی از نقصان‌های امنیتی، چالش‌ها و راهکارهای ارائه‌شده، زیرساخت دفاعی و زمینه‌های مطالعاتی گذشته شد (جدول ۱). جدول استخراجی علاوه بر جامعیت و ارائه یک دید انتزاعی و کلان از چالش‌ها، مخاطرات و راهکارهای ارائه‌شده قبلی، امکان تعمیم و به‌کارگیری در صنایع و سازمان‌های مختلف را دارد. همچنین این جدول می‌تواند به‌عنوان یکی از مواد اولیه طراحی ریسک مدل‌ها و مدل‌های پیش‌بینی احتمال خطر به‌کاربرده شود.

جدول ۱ ــ جدول جامع سامانه‌های اسکادا

زمینه‌های کلی اشاره‌شده	زیرساخت دفاعی	نیازهای امنیتی	مشکلات و چالش‌ها	راهکارها و پیشنهادها
بررسی اجمالی روی امنیت سایبری زیرساخت‌های حیاتی (با تمرکز بر شبکه برق)	ـ مدل‌سازی حمله و دفاع (مبتنی بر حملات درختی و سلسله مراتبی) ـ شبیه‌سازی جریان برق و رفتار حالت پایدار	ـ ارتباط امن مرکز کنترل و ایستگاه‌های فرعی ـ کاهش ریسک ـ احراز هویت روی دارایی‌ها ـ تعیین حالت ارتجاعی (برگشت‌پذیری) ـ محاسبه شاخص آسیب‌پذیری	ـ حمله به سیستم، حمله توسط سیستم، حمله از طریق سیستم ـ امنیت فیزیکی زیرساخت‌های برق ـ نقاط ضعف ناشی از استفاده از پروتکل‌های استاندارد و عمومی ـ زیرساخت یکپارچه‌شده برق و IT باعث افزایش ریسک ـ حملات منع سرویس	ـ چارچوب امنیتی برای اسکادا با چهار مؤلفهٔ نظارت بلادرنگ، شناسایی ناهنجاری‌ها، تجزیه‌وتحلیل آثار، استراتژی‌های کاهش مخاطرات ـ به‌کارگیری حسگرها برای پایش سلامت انتقال و کاهش آسیب‌پذیری‌ها ـ احراز هویت برای دسترسی به توابع کنترلی خاص از طریق بیومتریک ـ ارزیابی سیستم‌های کنترل فرایند به‌عنوان یک وظیفه ـ تشخیص ناهنجاری‌های مبتنی بر تکنیک‌های همبستگی برای ایجاد ارتباط منظم و سیستماتیک بین مجموعه داده‌های آماری به‌دست‌آمده از منابع مختلف ـ حداکثر شاخص‌های آسیب‌پذیری سناریوها به‌عنوان شاخص آسیب‌پذیری اسکادا در نظر گرفته شود.
مدیریت منابع توزیع‌شده انرژی با استفاده از اسکادا و شبکه‌های هوشمند (توزین عرضه و تقاضا)	ـ بهره‌گیری از روش‌های هوش مصنوعی در مدیریت منابع و شبکه توزیع	ـ ایجاد توسعه پایدار و دسترسی مستمر به انرژی (تداوم کسب‌وکار) ـ ایجاد محیط رقابتی امن ـ اتوماسیون‌سازی به	ـ بروکراسی و قواعد زائد موجب جلوگیری از عرضه On-Demand می‌شود. ـ محدودیت‌های فنی اسکاداهای قدیمی ـ گستردگی و عدم تراکم نقاط، حفاظت و کنترل را سخت کرده و	ـ ارائه چارچوب محاسباتی توانمندی شبکه انرژی و شبیه‌سازی بازار (این روش مدیریت بهینه منابع انرژی با توجه به اهداف و رفتار طرف‌های درگیر را پیش‌بینی می‌کند.) ـ به‌کارگیری یک اسکادای هوشمند و قابل‌انعطاف با استفاده از الگوی

1. National Association of Insurance Commissioners

		اشتراک‌گذاری منابع به‌طور امن ـ فلسفه بهره‌برداری جدید از منابع برق متوازن با پیشرفت چشم‌گیر فنی	ریسک را افزایش داده است. فقدان توافق بر سر بهترین و امن‌ترین پروتکل‌های رایج اسکادا ـ وجود اطلاعات جامع و کامل درباره اجزا حین تصمیم‌گیری	امن، برای اشتراک‌گذاری منابع و اتوماسیون سازی و مدیریت سوییچینگ ـ لزوم اطلاع اسکاداهای هوشمند از سه مؤلفه اجزای سیستم برق: موجودیت فیزیکی و وابستگی‌های عملیاتی، در دسترس بودن اطلاعات اجزا در مراکز تصمیم‌گیری، اجازه به کار بردن آن‌ها
تهدیدها و مخاطرات سامانه‌های کنترل نظارت و کسب اطلاعات (اسکادا)	ـ استناد به طرح وزارت انرژی ایالات‌متحده (DOE) و استفاده از چارچوب پیشنهادی آن برای محافظت از زیرساخت انرژی در ۱۰ سال آینده با همکاری بخش خصوصی ـ تجاری‌سازی تأمین امنیت	ـ ادغام و یکپارچه‌سازی ایمن سیستم‌های کنترل داخلی با IT, ICT ـ روزآمد بودن آگاهی و فناوری به‌موازات یکدیگر ـ ایمنی ارتباطات برون و درون‌سازمانی و اجزای تحت کنترل اسکادا ـ ضرورت وجود سیستم‌های امنیتی پایه: تأیید هویت، تشخیص نفوذ، رمزنگاری و... ـ طراحی ایمن و جامعیت	ـ لحاظ نشدن امنیت در سامانه‌های اسکادای قدیمی (در بیشتر حالات این سامانه‌ها چرخه عمر طولانی و بیش از ۳۰ سال دارند.) ـ همگرایی تکنولوژی‌های روز با سیستم‌های رایانه‌ای کنترل فرایند داخلی (تعمیم مخاطرات) ـ اسکادا، پچها و سرویس‌های به‌روزرسانی روتین را مانند سامانه‌های IT دریافت نمی‌کنند. ـ خطای انسانی (قبل از سال ۲۰۰۱ حدود ۵۰ درصد رخدادها عامل انسانی و ۲۹ درصد عوامل برون‌سازمانی داشت، ولی در سال ۲۰۰۴ تغییر چشم‌گیر با ۶۹ درصد عوامل بیرونی و ۲۲ درصد خطای سهوی به وجود آمد.) ـ ضعف توپولوژی‌های ارتباطی ـ وابستگی بیش‌ازحد به اسکادا و اتوماسیون سازی به‌عنوان یک Trade-Off ـ حملات منع سرویس ـ تولیدکنندگان اسکادا برای طراحی ارزان‌تر رو به استانداردسازی آورده‌اند (اطلاعات سامانه‌ها در اختیار همگان است.) ـ نرم‌افزارها و اجزای جانبی آن‌ها ممکن است عامل به وجود آمدن نقاط آسیب‌پذیر شوند.	ـ جایگزینی اسکادای مدرن با نمونه قدیمی ـ کاهش خطای انسانی با کنترل و نظارت خود سامانه (Self-Checking & Monitoring) ـ توجه پیشگیرانه ساده‌تر و کم‌هزینه‌تر ـ آموزش (موارد امنیتی و کاربردی) در سطوح کارشناسان و همچنین تکنسین‌ها ـ بررسی‌های امنیتی و طرح‌های جدید باید بخشی از برنامه اجرایی سالانه باشد. ـ به‌روزرسانی مستمر در دو بعد نرم‌افزاری و سخت‌افزاری ـ سامانه‌های تشخیص نفوذ باعث مستحکم‌تر شدن اسکادا می‌شود.
بررسی تبادلات امن در شبکه هوشمند برق آینده مبتنی بر سامانه‌های اسکادا و نحوه پیاده‌سازی توابع امنیتی	ـ پیاده‌سازی توابع امنیتی و ارتباطی روی پلتفرم ریزپردازنده‌های چندهسته‌ای همه‌منظوره هم‌زمان با سایر توابع عملیاتی	ـ جمع‌آوری بلادرنگ، نظارت و کنترل تجهیزات و فرآیندها در زیرساخت‌های حیاتی توسط سامانه‌های کنترل نظارت وکسب اطلاعات (اسکادا) در محیطی ایمن ـ بستر ارتباطی امن فی‌مابین مرکز و	ـ شبکه‌های اسکادا مانند سابق ایزوله نیست و به سایر شبکه‌ها متصل است. ـ به کار نبردن پلتفرم‌ها و پروتکل‌های خاص ـ متکی بودن معماری ارتباطی بر پروتکل‌های استاندارد باز ـ توان محاسباتی پایین در سیستم‌های تعبیه‌شده در ایستگاه‌های فرعی (ناتوانی در انجام توابع امنیتی) ـ مدیریت تولید و توزیع کلیدهای	ـ بهره‌برداری بهینه از فضای تراشه‌ها برای بهبود توان محاسباتی و عملیاتی ایستگاه‌های فرعی و سیستم‌های تعبیه‌شده ـ تأکید بر بهره‌گیری از پردازنده‌های چندهسته‌ای به‌جای یک پردازنده پیچیده (چیپ های چندپردازنده‌ای CMP می‌توانند چندین نرم‌افزار را هم‌زمان روی یک تراشه واحد اجرا کنند.) – ارائه مدل اجرای موازی پردازش‌ها (توابع امنیتی توأمان با توابع عملیاتی)

		انشـــعابات (حفـــظ جامعیـــت و صـــحت داده‌ها) ـــ افـــزایش تـــوان محاسباتی و عملیاتی بـــه‌خصـــوص در انشعابات ـــ بررســـی Non-repudiation, Integrity در ارســـال و دریافـــت پیام‌ها	رمزنگاری و رمزگشایی ـــ اجـــرای ســـناریوهای حملـــه Man-In-The-Middle	ـ محرمانگی را به بخش کـوچکی از پیام‌ها محدود کرده، چـون محتـوای پیـام‌هـا عمومـاً قابـل سوءاسـتفاده نیستند. ـ استفاده از MAC به‌عنـوان روش تصدیق اصـالت فرسـتنده و جامعیـت پیام، بـدون سـربار محاسـباتی بـرای رمزنگاری و رمزگشایی

در گزارش اخیری که GAO[1] در دولت آمریکا منتشر کرده، پنج عامل رشـد ریسـک شبکه‌های اسکادا این‌طور بیان‌شده است:

- ✓ وفق‌پذیری فناوری‌های استانداردشده با آسیب‌پذیری‌های شناخته‌شده؛
- ✓ اتصال کنترل‌کننده‌های صنعتی به اینترنت؛
- ✓ محدودیت به‌کارگیری ابزارهای ماشینی موجود؛
- ✓ دسترسی‌های راه دور ناامن؛
- ✓ در دسترس بودن اطلاعات تکنیکال پیرامون کنترل‌کننده‌های صنعتی.

جدول ۱ و نتیجه تحقیقات ما نشان داد که گـزارش GAO و مـوارد یادشـده توسـط دولت آمریکا نیاز به بهبود و تغییراتی دارد؛ بنابراین مبتنی بر سامانه اسکادای به‌کاررفتـه در کشور و با توجه به جدول ۱، موارد زیر به‌جای گزارش GAO پیشنهاد می‌شود.

به‌طورکلی می‌توان چهار روند کلی را کـه باعـث افـزایش ریسـک در شـبکه اسـکادا می‌شود، این‌گونه بیان کرد:

۱. همگرایی فناوری اطلاعات و شبکه‌های اسکادا؛

۲. به‌کارگیری استانداردها و پروتکل‌های عمومی و شناخته‌شده؛

۳. مدنظر قرار ندادن مسائل امنیتی در زمان طراحی اسکاداهای قدیمی (فعال در صنعت)؛

۴. فقدان SOC، CERT، MSSP[2] اختصاصی برای شبکه‌های اسکادا که توان مقابلـه با حملات سایبری پیچیده را فراهم می‌کنند.

1. Government Accountability Office
2. Managed Security Service Provider

مرکز عملیات امنیت برای شبکه‌های اسکادا

زیرساخت‌های حیاتی در حوزه صنعت برای حفاظت از داده‌ها و فرآیندهای صنعتی خود با چالش‌های زیادی روبه‌رو هستند. همان‌طور که در بخش قبل اشاره شد، مخاطرات فزاینده‌ای شبکه‌های اسکادا را تهدید می‌کند. این تهدیدها روزبه‌روز پیچیده‌تر و پیشرفته‌تر می‌شوند. پیچیدگی و گوناگونی تجهیزات صنعتی، امر حفاظت از داده‌ها در مقابل حملات ناشناخته[1] یا حملات چند گامی[2] را دشوارتر می‌کند.

گستردگی و توزیع شبکه‌های اسکادا، پایش و حفاظت از آن‌ها را با ابزارهای جزیره‌ای (مستقل از هم) موجود، غیرممکن می‌سازد. در طراحی سامانه‌های اسکادای جدید به درخواست‌های مخاطب و همچنین ملاحظات امنیتی تا حدی توجه می‌شود (Hong, Phuong, Lee Dept, 2012)؛ اما اسکاداهای قدیمی‌تر از این امر مستثنی بوده‌اند و حداقل موارد امنیتی در آن‌ها رعایت نشده است. اقدامات زیادی برای ایمن‌سازی اسکاداهای قدیمی انجام‌گرفته است؛ اما نتایج محدود و هزینه بری در پی داشته است. حوزه صنعت و دفاع سایبری در حوزه زیرساخت باید راه‌حلی برای پایش، کنترل و شناسایی حملات سایبری پیاده‌سازی کند.

مرکز عملیات امنیت به‌عنوان پیشنهاد تجربه‌شده در حوزه فناوری اطلاعات برای حوزه صنعت نیز تجویز می‌شود. در ادامه به تشریح پیشنهاد فوق، مزایا و معایب آن، تغییرات موردنیاز و ارائه معماری انتزاعی از SOC برای حوزه صنعتی می‌پردازیم.

اگرچه به‌کارگیری راهکارهای امنیتی نظیر استفاده از ضد بدافزارها، سامانه‌های احراز هویت، فایروال‌ها، IDS[3] و IPS[4] و سامانه‌های کنترل دسترسی تا حدی می‌تواند شبکه را از حالت انفعالی و بدون نظارت نجات دهد و به تأمین امنیت آن کمک کند، ولی باید به این نکته مهم توجه کرد که به‌کارگیری این تجهیزات امنیتی خود باعث تولید حجم عظیمی از رخدادهای امنیتی در قالب‌های متفاوت می‌شود. این حجم بالای داده‌های امنیتی تولیدشده به سردرگمی و سلب امکان مدیریت و استفاده از آن‌ها می‌انجامد. استفاده از راهکارهای

1. Zero-day Attacks
2. Multi-step Attacks
3. Intrusion Detection System
4. Intrusion Prevention System

مدیریت و رصد امنیتی به‌ضرورتی اجتناب‌ناپذیر برای افزایش امنیت و پایداری شبکه و سامانه‌های اطلاعاتی و ارتباطی تبدیل‌شده است. رخدادهای امنیتی در یک زیرساخت اطلاعاتی توسط حسگرهای شبکه آن تولید می‌شوند. حسگرهای شبکه شامل همه سیستم‌عامل‌ها، کاربردها، نرم‌افزارها و تجهیزات سخت‌افزاری شبکه است. رخدادهای امنیتی به روش‌های مختلف از حسگرها جمع‌آوری و با قالب یکسانی در بانک اطلاعاتی رخدادها ذخیره می‌شوند (غزنوی، ۱۳۹۱). رخدادهای جمع‌آوری‌شده توسط SOC مورد تحلیل قرار می‌گیرد و پس از بررسی همبستگی بین رخدادها، حملات و تهدیدهای امنیتی زیرساخت اطلاعاتی مربوط به‌صورت رویداد اعلام می‌شود.

تحلیلگر SOC برای آنالیز و تشخیص همبستگی بین رخدادها از دانش ذخیره‌شده در پایگاه دانش مرکز عملیات امنیت بهره می‌برد. معیار اصلی کشف حملات و تهدیدها، اطلاعات پایگاه دانش است. اطلاعات مربوط به آسیب‌پذیری‌های سامانه، سیاست‌های امنیتی تعریف‌شده و همچنین وضعیت فعلی سامانه‌ها از اطلاعات مهم ذخیره‌شده در پایگاه دانش به‌طور مرتب باید توسط واحدی در SOC به‌روز شود.

ضرورت وجود SOC

علاوه بر نکات یادشده در بخش‌های قبل مقاله، SOC کمک به بهبود و حل مسائل زیر می‌کند (Cheung, Valdes,2009; Morris, Vaughn, Dandass, 2012; غزنوی، ۱۳۹۱؛ مرکز پدافند غیرعامل فاوا، ۱۳۸۸):

- ✓ پاسخگو نبودن به تهدیدها به‌صورت بلادرنگ و روشمند؛
- ✓ کمبود رویکرد هماهنگ تکنیکال برای پیشگیری، تشخیص و بازیابی و مقابله با حملات سایبری؛
- ✓ عدم به اشتراک‌گذاری اطلاعات پیرامون تهدیدها و حملات که منتج به آسیب دیدن سایت‌های صنعتی گوناگون از یک حمله می‌شود.
- ✓ فقدان پایش شفاف از وضعیت رخداد تا مرحله بازیابی؛
- ✓ تشخیص ندادن نقاط آسیب‌پذیر و بدافزارهای غیرفعال؛
- ✓ پایین بودن ضریب تداوم کسب‌وکار و محرمانگی داده‌ها؛

- ✓ عدم کارایی سامانه‌های تشخیص نفوذ و پیشگیری از نفوذ در حملات توزیع‌شده و چند گامی؛
- ✓ پایین بودن قدرت تشخیص تغییر و دست‌کاری پیکربندی ادوات و ابزارها؛
- ✓ فقدان گزارش‌های سطح بالای مدیریتی از تجمیع و همبستگی سنجی رخدادها.

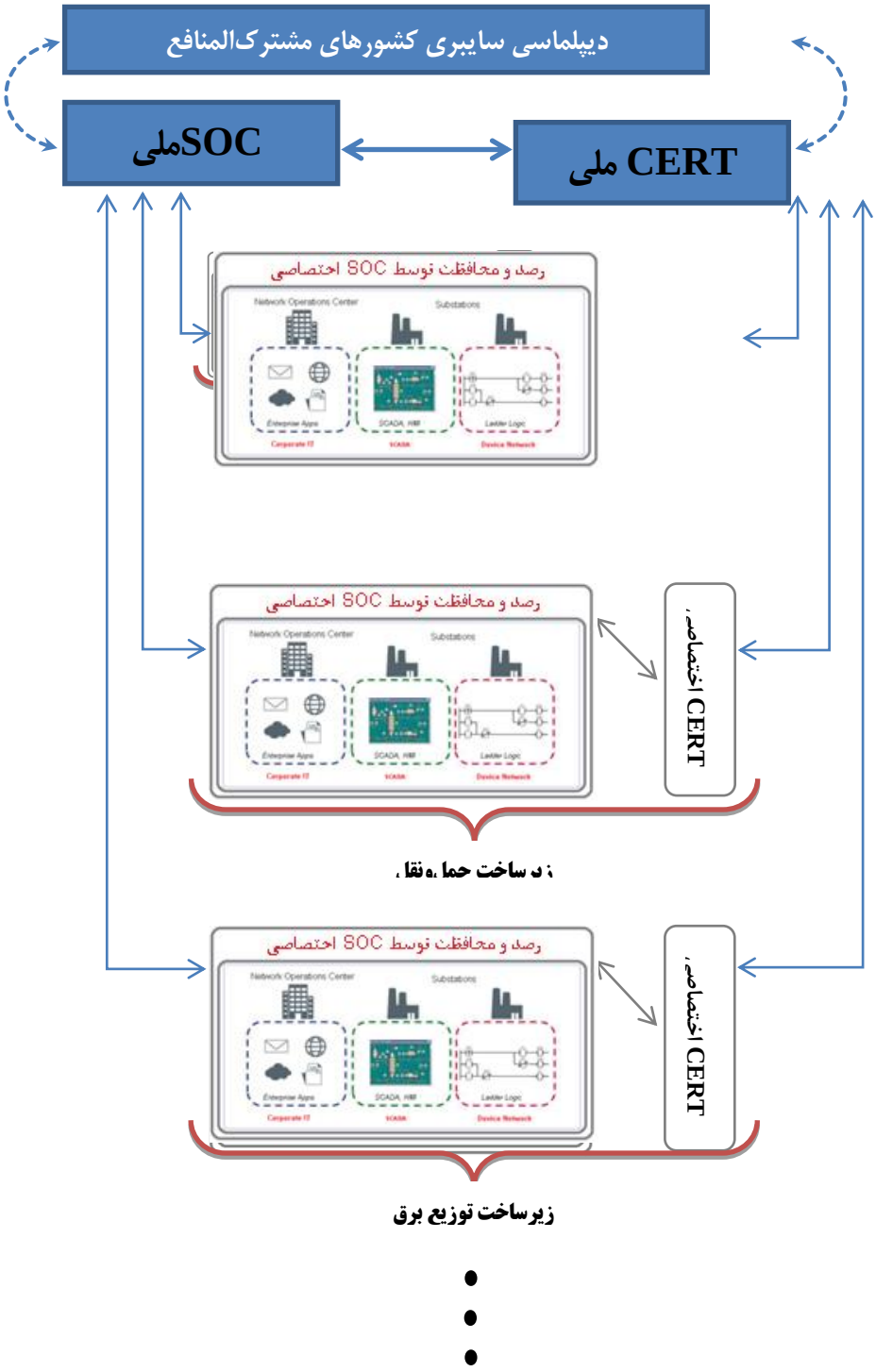
پیچیدگی پیاده‌سازی SOC زمانی بروز می‌کند که باید تمامی اجزا و مؤلفه‌های موجود را یکپارچه کنیم. استانداردها و پروتکل‌های مدرن، بسیاری از مشکلات یکپارچه‌سازی و همبستگی را رفع کرده‌اند؛ اما همان‌طور که در قسمت‌های پیشین اشاره شد، عمومیت و در دسترس بودن اطلاعات فنی این پروتکل‌ها خود به‌مثابه چاقوی دو لبه‌ای است که از یک‌سو مزیت فوق را همراه دارد و از سوی دیگر باعث شناخته شدن عمومی آسیب‌پذیری‌های این پروتکل‌ها می‌شود که می‌تواند مورد سوءاستفاده قرار گیرد.

سامانه‌های تشخیص نفوذ کنونی، به‌صورت جزیره‌ای عمل می‌کنند. هرقدر این سامانه‌ها به‌روز و بهینه باشند، در مقابل حملات چندمرحله‌ای و چند گامی[1] کاملاً منفعل‌اند و قدرت تشخیص خود را از دست خواهند داد. به‌عبارت‌دیگر سناریو یک حمله پیچیده و توزیع‌شده، فقط در حد یک حمله اولویت پایین تشخیص داده می‌شود و فرآیندهای دفاع سایبری سطح پایین برای آن انجام می‌گیرد.

با توجه به حملات سایبری اخیر به کشور و با در نظر گرفتن آناتومی و رفتارشناسی حملاتی همچون استاکس نت، خلأ روش‌های مقابله کارا کاملاً حس می‌شود. درمجموع، ضرورت وجود مکانیزمی در حوزه دفاع سایبری در کشورمان که توانایی تشخیص و مقابله با حملات سایبری در حوزه صنعتی و مصون نگه‌داشتن زیرساخت‌های حیاتی از تهاجمات سایبری را داشته باشد، امری اجتناب‌ناپذیر است.

تجارب پیاده‌سازی SOC در حوزه فناوری اطلاعات نشان می‌دهد که رویکرد توأمان انتزاعی- عملیاتی، نتایج اطمینان‌بخش‌تری همراه دارد. ایده اصلی این مقاله ارائه معماری انتزاعی از مرکز عملیات امنیت برای زیرساخت‌های حیاتی کشور است که با بهره‌گیری از معماری‌های فناورانه، عملیاتی، C4ISR (پیوست ۳) گذشته به‌دست‌آمده است:

1. Cascading & Multistep



شکل ۶ ــ معماری انتزاعی مرکز عملیات امنیت

در معماری پیشنهادی، SOC وCERT -اختصاصی برای هر زیرساخت حیاتی (انرژی، حمل‌ونقل، مخابرات و...) تعریف‌شده است که تعامل دوطرفه با یک SOC ملی و CERT ملی دارد. SOC وCERT اختصاصی هر حوزه صنعتی این امکان را فراهم می‌کند تا متخصصین برای همان حوزه تربیت شوند و توانایی واکنش مناسب را در حوزه خود داشته باشند.

ارتباط دوطرفه با SOC ملی و CERT ملی امکان مدیریت متمرکز و پایش مستمر زیرساخت‌های حیاتی کشور را فراهم می‌آورد و واکنشی هماهنگ را به دنبال دارد. توان تشخیص صحیح دامنه حملات سایبری و پیچیدگی آن‌ها از مزایای دیگر معماری پیشنهادی است.

با توجه به توزیع جغرافیایی حملات سایبری و متدهای شیوع آن‌ها و با نظر کردن به گستردگی حملاتی همچون STUXNET، Duqu، Flame و... پیشنهاد دیپلماسی فضای سایبری را در این معماری ارائه کرده‌ایم. درواقع مسری بودن و شیوع بدافزارهای مختلف و دینامیسم فضای سایبر و گردش اطلاعات ایجاب می‌کند تا کشورهای مشترک‌المنافع در موضوع فضای سایبری نیز مشارکت و همکاری داشته باشند. این امر سبب مصونیت هر چه بیشتر سایر کشورهای مشترک‌المنافع از گزند یک حمله سایبری تشخیص داده‌شده می‌شود.

در شکل ۶ خطوط نقطه‌چین ارتباط و تعامل دوطرفه SOC ملی و CERT ملی را با سازمان‌های همتای خود در سایر کشورهای دوست نشان می‌دهد. در معماری پیشنهادی، این ارتباط به شکل افقی دیده‌شده به معنای یک تعامل پشتیبان و نه یک ارتباط سلسه‌مراتبی و حاکمیتی است.

مزایای معماری پیشنهادی

- ✓ ارتقای ظرفیت تشخیص و پاسخ‌دهی به حملات سایبری در زیرساخت‌های حیاتی (واکنش هوشمند) مدیریت‌شده و هماهنگ بین شبکه‌های اسکادا برای پاسخ و کاهش تهدیدها؛
- ✓ پایش وضعیت امنیتی سامانه‌های اسکادا و کاهش گزارش‌های مازاد؛
- ✓ همگام شدن با مراکز آپا و CERT ملی؛

- ✓ استخراج آنالیز و تحلیل از وضعیت رخدادهای امنیت سایبری؛
- ✓ ایجاد پایگاه دانش بومی از حملات سایبری؛
- ✓ استخراج پایگاه امضای بومی؛
- ✓ فراهم آمدن امکان گزارش‌گیری در سطوح مختلف انتزاع؛
- ✓ مدیریت یکپارچه تهدیدها در زیرساخت‌های حیاتی کشور؛
- ✓ فرایند مدیریت پایدار و روشمند؛
- ✓ توان تشخیص حملات ناشناخته و افزایش توان دفاع سایبری در مقابل حملات توزیع‌شده و چندمرحله‌ای؛
- ✓ مدیریت یکپارچه نقاط آسیب‌پذیر و اعمال وصله مناسب؛
- ✓ تمرکز بر رفتارشناسی، آناتومی و داده‌کاوی حملات سایبری و به‌تبع آن گزینش واکنش هوشمندانه تدافعی.

از فواید دیگر SOC- و CERT برای زیرساخت‌های حیاتی، ایجاد پایگاه دانش حملات و امضاها و همچنین ره آرایی[1] بومی از آن‌هاست. این ثمرات کمک شایانی به ارتقای سطح ارزیابی ابزارهای امنیتی در آینده نزدیک خواهد کرد.

مورد دیگری که نیاز به توجه دارد، تمرکز بر پروتکل‌های شبکه‌های اسکادا نظیر Modbus، Profibus، DMP3 و... است که در کشور ما کاربرد گسترده‌ای دارند. متأسفانه سامانه‌های تشخیص نفوذ که رکن اصلی یک مرکز عملیات امنیت سایبری هستند، روی این پروتکل‌ها عملکرد ضعیفی دارند یا به علت تحریم، دسترسی به پایگاه امضای آن‌ها مقدور نیست. خوشبختانه به‌رغم مسئله فوق، سایر فرآیندهای SOC، مانند جمع‌آوری، همبستگی سنجی، اولویت‌بندی، صدور تیکت، ارجاع به CERT در موارد ناشناخته و... مشابه حوزه فناوری اطلاعات در حوزه صنعتی نیز قابل پیاده‌سازی و اجراست.

در یک جمع‌بندی انجام‌شده در این پژوهش می‌توان محدودیت‌ها و مشکلات پیش رو برای پیاده‌سازی و اجرای SOC را برای سامانه‌های اسکادا و حوزه صنعتی این‌طور برشمرد:

- ✓ محتوای جمع‌آوری از شبکه‌ای به شبکه دیگر متفاوت است؛ برای مثال در شبکه

1. Taxonomy

توزیع برق، جریان محتوای نهایی است که باید توسط حساسه ها[1] رصد شود.

- ✓ بر اساس بند قبل، حساسه های گوناگون برای زیرساخت‌های متفاوت نیاز است.
- ✓ نیاز به زبان مشترک برای همبستگی و یکپارچه‌سازی گزارش‌های دریافتی از زیرساخت‌های متفاوت؛
- ✓ در بسیاری از حوزه‌ها مانند مخابرات، دیتای رمزشده قابل کاوش و بررسی نیست که خود از چالش‌های مرکز عملیات امنیت است.
- ✓ بعضی از سرویس‌ها نیازمند نصب برنامه‌های سمت سرور و سمت مشتری[2] است که در حوزه صنعتی کمبود برنامه‌های سازگار با PLC های صنعتی چالش‌انگیز است.
- ✓ حجم بالای ترافیک تولیدشده امکان تحلیل را برای SOC دشوار می‌کند.

نتیجه‌گیری

این مقاله با ارائه معماری انتزاعی از مرکز عملیات امنیت (SOC) و مرکز واکنش به رخدادهای رایانه‌ای (CERT) برای شبکه‌های اسکادا که کنترل‌کننده زیرساخت‌های حیاتی کشورند، سعی بر بهبود وضعیت امنیتی و پایش این سامانه‌ها دارد. SOC اختصاصی برای حوزه صنعتی راهکار دفاعی مناسب و تجربه‌شده‌ای است در مقابله با تهاجمات سایبری به‌خصوص حملات پیچیده چند گامی و چندمرحله‌ای.

بررسی مخاطرات و تهدیدها در شبکه‌های اسکادا و ارائه جدول جامعی از آن‌ها از خروجی‌های دیگر این پژوهش به شمار می‌آید و می‌تواند منشأ تحقیقات آتی و استخراج ریسک مدل یا مدل‌های پیش‌بینی خطر شود. همچنین با رفتارشناسی و تحلیل شیوع بدافزارهایی مانند Stuxnet، Duqu و Flame، دیپلماسی سایبری کشورهای مشترک‌المنافع پیشنهادشده است.

1. Sensors
2. Client

پیوست ۱: تحقیقات و پژوهش‌های گذشته

۱. پروژه‌های تحقیقاتی

عنوان تحقیق: الزامات جنگ‌های نوین در فضای مجازی (سایبر)

این تحقیق به کوشش وزارت دفاع و پشتیبانی نیروهای مسلح، مؤسسه آموزشی و پژوهشی صنایع دفاعی، مرکز آینده‌پژوهی علوم و فناوری دفاعی در دی ۱۳۸۴ به انجام رسید.

محورهای تحقیق

- آثار انقلاب اطلاعات و نقش آن در جنگ
- تجارب و رویکردهای کشورهای مختلف در دفاع سایبر
- انواع حملات نفوذگرها
- اصول امنیت در دفاع سایبر

۲. پایان‌نامه‌ها و رساله‌ها

رساله جهانی‌شدن فناوری اطلاعات و ارتباطات و تأثیر آن بر امنیت ملی جمهوری اسلامی ایران (اصلانی مقدم، ۱۳۸۵)

رساله فوق متعلق به دکتر مصطفی اصلانی مقدم در اردیبهشت ۱۳۸۵ دفاع شد. سؤال اصلی رساله به این شرح است: تأثیر جهانی‌شدن فناوری اطلاعات و ارتباطات بر عناصر ساختار، آموزش (حوزه مطالعات راهبردی)، تجارب جنگی (قدرت عملیات) و سیستم جنگ‌افزاری و تجهیزات نظامی (سامانه‌ها و فناوری‌های نظامی اثرگذار در ارتقای قدرت نظامی) و قدرت نظامی جمهوری اسلامی ایران چگونه بوده است؟

۳. مقاله‌ها و همایش‌های علمی و پژوهشی داخلی

- عنوان مقاله: «تهدیدات شبکه‌ای» (گروه پدافند غیرعامل وزارت دفاع، ۱۳۸۷)

این مقاله به کوشش گروه پدافند غیرعامل وزارت دفاع در سال ۱۳۸۷ به بررسی حملات شبکه‌ای در حوزه امنیت شبکه‌ای و سامانه‌های اطلاعاتی و مشکلات پیچیده ناشی از آن پرداخته است.

محور تحقیق: تروریسم شبکه‌ای و حملات شبکه‌ای چیست و چه تهدیدهایی را علیه

زیرساخت‌های اساسی همراه خواهد داشت؟

ـ عنوان مقاله: «ضرورت ایجاد مرکز عملیات امنیت از نگاه پدافند غیرعامل»

این تحقیق به کوشش مرکز پدافند غیرعامل فاوا در سال ۱۳۸۸ تهیه شد.

۴. پروژه‌های ملی مرتبط

در حال حاضر پروژه معماری و طراحی مرکز عملیات امنیت بومی مبتنی بر راهکارهای متن‌باز، مرکز پدافند غیرعامل فاوا و همچنین مرکز تحقیقات مخابرات در حال پیگیری است.

مطالعات و تحقیقات متعددی در حوزه‌های صنعتی به‌خصوص شبکه‌های اسکادا و ایمن‌سازی و امنیت سایبری آن‌ها در سراسر دنیا انجام‌گرفته است که در ادامه به بارزترین آن‌ها اشاره می‌شود:

ـ پژوهش پیرامون بسترهای صنعتی و امنیت سامانه‌های اسکادا توسط آقایان Junaid Zubairi, Athar Mahboob به‌صورت Case Study روی چهار موردحمله صنعتی ۱۹۹۹ تا ۲۰۰۳ رخداده است. در خروجی این تحقیقات که در (Mahboob A. Zubairi J. 2010) اشاره‌شده است، راهکارهای کلی و کلان برای ایمن‌سازی شبکه‌های اسکادا بیان‌شده است.

ـ مقالات متعددی در حوزه سامانه‌های تشخیص نفوذ برپایه ناهنجاری منتشرشده که پس از بررسی به علت یادشده در قسمت بیان موضوع، تحلیل و بررسی شد. نمونه آن‌ها (Shosha, Gladyshev, Chen-Ching, 2009; Fovino, Carcano, Murel, Trombetta, 2010; Carcano, Coletta, Masera, 2011; Mathew, Britt, Sudit, Stotz, Upadhyaya, 2011) و کارهای مرتبط قبلی اشاره‌شده در آن‌هاست.

ـ دسته دیگری از پژوهش‌ها از منظر دیگری به سامانه‌های تشخیص نفوذ برای سامانه‌های اسکادا نگاه کرده‌اند. بررسی وضعیت فعلی اسکادا و پیش‌بینی وضعیت بعدی، ایده اصلی این تحقیقات بوده است. State-Based IDSها با شبیه‌سازی PLCها، RTU ها و MTU و تحلیل رفتار این اجزا، به کشف مخاطرات و حملات می‌پردازند. در مقالات (ICS-CERT Incident Response Summary Report, USA, 2009–2011; Shosha, Gladyshev, Chen-Ching, 2009; Mathew. Britt, Sudit, Stotz, Upadhyaya, 2011) بخشی از خروجی‌ها و نحوه عملکرد آن‌ها تشریح شده است.

ـ تعداد معـدودی از پـژوهش‌هـا تمرکـز خـود را روی دسـته‌بنـدی حمـلات و ارائـه راهکارهای تشخیصی بر اساس رفتارشناسی و آناتومی حمله قـرار داده‌انـد. ازجملـه ایـن تحقیقات می‌توان به (Cheung, Valdes, 2009) اشـاره کـرد کـه دپارتمـان مهندسـی و کامپیوتر دانشگاه نیویورک انجام داده است. رویکرد اصلی گروه‌بندی آن، جدول حمـلات پیشنهادشده در این مقاله است که از آناتومی آن‌ها استخراج‌شده است.

پیوست ۲: گزارش حملات سایبری ارائه‌شده توسط NIAC

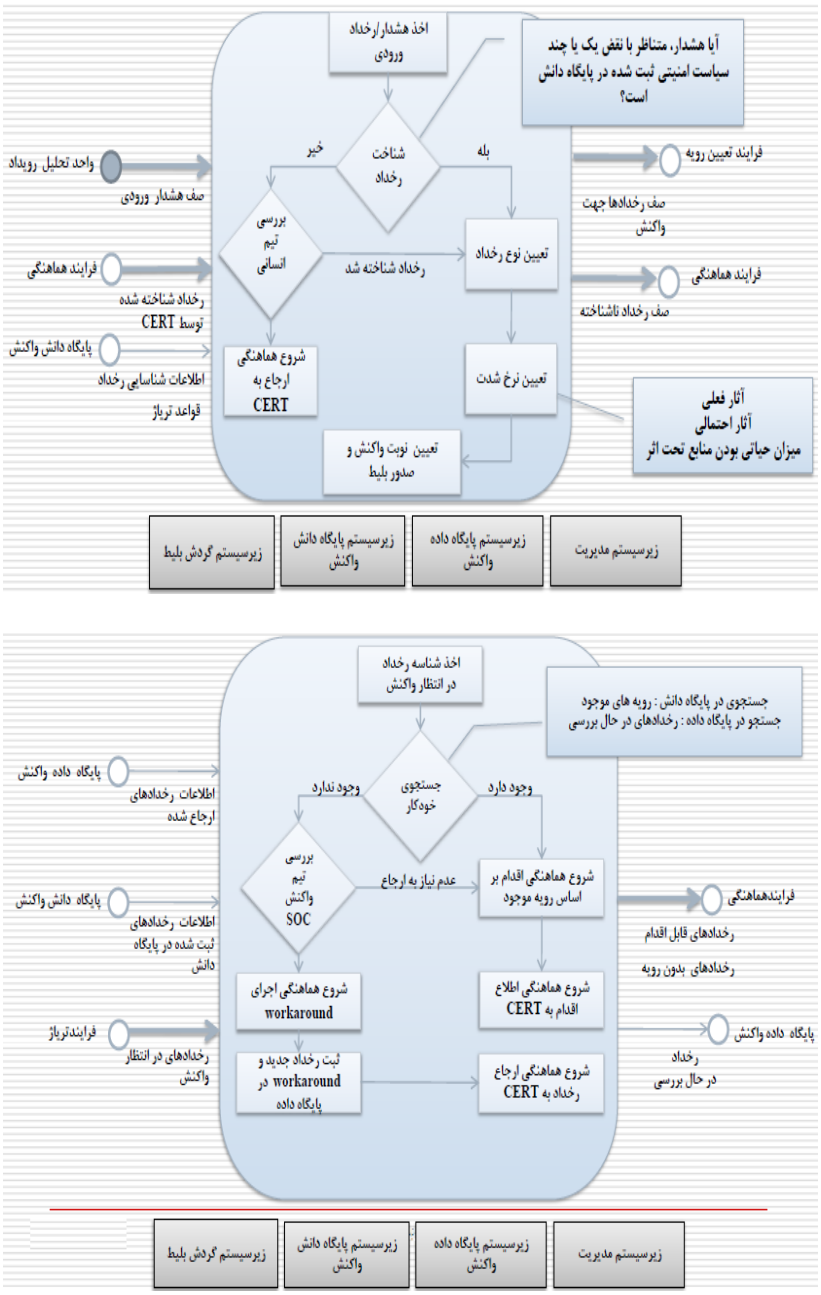
(National Association of Insurance Commissioners)

A Short Chronological List of Widely Reported Incidents of Hacking and Disruption	
Feb 2009	Highly evasive Conficker/Downadup worm infects 12 million computers, stealing information. - BBC
Jun 2008	"Security Hole Exposes Utilities to Internet Attack" - Associated Press
May 2008	SCADA vulnerability...control software used by one-third of industrial plants. - SC Magazine
Mar 2008	Emergency 2-day shutdown of Hatch nuclear plant from software update on one business computer.
Feb 2008	Retail Chinese digital picture frame virus steals passwords and financial info. - SF Chronicle
Jan 2008	Hackers turn out the lights in multiple cities and demand extortion payments." - Associated Press
Sep 2007	DOE Idaho National Lab video shows the remote destruction of a large SCADA controlled generator.
Sep 2007	Hackers compromise Homeland Security computers, moving information to Chinese websites. - CNN
Jul 2007	3Com's security division demonstrates how SCADA system flaws can be exploited.
Nov 2007	"Insider Charged with Hacking California Canal System" - ComputerWorld
Nov 2007	"Solar Sunrise" - Three teenagers penetrate USAF logistic systems at Middle East support bases.
Aug 2007	"Hackers Take Down the Most Wired Country in Europe" for two weeks. - Wired Magazine
Jun 2006	"Information on SCADA systems can be found by a determined attacker." - US-CERT
Jan 2006	Homeland Security Conference - SCADA systems are vulnerable to intrusion. - UrgentComm
Jan 2006	"SCADA Security & Terrorism: We're Not Crying Wolf" conference presentation. - Xforce Security
Aug 2005	175 companies including Caterpillar, General Electric, UPS and DaimlerChrysler attacked by Zotob worm.
2003-2005	Undetected for 2 years, Chinese Army downloads 10-20 terabytes data from Pentagon, DOE, others.
Aug 2003	CSX loses signaling & dispatch control over 23 state railroad due to a worm virus. - InformationWeek
2003	"Cyber War" - PBS Frontline documents penetration of US utilities using commonly known methods.
Jan 2003	Davis-Besse nuclear plant safety monitoring system knocked offline 5-hours by the Slammer worm.
Jan 2003	"Slammer" worm infects 300,000 computers in the first 15 minutes, interrupting 911 and airlines.
Sep 2001	"Nimda" worm infects millions of computers causing billions of dollars in damage. Originator unknown.
Jul 2001	"Code Red" worm infects 300,000 computers in a month and then launches an attack on White House web.
Apr 2000	Hackers succeeded in gaining control of the world's largest natural gas pipeline network (GAZPROM).
Apr 2000	Hacker uses a SCADA system to dump millions of gallons of sewage onto hotel grounds for 3 months.
1998-2000	"Moonlight Maze" - For two years, hackers penetrated the Pentagon, NASA, DOE, university research labs.
1998	A 12-year-old hacks into Roosevelt Dam, with complete SCADA system control of massive floodgates.
1997	"Eligible Receiver" - DOD & Joint Chief Command hacked in 48 hours with publicly available methods.
1997	A teenager hacks into NYNEX and cuts off air/ground communication to Worchester Airport for 6 hours.
	Many more incidents go unreported for reasons of national security or corporate embarrassment. Even more go undetected. Properly executed, successful hacks are undetectable and untraceable.

شکل ۷ ــ گزارش حملات سایبری ارائه‌شده توسط NIAC

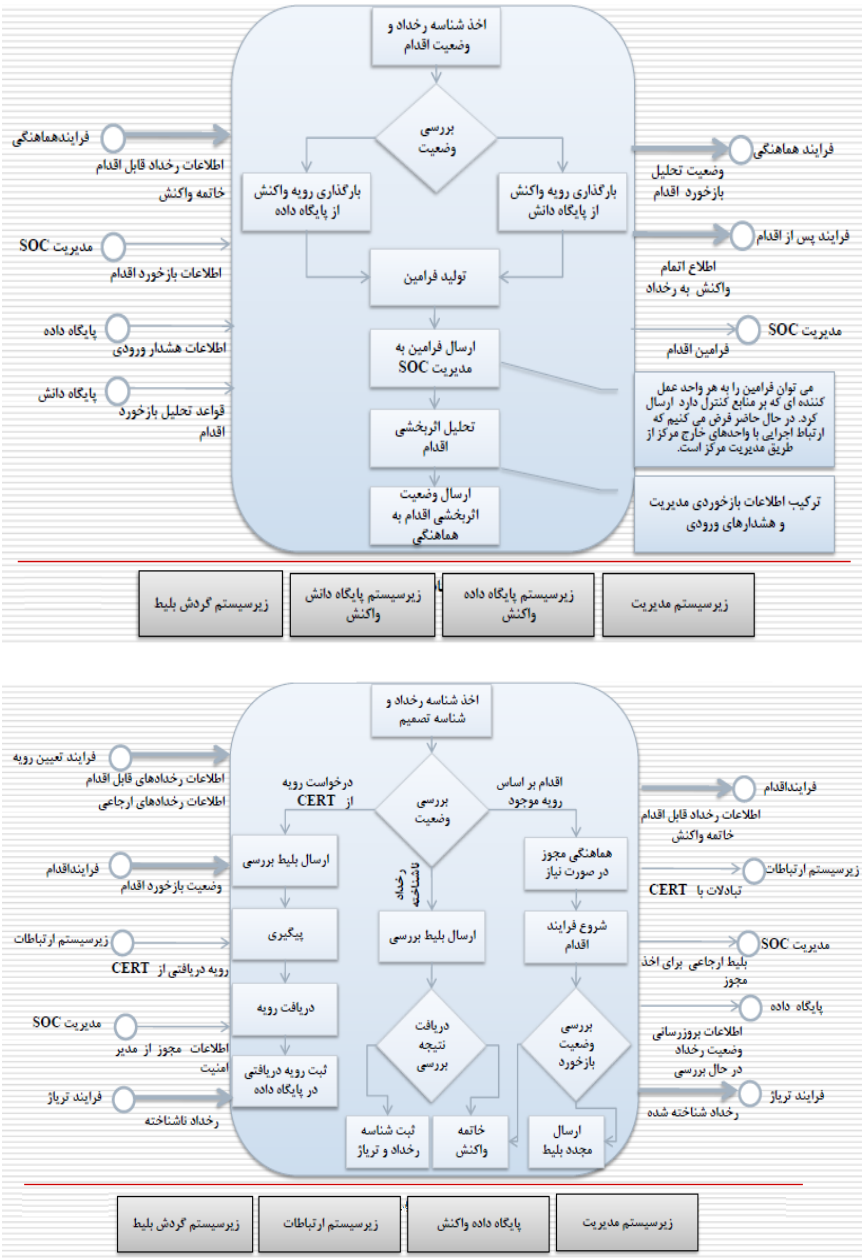
پیوست ۳: معماری‌ها و فرآیندهای عملیاتی مرکز عملیات امنیت

۱. تریاژ و تحلیل حادثه، تعیین رویه (معماری عملیاتی)



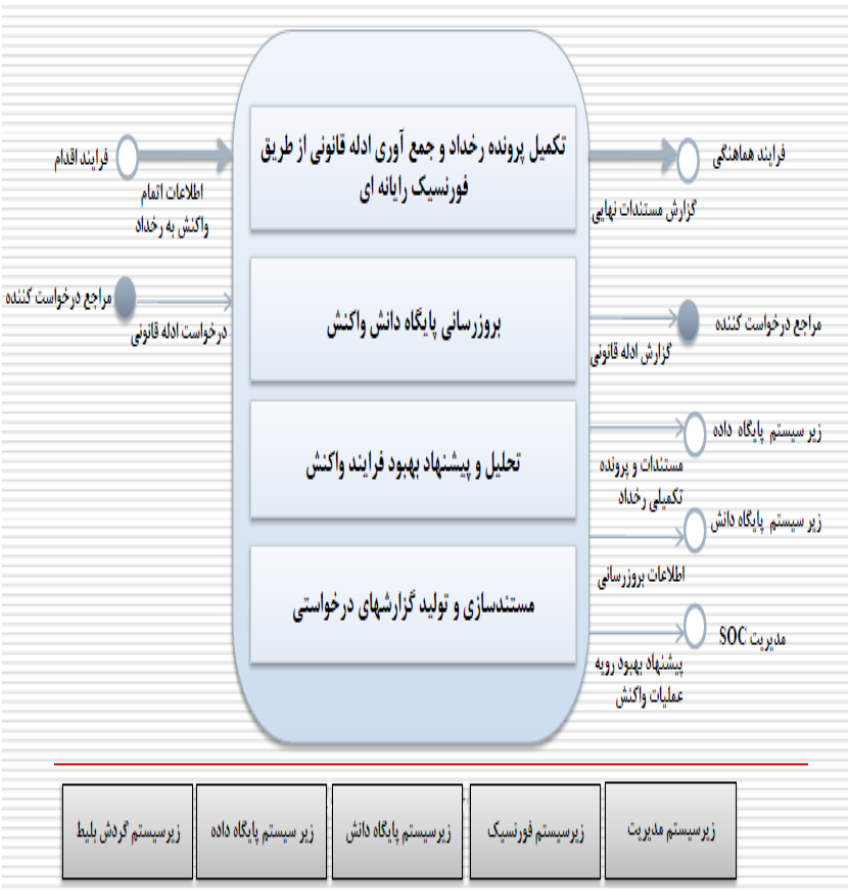
شکل ۸ ــ تریاژ و تحلیل حادثه تعیین رویه (معماری عملیاتی) (غزنوی، ۱۳۹۱)

۲. هماهنگی و اقدام (معماری عملیاتی)



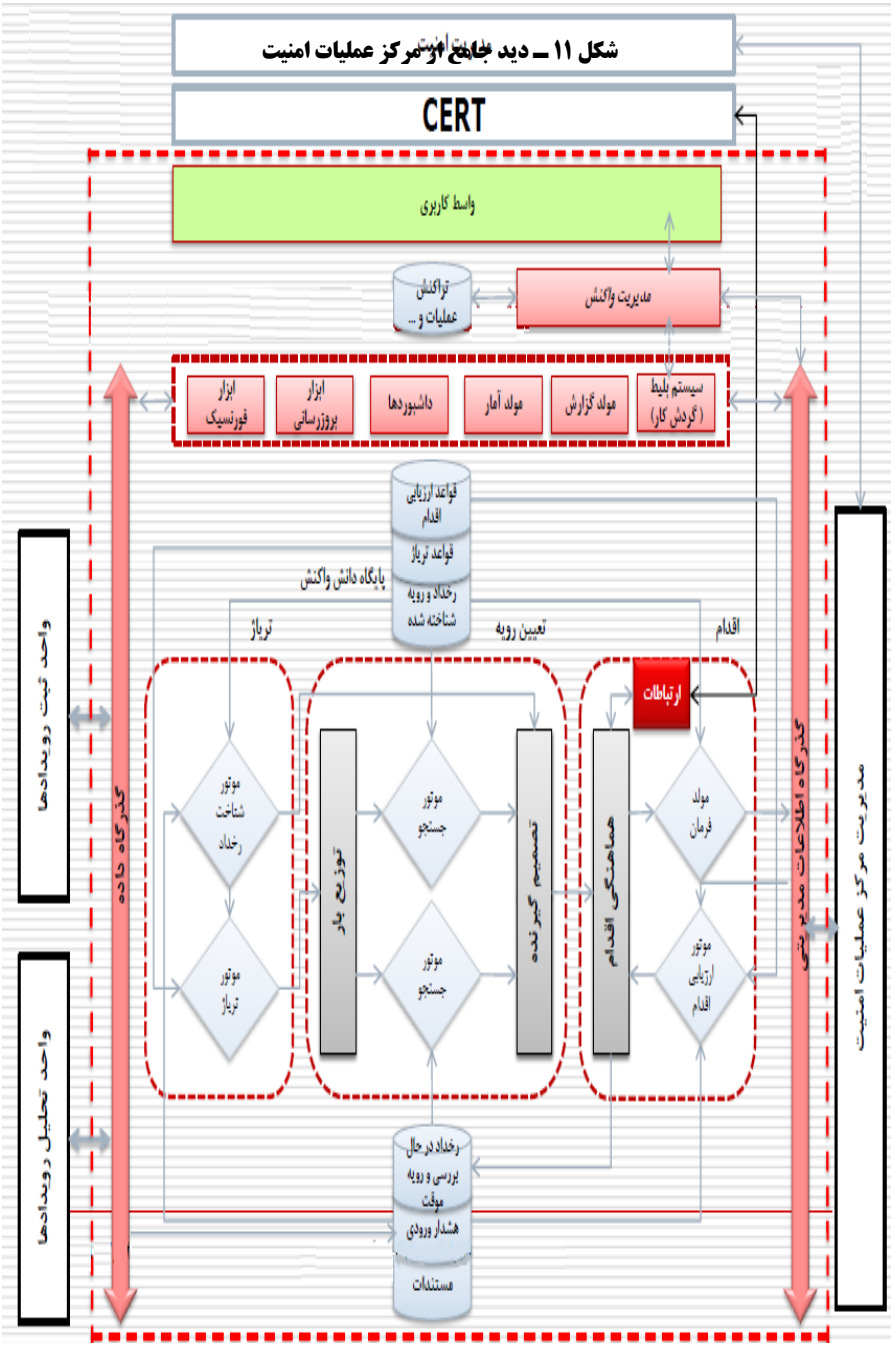
شکل ۹ ــ هماهنگی، اقدام (معماری عملیاتی) (غزنوی، ۱۳۹۱)

۳. پس از اقدام (معماری عملیاتی)



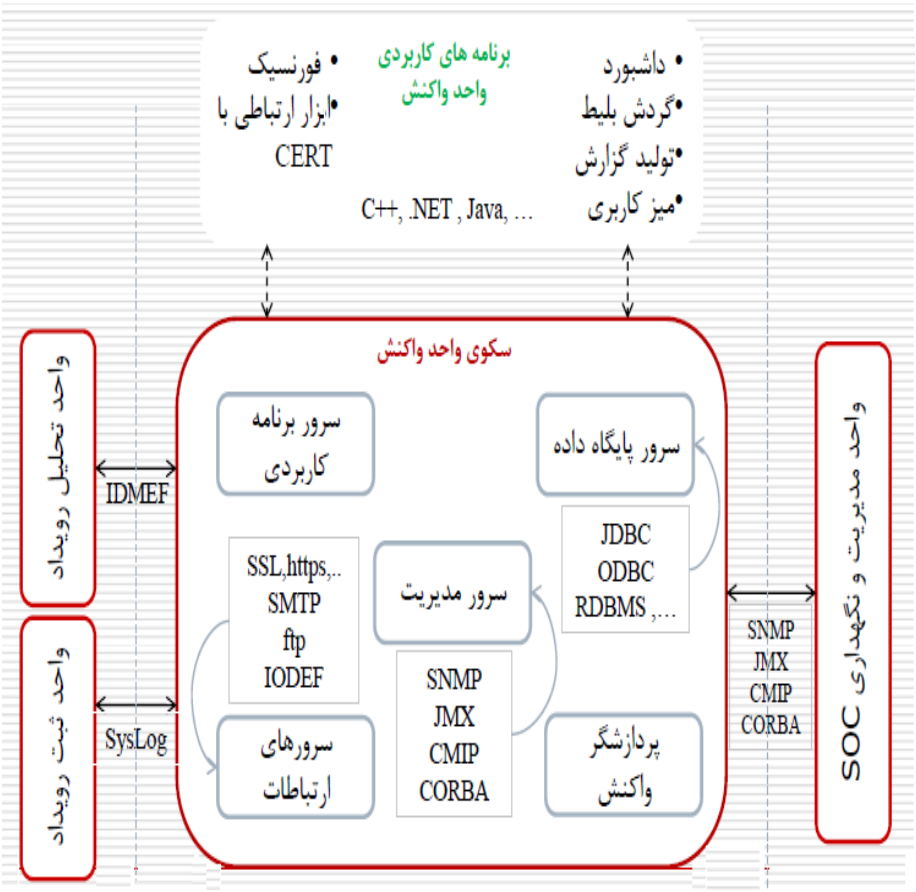
شکل ۱۰ ــ پس از اقدام (معماری عملیاتی)

۴. دید جامع از مرکز عملیات امنیت



شکل ۱۱ ــ دید جامع از مرکز عملیات امنیت

۵. معماری فناورانه



شکل ۱۲ ــ معماری فناورانه (غزنوی، ۱۳۹۱)

منابع و مآخذ

منابع فارسی

ـ افروز (۱۳۹۰)، مدیریت امنیت فناوری اطلاعات و ارتباطات، انتشارات مؤسسه آموزشی و تحقیقاتی صنایع دفاع.

ـ ایزدی، فؤاد (۱۳۹۰)، «راهکارها و راهبردهای ایالات‌متحده برای امنیت سایبر»، گزارش راهبردی، انتشارات فارس.

ـ بولتن ویژه سمینار امنیت جهانی ۲۰۱۲ (۱۳۹۱)، انتشار معاونت سیاسی صداوسیمای جمهوری اسلامی ایران.

ـ پایگاه اطلاع‌رسانی شورای انقلاب فرهنگی (۱۳۸۶)، نقشه جامع علمی کشور، www.iranculture.org.

ـ دنینگ، دی. ای (۱۳۸۶)، جنگ اطلاعات و امنیت، انتشارات پژوهشکده پردازش هوشمند

ـ سازمان پدافند غیرعامل (۱۳۹۰)، پدافند غیرعامل در حوزه جنگ سایبر.

ـ شیخ‌زادگان، جواد و سید جلیل جلیلی (۱۳۸۸)، «مقابله با تروریسم فضای تبادل اطلاعات (سیستم‌های ارتباطی) تهدیدات و مقابله با تهدیدات»، مقاله برگرفته از پایان‌نامه کارشناسی ارشد.

ـ غزنوی، احمدرضا (۱۳۹۱)، کارگاه واکنش به حوادث رایانه‌ای، مؤسسه تحقیقات ارتباطات و فناوری اطلاعات.

ـ گروه پدافند غیرعامل وزارت دفاع (۱۳۸۷)، تهدیدات شبکه‌ای.

ـ گروه مطالعات سیاسی مرکز پژوهش‌های مجلس شورای اسلامی (۱۳۹۱)، «استراتژی وزارت دفاع آمریکا در فضای مجازی»، ترجمه گزارش.

ـ مرکز پدافند غیرعامل فاوا (۱۳۸۸)، پروژه معماری و طراحی مرکز عملیات امنیت بومی مبتنی بر راهکارهای متن‌باز.

ـ وزارت دفاع و پشتیبانی نیروهای مسلح مرکز آینده‌پژوهی علوم و فناوری دفاعی (۱۳۸۴)، جنگ و دفاع سایبر، پروژه الزامات جنگ‌های نوین در فضای مجازی (سایبر).

ـ فصلنامه مبانی حقوق امنیت و تجارت الکترونیک (۱۳۸۹)، نشریه مرکز تحقیقات استراتژیک.

منابع لاتین

- Carcano A. Coletta M. Masera I. (2011), "A Multidimensional Critical State Analysis for Detecting Intrusions in اسکادا Systems", IEEE TRANSACTION on Industrial Informatics, Vol. 7, No. 2, May.
- Centre for Strategic & International Studies Report, April 19, 2011.
- Centre for Strategic & International Studies Report, USA, April 19, 2011.
- Cheung, S. Valdes, A. (2009), Communication Pattern Anomaly Detection in Process Control Systems, IEEE International Conference on Technologies for Homeland Security,

Waltham, MA. May 11-12.
- Critical Infrastructure in the Age of Cyber War, CSIS, McAfee, 2011.
- Cyber Security Concerns of Supervisory Control and Data Acquisition Systems, Dennis Dumont, Enterprise Preparedness Project Manager Raytheon Enterprise Preparedness Program Billerica, MA, USA, IEEE HST 2010 Conference.
- Fovino I. Carcano A. Murel D. Trombetta A. (2010), DNP3 State-based Intrusion Detection System, 24th IEEE International Conference on Advanced Information and Applications.
- Gao, W. Morris, T. Reaves, B. Richey, D. (2010), On SCADA Control System Command and Response Injection and Intrusion Detection, in the Proceedings of 2010 IEEE eCrime Researchers Summit, Dallas, TX. Oct 18-20.
- Hong, Sugwon, Tran Nhat Phuong, and Myongho Lee Dept(2012), Development of Smart Devices for - Secure Communication in the SCADA System, of Computer Science and Engineering, Myongji University, Korea.
- ICS-CERT Incident Response Summary Report, USA, 2009−2011.
- Mahboob A. Zubairi J. (2010), Intrusion Avoidance for اسکادا Security in Industrial Plants, IEEE.
- Mathew S. Britt D. Sudit M. Stotz A. Upadhyaya S. (2011), Real-Time Multistage Attack Awareness Through Enhanced Intrusion Alert Clustering, Springer.
- Morris T. Vaughn R. Dandass Y. (2012), A Retrofit Intrusion Detection System for MODBUS RTU and ASCII Industrial Control Systems, 45th Hawaii International Conference on System Sciences.
- Rrushi, J. Kang, K. (2009), Detecting Anomalies in Process Control Networks, IFIP International Federation for Information Processing.
- Shosha F. Gladyshev P. Chen-Ching L. (2009), Detecting Cyber Intrusions in اسکادا Networks Using Multi-Agent Collaboration, IEEE.
- Symantec - w32_stuxnet_dossier, 2011.
- The Economist Mag, Vol. 4, 2010.
- The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028, TRADOC Pamphlet 525-7-8, 22 February 2010.
- Valdes, A. Cheung, S. Intrusion Monitoring in Process Control Systems, (2009), Proceedings of the 42nd Hawaii International Conference on System Sciences.
- Vale, Z. Morais, H. Faria, P. Khodr, H. Ferreira, J. Peter Kadar (GECAD) (2011), Distributed Energy Resources Management with Cyber-Physical SCADA in the Context of Future Smart Grids,