هشدار به صنایع دارای تجهیزات Schneider Electric، OMRON و پروتکل OPC UA

کد گزارش: AMAN-SA-APT0102 **نسخه:** 0.4.5

طبقه‌بندی سند: عادی

تاریخ: ۸ اردیبهشت ۱۴۰۱

(۰۲۱) ۸۸۵۸۱۷۹۸ (۰۲۱) ۸۸۵۸۱۷۹۸
www.AmanSec.ir info@AmanSec.ir Social Media: @Aman_Sec
تهران، شهرک قدس، انتهای(غربی) بلوار شهید دادمان، پژوهشگاه نیرو، مرکز توسعه فناوری صنعت برق و انرژی (ساختمان رویش)، طبقه ۲

شناسنامه سند

عنوان سند	هشدار به صنایع دارای تجهیزات Schneider Electric، OMRON و پروتکل OPC UA
کد سند	AMAN-SA-APT0102
نسخه سند	0.4.5
موضوع سند	پیشنهاد پروژه
طبقه‌بندی سند	عادی
تعداد صفحات	۲۷
تهیه‌کننده	واحد فنی شرکت پیشگامان امن‌آرمان (امان)
تأییدکننده	شرکت پیشگامان امن‌آرمان (امان)
تاریخ تنظیم سند:	۰۱/۰۲/۰۴
تاریخ تحویل:	۰۱/۰۲/۰۸
تاریخ انتشار نسخه عمومی:	۰۱/۰۲/۱۰

فهرست مطالب

مالکیت معنوی و حق کپی‌برداری

چنانچه تمایل دارید گزارش حملات، آسیب‌پذیری‌ها و ویژه‌نامه‌هایی مشابه این گزارش را دریافت نمایید، اطلاعات تماس به‌ویژه آدرس ایمیل به همراه معرفی سازمان/صنعت خود را به نشانی info@AmanSec.ir ارسال نمایید تا به شکل رایگان این گزارش‌ها را دریافت نمایید.

[۱] حقوق این اثر برای امان شامل برگردانی فارسی تخصصی متن از مرجع انگلیسی و اضافه کردن تجارب تخصصی شرکت امان است.

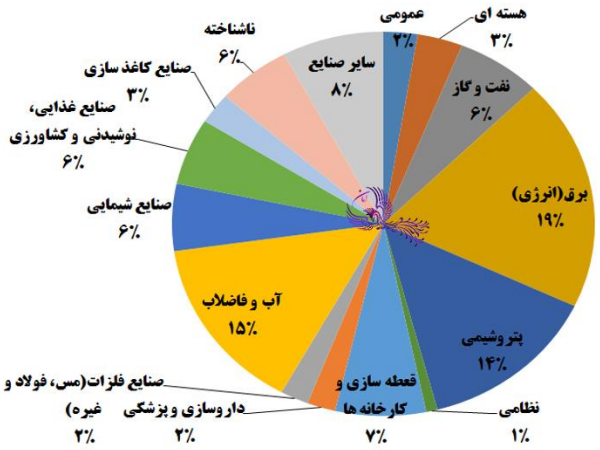
سلب مسئولیت

هدف این سند آگاهی بخشی و اطلاع‌رسانی به سازمان‌ها، صنایع و زیرساخت‌های حیاتی کشور است و محتوای آن در راستای ارتقاء امنیت سامانه‌های کنترل صنعتی کشور تأمین‌شده است؛ لذا عواقب هرگونه استفاده سوء از آسیب‌پذیری‌های امنیتی و ابزارهای معرفی‌شده یا عدم پیاده‌سازی صحیح راهکارهای پیشنهادی بر عهده مخاطب است.

این نسخه از گزارش عاری از ایراد نیست؛ در مورد جمله به جمله آن، انتقادها و پیشنهادهای دلسوزانه‌ی شما را با آغوشی باز و باافتخار، پذیرا هستیم.

مقدمه

اهمیت صنایع برق، نفت و گاز، آب و آبفا، پتروشیمی، هسته‌ای، فلزات و غیره به‌عنوان زیرساخت‌های حساس و حیاتی کشور به حدی است که می‌تواند به‌عنوان هدف مهاجمین برای ایجاد مشکلات ملی قرار گیرند. این امر می‌تواند آثار بسیار مخرب و زیان‌باری در ابعاد بسیار وسیع در پی داشته باشد. با افزایش به‌کارگیری فناوری در سامانه‌های کنترل صنعتی، DCS، SIS/ESD و نظایر آن، حوادث در این سامانه‌ها به‌جای اینکه صرفاً ناشی از عوامل داخلی و اتفاقات فنی باشد با رخدادها و حملات سایبری همگرا شده است. بر اساس بررسی‌های انجام‌گرفته توسط محققین شرکت امان که دریکی از معتبرترین ژورنال‌های تخصصی این حوزه به چاپ رسیده است[۱]، صنایع برق(انرژی)، آب و فاضلاب، پتروشیمی‌ها در صدر حوادث و حملات سایبری صنعتی در دنیا قرار دارند.



شکل ۱: وضعیت صنایع از حیث تعداد حوادث و حملات سایبری

[۱] Ahmadian et al., Industrial Control System Security Taxonomic Framework with Application to a Comprehensive Incidents Survey. International Journal of Critical Infrastructure Protection (Elsevier), 2020.doi: j.ijcip.2020.100356

سامانه‌های کنترل و اتوماسیون صنعتی (DCS، PLC، اسکادا، تله‌متری، دیسپاچینگ، ESD و غیره) ازجمله اهداف آسیب‌پذیر در مقابل حملات سایبری‌اند. دلایل متعددی برای این آسیب‌پذیری‌های قابل‌توجه می‌توان ذکر کرد. افزایش انگیزه مهاجمان و سوق پیدا کردن جنگ‌های سایبری به سمت زیرساخت‌های حیاتی صنعتی یکی از این دلایل است.

بهره‌گیری روزافزون صنایع از فناوری‌های جدید به‌ویژه در بخش سامانه‌های حفاظت و کنترل، دلیل دیگر گسترده بودن اهداف قابل تهدید در صنایع است. گستردگی و پیچیدگی‌های فنی، جغرافیایی و سازمانی صنایع که معمولاً با عدم یکپارچگی مدیریت امنیت سایبری نیز همراه است موجب می‌شود بخش‌های مختلفی از سامانه‌ها و تجهیزات این مجموعه‌ها در معرض تهدید باشد.

شکل ۲: آرام بودن به معنی امنیت نیست!

به‌تازگی سازمان‌های NSA، DOE، FBI،CISA [۱] در خصوص هک و نفوذ به سامانه‌های کنترل صنعتی (ICS)، سامانه‌های اسکادا (SCADA)و PLCهای مرتبط با برندها و پروتکل ذیل هشدار داده‌اند:

- Schneider Electric programmable logic controllers (PLCs)
- OMRON Sysmac NEX PLCs
- Open Platform Communications Unified Architecture (OPC UA) servers

در این هشدار تأکید شده است که مهاجمین در این نفوذها توانسته‌اند دسترسی کاملی به شبکه‌های صنعتی قربانی پیدا نمایند. یکی از نکات قابل‌توجه که در این حملات گزارش داده‌شده، این است که مهاجمین از ابزارهای توسعه داده‌شده خاص‌منظوره‌ای استفاده کرده‌اند تا بتوانند سطح دسترسی و ابعاد حمله را تا عمق سامانه‌های کنترل صنعتی (که PLCها و DCSها هستند) گسترش دهند. در این حملات مهاجمین از مرحله شناسایی، نفوذ اولیه، گسترش نفوذ و ایجاد خسارت از این ابزارهای خاص‌منظوره استفاده می‌نمایند که در تجارب بالغبر هشت‌ساله رصد حملات توسط شرکت امان نیز کمتر شاهد آن بودیم.

در این حملات شاهد این بودیم که سامانه‌های کنترل صنعتی از نوع ایستگاه‌های مهندسی دارای سیستم‌های‌عامل ویندوز، از اکسپلویت‌های آسیب‌پذیری‌های شناخته‌شده درایورهای مادربردهای ASRock مورد نفوذ قرار گرفتند.

[۱] https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

جزئیات فنی

همان‌طور که در ابتدای این گزارش بیان شد، اخیراً در خصوص هک و نفوذ به شبکه‌ها و تجهیزات کنترل صنعتی Schneider Electric، OMRON و پروتکل OPC UA هشدار جدی داده‌شده است. در لیست ذیل جزئیات بیشتری از این دارایی‌های آسیب‌پذیر را مشاهده می‌کنیم:

- Schneider Electric MODICON and MODICON Nano PLCs, including (but may not be limited to) TM251, TM241, M258, M238, LMC058, and LMC078;
- OMRON Sysmac NJ and NX PLCs, including (but may not be limited to) NEX NX1P2, NX-SL3300, NX-ECC203, NJ501-1300, S8VK, and R88D-1SN10F-ECT
- OPC Unified Architecture (OPC UA) servers.

ابزارهای مذکور ماژولار بوده و می‌توانند به شکل کاملاً خودکار توسط مهاجمین اجرا شوند. این ابزارها دارای یک کنسول مجازی با یک رابط فرمان شبیه به رابط دستگاه‌های کنترل و اتوماسیون صنعتی هستند. متأسفانه این ماژول‌های خطرناک این امکان را ایجاد می‌نمایند که حتی مهاجمین با سطح مهارتی پایین، بتوانند قابلیت‌های پیشرفته مهاجمان حرفه‌ای را شبیه‌سازی نمایند و این برای صنایع کشور می‌تواند بسیار خطرناک باشد.

علاوه بر این، این گروه از مهاجمین از ابزاری استفاده می‌کنند که یک درایور مادربرد آسیب‌پذیر شناخته‌شده به نام AsrDrv103.sys را نصب می‌کنند و از آسیب‌پذیری با شناسه CVE-2020-15368 موجود در آن برای اجرای بدافزار در سطح هسته ویندوز استفاده می‌کنند. در ادامه مهاجمین با استفاده از تکنیک‌های حرکات جانبی سعی می‌کنند از راه‌های آشکار و پنهان میان شبکه‌های اداری، فاوا و نظایر آن به شبکه‌های صنعتی نفوذ کنند که لازم است صنایع کشور نسبت به آن آگاه باشند. در ادامه به تفکیک سازنده و پروتکل به این موضوع خواهیم پرداخت.

ابزار APT برای دستگاه‌های Schneider Electric

ابزار موردنظر برای تجهیزات شرکت اشنایدر دارای ماژولی‌هایی است که امکان ارتباط از طریق پروتکل معمول مدیریتی و مدباس TCP بر روی پورت ۵۰۲ را فراهم می‌کند. این ماژول‌ها می‌تواند این امکان را بدهند که:

- مهاجمین یک اسکن سریع جهت شناسایی PLCهای شرکت اشنایدر بر روی شبکه محلی صنعت انجام دهند. این اسکن با ارسال پیام‌های مالتی کست[۱] UDP با پورت مقصد ۲۷۱۲۷ انجام می‌گیرد. لازم به ذکر است اسکن از طریق پروتکل UDP با پورت مقصد ۲۷۱۲۷ یک اسکن استاندارد است که توسط ایستگاه‌های کاری مهندسی برای شناسایی عادی PLC ها در شبکه‌های صنعتی استفاده می‌شود و ممکن است لزوماً نشان‌دهنده فعالیت‌های مخرب نباشد. این نکته بسیار مهم است که در تنظیم قواعد سامانه‌های تشخیص نفوذ صنعتی و SIEM به نحوی عمل نماییم که هشدارهای منفی کاذب را (به دلیل رفتار طبیعی شبکه) گزارش ندهیم. ما در امان، در حوزه خدمات شناسایی حملات به این نکات کلیدی نهایت توجه را داریم تا در بالاترین سطح کیفی بتوانیم به شرکت‌ها و صنایع کشور ارائه خدمات داشته باشیم.

- این ماژول‌ها امکان اجرای حملات جست‌وجوی رمزهای عبور دستگاه‌های PLC را با استفاده از پروتکلCODESYS یا سایر پروتکل‌های رایج و از طریق پورت ۱۷۴۰ UDP را میسر می‌کند. همان‌طور که در دوره‌های آموزشی تخصصی امنیت صنعتی امان همیشه تذکر می‌دهیم، چنانچه برای دسترسی به PLCها، DCS و حتی ESD از رمزهای عبور پیش‌فرض یا ساده استفاده نماییم مهاجمین با استفاده از این ابزارها می‌توانند حتی به تجهیزات لایه کنترل محلی مانند PLCها نیز دسترسی پیدا نمایند. در این هشدار تذکر داده‌شده است که امکان دارد این ماژول‌ها، سایر

[۱] multicast

تجهیزاتی کـه از طریق CODESYS ارتبـاط برقرار می‌کننـد را نیز موردحملـه قرار دهند که زنگ خطری است برای برخی صنایع که از این تجهیزات و پروتکل مربوطه استفاده می‌کنند.

- همان‌طور که در تصـور نمادین ذیل مشاهده می‌کنیم، این ماژول‌ها امکان اجرای حملات ممانعت از خـدمات (DoS) بر روی تجهیزات PLC را به نحوی فراهم می‌کنند که از طریق شـــبکه امکان دسترسی به کنترل‌کننده‌ها و مدیریت فرایند وجود نخواهد داشت.

شکل ۳: تصویر نمادین نفوذ به یک DCS

- این مـاژول‌ها امکان اجرای حملات ممانعت از خدمات(DoS) با ارســـال بســـته‌های مرگ[۱] علیه تجهیزات PLC را به نحوی فراهم می‌کند که امکان پیکربندی مجدد و راه‌اندازی مجدد PLC سلب خواهد شد.

- این ماژول‌ها باعث قطع ارتباط کاربران مربوطه و سـیسـتم مهندسی با PLC می‌شود و مهندسین بهره‌بردار یا تعمیر و نگهداری، مجبور خواهند شـد مجدد به PLC درخواست تصدیق اصالت دهند. احتمال می‌رود مهاجمین از این طریق بتوانند نام کاربری و رمزهای عبور PLCها را به دست آورند.

- این ماژول‌ها امکان ارســـال فرمان‌های مختلف از طریق پروتکل مدباس را نیز فراهم می‌کند و این ویژگی می‌تواند برای PLCهای غیر از برند اشنایدر نیز کارا باشد که واحدهای متولی امنیت صنایع کشور لازم است در این مورد تدابیری را اتخاذ نمایند.

در جدول ذیل مشـــخصـــات فنی تاکتیک‌ها و تکنیک‌های این ابزار در مورد برند اشـــنایدر را بر اســـاس چارچوب ATT&CK for ICS مشاهده می‌کنیم.

Tactic	Technique
Execution	Command-Line Interface [T0807]
	Scripting [T0853]
Persistence	Modify Program [T0889]
	System Firmware [T0857]
	Valid Accounts [T0859]
Discovery	Remote System Discovery [T0846]
	Remote System Information Discovery [T0888]
Lateral Movement	Default Credentials [T0812]
	Program Download [T0843]
	Valid Accounts [T0859]

[۱] packet of death

Collection	
	Monitor Process State [T0801]
	Program Upload [T0845]
	Monitor Process State [T0801]
Command and Control	Commonly Used Port [T0885]
	Standard Application Layer Protocol [T0869]
Inhibit Response Function	Block Reporting Message [T0804]
	Block Command Message [T0803]
	Denial of Service [T0814]
	Data Destruction [T0809]
	Device Restart/Shutdown [T0816]
	System Firmware [T0857]
Impair Process Control	Modify Parameter [T0836]
	Unauthorized Command Message [T0855]
Impact	Denial of Control [T0813]
	Denial of View [T0815]
	Loss of Availability [T0826]
	Loss of Control [T0827]
	Loss of Productivity and Revenue [T0828]
	Manipulation of Control [T0831]
	Theft of Operational Information [T0882]

ابزار APT برای دستگاه‌های OMRON

ابزار موردنظر برای تجهیزات شرکت OMRON دارای ماژولی‌هایی است با امکانات ذیل:

- این ماژول‌ها به مهاجمین این قابلیت را می‌دهد که از طریق پروتکل FINS اقدام به شناسایی تجهیزات OMRON نمایند.
- در شناسایی به کمک این ابزارها امکان دریافت و شناسایی آدرس MAC تجهیزات صنعتی وجود دارد.
- این ماژول‌ها به مهاجمین این قابلیت را می‌دهد که اطلاعات پروتکلHTTP را که سوی تجهیزات صنعتی دریافت می‌شود را تجزیه‌وتحلیل نمایند.
- این ماژول‌ها به مهاجمین این قابلیت را می‌دهد که به کمک روش سرشماری[۱] به تجهیزات متصل به PLC دسترسی پیدا کنند و همچنین بتوانند از تجهیزات متصل به PLC، نمونه یا داده‌برداری انجام دهند.
- این ماژول‌ها به مهاجمین این قابلیت را می‌دهد که هر نوع فایل دلخواهی را بر روی PLCها بازیابی یا از PLCها پشتیبان‌گیری نمایند.
- درنهایت، این ماژول‌ها به مهاجمین این قابلیت را می‌دهد که بر روی این PLCها یک کد مخرب سفارشی را برای اهداف حملات دیگر و برای روز مبادا بارگذاری نمایند که امان در مورد این ویژگی‌های به جد هشدار می‌دهد. این ماژول‌ها امکان غالب تعاملاتی که در بردار حملات، توسط مهاجمین در چارچوب ATT&CK for ICS ارائه‌شده است را فراهم می‌کند. تمامی این تکتیک‌ها و

[۱] Polling

تاکتیک‌ها در دوره‌های آموزشی پیشگامان امن آرمان تبیین می‌شود. در جدول ذیل این تکنیک‌ها و تاکتیک‌ها مشخص‌شده‌اند.

Tactic	Technique
Initial Access	Remote Services [T0886]
Execution	Command-Line Interface [T0807]
	Scripting [T0853]
	Change Operating Mode [T0858]
	Modify Controller Tasking [T0821]
	Native API [T0834]
Persistence	Modify Program [T0889]
	Valid Accounts [T0859]
Evasion	Change Operating Mode [T0858]
Discovery	Network Sniffing [T0842]
	Remote System Discovery [T0846]
	Remote System Information Discovery [T0888]
Lateral Movement	Default Credentials [T0812]
	Lateral Tool Transfer [T0867]
	Program Download [T0843]
	Remote Services [T0886]
	Valid Accounts [T0859]
Collection	Detect Operating Mode [T0868]
	Monitor Process State [T0801]
	Program Upload [T0845]
Command and Control	Commonly Used Port [T0885]
	Standard Application Layer Protocol [T0869]
Inhibit Response Function	Service Stop [T0881]
	Modify Parameter [T0836]

Impair Process Control	Unauthorized Command Message [T0855]
Impact	Damage to Property [T0879]
	Loss of Safety [T0837]
	Manipulation of Control [T0831]
	Theft of Operational Information [T0882]

ابزار APT برای پروتکل OPC UA

ابزار موردنظر برای تجهیزاتی که پروتکل OPC UAرا پشتیبانی می‌کنند یا از آن استفاده می‌کنند دارای ماژولی‌هایی است با امکانات ذیل:

- این ماژول‌ها به مهاجمین این قابلیت را می‌دهد که سرورهای OPC UA را شناسایی نمایند.
- این ماژول‌ها به مهاجمین این قابلیت را می‌دهد که سرورهای OPC UA را به کمک نام‌های کاربری و رمز عبور پیش‌فرض یا سرقت شده مورد دسترسی قرار دهند.
- علاوه بر موارد فوق این ماژول‌ها امکان نوشتن تگ‌ها توسط OPC UA را فراهم می‌کند که به جد قابلیتی با سطح ریسک بالا است و شرکت امان در مورد سوءاستفاده‌های آتی احتمالی در صنایع کشور (در صورت عدم ارتقاء) هشدار می‌دهد. لازم به ذکر است که در چند سال اخیر، در مورد قابلیت‌های OPC UA و ویژگی‌های امنیتی آن در دوره‌های آموزشی مطالب متعددی را خدمت مخاطبین گرامی امان ارائه کرده‌ایم. باوجوداین قابلیت‌ها، مشابه هر پروتکل دیگری لازم است مقوله به‌روزرسانی تجهیزات مرتبط را در دستور کار قرار دهیم.

در جدول ذیل این تکنیک‌ها و تاکتیک‌ها مشخص‌شده‌اند.

Tactic	Technique
Execution	Command-Line Interface [T0807]
	Scripting [T0853]
Persistence	Valid Accounts [T0859]
Discovery	Remote System Discovery [T0846]
	Remote System Information Discovery [T0888]
Lateral Movement	Valid Accounts [T0859]
Collection	Monitor Process State [T0801]
	Point & Tag Identification [T0861]

Command and Control	Commonly Used Port [T0885]
	Standard Application Layer Protocol [T0869]
Impact	Manipulation of View [T0832]
	Theft of Operational Information [T0882]

راهکارهای مقابله و کاهش ریسک

بر اساس اطلاعات در دسترسی فعلی امان تاکنون در کشور آلودگی مرتبط با این ابزارهای APT گزارش نشده است. در ادامه برخی راهکارهای کاهش ریسک و مقابله با ابزارهای فوق همراه با تجربیات امان در این حوزه ارائه می‌شود. لازم به ذکر است که این راهکارها برای تمامی محیط‌های صنعتی آزموده نشده است و حتماً توصیه می‌شود که قبل از پیاده‌سازی در شبکه صنعتی در شرایط آزمایشگاهی یا محدود مورد آزمایش قرار گیرند.

- توصیه معمول در این موارد این است که شبکه‌های صنعتی (OT) چنانچه ارتباطی با شبکه اداری، فاوا، اینترنت و نظایر آن دارند در سریع‌ترین زمان این ارتباطات قطع یا محدود شود. لازم به ذکر است در بسیاری از صنایع مشاهده می‌کنیم که تصور به ایزوله بودن کامل شبکه صنعتی وجود دارد اما در ارزیابی‌های متعدد شاهد آن بودیم که اتصالاتی میان شبکه OT با شبکه ITوجود دارد.

- چنانچه در صنعت خود از ضدبدافزار[۱]یا سامانه تشخیص نفوذ (IDS) استفاده می‌کنید (در صورت به‌روزرسانی شرکت ارائه‌دهنده) هرچه سریع‌تر محصول امنیتی خود را به‌روزرسانی نمایید.

- استفاده از تجهیزات جمع‌آوری لاگ‌های امنیتی نظیر IDSها و SIEM توصیه می‌شود. به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک محصولاتی مانند SIEM کنترل صنعتی و سامانه تشخیص نفوذ صنعتی (IDS) به شکل مستمر کلیه تجهیزات سامانه و ترافیک عبوری را پایش نمایید.

---

[۱] antivirus

- چنانچه در شبکه صنعتی یا تجهیزات مربوطه امکان تصدیق هویت چند عامله یا چندمرحله‌ای دارید حتماً آن را فعال نمایید.

- حتماً برای صنعت خود برنامه مقابله با حوادث و طرح تداوم کسب‌وکار (BCP) تهیه نمایید و طبق برنامه چندین بار آن را تمرین نمایید. ما در امان همراه شما هستیم تا چنانچه صنعت شما در این بخش ضعف دارد، این مستندات و دستورالعمل‌ها را برای شما آماده نماییم.

- اکیداً توصیه می‌کنیم در مورد تجهیزاتی که در این گزارش به آن‌ها اشاره شد رمزهای عبور پیش‌فرض را تغییر دهید. همچنین به دلیل سطح حساسیت این نوع از مخاطرات توصیه می‌شود که رمزهای عبور را به شکل دوره‌ای تغییر دهید.

- اکیداً توصیه می‌کنیم از تمامی تجهیزات مذکور پشتیبان‌گیری آفلاین صورت گیرد و از صحت فایل‌های پشتیبان اطمینان حاصل نمایید. چنانچه در مورد نحوه کنترل صحت فایل‌ها اطلاعات کافی ندارید، بخش آموزش امان می‌تواند این موارد را به صنعت شما آموزش دهد.

- به مدیران شبکه‌های سازمانی یا کنترل صنعتی توصیه می‌شود که دسترسی به محصولات احتمالاً تحت تأثیر و سامانه مدیریت و نظارت بر آن را محدود کنند. لازم است دسترسی‌ها به تجهیزات مذکور صرفاً از طریق ایستگاه‌های کاری مهندسی مجاز صورت پذیرد و سایر دسترسی‌های غیرضروری به این تجهیزات مسدود شود. در صورت عدم به‌روزرسانی محصولات امنیتی نامبرده در صورت امکان، حتماً دسترسی آن‌ها به شبکه عمومی (به‌ویژه اینترنت یا VPN های پیمانکاران) قطع گردد.

- تا جایی که امکان دارد باید نمای حمله مهاجمین جهت دسترسی به دارایی‌های سایبر-فیزیکی (تجهیزات و سیستم‌ها) شما به حداقل برسد؛ اتصال این تجهیزات را به شبکه‌های غیر امن به حداقل برسانید.

- لازم است ایستگاه‌های کاری مهندسی و مدیریتی توسط ابزارهای محافظتی از نوع Device Guard، Credential Guard، Hypervisor Code Integrity (HVCI) و EDR محافظت شوند.

- به مدیران شبکه‌های کنترل صنعتی توصیه می‌شود که به کمک راهکارهای کنترل دسترسی تنها به کاربران مجاز امکان دسترسی به شبکه داده شود (ترجیحاً این دسترسی مبتنی بر نقش اعمال شود). در دسترسی‌های اعطایی باید راهبرد حداقل دسترسی اعمال شود و تغییر در نرم‌افزارهای سامانه‌های صنعتی صرفاً در اختیار مدیر یا سرپرست مجاز واحد باشد.

- توصیه می‌شود از سازوکارهای انتقال امن فایل برای مبادله فایل‌های دریافتی از اینترنت یا پیمانکار (برنامه‌ها، به‌روزرسانی‌ها و غیره) استفاده گردد.

- توصیه می‌شود که در صورت اتصال شبکه‌ی کنترل صنعتی به شبکه‌های دیگر حتماً از دیواره آتش کنترل صنعتی یا یک‌سوساز کنترل صنعتی استفاده نمایید.

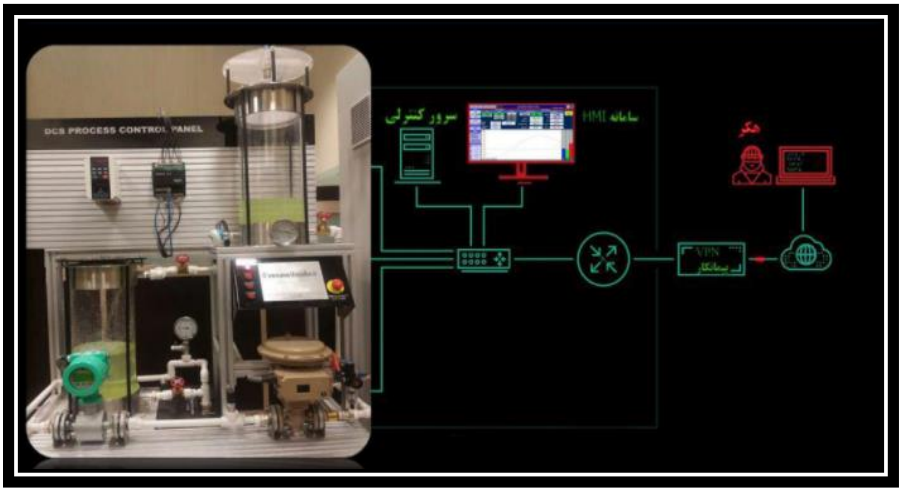
- ما در امان توصیه می‌کنیم که در صورت محدودیت در شبکه یا پلنت صنعتی و جهت اتخاذ رویکرد کاهش مخاطره، سامانه‌های تحت تأثیر را در یک زیر شبکه ایزوله یا محدوده‌ی امن قرار دهید.

- توصیه می‌شود برنامه‌ها و نرم‌افزارهای غیرضروری از تجهیزات مذکور یا سامانه‌های متصل به شبکه‌های دارای تجهیزات مذکور پاک شوند.

- لازم است هرگونه ترافیک مشکوک، ترافیک ناخواسته، شواهد حملات ممانعت از خدمات (DoS)، تأخیر یا اختلال در عملکرد PLCها، سامانه‌های HMI و مهندسی، DCSها و نظایر آن به واحد امنیت یا حراست مجموعه گزارش شود.

- لازم است کلیه سامانه‌های یادشده در این گزارش نظیر نصب درایورهای ناخواسته به‌ویژه ASRock بررسی شوند (چنانچه از قبل و به شکل مجاز ASRock نصب نبوده باشد).

- درصورتی‌که در شبکه یا واحد صنعتی شما نیاز به اتصال از راه دور دارید حتماً از راهکارهای اتصال راه دور امن نظیر VPN استفاده کنید؛ توجه شود که خودِ راهکار VPN داری آسیب‌پذیری نباشد و پاشنه آشیل نباشد؛ در شکل ۴، نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر را مشاهده می‌کنید ما در قالب دوره آموزشی می‌توانیم این تهدیدات و راهکارهای امن‌سازی آن‌ها را به شما ارائه نماییم.



شکل ٤: نمونه شماتیک سناریو نفوذ مهاجم از طریق VPN آسیب‌پذیر

- همانند غالب آسیب‌پذیری‌ها و حملات به سامانه‌های فناوری اطلاعات و کنترل صنعتی و زیرساخت‌های حساس (حساس، حیاتی و مهم) پیاده‌سازی دفاع در عمق و سایر

راهبردهای امنیتی نظیر تنوع در دفاع، موضع ایمنی در برابر خرابی، نقطه وارسی و غیره به شما توصیه می‌شود.

- درصورتی‌که هر یک از موارد بالا برای شما مبهم است، امان می‌تواند با سازمان یا صنعت شما جلسه‌ی گذاشته و راهکارهای امنیتی خود را، همراه با مجموعه خدمات امنیتی، به شما معرفی نماییم (به بخش درباه امان و ارتباط با امان، جهت مشاهده خدمات و راه ارتباطی مراجعه نمایید.)

درباره امان

شرکت پیشگامان امن‌آرمان (امان)، با استعانت از خداوند متعال و به‌منظور صیانت از سرمایه‌های عملیاتی و اطلاعاتی کشور، رسالت خویش را ارائه خدمات و محصولات بسیار باکیفیت در حوزه‌های امنیت سایبری فناوری‌های عملیاتی (OT)، با تمرکز ویژه بر روی امنیت سامانه‌های کنترل و اتوماسیون صنعتی، سامانه‌های اسکادا و نظارت، تله‌متری، دیسپاچینگ می‌داند.

متدولوژی‌های ارزیابی و مدیریت مخاطرات امنیت سایبری امان با پشتوانه علمی و عملی بالغبر ۸ سال طراحی و تبیین شده‌اند و در حال بهره‌برداری در پروژه‌های متعددی می‌باشند. آموزش‌های تخصصی امان در حوزه امنیت سایبری صنعتی، در صنایع مختلفی با موفقیت برگزار می‌گردد. در ادامه اهم خدمات قابل‌ارائه امان جهت ارائه به سازمان‌ها و صنایع محترم کشور فهرست شده‌اند:

- **ارزیابی امنیت سامانه‌های کنترل و اتوماسیون صنعتی**
  - مشاوره و اجرای فرایندهای ارزیابی امنیت سایبری بر اساس استانداردهای مرجع، به‌روش‌ها و متدولوژی‌های به‌روز و ابداعی امان
- **مدیریت مخاطرات امنیت در صنایع و سازمان‌های بالادستی**
  - مشاوره و اجرای پروژه‌های مدیریت مخاطرات امنیت سایبری بر اساس دستورالعمل‌های بالادستی و با بالاترین سطح کیفی در ایران
- **تدوین الزامات ارتقاء امنیت سایبری، دستورالعمل‌ها، نقشه راه و غیره**
  - تهیه انواع اسناد امنیتی نظیر الزامات امنیتی، دستورالعمل‌ها، توصیه‌نامه‌ها، نقشه راه، نظام‌نامه‌های امنیت سایبری، آئین‌نامه‌های نظارتی در صنایع و زیرساخت‌های حیاتی
- **امن‌سازی سایبری در صنایع و زیرساخت‌های صنعتی**
  - مشاوره، اجرا و نظارت بر انواع پروژه‌های ارتقاء امنیت سایبری در شبکه‌های صنعتی و سامانه‌های اسکادا،DCS، تله‌متری، دیسپاچینگ و غیره

- **ارائه معماری امن سایبری فناوری عملیاتی**
  - طراحی و پیاده‌سازی معماری امن سایبری در زیرساخت‌های صنعتی، صنایع و سازمان‌های بالادستی بر اساس راهبردهای امنیتی و فناوری‌های به‌روز مبتنی بر تحلیل هزینه - فایده
- **برگزاری دوره‌های آموزشی و کارگاه‌های تخصصی امنیت شبکه‌های کنترل و اتوماسیون صنعتی**
  - آموزش ارزیابی و مدیریت مخاطرات امنیتی سامانه‌های اسکادا،DCS، تله‌متری، دیسپاچینگ و غیره
  - آموزش ارتقاء امنیت سایبری سیستم‌های کنترل صنعتی و اسکادا
  - سخنرانی و ارائه انواع همایش‌های در حوزه امنیت سیستم‌های کنترل صنعتی و Industry 4.0
- **تحلیل آسیب‌پذیری‌ها و تهدیدات امنیتی سیستم‌های کنترل صنعتی و اسکادا**
  - مدل‌سازی حوادث امنیتی، حملات، تهدیدات در زیرساخت‌های صنایع و سازمان‌ها و تحلیل آسیب‌پذیری‌های امنیتی همراه با اجرای سناریوهای نفوذ
- **تهیه گزارش‌های امنیتی از حملات و حوادث سایبری**
  - تحلیل و بررسی حملات و رخدادهای سایبری و تهیه گزارش‌های دقیق، جامع از سطوح فنی تا مدیریتی
- **تحلیل و بررسی حفاظت اطلاعات در سازمان‌ها و صنایع**
  - انجام رویه‌های ارزیابی و مستندسازی حفاظت اطلاعات سایبر-فیزیکی در سازمان‌ها و صنایع
- **تدوین و ارائه برنامه‌های آگاهی‌بخشی و حساس‌سازی امنیتی**
  - برنامه‌های آگاهی‌بخشی و حساس‌سازی امنیت سایبری شامل ارائه محتواهای آموزشی و هشداردهی، تهیه پوسترها و کلیپ‌های امنیتی، ارزیابی و سنجش سطح بلوغ پرسنل و غیره است که میزان فرهنگ امنیت صنعت یا سازمان را افزایش می‌دهد.

همچنین حوزه‌های فعالیت امان در ادامه مشخص شده اند:

امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی، اسکادا، DCS، دیسپاچینگ، ESD، تله‌متری

مدیریت مخاطرات (ریسک) امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی	★★★★★★★★★★
آموزش تخصصی امنیت سایبری سامانه‌های کنترل صنعتی و اسکادا	★★★★★★★★★★
مشاوره در اجرای راهکارهای امنیت سایبری سامانه‌های کنترل و اتوماسیون صنعتی	★★★★★★★★★★
ارزیابی مخاطرات سایبری سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی	★★★★★★★★★★
طراحی و پیاده‌سازی معماری امن صنعتی مطابق با استانداردهای خارجی و داخلی	★★★★★★★★★★
تحلیل و بررسی تخصصی افشاء اطلاعات در سامانه‌های صنعتی	★★★★★★★★★☆
تحلیل آسیب‌پذیری‌ها، تهدیدات و تست نفوذ در سامانه‌های کنترل صنعتی	★★★★★★★★☆☆

مدیریت امنیت اطلاعات

مدیریت و ارزیابی مخاطرات امنیتی سامانه‌های سایبری و شبکه‌های اداری	★★★★★★★★☆☆
تحلیل و بررسی تخصصی افشاء اطلاعات در سامانه‌های اداری	★★★★★★★★★☆
تحلیل آسیب‌پذیری‌های امنیتی سامانه‌های سایبری	★★★★★☆☆☆☆☆

ارتباط با امان

جهت ارتباط با ما از راه‌های ذیل اقدام فرمایید. کارشناسان و متخصصان ما آماده ارائه خدمات، به شما همراهان همیشگی امان هستند.

تلفن تماس

(۰۲۱) ۸۸۵۸۱۷۹۸

پست الکترونیک

info@AmanSec.ir

ساعت کاری

شنبه - پنج شنبه

۸ الی ۱۸

چنانچه تمایل دارید گزارش حملات، آسیب‌پذیری‌ها و ویژه‌نامه‌هایی مشابه این گزارش را دریافت نمایید، اطلاعات تماس به‌ویژه آدرس ایمیل به همراه معرفی سازمان/صنعت خود را به نشانی info@AmanSec.ir ارسال نمایید تا به شکل رایگان این گزارش‌ها را دریافت نمایید.