پیوست

شورای اجرایی (عالی) فناوری اطلاعات کشور

کمیسیون توسعه دولت الکترونیکی

چارچوب معماری سازمانی ایران

معماری مرجع امنیت

استانداردهای امنیتی حوزه زیرساخت‌های حیاتی و سیستم‌های کنترل

نسخه ۱,۰ – اردیبهشت ماه ۱۳۹۶

پیشگفتار

زیرساخت‌های حیاتی[1] به صورت کلی به آن دسته از سامانه‌ها، خدمات و یا عملیاتی اطلاق می‌شود که اختلال و یا تخریب آن‌ها موجب تضعیف و یا ناتوانی در خدمات بهداشت عمومی، تجارت و اقتصاد، امنیت ملی و یا هر ترکیب دیگری از این قبیل موارد شود. این موارد شامل ارتباطات، انرژی، سامانه‌های بانکی، خطوط حمل و نقل، بهداشت عمومی و خدمات ضروری دولتی می‌شود.

سیستم‌های کنترل صنعتی (ICS)[2] در قلب زیرساخت‌های حیاتی قرار دارند، بنابراین امنیت برای چنین سیستم‌هایی مهم است. این سیستم‌ها تا چند سال پیش به صورت فیزیکی از سیستم‌ها و شبکه‌های خارجی ایزوله بوده‌اند ولی امروزه تمامی آن‌ها در جهت بالا بردن بهره‌وری می‌توانند به شبکه‌ی اینترنت متصل شوند که این اتصال می‌تواند یک خطر امنیتی بزرگ برای آن‌ها ایجاد کند. مدنظر قرار ندادن بحث امنیت فناوری اطلاعات در این سیستم‌ها به دلیل وجود محیط اختصاصی در نسل‌های اول و دوم، باعث ایجاد ضعف‌های امنیتی زیادی در نسل جدید شده است. عدم اعتبارسنجی مناسب ورودی‌ها، ضعف در کنترل سطح دسترسی، عدم استفاده از رمزنگاری، ضعف در تعریف دیواره آتش، اشکالات نرم‌افزاری، ضعف در پیکربندی و طراحی شبکه، سیستم احرازهویت ضعیف و ضعف‌های امنیتی متعدد تجهیزات کنترلی و غیره از جمله آسیب‌پذیری‌های شایع این سیستم‌ها می‌باشند.

آسیب‌پذیری‌های موجود در سیستم‌های صنعتی این امکان را برای مهاجمین فراهم ساخته تا به فکر حمله به زیرساخت‌های حیاتی کشور، آسیب رساندن به آن‌ها و یا ایجاد اختلال در فرآیند کاری آن‌ها باشند.

---

[1] Critical Infrastructure

[2] Industrial Control System (ICS)

محیط ICS دارای ویژگی‌ها و پیچیدگی‌های بسیار متفاوتی با سیستم‌های IT[3] است؛ از جمله تهدیدات و اولیت‌بندی‌های متفاوت. برخی از این خطرات شامل خطرات قابل‌توجهی بر روی ایمنی زندگی انسان، همچنین آسیب‌های جدی به محیط‌زیست و مسائل مالی مانند کاهش تولید و تاثیر منفی بر اقتصاد یک کشور می‌باشد. ICS نیازمندی‌های عملیاتی، قابلیت‌های اطمینان، سیستم‌عامل‌ها و برنامه‌های کاربردی متفاوتی نیز دارد که ممکن است برای کارکنان پشتیبانی IT غیرمتعارف به نظر برسد. از این رو برای تامین امنیت در این سیستم‌ها اسناد اختصاصی توسعه پیدا کرده است که می‌توان از آن‌ها بهره برد. در اینجا به مهمترین و برترین این اسناد اشاره خواهد شد.

لازم به ذکر است که برخی از اسناد مربوط به تامین امنیت زیرساخت‌های حیاتی به صورت اختصاصی برای یک بخش خاص ارائه شده‌اند و مابقی به صورت عمومی برای تمام زیرساخت‌ها کارایی دارند.

تقسیم‌بندی زیرساخت‌های حیاتی

در کشورهای مختلف دنیا تعاریف و تقسیم‌بندی‌های متفاوتی برای زیرساخت‌های حیاتی وجود دارد که تنها در برخی جزئیات با یکدیگر اختلاف دارند، ولی کلیات امر در همه یکسان است. ایالات متحده آمریکا از پیشروترین کشورهای فعال در زمینه امنیت زیرساخت‌های حیاتی می‌باشد که بنا بر تعاریف خود، زیرساخت‌های حیاتی را به ۱۶ بخش تقسیم می‌کند. این ۱۶ قسمت عبارتند از: بخش شیمی، بخش تاسیسات تجاری، بخش ارتباطات، بخش تولیدات حساس و حیاتی، بخش سدها، بخش پایه صنعت دفاع، بخش خدمات اورژانسی، بخش انرژی، بخش خدمات مالی، بخش کشاورزی و مواد غذایی، بخش سلامت عمومی و مراقبت‌های بهداشتی، بخش تکنولوژی اطلاعات، بخش ضایعات، مواد و راکتورهای هسته‌ای، بخش سیستم‌های حمل و نقل، بخش سیستم‌های آب و فاضلاب.

---

[3] Information System

لیست استانداردهای امنیتی حوزه حوزه زیرساخت‌های حیاتی و سیستم‌های کنترل

نام استاندارد	شماره استاندارد
Guide to Industrial Control Systems (ICS) Security, Rev 2 (2015) راهنمایی برای امنیت سیستم‌های کنترل صنعتی	SP 800-82
Recommended Security and Privacy Controls for Federal Information Systems and Organizations, Rev 4 (2013) کنترل‌های امنیتی و حریم خصوصی برای سازمان‌ها و سیستم‌های اطلاعاتی فدرال	SP 800-53
Cybersecurity Framework Manufacturing Profile (Draft), (2016) مشخصات تولیدی چارچوب امنیت سایبری	
An Industrial Control System Cybersecurity Performance Testbed (2015) بستر آزمایشی عملکرد امنیت سایبری یک سیستم کنترل صنعتی	IR 8089
Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (draft) (2017) چارچوبی برای بهبود امنیت سایبری زیرساخت‌های حیاتی	
Guidelines for Smart Grid Cyber Security (2014) راهنمایی برای امنیت سایبری شبکه هوشمند برق	IR 7628
NIST Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications, Rev. 1 طرح اولویت اقدامات پنل تعاملی شبکه‌های هوشمند: دستورالعمل‌هایی برای ارزیابی استانداردهای بی سیم برای کاربردی‌های شبکه هوشمند	IR 7761
Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts استفاده از نرم‌افزار آنتی‌ویروس مبتنی بر میزبان بر روی سیستم‌های کنترل صنعتی: دستورالعمل‌ها و روش آزمونی برای ارزیابی اثرات عملکرد	SP 1058
NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0 (2014) چارچوب و نقشه راه NIST برای استانداردهای قابلیت همکاری شبکه‌های هوشمند	SP 1108R3
Security for Industrial Automation and Control Systems امنیت برای سیستم‌های کنترل و اتوماسیون صنعتی	ISA / IEC-62443ANSI / ISA-99

شماره استاندارد	نام استاندارد
ANSI/ISA-95	Enterprise-Control System Integration یکپارچه‌سازی سیستم کنترل و شرکت
ISA100.11A	Wireless Systems for Automation: Process control and related applications سیستم‌های بی‌سیم برای خودکارسازی: کنترل فرآیند و برنامه‌های کاربردی مربوطه
	NERC CIP (critical infrastructure protection) حفاظت از زیرساخت‌های حیاتی
IEC Technical Committee 57	Power systems management and associated information exchange مدیریت سیستم‌های برق و تبادل اطلاعات مربوطه
API 1164	Pipeline SCADA Security, Second Edition (2009) امنیت اسکادای خط لوله
IEEE Std 1686	IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities (2013) استاندارد IEEE برای قابلیت‌های امنیت سایبری دستگاه‌های الکترونیکی هوشمند در ایستگاه فرعی
IEEE P1711	Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links (2010) استانداردی برای یک پروتکل رمزنگاری برای امنیت سایبری پیوندهای سریال ایستگاه‌های فرعی
IEEE P1711.3	Standard for Secure SCADA Communications Protocol (SSCP) (2013) استانداردی برای پروتکل ارتباطات امن اسکادا
IEEE Std 1815	IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3) استاندارد IEEE برای پروتکل شبکه توزیع‌شده ارتباطات سیستم‌های برق
	Catalog of Control Systems Security: Recommendations for Standards Developers (2011) کاتالوگ امنیت سیستم‌های کنترل: توصیه‌هایی برای توسعه‌دهندگان استانداردها
	Control Systems Cyber Security: Defense in Depth Strategies (2016) امنیت سایبری سیستم‌های کنترل: استراتژی‌های دفاع در عمق

شماره استاندارد	نام استاندارد
	Cyber Security Assessments of Industrial Control Systems (2010)
	ارزیابی امنیت سایبری سیستم‌های کنترل صنعتی
	21 Steps to Improve Cyber Security of SCADA Networks
	۲۱ گام برای بهبود امنیت سایبری شبکه‌های اسکادا
	Recommended Practice: Creating Cyber Forensics Plans for Control Systems (2008)
	رویه‌های توصیه شده: ارایه طرح‌های جرم‌یابی سایبری برای سیستم‌های کنترل
	Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability (2009)
	رویه توصیه شده: توسعه یک قابلیت پاسخ به رویداد امنیت سایبری برای سیستم‌های کنترل صنعتی
	Recommended Practice Case Study: Cross-Site Scripting (2007)
	رویه‌های توصیه شده- مطالعه موردی: حمله Cross-Site Scripting
	Recommended Practice for Patch Management of Control Systems (2008)
	رویه‌های توصیه شده برای مدیریت وصله سیستم‌های کنترلی
	Recommended Practice for Securing Control System Modems (2008)
	رویه‌های توصیه شده برای تامین امنیت مودم‌های سیستم کنترلی
	Recommended Practice: Configuring and Managing Remote Access for Industrial Control Systems (2010)
	رویه‌های توصیه شده: پیکربندی و مدیریت دسترسی راه دور برای سیستم‌های کنترل صنعتی
	Firewall deployment for scada and process control networks (2005)
	استقرار دیواره‌آتش برای اسکادا و شبکه‌های کنترل فرآیند
	(2014)NESCOR[۴] Guide to Penetration Testing for Electric Utilities
	راهنمای NESCOR برای آزمون نفوذپذیری تجهیزات الکتریکی
	Object Linking and Embededding (OLE) for Process Control (OPC) standards

[۴] National Electric Sector Cybersecurity Organization Resource

شماره استاندارد	نام استاندارد
	OLE برای استانداردهای کنترل فرآیند
AGA Standard 12	Cryptographic Protection of SCADA Communications
	محافظت به وسیله رمزنگاری از ارتباطات اسکادا
RFC 6272	Internet Protocols for the Smart Grid
	پروتکل‌های اینترنت برای شبکه هوشمند برق
MTR070050	MITRE TECHNICAL REPORT: Addressing Industrial Control Systems in NIST Special Publication 800-53
	پرداختن به سیستم‌های کنترل صنعتی در NIST SP 800-53

در ادامه هر کدام از استانداردها به طور مختصر شرح داده می‌شود:

- **NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security**

این استاندارد مقدمه‌ای از سیستم‌های کنترل صنعتی را ارایه می‌دهد و تفاوت‌های محیط‌های سیستم‌های کنترل صنعتی و فناوری اطلاعات را برمی‌شمارد. اشاره‌ای به مدیریت و ارزیابی ریسک در سیستم‌های صنعتی می‌کند و توصیه‌هایی برای معماری امن ICS ارایه می‌دهد و در نهایت یک سری کنترل‌های امنیتی برای بررسی و تامین امنیت این سیستم‌ها نام می‌برد. این کنترل‌ها در سه خانواده: فنی (شامل کنترل‌های از قبیل کنترل دسترسی، ممیزی و حسابرسی، شناسایی و احرازهویت، حفاظت سیستم و ارتباطات)، مدیریتی (شامل کنترل‌های ارزیابی امنیتی و اعطای امتیاز، برنامه‌ریزی، ارزیابی ریسک، استفاده از خدمات و سیستم، مدیریت برنامه) و عملیاتی (شامل کنترل‌های آموزش و آگاهی، مدیریت پیکربندی، برنامه‌ریزی پیش‌آمد احتمالی، پاسخ رویداد، نگهداری و تعمیر، حفاظت رسانه، حفاظت فیزیکی و محیطی، امنیت اشخاص، یکپارچگی سیستم و اطلاعات) قرار می‌گیرند.

- **NIST SP 800-53: Recommended Security and Privacy Controls for Federal Information Systems and Organizations**

این سند یک کاتالوگ از کنترل‌های امنیتی و حفظ حریم خصوصی برای سیستم‌های اطلاعات فدرال و سازمان‌ها فراهم می‌کند. همچنین فرایندی برای انتخاب کنترل‌های مناسب برای محافظت از عملیات سازمانی (رسالت، توابع، نمود و شهرت)، دارایی‌های سازمانی، افراد، سازمان‌های دیگر و ملت از مجموعه‌ای متنوع از تهدیدات از جمله حملات خصمانه سایبری، بلایای طبیعی، شکست‌های ساختاری و خطاهای انسانی ارایه می‌دهد. لازم به ذکر است که نسخه پنج این سند در دست تهیه است.

- **Cybersecurity Framework Manufacturing Profile**

این سند جزئیات پیاده‌سازی چارچوب امنیت سایبری توسعه یافته برای محیط تولیدی را فراهم می‌کند. چارچوب امنیت سایبری می‌تواند به عنوان یک نقشه راه برای کاهش خطرات امنیت سایبری برای تولیدکنندگان استفاده شود که با اهداف بخش تولید و بهترین شیوه‌های صنعت هم تراز می‌باشد. مشخصات ارایه شده در این سند موارد زیر را برای تولیدکنندگان فراهم می‌کنند:

مجموعه‌ی این چارچوب به تولیدکنندگان موارد زیر را ارایه می‌دهد:

۱- روشی برای شناسایی فرصت‌ها جهت بهبود وضعیت امنیت سایبری کنونی سیستم‌های تولیدی. ۲- ارزیابی از توانایی‌های خود در سطح قابل قبولی از ریسک. ۳- یک روش استاندارد برای آماده‌سازی طرح امنیت سایبری برای اطمینان مداوم از امنیت سیستم تولید.

پروفایل فعالیت‌های خاص امنیت سایبری و نتایج را برای حفاظت از سیستم‌های تولیدی، اجزای آن‌ها، تجهیزات و محیطشان تعریف می‌کند. از طریق استفاده از پروفایل تولیدکننده می‌تواند فعالیت‌های امنیت سایبری را با توجه به نیازهای کسب‌وکار، تحمل خطر و منابع خود تنظیم کند. پروفایل یک رویکرد اختصاصی به هر بخش تولیدی را برای امنیت سایبری از استانداردها، راهنماها و بهترین شیوه‌های صنعتی فراهم می‌کند.

- **Framework for Improving Critical Infrastructure Cybersecurity**

این چارچوب یک رویکرد مبتنی بر ریسک برای مدیریت ریسک امنیت سایبری ارایه می‌کند. چارچوب بر روی استفاده از اطلاعات خروجی کسب‌وکار برای هدایت فعالیت‌های امنیت سایبری و رسیدگی به ریسک‌های امنیت سایبری به عنوان بخشی از فرآیند مدیریت ریسک سازمان تمرکز کرده است. این چارچوب از سه بخش تشکیل شده است: هسته چارچوب، پروفایل چارچوب و رده‌های پیاده‌سازی چارچوب. هسته چارچوب مجموعه‌ای از فعالیت‌ها و مراجع حاوی اطلاعات مفید و نیز پیامدهای امنیت سایبری را که در تمام بخش‌های زیرساخت‌های حیاتی مشترکند ارایه می‌کند و راهنمایی‌های دقیقی جهت توسعه پروفایل سازمانی فردی فراهم می‌کند. در طول استفاده از پروفایل، چارچوب به سازمان کمک می‌کند تا فعالیت‌های امنیت سایبری خود را با نیازمندی‌های کسب‌وکار، تحمل ریسک و منابعش تنظیم و هم‌تراز کند. بخش رده‌ها، مکانیسمی را برای سازمان‌ها جهت درک ویژگی‌های رویکرد خود برای مدیریت ریسک امنیت سایبری فراهم می‌کنند.

توجه! این چارچوب یک رویکرد ثابت برای مدیریت ریسک امنیت سایبری برای تمام زیرساخت‌های حیاتی نیست. سازمان‌ها خطرات منحصر به فرد، تهدیدات مختلف، آسیب‌پذیری‌های مختلف، تحمل ریسک‌های مختلف، خواهند داشت و چگونگی به کارگیری روش‌ها در چارچوب توسط آن‌ها متفاوت خواهد بود.

توضیحات تکمیلی

وزارت امنیت داخلی آمریکا با توجه به این چارچوب و اطلاعاتی که از سهامداران هر یک از بخش‌های زیرساخت‌های حیاتی این کشور جمع‌آوری نموده است، اسنادی به عنوان راهنمای پیاده‌سازی چارچوب امنیت سایبری هر یک از این بخش‌های حیاتی ارائه داده است که در ادامه بیان می‌شوند. در هر یک از راهنماهای پیاده‌سازی، سند مربوطه منابع و ابزاری برای امنیت سایبری و ارزیابی ریسک بخش حیاتی مورد نظر فراهم می‌کند. سپس پیاده‌سازی چارچوب را در هفت گام: اولویت‌بندی و محدوده، جهت‌یابی، ایجاد یک پروفایل جاری، انجام یک ارزیابی ریسک، ایجاد یک پروفایل هدف، تعیین، تجزیه و تحلیل، و اولویت‌بندی شکاف‌ها، اجرا و استقرار برنامه اجرایی تشریح می‌نماید.

- Commercial Facilities Sector Cybersecurity Framework Implementation Guidance (2015)
- Critical Manufacturing Cybersecurity Framework Implementation Guidance (2015)
- Dams Sector Cybersecurity Framework Implementation Guidance (2015)
- Chemical Sector Cybersecurity Framework Implementation Guidance (2015)
- Emergency Services Sector Cybersecurity Framework Implementation Guidance (2015)
- Nuclear Sector Cybersecurity Framework Implementation Guidance for U.S. Nuclear Power

Reactors (2015)

همچنین سازمان‌های دیگری نیز این چارچوب را متناسب برای بخش خود انتشار داده‌اند:

- Energy Sector Cybersecurity Framework Implementation Guidance (2015, U.S. Department of energy office of electricity delivery and energy reliability)
- Process Control System Security Guidance for the Water Sector (2014, American Water Works Association (AWWA))

➢ **NISTIR 7628 Revision 1 Guidelines for Smart Grid Cybersecurity**

این گزارش سه جلدی، راهنمایی برای امنیت سایبری شبکه هوشمند برق می‌باشد. در واقع یک چارچوب تحلیلی است که سازمان می‌تواند برای توسعه استراتژی‌های امنیت سایبری موثر متناسب با ویژگی‌ها، خطرات و آسیب‌پذیری‌های مربوط به شبکه هوشمند برق خاص آن سازمان استفاده نماید. سهامداران شبکه هوشمند- از ارایه‌دهندگان خدمات مدیریت انرژی تا تولیدکنندگان وسایل نقلیه الکتریکی و ایستگاه‌های شارژ- می‌توانند از روش‌ها و اطلاعات پشتیبان این گزارش به عنوان راهنمایی برای ارزیابی ریسک و شناسایی و به کارگیری نیازمندی‌های امنیتی مناسب استفاده کنند.

این سند یک سند همراه با چارچوب NIST و "نقشه راه برای استانداردهای قابلیت همکاری با شبکه هوشمند[۵]"، ویرایش ۲,۰ (انتشارات ویژه 1108)، که NIST در فوریه ۲۰۱۲ منتشر کرده است، می‌باشد. در این سند فرض بر این است که خوانندگان یک دانش کاربردی از شبکه برق و درک کاربردی از امنیت سایبری دارند. در ادامه سه جلد منتشر شده به اختصار معرفی می‌شود:

جلد ۱- استراتژی، معماری، و الزامات سطح بالای امنیت سایبری شبکه هوشمند[۶]:

- فصل ۱: استراتژی توسعه: شرح استراتژی امنیت سایبری برای شبکه‌های هوشمند و وظایف خاص در این استراتژی

- فصل ۲: معماری منطقی و واسط‌های شبکه هوشمند: شامل یک نمودار از یک دید سطح بالا از بازیگران در هر یک از حوزه‌های شبکه هوشمند و نیز یک مدل کلی مرجع منطقی از شبکه هوشمند

[5] NIST Framework and Roadmap for Smart Grid Interoperability Standards

[۶] Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements

- فصل ۳: الزامات امنیتی: الزامات سطح بالای امنیتی برای هر یک از ۲۲ واسط منطقی در فصل ۲

- فصل ۴: رمزنگاری و مدیریت کلید: مسایل فنی رمزنگاری و مدیریت کلید در سراسر دامنه سیستم‌ها و دستگاه‌های موجود در شبکه هوشمند

جلد ۲ - حفظ حریم خصوصی و شبکه هوشمند[۷]

- فصل ۵: حفظ حریم خصوصی و شبکه هوشمند: شامل یک ارزیابی اثرات حفظ حریم خصوصی برای شبکه‌های هوشمند

جلد ۳ - تجزیه و تحلیل‌ها و منابع حمایتی[۸]

- فصل ۶: کلاس‌های آسیب پذیری: شامل کلاس آسیب پذیری‌های بالقوه برای شبکه‌های هوشمند

- فصل ۷- تجزیه و تحلیل امنیتی پایین به بالای شبکه هوشمند: شناسایی تعدادی از مشکلات امنیتی خاص در شبکه‌های هوشمند

- فصل ۸– زمینه[۹]های تحقیق و توسعه برای امنیت سایبری در شبکه هوشمند

- فصل ۹- بررسی اجمالی استانداردها: شامل یک نمای کلی از فرایند ارزیابی استانداردها در برابر الزامات امنیتی سطح بالا

- فصل ۱۰- موارد کاربرد کلیدی سیستم‌های قدرت با توجه به الزامات امنیتی

- **NISTIR 8089: An Industrial Control System Cybersecurity Performance Testbed**

موسسه ملی استاندارد و فناوری، در حال توسعه یک بستر آزمایشی عملکرد امنیت سایبری برای سیستم‌های کنترل صنعتی است. هدف از این بستر آزمایشی، اندازه‌گیری عملکرد سیستم‌های کنترل

---

[۷] Volume 2- Privacy and the Smart Grid

[8] Volume 3- Supportive Analyses and References

[9] Theme

صنعتی است که با حفاظت‌های امنیت سایبری بر اساس بهترین شیوه‌ها و الزامات تجویزشده توسط استانداردها و دستورالعمل‌های ملی و بین‌المللی حمایت می‌شوند. نمونه‌هایی از این استانداردها و دستورالعمل‌ها ISA/IEC-62443 و NIST SP 800-82 می‌باشند.

- **NISTIR 7761 Rev. 1 NIST Smart Grid Interoperability Panel Priority Action Plan 2: Guidelines for Assessing Wireless Standards for Smart Grid Applications**

این گزارش حاوی ابزارهای کلیدی و روش‌هایی برای کمک به طراحان سیستم شبکه هوشمند در زمینه تصمیم‌گیری آگاهانه در مورد فناوری‌های بی‌سیم موجود و در حال ظهور است و همچنین یک مجموعه اولیه از الزامات برای ارتباطات زیرساخت‌های پیشرفته اندازه‌گیری[10] و اتوماسیون توزیع اولیه[11] آورده شده است. در این گزارش یک مجموعه اولیه از دستورالعمل‌ها جهت کمک به طراحان و توسعه-دهندگان شبکه هوشمند برق برای ارزیابی خود از فن‌آوری‌های بی‌سیم نیز فراهم شده است.

- **NIST SP 1058: Using Host-Based Antivirus Software on Industrial Control Systems: Integration Guidance and a Test Methodology for Assessing Performance Impacts**

این سند تلفیقی از تمامی مطالعات در زمینه ضدویروس‌ها بر پایه سیستم‌های کنترل صنعتی می‌باشد و به عنوان نقطه شروع و یا به عنوان یک منبع ثانویه در هنگام نصب، پیکربندی، اجرا و نگهداری نرم افزار ضدویروس بر روی یک سیستم کنترل صنعتی عمل می‌کند. این سند به طور انحصاری برای نرم-افزار ضدویروس مبتنی بر میزبان، مورد استفاده در سیستم‌های کنترل صنعتی متمرکز است.

- **NIST SP 1108R3: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0**

---

[10] Advanced metering infrastructure (AMI)

[11] Distribution *automation* (*DA*)

نسخه سوم چارچوب و نقشه راه NIST برای استاندارد قابلیت همکاری شبکه‌های هوشمند برق، براساس کار بر روی نسخه اول (ژانویه ۲۰۱۰) و دوم (فوریه ۲۰۱۲) ایجاد شده است. نسخه اول و دوم سند چارچوب NIST شامل اطلاعات به دست آمده از طریق فرایندی است که از هر دو طیف جامعه سهامداران شبکه هوشمند و عموم مردم درگیر فراهم شده است. نسخه سه نشان‌دهنده پیشرفت در فناوری شبکه هوشمند برق و تحولات کار مشارکتی NIST با سهامداران صنعت است. همچنین بازنگری بر روی دستورالعمل‌های خود برای امنیت سایبری شبکه هوشمند برق را نیز در دسترس قرار می‌دهد.

- **ISA / IEC-62443: Security for Industrial Automation and Control Systems**

ISA/ IEC-62443 یک سری از استانداردها، گزارش‌های فنی و اطلاعاتی است که روشی برای پیاده‌سازی الکترونیکی امن سیستم‌های کنترل و اتوماسیون صنعتی[۱۲] (IACS) تعریف می‌کند. این راهنما برای کاربران پایانی (به عنوان مثال صاحب دارایی)، ایجادکننده سیستم، دست اندرکاران امنیتی و تولیدکنندگان سیستم‌های کنترلی و مسئولان تولید، طراحی، پیاده‌سازی و یا مدیریت سیستم‌های اتوماسیون و کنترل صنعتی کاربرد دارد.

این اسناد در اصل با عنوان استاندارد ANSI/ ISA-99 یا ISA99 که توسط جامعه بین المللی برای اتوماسیون[۱۳] (ISA) ایجاد شده بود، منتشر شده بودند. در سال ۲۰۱۰، آن‌ها به عنوان سری ANSI / ISA-62443 شماره‌گذاری مجدد شدند. این تغییر برای هماهنگ کردن شماره‌گذاری اسناد ISA و ANSI با استانداردهای مربوط به کمیسیون بین المللی الکتروتکنیک[۱۴] (IEC) در نظر گرفته شده بود.

همه استانداردها و گزارش‌های فنی ISA-62443 از چهار دسته کلی به نام عمومی، سیاست‌ها و رویه‌ها، سیستم و اجزا تشکیل شده‌اند. اسناد برنامه‌ریزی شده و منتشر شده ISA-62443 عبارتند از:

گروه ۱: عمومی:

---

12 Industrial Automation and *Control Systems* (*IACS*)

13 International Society for Automation

14 International Electrotechnical Commission

- (IEC / TS 62443-1-1) ISA-62443-1-1 : (که قبلا به عنوان "ISA-99 Part 1" نامیده می‌شد) در اصل به عنوان استاندارد ANSI / ISA-99.00.01-2007 و همچنین به عنوان مشخصات فنی IEC/TS 62443-1-1 منتشر شد. این استاندارد مقدمه‌ای است بر مفاهیم و مدل‌هایی که در طول سری از آن‌ها استفاده می‌شود.
- (IEC 62443-1-2) ISA-TR62443-1-2: گزارش فنی شامل یک واژه‌نامه ارشد از اصطلاحات مورد استفاده در طول این سری است.
- (IEC 62443-1-3) ISA-62443-1-3: استانداردی که معیارهای فنی استخراج شده از الزامات عملیاتی و الزامات سیستمی را توصیف می‌کند.
- (IEC / TS 62443-1-4) ISA-62443-1-4: گزارش فنی که چرخه زندگی امنیتی و مورد استفاده سیستم‌های کنترل و اتوماسیون صنعتی را تعریف می‌کند.

گروه ۲: سیاست‌ها و روش‌ها:

- (IEC 62443-2-1) ISA-62443-2-1: IACS (که قبلا به عنوان "ANSI/ ISA 99.02.01-2009 یا ISA-99 Part 2" نامیده می‌شد) استانداردی که به چگونگی برقراری یک برنامه موثر امنیتی برای سیستم‌های کنترل و اتوماسیون صنعتی پرداخته است.
- (IEC 62443-2-2) ISA-62443-2-2: استانداردی که به چگونگی کار برنامه‌های امنیتی سیستم‌های کنترل و اتوماسیون صنعتی پرداخته و راهنمایی برای بیان نیازمندی‌های اجرای یک برنامه امنیتی موثر برای سیستم‌های کنترل و اتوماسیون صنعتی می‌باشد.
- (IEC TR 62443-2-3) ISA-TR62443-2-3: یک گزارش فنی که راهنمایی را جهت مدیریت وصله در محیط سیستم‌های کنترل و اتوماسیون صنعتی ارایه می‌دهد.
- (IEC 62443-2-4) ISA-62443-2-4: استانداردی که الزامات کارپردازان سیستم‌های کنترل و اتوماسیون صنعتی را مشخص می‌کند.

گروه ۳: ایجادکننده سیستم

- ISA-TR62443-3-1 (IEC / TR 62443-3-1): یک گزارش فنی در مورد کاربرد فناوری‌های امنیتی متفاوت برای محیط سیستم‌های کنترل و اتوماسیون صنعتی است.
- ISA-62443-3-2 (IEC 62443-3-2): استانداردی که به ارزیابی ریسک امنیتی و طراحی سیستم برای سیستم‌های کنترل و اتوماسیون صنعتی پرداخته است.
- ISA-62443-3-3 (IEC 62443-3-3): استانداردی که به توصیف الزامات امنیتی سیستم‌های عملیاتی و سطوح اعتماد امنیتی پرداخته است.

گروه ۴: اجزا

- ISA-62443-4-1 (IEC 62443-4-1): این استاندارد الزامات مورد نیاز برای توسعه محصولات امن را توصیف می‌کند.
- ISA-62443-4-2 (IEC 62443-4-2): این استاندارد شامل یک مجموعه از الزامات است که جزئیات نگاشت نیازمندی‌های سیستمی به زیرسیستم‌ها و اجزا سیستم را تحت شرایط خاص فراهم می‌کند.

- **ANSI/ISA-95: Enterprise-Control System Integration**

این سند یک استاندارد بین‌المللی از جامعه بین‌المللی اتوماسیون[۱۵] برای توسعه‌ی یک رابط خودکار بین شرکت و سیستم‌های کنترل صنعتی است. این استاندارد برای کارخانه‌های جهانی توسعه یافت و تبادل اطلاعات قوی، امن و مقرون به صرفه‌ای را تعریف می‌نماید. این استاندارد برای تمام صنایع و در همه فرآیندها مانند فرآیندهای دسته‌ای و فرآیندهای مستمر و تکرارشونده به کار می‌رود. بخش‌های این استاندارد به شرح زیر است:

- **ISA100.11A Wireless Systems for Automation: Process control and related applications**

[15] *International* Society of *Automation (ISA)*

کمیته ISA100 استانداردها، روش‌های توصیه‌شده، گزارش‌های فنی و اطلاعات مربوطه جهت پیاده‌سازی سیستم‌های بی‌سیم در اتوماسیون و محیط‌های کنترلی را با تمرکز بر سطح فیلد ارایه می‌کند. راهنما به افراد مسئول در چرخه حیات سیستم‌های کنترل و اتوماسیون صنعتی از جمله طراحی، اجرا، تعمیر و نگهداری، مقیاس‌پذیری و یا مدیریت اشاره دارد، و باید کاربران، ایجادکنندگان سیستم، شاغلان، و تولیدکنندگان و فروشندگان سیستم‌های کنترلی آن را به کارگیرند. این استاندارد مشخصات لایه OSI، مشخصات امنیتی و مشخصات مدیریتی را برای دستگاه‌های بی‌سیم در خدمت برنامه‌های کاربردی دستگاه‌های ثابت، قابل حمل و در حال حرکت تعریف می‌کند.

- **NERC CIP (Critical Infrastructure Protection)**

طرح NERC CIP شامل ۹ استاندارد و ۴۵ نیازمندی است که امنیت محیطی الکترونیکی و حفاظت از دارایی‌های حیاتی سایبری و همچنین پرسنل و آموزش، مدیریت امنیت و برنامه‌ریزی بازیابی فاجعه را پوشش خواهد داد. این نه استاندارد به شرح زیر است:

CIP-002-1: شناسایی دارایی حیاتی سایبری

CIP-003-1: کنترل‌های مدیریت امنیت

CIP-004-1: پرسنل و آموزش

CIP-005-1: معیارهای امنیت الکترونیک

CIP-006-1: امنیت فیزیکی دارایی‌های سایبری حیاتی

CIP-007-1: مدیریت امنیت سیستم‌ها

CIP-008-1: برنامه‌ریزی گزارش و پاسخ حادثه

CIP-009-1: برنامه‌های بازیابی برای دارایی‌های سایبری حیاتی

طرح CIP شامل توسعه استانداردها، اعمال مقررات، ارزیابی ریسک و آمادگی، انتشار اطلاعات حیاتی و افزایش آگاهی در مورد مسائل امنیتی کلیدی می‌باشد.

- **IEC Technical Committee 57: Power systems management and associated information exchange**

IEC TC 57 بر مدیریت سیستم‌های برق و تبادل اطلاعات مرتبط با آن‌ها متمرکز شده است و به یک سری از گروه‌های کاری تقسیم می‌شود. هر گروه کاری از اعضای کمیته‌های استاندارد ملی کشورهای عضو IEC تشکیل شده است. هر گروه کاری مسئول توسعه استانداردها در حوزه خود می‌باشد. گروه کاری WG 15 در زمینه امنیت داده‌ها و ارتباطات در سیستم‌های کنترل صنعتی فعالیت می‌کنند و استاندارد توسعه یافته توسط این گروه IEC 62351 می‌باشد.

- **American Petroleum Institute (API) Standard 1164, "Pipeline SCADA Security", Second Edition**

API 1164 راهنمایی برای اپراتورهای سیستم‌های خط لوله نفت و گاز طبیعی برای مدیریت یکپارچگی و امنیت سیستم‌های اسکادا فراهم می‌کند. این راهنما به طور خاص برای ارائه به اپراتورها همراه با شرح شیوه‌های صنعتی در امنیت اسکادا طراحی شده است. این سند بر روی اهمیت درک اپراتورها از آسیب‌پذیری‌های سیستم و خطرات در زمان بررسی سیستم اسکادا جهت بهبود احتمالی سیستم، تاکید می‌کند. API 1164 بهبود امنیت عملیات اسکادای خط لوله را با استفاده از موارد زیر فراهم می‌کند:

- لیست کردن فرآیندهای مورد استفاده برای شناسایی و تجزیه و تحلیل حساسیت سیستم اسکادا به حوادث.
- ارائه یک لیست جامع از شیوه‌هایی جهت ایمن‌سازی معماری.
- ارائه نمونه‌هایی از شیوه‌های توصیه‌شده صنعتی.

ضمایم این سند شامل یک چک لیست برای ارزیابی یک سیستم اسکادا و نمونه‌ای از یک طرح امنیتی سیستم کنترل اسکادا می‌شود.

- **IEEE 1686- IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities**

توابع و ویژگی‌های دستگاه‌های الکترونیکی هوشمند برای لحاظ کردن برنامه‌های حفاظت از زیرساخت‌های حیاتی در این استاندارد تعریف شده است. امنیت در مورد دسترسی، بهره‌برداری، پیکربندی، نسخه میان‌افزار و بازیابی داده‌ها در یک IED در این استاندارد مورد بررسی قرار گرفته است. لازم به ذکر است که ارتباطات به منظور حفاظت از سیستم‌های قدرت (راه دور) در این سند مورد بررسی قرار نگرفته است. رمزگذاری برای انتقال امن داده‌ها در داخل و خارج از ایستگاه، از جمله کنترل نظارتی و اکتساب داده‌ها نیز بخشی از این استاندارد نمی‌باشد.

- **IEEE P1711 - Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links**

استانداردی برای یک پروتکل رمزنگاری برای امنیت سایبری پیوندهای سریال ایستگاه‌های فرعی است. این استاندارد یک پروتکل رمزنگاری برای ارائه یکپارچگی و محرمانگی اختیاری برای امنیت سایبری لینک‌های سریال تعریف می‌کند. این استاندارد به برنامه‌های کاربردی یا پیاده‌سازی‌های سخت‌افزاری خاصی رسیدگی نمی‌کند، و مستقل از پروتکل‌های ارتباطی اساسی است.

- **IEEE P1711.3 - Standard for Secure SCADA Communications Protocol (SSCP)**

این استانداردی برای پروتکل ارتباطات امن اسکادا (SSCP) تعریف می‌کند. یک پروتکل رمزنگاری برای ارائه یکپارچگی، و محرمانگی اختیاری، برای امنیت سایبری لینک ارتباطی سریال ایستگاه فرعی بدون حمایت از پیام همه‌پخشی و بدون هیچ گونه نیازمندی‌های زمانی تعریف می‌کند. این استاندارد به

برنامه‌های کاربردی یا پیاده‌سازی‌های سخت‌افزاری خاصی رسیدگی نمی‌کند، و مستقل از پروتکل‌های ارتباطی اساسی است.

- **IEEE 1815- IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3)**

استانداردی برای پروتکل شبکه توزیع شده[16] ارتباطات سیستم‌های برق می‌باشد. این استاندارد پروتکل DNP3 اسکادا را توصیف می‌کند.

- **Catalog of Control Systems Security: Recommendations for Standards Developers**

این کاتالوگ تلفیقی از شیوه‌هایی که صنعت‌های مختلف جهت افزایش امنیت سیستم‌های کنترلی در برابر هر دو حملات فیزیکی و شبکه‌ای توصیه کرده‌اند را ارایه می‌دهد. توصیه‌ها در این کاتالوگ به ۱۹ خانواده یا دسته گروه‌بندی می‌شوند، که درجه اهمیت مشابه‌ای دارند. توصیه در هر خانواده با یک توضیح خلاصه از توصیه، راهنمایی‌های مکمل یا تصریح‌کننده نمایش داده می‌شود، و در توضیح بیشتر الزامات، توضیحی برای الزامات تحت شرایط خاص فراهم می‌شود. این ۱۹ خانواده عبارتند از: ۱- سیاست امن. ۲- امنیت سازمانی. ۳- امنیت کارکنان. ۴- امنیت محیط و فیزیکی. ۵- اکتساب سرویس و سیستم. ۶- مدیریت پیکربندی. ۷- برنامه‌ریزی استراتژیک. ۸- حفاظت ارتباطات و سیستم. ۹- مدیریت اسناد و اطلاعات. ۱۰- نگه‌داری و توسعه سیستم. ۱۱- آموزش و آگاهی امنیت. ۱۲- پاسخ رویداد. ۱۳- حفاظت رسانه. ۱۴- جامعیت داده و سیستم. ۱۵- کنترل دسترسی. ۱۶- ممیزی و حسابرسی. ۱۷- نظارت و بازبینی سیاست‌های امنیتی سیستم کنترل. ۱۸- ارزیابی و مدیریت ریسک. ۱۹- مدیریت برنامه امنیتی.

این کاتالوگ برای استفاده در یک بخش خاص صنعت محدود نمی‌شود. همه بخش‌ها می‌توانند از آن برای توسعه یک چارچوب مورد نیاز برای تولید یک برنامه امنیت سایبری استفاده کنند. مجموعه‌ای از

---

[16] Distributed Network Protocol (DNP3)

استانداردها و دستورالعمل‌های امنیت سایبری منتشر شده که می‌تواند به عنوان ورودی تولید و توسعه یک برنامه امنیت سایبری در نظر گرفته شود در این کاتالوگ قرار گرفته است.

- **Control Systems Cyber Security: Defense in Depth Strategies**

این سند راهنمایی‌هایی را برای توسعه استراتژی‌های بهبوددهنده تهدیدات سایبری ویژه و همچنین توصیه‌هایی برای ایجاد یک برنامه امنیتی دفاع در عمق برای محیط سیستم‌های کنترلی فراهم می‌کند. این سند این اطلاعات را در چهار بخش ارایه می‌نماید:

۱- سابقه و بازبینی: تشریح وضعیت فعلی امنیت سایبری ICS و مروری بر معنا و مفهوم دفاع در عمق در بستر سیستم‌های کنترل صنعتی.

۲- استراتژی‌های دفاع در عمق ICS: فراهم کردن استراتژی‌ها و راهکارهایی برای امنیت محیط‌های سیستم کنترل صنعتی.

۳- حملات امنیتی: تشریح عملکرد عوامل تهدید زیرساخت‌های حیاتی و نتایج بالقوه آن بر روی شبکه و سیستم کنترل صنعتی.

۴- توصیه‌هایی برای تامین امنیت ICS: فراهم کردن منابعی برای تامین امنیت سیستم‌های کنترل صنعتی بر اساس روش‌ها و تکنولوژی‌های جدید، فعالیت‌های ICS-CERT، ابزار و خدمات در دسترس از طریق ICS-CERT و سایر موارد بهبوددهنده وضعیت امنیتی سیستم‌های کنترل صنعتی.

- **Cyber Security Assessments of Industrial Control Systems**

در سال ۲۰۱۰ اداره امنیت میهن و مرکز حفاظت از زیرساخت‌های ملی[17] سندی برای ارزیابی امنیت سایبری سیستم‌های کنترل صنعتی ارایه کردند. این سند شامل نمای کلی فرآیند ارزیابی است به

[17] Center for the protection of national infrastructure (CPNI)

طوری که کاربران قادرند نحوه ارزیابی امنیت سایبری ICS را درک کنند. اولین مرحله در این استاندارد آماده‌سازی و برنامه‌ریزی است که طی جلسه‌ای با صاحب دارایی انجام می‌شود. در این جلسه نقاط مورد بررسی، نقش‌ها و مسئولیت‌ها و اولویت‌های موردنظر صاحب دارایی مشخص می‌شود. سپس به جمع‌آوری اطلاعات و طراحی بردارهای حمله پرداخته می‌شود. در مرحله بعد، ارزیابی امنیتی و آزمون‌های طراحی شده اجرا می‌شود و در نهایت گزارشی از آسیب‌پذیری‌های کشف شده و در آخرین مرحله اقداماتی برای کاهش آسیب‌پذیری‌ها توصیه می‌شود. همچنین این سند سه نوع ارزیابی (ارزیابی آزمایشگاهی، ارزیابی محصول و آزمون نفوذپذیری انتها به انتها[۱۸]) را برای قسمت‌های مختلف سیستم کنترل صنعتی پیشنهاد می‌نماید.

- **21 Steps to Improve Cyber Security of SCADA Networks**

۲۱ گام شامل اقدامات لازم برای بهبود حفاظت شبکه‌های اسکادا را توصیه می‌کند. این گام‌ها به دو دسته تقسیم می‌شود: اقدامات خاص برای بهبود پیاده‌سازی و اقداماتی برای برقراری فرآیندها و سیاست‌های مدیریتی اساسی.

- **Recommended Practice: Creating Cyber Forensics Plans for Control Systems**

هدف ارایه راهنمایی‌هایی همراه با پیچیدگی‌های خاص جرم‌یابی سایبری سیستم‌های کنترل صنعتی است، راهنمایی‌هایی که به سازمان‌ها اجازه ساخت یک برنامه جرم‌یابی سایبری خودکفا برای محیط سیستم کنترل صنعتیشان را می‌دهد و راهنمایی‌هایی که تکامل و نگهداری این برنامه‌ها را پشتیبانی می‌کند.

این سند به سه بخش عمده سازماندهی می‌شود:

۱- جرم‌یابی سنتی و چالش‌های سیستم‌های کنترل صنعتی.

---

[۱۸] End-to-End

۲- ایجاد یک برنامه جرم‌یابی برای محیط سیستم‌های کنترل صنعتی.

۳- به کار انداختن و تقویت کردن یک برنامه جرم‌یابی سایبری.

این سند به مسائلی که هنگام توسعه و بکارگیری یک برنامه جرم‌یابی سایبری برای سیستم‌های کنترل صنعتی با آن‌ها مواجه می‌شویم پرداخته است. هدف از این توصیه‌ها دوباره‌نویسی روش‌های اثبات‌شده نیست، بلکه هدف استفاده از آن‌ها به بهترین شیوه ممکن است.

- **Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability**

این سند شامل توصیه‌هایی برای کمک به مراکز استفاده کننده از سیستم‌های کنترلی جهت آمادگی بیشتر برای پاسخگویی به حوادث سایبری بدون در نظر گرفتن منبع آن‌ها می‌باشد. این سند همچنین راه‌هایی برای یادگیری از حادثه و تقویت سیستم علیه حملات بالقوه را پیشنهاد می‌دهد. این سند شامل روش‌های پذیرفته شده و رویکردهایی از فناوری اطلاعات سنتی است، اما در درجه اول بر روی جنبه‌های منحصر به فرد سیستم‌های کنترل صنعتی تمرکز می‌کند.

- **Recommended Practice Case Study: Cross-Site Scripting**

این سند جزئیات حمله امنیت اطلاعات، حمله Cross-Site Scripting، که می‌تواند علیه سیستم‌های کنترل صنعتی اجرا شود را تشریح می‌کند و روش‌هایی را به منظور کاهش این تهدیدات ارایه می‌دهد. حمله تزریق کد نقطه ورودی برای حمله‌کننده‌ها جهت دسترسی و دستکاری شبکه کنترل صنعتی می‌باشد.

- **Recommended Practice for Patch Management of Control Systems**

مدیریت وصله نرم‌افزار سیستم‌های کنترل صنعتی که در زیرساخت‌های حیاتی و منابع کلیدی استفاده می‌شود در بهترین حالت ناسازگار و در بدترین حالت ناممکن است. وصله‌ها برای برطرف کردن آسیب‌پذیری‌ها و مسائل عملیاتی مهم‌اند. این گزارش شیوه‌های مدیریت وصله برای صاحبان دارایی‌های

سیستم‌های کنترل صنعتی را توصیه می‌کند. بر اساس این سند برنامه مدیریت وصله خوب شامل عناصر زیر می‌باشد: طرح مدیریت پیکربندی، طرح مدیریت وصله، تست وصله، طرح تهیه پشتیبان/ بایگانی، طرح پاسخگویی به رخدادها و طرح جبران فاجعه. هر یک از این طرح‌ها نیاز به ورودی و تصویب از طرف تمامی سازمان‌های تحت تاثیر و پشتیبانی از طرف مدیریت ارشد دارد.

- **Recommended Practice for Securing Control System Modems**

این سند راهنمایی‌هایی برای تجزیه و تحلیل متدولوژی‌های ارزیابی خطرات امنیتی درمورد مودم‌ها و استفاده از آن‌ها در یک سازمان را فراهم می‌کند. همچنین برای محافظت از عناصر سیستم‌هایی که از مودم برای اتصال استفاده می‌کنند، روش‌های مفیدی جهت ایجاد یک معماری دفاع در عمق ارایه می‌کند. فرض بر این است که خواننده این سند درک پایه‌ای از آسیب‌پذیری‌های مربوط به مودم و ارتباطات مودم دارد.

بخش دو و سه این سند روش‌هایی برای ارزیابی امنیت مودم و منابعی برای شناسایی ابزارهای ارزیابی و روش‌هایی برای شناسایی و تحلیل اتصالات مودم ارایه می‌دهد. بخش چهار، گزینه‌هایی برای پیاده‌سازی امنیت مودم با توجه به انواع اتصالات و/یا دستگاه‌هایی که استفاده می‌شوند فراهم می‌کند. همچنین روش‌هایی از قبیل احراز هویت، ورود به سیستم، فیلتر شناسه تماس‌گیرنده و امنیت دستگاه سیستم کنترلی را مورد بحث قرار می‌دهد.

- **Recommended Practice: Configuring and Managing Remote Access for Industrial Control Systems**

در گذشته امنیت سیستم‌های کنترل صنعتی با ایزوله کردن آن‌ها از شبکه‌های خارجی فراهم می‌شد. اما امروزه نیازمندی‌های کسب‌وکار منجر به اتصال این سیستم‌های ایزوله به شبکه‌های دیگر شده است. این اتصالات به صاحبان دارایی‌ها توانایی بیشینه کردن عملیات کسب‌وکار و کاهش دادن هزینه‌های مربوط به تجهیزات نظارتی و تعمیر و نگهداری را داده است در حالی که این اتصالات نیاز به یک الگوی امنیتی برای حفاظت از سیستم‌های کنترلی در برابر حوادث سایبری دارند. با این حال، راه‌حل‌های مورد

قبول در دسترسی از راه دور ممکن است بطور کامل بر روی این سیستم‌ها قابل نگاشت نباشد. الزامات مورد نیاز برای دسترس‌پذیری، جامعیت و صحت با تفاوت جزئی منحصر به فردی ترکیب شده است و این موضوع نیاز به ایجاد یک راهنما برای امنیت دسترسی از راه دور برای سیستم‌های کنترل صنعتی را ایجاب می‌کند.

این سند پشتیبانی برای راه‌های دسترسی از راه دور برای سیستم‌های کنترل صنعتی فراهم می‌کند. شیوه‌های متداول استانداردهای فناوری اطلاعات در بستر محیط‌های سیستم‌های کنترلی ارایه می‌گردد، همراه با آگاهی از این که راه‌های دسترسی از راه دور چگونه می‌توانند برای معماری سیستم کنترلی در جهت کاهش خطرهای سایبری به کار گرفته شوند. هدف این سند ایجاد راهنمایی در خصوص توسعه امن استراتژی‌های دسترسی از راه دور برای محیط سیستم‌های کنترلی است.

- **Firewall Deployment for Scada and Process Control Networks**

یکی از راه‌کارهای امنیتی برای سیستم‌های اسکادا و شبکه‌های کنترل، فرآیند ایزوله کردن آن‌ها از اینترنت و شبکه سازمانی از طریق دیواره‌های آتش می‌باشد. اما اطلاعات کمی درمورد چگونگی بکارگیری، پیکربندی، معماری و مدیریت آن‌ها در سیستم‌های کنترلی موجود است. یکی از اسنادی که درمورد دیواره‌های آتش، مدیریت و پیکربندی و به کارگیری آن‌ها در معماری شبکه کنترلی توضیح می‌دهد این سند می‌باشد. این سند، شرایط سیستم کنترلی و همچنین موارد امنیتی خاص آن‌ها را در نحوه پیاده‌سازی و مدیریت دیواره‌های آتش مدنظر قرار داده است.

- **NESCOR Guide to Penetration Testing for Electric Utilities**

این استاندارد توسط "منابع سازمان امنیت سایبری بخش برق ملی ایالات متحده آمریکا" در سال ۲۰۱۴ برای تاسیسات الکتریکی و در جهت ارزیابی امنیتی شبکه‌های هوشمند و سایر سیستم‌های مدیریت انرژی ارایه شده است. این سند فقط بر آزمون نفوذپذیری تمرکز دارد و شامل جزئیات و ابزارهای خاص و نیز روش گام به گام انجام آزمون نمی‌شود ولی توصیف سطح بالایی از آزمون در حال انجام و

هدف آن ارایه می‌کند. اولین گام، برنامه‌ریزی و حوزه‌بندی مناسب سیستم مورد ارزیابی می‌باشد. بعد از تکمیل این مرحله، فرآیند آزمون به چهار وظیفه اصلی تقسیم می‌شوند: "آزمون نفوذپذیری سیستم عامل سرویس‌دهنده" که به شناسایی آسیب‌پذیری‌های شناخته شده یا ناشناخته‌ای که می‌تواند به مهاجم امکان کنترل سرویس‌دهنده کنترل را بدهد، می‌پردازد. "آزمون نفوذپذیری سرویس‌دهنده برنامه کاربردی" که به سوء استفاده از برنامه در حال اجرا در سرویس‌دهنده کنترل می‌پردازد، "آزمون نفوذپذیری شبکه ارتباطات" که با شنود ارتباطات به شناسایی و بررسی آسیب‌پذیری‌های پروتکل می‌پردازد و "آزمون نفوذپذیری دستگاه تعبیه‌شده" که به شناسایی حملات فیزیکی علیه دستگاه‌های ICS می‌پردازد. این فرآیند با یک تجزیه و تحلیل کلی و گزارش نتایج به دست آمده به پایان می‌رسد.

- **Object Linking and Embededding (OLE) for Process Control (OPC) standards**

OPC یک سری از استانداردهای تعامل متقابل برای تبادل امن و قابل اعتماد اطلاعات در فضای اتوماسیون صنعتی و در صنایع دیگر است. بنیاد OPC مسئول توسعه و نگهداری این استاندارد است. استاندارد OPC یک سری مشخصات توسعه‌یافته توسط فروشندگان صنعت، کاربران نهایی و توسعه‌دهندگان نرم‌افزار می‌باشد. این مشخصات رابطی بین کاربران و سرورها و همچنین سرور و سرور، از جمله دسترسی به اطلاعات در زمان واقعی، نظارت بر هشدارها و حوادث، دسترسی به داده‌های تاریخی و کاربردهای دیگر را تعریف می‌کند. OPC برای ارائه یک پل مشترک برای برنامه‌های کاربردی نرم‌افزارهای مبتنی بر ویندوز و سخت‌افزار کنترلی طراحی شده است.

- **American Gas Association (AGA) Standard 12, “Cryptographic Protection of SCADA Communications”**

سری AGA 12 شیوه‌های توصیه‌شده‌ای برای محافظت از ارتباطات اسکادا در برابر حوادث سایبری را ارایه می‌کند. این شیوه‌ها بر روی حصول اطمینان از محرمانه بودن ارتباطات اسکادا تمرکز کرده‌اند. هدف از سری AGA 12 صرفه‌جویی در وقت و تلاش صاحبان سیستم اسکادا با ارایه یک سیستم جامع

جهت محافظت از ارتباطات اسکادا با کمک رمزنگاری می‌باشد. سری AGA 12 ممکن است برای سیستم آب، فاضلاب، برق و سیستم‌های توزیع مبتنی بر اسکادا به دلیل تشابه آن‌ها با سیستم‌های گاز طبیعی قابل استفاده باشد، با این حال ممکن است نیازمندی‌های زمان‌بندی متفاوتی داشته باشند. این سری از استانداردها در چهار بخش زیر به بحث امنیت ارتباطات سیستم‌های اسکادا می‌پردازد:

- AGA گزارش شماره ۱۲، قسمت ۱ (۲۰۰۶) - "توصیه‌های عمومی"، شامل پیش زمینه، اصول سیاست امنیتی و یک طرح آزمون می‌باشد که به طور کلی به تمام زمینه‌های حفاظت به‌وسیله رمزنگاری از سیستم‌های اسکادا اعمال می‌شود.
- AGA گزارش شماره ۱۲، قسمت ۲ (۲۰۰۷) – "نتایج تست عملکرد"، بر حفاظت تجهیزات نصب شده، کم‌سرعت و دارای ارتباطات سریال تمرکز دارد. این سند شامل الزامات عملکردی و مشخصات فنی دقیق برای دستگاه‌های سازگار با AGA 12 است.
- AGA گزارش شماره ۱۲، قسمت ۳ (منتشر نشده) – "حفاظت از سیستم‌های شبکه‌ای"، بر سیستم‌های ارتباطی با سرعت بالا، از جمله تعاملات داخلی تمرکز می‌کنند.
- AGA گزارش شماره ۱۲، قسمت ۴ (منتشر نشده) – "حفاظت تعبیه شده از قطعات اسکادا"، مشخص خواهد کرد که چگونه از سیستم‌های اسکادا به وسیله ترکیب رمزنگاری در داخل قطعات سیستم در زمان تولید حفاظت شود، این موضوع تا حد زیادی هزینه‌های حفاظت را کاهش می‌دهد، در حالی که عملکرد بهبود می‌یابد.

- **RFC 6272 - Internet Protocols for the Smart Grid**

این سند به شناسایی پروتکل‌های زیرساخت کلید از سلسله پروتکل‌های اینترنت برای استفاده در شبکه هوشمند می‌پردازد. مخاطبان هدف، آن دسته از افرادی هستند که به دنبال راهنمایی در مورد چگونگی ساخت یک سلسله پروتکل اینترنت مناسب برای شبکه هوشمند هستند.

- **MTR070050- MITRE TECHNICAL REPORT: Addressing Industrial Control Systems in NIST Special Publication 800-53**

هدف کلی از این گزارش تجزیه و تحلیل نحوه پرداختن استاندارد SP 800-53 به امنیت سایبری در سیستم‌های کنترل صنعتی (ICS) است، با تمرکز خاص بر روی سیستم‌های انرژی الکتریکی که بخشی از زیرساخت‌های حیاتی می‌باشند.