ملاحظات پدافند غیرعامل مرکز کنترل ترافیک راه‌آهن ج.ا.ایران در برابر حملات سایبری
(مطالعه موردی: مرکز کنترل ترافیک یزد)

بهروز ابراهیمی[1]

تاریخ دریافت: ۱۳۹۵/۱۰/۰۵ تاریخ پذیرش: ۱۳۹۵/۱۲/۰۸

چکیده

پژوهش حاضر باهدف تعیین ملاحظات پدافند غیرعامل مرکز کنترل ترافیک شرکت راه‌آهن ج.ا.ایران در برابر حملات سایبری که شامل تعیین حملات سایبری مؤثر، تعیین آسیب‌پذیری‌های مؤثر و تعیین راهکارهای پدافندی مقابله با حملات سایبری مرکز کنترل ترافیک راه‌آهن ج.ا.ایران صورت گرفته و این پژوهش از نوع کاربردی است و با استفاده از روش پژوهش توصیفی تحلیلی انجام شده است. روش‌ها و ابزار گردآوری اطلاعات در این پژوهش پرسشنامه، مصاحبه، مشاهده و استفاده از فضای سایبری (اینترنت و اینترانت) بوده است. جامعهٔ آماری این پژوهش را صاحب‌نظران، مدیران و کارشناسان آگاه و متخصص در زمینهٔ پدافند غیرعامل، فناوری اطلاعات و راه‌آهن ج.ا.ایران تشکیل داده‌اند. یافته‌های پژوهش نشان می‌دهد که مهم‌ترین ملاحظات پدافند غیرعامل مرکز کنترل ترافیک راه‌آهن در برابر حملات سایبری در سه بخش زیر عبارت‌انداز: مهم‌ترین حملات: محرومیت از خدمات[2]، تغییر محتوای پیام و موارد دیگراست. مهم‌ترین آسیب‌پذیری‌ها: وجود کارمندان ناراضی، عدم کنترل دقیق ورود و خروج افراد به اتاق سرور و مرکز کنترل ترافیک، کمبود نیروی انسانی متخصص جهت تعمیر و نگهداری تجهیزات و موارد دیگر است. مهم‌ترین راهکارها: پشتیبان‌گیری مداوم از داده‌های حیاتی و حساس، مستندسازی و ارائهٔ گزارش تهاجم‌های تشخیص داده‌شده قبلی به تیم امنیت، مرور گزارش‌های روزانهٔ مربوط به تجهیزات و موارد دیگر است.

واژگان کلیدی: *مرکز کنترل، حملات سایبری، امنیت، ملاحظات پدافند غیرعامل، راه‌آهن*

---

۱. کارشناس ارشد پدافند غیرعامل گرایش امنیت دانشکده فارابی (behrouz_lame@yahoo.com)

2.Denial Of Service

بیان مسئله

هرچه زمان پیش می‌رود از یک‌سو وابستگی ما به سامانه‌های فناوری اطلاعات بیشتر و از سوی دیگر تهدیدهای ما در این سامانه‌ها جدی‌تر می‌شود. به‌طور مثال درگذشته کلیهٔ امور بانکی از طریق مراجعه‌های حضوری پیگیری می‌شدند و به همین خاطر عمدهٔ خطراتی که ما را تهدید می‌کرد دزدی و عوامل فیزیکی بود. ولی در حال حاضر شما می‌توانید کلیهٔ قبوض آب، برق، گاز، تلفن و موارد دیگر را توسط اینترنت پرداخت نمایید و همچنین بسیاری از خریدهای خود را نیز از اینترنت و فضای فناوری اطلاعات به سرعت و با کمترین زمان و هزینه انجام دهید. با توجه به این تغییرات، خطرات گذشته شکل خود را تغییر داده و به این حوزه مهاجرت نموده‌اند. مفهوم امنیت در زمینهٔ فناوری اطلاعات، مواردی چون حفاظت داده‌ها در مقابل حوادث، خرابکاری‌ها، تغییرات و یا افشاء اطلاعات را شامل می‌شود. با استفاده روزافزون از رایانه‌های شخصی و توزیع توانایی پردازش اطلاعات بین سطوح مختلف کارکنان مسئولیت امنیت نیز بین کارکنان، مسئولین و مدیران توزیع‌شده است ازاین‌رو هیچ مدیری نمی‌تواند با خیالی آسوده تصور نماید که فرد دیگری این مسئولیت را دارا می‌باشد. متخصصین این امر با توجه به سطح دانش و آگاهی بالایی که در این زمینه‌دارند می‌بایست برنامه‌ریزی مطلوبی را جهت حفاظت داده‌ها و اطلاعات، متناسب با ماهیت داده‌های سازمان خود ارائه دهند. با توجه به رشد روزافزون اطلاعات و ارتباطات و توسعه سیستم‌های رایانه‌ای نیاز به تأمین امنیت داده‌ها بیش‌ازپیش به نظر می‌رسد ازاین‌رو برای رسیدن به یک حد مطلوب امنیت، لازم است که بر اساس یک‌روال مشخص و این امر را پیگیری نمود.

سازمان‌ها دائماً خطراتی که اطلاعات و سیستم‌های اطلاعاتی را تهدید می‌کنند، مانند حملات عدم پذیرش سرویس و ویروس رایانه‌ای را مورد بازبینی و بررسی قرار می‌دهند. با توجه به افزایش محصولات امنیتی در بازار، می‌بایست شخص یا اشخاصی بادانش کافی مسئول بررسی این محصولات در سازمان‌ها باشند. این‌که هیچ‌چیزی به‌عنوان امنیت کامل و تمام‌عیار وجود ندارد، کاملاً پذیرفته‌شده است. محصولات امنیتی می‌توانند بخشی از امنیت را تأمین نمایند، اما آنچه مهم است، واکنش سریع حفاظتی و اصلاح آسیب‌پذیری‌ها است. به دلیل افزایش اتصالات زیرساخت‌های اطلاعاتی (مخابرات، بانکداری و مالی، انتقال و توزیع، انرژی، سرویس‌های اطلاعاتی و...) حدومرز سیستم‌ها به‌سرعت ناپدید می‌شوند. سازمان‌ها می‌بایست برای ارزیابی کارایی و در دسترس بودن سیستم خود، به‌مرور روش‌های امنیتی موجود را موردبررسی و بازنگری قرار دهند.

راه‌آهن به‌واقع یکی از مهم‌ترین ملزومات حمل‌ونقل در هر کشور است که می‌تواند اقتصادی‌ترین نتیجه را با توجه به‌سرعت، توان حمل بالا و مصرف اندک انرژی به بار آورد. ارسال به‌موقع مواد اولیه به مراکز تولید، حمل سریع، ایمن و مطمئن محصولات به بازارهای مصرف و مرزهای صادراتی، چرخ‌های عظیم صنعت را به حرکت درآورده و کشور را در جهت تحقق اهداف توسعه اقتصادی یاری می‌دهد. راه‌آهن با داشتن شاخصه‌هایی مانند ایمنی ترافیک، حجم بارگیری زیاد، امکان ایجاد ارتباط میان اغلب نقاط داخل کشور و مرزهای بین‌المللی، به‌عنوان حمل‌ونقل سبز از اهمیت زیادی در میان سایر بخش‌های حمل‌ونقل برخوردار است. در این شرایط سیروحرکت قطارها به‌صورت منظم و در زمان‌بندی دقیق اهمیت بسیاری دارد زیرا بروز حادثه در یک محور برای هر یک از قطارها معمولاً باعث بسته شدن کل آن مسیر تا رفع کامل حادثه خواهد شد و عملاً بهره‌برداری از محور مذکور به‌طورکلی مختل و متوقف می‌شود. مرکز کنترل ترافیک محوری شرکت راه‌آهن ج.ا.ایران که در حال حاضر از چهار محور تشکیل‌شده است (محور یزد، محور شاهرود، محور طبس، محور سیرجان) و تحت نظارت کنترل مرکزی تهران قرار دارند، به‌عنوان هماهنگ‌کننده حمل‌ونقل و سیر قطارها در هر محور، ترسیم نمودار و گراف حرکت کلیهٔ قطارهای عبوری و... با استفاده از رایانه‌ها، نمایشگرهای بزرگ، ابزارهای الکترونیکی، مخابراتی و شبکه و... به‌عنوان مغز فعال سیر و حرکت قطارها انجام‌وظیفه می‌نماید و وجود هرگونه اشکال و ایراد در ابزارهای مورداستفاده در این مرکز و یا ارسال اطلاعات نادرست از این مرکز به اینترلاکینگ‌ها و تجهیزات دیگر تحت پوشش باعث بروز سانحه و ازهم‌گسیختگی حمل‌ونقل ریلی و کاهش بهره‌وری شرکت راه‌آهن ج.ا.ایران خواهد گردید. با توجه به سند چشم‌انداز ۱۴۰۴ شرکت راه‌آهن ج.ا.ایران و همچنین پیشرفت فناوری در سال‌های اخیر و استفاده از فن‌آوری‌های نوین[1] مانند رایانه‌ها، خطوط ارتباطی، انواع شبکه انتقال داده (باسیم و بی‌سیم) در شرکت راه‌آهن ج.ا.ایران و مرکز کنترل ترافیک، این مرکز نیز مانند سایر مراکز مهم در معرض حملات سایبری دشمن و خرابکاران سایبری قرار دارد و عدم اقدام در خصوص رفع آسیب‌پذیری‌های سایبری و همچنین عدم وجود راهکارهای مقابله با این حملات سایبری در مرکز مذکور می‌تواند لطمه‌های سنگینی به عملکرد این مرکز و درنتیجه کل سیستم حمل‌ونقل کشور وارد سازد. با توجه به رسالت مهم مرکز کنترل ترافیک، رعایت اصول پدافند غیرعامل سایبری که حاصل آن در یک دید کلی امنیت ارتباطات و اطلاعات ردوبدل شده است را به دنبال می‌کند.

1.Information and Commiunication Technology

پدافند غیرعامل در فضای سایبری از یک‌سو توان دفاعی و تحمل‌پذیری مجموعه را در زمان حملات سایبری افزایش داده و از سوی دیگر پیامدهای بحران ناشی از حملات سایبری را کاهش و امکان بازسازی نقاط آسیب‌دیده را با کمترین هزینه فراهم می‌سازد. طرح‌های پدافند غیرعامل معمولاً قبل از انجام مراحل تهاجم و در زمان صلح تهیه و اجرا می‌گردند. با توجه به فرصتی که در زمان صلح جهت تهیهٔ چنین طرح‌هایی فراهم می‌گردد ضروری است این قبیل تمهیدات در متن طراحی‌ها لحاظ گردند. هدف از حملهٔ سایبری در سطح ملی، دست‌یابی به اطلاعات سایر کشورها و سازمان‌ها، ایجاد وقفه در تجارت یا ارائهٔ خدمات و یا ایجاد خدشه در زیرساخت‌هایی مانند آب، برق، حمل‌ونقل و... به‌نحوی‌که هزینه‌های اقتصادی را برای کشور یا سازمان هدف افزایش دهد و موجب نارضایتی عمومی میان مردم گردد، می‌باشد؛ بنابراین می‌توان گفت: مسئلهٔ اصلی در این پژوهش " فقدان ملاحظات پدافند غیرعامل مرکز کنترل ترافیک راه‌آهن در برابر حملات سایبری است".

اهمیت و ضرورت پژوهش

با توجه به اهمیت فناوری اطلاعات در عصر حاضر و رشد سریع آن، این بستر به یکی از نقاط بالقوه آسیب‌پذیر و خطرناک در فضای سایبری تبدیل‌شده است که ضرورت توجه و پرداخت سریع و درعین‌حال نظام‌مند، معقول و هدفمند به‌منظور مصون‌سازی این بستر از تهدیدات موجود در جهت حفظ امنیت و ایمنی مرکز کنترل ترافیک و درنتیجه سیر و حرکت قطارها را اجتناب‌ناپذیر می‌نماید.

مراکز تحت پوشش پدافند غیرعامل می‌بایست جزء یکی از دسته‌بندی‌های حیاتی، حساس و مهم قرار داشته باشند تا تمهیدات و ملاحظات درخور و متناسب با آن دسته‌بندی موردنظر قرارگرفته، تهیه و اعمال گردد. در تئوری واردن که به حلقه‌های راهبردی واردن مشهور است، مراکز اصلی یک کشور به پنج حلقه متحدالمرکز تقسیم‌شده است، این حلقه‌ها همانند اعضای حیاتی بدن انسان هستند و آسیب‌پذیری هرکدام موجب فلج شدن سیستم حیاتی کشور خواهد شد. این حلقه‌ها عبارت‌اند از: رهبری، محصولات کلیدی، سیستم حمل‌ونقل، ارادهٔ ملی، نیروهای عملیاتی. همان‌گونه که ذکر شد، حمل‌ونقل حلقه سوم از این پنج حلقه است و برای بدنه کشور به‌مثابه دست‌وپا می‌باشد؛ ازاین‌رو باید از پیاده‌سازی و اجرای اصول پدافند غیرعامل در پروژه‌های حمل‌ونقلی و به‌ویژه ریلی کشور حمایت به عمل آید تا شریان‌های اقتصادی و سیاسی کشور همواره و در هر شرایطی پایدار مانده و یا کمترین آسیب‌پذیری را در برابر هجوم دشمنان داشته باشد. مرکز کنترل ترافیک به‌عنوان یک مرکز مهم در کنترل و هماهنگی اعزام قطارها می‌بایست در راستای پایداری سیستم حمل‌ونقل ریلی کشور جهت خدمت‌رسانی به

مشتریان در برابر حملات سایبری دشمن و خرابکاران موردحمایت قرارگرفته و ملاحظات پدافند غیرعامل سایبری در مورد آن استخراج گردد. حملات سایبری احتمالی به این مرکز به‌منظور اهداف خاصی که عبارت‌اند از: ایجاد اختلال در فعالیت‌های روزانه، ناکارآمدی یا محروم‌سازی از منابع موجود و ایجاد اختلال در حمل‌ونقل بار و مسافر است صورت می‌پذیرد. اساساً برقراری امنیت سایبری در مکان‌های مختلف با توجه به ویژگی‌های هر یک از مکان‌ها دارای نقاط اشتراک و افتراق می‌باشد؛ بر همین اساس رعایت یک الگوی استاندارد در زمینهٔ ایجاد امنیت سایبری می‌تواند به کمک مسئولین امر آمده و بستر مناسبی جهت تبادل اطلاعات و فرماندهی و کنترل در محیط کار به وجود آورد.

در این پژوهش سعی بر این است تا با استخراج ملاحظات پدافند غیرعامل سایبری، موارد و نکات موردنیاز جهت تأمین امنیت سایبری مرکز کنترل ترافیک راه‌آهن ج.ا.ایران را مشخص نموده تا باتدبیر دست‌اندرکاران در طول زمان اعمال گردد. استخراج و تعیین این ملاحظات در تحقق اهداف موردنظر پدافند غیرعامل در مرکز مذکور لازم و ضروری است. اعمال ملاحظات پدافند غیرعامل در این مرکز منجر به ارتقاء پایداری مرکز و درنتیجه تداوم مستمر رفت‌وآمد قطارهای مسافری و باری خواهد گردید. کاهش آسیب‌پذیری در برابر حملات سایبری، افزایش بازدارندگی در مقابل حملات سایبری، تداوم فعالیت‌های موردنظر در مرکز کنترل ترافیک موردنظر از دیگر نتایج استخراج و اعمال ملاحظات پدافندی است تا با ایجاد یک محیط امن از یک‌سو وظیفه اصلی حمل‌ونقل ریلی که همانا جابجایی بار و مسافر است صورت پذیرد و از سویی با ایجاد این بستر امن زمینه ارتقاء بهره‌وری در شرکت راه‌آهن ج.ا.ایران فراهم شود.

توجه نکردن به ملاحظات پدافندی در برخی موارد موجب ضررهای جبران‌ناپذیر در محیط کار می‌گردد و شرایط را برای بروز سوانح مختلف، قطع خدمت‌رسانی یا تأخیر در آن، کاهش بازدهی سازمان، افزایش هزینه‌ها، تلفات انسانی، کاهش اعتبار سازمان و سایر موارد مضر فراهم خواهد کرد.

هدف، سؤال و فرضیهٔ پژوهش

هدف: هدف این مقاله تعیین ملاحظات پدافند غیرعامل مرکز کنترل ترافیک راه‌آهن ج.ا.ایران در برابر حملات سایبری است.

سوال: ملاحظات پدافند غیرعامل مرکز کنترل ترافیک راه‌آهن ج.ا.ایران در برابر حملات سایبری کدامند؟

فرضیه: ملاحظات پدافند غیرعامل مرکز کنترل ترافیک راه‌آهن ج.ا.ایران در برابر حملات سایبری شامل تعیین حملات سایبری مؤثر، تعیین آسیب‌پذیری‌های مؤثر و تعیین راهکارهای پدافندی مقابله با تهدیدها و حذف یا کاهش آسیب‌پذیری‌ها است.

مفاهیم و مبانی نظری پژوهش

پدافند غیرعامل: عبارت است از مجموعه اقدامات غیرمسلحانه که موجب افزایش بازدارندگی، کاهش آسیب‌پذیری، تداوم فعالیت‌های ضروری، ارتقاء پایداری شبکه و تسهیل مدیریت بحران در مقابل تهدیدات و اقدامات نظامی دشمن می‌گردد (اسکندری، ۱۳۹۰: ۲۱).

پدافند غیرعامل در حوزه سایبری: پدافند غیرعامل در فضای سایبری شامل کلیهٔ اقدامات لازم (و غیرمسلحانه) به‌منظور حفظ امنیت، ایمنی و پایداری شبکه و تجهیزات وابسته و متصل به شبکه و رایانه‌های شخصی می‌باشد (شرکت ایزایران، ۱۳۸۷: ۵).

مرکز کنترل ترافیک: ناظر دائمی حسن انجام عملیات ریلی در شبکه می‌باشد که همواره از آن به‌عنوان قلب تپنده سیر و حرکت راه‌آهن نام‌برده می‌شود (راه‌آهن ج.ا.ایران، ۱۳۹۳: ۷۷).

حملات سایبری: حملات سایبری مجموعه‌ای از تکنیک‌ها شامل جمع‌آوری، انتقال، حفاظت، ممانعت از دسترسی، ایجاد اغتشاش و افت کیفیت در اطلاعات است که از طریق آن‌یکی از طرفین درگیربردشمنان خود به مزیتی چشمگیر دست‌یافته و آن را حفظ می‌کند (مگان برنز، ۱۳۷۸: ۱)

الگوهای امنیت سایبری چندلایه جهت امن سازی مراکز صنعتی: امروزه امنیت شبکه یک مسئلهٔ مهم برای ادارات و شرکت‌های دولتی و سازمان‌های کوچک و بزرگ است. تهدیدهای پیشرفته از سوی تروریست‌های فضای سایبر، کارمندان ناراضی و هکرها رویکردی نظام‌مند را برای امنیت شبکه می‌طلبد. در بسیاری از صنایع، امنیت به شکل پیشرفتهٔ یک انتخاب نیست بلکه یک ضرورت است. رویکرد لایه‌بندی راهبرد تکنیکی است که هم ابزار و امکان مناسبی را در سطوح مختلف در زیر ساختار شبکهٔ شما قرار می‌دهد و هم یک استراتژی سازمانی است که مشارکت همه از هیئت‌مدیره تا قسمت فروش را می‌طلبد.

رویکرد امنیتی لایه‌بندی شده روی نگهداری ابزارها و سیستم‌های امنیتی و روال‌ها در پنج لایه مختلف در محیط فناوری اطلاعات متمرکز می‌گردد.

۱- پیرامون ۲- شبکه ۳- میزبان ۴- برنامهٔ کاربردی ۵- دیتا

هدف در اینجا ایجاد درکی در سطح پایه از امنیت شبکه و پیشنهاد یک رویکرد عملی مناسب برای محافظت از دارایی‌های دیجیتال است زیرا محافظت از اطلاعات اختصاصی، به منابع مالی

نامحدود و عجیب‌وغریب نیاز ندارد. با این روش می‌توانید بدون هزینه کردن بودجه‌های کلان، موانع مؤثری بر سر راه اخلال گران امنیتی ایجاد کنید (پاکدل پرگل، علیرضا، ۱۳۸۹: ۱)

ای‌اس‌ام‌اس[1] چیست؟ به معنای سیستم مدیریت امنیت اطلاعات می‌باشد و استانداردهایی را برای ایمن‌سازی فضای تبادل اطلاعات در سازمان‌ها ارائه می‌دهد. این استانداردها شامل مجموعه‌ای از دستورالعمل‌هاست تا فضای تبادل اطلاعات یک سازمان را با اجرای یک طرح مخصوص به آن سازمان ایمن نماید. اقدامات لازم جهت ایمن‌سازی فضای تبادل اطلاعات عبارت‌اند از:

- تهیه طرح‌ها و برنامه‌های امنیتی موردنیاز سازمان؛
- ایجاد تشکیلات موردنیاز جهت ایجاد و تداوم امنیت فضای تبادل اطلاعات سازمان؛
- اجرای طرح‌ها و برنامه‌های امنیتی سازمان.

مستندات ای‌اس‌ام‌اس

- اهداف، راهبردها و سیاست‌های امنیتی فضای تبادل اطلاعات دستگاه؛
- طرح تحلیل مخاطرات امنیتی فضای تبادل اطلاعات دستگاه؛
- طرح امنیت فضای تبادل اطلاعات دستگاه؛
- طرح مقابله با حوادث امنیتی و ترمیم خرابی‌های فضای تبادل اطلاعات دستگاه؛
- برنامهٔ آگاهی‌رسانی امنیتی به پرسنل دستگاه؛
- برنامهٔ آموزش امنیتی پرسنل تشکیلات تأمین امنیت فضای تبادل اطلاعات دستگاه.

مزایای استفاده از ای‌اس‌ام‌اس

- اطمینان از تداوم تجارت و کاهش صدمات توسط ایمن ساختن اطلاعات و کاهش تهدیدها
- اطمینان از سازگاری با استاندارد امنیت اطلاعات و محافظت از داده‌ها
- قابل‌اطمینان کردن تصمیم‌گیری‌ها و محک زدن سیستم مدیریت امنیت اطلاعات
- ایجاد اطمینان نزد مشتریان و شرکای تجاری
- امکان رقابت بهتر با سایر شرکت‌ها
- ایجاد مدیریت فعال و پویا در پیاده‌سازی امنیت داده‌ها و اطلاعات
- به خاطر مشکلات امنیتی اطلاعات و ایده‌های خود را در خارج سازمان پنهان نسازید. (محمدی، ۱۳۹۲: ۳-۲).

1.Information Security Management System

سی‌ای‌آرتی[1] **چیست؟** در علوم رایانه و امنیت، به گروهی از متخصصین امنیت اطلاق می‌گردد که در مواقع بروز حوادث و یا بحران‌های مرتبط با حوزهٔ فناوری اطلاعات، در کوتاه‌ترین زمان ممکن اقدام به ارائهٔ راه‌حل نهایی برای رفع مشکل و یا شرکت در کارگروه‌های شکل‌گرفته به‌منظور ارائهٔ راه‌کارهای مؤثر و قابل‌قبول برای به حداقل رساندن صدمات ناشی از وقوع بحران می‌نمایند. هرچند در سال‌های اخیر با گسترش تهدیدات امنیتی، مسئولیت‌ها و راهکارهای مرتبط با پیشگیری از وقوع حوادث و بحران‌های امنیتی نیز بر عهده این گروه‌ها گذارده شده است. با توجه به تعریف ارائه‌شده، اولین و مهم‌ترین مسئولیت این گروه، در گام اول پاسخ مؤثر به حوادث و بحران‌های امنیتی به وقوع پیوسته، در گام بعدی نظارت دقیق بر وقایع جاری و تشخیص سریع و به‌موقع بحران و درنهایت انجام فعالیت‌های پیشگیرانه و تدافعی در شرایط آرامش می‌باشد. اهداف گروه مذکور متناسب با اهداف سازمان و جامعه قلمرو آن تعیین می‌گردد. در بیشتر موارد محافظت از سرمایه‌های حیاتی اطلاعات به‌عنوان هدف بنیادین موردقبول بوده و ازاین‌رو در صورت وقوع حادثه، حداقل کردن خرابی‌ها و کنترل آن، پاسخ مؤثر، بازیابی اطلاعات و جلوگیری از حوادث مشابه در آینده، به‌عنوان اهداف اساسی مورد اجماع می‌باشد. این گروه جهت تحقق اهداف فوق اطلاعات جامعی از حوادث، ضعف‌های امنیتی و آسیب‌پذیری‌های سامانه‌ها و نرم‌افزارهای مورداستفاده در زیرساخت‌های سازمانی و جامعهٔ قلمرو را جمع‌آوری می‌نماید و به یک نقطه کانونی و منبعی قابل‌اعتماد تبدیل می‌گردد. همچنین به‌عنوان یک پایگاه مرکزی اطلاعات، اجازه می‌یابد که کلیهٔ موارد مرتبط با امنیت را در سطح سازمان جمع‌آوری و ساماندهی نماید. این امر فرصتی جهت تجزیه‌وتحلیل و ارتباط دهی کلیهٔ وقایع که هر یک به‌تنهایی مرتبط به نظر نمی‌رسند را فراهم آورده و نقش گروه را به‌عنوان یک عنصر کلیدی در حداقل کردن تلفات و کاهش مخاطرات ارتقاء می‌بخشد.

انواع آن:

- بر اساس اهداف و وظایف؛
- بر اساس ساختار سازمانی؛
- بر اساس قلمرو (پلیس فتا، ۱۳۹۳: ۲-۱).

مرکز عملیات امنیت شبکه[2]**:** با گسترش روزافزون استفاده از ارتباطات و انتقال اطلاعات در بستر شبکه ها و اینترنت، حجم وسیعی از مبادلات تجاری و اداری، از این طریق صورت

1.Computer Emergency Readiness Team
2.Security Operations Center

می‌پذیرد. امروزه سرویس‌های اینترنتی و تحت شبکه، به‌عنوان قابل‌اعتمادترین، سریع‌ترین و در دسترسی‌ترین ابزارهای ارتباطی به شمار می‌روند. با توجه به اهمیت فوق‌العاده‌ای که شرکت‌های بزرگ به استفاده از چنین بسترهایی در ادارهٔ امور خود می‌دهند، جایگاه و اهمیت مقوله امنیت به‌وضوح مشخص است. زمانی که نوبت به امنیت می‌رسد، هر سازمانی نیاز و سیاست مختص خود را دارد. به‌این‌ترتیب راه‌حل‌های امنیتی، باید به‌گونه‌ای استاندارد طراحی شوند تا بتوانند نیازهای کلیهٔ سازمان‌ها را بدون نیاز به تغییرات اساسی در ساختار سیستم‌های آن ها، پوشش دهند. در اینجا قصد داریم به نحوه مدیریت یکپارچهٔ امنیت اطلاعات و ارتباطات با استفاده از استاندارد **بی‌اس ۷۷۹۹**[1] در یک مرکز امنیت شبکه اشاره نماییم.

مرکز عملیات امنیت کجاست؟ مرکز عملیات امنیت شبکه مکانی جهت مانیتورینگ و کنترل ۲۴ ساعته ورود و خروج اطلاعات در شبکه می‌باشد. به‌طورکلی هر مرکز عملیات امنیت به سه سطح عمده تقسیم می‌شود که هر یک وظایف خاصی را بر عهده‌دارند. این سطوح عبارت‌اند از:

سطح یکم: نقطه تماس کاربرها[2] و مسئول پاسخ‌گویی به اخطارهای دریافتی از کاربرهاست. در این سطح به کلیه اخطارهایی که از پیچیدگی پایین‌تری برخوردارند، پاسخ داده می‌شود.

سطح دوم: در حقیقت مکمل سطح یکم است و مسئول پاسخ‌گویی به مشکلات پیچیده‌تر در سیستم‌های امنیتی شبکه می‌باشد. برای اخطارهایی که از اهمیت بالایی برخوردارند، سیستم‌های سطح دوم به‌طور کامل درگیر می‌شوند.

سطح سوم: در این سطح کارشناسان ارشد و مشاوران امنیتی شبکه قرار دارند. این سطح در حقیقت پشتیبان دو سطح پایین تر است. درصورتی که به اشکالات امنیتی در دو سطح پایین پاسخ داده نشود، کارشناسان و سیستم های این سطح، درگیر می شوند. کلیه تدابیر امنیتی و مدیریت امنیت شبکه، در این سطح اندیشیده می‌شود (دشتی، افسانه، ۱۱۳۸۴).

مرکز کنترل ترافیک: این مرکز با شبکهٔ گسترده‌ای از ارتباطات و تجهیزات و با ارتباط دائم و مستمر بر کلیهٔ مراکز کنترل محلی مسیرهای ریلی تحت پوشش اقدام به مسیر سازی، کنترل، پایش مداوم حرکت و موقعیت قطارها، برقراری ارتباط و ابلاغ فرامین کنترلی به آن‌ها به عملیات کنترل ترافیک خطوط ریلی می‌پردازد و قادر است کلیهٔ وقایع و محدوده‌های مراکز کنترل محلی در سراسر مسیرهای ریلی را به‌صورت یکجا مشاهده و تصمیم‌گیری نماید. هر خط دارای نرم‌افزار کنترل ترافیک جداگانه و با برنامهٔ زمان‌بندی متفاوت می‌باشد و تنها بخش

---

۱. نوعی استاندارد امنیت سایبری در سازمان‌ها

2. Client

مشترک بین خطوط مسیرهای ارتباطی تک خطه می‌باشند که طی ضوابطی خاص تحت کنترل مشترک قرار داده‌شده‌اند و جابجایی قطارها را بین خطوط میسرمی‌سازند.

عملیات کنترل ترافیک: عبارت است از نظارت و کنترل تردد قطارها از طریق رایانه‌های مراکز محلی و بر روی پانل مرکز کنترل و فرمان مرکزی[1]. این عملیات بنا به مقتضیات زمانی و مکانی به شیوه‌های متفاوتی و با بهره‌گیری از مدهای کنترلی متفاوتی انجام می‌پذیرد.

این قسمت اصلی‌ترین قسمت برنامه می‌باشد که به کمک آن توزیع‌کنندگان ترافیک قادر هستند کلیه جزئیات منطقهٔ کنترلی را ببینند و دستورات موردنظر را اعمال کنند. این پنجره یکی از مهم‌ترین پنجره‌های برنامه می‌باشد که در این قسمت عملیات کنترل ترافیک، نظارت، هدایت، کنترل و تنظیمات برنامه انجام می‌شود. توزیع‌کنندهٔ ترافیک با دقت و نظارت مستمر در این صفحه، علاوه بر دقت در اعزام و دریافت قطارها، نسبت به هدایت قطارها در طول مسیر نیز دقت کافی را خواهد داشت. درصورتی‌که توزیع‌کنندهٔ کنترل ترافیک فقط چند ثانیه از این پنجره غافل شود و متناسب با وضعیت ترافیک خط واکنش مناسب آن را نداشته باشد ممکن است ترافیک یک بخش و یا کل خط دچار اختلال گردد. با توجه به گستردگی طول خط از پانل کنترل به‌عنوان ابزار دیداری توزیع‌کنندگان استفاده می‌شود و صدور دستورات در منطقهٔ موردنیاز از طریق پنجره مذکور صورت می‌گیرد. برای پیمایش کامل این پنجره می‌توان از نوارهای عمودی و افقی استفاده نمود. در ضمن می‌توان با استفاده از انتخاب گروهی محدودهٔ قابل‌کنترل با انتخاب نام ایستگاه یا مشخص نمودن محدوده به آن قسمت دسترسی پیدا کرد. (صندیدزاده، ۱۳۹۲: ۶-۵)

حملات مؤثر بر مراکز کنترل و صنعتی

- **حملات غیرفعال (خاموش):** در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می‌یابد ولی اقدام به تغییر محتوای اطلاعات منبع نمی‌کند. این نوع حمله می‌تواند تنها به یکی از اشکال شنود ساده یا آنالیز ترافیک باشد که به دو صورت زیر وجود دارد:

۱- شنود[2]: در این نوع، نفوذگر تنها به پایش اطلاعات ردوبدل شده می‌پردازد. برای مثال شنود ترافیک روی یک شبکهٔ محلی یا یک شبکهٔ بی‌سیم (که مدنظر ما است) نمونه‌هایی از این نوع حمله به شمار می‌آیند.

1. Mimic Panel
2.Eavesdropping

۲- آنالیز ترافیک[1]: در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده‌ها می‌پردازد. به‌عبارت‌دیگر بسته یا بسته‌های اطلاعاتی به همراه یکدیگر اطلاعات معنی‌داری را ایجاد می‌کنند.

- **حملات فعال**: در این نوع حملات، برخلاف حملات غیرفعال، نفوذ گر اطلاعات موردنظر را که از منابع به دست می‌آید، تغییر می‌دهد که در واقع انجام این تغییرات مجاز نیست. ازآنجایی‌که در این نوع حملات اطلاعات تغییر می‌کنند، شناسایی رخداد حملات فرآیندی امکان‌پذیر است. این نوع از حملات به چهار دستهٔ زیر تقسیم‌بندی می‌گردند:

۱- تغییر هویت[2]: در این نوع حمله، نفوذگر هویت اصلی را جعل می‌کند. این روش شامل تغییر هویت اصلی یکی از طرف‌های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرایند پردازش اطلاعات نیز می‌گردد.

۲- پاسخ‌های جعلی[3]: نفوذگر در این قسم از حملات، بسته‌هایی که طرف گیرندهٔ اطلاعات در یک ارتباط دریافت می‌کند را پایش می‌کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می‌گردد ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می‌گردند. این نوع حمله بیش‌تر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می‌کند. در این حالت بسته‌های پاسخی که برای فرستنده به‌عنوان جواب به سؤالات فرستنده ارسال می‌گردند به معنای پرچمی برای شناسایی گیرنده محسوب می‌گردند.

۳- تغییر پیام[4]: در برخی از موارد مرسوم‌ترین و متنوع‌ترین نوع حملات فعال تغییر پیام است. ازآنجایی‌که گونه‌های متنوعی از ترافیک بر روی شبکه رفت‌وآمد می‌کنند و هریک از این ترافیک‌ها و پروتکل‌ها از شیوه‌ای برای مدیریت جنبه‌های امنیتی خود استفاده می‌کنند، ازاین‌رو نفوذگر بااطلاع از پروتکل‌های مختلف می‌تواند برای هر یک از این انواع ترافیک نوع خاصی از تغییر پیام‌ها و درنتیجه حملات را اتخاذ کند.

۴- حمله‌های (دی‌اس)[5]: این نوع حمله، در حالات معمول، مرسوم‌ترین حملات را شامل می‌شود. در این نوع حمله نفوذگر یا حمله‌کننده برای تغییر نحوهٔ کارکرد یا مدیریت یک سامانهٔ ارتباطی یا اطلاعاتی اقدام می‌کند. ساده‌ترین نمونه سعی در از کار انداختن خادم‌های نرم‌افزاری

1.Traffic Analysis
2.Masquerade
3.Replay
4.Message Modification
5.Denial Of Service

و سخت‌افزاری است. پیرو چنین حملاتی، نفوذگر پس از از کار انداختن یک سامانه که معمولاً سامانه‌ای است که مشکلاتی برای نفوذگر برای دسترسی به اطلاعات فراهم کرده است، اقدام به سرقت، تغییر یا نفوذ به منبع اطلاعاتی می‌کند. در برخی از حالات، در پی حملهٔ انجام‌شده، سرویس موردنظر به‌طور کامل قطع نمی‌گردد و تنها کارایی آن مختل می‌گردد. در این حالت نفوذگر می‌تواند با سوءاستفاده از اختلال ایجادشده به نفوذ به همان سرویس اقدام کند (گروه امداد امنیت کامپیوتر ایران،۱۳۹۳: ۲-۱).

پیشینهٔ پژوهش

در خصوص ملاحظات پدافند غیرعامل مرکز کنترل ترافیک راه‌آهن ج.ا.ایران در برابر حملات سایبری تاکنون پژوهش مدونی انجام نگرفته است.

- پایان‌نامهٔ مجتبی رنجبر در سال ۱۳۹۲ با موضوع الزامات سامانهٔ مدیریت امنیت فناوری اطلاعات وارتباطات در فضای سایبری با رویکرد پدافند غیرعامل که باهدف تبیین الزامات سامانه مدیریت امنیت فناوری اطلاعات و ارتباطات در فضای سایبری با رویکرد پدافند غیرعامل صورت گرفته است. پژوهش انجام‌شده به‌منظور فراهم ساختن زمینه‌های علمی و به دست آوردن دانش به‌روز و کارآمد جهت حل مسائل امنیتی کنونی فناوری اطلاعات و ارتباطات در فضای سایبر با رویکرد پدافند غیرعامل صورت پذیرفته است.

- پایان‌نامهٔ حسین خوش عمل در سال ۱۳۹۰ با عنوان الزامات ملاحظات و راهبردهای دفاع غیرعامل در حوزهٔ فناوری اطلاعات باهدف تبیین الزامات و ملاحظات دفاع غیرعامل در حوزهٔ فناوری اطلاعات برای پایداری زیرساخت‌های حیاتی در برابر تهدیدات سایبری صورت گرفته است. در این پایان‌نامه مهم‌ترین اقدامات دفاع غیرعامل در برابر تهدیدات سایبری را می‌توان کاهش ضریب جراحات و تلفات انسانی در حملات سایبری، کنترل سطح آسیب پذیری‌های اطلاعاتی تأسیسات حیاتی، سناریونویسی و آینده پژوهی در محیط سایبری، ایجاد بخش سازمانی امنیت فضای سایبر ملی، کنترل طیف تهدیدات سایبری (خرابکاری، فریب، دزدی، جاسوسی، افشاگری، نفوذ)، تبیین تاکتیک‌های ضد عملیات روانی برای ترغیب نهادهای بین‌المللی بیان کرد.

روش پژوهش

ازآنجایی‌که در پژوهش حاضر به بررسی وضعیت موجود متغیرها پرداخته می‌شود و تعیین ملاحظات پدافند غیرعامل مرکز کنترل ترافیک راه‌آهن ج.ا.ایران بر اساس تحلیل یافته‌های به‌دست‌آمده از منابع علمی و ابزار (پرسشنامه) انجام می‌گردد، ازاین‌رو از روش توصیفی -

تحلیلی استفاده می‌شود. همچنین پژوهش از نوع کاربردی می‌باشد زیرا اقدام به ارائهٔ راهکارهای سودمند جهت برقراری امنیت و کاهش آسیب‌پذیری مرکز خواهد نمود.

جامعهٔ آماری این پژوهش، گزیده‌ای از متخصصین، مدیران و کارشناسان آگاه به مسائل پدافند غیرعامل، فضای سایبری و انواع حملات و آسیب‌پذیری‌های آن و مرکز کنترل ترافیک راه‌آهن تشکیل می‌دهند. با توجه به تعداد کم متخصصین در این زمینه جامعهٔ آماری مذکور به تعداد ۳۰ نفر به شرح موردبررسی قرار می‌گیرد.

جامعه نمونه و روش نمونه‌گیری: پرسشنامه بر اساس مقیاس طیف لیکرت طراحی شده است. با توجه به‌عنوان پژوهش، مدیران (۳ نفر)، صاحب‌نظران و کارشناسان متخصص و فعال در فضای سایبری شرکت راه‌آهن ج.ا.ایران (۲۷ نفر) جامعهٔ نمونه ما را تشکیل می‌دهند. جامعهٔ نمونه با تعداد جامعهٔ آماری برابر در نظر گرفته‌شده و به میزان (۳۰ نفر) منطبق است.

جهت گردآوری اطلاعات و داده‌ها از روش کتابخانه‌ای و میدانی استفاده‌شده است و برای تدوین مبانی نظری و پیشینهٔ پژوهش از روش کتابخانه‌ای و برای گردآوری داده‌ها از جامعهٔ آماری با استفاده از پرسشنامه و از روش میدانی استفاده‌شده است.

روایی پرسشنامه‌ها از طریق روایی صوری به‌دست‌آمده و برای به دست آوردن روایی پرسشنامه، سؤالات آن‌که نتیجه مطالعهٔ منابع علمی، جستجو در اینترنت، طوفان فکری و استفاده از نظرات نخبگان بوده، در اختیار متخصصان و کارشناسان آگاه به مسائل پدافند غیرعامل، فضای سایبری و مرکز کنترل ترافیک راه‌آهن ج.ا.ایران قرارگرفته و طی جلساتی با استفاده از خرد جمعی متخصصین نسبت به اصلاح و استانداردسازی آن اقدام شده است.

اعتبار پرسشنامه از طریق آلفای کرونباخ و تجزیه‌وتحلیل داده‌های به‌دست‌آمده توسط نرم‌افزار تحلیل آماری اس‌پی‌اس‌اس[1] محاسبه شده است. ضریب آلفای کرونباخ بدست آمده ۰.۸۹۱ است که نشان می‌دهد که پرسشنامه از اعتبار بالا و قابل‌قبولی برخوردار است.

بحث، نتیجه‌گیری و پیشنهاد

بر اساس نتایج به‌دست‌آمده در این پژوهش مهم‌ترین حملات سایبری مؤثر بر مرکز کنترل ترافیک راه‌آهن ج.ا.ایران به ترتیب اولویت عبارت‌اند از:

۱- حملات محرومیت از خدمات
۲- حملات تغییر محتوای پیام
۳- حملات پاسخ‌های جعلی

1.spss

۴- حملات تغییر هویت
۵- حملات آنالیز ترافیک
۶- حملات شنود

همان‌گونه که بیان شد سیر و حرکت قطارها به‌صورت منظم و در زمان‌بندی دقیق اهمیت بسیاری دارد زیرا بروز حادثه در یک محور برای هر یک از قطارها معمولاً باعث بسته شدن کل آن مسیر تا رفع کامل حادثه خواهد شد و عملاً بهره‌برداری از محور مذکور به‌طورکلی مختل و متوقف می‌شود. وجود هرگونه اشکال و ایراد در ابزارهای مورداستفاده در مرکز کنترل ترافیک و یا ارسال اطلاعات نادرست از این مرکز به تجهیزات تحت پوشش احتمال بروز سانحه و ازهم‌گسیختگی حمل‌ونقل ریلی، خارج شدن کنترل سیر و حرکت قطارها از حالت مکانیزه به دستی و درنتیجه کاهش بهره‌وری شرکت راه‌آهن ج.ا.ایران را در پی خواهد داشت. به‌واسطه این احتمالات می‌بایست کلیهٔ تمهیدات لازم در خصوص ملاحظات پدافند غیرعامل سایبری را در این مرکز در برابر حملات مذکور موردنظر قرار داده و بر اساس اولویت ذکرشده در بالا نسبت به اجرایی نمودن این تمهیدات اقدام نمود. مهم‌ترین حمله به‌دست‌آمده از نظرسنجی حملهٔ محرومیت از خدمات می‌باشد که باعث از کار انداختن سرورهای تصمیم‌گیرنده مرکز کنترل خواهد گردید و درنتیجه حداقل لطمه‌ای که به حمل‌ونقل ریلی وارد خواهد شد کاهش تردد قطارها در محور مذکور تا برطرف شدن مشکل می‌باشد زیرا سیستم از حالت مکانیزه به حالت دستی تغییر خواهد نمود و مدیریت سیر و حرکت قطارها دشوارتر و تعداد قطارهای عبوری از محور مذکور کاهش خواهد یافت. بر اساس نتایج به‌دست‌آمده مهم‌ترین آسیب‌پذیری‌ها در برابر حملات سایبری در مرکز کنترل ترافیک راه‌آهن ج.ا.ایران به ترتیب اولویت عبارت‌اند از:

۱. وجود کارمندان ناراضی
۲. کنترل نکردن دقیق ورود و خروج افراد و تجهیزات به اتاق سرور و مرکز کنترل ترافیک
۳. کمبود نیروی انسانی متخصص جهت تعمیر و نگهداری تجهیزات
۴. استفاده نکردن از نرم‌افزارهای امنیتی
۵. استفاده نکردن از پروتکل‌های ارتباطی امن
۶. رعایت نکردن اتصال امن و ایمن پیمانکاران و کارشناسان با سرورها و رایانه‌ها
۷. تصمیمات مدیریتی نامناسب
۸. کمبود منابع مالی، تجهیزات و قطعات مرتبط
۹. به‌روزرسانی نکردن سیستم‌عامل و نرم‌افزارها

۱۰. سیستم‌های عامل و برنامه‌های کاربردی غیربومی
۱۱. استفاده از تکنولوژی‌های سخت‌افزاری غیربومی
۱۲. فرآیندهای سازمانی و بروکراسی اداری دست‌وپا گیر

بر اساس نتایج به‌دست‌آمده عوامل انسانی سه اولویت نخست در به وجود آمدن آسیب‌های مرکز کنترل ترافیک راه‌آهن ج.ا.ایران است. عوامل انسانی به‌ویژه زمانی که نارضایتی در خصوص مسائل اقتصادی، رفاهی و معیشتی و یا ارتقاء شغلی کارکنان در میان باشد مهم‌ترین و تأثیرگذارترین مؤلفه‌های آسیب‌پذیری در این مرکز هستند. ازاین‌رو می‌بایست تا حد امکان و همگام با اهداف عالیهٔ سازمان و در چارچوب قوانین سازمانی نسبت به رضایتمندی کارکنان اقدام نمود. همچنین اولویت‌های چهارم و پنجم و ششم در آسیب‌پذیری‌ها به موارد نرم‌افزاری اشاره دارد. تهیهٔ برخی نرم‌افزارهای امنیتی و به‌کارگیری آن‌ها، وضع قوانین امنیتی جهت اتصال امن به رایانه‌ها، سرورها و دیگر تجهیزات سخت‌افزاری باعث کاهش آسیب‌پذیری‌ها و درنتیجه ارتقاء پایداری قسمت‌های مختلف سازمان ازجمله مرکز کنترل ترافیک خواهد شد. در پایان‌بر اساس نتایج به‌دست‌آمده در این پژوهش مهم‌ترین راهکارها در برابر حملات سایبری در مرکز کنترل ترافیک راه‌آهن به ترتیب اولویت عبارت‌اند از:

۱- پشتیبان‌گیری مداوم از داده‌های حیاتی و حساس
۲- مستندسازی و ارائهٔ گزارش تهاجم‌های تشخیص داده‌شده قبلی به تیم امنیت
۳- مرور گزارش‌های روزانه مربوط به تجهیزات نرم‌افزاری و سخت‌افزاری (لوگ[۱]) ها
۴- استفاده از سامانه‌های موازی[۲]
۵- استفاده از پروتکل‌های رمزنگاری جهت کد کردن اطلاعات مبادله شده
۶- استفاده از تیم‌های سی‌ای‌آرتی[۳]
۷- پیاده‌سازی استاندارد آی‌اس‌اس[۴] در سازمان
۸- تدوین سیاست‌های امنیتی جامع در سازمان مانند کنترل دسترسی، استفاده از رمز عبور
۹- آموزش، فرهنگ‌سازی و آگاهی کاربران
۱۰- استفاده از سامانه اس‌اوسی[۵] بومی (کنترل ۲۴ ساعتهٔ ورودی‌ها و خروجی‌های شبکه)

---

۱. لیست فرآیندهای انجام‌شده

2.REDANDANT

۳. گروه واکنش سریع رایانه‌ای
۴. سامانه مدیریت امنیت اطلاعات
۵. مرکز عملیات امنیت

۱۱- امنیت فیزیکی مناسب و تخصیص مکان‌های امن برای تأسیسات
۱۲- استفاده از فن‌آوری‌های نوین بومی (نرم‌افزاری و سخت‌افزاری)

بر اساس نتایج به‌دست‌آمده اولویت‌های اول تا چهارم راهکارهای ارائه‌شده در برابر حملات سایبری برای مرکز کنترل ترافیک راه‌آهن، جملگی بر استفاده از پشتیبان گیری، افزونگی، مستندسازی و مرور مستندات روزانه دلالت دارد و استفاده از فن‌آوری‌های بومی نرم‌افزاری و سخت‌افزاری در اولویت آخر قرار دارد و احتمالاً با توجه به عقب‌ماندگی کشورمان در زمینهٔ فناوری‌های نرم‌افزاری و سخت‌افزاری، در حال حاضر بومی‌سازی این دو مقوله راهکار مناسبی به نظر نرسیده است و می‌بایست جهت خودکفایی و ارتقاء دانش فناوری اطلاعات (نرم‌افزاری و سخت‌افزاری) همت بیشتری در سطح کشور گمارده شود .به‌منظور اندازه‌گیری میزان انطباق راهکارهای دوازده‌گانه ارائه‌شده برای مرکز کنترل ترافیک راه‌آهن با اهداف پدافند غیرعامل سایبری کشور، توسط پرسشنامهٔ دیگری میزان تأثیر هر یک از راهکارهای ارائه‌شده بر هریک از اهداف پنج‌گانه پدافند غیرعامل (کاهش آسیب‌پذیری، افزایش بازدارندگی، ارتقاء پایداری ملی، تسهیل در مدیریت بحران و تداوم فعالیت‌های ضروری) تعیین گردید. با توجه به نتایج به‌دست‌آمده مشخص شد راهکار استفاده از پروتکل‌های رمزنگاری جهت کد کردن اطلاعات مبادله شده بیشترین تأثیر را میان کلیهٔ راهکارهای ارائه‌شده بر کاهش آسیب‌پذیری با میانگین رتبه‌ای ۳.۸۳ داشته است. همچنین همین راهکار کمترین تأثیر را میان کلیهٔ راهکارهای ارائه‌شده بر تسهیل در مدیریت بحران با ۲.۴۲ داشته است. همچنین مشخص گردید از ۱۲ راهکار ارائه‌شده ۵ راهکار در اولویت نخست خود بر کاهش آسیب‌پذیری بیشترین تأثیر رادارند و ۵ راهکار دیگر در اولویت نخست خود بیشترین تأثیر را برافزایش بازدارندگی (جلوگیری از حمله) داشته‌اند که این مهم با در نظر گرفتن میانگین رتبه‌ای ۳.۳۲ و ۳.۲۱ برای کاهش آسیب‌پذیری و افزایش بازدارندگی مورد تأیید قرار می‌گیرد.

منابع

۱. اسکندری، حمید (۱۳۸۸)؛ ***مقالهٔ الگوهای سناریونویسی در مدیریت بحران***، محل نشر: تهران، نام ناشر: انتشارات بوستان حمید.

۲. پاکدل پرگل، علیرضا (۱۳۸۹)؛ ***مقالهٔ طبقه‌بندی امنیت شبکه‌ها***، (۱۰-۱)، محل نشر: خراسان رضوی، ادارهٔ برنامه‌ریزی و فناوری اطلاعات

۳. خوش عمل، حسین (۱۳۹۰)؛ ***پایان‌نامهٔ الزامات ملاحظات و راهبردهای دفاع غیرعامل در حوزه فناوری اطلاعات***، محل نشر: تهران، انتشارات: دانشکده علوم و فنون فارابی

۴. دشتی، افسانه (۱۳۸۴)؛ مقالهٔ مرکز عملیات امنیت شبکه، نام مجله: ***ماهنامهٔ شبکه***، دوره: سال ۳، شماره ۵۵، شماره صفحات (۵-۱)، محل نشر: تهران، نام ناشر: هرمز پور رستمی

۵. رنجبر، مجتبی (۱۳۹۲)؛ ***پایان‌نامهٔ الزامات سامانه مدیریت امنیت فناوری اطلاعات و ارتباطات در فضای سایبری با رویکرد پدافند غیرعامل***، محل نشر: تهران، نام ناشر: انتشارات دانشکدهٔ علوم و فنون فارابی

۶. شرکت ایزایران (۱۳۸۷)؛ ***کتاب پدافند غیرعامل در حوزهٔ جنگ سایبر***، محل نشر: تهران، انتشارات: مرکز پدافند غیرعامل شرکت ایزایران

۷. صندیدزاده، محمدعلی (۱۳۹۲)؛ ***کتاب مفاهیم ترافیک در شبکه حمل‌ونقل ریلی و مترو***، محل نشر: تهران، انتشارات: دانشگاه علم و صنعت

۸. محمدی، ابوالفضل (۱۳۹۲)؛ مقاله ISMS چیست، ***مجلهٔ الکترونیکی امنیت فناوری اطلاعات شماره صفحات (۱۱-۱)***، محل نشر: تهران، نام انتشارات: سایت امنیت فناوری اطلاعات

۹. مگان، برنز (۱۳۷۸)؛ ***سخنرانی دربارهٔ جنگ سایبری، مرجع تدوین‌کننده***:

۱۰. پایگاه اطلاع‌رسانی پلیس فتا، عنوان: cert چیست، www.cyberpolice.ir

۱۱. ***پایگاه اطلاع‌رسانی گروه امداد و امنیت کامپیوتر ایران***، عنوان: امنیت در شبکه‌های بی‌سیم، www.ircert.com.

۱۲. وب‌سایت ***شرکت راه‌آهن ج.ا.ایران، عنوان***: شرح وظایف مرکز کنترل ترافیک، www.rai.ir،