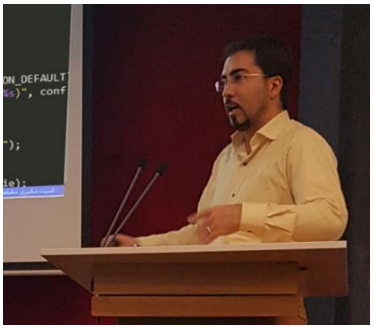
حل بحران‌های حملات سایبری به زیرساخت‌های حیاتی و حساس نظیر شرکت ملی پخش فرآورده‌های نفتی ایران با راهکارهای علمی، اصولی و عملی ممکن است نه صرفاً با دنبال مقصر گشتن!

طبقه‌بندی: عادی

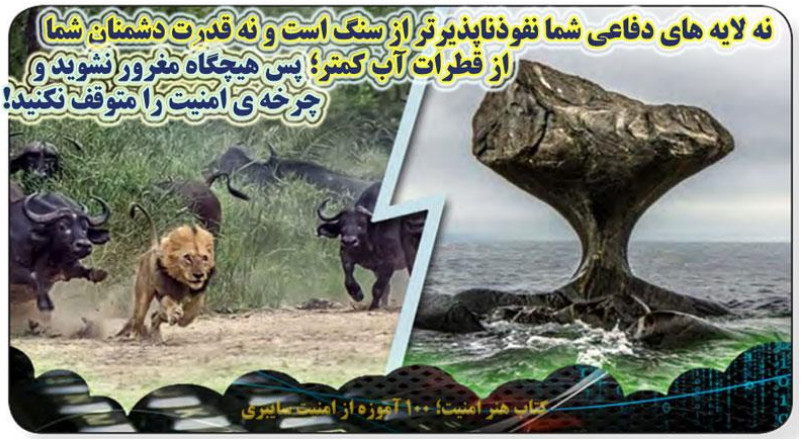
به گزارش افتانا (پایگاه خبری امنیت فناوری اطلاعات)، روز سه‌شنبه ۴ آبان تمام کشور درگیر یک اختلال در سامانه هوشمند سوخت شدند. مراجعه‌کنندگان به جایگاه‌های سوخت با پیام‌هایی از قبیل «حمله سایبری» و شماره تلفن ۶۴۴۱۱ بر روی صفحه دیجیتال پمپ‌ها مواجه می‌شدند. این موضوع واکنش‌های گوناگونی در میان مردم و کارشناسان امنیت سایبری داشت که همواره نگرانی و دغدغه‌های خود را بیان می‌کنند.



محمدمهدی احمدیان، مدرس و مشاور امنیت سایبری سیستم‌های کنترل صنعتی و اسکادا و مدیرعامل شرکت پیشگامان امن‌آرمان (امان)، در مصاحبه با افتانا می‌گوید:

متأسفانه کشور عزیزمان ایران از سال ۱۳۸۹-۱۳۸۸ به شکل جدی و علنی درگیر جنگ‌های سایبری از سوی کشورهای متخاصم شده است و در این سال‌ها تجارب متعدد مواجهه با حملات سایبر-فیزیکی را در سازمان‌ها و صنایع متعدد کشور داشته‌ایم.

روند این حملات در این سال‌ها ادامه داشته و هر ساله شاهد حوادث متعددی در صنایع و سازمان‌ها هستیم که در بسیاری از موارد با وجود زحمات مدیران و کارشناسان مربوطه، منشأ سایبری برای آن‌ها شناسایی نمی‌شود. بر اساس بررسی‌های کارشناسی و با استناد به بیانیه‌های مراجع ذی‌صلاح کشور، بسیاری از این حوادث منشأ سایبری ندارند. بااین‌وجود همانطور که برای ریشه‌یابی و تحلیل سقوط هواپیما جعبه سیاه در آن تعبیه شده، یکی از پیش‌نیازهای زیرساختی در سازمان‌ها و صنایع، پیاده‌سازی و بهره‌گیری از تجهیزات و رویه‌های ثبت، تحلیل و پایش رویدادهای امنیتی و عملکردی است تا بتوانیم در زمان وقوع حوادث و حملات سایبری یا سایبر-فیزیکی، فرایندهای جرم‌یابی سایبری (Forensic) را به شکل علمی و عملی انجام دهیم. متأسفانه علیرغم تلاش‌ها و زحمات مسئولین محترم و کارشناسان زحمت‌کش، آن‌گونه که باید در زمینه‌ی پیاده‌سازی مناسب و جامع این پیش‌نیازها موفق نبوده‌ایم و لازم است با همت مضاعف این نقاط ضعف را تبدیل به نقطه قوت نماییم.



شکل ۱: در حوزه امنیت سایبری هیچ‌گاه نباید مغرور شویم.

بر اساس تحلیل‌های تخصصی حملات سایبری که ما در امان انجام می‌دهیم به این نتیجه رسیدیم که متأسفانه به دلیل تشدید مناقشات در منطقه، از بیستم اردیبهشت ۱۳۹۹، روند جنگ‌های سایبری علیه کشور وارد مرحله جدیدی شده است. از سال گذشته تاکنون این روند به شکل روزافزونی در حال افزایش است و همواره شاهد تلاش‌های متعدد مهاجمین و نفوذگران برای ورود به شبکه‌های سازمانی و صنایع کشور هستیم. هدف برخی از این تلاش‌ها دسترسی به اطلاعات دارای طبقه‌بندی سازمان‌ها است و در مواردی دیگر متأسفانه شاهد تخریب یا خرابکاری سایبری در سامانه‌ها هستیم.

حمله اخیر به سامانه‌های هوشمند سوخت بنزین و دیزل

در مورد حمله سایبری سه‌شنبه ۴ آبان که منجر به اختلال در سامانه هوشمند سوخت شد لازم می‌دانم در ابتدا به این نکته اشاره کنیم که قطعاً تلاش‌های متعددی برای ارتقاء امنیت سایبر-فیزیکی شرکت ملی پخش فرآورده‌های نفتی ایران و زیرمجموعه‌های آن انجام گرفته است اما آنچه به نظر می‌رسد وجود ضعف در بخش‌هایی از فرایندهای امن‌سازی است. قطعاً می‌دانیم که امنیت همچون زنجیری است که حتی اگر یکی از حلقه‌های آن ضعیف باشد، آن زنجیر به‌سادگی ازهم‌گسیخته خواهد شد.

در مورد حمله مذکور، می‌دانیم که سامانه‌های هوشمند سوخت بنزین و دیزل یک شبکه بسیار وسیع و گسترده در سطح کشور است که تجهیزات متعدد و متنوعی را از جایگاه‌های سوخت تا مراکز داده و ستاد شرکت ملی پخش فرآورده‌های نفتی ایران دارد. این سامانه‌ها مدیریت، کنترل و نظارت بالغ بر چهار هزار جایگاه سوخت که شامل ۵۸ هزار نازل است را بر عهده دارند. همچنین این شبکه گسترده ارتباطات تنگاتنگی با مراکز تلفن جایگاه‌های سوخت، مناطق پخش، دفاتر خدمات کارت و مرکز مدیریت کارت دارد.

از سوی دیگر این شبکه ارتباطات دیگری را با سازمان‌های دیگر نظیر بانک‌ها و سامانه پلیس دارد. وجود این تجهیزات متنوع و متعدد و گستردگی جغرافیایی آن باعث می‌شود که اگر راهکارهای علمی، اصولی و عملی برای امن‌سازی این‌گونه شبکه‌ها طراحی، پیاده‌سازی و پایش نشود قطعاً با توجه به وضعیت بحرانی جنگ‌های سایبری در منطقه و جهان شاهد تکرار این‌گونه حملات خواهیم بود.

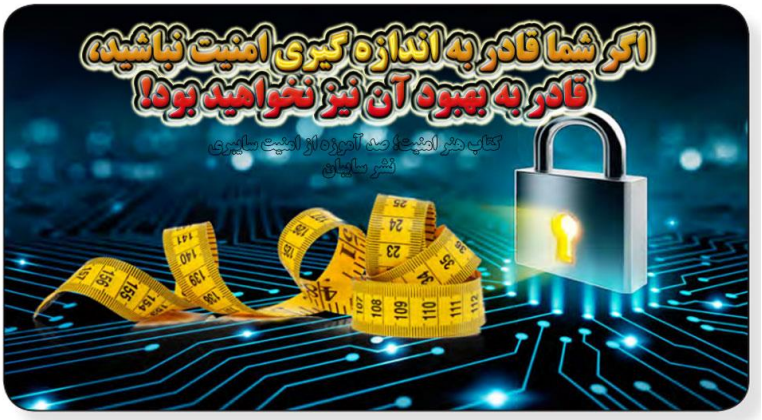
یکی از چالش‌های مقوله امن‌سازی این نمونه شبکه‌ها و سازمان‌ها وجود تجهیزات خاص‌منظوره نظیر دستگاه‌های کارت‌خوان سوخت، سامانه‌های میترینگ و تجهیزات دیگر مرتبط در جایگاه‌های سوخت است. در این نمونه شبکه‌ها قطعاً باید بر اساس راهبردهای امنیتی نظیر دفاع در عمق، امن‌سازی لایه‌ای بخش‌های مختلف شبکه نظیر کارت‌های سوخت، جایگاه‌های سوخت، مخازن، Poolerها، مراکز منطقه‌ای و پخش، مراکز پشتیان و مراکز داده در نظر گرفته شود.

چالش‌های امنیتی مرتبط با حمله اخیر به سامانه‌های هوشمند سوخت بنزین و دیزل

متأسفانه علیرغم زحمات بسیاری که مسئولین و متولیان امر در مقوله امن‌سازی سایبری اغلب سازمان‌ها و صنایع کشور کشیده‌اند، شاهد این هستیم که در برخی موارد فرایند امن‌سازی به شکل غیراصولی، غیرمنسجم و به شکل سلیقه‌ای طی شده است. لازم به ذکر است که در آغاز، پروژه سامانه هوشمند سوخت با قدرت شروع شد و حمایت‌های مناسبی از آن صورت گرفت اما به‌مرور همانند پروژه‌های متعددی در کشور از این حمایت‌ها کاسته شد و همین امر موجب کاهش توان امنیتی این شبکه شد.

می‌دانیم امنیت یک دانش است و طراحی تا اجرای فرایندهای آن نیاز به دانش فنی و تخصص دارد. از سویی دیگر باید همیشه در کنار حفظ و توسعه کسب‌وکار، امنیت آن را ارتقاء داد و به‌روز نگه داشت چرا که به‌عنوان‌مثال، سامانه‌ای که ده سال پیش امن بوده است با توسعه فناوری و از رده خارج شدن برخی تجهیزات لزوماً دیگر امن نخواهد بود.

یکی از ابزارهای این دانش استانداردهای معتبر و الزامات امنیتی بالادستی است که توسط مراجع ذی‌صلاح توصیه یا ارائه می‌شوند. این استانداردها و به‌روش‌ها به ما کمک می‌کنند تا بتوانیم در قالب انجام فرایندهای مدیریت ریسک و ارزیابی امنیتی، مبتنی بر دانش روز دنیا طرح‌های امنیتی را ارائه نماییم و بر اساس تجارب سازنده بین‌المللی و داخلی راهکاری مناسب و مورد تائید نهادهای امنیتی کشور را اجرایی نماییم. یکی از اصول اولیه امن‌سازی اصولی سامانه‌ها و شبکه انجام فرایندهای کمی و غیرسلیقه‌ای است به‌نحوی‌که بتوانیم امنیت را اندازه‌گیری نماییم و میزان موفقیت خود را در تحقق اهداف امنیت محاسبه نماییم. اگر قادر به اندازه‌گیری امنیت نباشیم قادر به بهبود آن نیز نخواهیم بود.

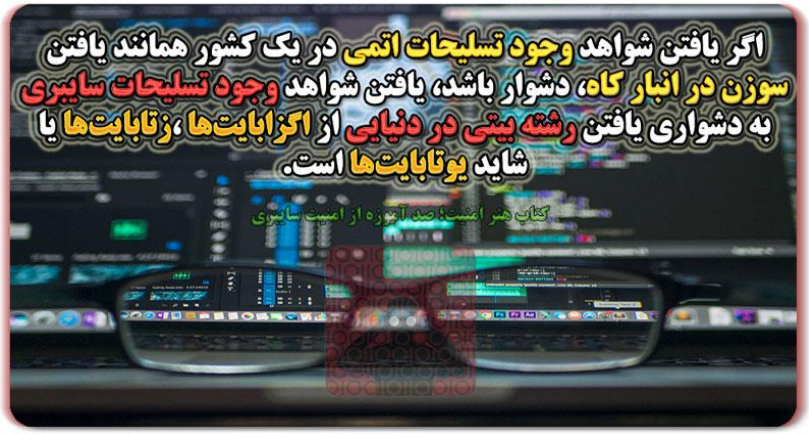


شکل ۲: در امنیت باید کمی‌سازی را جدی بگیریم!

متأسفانه در حمله مذکور شاهد این بودیم که تمام اطلاعات ۵۸ هزار نازل جایگاه‌های سوخت که شامل ۴۴ هزار نازل بنزینی و ۱۴ هزار نازل دیزلی بود توسط مهاجمین از بین رفتند. به تعبیری دیگر در جایگاه‌های سوخت اطلاعات رایانه‌های صنعتی و کارت‌خوان‌های سوخت به‌طور کامل، هم‌زمان و هماهنگ و بر اساس یک سناریو از پیش تعیین‌شده حذف شدند. همین مقوله باعث اختلال سراسری در ۴ هزار جایگاه سوخت در سراسر کشور شد و ارتباط جایگاه‌های سوخت با مراکز داده سامانه هوشمند سوخت قطع شد. در کنار این حمله گسترده، هم‌زمان شاهد حملات سایبری جانبی دیگری به تابلوهای شهری بودیم.

افزایش تبعات حمله و حملات مشابه

این نوع حملات گسترده و چندجانبه برای اولین بار در دنیا نیست که اتفاق می‌افتد و نمونه‌های متعددی در خارج از کشور توسط تیم تخصصی تحلیل حملات سایبری امان، شناسایی، مورد بررسی و موشکافی قرار گرفته است. اگرچه اظهارنظر در مورد بردارهای حمله به سامانه‌های هوشمند سوخت و نقاط ورود مهاجمین به شبکه در حال حاضر ممکن نیست و نیاز است تا بررسی‌های گروه‌های تخصصی فنی تکمیل گردد اما قاعدتاً تمامی سناریوهای نفوذ و اختلال در حال بررسی و تحلیل می‌باشد و نتایج آن توسط مراجع ذی‌صلاح کشور در صورت صلاحدید منتشر خواهد شد. با این وجود شاهد این هستیم که مهاجمین کاملاً با برنامه اقدام به طرح‌ریزی و اجرای این حمله نمودند و اشراف اطلاعاتی مناسبی از زیرساخت‌های مورد نفوذ داشتند.



شکل ۳: اظهارنظر در مورد منشأ حملات سایبری کار ساده‌ای نیست

بر اساس تجارب ما در حملات مشابه، در این سبک از حملات، مهاجمین تلاش می‌کنند ضمن آسیب زدن به سامانه‌های هدف، جهت گسترش تبعات حمله و افزایش خسارات، به نحوی عمل نمایند که فرایند مقابله با بحران و بازیابی بعد از حادثه با کندی روبه‌رو شود. در این حمله شاهد این بودیم که میزان تخریب و نحوه‌ی پاک کردن اطلاعات و اختلال در شبکه به نحوی بود که نیاز شد برای بازیابی جایگاه‌ها و ارائه خدمت به مردم در حوزه سوخت‌رسانی، کارشناسان شرکت ملی پخش فرآورده‌های نفتی به تک‌به‌تک جایگاه‌های سوخت مراجعه حضوری نمایند و هر نازل و رایانه صنعتی را با اختصاص زمان قابل‌توجه به شکل محلی مجدد برنامه‌ریزی نمایند، همین امر باعث شد که فرایند بازیابی حمله به‌سرعت امکان‌پذیر نباشد و اختلال در شبکه نیز مزید بر علت شود.

این نوع اختلال که یک سازمان را با این مشکل روبه‌رو می‌کند که لازم باشد کارشناسان خود را در ابعاد وسیع جغرافیایی به‌تمامی نقاط موردحمله اعزام نمایند تا بتوانند فرایند بازیابی را به شکل دستی و محلی

انجام دهند در حملات سایبری دیگر نیز خاموشی سراسری غرب اوکراین در سال ۲۰۱۵ (در حوزه توزیع و فوق توزیع برق) دیده شده بود. می‌توانیم از این تجارت و حملات گذشته درس بگیریم و با همکاری با متخصصین امر، رویه‌های پیشگیری از حملات، مقابله با حملات و اقدامات بازیابی پس از حادثه را به شکل مناسب پیاده‌سازی نماییم تا در این زمان‌ها کمتر غافل‌گیر شویم. طرح‌های تاب‌آوری سایبری یا تداوم کسب و کار برهمین اساس تدوین می‌شوند و کمک می‌نمایند تا در بدترین حالت فرضی که مهاجمین بیشترین خسارات را وارد می‌نمایند نیز بتوان به فرایند کسب و کار سازمان تداوم بخشید.

سخن آخر

همان‌طور که بیان شد در یک سال گذشته شاهد حملات متعددی به سازمان‌ها و صنایع کشور بودیم و به نظر می‌رسد علیرغم زحمات مسئولین مربوطه آن‌گونه که باید مقوله امنیت سایبری در سازمان‌های و صنایع کشور جدی گرفته نشده است. یکی از چالش‌های دیگر ما در کشور این است که برخی پروژه‌های با حمایت خوبی شروع می‌شوند و مسائل امنیتی در ابتدای امر دیده می‌شود اما به‌مرور، از توجه به امنیت کاسته می‌شود، این مهم فراموش می‌شود یا توسعه متوازن در همه بخش‌ها به فراموشی سپرده می‌شود. ما معتقدیم که حل بحران‌های مرتبط با حملات سایبری به زیرساخت‌های حیاتی و حساس نظیر شرکت پخش فرآورده‌های نفتی با راهکارهای علمی، اصولی و عملی، همراه با اتحاد و همدلی همه بازیگران فعال در امنیت سایبری کشور ممکن است و در این موارد صرفاً به دنبال مقصر گشتن راهگشا نخواهد بود.

استانداردها، به‌روش‌ها، تجارب ملی و بین‌المللی می‌توانند راهگشا باشد تا در قالب انجام فرایندهای مدیریت ریسک و ارزیابی امنیتی، مبتنی بر دانش روز دنیا طرح‌های امنیتی را ارائه نماییم و بر اساس تجارب سازنده راهکاری مناسب و مورد تائید نهادهای امنیتی کشور را اجرایی نماییم. البته که وحدت رویه بین نهادهای امنیتی و مشخص بودن نهاد مرجع در هر حوزه، از ضرورت‌هایی است که علیرغم تلاش‌های فراوان، متأسفانه به شکل مطلوب در کشور اجرایی نشده است. متأسفانه در پی این حمله شاهد بروز علنی اختلافات بین برخی مسئولین محترم و نهادی‌های بالادستی بودیم که در فضای عمومی تأثیر مثبتی ندارد و راهگشا نیست. به نظر ضروری است طی یک توافق ملی تنها یک نهاد حاکمیتی اجازه اظهار نظر در خصوص حادثه سایبری و جزئیات آن داشته باشد تا افکار عمومی دچار ابهام و سردرگمی نشود.

بر خود واجب می‌دانم که به این نکته نیز اشاره کنم که در این نمونه حملات، چنانچه به مردم و سرمایه‌های مردمی آسیب رسیده است لازم است مسئولین مربوطه ضمن پذیرش کاستی‌ها از مردم فهیم ایران عذرخواهی نمایند؛ به‌طور خاص در این حمله شاهد این بودیم که مقام محترم ذی‌ربط، از مردم عذرخواهی نمودند. امیدواریم این رفتار پسندیده به‌عنوان یک اقدام ارزشمند در نظر گرفته شود و فرهنگ عذرخواهی، بیش‌ازپیش، به یک فرهنگ سازمانی در کشور تبدیل شود و همیشه به درک عمیق و دقت نظر مردم عزیزمان که سرمایه اصلی کشور هستند احترام بگذاریم.

در نهایت لازم می‌دانیم توصیه نماییم که در حوزه راهکارهای بازیابی شبکه و سامانه‌ها، نهایت دقت و اصول فنی امنیتی را در بالاترین سطح ممکن در نظر بگیریم تا مشابه تجارب برخی حملات در دنیا، مجدد این شبکه مورد حمله سایبری قرار نگیرد. همچنین سایر سازمان‌ها و صنایع کشور به‌ویژه در حوزه برق، آب، گاز

و غیره نیز (علی‌رغم همه اقدامات ارزشمندی که تاکنون داشته‌اند) لازم است بیش‌ازپیش به مقوله امنیت سایبری توجه نمایند تا به سرمایه‌های ملی و مردمی کمتر آسیب رسد.