ماهنامه اداره کل پدافند غیر عامل
شماره ۴۲/ اسفند ماه ۱۳۹۸

ماهنامه دیجیتالی پدافند غیرعامل

استاندار آذربایجان شرقی:
حفظ سلامت روحی و روانی جامعه و افزایش آمادگی در برابر بیماری کرونا اهمیت زیادی دارد

مدیرکل پدافند غیرعامل استانداری:
مدیریت افکار عمومی باید مورد تجدید نظر قرار گیرد و این امر نیازمند تشکیل تیم‌های تخصصی و استفاده از تمام ظرفیت‌هاست

در این شماره می‌خوانید:


بسم الله الرحمن الرحیم

فهرست مطالب:

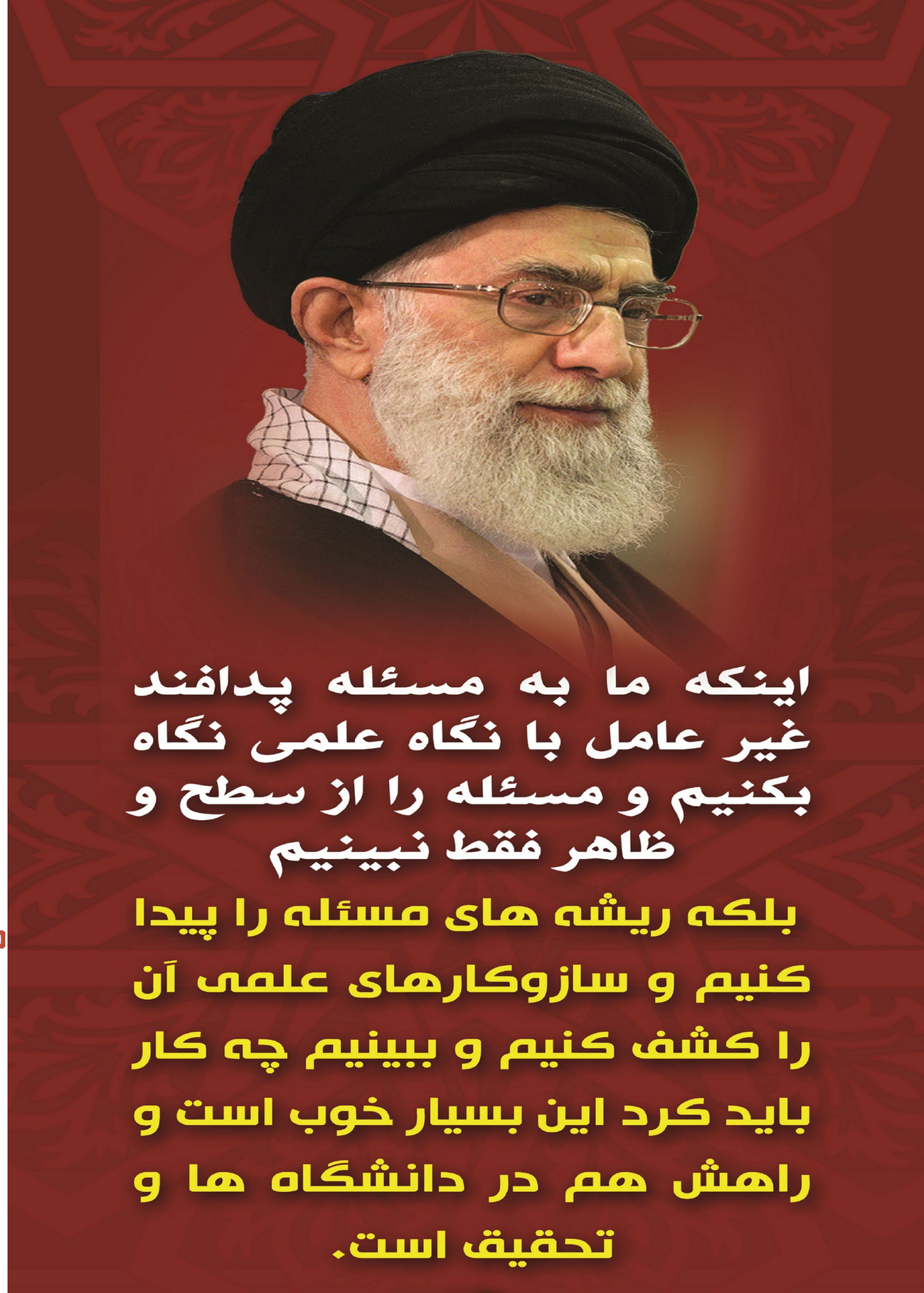
مدیر مسئول:
محمد باقر آقایی

سردبیر:
لیدا رسول اهری

نشانی:
تبریز، میدان شهدا، استانداری آذربایجان شرقی، اداره کل
پدافند غیرعامل
تلفن: ۰۴۱-۳۵۲۹۱۳۱۸
دورنگار: ۰۴۱-۳۵۲۹۱۳۵۹

استادان، پژوهشگران و دانشجویان علاقمند، می‌توانند مقاله‌های آموزشی، پژوهشی و ترویجی خود را برای درج در نشریه پدافند غیر عامل به نشانی زیر ارسال کنند.

passivedefense@ostan-as.gov.ir



جلسه کارگروه اطلاع رسانی و آرام بخشی قرارگاه پدافند زیستی استان

مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی با بیان اینکه اعتماد عمومی بزرگترین سرمایه کشور است، افزود: رسانه‌ها در خط مقدم صیانت از این سرمایه قرار دارند.

محمدباقر آقایی در جلسه کارگروه اطلاع رسانی و آرام بخشی قرارگاه پدافند زیستی استان، اظهار داشت: مدیریت افکار عمومی باید مورد تجدید نظر قرار گیرد و این امر نیازمند تشکیل تیم‌های تخصصی و استفاده از تمام ظرفیت‌هاست.

وی بر جدیت در برخورد با افرادی که مغرضانه و عامدانه، امنیت روانی مردم را هدف قرار می‌دهند تأکید کرد و گفت: امنیت روانی مردم و آرامش جامعه تعارف بردار نیست.

آقایی با بیان اینکه آموزش و اطلاع رسانی مردم در قالب‌های مختلف انجام می‌شود افزود: مشکل اساسی در شرایط کنونی در زمینه آرامش بخشی به جامعه است.

شایعات موجود در جامعه باید رصد شده و با ترویج آموزش‌های خود مراقبتی و همگانی پیشگیرانه، امنیت روانی مردم حفظ شود. مغایرت آمارهای مبتلایان به ویروس کرونا در کشور، به مغایرت زمان اعلام نتایج آزمایش برمی‌گردد و دلیلی بر کتمان آمار وجود ندارد.

مدیرکل صدا وسیمای مرکز آذربایجان شرقی نیز با اشاره به تلاش‌های سایبری گروهک‌های منافقین و وهابیون برای ایجاد نگرانی در جامعه، گفت: متأسفانه میزان خبرهایی که این رسانه‌ها در رابطه با شیوع کرونا در ایران تولید می‌کنند چندین برابر چین است که منشأ ویروس کرونا بود.

با بازنمایی محیط‌های بیمارستانی، سعی داریم ترس و نگرانی ایجاد شده در فضای مجازی را کمتر کنیم و قطعاً نشان دادن توانایی، مجرب بودن و با انگیزه بودن کادر درمان در آرامش بخشی جامعه مؤثر است.

موضوع انتشار ویروس یک مقوله است، اما آنچه که این مشکل را دو چندان می‌کند، موج سواری ضد انقلاب بر روی این فضا برای التهاب آفرینی است.

جلسات ستاد استانی مدیریت و مقابله با کرونا

مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی در جلسه کارگروه‌های هشت‌گانه قرارگاه پدافند زیستی تأکید کرد که این کارگروه‌ها نسبت به انجام وظایف خود آمادگی کامل داشته باشند.

محمدباقر آقایی گفت: کارگروه‌های هشت گانه با توجه به انجام رزمایش‌ها و تمرین‌های قبلی باید آمادگی کامل داشته تا در صورت بروز حادثه غافلگیر نشوند. رصد و پایش تهدیدات ویروس جدید کرونا توسط کارگروه رصد، پایش و هشدار سریع به صورت مستمر انجام شود تا اخبار صحیح در اختیار مردم قرار گرفته و آرامش روانی مردم مختل نشود.

آقایی همچنین به شیوع این ویروس در استان‌های دیگر و جایگاه‌های قرنطینه موجود در سطح استان اشاره کرد و اظهار داشت: مراکز قرنطینه باید آماده باشند تا در صورت مشاهده موارد مشکوک در استان فوراً به قرنطینه انتقال یابند.

مدیرکل پدافند غیرعامل با تأکید بر جلوگیری از انتشار شایعات در فضای مجازی خواستار مدیریت افکار عمومی در حوزه مسائل زیستی شد. مدیریت افکار عمومی توسط صدا و سیما به عنوان رئیس کارگروه اطلاع‌رسانی و مدیریت افکار عمومی در این شرایط حساس بسیار مهم و ضروری بوده است.

در حال حاضر تنها دستگاهی که آخرین اطلاعات و اخبار موثق و صحیح را می‌تواند ارائه دهد دانشگاه علوم پزشکی تبریز است.

آقای دکتر پورمحمدی استاندار محترم آذربایجان شرقی با بیان اینکه علاج واقعه قبل از وقوع باید کرد، بر آمادگی کامل مسئولان ذیربط استانی، آموزش و اقدامات پیشگیرانه تأکید کرده و برخورد جدی با رسانه‌هایی که به تشویش اذهان عمومی دامن می‌زنند را خواستار شد. ایشان اطلاع رسانی و کارهای مقابله‌ای نظیر بهداشت فردی، جمعی و محیطی را از مهمترین اقدامات خوانده و از دستگاه‌های مربوطه خواستند تا با استفاده از ظرفیت سازمان‌های مردم نهاد مخصوصاً بسیج در این امر مهم تلاش نمایند. همچنین اقدامات انجام یافته را برای آرامش روانی به سمع نظر مردم برسانند.

رئیس ستاد استانی مقابله با بیماری کرونا از جامعه فداکار و ایثارگر پزشکی، پرستاری و دست‌اندرکاران دانشگاه علوم پزشکی تبریز قدردانی کرده و افزودند: بیماری کرونا، سلامت جسمی مردم را به خطر انداخته و آنچه امروز مهم است حفظ سلامت روحی و روانی جامعه و افزایش آمادگی در برابر این بیماری است.

امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور

تهیه و تنظیم: لیدا رسول اهری (کارشناس آموزش و پژوهش اداره کل پدافند غیرعامل)

منابع:
۱. محمودزاده، ابراهیم؛ حسنی اصل، حمیدرضا؛ قوچانی، محمد مهدی؛ نیک نفس، علی، «تدوین راهبردهای امنیت سایبری سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور»، فصلنامه علمی پژوهشی مطالعات بین رشته‌ای دانش راهبردی، سال هشتم، شماره ۳۱، تابستان ۱۳۹۷، صفحات ۲۸۱-۲۵۲.
۲. مشهد نعمتی، حسن؛ امیدی، حمید؛ خالقی راد، حسن، « تست نفوذ و ضرورت آن در ارتقاء امنیت سایبری سیستم های کنترل صنعتی».
۳. بیگ زاده، یحیی؛ قاسمی، رضا؛ توتونچی، علی قاسم، « امنیت سایبری در سیستم‌های کنترل صنعتی».
٤. ترمه چی، عاطفه؛ « کنترل آسیب‌های ناشی از حملات سایبری به زیرساخت‌های حیاتی»، پایان نامه کارشناسی ارشد، دانشگاه صنعتی امیرکبیر، ۲۰۱۳.
۵. مظفری، اعظم؛ «راهکارهای امنیتی حوزه شبکه در سیستم‌های کنترل صنعتی»، سی‌امین کنفرانس بین المللی برق، ۱۱ تا ۱۳ آبان ۱۳۹٤.
٦. افشار، احمد؛ ترمه چی، عاطفه، « مروری بر امنیت سایبری سیستم‌های کنترل صنعتی»، مجله کنترل، جلد ۸ شماره ۱، بهار ۱۳۹۳، صفحه ۳۱-٤٠

چکیده

زیرساخت‌های حیاتی و حساس نقش مهمی در پیشرفت و ثبات نظام‌های سیاسی، اقتصادی و اجتماعی کشورها دارند. توجه به وابستگی شدید زیرساخت‌های حیاتی به فضای سایبر به عنوان مغز مدیریت و راهبری پیکره زیرساخت‌های حیاتی از اهمیت ویژه‌ای برخوردار است. زیرساخت‌ها و سامانه‌های حیاتی و حساس کشور، یا خود بخشی از فضای سایبری کشور را تشکیل می‌دهند و یا از طریق این فضا، کنترل، مدیریت و بهره‌برداری می‌شوند. سامانه‌های کنترل صنعتی به عنوان مرکز راهبری و بخش جدایی‌ناپذیر این زیرساخت‌ها اهمیت و اولویت زیادی دارند. همچنین، کنترل و نظارت بر گستره وسیعی از فرآیندها و صنایع را بر عهده دارند. این سامانه‌ها در معرض چالش‌ها، آسیب‌ها و تهدیدهای گوناگونی نظیر ارتکاب جرائم سازمان یافته، جاسوسی، خرابکاری و... قرار دارند.

مقدمه

زیرساخت‌ها بسترهای مهم حیات، رشد و پویای صنایع و جوامع به شمار می‌روند. در این میان برخی از زیرساخت‌ها نقش حیاتی در منافع ملی دارند و اختلال هرچند کوتاه مدت در عملکرد آن‌ها می‌تواند منجر به آسیب جدی در اقتصاد، امنیت یا ایمنی جامعه شود.

با توجه به گستردگی حوزه عملکرد سامانه‌های کنترل صنعتی، تأمین‌کنندگان به طور فزاینده‌ای دسترسی از راه دور مبتنی بر وب را به منظور تسهیل عملیات نظارت و کنترل در محصولات خود جایگذاری کرده‌اند.

دسترسی آنلاین به اطلاعات برای تصمیم‌گیرندگان مزایایی از قبیل پیاده‌سازی الگوهای کارآمدتر کنترل، افزایش ایمنی کارکنان و واحدهای صنعتی، کاهش هزینه‌های تولید و نهایتاً افزایش بهره‌وری به همراه داشته است.

اتصال روزافزون این ابزارها به فضای سایبر به صورت مستمر مسیرهای تهدید و ناامنی بیشتری را بر ضد این زیرساخت‌ها فراهم می‌سازد.

بخش عمده‌ای از تهدیدات موجود علیه کشور، به ویژه در زیرساخت‌های حیاتی یا مستقیماً از فضای سایبر سامانه‌های کنترل صنعتی نشأت می‌گیرند و یا این فضا را هدف تهدید مستقیم خود قرار می‌دهند.

بررسی تهدیدها و آسیب‌پذیری‌های سایبری سیستم‌های کنترل و مقابله با آن‌ها بعد از حمله استاکس نت، به عنوان یک چالش جدی وارد حوزه مطالعاتی و کاربردی گرایش کنترل در دانشگاه‌ها شده است.

فضای سایبر پنجمین عرصه جنگ بعد از زمین، دریا، هوا و فضا محسوب می‌شود و این مسئله نشان می‌دهد که فضای سایبری یک فضای درگیری است که در استراتژی‌های دشمنان به وضوح دیده می‌شود.

زیرساخت‌های حیاتی یک کشور تأثیر زیادی بر روی رقابت جهانی در حوزه اقتصادی و سیاسی می‌گذارد. اگر در یک زیرساخت اختلالی ایجاد شود حداقل یکی از بخش‌های مهم کشور از نظر سیاسی، اقتصادی، اجتماعی و یا امنیتی به خطر می‌افتد.

اهمیت زیرساخت‌های حیاتی در عصر رقابت در عرصه اینترنت و اطلاعات بر کسی پوشیده نیست اما حفاظت از آن‌ها اهمیت زیادی پیدا کرده است. یکی از مهم‌ترین انواع حفاظت‌ها که با رشد اینترنت و استفاده از آن و ظهور پدیده‌ای به نام فضای سایبر احساس می‌شود، حفاظت سایبری از زیرساخت‌ها است.

زیرساخت‌های حیاتی

واژه زیرساخت‌های حیاتی معمولاً از سوی دولت‌ها برای توصیف دارایی‌هایی استفاده می‌شود که مدیریت و عملیات ساختارهای اساسی جامعه را ممکن می‌سازد. زیرساخت‌های حیاتی و منابع کلیدی در بخش‌های مختلف شناسایی و معرفی شده است.

- انرژی (الکتریسیته، گاز، بنزین)
- اطلاعات و ارتباطات (ارتباطات راه دور دستگاه‌های اطلاعات جمعی: رادیو و تلویزیون)
- حمل و نقل (کشتیرانی، هوانوردی، حمل و نقل ریلی، حمل و نقل جاده‌ای، حمل و نقل نظامی)
- سلامت (دارو، داروخانه‌ها، شرکت‌های ساخت دارو)
- آب (سدها، ذخایر آبی، شبکه آب‌رسانی)
- پول و بیمه (بانک‌ها، بها بازار، شرکت‌های بیمه)
- دولت و مراکز اداری دولت (دولت، مجلس، مؤسسات دولتی)

– غذا و کشاورزی (تجارت، غذا، کشاورزی)
– رسانه و دارایی‌های فرهنگی (رادیو، انتشارات، بناهای تاریخی و باستانی)

تهدیدات متوجه زیرساخت‌ها در قالب حملات تروریستی فیزیکی یا سایبری، تهدید مصنوعی، بلایای طبیعی، اختلال‌های فناورانه، سوانح، حوادث و غیره دسته‌بندی می‌شود.

وابستگی زیرساخت‌های حیاتی به فضای سایبر

زیرساخت‌ها بر اساس ماهیت و عملکرد به یکدیگر وابسته هستند. وابستگی متقابل زیرساخت‌ها به چهار نوع تقسیم شده است که عبارتند از: وابستگی فیزیکی، وابستگی جغرافیایی، وابستگی منطقی و وابستگی سایبری. با توجه به ساختار زیرساخت‌های مدرن امروزی وابستگی سایبری وجه مشترک وابستگی در همه زیرساخت‌های حیاتی به شمار می‌رود.

وابستگی سایبری عبارت است از حالت یک سامانه که وابسته است به اطلاعاتی که از یک زیرساخت اطلاعاتی تأمین می‌شود. تهدیدهای فضای سایبر کشور، مستقیماً تهدید علیه زیرساخت‌های حیاتی کشور محسوب شده و قادر به ایجاد مخاطره در این زیرساخت‌ها را خواهند داشت.

فضای سایبر و سامانه‌های کنترل صنعتی

سامانه‌های کنترل صنعتی به عنوان هسته اصلی فضای سایبر زیرساخت‌های حیاتی و یکی از مهم‌ترین اجزای آن، اهمیت و اولویت زیادی دارند.

سامانه‌های کنترل دربرگیرنده انواع مختلفی از سیستم‌های کنترلی از جمله سیستم‌های کنترل، نظارت و اکتساب داده‌ها (*SCADA*)، سیستم‌های کنترل توزیع شده (*DCS*) و سیستم‌های کنترلی کوچک‌تر مانند کنترل‌کننده‌های منطقی برنامه پذیر (*PLC*) و واحد پایانه راه دور (*RTU*) است.

الف) سیستم کنترل نظارتی و کسب داده‌ها

این سامانه‌ها بخش مهمی از زیرساخت‌های حیاتی بسیاری از کشورها را پشتیبانی می‌کنند. خطوط لوله نفت و گاز، سیستم‌های جمع آوری فاضلاب، شبکه توزیع، حمل و نقل ریلی و طیف گسترده‌ای از فعالیت‌های صنعتی که در سرتاسر یک منطقه گسترده جغرافیایی پراکنده شده‌اند، توسط این سیستم‌ها کنترل می‌شوند.

اسکادا، فناوری است که کاربر را قادر می‌سازد داده‌ها را از یک یا تعدادی تأسیسات راه دور جمع‌آوری کرده و / یا دستورالعمل‌های محدود کنترلی را به آن تأسیسات ارسال نماید.

ب) سامانه‌های کنترل توزیع‌شده:

این سیستم‌ها زیرمجموعه‌ای از سامانه‌های کنترل صنعتی است که برای کنترل فرایندهای صنعتی از قبیل ایستگاه تولید برق، پالایشگاه‌های نفت، تأسیسات آب و فاضلاب و همچنین در کارخانه‌های شیمیایی، مواد غذایی و صنایع خودروسازی کاربرد دارند؛ بنابراین، معمولاً با کنترل یک فرایند در یک منطقه محدود مرتبط هستند.

ج) کنترل‌کننده‌های منطقی برنامه‌پذیر: *PLC* ها در سامانه‌های کنترل صنعتی به منظور تضمین عملکرد مداوم مطابق با توالی کنترل از پیش تعریف‌شده، بکار گرفته می‌شوند.

د) واحد پایانه راه دور: *PLC* و *RTU* هر دو به یک منظور طراحی و در *ICS* بکار گرفته می‌شوند هر دو وظیفه کنترل و جمع‌آوری داده‌های سایت را انجام می‌دهند.

آسیب‌پذیری سامانه‌های کنترل صنعتی:

بزرگترین تهدید برای سیستم‌های کنترل صنعتی، خرابی های عمدی هدف دار است که در گذشته به صورت حمله فیزیکی به اجزای سیستم کنترل صورت می پذیرفت و هدف آن‌ها مختل کردن عملکرد سیستم بود. حملات سایبری، تکامل طبیعی برای این نوع حمله‌ها می‌باشند که برای مهاجمان ارزان تر و کم خطرتر بوده و تحت اثر فاصله نیستند، در عین حال تکرار و هماهنگی آن‌ها بسیار راحت‌تر است.

در هر دو دسته برخی عوامل زیر منجر به آسیب‌پذیر شدن بیشتر این سیستم‌ها در مقابل حملات سایبری گردیده است:

– ضعف و آسیب‌پذیری فناوری‌های بکار رفته
– ضعف تنظیمات
– ضعف در سیاست‌گذاری

شناسایی آسیب‌پذیری‌ها و سناریوهای مختلف حمله به سیستم‌های کنترل صنعتی و تلاش برای جلوگیری از حمله

با پیشرفت سیستم‌های کنترل صنعتی و استفاده آن‌ها از سکوهای نرم افزاری، سخت افزاری و شبکه‌ای یکسان

و دارای استانداردهای واحد، دسترسی افراد غیرمجاز به لایه‌های درونی این سیستم‌ها امکان‌پذیر شده است. به طور کلی مهاجمی که قصد حمله سایبری و صدمه به یک سیستم کنترل صنعتی را دارد، با دو چالش عمده مواجه است:

۱) شناسائی سیستم، نفوذ و دسترسی به آن
۲) در دست گرفتن کنترل کامل و یا قسمتی از فرآیند و ایجاد صدمه به آن

بنابراین قدم اول در امن کردن سیستم‌های کنترل صنعتی، شناسائی آسیب پذیری‌ها و نقاط دسترسی به آن‌ها می‌باشد که می‌توان آن را در دو زمینه عمده تجهیزات و پروتکل‌های ارتباطی تقسیم‌بندی کرد. تجهیزاتی که در سیستم‌های کنترل صنعتی به کار گرفته می‌شوند به دو دسته تقسیم می‌شوند:

۱) تجهیزاتی که صرفاً در سیستم‌های کنترل مورد استفاده قرار می‌گیرند مانند سنسورها، *PLC* ها، *RTU* ها و ...
۲) تجهیزات فناوری اطلاعات که در دیگر سیستم‌ها و شبکه‌ها نیز استفاده می‌شوند مانند روترها، سوئیچ ها

آسیب پذیری‌های پروتکل‌های ارتباطی و تلاش برای جلوگیری از نفوذ مهاجم

امروزه پروتکل‌های بسیار زیادی در سیستم‌های کنترل صنعتی استفاده می‌شوند. بیشتر این پروتکل‌ها با هدف افزایش کارایی، قابلیت اطمینان در عملیات بلادرنگ و پشتیبانی از الزامات اقتصادی و عملکردی طراحی شده‌اند. متأسفانه اکثر این پروتکل‌ها به جهت بالا بردن کارائی، از هر ویژگی غیرضروری از جمله ویژگی‌های امنیتی نظیر احراز اصالت و رمزنگاری صرف نظر کرده‌اند.

از سوی دیگر بسیاری از آن‌ها برای استفاده از پروتکل اترنت و اتصال به شبکه اینترنت توسعه داده شده‌اند. بنابراین پروتکل‌های ارتباطی سیستم‌های کنترل صنعتی بسیار آسیب پذیر بوده و در معرض حملات زیادی قرار گرفته‌اند.

یکسان‌سازی پروتکل‌های اسکادا منجر به کسب اطلاعات بسیار دقیق مهاجمان از کارکرد و ساختار آن‌ها شده است. به این ترتیب مهاجمان با شناسایی آسیب پذیری‌های این پروتکل‌ها می‌توانند به بسته‌های داده دسترسی پیدا کرده و به دلخواه در آن‌ها تغییراتی ایجاد کنند.

در راستای جلوگیری از ورود غیرمجاز به سیستم تحت حفاظت، دیوار آتش به عنوان راهکار امنیتی پیشنهاد می‌شود.

یکی از وظایف آن ممانعت از ورود پیام‌هایی است که ساختار آن‌ها مطابق با پروتکل ارتباطی ناحیه تحت حفاظت نمی‌باشد. برای جلوگیری از نفوذ مهاجمان در سیستم، وجود سیستم‌های تشخیص نفوذ به همراه دیوار آتش لازم و ضروری است.

البته بهبود این سیستم‌ها وابسته به شناسایی آسیب پذیری شبکه و پروتکل‌های اسکادا می‌باشد. یکی دیگر از راهکارهای رایج در افزایش امنیت پروتکل‌های ارتباطی استفاده از رمزنگاری است. روش‌های سنتی گوناگونی برای رمزنگاری وجود دارد، اما اکثر آن‌ها قابلیت استفاده در سیستم‌های کنترل صنعتی را ندارند.

دلیل این امر، توانایی محاسباتی محدود و سرعت انتقال داده کم اجزای این سیستم‌ها می‌باشد که در عین حال باید پاسخگوی ضرورت عملکرد بلادرنگ نیز باشند. این محدودیت‌ها، اجرای رمزنگاری پیچیده را با مشکل مواجه می‌کنند.

آسیب پذیری تجهیزات کنترلی

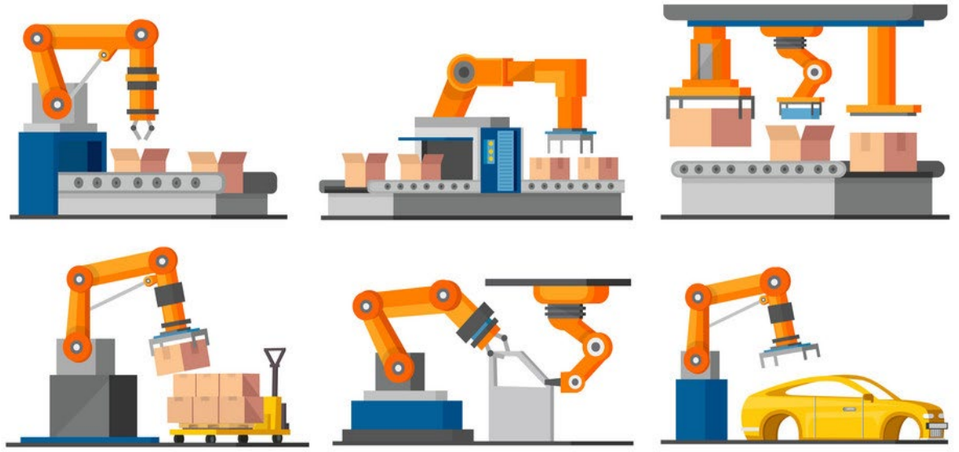
بسیاری از حملات سایبری در سیستم‌های کنترل صنعتی با سوءاستفاده از آسیب پذیری‌های موجود در تجهیزات کنترلی انجام گرفته که یکی از مشهورترین آن‌ها، حمله استاکس نت است. علاوه بر آسیب پذیری‌های نرم افزاری، انواع سخت افزاری و سفت افزاری نیز به شدت مورد توجه کارشناسان امنیت قرار گرفته است.

تهدیدات سایبری در زیرساخت‌های حیاتی

گسترش کاربرد فرآورده‌های فناوری اطلاعات، پذیرش فناوری‌های استاندارد شده و اتصال روزافزون سامانه‌های کنترل صنعتی به سایر شبکه‌ها باعث افزایش قابل توجه سطح تهدیدات سایبری شده است.

این تهدیدات شامل دامنه وسیعی از حملات جهت‌دار، نفوذهای مخرب، هجوم انواع ویروس‌ها، کرم‌ها و سایر بدافزارها و حتی نقص ناخواسته اصول امنیتی در نتیجه اشتباهات انسانی است. برخی از عوامل تهدیدات سایبری کاملاً خارجی و بدون عمد قبلی هستند نظیر خرابی سامانه‌ها در اثر حوادث محیطی، ضعف و آسیب‌پذیری ذاتی سامانه‌ها، اشتباهات اپراتوری در زمان بهره‌برداری از سامانه‌ها، اشتباهات متخصصان تعمیر و نگهداری؛ اما برخی از عوامل کاملاً بر اساس برنامه‌ریزی و به صورت

منسجم عمل می‌کنند. مهم‌ترین منشأ تهدیدات سایبری به ترتیب اهمیت عبارتند از:
دولت‌های متخاصم، مزدوران سایبری یا گروه‌های تحت حمایت پنهان دولت‌های متخاصم، جاسوسان سایبری، تروریست‌های سایبری، مجرمان سازمان‌یافته سایبری، هکرهای دارای انگیزه سیاسی و بدافزارها و ویروس‌ها.



چالش‌های امنیت سامانه‌های کنترل صنعتی

مؤلفه‌های بنیادین سامانه‌های کنترل صنعتی عبارتند از انسان، فرایند و فناوری که باید به طور کامل مورد توجه باشد.

الف) چالش‌های فناوری: شناسایی آسیب‌پذیری‌های مرتبط با فناوری، از چالش‌های مهم محیط‌هایی است که از سامانه‌های کنترل صنعتی برای راهبری فرایندهای صنعتی استفاده می‌کند.
نمونه‌های زیادی از آسیب‌پذیری‌ها مانند انواع کدهای مخرب، افزایش دسترسی از طریق کد نویسی، تجزیه و تحلیل ترافیک شبکه، نفوذ غیرمجاز به شبکه و... وجود دارد که در یک معماری باز قادر هستند از محیط شبکه به درون سامانه‌های کنترل صنعتی منتقل شوند.

از طرف دیگر، علیرغم اینکه *ICS* ها از فناوری‌های معمول *IT* استفاده می‌کنند، نمی‌توان به سادگی از راهکارهای امنیت *IT* در محیط *ICS* استفاده کرد. به طور مثال به دلیل تأثیرگذاری بر این نوع سامانه‌ها استفاده از آنتی‌ویروس و کدهای سیار می‌تواند بسیار مشکل باشد، سامانه‌های قدیمی ممکن است غیرقابل تعمیر باشند. مدیریت وصله در سامانه‌های کنترل صنعتی بسیار

زمان‌بر و بر عملکرد تأثیرگذار هستند.

ب) چالش‌های فرایندی: حداکثر فعالیت سازمان‌ها محدود به نگارش و یا کپی‌برداری از تعدادی دستورالعمل مشابه است. در خوش‌بینانه‌ترین حالت نیز اجرای سامانه مدیریت امنیت اطلاعات *ISMS* در سامانه صنعتی بخش دولتی منجر به تولید چندین جلد سند الزامات و دستورالعمل است که بایستی با توجه به نیاز سازمان طراحی و تدوین گردد.

ج) چالش‌های نیروی انسانی: کمبود نیروی انسانی متخصص در ساختارهای بخش دولتی موضوع قابل توجهی است. مانع عمده، عدم تعهد و همراهی مدیریت ارشد سازمان‌های دولتی با برنامه‌های امنیت است که ناشی از عدم آگاهی و درک اهمیت موضوع است. مقاومت کارکنان در مقابل هرگونه تغییر در فرایندها نیز مانع مهم دیگری است که در این رابطه وجود دارد.

نتیجه‌گیری

از آنجا که زیرساخت‌های حیاتی و تأمین امنیت آن‌ها نقش ویژه‌ای در توسعه و پیشرفت همه جانبه کشور بر عهده دارند، به منظور کاهش آسیب پذیری زیرساخت‌ها، ارتقاء پایداری ملی، حفاظت از مردم و منابع ملی کشور و تضمین استمرار خدمات آن‌ها که از اهداف پدافند غیرعامل می‌باشد با تدوین راهبردهای مناسب می‌توان جهت گیری‌های ملی و کلان را هدایت نمود. چهار سطح راهبردی در ذیل آورده شده است:

مناسب‌ترین راهبردها در چهار سطح فنی تخصصی، انسانی، مدیریتی ساختاری، قانونی نظارتی قضائی

۱) راهبردهای فنی تخصصی:
– حمایت از تولید محصولات ملی و بومی‌سازی تدریجی سیستم‌های کنترل صنعتی
– طبقه‌بندی و حفاظت ویژه از اطلاعات فنی و جغرافیایی زیرساخت‌های حیاتی
– توجه به اصل تولید، توسعه و سفارشی‌سازی فرایندها، استانداردها و پروتکل‌های امنیت سیستم‌های کنترل صنعتی
– تلاش در جهت رفع و یا کاهش آسیب‌پذیری‌ها، امن سازی، مستحکم سازی و تقویت بازدارندگی
– رصد فضای سایبر زیرساخت‌های حیاتی به منظور کشف و مواجهه فعال و پیش کنشگر با تهدیدات سایبری
– کشف و تحلیل روندهای جهانی و شناسایی تهدیدات سایبری زیرساخت‌های حیاتی

۲) راهبردهای انسانی
– ساماندهی و سازمان‌دهی نیروی انسانی متعهد و متخصص
– سازمان‌دهی تیم‌های مدیریت کشف و پاسخگویی به حوادث سایبری و تعامل با سازمان‌های مشابه منطقه‌ای و بین‌المللی
– فرهنگ‌سازی و ارائه آموزش‌های عمومی و تخصصی به ذینفعان و بازیگران
– ایجاد مکانیسم‌های احراز صلاحیت پیمانکاران و مشاورین سایبری زیرساخت‌های حیاتی
– مدیریت دانش حاصل از تجارب اجرای راهبردهای امنیت فضای سایبر زیرساخت‌های حیاتی

۳) مدیریتی و ساختاری
– ایجاد نظام جامع بومی امنیت سیستم‌های کنترل صنعتی
– ایجاد فرایندهای ارتباطی و سازماندهی و هماهنگی بین دستگاهی
– ایجاد مرکز ملی امنیت، حفاظت و نظارت بر زیرساخت‌های حیاتی کشور
– کشف وابستگی متقابل بین انواع زیرساخت‌های حیاتی و شدت و تأثیر آن
– مدیریت مخاطرات فضای سایبر زیرساخت‌های حیاتی
– طبقه‌بندی زیرساخت‌های فیزیکی و اطلاعاتی حیاتی بر اساس سطح اهمیت و شدت تأثیر بر جنبه‌های مختلف حیات

٤) قانونی نظارتی قضائی
– تدوین سیاست‌ها و اصول امنیت فضای سایبر زیرساخت‌های حیاتی
– وضع قوانین و مقررات مناسب کیفری متناسب با اهمیت و نقش زیرساخت‌های حیاتی
– ایجاد فرایند نظارت و ممیزی امنیت سایبری زیرساخت های حیاتی

واکاوی خاموشی‌های سراسری برق در جهان و راهکارهای پدافند غیرعامل

تهیه و تنظیم: رضا خوش رواء کارشناس امریه پدافند غیرعامل

منابع:
الف) دشتی، رضا؛ «واکاوی خاموشی‌های سراسری برق در جهان و راهکارهای پدافند غیرعامل، سازمان پدافند غیرعامل کشور»، (۱۳۹۴)
ب) خبرگزاری ایرنا، خبرگزاری افق و خبرگزاری تسنیم،

مقدمه

اهمیت صنعت برق امروزه بر هیچ‌کس پوشیده نیست. زندگی امروز بشر آنچنان با این صنعت پیوند دارد که نبود آن می‌تواند بر بخش‌های اجتماعی، سیاسی و اقتصادی جوامع اثرات سوء داشته باشد. به همین دلیل قطع برق علاوه بر خسارت بر بخش‌های خانگی، صنعتی، تجاری و کشاورزی می‌تواند به عنوان یک تهدید فرا روی امنیت ملی به حساب آید. از سوی دیگر امروزه قطع برق به عنوان یک آماج با اهمیت از سوی گروه‌های تروریستی و دولت‌های متخاصم برای فلج کردن جوامع استفاده می‌شود لذا شناسایی تهدیدات و اتخاذ راهکارهای مناسب در برخورد با آن‌ها امری ضروری است.

انرژی برق دارای مصارف و نیازهای متنوعی است و نیازهای متعددی از جامع را پاسخ می‌دهد. از جمله این مصارف می‌توان به موارد زیر اشاره نمود:

- مصارف خانگی و تجاری
- روشنایی، گرمایش و سرمایش
- مصارف صنعتی و کشاورزی
- روشنایی، گرمایش و سرمایش، انرژی مکانیکی و کنترل دقیق
- مصارف نظامی
- روشنایی، ارتباطات، انرژی مکانیکی و کنترل دقیق
- مصارف عمومی
- بیمارستان‌ها و...

شبکه‌های انتقال و همچنین نیروگاه‌ها به عنوان دارایی‌های حساس شمرده می‌شوند به طوری که با قطع و اختلال در آن‌ها حجم زیادی از شبکه و حوزه‌های جغرافیایی در خاموشی برق فرو می‌رود. باید توجه داشت انجام تدابیری در شبکه‌های توزیع می‌تواند تأثیر بسزایی بر کاهش اثرات تهدیدات و یا سطح آسیب داشته باشد. اهداف پدافند غیرعامل در شبکه‌های انرژی برق را می‌توان به شرح زیر بیان داشت:

- حفاظت از سرمایه‌ها
- افزایش قابلیت اطمینان برق رسانی به ویژه برای مناطق حیاتی، حساس و مهم
- افزایش کیفیت توان به ویژه برای مصارف حیاتی، حساس و مهم

با توجه به اهداف و مطالب بیان شده، اهمیت شبکه

های انرژی برق از نگاه پدافند غیرعامل به منظور حفظ تداوم تأمین این انرژی مهم در مواقع بحران و مورد توجه بودن این شبکه‌های زیرساختی برای کشور متخاصم و گروه‌های تروریست انکار ناپذیر است.

تهدیدات پیش‌روی صنعت برق

۱- تهدیدات عمدی:

۱-۱- جنگ: قطع برق به عنوان یک رویکرد نظامی در جنگ‌ها مورد استفاده قرار می‌گیرد. از جمله این اقدامات می‌توان به موارد زیر اشاره کرد:

۱- در ۳۰ خرداد ۱۳۹۳ رژیم صهیونیستی جهت مجازات شهروندان فلسطینی در کرانه باختری و اعمال فشار بر آن‌ها جهت همکاری برای پی بردن به سرنوشت سه صهیونیست ربوده شده، برق نوار غزه را به مدت یک هفته قطع نمود.

۲- در هشت سال جنگ تحمیلی عراق علیه ایران، بارها تأسیسات برقی ایران مورد تهاجم قرار گرفت.

۱-۲- حملات تروریستی: یکی از اهداف گروه‌های تروریستی وارد آوردن ضربه‌های سنگین به جامعه و فلج کردن آن است. امروزه قطع برق نیز به عنوان یکی از روش‌های این گروه‌ها برای دستیابی به اهداف خود می‌باشد که در ادامه به چند مورد اشاره می‌گردد:

۱- در ۲ آبان ۱۳۹۲ وزیر برق سوریه از قطعی برق در دمشق در پی حمله تروریستی به پایتخت سوریه خبر داد.

۲- در ۱۴ تیر ۱۳۹۴ ارتش سوریه اعلام کرد دو فرد انتحاری وابسته به گروه تروریستی داعش کامیونی بمب گذاری شده را نزدیک نیروگاه برق شهر «حسکه» واقع در شمال شرق سوریه منفجر کردند.

۳- در ۵ تیر ۱۳۹۴ تروریست‌ها به یک پایگاه وابسته به ارتش ملی الجزایر در منطقه «وادی الشعبه» در فاصله ده کیلومتری استان باتنه در شرق الجزایر حمله کردند. با حمله خمپاره‌ای جمع زیادی از تروریست‌ها کابل‌های برق آسیب دید که در نتیجه برق منطقه قطع شد.

۲- تهدیدات غیر عمدی:

۲-۱- عوامل جغرافیایی: عوامل جغرافیایی و جوی را نیز می‌توان به عنوان یک تهدید برای پایداری برق به حساب آورد. موارد ذیل از جمله مصادیق این بحث هستند.

۱- در ۵ اسفند ۱۳۹۳ مسئولین شرکت برشنا اعلام کردند که به دلیل سرازیر شدن برف در شاهراه سالنگ، خط برق وارداتی از ازبکستان قطع شد و دستگاه‌های تولید

برق موقتاً غیرفعال شدند.

۲- در ۷ دی ۱۳۹۳ برف و یخبندان و سرمای شدید هوا بخش‌هایی از اروپا را در برگرفت. بارش شدید برف در انگلیس باعث شد برق هزاران خانه در این کشور قطع شود.

۲-۲- عوامل فنی: در برخی موارد خاموشی‌های برق ناشی از عوامل فنی است که عمدتاً ناشی از فرسودگی شبکه و یا تقاضای بیش از حد مصرف و یا از کار افتادن یک نیروگاه و... می‌باشد. موارد ذیل از جمله مصادیق این بحث هستند.

۱- در ٦ اسفند ۱۳۹۱ در کشور پاکستان به علت از کار افتادن یک نیروگاه اصلی برق در این کشور بیش از دو ساعت خاموشی سراسری اتفاق افتاد.

۲- در ١٤ اردیبهشت ۱۳۹٤ خط پنج مترو تهران که خط ارتباطی دو کلانشهر تهران و کرج است، به دلیل قطع برق تعطیل شد.

۳- در ۷ تیر ۱۳۹۳ قطع سراسری برق بیشتر بخش‌های ونزوئلا را فراگرفت. توقف فعالیت نیروگاه مرکزی ونزوئلا باعث از جریان خارج شدن دیگر مراکز تولید برق و اختلال در عرضه برق در بخش‌های زیادی از این کشور شد.

راهکارهای پدافند غیرعامل جهت مقابله با پیامد خاموشی سراسری

راهکارهای پدافند غیرعامل در هر دسته تهدید:

در این بخش چند مورد مهم از راهکارهای پدافند غیرعامل به تفکیک هر یک از تهدیدات دارای پیامد خاموشی سراسری ارائه می‌شود:

دسته اول تهدیدات: تخریب و ایجاد عیب در دارایی‌ها

مهم‌ترین راهکار در برابر این تهدید کاهش حساسیت و وابستگی خاموشی سراسری شبکه به یک دارایی خاص و یا به عبارتی کوچک‌سازی و ایجاد پراکندگی در فضای سرزمینی، ملی و استانی است. بدین ترتیب راهکارهای پدافند غیرعامل در دسته اول تهدیدات عبارتند از:

- اصلاح خط مشی مدیریت تولید به توسعه تولید در توزیع
- امکان جزیره سازی شبکه در هنگام وقوع حادثه
- کوچک‌سازی و ایجاد پراکندگی

دسته دوم تهدیدات: استفاده از بمب‌ها و تهدیدات نوین

تهدیدات نوین شامل بمب‌های الکترومغناطیسی، گرافیتی و لیزری است که به ترتیب از طریق ایجاد اضافه ولتاژ، اتصال کوتاه و ایجاد حرارت متمرکز نسبت به تخریب دارایی‌های شبکه اقدام می‌کند. بدین ترتیب راهکارهای پدافند غیرعامل در دسته دوم تهدیدات عبارتند از:

- شیلدینگ تجهیزات کنترلی و الکترونیکی
- کوتینگ و عایق کردن هادی‌ها
- ارتینگ بدنه و تجهیزات و تابلوها و...

دسته سوم تهدیدات: حملات سایبری

پس از پیاده‌سازی اتوماسیون و انجام پروژه‌های هوشمند سازی شبکه، کلیه شبکه صنعت برق به صورت دیجیتالی و کامپیوتری فرمان‌پذیر می‌شوند و با حملات سایبری اطلاعات شبکه قابل برداشت و تغییر خواهد بود.

بدین ترتیب راهکارهای پدافند غیرعامل در دسته سوم تهدیدات عبارتند از:

- طراحی بهینه شارش اطلاعات شبکه با حفظ امنیت آن‌ها و دسترس‌پذیری آن‌ها برای واحدهای اجرایی و تصمیم گیر
- ایجاد شبکه مخابراتی مستقل جهت بهبود امنیت و پایداری سیستم‌های مخابراتی
- ایجاد مقاوم‌سازی سایبری
- مجهزسازی شبکه به سیستم اتوماسیون و هوشمندسازی

دسته چهارم تهدیدات: تحریک مصرف کنندگان به مصرف همزمان

این بخش از جمله تهدیدات مردم محوری است با تحریک مردم نسبت به افزایش ناگهانی مصرف شروع می‌شود و با ضعف‌های شبکه‌ای توسعه می‌یابد. چند روش مقابله با این تهدید عبارتند از:

- توسعه متوازن مراکز تولید
- توسعه متوازن نیروگاه‌ها با بار و متوازن در مناطق جغرافیایی مختلف
- امکان سازی حذف بار
- استفاده از روش‌های حذف بار زیر نوین در زمان وقوع خطا یا عیب

دسته پنجم تهدیدات: شناسایی و ایجاد عیب در نقاط ضعف شبکه

شناسایی نقاط ضعف شبکه یا از طریق برداشت و تحلیل اطلاعات صورت می‌پذیرد و یا با تطمیع عناصر مطلع در سیستم جمع‌آوری می‌شود. بدین ترتیب راهکارهای پدافند غیرعامل در دسته پنجم تهدیدات عبارتند از:

- با از دست رفتن یکی از خطوط و یا پست‌ها شبکه پایدار باقی بماند
- ملاحظات صادرات برق در نظر گرفته شود
- مدیریت بهینه بهره‌برداری از ادوات حفاظتی از جهت تعمیر و تنظیم آن‌ها
- هماهنگی مطمئن بین حفاظت شبکه و تولید

راهبردهای مؤثر در پیاده‌سازی راهکارهای پدافند غیرعامل در راستای پیامد خاموشی سراسری:

با جمع‌بندی راهکارهای پدافند غیرعامل قابل استخراج است. هرکدام از این رویکردها یا جنبه راهبردی دارند یا جنبه عملیاتی. بطوریکه هر یک از راهکارهای پدافند غیرعامل قابل تخصیص به یک رویکرد می‌باشند. در ادامه به تشریح چند مورد از رویکردها پرداخته می‌شود:

• اصلاح رویکرد توسعه شبکه انرژی برق:

به منظور جلوگیری از خاموشی‌های سراسری می‌بایست سیاست‌های توسعه شبکه برق به کوچک سازی و متعدد نمودن نیروگاه‌ها، حذف شبکه انتقال و توسعه تولید در توزیع تغییر کند. البته باید توجه داشت این مهم جز با ایجاد ساز و کارهای توسعه تولیدات پراکنده امکان‌پذیر نیست .

• ساماندهی خصوصی سازی:

جهت ساماندهی خصوصی‌سازی در صنعت برق ابتدا می‌بایست با اصلاح قیمت و سپس مقررات صورت پذیرد. اصلاح قیمت برق باعث بهبود ساز و کارهای سرمایه‌گذاری در بخش تولید و شبکه می‌شود و به کمک اصلاح مقررات می‌توان بخش خصوصی را به سرمایه‌گذاری بخش تولید در توزیع تشویق نمود.

• اصلاح و ارتقاء روش‌های نگهداری شبکه:

نگهداری شبکه و دارایی‌های آن با دو بعد روبرو است. در بعد اول باید وضعیت فیزیکی دارایی‌ها استاندارد باشد که این مهم جز با تعمیر و نگهداری منظم امکان پذیر نیست. بهترین استراتژی تعمیرات شبکه انتقال و تولید استراتژی وضعیت محور است تا بالاترین اطمینان را از سلامت دارایی نتیجه دهد. در بعد دوم می‌بایست بار هر دارایی متناسب با ظرفیت آن بوده و به گونه‌ای باشد که امکان مانور و تأمین اضافه بارهای مقطعی را پاسخگو باشد.

• اصلاح و ارتقاء سیستم حفاظت:

عدم عملکرد صحیح و بهینه سیستم حفاظت می‌تواند یک خاموشی محدود را تبدیل به یک خاموشی سراسری کند. بنابراین لازم است شبکه برق مطالعه مجدد شود و رله‌های حفاظتی بصورت مستمر تنظیم و تعمیر گردد.

• ساماندهی مدیریت بحران:

مدیریت بحران خود دارای ابعاد گسترده‌ای است. اهمیت مدیریت بحران در جلوگیری از خاموشی‌های سراسری است، مهمترین عوامل در مدیریت بحران از نگاه سیستم ایجاد مدیریت و فرماندهی واحد شبکه و از نگاه شبکه افزایش تعداد، ظرفیت و توانایی واحدهای اضطراری استارت سریع و مانور است.

نتیجه‌گیری:

اهمیت روز افزون برق در بخش‌های مختلف جامعه و وابستگی اکثریت قریب به اتفاق فعالیت‌ها به این انرژی باعث می‌شود تا نبود آن اثرات منفی گسترده‌ای در سطح جامعه ایجاد کند. بدین ترتیب قطع برق علاوه بر خسارت بر بخش‌های مختلف می‌تواند به عنوان یک تهدید برای امنیت ملی به حساب آید. از این رو قطع برق از سوی گروه‌های تروریستی و دولت‌های متخاصم به عنوان یک تاکتیک نظامی و راهکار وارد کردن ضربه به شمار می‌رود. بدین منظور راهکارهای پدافند غیرعامل جهت جلوگیری از پیامدهای خاموشی سراسری برق در سطح کشور راهگشا خواهد بود.

۵- از دیگر جنبه‌های جنگ روانی می‌توان دلایل پذیرش و یا نپذیرفتن آن را نام برد. کسانی که تحت دکترین‌ها به تحقیق و تفحص در این موارد همت می‌گمارند باید از گفتن کلمات کلی و انتزاعی بپرهیزند و نیز از طرح مباحث ایدئولوژیک و عمیق دوری کنند زیرا مخاطبین عامی اکثراً دانش فهم آن را ندارند و نمی‌توانند پیام مطلب را درست دریافت کنند برای همین پیام رسانی باید در عین سادگی انجام گیرد، مانند یک ارتباط ساده و معمولی که مردم در کوچه و خیابان با یکدیگر برقرار می‌کنند ولی نقطه تفرق در این است که برای پذیرش و نهادینه کردن از جلوه‌های ویژه و فنون خاص تصویری و یا جابه جایی کلامی در اخبار استفاده می‌شود البته شایان ذکر است که عواطف و عقاید مخاطب نباید مورد تاخت و تاز قرار گیرد. مخاطب تنها باید به تدریج در روند احساساتی‌تر شدن قرار گیرد تا در موقع لزوم طغیان کند و خودش به دست خودش عقایدش را دور بریزد.

پیشگیری و کنترل عفونت در مراقبت‌های بهداشتی هنگام شیوع عفونت کروناویروس جدید (nCoV)

این نسخه راهنمایی در مورد راهبردهای پیشگیری و کنترل عفونت (IPC) در هنگام شیوع عفونت کروناویروس جدید (nCoV-۲۰۱۹) است. راهکارهای *IPC* برای جلوگیری یا محدود کردن سرایت بیماری در مراکز درمانی شامل موارد زیر است:

۱. ایمن سازی تریاژ، تشخیص سریع و کنترل منبع آلودگی (جداسازی بیماران مشکوک به عفونت به *nCoV*).

۲. انجام اقدامات احتیاطی استاندارد برای همه بیماران.

۳. انجام اقدامات احتیاطی تجربی جانبی (قطرات تنفسی و تماس‌ها و اقدامات احتیاطی در مورد هوای تنفسی) برای موارد مشکوک به عفونت *nCoV*.

٤. اجرای کنترل‌های اداری.

۵. استفاده از کنترل‌های زیست محیطی و مهندسی.

۱. ایمن سازی تریاژ، تشخیص سریع و کنترل منبع آلودگی (جداسازی بیماران مشکوک به عفونت به *nCoV*):

• برای تسهیل در شناسایی زود هنگام موارد مشکوک به عفونت *nCoV* مراکز درمانی باید:

– کارکنان مراقبت‌های بهداشتی (*HCW*) را به سطح بالایی از آمادگی تشویق کنید.

– یک ایستگاه تریاژ مجهز در ورودی مراکز درمانی، که توسط کارمندان آموزش دیده پشتیبانی می‌شود ایجاد کنید.

– علائم هشدار دهنده را در مناطق عمومی نصب کنید تا بیماران علامت دار خود را به *HCW* ها معرفی کنند.

۲. ارتقاء بهداشت دست و بهداشت تنفس از اقدامات پیشگیرانه ضروری است:

اقدامات احتیاطی استاندارد شامل بهداشت دست و تنفس، استفاده از تجهیزات محافظت شخصی مناسب (*PPE*) مطابق ارزیابی ریسک، اقدامات ایمنی مربوط به تزریق، مدیریت ایمن زباله، ملافه‌های مناسب، تمیز کردن محیط و استریل‌سازی تجهیزات مراقبت از بیمار است.

اطمینان حاصل کنید که اقدامات بهداشتی تنفسی زیر انجام شده است:

– همه بیماران هنگام سرفه یا عطسه، بینی و دهان خود را با یک پوشش یا آرنج بپوشانند.

– به بیماران مشکوک به عفونت *nCoV*-۲۰۱۹ در حالی که در مکان‌های انتظار عمومی یا اتاق‌های هماهنگی قرار دارند ماسک پزشکی ارائه دهید.

– بهداشت دست را بعد از تماس با ترشحات تنفسی رعایت کنید.

– قبل از انجام هرگونه عملیات تمیز یا آسپتیک، بعد از تماس با مایعات بدن، بعد از تماس با بیمار و بعد از تماس با محیط بیمار، *HCW* ها باید رویکرد «۵ قدم من» برای بهداشت دست‌ها *WHO* را انجام دهند.

– بهداشت دست شامل شستشوی دست با الکل (*ABHR*) یا صابون و آب است.

– شستشوی دست با الکل در صورتی که آلودگی دست‌ها به وضوح قابل لمس نباشند ارجح است.

– در صورتی که دست‌ها به صورت آشکار آلوده هستند آن‌ها را با آب و صابون بشویید.

همچنین استفاده منطقی، صحیح و مداوم از *PPE* به کاهش شیوع پاتوژن‌ها کمک می‌کند. اثربخشی *PPE* کاملاً به منابع کافی و منظم، آموزش کافی کارکنان، بهداشت و رفتار مناسب انسانی بستگی دارد.

مهم است اطمینان حاصل شود که روش‌های تمیز کردن و ضد عفونی محیط به طور مداوم و صحیح دنبال می‌شوند. تمیز کردن سطوح محیطی با آب و مواد شوینده و استفاده از مواد ضد عفونی کننده معمولی (مانند هیپوکلریت سدیم) روش مؤثر و کافی است. وسایل و تجهیزات پزشکی، لباسشویی، ظروف سرویس مواد غذایی و زباله های پزشکی باید مطابق با روال‌های ایمن اداره شوند.

۳. اقدامات احتیاطی تجربی جانبی برای موارد مشکوک به عفونت *nCoV*:

• اقدامات احتیاطی در مورد تماس و قطرات تنفسی:

– علاوه بر رعایت اقدامات احتیاطی استاندارد، کلیه افراد از جمله اعضای خانواده، ملاقات کنندگان و *HCW* باید قبل از ورود به اتاق بیماران *nCoV* مشکوک یا تأیید شده، اقدامات احتیاطی مربوط به تماس و قطرات تنفسی را انجام دهند.

– بیماران باید در اتاق‌های جداگانه با تهویه مناسب قرار

بگیرند. برای اتاق‌های بخش عمومی که دارای تهویه طبیعی هستند، تهویه کافی برای هر بیمار ۶۰ لیتر در ثانیه در نظر گرفته شده است.

– وقتی اتاق‌های جداگانه در دسترس نباشند، بیمارانی که مشکوک به *nCoV* هستند باید در کنار هم گروه‌بندی شوند.

– تختخواب همه بیماران باید حداقل ۱ متر از هم جدا شوند.

– در صورت امکان، تیمی از *HCW* باید به طور انحصاری وظیفه مراقبت از بیماران مبتلا را برعهده گیرند تا خطر سرایت بیماری کاهش یابد.

– *HCW* ها باید از ماسک پزشکی استفاده کنند.

– *HCW* ها باید از محافظ چشم (گوگل) یا محافظ صورت (سپر صورت) برای جلوگیری از آلودگی غشاهای مخاطی استفاده کنند.

– *HCW* ها باید از لباس تمیز و آستین بلند استفاده کنند.

– *HCW* ها همچنین باید از دستکش استفاده کنند.

– در هنگام مراقبت‌های روتین استفاده از چکمه، پوشش و پیش بند مورد نیاز نیست.

– پس از مراقبت از بیمار باید همه تجهیزات محافظت شخصی کنده و دفع مناسب و بهداشت دست انجام شود.

– تجهیزات، یکبار مصرف یا اختصاصی باشند.

– اگر نیاز به استفاده از تجهیزات بین بیماران وجود دارد، بین استفاده برای هر بیمار جداگانه آن را تمیز کرده و ضد عفونی کنید.

– *HCW* ها باید از دست زدن به چشم، بینی یا دهان خود با دستکش‌های آلوده یا دست‌های برهنه خودداری کنند.

– از جابجایی و حمل و نقل بیماران به بیرون از اتاق یا محل خود خودداری کنید مگر اینکه از نظر پزشکی ضروری باشد. از تجهیزات پرتوی ایکس قابل حمل و/ یا سایر تجهیزات تشخیصی تعیین شده استفاده کنید. در صورت نیاز به حمل و نقل، از مسیرهای حمل و نقل از پیش تعیین شده استفاده کنید تا قرار گرفتن در معرض دید کارمندان، سایر بیماران و ملاقات کنندگان به حداقل برسد و همچنین برای بیمار از ماسک طبی استفاده کنید.

– اطمینان حاصل کنید که *HCW* هایی که بیماران را حمل می‌کنند بهداشت دست را رعایت کرده و *PPE* مناسب به تن می‌کنند.

– هرچه زودتر قبل از رسیدن بیمار اطرافیان را در مورد هرگونه اقدامات احتیاطی لازم در مورد بیمار آگاه کنید.

– مرتباً سطحی را که بیمار در تماس است، تمیز و ضد عفونی کنید.

– تعداد *HCW* ها، اعضای خانواده و بازدید کنندگان در تماس با بیمار مشکوک به *nCCV*-۲۰۱۹ تأیید شده را محدود کنید.

– سوابق مربوط به کلیه افرادی که وارد اتاق بیمار می شوند، از جمله کلیه کارمندان و بازدید کنندگان را حفظ کنید.

٤. اجرای کنترل‌های اداری:

کنترل‌ها و سیاست‌های اداری برای جلوگیری و کنترل انتقال عفونت *nCoV*-۲۰۱۹ در محیط مراقبت‌های بهداشتی شامل موارد زیر است، اما محدود به این‌ها نیست: ایجاد زیرساخت‌ها و فعالیت‌های *IPC* پایدار؛ آموزش همراهان بیماران؛ تدوین راهکارهایی برای تشخیص سریع عفونت ناشی از *nCoV*-۲۰۱۹؛ حصول اطمینان از دسترسی سریع به آزمایشگاهی برای شناسایی عامل بیماری؛ جلوگیری از ازدحام جمعیت به ویژه در بخش اورژانس؛ تأمین محل انتظار ویژه برای بیماران مشکوک؛ قرنطینه مناسب بیماران بستری؛ تضمین منابع کافی *PPE*؛ اطمینان از پیروی از سیاست‌ها و رویه‌های *IPC* برای همه جنبه‌های مراقبت‌های بهداشتی.

اقدامات اداری مربوط به کارکنان مراقبت‌های بهداشتی:

– آموزش کافی برای *HCW* ها.

– اطمینان از نسبت کافی بیمار به کارکنان.

– ایجاد فرآیند نظارت بر عفونت‌های حاد تنفسی ناشی از *nCoV* در بین *HCW* ها.

– اطمینان از اینکه *HCW* و مردم اهمیت مراقبت‌های پزشکی را درک می‌کنند.

– نظارت بر رعایت اقدامات احتیاطی استاندارد توسط *HCW* و ارائه مکانیسم‌های بهبود در صورت لزوم.

۵. استفاده از کنترل‌های محیطی و مهندسی:

این کنترل‌ها زیرساخت‌های اساسی مرکز مراقبت‌های بهداشتی را دربرمی‌گیرد. این کنترل‌ها با هدف اطمینان از تهویه مناسب در کلیه مناطق در مرکز بهداشت و همچنین تمیز کردن کافی محیط انجام می‌گیرد. علاوه بر این، فاصله مکانی حداقل ۱ متر باید بین تمام بیماران حفظ شود. جداسازی مکانی و تهویه مناسب کمک کننده است. باید فرایندهای تمیز و ضد عفونی کردن به طور مداوم و صحیح انجام می‌شوند.

آسیب‌پذیری

آسیب‌پذیری‌های چندگانه اجرای کد دلخواه در مرورگر گوگل کروم

آسیب‌پذیری‌های چندگانه جدید در گوگل کروم کشف شده است که شدیدترین آن‌ها می‌توانند باعث اجرای کد دلخواه بر روی سیستم هدف شوند. سوءاستفاده موفقیت‌آمیز از شدیدترین این آسیب‌پذیری‌ها می‌تواند به مهاجمان اجازه دهد کد دلخواه خود را در مرورگر سیستم قربانی اجرا کنند. بسته به دسترسی‌های داده شده به برنامه، مهاجم می‌تواند اقدام به نصب برنامه، بازدید یا تغییر در اطلاعات موجود یا حتی ایجاد حساب‌های کاربری جدید نماید. اگر در تنظیمات و پیکربندی به نکات امنیتی توجه شود، حتی سوءاستفاده از شدیدترین این آسیب‌پذیری‌ها نیز تأثیر کمتری را نسبت به حالت تنظیمات پیش‌فرض خواهد داشت.

نسخه آسیب‌پذیر این برنامه مربوط به نسخه‌های قبل از ۸۰,۰,۳۹۸۷,۱۱۶ گوگل کروم می‌شود. این آسیب‌پذیری‌ها می‌توانند در صورت مراجعه یا تغییر مسیر دادن کاربر به یک صفحه وب ساختگی خاص، مورد بهره‌برداری قرار گیرند.

بهره‌برداری موفقیت‌آمیز از شدیدترین این آسیب‌پذیری‌ها می‌تواند به مهاجمان اجازه دهد کد دلخواه را در متن مرورگر اجرا کنند، اطلاعات حساس را بدست آورد، محدودیت‌های امنیتی را دور بزنند و کارهای غیرمجاز انجام دهند یا باعث منع از سرویس شوند.

توصیه می‌شود اقدامات زیر انجام شود:

- بلافاصله پس از آزمایش مناسب، وصله مناسب ارائه شده توسط گوگل به سیستم‌های آسیب‌پذیر اعمال شود.
- برای کاهش اثر حملات موفقیت‌آمیز، همه نرم‌افزارها را به عنوان یک کاربر با سطح دسترسی پایین اجرا کنید.
- تذکر به کاربران برای بازدید نکردن وب‌سایت‌هایی با منبع نامعتبر و همچنین دنبال نکردن لینک‌های ناشناس.

آسیب پذیری اجرای کد از راه دور در ZyXEL NAS

شرکت *Zyxel* اعلام کرد که یک آسیب پذیری در دستگاه ذخیره ساز متصل به شبکه یا *NAS* کشف کرده است که به مهاجم اجازه می‌دهد تا از راه دور و بدون احراز هویت کدهای مخرب را در دستگاه آسیب پذیر اجرا کند.

کد بهره برداری از این آسیب پذیری به صورت عمومی منتشر شده است. دستگاه‌های *ZyXEL NAS* با استفاده از برنامه *weblogin.cgi* احراز هویت انجام می‌دهند. آسیب پذیری در این برنامه که در قسمت وارد کردن نام کاربری وجود دارد باعث می‌شود که مهاجم بتواند کاراکترهای خاصی را در این قسمت وارد کند و به این ترتیب کدهای مخرب را از این طریق به دستگاه تزریق کند. با اینکه در این حالت وب سرور با دسترسی *root* فعال نیست ولی مهاجم می‌تواند با تنظیم *uid* دسترسی خود را به کاربر *root* تغییر دهد و با بالاترین سطح دسترسی کدهای دلخواه خود را اجرا کند.

به طور کلی دستگاه‌های *NAS* که نسخه *firmware* آن ها ۵,۲۱ و قبل از آن می‌باشد آسیب پذیر هستند. *ZyXEL* برای مدل‌های زیر به‌روز رسانی منتشر کرده است بنابراین به کاربران این مدل از *NAS* ها توصیه می‌شود تا هرچه سریع‌تر این به‌روز رسانی را نصب کنند:

- *NAS326*
- *NAS520*
- *NAS540*
- *NAS542*

اما *ZyXEL* برای تعدادی از مدل‌هایش به‌روز رسانی منتشر نکرده است چون دیگر از این مدل‌ها پشتیبانی نمی کند. بنابراین به کاربران این مدل از *NAS* ها توصیه می‌شود تا در صورت امکان دسترسی این تجهیزات از اینترنت را قطع کنند و یا برای امن‌سازی، آن را در پشت فایروال قرار دهند.

مهمترین به‌روزرسانی‌های ماه جاری شرکت‌های تولید کننده سخت افزار و نرم افزار

شرکت *Cisco* از وجود ضعفی «حیاتی» در محصول *Cisco Smart Software Manager On-Prem* پرده برداشته که بهره‌جویی از آن مهاجم را قادر به دسترسی یافتن به بخشی حساس از سیستم می‌کند. *SSM* ابزاری برای مدیریت لیسانس و کلیدهای فعالسازی محصولات Cisco است.

SSM On-Prem حاوی یک حساب کاربری سیستمی است که با رمز عبور پیش‌فرض و ایستای تخصیص داده شده به آن دسترسی به بخشی حساس از سیستم را فراهم می‌کند.

Cisco این باگ را در نسخه ۷-۲۰۲۰۰۱ محصول *SSM On-Prem* ترمیم کرده است. دستگاه‌هایی که از نسخ قبلی استفاده می‌کنند همگی دارای رمز ایستای اشاره شده در این مطلب هستند.

لازم به ذکر است که سیستم‌های *SSM On-Prem* تنها زمانی آسیب‌پذیر هستند که قابلیت *High Availability* – به اختصار *HA* – بر روی آن‌ها فعال شده باشد. بر طبق توضیحات سیسکو این قابلیت به‌صورت پیش‌فرض فعال نیست.

این شرکت همچنین ٦ آسیب‌پذیری با درجه حساسیت «بالا» را در محصولاتی که از آن‌ها تأثیر می‌پذیرند ترمیم کرده است.

شرکت *Siemens* آسیب‌پذیری از نوع «منع سرویس» را در برخی محصولات خود ترمیم کرد. در صورت فعال بودن قابلیت «ارتباط رمزگذاری شده» روی دستگاه آسیب‌پذیر، مهاجم قادر خواهد بود تا با ارسال یک پیام دستکاری‌شده به آن در بستر شبکه، موجب از کاراندازی سرویس شود.

نسخ ۷,۳ و ۸.۱ به‌ترتیب در محصولات *SIMATIC WinCC* و۷ *SIMATIC PCS* به دلیل عدم وجود قابلیت «ارتباط رمزگذاری شده» در آن‌ها به این ضعف امنیتی آسیب‌پذیر نیستند .

دیگر آسیب‌پذیری «منع سرویس» ترمیم‌شده، ضعفی است که خانواده پردازنده‌های *CPU* بکار رفته در تجهیزات *SIMATIC S*۷ از آن تأثیر می‌پذیرند.

همچنین در محصولاتی از این شرکت که در آن‌ها از نسخ قبل از ۰٦,۰۰ پشته در *Profinet-IO* استفاده شده نیز وجود ضعفی از نوع «منع سرویس» گزارش شده که در اصلاحیه‌ها ترمیم و اصلاح شده است.

Siemens دو ضعف امنیتی دیگر را در چندین محصول صنعتی خود ترمیم کرده که هر دوی آن‌ها از نحوه مدیریت پیام‌های *SNMP* در این محصولات ناشی می‌شوند.

این شرکت اشکالی را نیز در خانواده پردازنده‌های *CPU* محصولات *S*۷-۱۵۰۰ ترمیم کرده است.

شرکت *Adobe* برای رفع دو آسیب‌پذیری بحرانی در برنامه‌های *After Effects* و *Media Encoder*، به‌روزرسانی‌های نرم‌افزاری را منتشر کرد.

این دو آسیب‌پذیری، ناشی از نقص بحرانی نوشتن در حافظه است که با اجرای کد دلخواه بر روی سیستم قربانی و فریب وی از طریق باز کردن یک فایل مخرب با استفاده از نرم‌افزارهای مذکور، می‌توانند مورد اکسپلویت قرار گیرند.

گوگل به‌روزرسانی جدیدی برای مرورگر کروم برای کاربران دسکتاپ منتشر کرده است. نسخه جدید این مرورگر(۸۰,۰,۳۹۸۷,۱۲۲) سه آسیب‌پذیری مهم را برطرف می‌کند که یکی از آن‌ها با شناسه ٦٤١٨-۲۰۲۰-*CVE* توسط مهاجمان نیز مورد بهره‌برداری قرار گرفته بود.

شرکت مایکروسافت اخیراً وصله امنیتی را برای تمامی نسخه‌های *Microsoft Exchange* انتشار داده است که این وصله امنیتی یک نقص اجرای کد از راه دور *(RCE)* را مرتفع می‌سازد. این نقص به مهاجم این امکان را می‌دهد تا با ارسال *payload* دستکاری شده بتواند دستورات خود را در سرور اجرا کند.

این آسیب پذیری بر روی *Exchange Control Panel* تاثیرگذار خواهد بود و در تمامی نسخه‌های *Exchange Server* به دلیل داشتن کلید اعتبارسنجی و الگوریتم یکسان بر روی فایل *web.config* صدق می‌کند. آسیب پذیری به‌صورت *authenticated* است و مهاجم برای اجرا، نیازمند اطلاعات ورود به یک حساب کاربری می‌باشد.

معرفی کتاب حوزه پدافند زیستی

کتاب حاضر نتیجه یک پروژه تحقیقاتی مشترک در زمینه امنیت زیستی محصولات کشاورزی با حمایت مالی سازمان ناتو است که هیئت مشاوره امنیت زیستی این سازمان آن را بسیار مثبت ارزیابی کرده است.

تیمی از دانشمندان به رهبری پروفسور لودویکا گالینو پروژه مشترکی را در زمینه امنیت زیستی محصولات کشاورزی پیشنهاد کردند که ناتو آن را فرصتی مهم برای افزایش سطح آگاهی درباره تهدیدهای احتمالی فراروی تولید محصولات کشاورزی و مواد غذایی به علت استفاده از بیماری‌زاهای گیاهی به عنوان سلاح‌های بیولوژیکی قلمداد کرد.

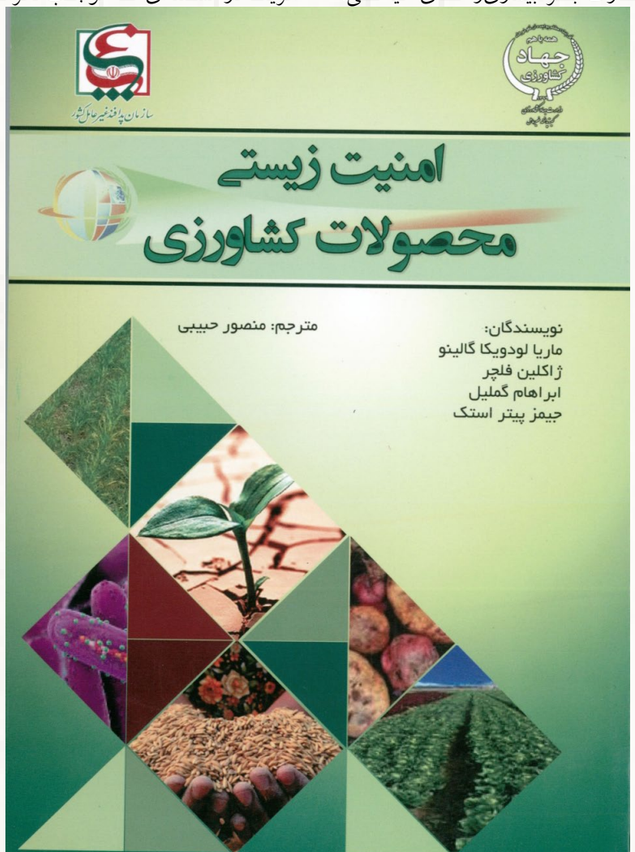
اهداف این پروژه (ابزارهای تشخیصی مبتکرانه، پروتکل‌هایی برای نظارت بر بیماری‌زاهای گیاهی، روش‌های ریشه‌کنی و سیستم‌های اخطار سریع) جاه‌طلبانه و همچنین منطبق بر سطح مهارت فنی تیم‌های تحقیقاتی مشارکت‌کننده (از جمله دانشمندانی از مصر، اسراییل، ایالات متحده، و البته ایتالیا) بود.

اثر حاضر نتیجه کاری است که پروفسور گالینو و همکارانش به ثمر رسانده‌اند. در کتاب حاضر نقش امنیت زیستی محصولات کشاورزی تشریح شده؛ پیامدهای بیماری‌زاهای گیاهی بر تولید و امنیت محصولات کشاورزی تبیین گشته و وضعیت امنیت محصولات کشاورزی در سطوح محلی، منطقه‌ای و جهانی تجزیه و تحلیل شده است.

همچنین، نویسندگان این کتاب منابعی را برای ایجاد فرصت‌های همکاری بیشتر و منابع مرتبطی را نیز برای حمایت مالی احتمالی تهیه کرده‌اند. در مجموع، این کتاب ابزار مفیدی برای کسب آگاهی بیشتر در زمینه امنیت محصولات کشاورزی و همچنین شناخت شیوه‌های احتمالی انجام تحقیقات و تحلیل این مسئله خواهد بود.

کتاب حاضر روایتی از یک تجربه موفق است که با همکاری مؤثر دانشمندانی از اروپا، منطقه مدیترانه و شمال افریقا در مسئله‌ای که موجب نگرانی کشورها و دانشمندان بخش‌های مختلف دنیا شده، با قرار گرفتن در عصر بی‌ثباتی فزاینده و محدودیت منابع، به ثمر نشسته است.

این حقیقت که سازمانی همچون ناتو تحقیقاتی بین‌المللی را در زمینه امنیت و ایمنی محصولات کشاورزی ترویج می‌کند، نشان می‌دهد که مؤلفه‌های مختلف جامعه مدرن معلومات اندکی در خصوص این مفاهیم دارند.



طرح‌های کسر خدمت سربازی

به اطلاع می‌رساند که سازمان پدافند غیرعامل کشور (مرکز مطالعات پدافند غیرعامل کشور و مرکز مطالعات فنی و مهندسی پایداری ملی کشور) برای دانش‌آموختگان و فارغ‌التحصیلان مقاطع کارشناسی ارشد و دکتری طرح‌هایی برای کسر خدمت سربازی و نخبگی (جایگزین خدمت سربازی) در نظر گرفته است. علاقمندان می‌توانند علاوه بر مراجعه به وب‌سایت‌های مربوطه با مراجعه به اداره کل پدافند غیرعامل استانداری آذربایجان شرقی از روند ثبت‌نام مطلع شوند.

وب سایت مرکز مطالعات فنی و مهندسی پایداری ملی کشور: http://www.mafpa.ir

وب سایت مرکز مطالعات پدافند غیرعامل کشور: http://www.pdrc.ir

سایت های مرتبط با پدافند غیرعامل

وب سایت پایداری ملی
http://www.paydarymelli.ir

مرکز مطالعات پدافند غیرعامل
http://www.pdrc.ir

استانداری آذربایجان شرقی – پدافند غیرعامل
http://www.ostan-as.gov.ir/Page/٤٢/

پلیس فتا
http://www.cyberpolice.ir

مرکز مطالعات فنی و مهندسی پایداری ملی
http://www.mafpa.ir