ISSN: 2745-3673
http://www.Rcsj.ir

مجله‌ی علمی پژوهش در علوم رایانه (سال سوم)
شماره ۱۱ / پاییز ۱۳۹۷ / ص ۶۵-۵۴

متدلوژی برای شناسایی سطح بلوغ امنیت سایبری در شبکه های هوشمند

افسون سروقد [۱]، عرفانه نوروزی [۲]، پویا روزبه جوان [۳]
[۱] دانشجو کارشناسی ارشد مهندسی تجارت الکترونیک واحد سپیدان.
[۲] استادیار گروه کامپیوتر و فناوری اطلاعات واحد سپیدان.
[۳] کارشناسی ارشد مهندسی تجارت الکترونیک واحد سپیدان.

نام نویسنده مسئول:
افسون سروقد

چکیده
امنیت برای شبکه های هوشمند، توجه بر ترکیبی از امنیت اطلاعات برای سیستم های مبتنی بر فناوری اطلاعات، شبکه های ارتباطی و تجهیزات فیزیکی شبکه برق نیاز دارد. بنابراین، این پژوهش با هدف توسعه متدلوژی برای شناسایی سطح بلوغ امنیت سایبری در شبکه های هوشمند است. این روش بر اساس دو مرحله است. گام اول مربوط به شناسایی دارایی ها، تهدیدها و تأثیرات آنهاست و مرحله دوم مربوط به تجزیه و تحلیل و طبقه بندی الزاماتی است که در گروه هایی طبقه بندی شده اند. این تجزیه و تحلیل اجازه می دهد تا سطح بلوغ یک مورد خاص را مشخص سازیم. این روش با توجه به اسکادا (سیستم نظارت بر کنترل و دستیابی داده ها) یک شرکت توزیع انرژی، و با مقایسه اسکادای توسعه یافته توسط این شرکت و اسکادای تجاری، به مقاسیه ای خواهد پرداخت. نتایج به دست آمده اعتبار روش ارائه شده را تایید می کند، زیرا نشان می دهد که این روش قادر به شناسایی سطح بلوغ برای هر دو سیستم می باشد.

واژگان کلیدی: شبکه های هوشمند، امنیت سایبری، اینترنت چیزها.

مجلـه‌ی علمی پژوهش در علوم رایانه ، شماره ۱۱ ، پاییز ۱۳۹۷، ص ۶۵- ۵۴

ISSN: 2745-3673
http://www.Rcsj.ir

مقدمه

در حال حاضر روند رو به رشدی از ظهور دستگاه های خودمختار متصل به اینترنت وجود دارد. تا سال ۲۰۲۰، پیش بینی می شود که حدود ۶,۵ میلیارد دستگاه در سیاره ما وجود خواهد داشت. این دستگاه ها، بخش بزرگی از سنسورها و محرک هایی را تشکیل می دهند که اکثر اوقات بدون تعامل انسان کار می کنند و اصطلاح "اینترنت چیزها" یا "اینترنت اشیا" یا (IoT) بر آنها می گذارند. این تجهیزات به طور عمده برای خودکارسازی خدمات زیرساخت شهری مانند حمل و نقل، آموزش، آب و برق (آب، انرژی، گاز)، سلامت و دیگر موارد استفاده می شود. [۱].

در میان امکاناتی مانند آب و برق، بخش انرژی مورد استفاده سنسورها و محرکها، یکی از آن مواردی است که در مفهوم شبکه های هوشمند، با استفاده از اندازه گیری مصرف انرژی از راه دور، سنجش و کنترل نظارت و جمع آوری اطلاعات (SCADA) برای کنترل پستها و سوئیچ ها مهم جلوه می کند. این سنسورها و محرکها، همراه با یک شبکه با کارایی بالا و سیستم های خبره، سه راسی را تشکیل می دهد که از مفهوم شبکه هوشمند پشتیبانی می کند [۲].

از آنجاییکه شبکه های برق برای سلامتی فیزیکی و اقتصادی یک ملت ضروری است، با استفاده از راه حل های شبکه های هوشمند، ضروری است که ایمنی برای حفاظت از منابع بحرانی سیستم برق مورد توجه قرار گیرد. به یاد داشته باشید که بر اساس گزارش سالانه تیم واکنش اضطراری سایبری سیستم های کنترل صنعتی (ICS-CERT) در سال ۲۰۱۴، ۳۲ درصد از حملات سایبری در ایالات متحده، در حوزه خدمات زیرساختی شهری، در بخش انرژی بوده است.

به طور سنتی، امنیت سایبری با تمرکز بر سیستم های اطلاعاتی فناوری اطلاعات (IT) همراه است که هدف آن محافظت از اطلاعات و سیستم های اطلاعاتی در خصوص دسترسی غیر مجاز، استفاده، اصلاح و یا هر نوع اقدامی که می تواند محرمانه بودن، یکپارچگی یا دسترسی اطلاعات را به خطر بیندازد، می باشد. با این حال، امنیت سایبری برای شبکه های هوشمند نیاز به یک ترکیبی از تمرکز بر امنیت اطلاعات برای سیستم های IT، برای شبکه ارتباطی و برای تجهیزات فیزیکی شبکه برق می باشد.

این مقاله با هدف ارائه روش شناسی (متدلوژی) برای شناسایی سطح بلوغ امنیت سایبری در شبکه های هوشمند است. این روش می تواند به عنوان یک راهنمای مرجع برای شرکت های برق مورد استفاده قرار گیرد که در حال اجرای یک شبکه برق هوشمند هستند، که نشان دهنده الزامات امنیت سایبری است.

۱. شبکه هوشمند

آژانس بین المللی انرژی، شبکه هوشمند را به عنوان یک شبکه برق معرفی می کند که از فناوری های پیشرفته دیجیتال برای نظارت و مدیریت انتقال برق از تمام منابع تولیدی استفاده می کند تا انرژی به دست مصرف کنندگان نهایی برسد. شبکه هوشمند با هدف هماهنگی بین نیازها و ظرفیت هر ژنراتور، اپراتورهای شبکه، مصرف کنندگان نهایی و ذینفعان بازار انرژی برای به حداقل رساندن هزینه ها و اثرات زیست محیطی و به حداکثر رساندن قابلیت اطمینان، انعطاف پذیری و ثبات سیستم طراحی و مورد استفاده قرار می گیرد [۳].

بر اساس مرجع [۳]، برخی از مزایای استفاده از شبکه های هوشمند عبارتند از:

- افزایش قابلیت اطمینان، ایمنی و بهره وری انرژی
- بهینه سازی پویا از منابع شبکه
- پیاده سازی مفاهیم پاسخ تقاضا، منابع تقاضا و منابع انرژی بهره وری.
- فنآوری اندازه گیری از راه دور، نظارت متمرکز بر شبکه و اتوماسیون توزیع
- ادغام شبکه با تجهیزات هوشمند مصرف کنندگان
- پیاده سازی و ادغام فن آوری ذخیره سازی انرژی، وسایل نقلیه الکتریکی، گرمایش خورشیدی و تولید انرژی خورشیدی
- به اشتراک گذاری اطلاعات با مصرف کننده و در دسترس بودن گزینه های کنترل.

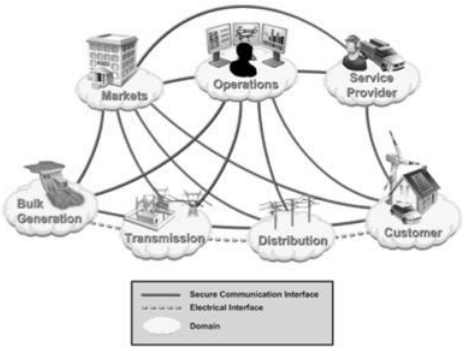
NIST (موسسه ملی استاندارد و فناوری) معماری شبکه های هوشمند را با یک مدل که از هفت حوزه تعیین شده است تعریف می کند [۲]:

- مصرف کننده (کاربر نهایی) برق می تواند تولید، ذخیره و مدیریت مصرف انرژی را نیز داشته باشد. به طور سنتی مصرف کنندگان به عنوان مسکونی، تجاری و صنعتی دسته بندی می شوند.
- بازار - اپراتورها و شرکت کنندگان در بازار خرید و فروش انرژی
- ارائه دهندگان خدمات - سازمان هایی هستند که خدمات الکتریکی را به مصرف کنندگان و کنسرسیون ها ارائه می دهند.

ISSN: 2745-3673
http://www.Rcsj.ir

• عملیات - مدیران جریان انرژی در تمام سطوح، از تولید، انتقال و توزیع قرار دارند.
• تولید - که شامل تولید متمرکز سنتی و تولید توزیع شده است.
• انتقال - مسئول حمل و انتقال انرژی در مسافت های طولانی می باشند.
• توزیع - که برق را بین مصرف کنندگان توزیع می کند.

به منظور پیاده سازی مفاهیم شبکه های هوشمند، تعامل بین حوزه های مختلف که در بالا ذکر شد، بصورتیکه که در شکل ۱ نشان داده شده است، مورد نیاز است.



شکل ۱ مدل مفهومی شبکه های هوشمند - منبع: [۲].

بر اساس مرجع [۲]، سه ستون اصلی پشتیبانی از یک شبکه هوشمند عبارتند از: تجهیزات و افراد، شبکه ارتباطی، که می تواند خصوصی، برون سپاری، سیمی یا بی سیم باشد، و سیستم های تخصصی و اپراتورهایی که برای تجزیه و تحلیل و تصمیم گیری متمرکز بکار گرفته می شوند، همانطور که در شکل ۲ نشان داده شده است.

شکل ۲ ستون های هوشمند شبکه

این سه عنصر در ادامه به صورت دقیق عبارتند از:

۲,۱. تجهیزات و مردم

این دستگاه ها بخشی از سیستم شبکه هوشمند هستند که به طور مستقیم با سیستم برق الکتریکی ارتباط برقرار می کنند، از جمله دستگاه های میدانی، دستگاه های هوشمند، تجهیزات مصرفی، وسایل الکتریکی، میتر (اندازه گیر) درجه حرارت را می توان برشمرد. مردم، مصرف کنندگان نهایی، مشارکت کنندگان در تعمیر و نگهداری شبکه، نگهداری میتر، نگهداری از وقایع تجاری و غیره هستند.

۲,۲. ارتباطات شبکه

شبکه هوشمند شامل انواع مختلفی از شبکه های عمومی و خصوصی، سیمی و بی سیم، می باشد که عبارتند از:

• WAN - شبکه های محدوده ی گسترده - که از نقاط جغرافیایی با فاصله زیاد تشکیل شده و ستون فقرات ارتباطی است.
• FAN شبکه های محدوده ی کوتاه - که دستگاه هایی مانند ترمینال ها و ترانسفورها را متصل می کند.
• NAN - شبکه های محدوده ی همسایگی - که متصل به برق هستند و در بعضی موارد نیز دستگاه های میدان را متصل می کند.
• HAN شبکه محدوده ی خانه ای- که متصل به لوازم مصرفی خانگی یا لوازم مصرفی است، نمایش داده می شود که به نوبه خود از طریق متر به NAN متصل می شود.

این شبکه ها می توانند با استفاده از ترکیبی از شبکه عمومی (به عنوان مثال اینترنت) و شبکه خصوصی اجرا شوند و در همه موارد، اجرای امنیت و کنترل دسترسی از الزامات اساسی آن می باشد.

ISSN: 2745-3673
http://www.Rcsj.ir

۳,۲. سیستم ها

سیستم های تخصصی، اجزای اساسی شبکه های هوشمند هستند و مسئولیت محوریت و ادغام (یکپارچگی) اطلاعات تولید شده توسط سنسورها، محرک ها، مشتریان و همکاران در حوزه و مرکز عملیات را بر عهده دارند. در ادامه، سیستم های اصلی که شبکه را تشکیل می دهند بر می شماریم.

• AMI - زیرساخت اندازه گیری پیشرفته: این یک راه حل پیشرفته اندازه گیری است که در آن ممکن است انجام برش های دور و ارتباط صورت گیرد. این زیرساخت شامل سیستم های اندازه گیری هوشمند، شبکه ارتباطی و مجموعه داده های اندازه گیری تخصصی MDC و مدیریت داده های اندازه گیری MDM می باشد.

• EMS - سیستم مدیریت انرژی: یک راه حل با نظارت، کنترل و بهینه سازی شبکه در زمان واقعی (آنی)، که در زمینه تولید و انتقال انرژی مورد استفاده قرار می گیرد. به طور خاص، از ویژگی های کنترل از راه دور، مدیریت خرابی قدرت، تجزیه و تحلیل شبکه در زمان واقعی، تولید گزارش با آمار شبکه، محاسبه و شبیه سازی در شبکه، آموزش اپراتور، ثبت و مدیریت دارایی های شبکه با موقعیت جغرافیایی را دارا می باشد.

• DMS - سیستم مدیریت توزیع: مانند راه حل EMS استفاده در دامنه توزیع قدرت، طراحی شده برای نظارت و کنترل شبکه توزیع و پشتیبانی از اپراتورهای توزیع و اپراتورهای زمینه می باشد.

• OMS - سیستم مدیریت خرابی: این سیستم در شرایطی که کمبود انرژی وجود دارد، به منظور تحکیم تماس مصرف کنندگان و شناسایی علت اصلی عدم انرژی، به عنوان یک ترانسفورماتور خاموش عمل خواهد کرد.

• SCADA - کنترل نظارت و دستیابی داده ها(اسکادا): سیستم ارتباطی از راه دور با دستگاه های میدان، جهت نظارت و کنترل در توزیع، انتقال و تولید استفاده می شود.

• GIS - سیستم اطلاعات جغرافیایی: راه حلی است که مدیریت دارایی های جغرافیایی را برای پشتیبانی از برنامه ریزی، طراحی و تجزیه و تحلیل شبکه برق فراهم می کند.

• CIS - سیستم اطلاعات مشتری: سیستم ارتباطی مصرف کننده برای ذخیره اطلاعات ثبت نام و مدیریت تعاملات طراحی شده است.

• BS - سیستم صورتحساب: راه حلی است که مسئول مدیریت و صدور صورتحساب مشتریان مسکونی، تجاری و صنعتی می باشد. این جزء همچنین به شما اجازه می دهد تا جمع آوری و جمع آوری هزینه ها و مالیات را مدیریت کنید.

۳.امنیت سایبری

هدف از امنیت سایبری، تضمین محرمانه بودن، یکپارچگی و دسترسی اطلاعات است [۷، ۸]. در محرمانگی، هدف این است که اطمینان حاصل شود که فقط افراد مجاز به اطلاعات دسترسی داشته باشند، از آنجمله ابزار حفاظت از حریم شخصی و اطلاعات اختصاصی می توان مثال زد و از دست دادن محرمانگی یعنی، افشای اطلاعات توسط فرد غیرمجاز است.

با این حال، یکپارچگی مربوط به حفاظت در برابر اصلاح یا تخریب اطلاعات است و حاوی تضمین صحت اطلاعات است و از دست دادن یکپارچگی، ویرایش یا تخریب اطلاعات توسط فرد غیر مجاز است. در نهایت، در دسترس بودن به منظور اطمینان از دسترسی اطلاعات در هر زمان است، و از دست دادن در دسترسی مربوط به عدم امکان دسترسی به اطلاعات یا استفاده از اطلاعات یا یک سیستم اطلاعاتی است.

۳,۱.امنیت سایبری در برق

در فناوری های شبکه های هوشمند انتظار میرود، اجزای جدیدی را در شبکه برق معرفی کنند که بسیاری از آنها میتوانند کلید هماهنگی و قابلیت اطمینان، ارتباط دوطرفه و محرمانگی، یکپارچگی و قابلیت دسترسی به سیستم های قدرت را نمایش می دهند.

امنیت سایبری برای شبکه های هوشمند باید از قابلیت اطمینان شبکه برق و محرمانه بودن (و حفظ حریم خصوصی) اطلاعات منتقل شده را پشتیبانی کند. با شناختن اینکه امنیت ملی و اقتصادی کشور به قابلیت های قابل اطمینان بودن زیرساخت های حیاتی بستگی دارد، لازم است که یک رویکرد ساختاری سایبری برای کمک به صاحبان و اپراتورهای این زیرساخت ها برای مدیریت خطرات مربوط به امنیت سایبری را داشته باشد و در عین حال برای محافظت از محرمانه بودن تجارت، حفظ حریم شخصی و آزادی های مدنی در نظر گرفته شود[۵،۶]. به طور سنتی امنیت سایبری برای فناوری اطلاعات بر حفاظت مورد نیاز برای اطمینان از محرمانه بودن، یکپارچگی و دسترسی به سیستم های گزارش الکترونیکی تمرکز دارد. هنگامی که در خصوص شبکه های هوشمند صحبت می شود، نیاز به امنیت

ISSN: 2745-3673
http://www.Rcsj.ir

سایبری نیز در سیستم ارتباطی فناوری اطلاعات، همراه با سیستم قدرت و دامنه هایی که قبلا ذکر شد، برای حفظ قابلیت اطمینان شبکه هوشمند و حفظ حریم خصوصی اطلاعات مصرف کننده، در نظر گرفته شود.

بنابراین، امنیت سایبری در شبکه های هوشمند باید شامل تعادل بین سیستم های سایبرنتیک و پروسه های فناوری اطلاعات و عملیات و حاکمیت سیستم برق باشد. علاوه بر این، ایمنی و قابلیت اطمینان در سیستم های قدرت مهم هستند. با این حال، تمام اقدامات امنیتی سایبری در این سیستم ها نباید مانع از کارکرد صحیح سیستم قدرت شوند.

این سناریو جدید حالت متفاوت حمله سایبری، به اصطلاح "حملات ترکیبی" را ارائه می دهد که در مقایسه با یک حمله فیزیکی فردی تاثیرات و یا عواقب مختلفی را نشان می دهد. به این ترتیب ضروری است که امنیت سایبری یک شبکه هوشمند اساسی و پایه ای باشد [۵،۶].

در این زمینه، در دسترس بودن (اولین ستون امنیت سایبری) به شبکه های هوشمند به عنوان یک ضرورت مورد نیاز است:

≤ ۴ میلی ثانیه برای حفاظت رله؛

ده ثانیه برای نظارت بر منطقه گسترده؛

ثانیه هایی برای ایستگاه های پست و داده های فیدر SCADA

دقایقی برای نظارت بر تجهیزات غیر بحرانی و برخی اطلاعات مربوط به قیمت های بازار

برای خواندن وسایل اندازه گیری براساس ساعت / روز و اطلاعات قیمت بلند مدت در بازار

جمع آوری داده ها از قبیل اطلاعات کیفیت انرژی در طولانی مدت روز / هفته / ماه.

یکپارچگی (ستون دوم امنیت سایبری) برای عملیات سیستم های قدرت باید اطمینان حاصل شود که:

داده ها بدون مجوز تغییر نیابند.

منبع داده معتبر است؛

تمبر زمانی مرتبط با داده ها شناخته شده و تأیید شده است.

کیفیت داده ها شناخته شده و تأیید شده است.

سرانجام، محرمانه بودن (سومین ستون امنیت سایبری) که در شبکه های هوشمند اعمال می شود، باید اطمینان حاصل شود:

حریم خصوصی اطلاعات مشتری؛

اطلاعات در بازار برق؛

اطلاعات کلی شرکتی، مانند حقوق و دستمزد، برنامه ریزی استراتژیک داخلی و غیره

۴.روش شناسی سطوح بالاتری از امنیت سایبری در شبکه های هوشمند

از آنجاییکه سیستم قدرت الکتریکی مطابق با یک سیستم زیربنایی حیاتی است، امنیت سایبری اعمال شده به این سیستم باید از ویژگی های زیر باشد:

- عملیات سیستم برق باید در طول هر حمله یا مصالحه در مورد ایمنی (تا آنجا که ممکن است) ادامه یابد.
- عملیات بازیابی سیستم قدرت باید پس از یک حمله امنیتی یا سازش با یک سیستم اطلاعاتی سریع شود.
- آزمایشات اقدامات ایمنی را نمی توان مجاز دانست در صورتی که بر عملکرد سیستم برق تأثیر بگذارد.

در این مقاله، تجزیه و تحلیل برخی از الزامات را برای شناسایی سطح امنیت سایبری در یک شبکه هوشمند ارائه می دهد. این الزامات می تواند به ۱۶ گروه تقسیم شود:

- Access Control- کنترل دسترسی
- Awareness & Training - آگاهی و آموزش
- Auditing and Accountability - حسابرسی و حسابرسی
- Security Assessment and AuthorizationA - ارزیابی امنیتی و مجوز
- Configuration Management - مدیریت پیکربندی
- Continuity of Operations- تداوم عملیات
- Identification and Authentication- شناسایی و تأیید اعتبار
- Information and Document Management- اطلاعات و مدیریت اسناد
- Incident Response- پاسخ حادثه

ISSN: 2745-3673
http://www.Rcsj.ir

- Physical Security- امنیت فیزیکی
- Planning- برنامه ریزی
- Personal Security- امنیت شخصی
- Risk Management and Evaluation- مدیریت ریسک و ارزیابی
- Acquisition of Services- خرید خدمات
- Communication Protection- حفاظت از ارتباطات
- Integrity of Information - یکپارچگی اطلاعات

روش شناسایی سطح بلوغ امنیت سایبری در شبکه های هوشمند، ابتدا شناسایی مورد استفاده است. پس از آن مرحله شناسایی دارایی ها، تهدیدها و تأثیرات وجود دارد و در نهایت در مرحله آخر تجزیه و تحلیل انجام شده است تا انطباق و استفاده از الزامات امنیتی که در بالا شرح داده شده است، مشخص گردد. همانطور که در شکل ۳ نشان داده شده است.

مهم است که تأکید داشته باشیم که در مرحله تجزیه و تحلیل، سطح که هر مورد کاربرد که اجرا می شود، باید مورد ارزیابی و مستند سازی قرار گیرد، هر نیازمندی به عنوان سطح ۱، سطح ۲، سطح ۳ یا سطح ۴ طبقه بندی می شود. مهم است که تأکید کنیم که هرچه سطح بلوغ سیستم / گروه / نیازمندیها بالاتر باشد، در نظر گرفته می شود. به عنوان مثال، گروه "Access Control -AC" به ۱۴ زیرگروه (از AC-1 تا AC-14) تقسیم می شود، با توجه به میزان بلوغ (۱ تا ۴) برای هر یک از الزامات هر زیر گروه ها تجزیه و تحلیل انجام می شود. استفاده از این روش بهتر است در مورد "نتایج" نشان داده شود.

بنابراین، ممکن است سطح بلوغ هر مجموعه ای از الزامات (۱۶ در مجموع)، سطح بلوغ عمومی مورد کاربرد و در نتیجه، سطح بلوغ امنیت سایبری سیستم های مرتبط با شبکه های هوشمند، شناسایی شود، و بهبود یابد.

۵. نتایج

به منظور اعتبارسنجی روش پیشنهادی، با انتخاب یک مورد کاربرد مربوط به یک سیستم شبکه هوشمند، که از مدیریت از راه دور بازخوردهای یک توزیع برق بزرگ را پشتیبانی می کند، بررسی می کنیم. در این سناریو، سیستم اسکادای کنونی که بصورت داخلی (درون توزیع کننده) توسعه یافته است، با سیستم اسکادای تولید بازار مقایسه می شود.

۵،۱. مرحله ارزیابی دارایی ها، تهدیدات و تأثیرات

برای تجزیه و تحلیل، دارایی های زیر شناسایی شد: سنسورها و سیستم های کنترل الکتریکی شبکه (از راه دور)؛ شبکه ارتباطی بین راه دور و مرکز داده؛ سیستم های متمرکز پردازش (SCADA)؛ مرکز عملیات، اپراتورها و ایستگاه های عملیاتی.

تهدیدهای احتمالی زیر نیز شناسایی شدند: انکار سرویس حمله؛ تخریب فیزیکی تجهیزات، که می تواند از طریق مهندسی اجتماعی آغاز شود؛ تروجان، یا تهدیدات پایدار (APT).

در نهایت، اثرات احتمالی شناسایی شده برای مورد در تجزیه و تحلیل عبارت بودند از: وقفه در تامین انرژی؛ زیان های مالی با جبران خسارت به مصرف کنندگان برق، کارکنان با قدرت غیر مجاز.

۵،۲.تحلیل

مرحله تجزیه و تحلیل برای ۱۶ گروه تعریف شده در روش شناسی ارائه شده در بند چهارم انجام شد. در این کار، به دلایل محدودیت فضا، تنها نتایج مربوط به گروه کنترل دسترسی - CA و "گروه آگاهی و آموزش - CT" ارائه می شود. برای این گروه ها، تجزیه و تحلیل تطبیقی سیستم SCADA که توسط شرکت توزیع انرژی (به نام "سیستم جدید") ایجاد شده است و یک سیستم SCADA تجاری (که به نام "سیستم اختصاصی" نامیده می شود) ارائه می شود. نتایج به دست آمده با استفاده از روش پیشنهادی شرح داده شده به شرح زیر است. نتایج به دست آمده برای گروه کنترل دسترسی – CA

ISSN: 2745-3673
http://www.Rcsj.ir

تمرکز کنترل دسترسی این است که اطمینان حاصل شود که منابع تنها توسط منابع مناسب دسترسی پیدا می کنند و منابع به درستی شناسایی می شوند و برای تجزیه و تحلیل مکانیزم های مورد نیاز برای نظارت بر فعالیت های دسترسی برای فعالیتهای نامناسب شناسایی شود. در این گروه، تمام الزامات متعلق به ۱۴ زیرگروه (-۱CA تا -۱۴CA) به شرح زیر مورد تجزیه و تحلیل قرار گرفتند

۵,۲,۱- خط مشی و روش کنترل دسترسی:

• سازمان باید به طور مرتب توسعه، گسترش، اصلاح و به روزرسانی سیاست ها و رویه های کنترل دسترسی داشته باشد.

• مدیریت، تطابق با سیاست امنیتی سازمان و سایر الزامات تنظیم را تضمین می کند.

• اطمینان حاصل کنید که خط مشی و روش های کنترل امنیت دسترسی مطابق با قوانین و مقررات فدرال، ایالتی، قبیله ای و منطقه ای است.

۵,۲,۲ CA- ۲ - سیاست و روش دسترسی از راه دور:

• سند باید روش های دسترسی از راه دور به سیستم های اطلاعات هوشمند شبکه را تعریف کند.

• ایجاد محدودیت استفاده و ایجاد یک راهنمای برای هر دسترسی مجاز؛

• ضرورت نیازهایی را برای ارتباطات راه دور به سیستم های اطلاعاتی

• آزادسازی دسترسی به سیستم را قبل از اتصالات.

۵,۲,۳ CA- ۳ - مدیریت حساب:

• تأیید، ایجاد، فعال کردن، اصلاح، غیرفعال کردن و حذف حسابها؛

• تعریف انواع حسابها، حقوق دسترسی و امتیازات؛

• بررسی حساب ها و امتیازات؛

• مدیریت حساب هر زمانی که مشارکت کننده اخراج، انتقال و یا وظایف خود را تغییر داده است؛

قبل از هر فعالیت، یک جریان تصویب داشته باشید.

۵,۲,۴ CA- ۴ - اجرای دسترسی:

• پیکربندی سیستم ها برای اجرای انطباق با قوانین تعیین شده در سیاست کنترل دسترسی.

۵,۲,۵ CA- ۵ - سلب مسئولیت:

• ایجاد و ثبت اسناد تقسیم مسئولیت ها و تفکیک توابع لازم برای از بین بردن اختلافات منافع و اطمینان از استقلال در مسئولیت ها و عملکرد افراد؛

• جداسازی توابع از سیستم اطلاعاتی شبکه هوشمند از طریق تقویت مجوزهای دسترسی اختصاص یافته

• محدود کردن توابع امنیتی به کوچکترین تعداد کاربران مورد نیاز برای اطمینان از امنیت سیستم اطلاعات شبکه هوشمند.

۵,۲,۶ – حقوق دسترسی کمتر:

• تنظیم مجموعه محدودی از حقوق و امتیازات و یا دسترسی های مورد نیاز کاربران برای انجام وظایف خاص؛

• پیکربندی سیستم اطلاعات شبکه هوشمند برای اعمال مجموعه ی محدودیت هایی از حقوق و امتیازات و یا دسترسی کاربران.

۵,۲,۷ CA- ۷ - تلاش های ورودی:

• سیستم اطلاعات شبکه هوشمند محدودیتی را برای تعداد تلاش های ورود نامعتبر متوالی توسط کاربر در طی یک دوره زمانی تعیین شده توسط سازمان اعمال کند.

• سیستم باید بعد از دسترسی نامعتبر سیستم را بلوکه کند.

۵,۲,۸ CA- ۸ - کنترل همزمان جلسه:

• حداکثر تعداد جلسات همزمان، باید توسط نوع حساب، یا با ترکیب این دو، باید تعریف و کنترل شود. محدوده این الزام برای کاربرانی که در صدد دسترسی به سیستم هستند می باشد، این امر برای دسترسی دستگاه های هوشمند شبکه برق اعمال نمی شود.

۵,۲,۹ CA- ۹ - قفل جلسه:

• برای جلوگیری از دسترسی ناخواسته، زمان لازم برای مسدود کردن خودکار جلسات پس از یک دوره عدم فعالیت تعیین می شود؛

• هنگام بازگشت به جلسه، کاربران باید از توصیف های لازم استفاده کنند؛

۵,۲,۱۰ CA- ۱۰ - دسترسی از راه دور:

• سازمان باید دسترسی از راه دور را تأیید و از رمزگذاری برای اطمینان از محرمانه بودن اطلاعات و یکپارچگی در جلسات از راه دور استفاده کند؛

ISSN: 2745-3673
http://www.Rcsj.ir

• سیستم اطلاعاتی شبکه هوشمند باید از دسترسی بی سیم با استفاده از احراز هویت و رمزگذاری محافظت کند.

توجه: کاربر، دستگاه یا هر دو احراز هویت به صورت مورد نیاز اعمال می شود.

• سازمان باید ارتباطات راه دور غیر مجاز را به سیستم اطلاعاتی شبکه هوشمند، از جمله دسترسی غیرمجاز به نقاط دسترسی بی سیم در فرکانس تعریف شده توسط سازمان، نظارت کند، و در صورتی که یک اتصال غیر مجاز کشف شود، اقدامات مناسب انجام می شود.

CA-۵,۲,۱۱ ۱۱ - محدودیت دسترسی به شبکه بی سیم:

• استفاده از محدودیت ها و راهنمایی های راه اندازی برای فن آوری های بی سیم؛

• مجوز، نظارت و مدیریت دسترسی بی سیم به سیستم اطلاعاتی هوشمندانه

CA-۵,۲,۱۲ ۱۲ - کنترل دسترسی برای دستگاه های تلفن همراه:

• محدودیت های استفاده و راهنماهای کاربر برای استفاده از دستگاه های تلفن همراه می باید تحت کنترل سازمان را ایجاد کرد و از آنجمله استفاده از رسانه های قابل جابجایی و رسانه های قابل جابجایی مالک شخصی؛

• مجوز اتصال دستگاه های تلفن همراه به سیستم های هوشمند شبکه های اطلاعاتی؛

• نظارت بر اتصالات غیر مجاز دستگاه های تلفن همراه به سیستم های اطلاعات شبکه هوشمند

• الزامات لازم برای اتصال دستگاه های تلفن همراه به سیستم های اطلاعاتی شبکه های هوشمند.

CA-۵,۲,۱۳ ۱۳ - استفاده از سیستم های اطلاعاتی خارجی:

• ایجاد سیاست ها و تعریف استانداردهای استفاده از اطلاعات خارجی و اتصال به سیستم های اطلاعاتی خارجی؛ و

• فرآیندهای ذخیره سازی و انتقال اطلاعات سازمان را با استفاده از سیستم اطلاعاتی خارجی تعریف کنید.

CA-۵,۲,۱۴ ۱۴ - کلمات عبور:

• توسعه و تقویت سیاست ها و رویه ها برای کاربران سیستم شبکه ای هوشمند از نظر تولید و استفاده از کلمه عبور؛

• قوانین پیچیده را براساس سطح بحرانی سیستم شبکه ای هوشمند که فرد باید دسترسی پیدا کند، ایجاد کنید. و

• نیاز به تغییر رمز عبور به طور منظم و پس از مدت زمان طولانی و فعال شدن آن.

در شکل های ۴ و ۵، می توان توزیع سطوح بلوغ الزامات گروه کنترل دسترسی (برای سیستم "مالک" و "سیستم جدید") را از سطح ۱ - ۱N تا سطح ۴ سازماندهی شده است - ۴N در این سناریو، سیستم های دارای صلاحیت های خود را به شرح زیر طبقه بندی شدند:

• سیستم اختصاصی: ۲۱٪ در سطح ۱، ۴۳٪ در سطح ۲،۲۹٪ در سطح ۳ و ۷٪ در سطح ۴

• سیستم جدید: ۰٪ در سطح ۱، ۱۴٪ در سطح ۲، ۰٪ ۳nonvel و ۸۶٪ در سطح۴

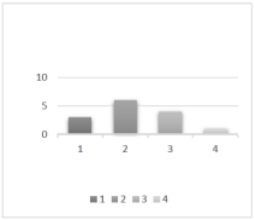
نتایج به دست آمده برای گروه "آگاهی الکترونیکی - CT"

هدف این گروه از الزامات این است که یکپارچه سازی نیازها را تضمین کند که شرکت دارای سیاست ها، فرآیندها و ابزارهایی برای انتشار بهترین شیوه های امنیت سایبری برای افزایش آگاهی طرفین به طور مستقیم و غیر مستقیم با سیستم های شبکه هوشمند است. در این گروه، تمام وسایل متعلق به ۴ زیرگروه (-۱CT تا -۴CT) به شرح زیر مورد تجزیه و تحلیل قرار گرفتند.

-۱CT - سیاست ها و روش های آگاهی و آموزش:

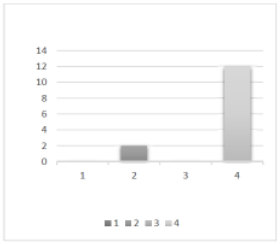
• توسعه، پیاده سازی، تجدید نظر و به روز رسانی دوره ای که توسط سازمان تعریف شده و آموزش اطلاعاتی که مورد نیاز است.

• رویه هایی برای اجرای سیاست های امنیتی



شکل ۴: بلوغ گروه کنترل دسترسی سیستم مالک.

ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۵: بلوغ کنترل دسترسی سیستم جدید

-۲CT - آگاهی از امنیت اطلاعات:

• تمامی رویه های طراحی و تغییرات سیستم اطلاعاتی شبکه هوشمند باید توسط سازمان بررسی شود تا بتوان آن را در آگاهی از آموزش سازمان ها مورد توجه قرار داد. و

• این سازمان شامل تمرینات عملی برای افزایش ایمنی برای شبیه سازی حملات سایبرنتیک است.

-۳CT - آموزش امنیت اطلاعات:

• پیش از ایجاد دسترسی به سیستم اطلاعاتی شبکه هوشمند یا انجام وظایف اختصاصی، آموزش امنیت را انجام دهید.

• هر زمان که نیاز به تغییر در سیستم اطلاعات شبکه هوشمند باشد، انجام دهید.

• در یک تناوب تعریف شده ابعادی از سازمان را تعریف کنید.

-۴CT - تماس با انجمن ها و گروه های امنیتی

• مهم است که این سازمان ارتباط با انجمن ها و گروه های امنیت اطلاعات را با آخرین توصیه ها، شیوه ها، تکنیک ها و فن آوری های امنیتی اطلاعات را برقرار کند و اشتراک گذاری اطلاعات در مورد تهدیدات، آسیب پذیری ها و حوادث به روز نگه دارد. ۶ و ۷ می توان توزیع سطوح بلوغ الزامات جزء گروه "آگاهی و آموزش" (برای "سیستم صاحبکار" و "سیستم جدید") را از سطح ۱N-۱ تا سطح N4 را مشاهده کرد.

در این سناریو، سیستم مورد نیاز خود را به شرح زیر طبقه بندی کرد:

سیستم اختصاصی: ۱۰۰٪ در سطح ۱

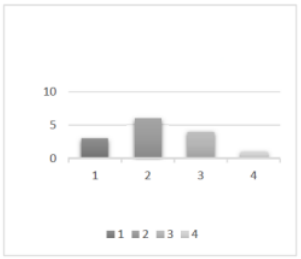
• سیستم جدید: ۰٪ در سطح ۱، ۸٪ در سطح ۲، ۱۵٪ در سطح ۳ و ۷۷٪ در سطح

شکل ۶. بلوغ گروه "آگاهی و آموزش" از سیستم اختصاصی.

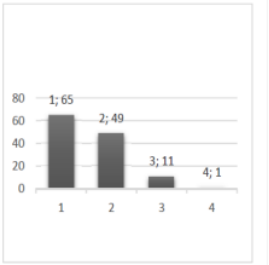
نتایج به دست آمده برای تثبیت مورد استفاده

روش پیشنهادی برای هر یک از ۱۶ گروه ذکر شده در بالا اعمال می شود، تا امکان تلفیق سطح بلوغ مورد نظر (سیستم SCADA) را فراهم می کند. در شکل های ۸ و ۹، ممکن است توزیع سطوح بلوغ الزامات یکپارچه (با توجه به ۱۶ گروه) برای تجزیه و تحلیل (به ترتیب سیستم های اختصاصی و "N (NovoSystem۱" به سطح ۴ - ۴N تجسم است. در این ارقام امکان شناسایی آن در مورد استفاده از سیستم اختصاصی وجود دارد، ۵۱٪ از الزامات به عنوان سطح ۱، ۳۹٪ سطح ۲، ۹٪ سطح ۳ و ۱٪ سطح ۴ طبقه بندی شده اند. برای، در سیستم جدید، ۱٪ از الزامات سطح ۱، ۲۴٪ سطح ۲، ۲۸٪ سطح ۳ و ۴۷٪ سطح ۴ است. واضح است که سیستم جدید و فرایندهای آن پشتیبانی از سطح بالاتری نسبت به سیستم قبلی برخوردار هستند

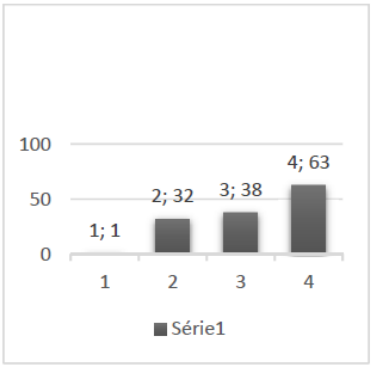
ISSN: 2745-3673
http://www.Rcsj.ir



شکل ۷. سطح بلوغ آگاهی و آموزش سیستم جدید.



شکل ۸. سطح بلوغ سیستم اختصاصی.



شکل ۹. سطح بلوغ سیستم جدید.

برای اختصاص یک سطح بلوغ به هر یک از سیستم ها (مالک سیستم و سیستم جدید)، می توان در نظر گرفت که هر دو سیستم دارای الزامات در سطح ۱ هستند، هر دو آنها با سطح بلوغ ۱ طبقه بندی می شوند. با این حال، تجزیه و تحلیل شکل ۸ و ۹ اجازه می دهد تا به طور واضح وضعیت واقعی هر یک از این سیستم ها را تشخیص دهد.

شکل ۹ نشان می دهد که با سرمایه گذاری تنها بر روی یک نیاز، می توان این سطح رتبه ۱ را برای سیستم جدید از رفع نمود و آن را با شرایط جدیدی که با سطح عمیق تر آن انجام خواهد شد. از سوی دیگر، تجزیه و تحلیل شکل ۸ نشان می دهد که برای سیستم مالک برای افزایش سطح بلوغ، لازم است که در ۶۵ مورد طبقه بندی شده با سطح بلوغ ۱ سرمایه گذاری شود.

ISSN: 2745-3673
http://www.Rcsj.ir

نتیجه گیری

پیاده سازی یک مدل شناسایی سطح بلوغ امنیت اطلاعات در شبکه های هوشمند بسیار ضروری است، زیرا بخش با پذیرش فناوری اطلاعات و ارتباطات الکترونیکی در بهره برداری از بخش برق است. در این زمینه، این مقاله روش شناسی برای ارزیابی سطح بلوغ امنیت سایبری در شبکه های هوشمند را بر اساس طبقه بندی ۱۶ گروه مورد نیاز ارائه کرد. روش پیشنهادی برای سیستم شبکه ای (SCADA) شرکت توزیع برق مورد استفاده قرار خواهد گرفت.

از نتایج به دست آمده امکان شناسایی کارایی روش پیشنهادی و همچنین انعطاف پذیری کاربرد در موارد استفاده چندگانه وجود دارد، که نشان می دهد که الزاماتی که دارای پایین ترین سطح بلوغ هستند، باید سطح بلوغ کل استفاده را تعیین کنند.

در نهایت مهم است، تأکید کنیم که پیشنهاد این کار نیز می تواند به راحتی به سایر سیستم های هوشمند منتقل شود و همچنین امکان اضافه کردن گروه های جدیدی از الزامات را فراهم می کند که ممکن است در آینده مورد توجه قرار گیرند

ISSN: 2745-3673
http://www.Rcsj.ir

منابع و مراجع

[1] Evans, D, The Internet of Things. How the Next Evolution of the Internet Is Changing Everything, 2011
[2] National Institute of Standards and Technology - NISTr 7628 revision 1-Guidelines for smart grid cybersecurity – volume 1,2 and 3 - 2014;
[3] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sen- sor networks in the context of the internet of things, Comput. Electr. Eng. 37 (2) (2011) 147–159 . Modern Trends in Applied Security: Architectures, Imple- mentations and Applications, doi: 10.1016/j.compeleceng.2011.01.009 .
[4] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for internet of things, J. Netw. Comput. Appl. 42 (2014) 120–134, doi: 10.1016/j.jnca.2014.01. 014 .
[5] K.T. Nguyen, M. Laurent, N. Oualha, Survey on secure communication pro- tocols for the internet of things, Ad Hoc Netw. 32 (2015) 17–31 . Inter- net of Things security and privacy: design methods and optimization, doi: 10.1016/j.adhoc.2015.01.006 .
[6] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279 . Towards a Science of Cyber SecuritySecurity and Identity Architecture for the Future Internet, doi: 10.1016/j.comnet.2012.12.018 .