پرونده ویژه پدافند سایبری

مدیرمسئول: سرتیپ پاسدار دکتر غلامرضا جلالی

جانشین مدیرمسئول: مهندس محمدرضا فرجی پور

سردبیر: ابوالقاسم رحمانی

تحریریه: محمد اسکندری، جواد غریبی، امیر عطاالله مقدمی
زهرا عدالت فر، زهرا طیبی و زینب مرزوقی

مدیر هنری: ابوالقاسم رحمانی

طراحی و صفحه‌آرایی: علی میرزاجعفری و راحله مظهری

ویراستاری: سیده معصومه معاف رودپیشی

اطلاعات تماس

تلفن: ۰۲۱۶۶۵۸۱۱۹۷

کد پستی: ۱۶۷۱۸-۳۸۷۳۱

صندوق پستی: ۱۵۱۴۷۴۷۷۱۱

ایمیل: Info@paydarymelli.ir

نشانی: تهران، بزرگراه شهید قاسم سلیمانی، خیابان استاد حسن بنا
شمالی، نبش کوچه شهید علی بخشی، موقعیت سلمان فارسی

تهیه و تدوین در روابط عمومی و امور بین‌الملل و مرکز آفرینش‌های هنری فاطر

فهرست

در مقابل شیوه‌های پیچیده تهاجم دشمنان، پدافند غیرعامل نیز باید کاملا هوشیار و جدی باشد و به‌صورت علمی، دقیق، به‌روز و همه‌جانبه عمل و با هرگونه نفوذ مقابله کند.

رهبر معظم انقلاب اسلامی در دیدار رئیس و مسئولان سازمان پدافند غیرعامل

۶ آبان ۱۳۹۷

ما کجا ایستاده‌ایم؟

سرتیپ پاسدار دکتر غلامرضا جلالی، رئیس سازمان پدافند غیرعامل کشور

گفت‌وگوی نخست این پرونده ویژه که به مناسبت هفته پدافند غیرعامل آماده شده با سردار جلالی رئیس سازمان پدافند غیرعامل کشور است. این که ما در مسائل مربوط به این حوزه کجا ایستاده‌ایم مسیر پیش‌رو چیست و چقدر برای آن آمادگی داریم و ... خصوصا در زمینه‌های سایبری مجموعه مسائلی است که حول آنها گپ زدیم، با هم بخوانیم.

در میان فرصت‌ها و تهدیدهای فضای سایبری، ما کجا ایستاده‌ایم؟

ما می‌خواهیم مدخل بحث را در سطح راهبردی در حوزه پدافند سایبری پیش ببریم. ازنظر شما، سازمان پدافند غیرعامل و حوزه پدافند سایبری ناظر به وضع موجود دنیا، کشورهای مختلف و تهدیدهایی که در فضای سایبری وجود دارد، چقدر دارای اهمیت است و در حوزه راهبردی چه اهدافی برای آن تهیه و تدوین شده‌اند و روی چه ریلی قرار است پیش برود؟ آمادگی‌های پیشینی چه بوده‌اند و ناظر به پیشرفت‌ها جایگاه و وضعیت ما چطور است؟

از منظر فناوری، فناوری سایبری که به‌تدریج توسعه می‌یابد با فناوری‌های دیگر ممزوج می‌شود و فناوری غالبی را ارائه می‌دهد. بعضی معتقد بودند فضای سایبری مساوی با فضای IT است، یعنی وقتی از فضای سایبری صحبت می‌کردیم، خیلی‌ها می‌گفتند همین IT است. اما IT بدون استفاده از فناوری دیگری به نام CT (communication technology) که موضوع ارتباطات است معنا ندارد. موضوع فنا.ری اطلاعات به انتقال اطلاعات از طریق امواج، فیبر نوری، سیم و کابل، لیزر و انواع مختلف محیط ها مربوط می شود، وزارت ارتباطات را به نام ICT می‌شناسند که IT + CT است، حوزه الکترونیک نیز با این دو حوزه ممزوج است. وقتی شبکه‌های اجتماعی و محتوا هم به میدان بیایند، وضعیت پیچیده تر می شود.

شبکه های اجتماعی به‌عنوان social media که زیست بوم زندگی جاری و آینده بشر است، چند قالب کلی را شکل می‌دهد که شامل زیرساخت، محتوا و مباحث دیگر است. بنابراین این هم یک حوزه دیگر است که به موارد قبلی اضافه می‌شود. امروز هم در نگاهی به شبکه‌های اجتماعی شاید جنبه مهم آن، بیشتر رسانه‌ای باشد تا جنبه سایبری، یعنی وسیله و ابزار نسبت به قابلیتی که بروز می‌دهد بروز و ظهور ندارد. وقتی محتوا شامل داده های حجیم مطرح گردید، بحث داده‌کاوی و پردازش و تحلیل داده و موضوع هوش مصنوعی هم به میدان آمد.

شاید بتوان اینطور گفت که از حیث فنی، تا اندازه‌ای فضای سایبری تلفیق حوزه الکترومغناطیس و الکترونیک است. هرقدر این پدیده جلو می‌رود، هم کارکردها بسیار متنوع می‌شود، هم خدمات بسیار زیاد می‌شود. یک روزی شاید می‌شد تصور کرد که می‌توان بدون اینها زندگی کرد، اما امروزه چنین چیزی ممکن نیست. به‌واقع مفهوم محوری تحلیل این اتفاق، زیرساخت‌های نرم است. الگوهای زندگی اجتماعی به‌نحوی تغییر کرده که با یک بررسی در ۱۰ سال گذشته مفهومی به نام Soft infrastructure اهمیت می‌یابد، یعنی هنگامی‌که در شهرهای مدرن نگاه می‌کنیم از ۵۰ زیرساخت ۳۸ زیرساخت جزء زیرساخت نرم و مبتنی‌بر فضای سایبری‌اند. به‌تعبیری امروز غلبه زیرساخت‌ها بر زندگی مردم، از طریق زیرساخت‌های سایبری و فضای الکترونیک و نرم است که انجام می‌گیرد. دیگر نمی‌توان به تفکرات و نگاه گذشته توجه کرد و باید از آن عبور کرد.

طبیعتا این فضا، خدمات و فرصت هایی دارد و درکنار این موارد مخاطرات و تهدیدات هم دارد. هیچ‌فناوری بدون‌تهدیدی وجود ندارد. فناوری‌ای که به شما قدرت اشراف بر دیگران را می‌دهد، روی دیگرش این است که دیگرانی که شما را تهدید می‌دانند، می‌توانند مثلا با فناوری سنجش از راه دور کشور ما را رصد کنند. این برای ما تهدیدزاست. این فناوری در ذات خود برای کشور صاحب فناوری فرصت و برای ما تهدید است، بنابراین یک مقوله

بسیار اساسی تهدیدها هستند. وقتی وارد این حوزه می شوید، وقتی ۳۸ زیرساخت مبتنی بر زیرساخت نرم و فضای سایبری داشته باشید، مثل خدمات آبرسانی، برق رسانی، خرید، فروش، مطالعه، رادیو، تلویزیون، تأسیسات شهری و...، تقریبا تمام زندگی شما همین هاست و چیز دیگری نیست. اینها در عین اینکه فرصت زیست راحت تر را در جوامع فراهم می کنند، می توانند در دسته تهدیدها هم طبقه بندی شوند، به زبانی ساده ما درکنار فرصت ها بروز تهدیدها را داریم، مثلا وقتی می توانید در خانه هوشمند و شهر هوشمند، شهر و خانه و زیرساخت ها را متناسب با خواست خود برنامه ریزی کنید، تحت فرمان قرار دهید و از راه دور کنترل کنید، طبیعتا دشمنان و مهاجمان نیز می توانند از راه دور ورود کنند و به آن محل های ورود بروند و تهدید درست کنند، بنابراین تهدید و فرصت با هم به صورت ترکیبی وارد زندگی می شوند. عقلانی اش این است که از تهدید، پرهیز و با آن مقابله کنید و از فرصت استفاده حداکثری کنید. توصیه نمی شود به خاطر مخاطرات فرصت ها را رها شوند، باید استفاده شوند و عقل هم ایجاب نمی کند خود را به خاطر فرصت ها کاملا در اختیار دشمن و تهدیدهای آن قرار دهید، پس رویکرد ما استفاده هوشمندانه از فناوری های فضای سایبر، استفاده حداکثری از همه قابلیت ها و همه فرصت ها درکنار شناسایی، کنترل، مدیریت و کاهش مخاطرات و مقابله با تهدیدهاست که بتوانیم در فضای موجود هم از قابلیت ها استفاده کنیم و هم از تهدیدها پرهیز کنیم.

عقلانی اش این است که از تهدید، پرهیز و با آن مقابله کنید و از فرصت استفاده حداکثری کنید. توصیه نمی شود به خاطر مخاطرات فرصت ها را رها شوند، باید استفاده شوند و عقل هم ایجاب نمی کند خود را به خاطر فرصت ها کاملا در اختیار دشمن و تهدیدهای آن قرار دهید، پس رویکرد ما استفاده هوشمندانه از فناوری های فضای سایبر، استفاده حداکثری از همه قابلیت ها و همه فرصت ها درکنار شناسایی، کنترل، مدیریت و کاهش مخاطرات و مقابله با تهدیدهاست که بتوانیم در فضای موجود هم از قابلیت ها استفاده کنیم و هم از تهدیدها پرهیز کنیم

این الگو به شما دو رویکرد می دهد:

یکی اینکه از این فناوری ها چطور باید استفاده کنیم. وقتی فناوری ها وارد کشورها می شوند در ذات خود استراتژی تهدید نهفته دارند. در فضای سایبری چند ویژگی برای فناوری ها وجود دارد:

اول: اینکه معمولا فناوری ها کنترل گریزند.

درون رگولاتور هستند، یعنی در فناوری شبکه اجتماعی رگولاتور داخل خود آنهاست. مشاغل، کار و شغل که درست می کنید رگولاتور داخل خود آنهاست.

دوم: حاکمیت گریزند، یعنی در کنترل دولت ها قرار نمی گیرند. یک نگاه جهانی و متصل شدن دنیا به

همدیگر بالای سر آنهاست، مثلا مقیاس شبکه‌های اجتماعی قاره‌ای است، نه مقیاس شهری و میدانی. به‌عبارت دیگر ۱۵-۱۰ کشور با هم کار کنند تا صرفه اقتصادی داشته باشد، بنابراین همه کشورها تحت‌تأثیر قرار می‌گیرند.

سوم: تا اندازه‌ای غیرملی هستند، یعنی متمرکز بر منافع ملی یک کشور نیستند، متمرکز بر منافع عمومی‌اند و متمرکز بر منافع توسعه‌دهندگان و صاحبان فناوری هستند، بنابراین این ویژگی‌ها که بعضی خوب و بعضی بدند، بالاخره کشورها را تحت‌تأثیر قرار می‌دهد. هر کشوری وقتی کشور می‌شود، یعنی حکمرانی خاص برای خود دارد. این کشور با آن کشور چرا یکی نمی‌شوند؟ چون الگوی حکمرانی متفاوت دارند، ارزش‌هایشان با هم متفاوتند، نظام، مردم و حوزه‌های اجتماعی‌شان با همدیگر متفاوتند.

رویکرد دیگر درنظر گرفتن تهدیدهاست. وقتی کسی می‌خواهد با فناوری سایبری همه را یکی کرده و خود کنترل کند با منافع این کشورها در تضاد قرار می‌گیرد. این تضاد در کشورهای اروپایی هم وجود دارد، مثلا سخنرانی‌های خاصی که مکرون، رئیس‌جمهور فرانسه راجع به فضای سایبری و اینترنت چینی و آمریکایی ایراد کرد و اینکه تسلط دنیا روی این حوزه شکل می‌گیرد و او نگرانی‌هایی از آشوب‌های اجتماعی سال گذشته در پاریس داشت، نشان می‌داد فضای اینترنت و سایبر در کنترل کشور نیست، بلکه علیه کشور است. اینها نگرانی‌هایی است که درست می‌شوند، بنابراین هر کشوری بخواهد ارزش‌ها و اصول خود را حفظ کند باید بتواند امنیت برقرار کند، باید بتواند. در این جهان بدون‌مرز سایبری مرز ملی خود را تعریف کند که چند کشور این کار را کرده‌اند. این امر هم ذهنیت ملی می‌خواهد و هم ذهنیت فنی. وقتی مفهومی به نام سرزمین یا قلمرو تعریف می‌کنیم، سرزمین جغرافیا دارد. جمهوری اسلامی ایران همین نقشه موجود کشور است و یک جغرافیا دارد. وقتی می‌خواهیم قلمروی سرزمینی خود را در فضای سایبری برای جمهوری اسلامی تعریف کنیم و بگوییم ایران سایبری کجاست، قاعده طور دیگری است. علوم استراتژیک و راهبردی باید به کمک فضای سایبری بیایند و قلمروی ملی را در فضای سایبری تعریف کنند که اگر این کار را نکنیم نمی‌توانیم از آن فضا حفاظت کنیم. برخی کشورها توانسته‌اند این کار را انجام دهند و برخی کشورها عقب‌مانده و تابعند و در واگنی نشسته‌اند که آن واگن متصل به ریل آمریکایی‌هاست و به هر سمتی که آنها بخواهند کشانده می شوند و اراده‌ای از خود ندارند.

ایران سایبری کجاست؟

در این محدوده سرزمینی که اشاره کردید، ما کجا قرار می‌گیریم؟ آیا کشوری هستیم که توانستیم محدوده خود را در فضای سایبری تعیین کنیم؟ این بخشی از قامت سازمان پدافند غیرعامل قابل‌پاسخگویی است، چون می‌دانیم بخشی از این تصمیم‌گیری‌ها و حیطه‌بندی‌ها خارج از وظایف سازمان است، اما در آن سطح که سازمان چه اقدامی انجام داده یا چه نقشی را ایفا کرده و هم خارج از آن چه اقدامی صورت گرفته است؟ چقدر توانستیم این مرزبندی را داشته باشیم؟

وقتی درباره قلمروی ملی سایبری کشور صحبت می‌کنیم، طبیعتا باید این قلمرو را نخبگان کشور تعریف و حاکمان آن را تأیید کنند، یعنی حاکمان در شورای عالی امنیت ملی تصویب کنند این مؤلفه‌های منافع ملی ماست که باید حفظ شود، همچنین باید تصویری ملموس از سرزمین سایبری جمهوری اسلامی ایران مطرح شود که این چگونه و کجاست و نخبگان کشور که شامل مسئولان و دانشمندانند بر سر این امر اجماع کنند.

مقاله‌ای بعد از حمله استاکس‌نت به ایران توسط یک ژنرال آمریکایی نوشته شده بود با این موضوع که چرا ایرانی‌ها درباره استاکس‌نت از ما شکایت نکردند؟ ۹ دلیل آورده بود؛ یکی این بود که احتمالا مسئولان جمهوری اسلامی ایران نتوانسته‌اند قلمروی سرزمینی خود را در فضای سایبری تشخیص دهند،

یعنی حمله به نطنز را خاک خود تلقی نکرده و به همین دلیل شکایت نکردند. اتفاقا من دیدم حدس او در اینجا حدس درستی بود. اگر در اینجا قرار باشد این کار انجام شود وفاق و فهم ملی نسبی نیاز دارد که میان نخبگان و مسئولان که کشور را اداره می‌کنند، فهم مشترکی وجود داشته باشد.

تعریفی که در فضای سایبری از قلمروی ملی می‌شود، این است که نخبگان کشور نسبت به این قلمرو فهم درستی داشته باشند. امروز می‌گوییم انسجام کشور منافع ملی است، چون همه کشور قبول دارند باید یکپارچه باشد، مثلا همین مفهوم در یک مقطعی در عراق اینطور نبود. وقتی کردهای عراق می‌خواستند جدایی‌طلبی کنند، مردم در بغداد احساس متفاوتی داشتند و بعضی می‌گفتند جدا شوند و دنبال کار خود بروند. در کشور ما روستایی بخواهد جدا شود همه می‌گویند اجازه نمی‌دهیم، یعنی وحدت و انسجام ملی برای ما ارزش و منافع ملی است ولی ممکن است برای کشوری اینطور نباشد. این فهم نسبت به سرزمین سایبری باید ایجاد شود. وقتی یک مفهوم تعریف شد می‌توانیم دارایی‌ها و ارزش‌های خود را تعریف کنیم. تنها کشوری که به‌صورت نسبتا موفقیت‌آمیز توانسته این کار را دقیق انجام دهد چین است. مقاله علمی تحت‌عنوان سازوکار و ساختار اینترنت در چین چگونه است، چاپ شده، حتی امانوئل مکرون در سخنرانی‌اش به اینترنت چینی اشاره می‌کند، پس چون چینی‌ها این کار را کرده‌اند ما هم می‌توانیم انجام دهیم. خیلی از دانشمندان و نخبگان ما می‌گویند نمی‌توان برای این فضای بیکران و بی‌انتها مرز تعیین کرد. اما چینی‌ها انجام دادند و موفق شدند، پس ما هم می‌توانیم. برای این کار لازم است یک محیط ملی logical تعریف کنیم که مبتنی‌بر منطق فضای سایبری باشد و دارایی‌ها را در آن تعریف کنیم، مثلا پول ما دیجیتال می‌شود. ۹۸٫۵ درصد پول دیجیتال و ۱٫۵ درصد فیزیکی است. این ۹۸٫۵ درصد را در کدام گاوصندوق گذاشته‌ایم؟ در گاوصندوقی که مبتنی‌بر اینترنت است و وصل به دریا، اقیانوس‌هاست. اگر دشمن به ما حمله کند چطور از پول خود دفاع کنیم؟ باید پستو، سنگر یا گاوصندوقی داشته باشیم. این گاوصندوق در فضای سایبری کجاست؟ وجود ندارد، پس باید تعریف شود. ما باید بگوییم در این اقیانوس جهانی یک دریاچه، حتی یک اسکله می‌خواهیم که دارایی‌ها، قایق‌ها و شناورهای خود را در آنجا نگه داریم تا سونامی آنها را از بین نبرد.

اگر این موضوع در فضای سایبری تعریف شد، می‌گوییم دارایی‌های ما چیست؟ آیا پول است؟ آیا افکار عمومی ما دارایی ما نیست؟ زیرساخت‌های شکل‌دهنده افکار عمومی در همه جای دنیا و در همه کشورها از جمله ایران، افکار عمومی و شاخص‌های اصلی افکار عمومی به‌عنوان منافع حیاتی مطرح است، ولی ما این را در فضای سایبری از دست داده‌ایم. در فضای افکار عمومی می‌گوییم سرزمین اشغال شده است، یعنی سرزمین سوخته اشغال شده است. وقتی نمی‌توانیم در مجلس یک لایحه داشته باشیم، افکار عمومی علیه ماست. دولت آقای روحانی، دولت شهید رئیسی و دولت آقای پزشکیان را مقایسه می‌کنم، رفتار مخالف جریان افکار عمومی با این سه دولت یکسان است، درصورتی که گرایش این دولت‌ها با هم متفاوت است، پس این امر ربطی به گرایش‌ها ندارد، بلکه برخی گرایش‌ها کمک می‌کنند و برخی گرایش‌ها نه، ولی گرایشی که هر اقدام اقتصادی به نفع مردم را تخریب کنید در شبکه اجتماعی وجود دارد و در افکار عمومی جلو می‌رود، مثلا اینکه کارهای ارزشمند ملی را تمسخر کنید از قبل بوده و الان نیز وجود دارد. درنتیجه جریانی است که بر افکار عمومی مدیریت می‌کند و تسلط دارد. افکار عمومی دارایی ماست. یکی از چیزهایی که در فضای سایبری باید از آن حفاظت کنیم افکار عمومی است، فقط پول نیست. دارایی‌های دیگری نیز وجود دارند. دارایی‌های فیزیکی ما در بازه زمانی خیلی سریع با شیب تند تبدیل به دارایی‌های مجازی و دارایی‌های سایبری شده‌اند.

اگر این دارایی‌ها وارد اقیانوس شوند، باید بدانیم چه کار کنیم. طبیعتا اگر این موضوع به فهم عمومی برسد، یعنی نخبگان و مسئولان کشور به فهمی مشترک برسند، درست کردنش کار سختی نیست. متأسفانه این فهم واحد درست نمی‌شود و یکی از مشکلات آن از سوی مسئولان است. بنابراین برخی از بحث‌هایی که اینجا انجام شد، این بود که محیط ملی‌مان را در فضای سایبری تعریف کنیم. اولویت‌های خود را نیز تعریف کنیم. در فضای معنوی و شناختی و محتوایی ارزش‌ها، اصول و چهارچوب‌های ملی و دینی‌مان را تعریف کنیم و آنها را پاس بداریم.

در حوزه ارزش‌های فیزیکی، حفاظت از آنها، زیرساخت‌ها، مدیریت و کنترل داشته باشیم. هریک از اینها ابزارها، مدل‌ها و زیرساخت‌های خاص خود را می‌خواهند. یکی از این ابزارها که می‌تواند به ما کمک کند شاید شبکه ملی اطلاعات باشد، ولی علی‌رغم اینکه نقشه‌ها و چهارچوب‌های آن تفصیلی بود، دولت آقای روحانی در این زمینه به‌جای اینکه کارها را انجام دهد، سفسطه می‌کرد. برقراری ارتباطات را به شبکه ملی اطلاعات تعبیر می‌کرد. همین شبکه ارتباطی را که داریم، ارتباطات تعبیر می‌کنند. آن زمان وزیر وقت گفته بود من در این مورد ۸۰ درصد کار را انجام داده‌ام و وقتی ارزیابی کردند، دیدند زیر ۳۰ درصد است. اینکه می‌گویند باید قلمروی منطقی تعریف شود، یکی از عناصر آن، مرکزداده ملی و دیگری محتواست. داده‌های ما از مهم‌ترین دارایی‌های ماست و اگر این بیرون برود و داده‌کاوی شود علیه ما می‌تواند به‌کار گرفته شود. باید اینها در جای معینی باشد.

برای حفظ ارتباط مردم و سرعت بالا، داده‌های نرم نیاز داریم درنتیجه باید دیتاسنتر ملی داشته باشیم. برای اینکه اگر شما یک کتابی را سرچ کردید و مطالعه شد و من خواستم آن را سرچ کنم دوباره از دانشگاه هاروارد سرچ نکنم. این یک نمونه است. این امر در دولت قبلی بود و دولت شهید رئیسی شروع کرد و پیشرفت‌هایی هم داشت. سیستم‌عامل نیاز است برای اینکه نظیر

یکی از این ابزارها که می‌تواند به ما کمک کند شاید شبکه ملی اطلاعات باشد، ولی علی‌رغم اینکه نقشه‌ها و چهارچوب‌های آن تفصیلی بود، دولت آقای روحانی در این زمینه به‌جای اینکه کارها را انجام دهد، سفسطه می‌کرد. برقراری ارتباطات را به شبکه ملی اطلاعات تعبیر می‌کرد. همین شبکه ارتباطی را که داریم، ارتباطات تعبیر می‌کنند. آن زمان وزیر وقت گفته بود من در این مورد ۸۰ درصد کار را انجام داده‌ام و وقتی ارزیابی کردند، دیدند زیر ۳۰ درصد است. اینکه می‌گویند باید قلمروی منطقی تعریف شود، یکی از عناصر آن، مرکزداده ملی و دیگری محتواست. داده‌های ما از مهم‌ترین دارایی‌های ماست و اگر این بیرون برود و داده‌کاوی شود علیه ما می‌تواند به‌کار گرفته شود. باید اینها در جای معینی باشد.
برای حفظ ارتباط مردم و سرعت بالا، داده‌های نرم نیاز داریم درنتیجه باید دیتاسنتر ملی داشته باشیم

ماجرای تلگرام و... آنجا اتفاق نیفتد که با یک تیک کل شبکه‌های ما را از بین ببرند. گوشی هوشمند ملی می‌خواهیم که هم پلتفرم و هم نرم‌افزارش در اختیار ما باشد تا بتوانیم خدماتی که به مردم می‌دهیم پایدار و در اختیار و کنترل‌مان باشد و بتوانیم از آنها استفاده کنیم، اما اکنون این را نداریم. ما باید سیستم پست الکترونیک و ابزارهایی داشته باشیم که فضای سایبری را تعریف می‌کنند. با مطالعه‌ای که روی کشور چین کردیم، دیدیم که چینی‌ها همه اینها را برای خود تعریف کرده‌اند، مثلا سیستم‌عامل چینی دارند. شبکه اجتماعی چینی خود را دارند، اینستاگرام و گوگل آنجا کار نمی‌کنند. ممکن است باشند، ولی هیچ‌کس به آنها متکی نیست و موتورجستجوی ملی در اختیار چینی‌هاست، حتی بسیاری فضاها به زبان چینی است که خیلی از کشورها نمی‌توانند از آنها استفاده کنند و مال خود کشور چین است. به‌عبارت دیگر آنان توانسته‌اند سیستم حاکمیت کشور خود را کنترل کنند. هرچقدر دوست دارند آزاد بگذارند یا ببندند در اختیار حاکمیت است. که این موضوع نوعی از حاکمیت را در اینجا تعریف می‌کند. متأسفانه هنوز در کشور موفق به فهم این موضوع به‌صورت جامع نشده‌ایم و این یکی از مشکلات است.

الان در شورای عالی فضای مجازی که جمعی از نخبگان و مسئولان در آن حضور دارند، برداشت واحدی نسبت به پدیده‌ها وجود ندارد. طبیعتا وقتی برداشت واحد وجود نداشته باشد، نسخه واحد نیز از آن بیرون نمی‌آید. در دولت شهید رئیسی تقریبا دیدگاه‌های فراوانی به هم نزدیک شدند، برای همین شبکه ملی اطلاعات و زیرساخت‌های وابسته به آن پیشرفت خوبی داشتند. آمار دقیقی ندارم، ولی وزیر ارتباطات قبلی تا حدود ۶۷ درصد اطلاع می‌داد و مرکز ملی هم تایید می‌کرد، یعنی تقریبا ۷۰ درصد پیشرفت را به‌صورت جمعی مرکز ملی هم با شاخص تایید می‌کرد که درست شده است. اگر همین مسیر با همین قوت ادامه پیدا کند. ان‌شاءالله بتوانیم به‌موقع به این موضوع دست پیدا کنیم.

اتکا به توانایی‌های داخلی در حوزه سایبری

بخشی از حکمرانی در این فضا یا اثرگذاری در آن به توانمندی‌های زیرساختی ما برمی‌گردد. به‌هرحال این فناوری‌ها، چه آخرینش که هوش‌مصنوعی است و چه خود اینترنت، فرآورده‌های ما نیستند و در جایی دیگر تولید شده‌اند و مالکیت‌شان با جای دیگری است. همان‌طور که شما بیان کردید به‌راحتی دسترسی‌هایی دارند که ما آن دسترسی‌ها را نداریم و نتوانسته‌ایم آنطور که لازم بوده و است به آنها اشراف داشته باشیم و از آنها حفاظت کنیم. اتفاقات اخیر هم در درگیری‌هایی که در منطقه وجود دارد یا در عرصه بین‌المللی است، در سطوح مختلف این را به ما نشان داده‌اند. ساده‌ترین آن هک و از دست رفتن اطلاعات برخی پلتفرم‌هاست که مردم از آن استفاده می‌کنند. پیچیده‌ترین آنها نیز اتفاقات نظامی و عجیب‌وغریبی است که در کشور می‌افتد و هنوز مشخص نیست چطور است، حتی سطح فناوری که استفاده می‌شود هم مشخص نیست. در این حوزه اینکه سازمان پدافند غیرعامل به‌عنوان سازمانی که شاید در نازل‌ترین سطحی که می‌تواند ورود و اینها را شناسایی کند و هشدار آن را به نهادهایی بدهد که باید تصمیم‌گیری و ورود کنند تا عالی‌ترین سطح که خود به‌عنوان بازیگر ایفای نقش کند، آیا اقداماتی صورت گرفته‌اند؟ چه از طرف سازمان‌های متولی دیگر و چه از طرف سازمان پدافند غیرعامل که ما در این حوزه به توانمندی برسیم تا اگر در شرایط اضطرار قرار گرفتیم بتوانیم از توانمندی خود استفاده کنیم؟ در گوشه‌وکنار موتور جست‌وجوی ملی دوره‌ای ایجاد شد که با اسامی مختلف همراه بود؛ هم شبکه اجتماعی داخلی داریم و هم ادعا این بود که تلفن همراه خود را داشته‌ایم، هرچند سیستم‌عامل برای ما نبود.

تا صحبت بومی‌سازی می‌شود به‌خاطر مهندسی افکار عمومی ذهن جامعه به‌سمت محدودیت می‌آید که می‌خواهند مدیریت کنند، یعنی فیلتر می‌شود،

یعنی دسترسی‌های ما کوتاه می‌شوند. مهندسی افکار می‌خواهد. دسترسی می‌خواهد. احتمال می‌خواهد. ما چه اقداماتی انجام داده‌ایم؟ شرکت‌ها و متخصصان ما در این حوزه چه کرده‌اند؟

این مباحث شما باید به دو قسمت کلی تقسیم شود: یکی زیرساخت‌های ملی است که به نظر من وظیفه دولت و حاکمیت است، مثلا در حوزه ارتباطات شرکت ملی مخابرات داشتیم. کار این شرکت این بود که بوق و «نود» (node) به ما بدهد. در سیم‌کارت ارتباط نود و در تلفن ثابت بوق می‌دهند. شرکت ملی باید شرکت دولتی باشد. امروزه نود شبکه اجتماعی لازم داریم که در دولت قبلی گفته می‌شد کار ما نیست و می‌گفتند به دولت ربطی ندارد، باید بخش خصوصی داشته باشد. بخش خصوصی هم داخل کشور ما چندان توانمند نیست که بتواند با شرکت‌های گردن‌کلفت جهانی در این حوزه رقابت کند. طبیعتا اینجا این است که اگر شبکه اجتماعی زندگی مردم است، اگر سبک زندگی مردم است، اگر نیازمندی‌های آموزشی، بانکی، پولی، خدماتی با این شبکه‌هاست، باید خدمات ملی باشد. اینطور نمی‌شود که امشب فردی شبکه را خاموش کند و فردا ملت نتوانند سرکارهایشان بروند. کمااینکه این را دیده‌اید، بنابراین در حوزه زیرساخت‌های ملی دولت به میدان بیاید، ایفای وظیفه کند و آن زیرساخت‌ها را برای کشور درست کند، البته به سرمایه‌گذاری دولت نیاز دارد. بخش خصوصی در کشور ما این اندازه توان ندارد که سرمایه‌گذاری اینچنینی کند، مثل آب، برق و گاز است. سد را بخش خصوصی نمی‌زند، باید دولت آن را احداث کند. جاده‌ها و اتوبان‌ها را باید دولت احداث کند، این امر هم همین‌طور است. در این خصوص متأسفانه قانون نداریم. پیشنهاد من این بود اولین موضوع اینکه قانون داشته باشیم که در مجلس به ناکجاآباد خورد. باید در این قانون تکالیف زیرساخت‌های دولتی را تصریح کرد. این چهار مورد زیرساخت دولت و حاکمیت است و دولت مکلف است یک، دو و حتی سه‌ساله این را درست کند. این

اگر شبکه اجتماعی زندگی مردم است، اگر سبک زندگی مردم است، اگر نیازمندی‌های آموزشی، بانکی، پولی، خدماتی با این شبکه‌هاست، باید خدمات ملی باشد. اینطور نمی‌شود که امشب فردی شبکه را خاموش کند و فردا ملت نتوانند سرکارهایشان بروند. کمااینکه این را دیده‌اید، بنابراین در حوزه زیرساخت‌های ملی دولت به میدان بیاید، ایفای وظیفه کند و آن زیرساخت‌ها را برای کشور درست کند، البته به سرمایه‌گذاری دولت نیاز دارد. بخش خصوصی در کشور ما این اندازه توان ندارد که سرمایه‌گذاری اینچنینی کند، مثل آب، برق و گاز است. سد را بخش خصوصی نمی‌زند، باید دولت آن را احداث کند. جاده‌ها و اتوبان‌ها را باید دولت احداث کند، این امر هم همین‌طور است. در این خصوص متأسفانه قانون نداریم. پیشنهاد من این بود اولین موضوع اینکه قانون داشته باشیم که در مجلس به ناکجاآباد خورد. باید در این قانون تکالیف زیرساخت‌های دولتی را تصریح کرد.

به‌صراحت در قانون وجود ندارد.

نکته دوم این است که زیرساخت‌ها و خدمات حاکمیتی دست دولت باشد. خدمات تصدی‌گری دست بخش خصوصی و مردم باشد. الان به کسی بگویند دیتاسنتر درست کند، بخش خصوصی پول دیتاسنتر درست کردن ندارد، مثلا بگویند سیستم‌عامل درست کنند، شاید برای بخش خصوصی درست کردن سیستم‌عامل برای یک کشور ۸۰ میلیونی مقرون‌به‌صرفه نباشد. طبیعتا این موارد را باید دولت پیگیری کند، پس یک‌سری موارد دولتی داریم که در دولت شهید رئیسی اینها تفهیم شد و رئیس‌جمهور برایشان تصمیم می‌گرفت. برخی را شروع کردند و با پیشرفت‌هایی کم‌وزیاد همچنان پیش می‌روند. بخش دیگر زیرساخت‌هایی است که باید در اختیار بخش‌های خصوصی و بخش‌های غیردولتی و نهادهای دیگر باشد تا به مردم خدمات بدهند. به نظر من در این حوزه نیز نسبت به گذشته پیشرفت بدی نداشته‌ایم. طبیعتا ممکن است به‌اندازه بیرونی‌ها قوی نباشد، مثلا اینجا سامانه مکان‌یاب داریم که ممکن است ویز (waze)اسرائیلی قابلیت بیشتری داشته باشد، ولی نشان و بلد را داخل کشور داریم که نیازمندی‌های ما را می‌توانند تأمین کند. برخی خدمات زیربنایی که برای دولت است مثل موتور جست‌وجو، ملی است که اگر مانند داستان سال قبل گوگل خواست چهره‌به‌چهره مقابل ما بایستد و با ما بجنگد بتوانیم خود را روی سیستم‌های بومی منتقل کنیم یا امروزه بعد از حوادث اخیر لبنان و داستان پیجرها راجع به اینکه دشمن در ذات فناوری خود تهدید درست کرده و یک روز استفاده می‌کند، برای عقلا شکی وجود ندارد. ممکن است برخی توهمی باشند و بگویند اشتباه بوده، ولی برخی که عقلایی‌اند اذعان دارند. اینکه به‌لحاظ زیرساخت کلا در اختیار برنامه‌های خارجی باشیم و روی ویزی که آنها دارند سوار باشیم، طبیعتا کار عاقلانه‌ای نیست. ممکن است برای کشورهایی که تابع آنها هستند خیلی مشکل ایجاد نشود، ولی ما که ادعای استقلال داریم و می‌گوییم «نه شرقی و نه غربی» نمی‌توانیم به زیرساخت‌های آنها اتکا کنیم، پس در این حوزه شاید تکالیف دولت قدری سنگین‌تر باشد، حمایت‌ها نیز سنگین‌تر خواهد شد. به نظر من این جزء نواقص اساسی و زیربنایی است که باید رفع شود و جلو برود.

ما در حوزه تئوری فضای سایبری توانمندیم

در بخش دوم ما- در مواردی که هم بخش دولتی و هم بخش غیردولتی می‌توانند تصدی‌گری کنند، به نظر من پیشرفت خوبی داشته‌ایم. در رویه و نگاه تقریبا موفق بوده‌ایم که از ۱۰ سال پیش سند راهبردی پدافند سایبری داشته باشیم، یعنی خطوط اصلی خود را تعریف کرده‌ایم. به یاد دارم در سال ۹۲-۹۱ که سند می‌نوشتیم آمریکایی‌ها هنوز وجود شرکت‌های خارجی در زیرساخت‌هایشان- مانند هوآوی را- داشتند. ولی بعدها آنها یقه چینی‌ها را گرفتند و بیرون‌شان کردند. دعوای اخیر آمریکایی‌ها از طریق شبکه اجتماعی تیک‌تاک را شاهدید که در همین حوزه است، این در حوزه شبکه اجتماعی و آن در حوزه زیرساخت است. آنجا سوئیچ‌های هوآوی بودند و تسلط بر زیرساخت داشتند و اینجا شبکه‌های اجتماعی چینی است، بنابراین آنها نیز برای خود چنین موضوعاتی را داشته‌اند. اینکه برای چشم‌انداز، راهبرد و هدف سند تنظیم کرده‌ایم به نظرم خوب کار کرده‌ایم، همچنین توانسته‌ایم رویه مستقلی از جنبه نظری تعریف کنیم. این نقطه قوت است. این امر به نظر نکته برتری است که توانسته‌ایم مبتنی‌بر آن برای کشور سند نظام دفاع سایبری تعریف کنیم، به شکلی که در این نظام بتوانیم سطوح دفاع، عناصر دفاع، روابط آنها، انواع فرماندهی، نقش‌های اصلی و پشتیبانی را درآوریم و به تصویب رساندیم.

به نظر من در منطقه و حتی شاید در دنیا جزء چهار، پنج کشور اول باشیم که سندی با این جامعیت نوشته ایم. چون تقریبا اغلب این دست از نظام‌ها را- که

موجود است- مطالعه کرده‌ایم و برای آنها تعریف داریم، این دستاورد بسیار خوبی برای ماست که درعین‌حال به ما چهارچوب کار می‌دهد. ما توانسته‌ایم در مطالعه علمی مدل دفاع کشور را در حوزه سایبری تعریف کنیم که لایه‌ها و نوع دفاع تعریف شوند، مثلا دفاع نقطه‌ای، دفاع منطقه‌ای، دفاع حوزه‌ای و دفاع ملی داریم. وقتی در اغتشاشات سال گذشته، ۹۰۰-۸۰۰ مورد حمله منع خدمت بر روی زیر ساخت‌های ملی داشتیم در سطح راهبردی به کشور حمله می‌شد، توانستیم با ابزارهایی جلوی آنها را بگیریم، یعنی ما ابزار ملی ساختیم و جلوی آنها را گرفتیم. معماری لایه دفاعی هم موضوع مهمی بود که ما این کار را کردیم و الان درحال تکمیلش هستیم. برای ما نقشه واضحی وجود دارد که می‌خواهیم چه کار انجام دهیم و ابهامی نسبت به این لایه‌ها نداریم. این مسئله به‌لحاظ نظری و دانشگاهی وجود دارد که خوشبختانه توانسته‌ایم هم رشت های کارشناسی ارشد و هم دکترای دفاع سایبری را تعریف کنیم. امروز فارغ‌التحصیلان قابل‌قبولی در این زمینه داریم. براساس الگوها و روش‌های علمی این موضوع را بررسی می‌کنیم و متدولوژی‌های خاص خود را در این زمینه تعریف و دنبال کردیم. به‌صورت مشخص دکترین پدافند سایبری را تعریف کرده‌ایم که مبتنی‌بر استراتژی‌های خود و نظریه‌های پایه دفاعی کشور است تا بتواند بخش دفاعی و غیرنظامی را با یکدیگر هماهنگ، همسو و هم‌افزا جلو ببرد. اینها در مراجع رسمی تصویب شده‌اند.

به نظرم به‌لحاظ مباحث نظری، دانشگاهی، علمی و اسناد بالادستی اقدامات خوبی صورت گرفته و الان خلأ عمده‌ای در این زمینه نداریم. در این اسناد به این جمع‌بندی رسیده‌ایم که امنیت و پدافند در فضای سایبری بدون داشتن سامانه ملی و بومی قابل اجرا نیست، هرچند ممکن است در برخی حوزه‌ها قدرت تولید نداشته باشیم یا ازنظر اقتصادی به‌صرفه نباشد، ولی بالاخره آنها را می‌توانیم با پروتکل امنیتی، معماری خاص دنبال کنیم یا وجود خرابکاری‌ها را در بررسی‌های تخصصی دربیاوریم که نمونه‌هایی مشابه پیجر اتفاق نیفتد. آن هم جزء سامانه‌هاست و به این نتیجه رسیده‌ایم که در حوزه امنیت باید به‌سمت بومی‌سازی برویم. ما تهدیدهایی ازجمله کاشت سنسور و کاشت سخت‌افزار و بدافزار در شبکه و برد داریم که آمریکایی‌ها صراحتا در سندی که در روزنامه نیویورک‌تایمز چاپ شد، آن را بیان کرده‌اند.

در حوزه‌های نرم‌افزار الی‌ماشاءالله از این دست مسائل وجود دارد، بنابراین به‌سمت بومی‌سازی محصولات رفته‌ایم؛ سامانه‌ها را دسته‌بندی کرده‌ایم. نزدیک به ۹۶ سامانه امنیت و دفاعی تعریف کرده‌ایم که باید حتما بومی شوند. اولویت‌بندی کرده‌ایم تا ۲۴ سامانه را به‌عنوان اولویت اول استخراج کنیم که در حوزه امنیتی باید حتما مرور شوند. اگر صحنه سایبری را جبهه‌بندی کنیم، جبهه اول ما صنایع و مدیریت صنعتی هستند. آنجا که شبکه‌ها و زنجیره‌های خدمت و تولید مدیریت و کنترل می‌شود، مثل آب، برق، هسته‌ای، گاز، پتروشیمی، پالایشگاه‌ها و... که با سامانه کنترل صنعتی اداره می‌شوند. یکی از چالش‌های ما در حمله استاکس‌نت این بود که از اسکادا زیمنس استفاده می‌کردیم و به هر دلیلی نفوذ اتفاق افتاد یا درها باز و ویروس وارد شد و به ما حمله کرد. جمع‌بندی ما این بود که می‌توانیم این کار را انجام دهیم. کانونی از اساتید دانشگاه را در این زمینه به‌عنوان هیئت‌مدیره و داور تعریف کردیم و همه کسانی را که در حوزه اسکادا کار می‌کردند و هم بهره‌بردار، هم مونتاژکننده، هم طراح بودند، دعوت و درعین‌حال بررسی‌های علمی کردیم. در دو مجموعه به تشخیص رسیدیم که اگر بخواهیم یکی شوند می‌توانند به تولیدکننده تبدیل شوند که این کار را انجام دهیم و توانستیم اولین محصول اسکادای بومی را داخل کشور با پشتیبانی معنوی و مادی تولید کنیم.

وقتی چنین چیزی تولید شد نیازمند حمایت مالی و رسیدن به حوزه‌های صنعتی بود. شرکتی که نیروگاه‌ها و توربین‌های برقی را تولید می‌کند نیازمند سامانه خارجی بود. گفتیم سامانه خارجی نمی‌شود و باید

سامانه داخلی باشد. کل مجموعه شرکتی دانش‌بنیان را خریداری کردند و به شرکت بردند و تبدیل به خط تولید کردند. امروز سیستم کنترل صنعتی برق آن شرکت یکی از افتخارات کشور است. در تمام پروژه‌هایی که این شرکت نیروگاه تولید می‌کند، سیستم کنترل صنعتی ایرانی است که منشأ آن از داخل بوده و امنیت بالایی دارد، حتی رئیس آن شرکت به من گفت در مناقصه بین‌المللی در یک کشور به آنان گفتم که می‌توانیم دو سیستم داشته باشیم؛ یکی سیستم اروپایی و دیگری سیستم ایرانی است. آنها گفتند ایرانی برای ما بهتر است. چون آنها جزء بلوک شرق بودند و می‌گفتند اعتمادی به آن‌طرف نداریم و ممکن است به ما آسیب برسانند، پس سیستم ایرانی مطمئن‌تر است. این امر برای ما افتخار بود، در مقایسه جهانی نیز سیستم کنترل صنعتی ما مورد اعتماد بود. از این ۲۴ مورد روز اول می‌خواستیم با فشار و تلاش یک مورد را تولید کنیم، اما الان تقریبا ۲۴ مورد اولیه کامل تولید شده‌اند و از آنها عبور کرده‌ایم. محصولاتی بودند که حدود هشت تا ۱۰ نمونه- و بعضا پنج نمونه- تولید و از آن عبور کردیم. محصولات ما به تکرار و تواتر هم رسیده است که منحصر به یک محصول هم نیستند.

نقشه ما سیاستگذاری ارزیابی و حمایت مادی و معنوی بود. سربازان، افسران و قهرمانان این حوزه شرکت‌های دانش‌بنیان بوده‌اند که در دانشگاه تلاش کرده‌اند و حمایت‌هایی هم شده‌اند و الان توانسته‌اند به محصول برسند. تلاش زیادی کرده‌ایم تا با اختیاراتی که قانون به ما داده در بازار هم از آنها حمایت کنیم. به یاد دارم برای اولین بار سه، چهارسال پیش ضدبدافزار بومی طراحی و تولید شد و این ضدبدافزار توانست در رتبه بندی جهانی رتبه بین ۶-۴ را به دست آورد که برای ما قابل‌قبول بود. در نمایشگاه امنیتی که داشتیم تقریبا تمام ضدبدافزارهای خارجی که در بازار کشور فروش دارند کاهش قیمت انجام و قیمت‌ها را ۹۰ درصد تخفیف دادند، یعنی به ۱۰ درصد قیمت رساندند، به شکلی که این ضدبدافزار داخلی ما آسیب ببیند و

نقشه ما سیاستگذاری ارزیابی و حمایت مادی و معنوی بود. سربازان، افسران و قهرمانان این حوزه شرکت‌های دانش‌بنیان بوده‌اند که در دانشگاه تلاش کرده‌اند و حمایت‌هایی هم شده‌اند و الان توانسته‌اند به محصول برسند. تلاش زیادی کرده‌ایم تا با اختیاراتی که قانون به ما داده در بازار هم از آنها حمایت کنیم. به یاد دارم برای اولین بار سه، چهارسال پیش ضدبدافزار بومی طراحی و تولید شد و این ضدبدافزار توانست در رتبه بندی جهانی رتبه بین ۶-۴ را به دست آورد که برای ما قابل‌قبول بود

نتوانـد رشـد کنـد، به‌قول‌معـروف در حـد مفـت اسـت. وقتی جنس ۱۰۰ تومانی را ۱۰ تومان بدهید، یعنی در حد مفت است. ما اینجا حمایت کردیم. هم سفارش دادیم و هم ظرفیت اقتصادی را پشت کار آوردیم و پشتیبانی کردیم. در کشـور چنیـن چیـزی نداشـتیم، بـرای همیـن در حـوزه اقتصـادی شـبکه‌های بیرونـی آمـده بودنـد کـه تولیدکننده داخلی را زمین بزنند و له کنند. الان ضدبدافزار در داخـل کشور وجود دارد؛ مدل‌هـای دیگری نیز از آن تولیـد شـده و قابلیـت درسـت کرده‌انـد، پـس محـور کلـی ما تولید محصولات بومی در حوزه امنیت و دفاع سایبری است که بتوانند تهدیدهای بیرونی را پاسخگو باشند و پایداری سیستم و خدمات ما را تضمین کنند. اکنون در ایـن حـوزه به‌انـدازه‌ای خـوب رشـد کرده‌ایـم کـه شـرکتها چنـدان محتـاج حمایـت مـا نیسـتند و درواقـع خودشـان کارهـا را انجـام می‌دهنـد و جلـو می‌رونـد. ایـن امـر جـای شکرگزاری دارد، ولی همواره نیاز حمایت دولت، کارفرما و بهره‌بـرداران وجـود دارد.

به‌لحاظ فنی و اجرایی توانسته‌اند به بلوغی برسند که نیازهای کشور را پاسخگو باشند. این به نظر من اقدام ارزشمندی بود که هنوز ادامه دارد و دنبال می‌شود.

ما سال گذشته موفق شدیم بعد از پیگیری‌های زیادی کـه در مجلـس کردیـم، قانونـی بـرای سـازمان پدافنـد غیرعامـل بگیریـم کـه بـه قانـون تشـکیل معـروف اسـت و در شـهریور سـال گذشـته از مجلـس و دولـت ابـلاغ شـد. ایـن قانـون ویژگی‌هایـی دارد:

اولا در ایـن قانـون مرجع تصمیمـات نهایـی و راهبـردی در عالی‌تریـن مرجـع پدافنـد غیرعامـل را یـک کمیتـه دائمـی تشـکیل داده کـه برپایـه اساسـنامه ۱۴ عضـو دارد کـه هفـت وزیـر و ۶ نفـر بخـش دفـاع، رییـس سـتاد، فرمانـده ارتـش و... اعضـای آن هسـتند. قابل‌ذکـر اسـت کـه آن مرجـع نهایـی تصمیمـات پدافنـد غیرعامـل شـده اسـت. چیـزی ماننـد شـوراهای اصلـی سیاسـت گـذار کشـور شـده اسـت.

ثانیـا قانـون ابـلاغ و اجـرای ایـن مصوبـات را بـه رئیـس سـتاد کل نیروهـای مسـلح تنفیـذ کـرده اسـت. کار مهمـی اسـت کـه سـبب می‌شـود در پیچ‌وخـم مـوارد اداری نیفتیـم.

ما سال گذشته موفق شدیم بعد از پیگیری‌های زیادی که در مجلس کردیم، قانونی برای سازمان پدافند غیرعامل بگیریم که به قانون تشکیل معروف است و در شهریور سال گذشته از مجلس و دولت ابلاغ شد.
این قانون ویژگی‌هایی دارد:
اولا در این قانون مرجع تصمیمات نهایی و راهبردی در عالی‌ترین مرجع پدافند غیرعامل را یک کمیته دائمی تشکیل داده که برپایه اساسنامه ۱۴ عضو دارد که هفت وزیر و ۶ نفر بخش دفاع، رییس ستاد، فرمانده ارتش و... اعضای آن هستند. قابل‌ذکر است که آن مرجع تصمیمات پدافند غیرعامل شده است. چیزی مانند شوراهای اصلی سیاست‌گذار کشور شده است.
ثانیا قانون ابلاغ و اجرای این مصوبات را به رئیس ستاد کل نیروهای مسلح تنفیذ کرده است. کار مهمی است که سبب می‌شود در پیچ‌وخم موارد اداری نیفتیم.
ثالثا اجرای آن را الزامی و عدم اجرا و استنکاف را جرم‌انگاری کرده است

ثالثا اجرای آن را الزامی و عدم اجرا و استنکاف را جرم‌انگاری کرده است، یعنی گفته شده اگر کسی اجرا نکند براساس ماده ۵۷۶ مجرم است و باید دادگاه رسیدگی کند که با دادستانی محترم توافقاتی داشته‌ایم که شکل اجرایی کار را دنبال کند، بنابراین مصوبات و الزامات ما شأن قانونی و ضمانت اجرایی دارد، اگر کسی اجرا نکند قابلیت پیگیری و برخورد دارد و نسبت به گذشته جدی‌تر است.

اگر ما تقسیم کارهای خود را داخل کشور دقیق‌تر و بهتر پی‌ریزی کنیم- که خیلی نمی‌خواهم به جزئیات آن وارد شوم- می‌تواند کارایی ما را افزایش دهد و به نظرم نقطه قوت‌مان خواهد بود. برای این نقاط قوت دستورالعمل‌های عملکردی نوشته‌ایم. برای حوزه صنعت که به‌خاطر کنترل صنعتی و حملات دو سال گذشته ازنظر ما حوزه بسیار بااهمیتی است، یک آیین‌نامه عملیاتی تعریف کرده‌ایم و در آن الزامات داده‌ایم که الزامات ما قانونی هستند و برای همه حوزه‌های صنعتی که سیستم‌های کنترل صنعتی دارند، لازم‌الاجراست. به‌لحاظ امنیتی و سطح زیرساخت اهمیت آن حیاتی و واجب‌الحفاظه است، با قابلیت‌هایی که باید ازنظر سامانه سخت‌افزار و نرم‌افزار داشته باشد، الزام قانونی تعریف کرده‌اند و این الزام را ابلاغ کرده‌ایم. درحال‌حاضر برای دستگاه لازم‌الاجراست. گفتنی است درپی پیاده‌سازی و اجرای آن هستیم، مثلا در مرکزی که سطح آن حیاتی تشخیص داده شده، هیچ‌دستگاهی مجاز به به‌کارگیری سامانه‌های خارجی نیست و باید حتما سامانه داخلی باشد. اگر نبود با تبصره و الزاماتی می‌تواند استفاده کند، نه اینکه همین‌طور برای خود استفاده کند! این امر کار را نظام‌مند می‌کند، همچنین ضمانت اجرایی و تقویتی برای بازار داخلی کشور و تولیدکنندگان داخلی درست می‌کند که می‌تواند برای کشور ارزشمند باشد. در این زمینه یک‌سری دستورالعمل را در دست اقدام داریم مثلا برای شهرهای هوشمند در حال کار هستیم، برای حوزه‌های دیگر نیز به این شکل کار می‌شود. به نظر من می‌تواند اجرایی شود.

یکی از موضوعات دیگر که بسیار مهم بود و در تقسیم کار در مرکز ملی نیز به ما واگذارشده، موضوع ارزیابی، آمادگی و رزمایش‌هاست. با توجه به اینکه مدل قرارگاهی داریم و با استفاده از قرارگاه سایبری، ظرفیت‌های نیروهای مسلح اعم از سپاه، ارتش، وزارت دفاع و نیروی انتظامی را متمرکز به‌کارگیری کرده‌ایم و در مأموریت‌هایی که مرکز ملی براساس تقسیم کار واگذار کرده، حوزه ارزیابی، آمادگی و کشف آسیب‌پذیری زیرساخت‌ها را به ما واگذار کرده‌اند. در دو، سه سال گذشته بیش از ۳۰۰ رزمایش تخصصی انجام داده‌ایم. سالی ۱۰۰ تا ۱۵۰ رزمایش با توجه به موضوعات برگزار شده‌اند، ولی درمجموع ۳۰۰ رزمایش انجام شده است. تمام دستگاه‌هایی که موردنظر بوده تک‌به‌تک ارزیابی و اشکالات را استخراج و آسیب‌ها را شناسایی کرده‌ایم و درنهایت معماری و اشکالات نرم‌افزاری و مدیریتی و غفلت‌ها و حفره‌های امنیتی و... استخراج شده‌اند، سپس در دستورات بعدی ابلاغ کرده‌ایم این اقدامات انجام شوند. هر دوره سراغ اینها می‌رویم که پیگیری انجام کارها را داشته باشیم. در گذشته که در این زمینه قانونی نداشتیم در حد توصیه و پیگیری بود، ولی امروز وقتی دستگاهی را ارزیابی و ۱۰ اشکال پیدا می‌کنیم، به دستگاه ابلاغ می‌شود و زمان می‌دهیم که اینها را براساس توافق برطرف کند، بعد از زمان تعیین‌شده اگر برطرف نکرد می‌توانیم برخورد قانونی داشته باشیم، یعنی برخورد حقوقی و قانونی معین شده است. اگر اتفاقی افتاد، داده‌ای از دست رفت، اشکالی به وجود آمد، قابلیت پیگیری برخورد تنبیهی، قانونی و تخلفی می‌توان داشت؛ این نکته مؤثری است که انجام شده است و دنبال می‌شود.

برای رزمایش‌ها نیز به این نتیجه رسیده‌ایم که سه دسته آسیب‌پذیری در کشور وجود دارند:

یک دسته آسیب‌پذیری معمولی است. مثلا ویندوز ۱۰ یا ویندوز ۸ دارید، ویندوز ۱۰ حفره یا آسیب‌پذیری دارد و در ورژن بعدی آنها را اصلاح و برطرف کرده است. شما اگر از سایت مادر اینها را تأمین کنید، آسیب‌پذیری‌ها برطرف می‌شوند، مثلا در حوزه ضدبدافزارها هریک خصوصیاتی خاص دارند. برای این کار دستورالعملی

آماده کرده‌ایم و دیده‌ایم سطح این آسیب‌پذیری‌ها حدود ۸۰ درصد است، یعنی از ۱۰۰ واحد آسیب‌پذیری حدود ۸۰ درصد از اینهاست، یعنی اکثریت از اینهاست. آسیب‌پذیری دوم، آسیب‌پذیری zero days است که پیچیده است. آسیب‌پذیری سوم، آسیب‌پذیری‌های کاشته شده است، یعنی ایمپلنت‌ند که کاشته شده‌اند. در سال گذشته با پدیده جدیدی به نام هوش‌مصنوعی در حملات مواجه شدیم که این چهار دسته تهدید برای ما وجود داشت؛ در بحث اول یک گام اضطراری تعریف کردیم. درواقع حدود ۶۰ هزار حفره امنیتی را در نرم‌افزارها شناسایی و آنها را در دی‌وی‌دی‌های خاص پیاده‌سازی کردیم و با دستورالعمل‌های خاصی در اختیار دستگاه‌ها قرار دادیم و تک‌تک برطرف شدند. کار پیچیده و سختی نیست، هزینه زیادی نیز نمی‌خواهد؛ ادمین سیستم باید بداند کدام‌یک را چه کار کند. اینها را به‌صورت آفلاین درآوردیم و در اختیار آنها قرار دادیم که مجبور نباشند به اینترنت متصل شوند. بخشی از دستگاه‌ها را شروع به اجرا و تک‌تک پیگیری کردیم که این کار انجام شده یا خیر. این عمل حجم زیادی از آسیب‌پذیری ما را کاهش می‌دهد. برای ایمپلنت‌ها و... طبیعتا بخش‌های تخصصی‌تر و فنی‌تر است که باید در مرحله دوم درباره آنها کار کرد. به‌عنوان یک شهروند احساس می‌کنم در مواردی سازمان پدافند غیرعامل مظلوم واقع می‌شود؛ از این نظر که پمپ‌بنزین هک می‌شود، سیستم‌ها دچار اختلال می‌شوند یا کسب‌وکاری هک می‌شود و اطلاعات مردم لو می‌رود یا به‌فروش می‌رسد یا منتشر می‌شود، حتی سازمانی- که در شهرداری یا برخی بانک‌ها این مشکل را داشتیم- پیکان حملات به‌سمت سازمان پدافند غیرعامل است.

در آن موضوع دو حوزه داریم؛ یک قانون داریم که سطح دفاع سایبری و پدافند سایبری به ما واگذار شده است. در قانون موضوع امنیت تعیین‌تکلیف جزئی نشده است. در قانون مرز امنیت و پدافند تعریف نشده است. مسئول امنیت هم معلوم نیست چطور است؛ وزارت اطلاعات مسئولیتی دارد، پلیس فتا مسئولیتی دارد. قانون واحدی نیاز است که تکلیف اینها را مشخص کند. مرکز ملی تقسیم‌بندی‌ای انجام داده؛ قسمتی را که به ما واگذار کرده‌اند پیگیری هم می‌کنیم و پاسخگو هستیم ولی خیلی از اینهایی که پیگیری می‌کنیم، در تقسیم‌بندی به ما واگذار نشده‌اند که به‌دلیل نوع تدبیری است که مرکز در پیش گرفته. اگر از ما کمک بخواهند انجام می‌شود، بنابراین پاسخگویی وجود دارد، منتها یک نکته وجود داشته که وزرا و رؤسای دستگاه‌ها در قانون هنوز مسئولیت خود را نمی‌دانستند. در جلسات می‌گفتیم مسئول امنیت شمایید و می‌گفتند به ما چه ارتباطی دارد؟ به مسئول می‌گفتیم امنیت سایبری با شماست و می‌گفت من بلد نیستم! می‌گفتم شما دستگاه خارجی می‌خرید و باید بدانید این دستگاه مشکل دارد یا ندارد. من نمی‌توانم در سیستم شما و پای دستگاه شما بنشینم و برای شما کنترل انجام دهم، این را باید خود کنترل کنید.

احساس من این بود که بسیاری از مسئولان نمی‌دانند این مسئولیت با آنهاست. وقتی نمی‌دانند مسئولیت با آنهاست به‌نوعی نسبت به مسئولیت استنکاف و تعلل و شانه خالی کردن دارند. مشکل اساسی ما قانون است. این مشکل ملی است، قانون وارد مجلس شد و به موضوعات فرعی پیچید که تحت‌عنوان صیانت و... سر آن بریده شد و موضوعات اساسی مثل بخش اول که باید توسط قانون تعیین‌تکلیف شود، مدام بدون‌تکلیف باقی ماند. در موضوع دفاع و امنیت نیز بلاتکلیف بوده و تعیین مسئولیت در دستگاه‌ها نیز اینچنین بوده است. اینها مسائل ساده‌ای است که قانون می‌تواند تعیین‌تکلیف کند و مطابق قانون نیز الزامات و ابزارها در اختیارشان قرار گرفته است تا پاسخگو باشند. در شرایط موجود به‌دلیل فقدان قانون چندان پاسخگویی دقیق و درستی وجود ندارد و ممکن است هرکسی از منظر خود پاسخ دهد. یک جنبه هم افکار عمومی است که برخی نمی‌دانند موضوع چیست و چه تقسیم‌بندی‌هایی دارد و ما نیز به‌دلیل طبقه‌بندی بسیاری از مسائل را نمی‌توانیم بیان کنیم.

اهمیت راهبردی پدافند سایبری برای امنیت ملی ایران

و معرفی اهداف کلان و راهبردهای این حوزه

سردار محمدرضا فرجی پور؛ جانشین قرارگاه پدافند سایبری کشور

اهمیت راهبردی امنیت و پدافند سایبری فقط در حفاظت از داده‌های حساس کشور نیست، بلکه در میان دستاوردهای ارزشمند حاصل از اقدامات این حوزه، رسالت پاسداری از امنیت ملی و ثبات اقتصادی نیز دیده می‌شود. حملات سایبری می‌توانند زیرساخت‌های حیاتی، حساس و مهم کشور را مختل و عملیات نظامی را دچار مخاطره کنند، حتی بر انتخابات کشور در مقاطع مختلف تأثیر بگذارد.

با ظهور جنگ سایبری، مفاهیم سنتی میدان‌های جنگ گسترش یافته و فضاهای مجازی را دربرمی‌گیرد، جایی که دشمنان کشور تلاش می‌کنند با نفوذ به زیرساخت‌های حیاتی، حساس و مهم کشور آنها را درخطر اختلال و خرابکاری قرار دهند.

با توجه به سرعت فزاینده توسعه فناوری‌های اطلاعاتی، ارتباطی و رایانه‌ای، برای پدافند سایبری کشور نیازمند تعریف رویکردهای جدید هستیم و باید به سمت بومی‌سازی محصولات امنیت حرکت کنیم. نگاه ما به جنگ در آینده، تلفیقی از جنگ نظامی و سایبری است. همین امروز اگر جنگی در دنیا روی دهد، بدون شک بخشی از آن جنگ سایبری خواهد بود؛ کمااینکه در حملات صورت‌گرفته در جهان بارها این پدیده را شاهد بوده‌ایم. ما به رویکردهای جدیدی برای پدافند سایبری در کشور نیاز داریم؛ چراکه کارشناسان جهان بر این باورند هکرها به‌راحتی از پروتکل‌های امنیتی موجود عبور می‌کنند. در این راستا باید ادبیات جدیدی تولید کنیم که پاسخگوی نیازهای کشور ما باشد و برای این کار نباید منتظر آمریکا یا هیچ کشور پیشرفته دیگری باشیم.

پدافند سایبری می‌تواند با نظارت بر تمامی سازمان‌های حیاتی، حساس و مهم در کشور، نقاط ضعف امنیت و پدافند سایبری در چنین سازمان‌هایی را شناسایی کند و راهنمایی‌ها و دستورالعمل‌هایی در اختیار آنها قرار دهد تا نقاط ضعف کشف‌شده را برطرف کنند و سطح امنیت و آمادگی پدافندی سایبری خود را به سطح مطلوب و موردنظر برسانند. همچنین سازمان‌های

علی‌رغم تمامی تهدیدهای سایبری که علیه زیرساخت‌ها و امنیت جمهوری اسلامی ایران وجود دارد و حملات هکری که هر روز رخ می‌دهند، مسئولان و سازمان‌ها نوعاً توجه زیادی به امنیت سایبری ندارند. درواقع می‌توان گفت بسیاری از مدیران حساس‌ترین سازمان‌ها درکشور، امنیت و پدافند سایبری را کالایی لوکس می‌دانند. این در حالی است که با افزایش تنش‌های بین ایران و غرب، تعداد حملات سایبری به زیرساخت‌های کشور روزبه‌روز در حال افزایش است.

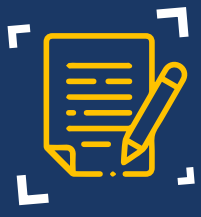
در عصری که چشم‌انداز آینده، میدان‌های دیجیتال نبرد جدیدند، نقش کارشناسان امنیت سایبری در حفاظت از زیرساخت‌های حیاتی و اطلاعات حساس یک کشور اهمیت زیادی یافته است

تجاری و غیردولتی نیز می‌توانند از مشاوره‌های سازمان پدافند غیرعامل کشور در موضوع حساس امنیت و پدافند سایبری استفاده کنند تا بخش‌های صنعت و تجارت در مقابل حملات سایبری مصون بمانند. البته علی‌رغم تمامی تهدیدهای سایبری که علیه زیرساخت‌ها و امنیت جمهوری اسلامی ایران وجود دارد و حملات هکری که هر روز رخ می‌دهند، مسئولان و سازمان‌ها نوعاً توجه زیادی به امنیت سایبری ندارند. درواقع می‌توان گفت بسیاری از مدیران حساس‌ترین سازمان‌ها در کشور، امنیت و پدافند سایبری را کالایی لوکس می‌دانند. این درحالی است که با افزایش تنش‌های بین ایران و غرب، تعداد حملات سایبری به زیرساخت‌های کشور روزبه‌روز درحال افزایش است. در عصری که چشم‌انداز آینده، میدان‌های دیجیتال نبرد جدیدند، نقش کارشناسان امنیت سایبری در حفاظت از زیرساخت‌های حیاتی و اطلاعات حساس یک کشور اهمیت زیادی یافته است. برای ذهن‌های جوانی که به آینده‌ای روشن و کشوری مصون دربرابر تهدیدهای سایبری فکر می‌کنند، درک اهمیت نقش‌های بالقوه آنها در پدافند سایبری کشور می‌تواند به تصمیم‌گیری آنها در روند ارتقای دانش و فناوری خود کمک کند.

سازمان‌ها، مدیران، متخصصان و کارشناسان امنیت و پدافند سایبری به‌عنوان پاسداران و محافظان حاکمیت دیجیتال یک کشور عمل می‌کنند و از امنیت ملی کشور دربرابر تهدیدهای سایبری پیچیده و حملات احتمالی محافظت می‌کنند. خبرگی و تخصص آنها می‌تواند به تقویت شبکه‌های دولتی، سامانه‌های نظامی و پایگاه‌های اطلاعاتی دربرابر عملیات جاسوسی خارجی و جنگ سایبری منجر شود و البته کوتاهی، ترک فعل، تقصیر و قصور آنها نیز می‌تواند تبعات ناگواری برای کشور درپی داشته باشد. در چشم‌انداز پویای پدافند سایبری ملی، کارشناسان امنیت و پدافند سایبری کمک شایان‌توجهی به توسعه فناوری‌های پیشرفته و راه‌حل‌های نوآورانه می‌کنند.

آنها همچنین تضمین می‌کنند کشور در خط مقدم قابلیت‌ها و توانمندی‌های پدافند سایبری باقی می‌ماند. مدیران، متخصصان و کارشناسان امنیت و پدافند سایبری نقشی محوری در ابداع استراتژی‌های دفاعی فعال و توسعه پروتکل‌های امنیت و پدافند سایبری قوی برای مقابله با چنین تهدیدهایی دارند. تخصص و خبرگی آنها به ایجاد سیستم‌های دفاعی پیچیده، الگوریتم‌های رمزگذاری و شبکه‌های ارتباطی امن کمک می‌کند، درنتیجه توانمندی کلی فناورانه کشور را افزایش می‌دهد.

حمله استاکس‌نت و تهدیدها و حوادث سایبری مشابه آن، نشان‌دهنده رابطه‌ای نزدیک بین امنیت ملی و امنیت و پدافند سایبری است. تضمین امنیت و پدافند سایبری برای حفظ امنیت ملی و قوی و بازدارنده بودن یک کشور در نظام بین‌الملل بسیار مهم است، بنابراین سرمایه‌گذاری در توسعه قابلیت‌های سایبری، اهمیت دادن به ارزش نیروی انسانی متخصص در این عرصه، به‌روز ماندن درخصوص آموزش‌ها، پژوهش‌ها و پیشرفت‌های علمی و فناوری فعلی و تدوین راهبردهای مؤثر امنیت ملی برای مبارزه با تهدیدهای سایبری بسیار حیاتی است، درنتیجه باید خط‌مشی امنیت و پدافند سایبری پویا را پی گرفت و برای رساندن کشور جمهوری اسلامی ایران به قدرت سایبری در تراز قدرت‌های تاثیرگذار جهانی و برخوردار از ابتکار عمل و قدرت تعامل با دیگر کشورها و حفاظت از منافع خود در سطح بین‌المللی و کاهش تهدیدهای سایبری با روحیه جهادی و بسیجی طراحی، برنامه‌ریزی و اقدام کنیم.



سرمقاله

پدافند سایبری ضامن امنیت ملی

ابوالقاسم رحمانی
سردبیر

روزگار امروز ما جهانی آمیخته با تکنولوژی و جهان های مجازی شده است. برخلاف دهه های پیشین و سال های اولیه توسعه تکنولوژی در جهان- که می شد تفکیکی جدی بین زیست واقعی و زیست مجازی شده- ایجاد کرد، این بار ادغام این دو ساحت به قدری درهم آمیختگی دارد که امکان انفصال شان چندان شدنی نیست. فراگیری توسعه تکنولوژی و به تبع آن، تغییراتی که در جوامع انسانی ایجاد کرده، به قدری است که می توان ردپایش را در ابعاد مختلف آن جست وجو کرد و یافت. از تحولات زیست روزمره انسانی، مسکن و حتی خوراک و پوشاک به عنوان نیازهای اولیه بشر گرفته تا کلان حوزه هایی همچون اقتصاد، سیاست و حتی آنسوتر، دیپلماسی و جنگ و صلح! در بین این تحولات اما آنچه بعضا از چشم تحلیلگران و فضای نخبگانی به دور است، توجه به قلب ماهیت مفهومی به نام «ایران» در میان زدوخوردها و حواشی مجازی است و اینکه

اساسا ایران و مرزهایش در این دنیای جدید مجازی شده و عصر سایبری چطور تعریف می‌شود؟ تهدیدها و فرصت‌های زیست در این دنیای جدید چیستند و راه‌های درست مقابله و مواجهه با آنها باید چطور فهم شوند؟ مسئله پدافند سایبری که امروزه باید بیش از پیش و فراتر از هر چیزی مورد توجه قرار بگیرد، در میان این پازل‌ها چطور قرار می‌گیرد و چه چشم‌اندازی برای پیشبرد این حوزه طراحی شده است؟ خصوصا آنکه اگر اقدامات پدافند غیرعامل را در سیر تاریخی مورد مطالعه قرار دهیم، اقدامات پیشگیرانه کشورها و دولت‌های مختلف با هدف حفظ امنیت، ادامه حیات و حفظ سرزمین، جلوگیری از غافلگیری‌های نظامی و امنیتی و ارتقای توان رزم محسوب کنیم، هنوز هم در آستانه قرن بیست‌ویکم، جهان آکنده از منازعات ژئوپلیتیک بوده و نشانه‌ای از خاتمه قریب‌الوقوع درگیری‌های مسلحانه دیده نمی‌شود، بنابراین انجام اقدامات پدافند غیرعامل توسط کشورهای مختلف استمرار داشته و جایگاهش را به عنوان نیاز حیاتی حفظ کرده و با روش‌های مختلف ادامه یافته است. اگر در جهان واقعی ما قدرت موشکی اول منطقه هستیم، امتداد این قدرت موشکی در فضای سایبری چه شرایط و الزامات و ضرورتی دارد؟

مروری کوتاه بر شکل‌گیری پدافند سایبری در ایران

پاسخ به سؤالات مطرح‌شده در این جستار، نیازمند مروری اجمالی بر چرایی شکل‌گیری پدافند غیرعامل و پدافند سایبری در ایران است. حتما مسئله دفاع در برابر تهدید این حوزه و تبیین الزامات و ضرورت‌هایش گامی مهم در راستای فهم «ایران سایبری» است.

سازمان پدافند غیرعامل کشور در سال ۱۳۸۲ براساس فرمان مقام معظم رهبری (مدظله العالی) تشکیل شد. این سازمان، سازمانی دولتی در ایران است که از حیث ساختاری زیرمجموعه ستاد کل نیروهای مسلح محسوب می‌شود. ازآنجاکه یکی از مهم‌ترین وظایف ستادی این سازمان «تبیین و برآورد تهدیدهای دشمن در حوزه‌های مختلف» است، رفته رفته قرارگاه‌هایی با محوریت‌های گوناگون حول این سازمان شکل گرفتند که یکی از مهم‌ترین‌های آن قرارگاه پدافند سایبری به شمار می‌رود.

پدافند سایبری که درواقع پدافند غیرعامل سایبری است، در بدو امر متمرکز بر اقدامات پیش‌کنشی و پیش‌نگری در حوزه تأمین توانمندی‌های پیشگیرانه دفاعی و مصون‌سازی است. به این معنا که با توجه به تهدیدهای مربوطه نقاط قوت و ضعف شناسایی می‌شود و برای کاهش مبتنی بر کم شدن نقاط ضعف و ارتقای نقاط قوت تلاش لازم صورت می‌گیرد.

درخصوص تهدیدهای این حوزه اما به گفته کارشناسان، ابعاد فنی مانند شبکه‌های بات، تهدیدهای فیشینگ، تهدیدهای شبکه‌های اجتماعی یا مهندسی اجتماعی و بدافزارهای مختلف، می‌تواند از تهدیدهای سایبری باشد، به عنوان مثال در سال ۲۰۱۰ حمله‌ای علیه تأسیسات هسته‌ای اتفاق افتاد که در آن زمان گفتند با استفاده از بدافزاری به نام استاکس‌نت انجام شده است. مشهور است که استاکس‌نت اولین سلاح سایبری در دنیا بود که توسط دولت‌های رسمی به‌کار گرفته شد و سعی کردند اختلالی را در زیرساخت حیاتی یک کشور ایجاد کنند. آمارهای تهدیدها و فراتر از آن حملات سایبری در ایران نیز این مؤید این مسئله‌اند، برای مثال طبق گزارش شرکت ارتباطات زیرساخت وزارت ارتباطات و فناوری اطلاعات، طی ۲۱ ماه ۴۳۰ هزار حمله DDoS به ۷۹ هزار مقصد سایبری در کشور صورت گرفته، همچنین در بخش تکمیلی این گزارش براساس اطلاعات منتشرشده، درطول این مدت ۴۳۰۳۲۲ مورد حمله به ۷۹۴۷۸ مقصد صورت گرفته است. از این تعداد حدود هزار مقصد بیش از ۴۳ مرتبه مورد حمله قرار گرفته‌اند و بیش از ۶۲۶۶۸۸۰ مقصد نیز تحت محافظت قرار گرفته‌اند، بنابراین چنانچه از آمارهای رسمی قابل برداشت است، تهدیدهای سایبری و حملات مرتبط با آن همه زیرساخت‌های حیاتی کشور را تهدید می‌کند و در این وضعیت جنگی، حتما بیش از هر زمان دیگری به پدافند سایبری نیازمندیم.

اکنون کجای راهیم؟

اتفاقاتی همچون هک اسنپ‌فود، تلویزیون و صداوسیما در زمان آشفتگی‌های سال ۱۴۰۱، هک پمپ بنزین‌ها و صف‌هایی طولانی که در پی اختلالات الکترونیکی در آن دوره پدید آمد و... ممکن است این مسئله را به ذهن متبادر کند که توانایی دفاعی یا همان پدافند سایبری ایران دارای ضعف‌ها و خلل‌های جدی

است. کما اینکه هرکدام از این ناامنی های سایبری با هر دلیل و انگیـزه‌ای کـه اتفاق بیفتد، ممکن اسـت اطلاعات و حریم خصوصی افراد زیادی را به خطر بیندازد و زندگی مردم جامعه رامختل کند؛ مشابه اتفاقی که اخیرا در ماجرای انفجار پیجرها و دستگاه‌های الکترونیکی در لبنان، مردم آن کشور با آن مواجه شدند و صدمات زیادی دیدند.

در ایـران یکـی از قابل توجه تریـن این حمـلات در آذر ۱۴۰۲ رخ داد کـه منابع سـوخت کشـور را هدف قـرار داد. گروهی به نام «گنجشک درنده» مسئولیت این حمله را برعهده گرفت. این حمله به اختلال شدید و تعطیلی بخشی از پمپ بنزین‌ها در سراسر ایران منجر شد. این گروه- که احتمالا با منافع اسرائیلی مرتبـط اسـت- پیش‌تر نیـز در حوادث سـایبری مختلف در ایران فعال بود و نقاط زیرساختی مختلفی مانند سیستم‌های راه‌آهن را هدف قرار داد. این ماجرا به خاطر درگیری وسیعی که در اذهان عمومی جامعه ایجاد کرد، در ذهن‌ها ماندگار شـد، اما جز این اتفاق، ماجرای دیگری که تهدید مهمی برای کشور تلقی می‌شد، حمله استاکس نت (Stuxnet) بود. این حمله یک برنامه ویژه مخرب سایبری بود که به صورت خاص برای هدف قرار دادن و اختلال در برنامه‌ی هسته‌ای ایران طراحی شده بود. این ویروس که اولین بار در سال ۲۰۱۰ کشف شد، قابلیت‌های پیچیده‌ای داشت و به نظر می‌رسید توسط یک یا چند دولت ساخته شده باشد. اما برای ارزیابی واقعی این مسئله که جایگاه ایران در این حوزه چطور قابل ارزیابی است و به عبارتی ما کجای راهیم؟ می‌توان به شاخصی ویژه اعتماد کرد. شاخص جهانی امنیت سایبری (GCI) یک ابزار ارزیابی است که توسط سازمان بین‌المللی ارتباطات (ITU) توسعه یافته که نهادی وابسته به سازمان ملل متحد است. این شاخص برای ارزیابی وضعیت آمادگی کشورها در مقابله با تهدیدهای سایبری و توانایی‌های آنها در حفظ امنیت فضای سایبری طراحی شده است.

در آخرین ارزیابی GCI که در سال ۲۰۲۰ منتشر شد، ایران امتیاز ۸۱٫۰۷ را از ۱۰۰ امتیاز دریافت کرده است. در این گزارش امنیت سایبری ایران از همسایه‌هایش یعنی افغانستان و عراق قوی‌تر ارزیابی شده است. این شاخص به کشورها کمک می‌کند درک بهتری از وضعیت خود در زمینه امنیت سایبری داشته باشند و نواقص و چالش‌های خود را شناسایی کنند، بنابراین در توصیف وضع موجود می‌توان چنین گفت که وضع‌مان بد نیست، اما با توجه به این گزاره که تکنولوژی متوقف شدنی نیست، توسعه این حوزه نیز انتها ندارد و همواره باید به‌روز بود و در صدر این توسعه‌یافتگی‌ها به اصل «بومی‌سازی» پایبند بود!

درواقع سند راهبردی پدافند سایبری کشور و اصول و راهبردهای ذکرشـده در آن حاوی اصول و نکاتی ضروری اسـت که حتما پایبندی به آنها، توسعه این حوزه را بیش از پیش شدنی می‌کند. در میان این اصول هفده‌گانه اما از منظر بسیاری از متخصصان این حوزه، مسئله بومی‌سازی یا همان دفاع بومی، از مهم‌ترین اصول به شمار می‌رود. مهم‌تر آنکه این بومی‌سازی بیش از هر چیزی، نیاز به ایده خودباوری و مامی توانیم دارد که لازمه آن تولید ادبیات و فرهنگ‌سـازی در این حوزه برای همراه کردن اذهان عمومی جامعه است. هرچند بومی‌سازی نیاز به تکنولوژی قوی و پیشرفته در این حوزه دارد، کاری شدنی است. جهت رسیدن به این مهم، می‌بایست در بحث شبکه و هسته‌های مرکزی از فناوری‌های بومی اسـتفاده شـود و اگر از محصولات خارجی اسـتفاده می‌شـود تا جای امکان باید آزمایش‌های استاندارد به خصوص در حوزه‌های امنیت سایبری- چه از نظر فیزیکی و چه از نظر نرم‌افزاری- انجام شود. هرچند پاسخ ایران به این تهدیدهای سـایبری در طول زمان تکامل یافته و ایران توانسته توانایی‌های سایبری خود را بهبود بدهد. یک نمونه اخیر از این توسعه‌یافتگی را می‌توان در حملات وعده صادق ۱ و ۲ مشاهده کرد. رویدادهای ویژه و عظیم نظامی- امنیتی که در بعد سایبری توانستند پیچیدگی دفاعی ایران را بیش از پیش نمایان کنند.

چه خواهد شد؟

اینکه چه چیزی در آینده پدافند سـایبری در انتظار ماسـت، چنـدان پیچیـده و غیرقابل حـدس نیسـت. باج‌افزارهـای پیچیده‌تر، افزایش تعداد حملات سایبری، افزایش تهدیدهای سـایبری و... از جمله خطرات و آسـیب‌هایی خواهند بود که این فضا را تهدید خواهد کرد. لازم به ذکر است اگر حداکثر توان اجرایی در جهت حرکت در چهارچوب اصول سـند راهبری پدافند سـایبری به کار گرفته شـود، این آسـیب‌ها به حداقل خواهند رسید. در دوره کنونی پدافند سایبری مهم‌ترین ضامن حفظ و ارتقای امنیت ملی است.

یادداشت

پدافند سایبری پاسداری از حکمرانی ملی در جغرافیای فناوری

محمد اسکندری

دکتری جامعه‌شناسی سیاسی جمهوری اسلامی ایران

در دنیای امروز، فناوری اطلاعات و ارتباطات به یکی از اساسی‌ترین پیشران‌های توسعه اجتماعی، اقتصادی، سیاسی و امنیتی بدل شده است. این فناوری با نفوذ عمیق درتمام ابعاد و مناسبت زندگی بشر، سازه‌های حکمرانی را نیز تحت‌تأثیر خود قرار داده است. در این طوفان فناورانه کشورهایی که بتوانند با تحولات سریع همگام شوند، توانایی استمرار و تقویت حکمرانی خود را خواهند داشت، درحالی‌که جوامعی که به مقابله با این تحولات برخیزند، محکوم‌به عقب‌ماندگی و شکست خواهند بود.

در جهانی که آینده آن وابسته به فناوری است، توانایی تسلط بر فناوری اطلاعات و ارتباطات از مؤلفه‌های کلیدی قدرت محسوب می‌شود. برخلاف

تصوری که برخی نورسانه‌ها تلاش می‌کنند برساخته کنند، مصرف فناوری الزاما نسبتی با پیشرفت ندارد و واقعیت این است که کشورها با تولید و توسعه زیرساخت‌های فناورانه است که می‌توانند تولید قدرت ملی کنند. به‌زعم راقم این سطور حکمرانی در آینده- چه در سطح ملی و حتی چه در سطح بین‌المللی- به کشورهایی تعلق خواهد داشت که به‌جای مصرف‌گرایی، تولیدگر فناوری باشند و بر عمق این حوزه اشراف کامل داشته باشند.

رهبر معظم انقلاب اسلامی چندی پیش در دیدار مسئولان دولت چهاردهم تعبیر دقیقی در این خصوص داشتند. ایشان درباره مصداق هوش‌مصنوعی فرمودند: «امروز هوش‌مصنوعی با یک شتاب حیرت‌دهنده‌ای [دارد پیش می‌رود]، یعنی انسان متحیر می‌شود از شتابی که این فناوری عجیب در دنیا پیدا کرده و دارد پیش می‌رود... در مسئله هوش‌مصنوعی، بهره‌بردار بودن امتیاز نیست؛ این فناوری لایه‌های عمیقی دارد که باید بر آن لایه‌ها مسلط شد؛ آن لایه‌ها دست دیگران است. اگر شما نتوانید لایه‌های عمیق و متنوع این فناوری هوش‌مصنوعی را تأمین کنید، فردا اینها یک ایستگاهی مثل آژانس اتمی درست می‌کنند برای هوش‌مصنوعی- که الان دارند مقدماتش را فراهم می‌کنند- که اگر چنانچه به آن ایستگاه رسیدید، باید اجازه بگیرید که در فلان بخش از هوش‌مصنوعی استفاده کنید، در فلان بخش دیگر حق ندارید استفاده کنید! این جوری است؛ زرنگ‌های دنیا، فرصت‌طلب‌ها و قدرت‌طلب‌های دنیا دنبال این چیزها هستند...»

تولید و کنترل زیرساخت‌های فناورانه، به‌ویژه در حوزه امنیت سایبری، به‌عنوان یکی از مهم‌ترین الزامات حفظ و ارتقای حکمرانی کشورها در عصر دیجیتال مطرح است. مصرف‌گرایی صرف نه‌تنها کشورهای وابسته را دربرابر تهدیدها آسیب‌پذیر می‌کند، بلکه آنها را از تسلط و استقلال فناورانه محروم می‌سازد.

کشورهایی که به‌جای مصرف‌گرایی به تولید فناوری و زیرساخت‌ها روی آورده‌اند، می‌توانند مدعی حکمرانی مؤثر در فضای دیجیتال باشند.

جمهوری اسلامی ایران با درک اهمیت تسلط بر فضای سایبری، طی دو دهه گذشته اقدامات متعددی در راستای حفظ امنیت و استقلال در دستور کار قرار داده است. تأسیس شورای فراقوه‌ای فضای مجازی و مرکز ملی فضای مجازی ازجمله این اقدامات است که با هدف سیاستگذاری و تحکیم حکمرانی ایرانی اسلامی در این عرصه شکل گرفته‌اند.

از سوی دیگر تشکیل سازمان پدافند غیرعامل کشور در دو دهه گذشته با تدبیر مقام معظم رهبری (مدظله‌العالی) نیز به‌منظور حفاظت از زیرساخت‌های حیاتی دربرابر تهدیدهای سایبری و نوین ایجاد یک جبهه جدید دربرابر الگویی از جنگ و تهدید است که به عرصه سایبری سرریز شده است.

این سازمان با تمرکز بر رصد تهدید، کشف آسیب‌پذیری‌ها، ارتقای آمادگی زیرساخت‌ها و همچنین توسعه نظام صنایع بومی پدافند سایبری، به‌دنبال ایجاد یک لایه دفاعی و آرایشی نوین از دفاع در بخش غیرنظامی است. برخلاف قاب‌های ناصحیح رسانه‌ای، جمهوری اسلامی ایران یکی از بزرگ‌ترین قربانیان حملات سایبری از گذشته تا امروز بوده و اکنون نیز به آزمایشگاه تهدیدهای نوین دشمن بدل شده است. در چنین فضایی توسعه و بسط مفاهیم پدافند سایبری به‌عنوان یکی از زیرساخت‌های اساسی اعمال حاکمیت جمهوری اسلامی در جغرافیای فناوری‌محور می‌تواند راهگشا باشد.

آنچه در پیش رو دارید گفت‌وشنودی بین ما و صاحب‌نظران حوزه پدافند غیرعامل است تا به‌مرور راهی پرداخته شود که آمده‌ایم و آینده‌ای که پیش روست. امید است موردتوجه مخاطبان عزیز و ارجمند نشریه «عماد» قرار گیرد.

تهدیدها و فرصت‌های هوش مصنوعی در امنیت سایبری

هادی کریمی‌نیسیانی

معاون فنی قرارگاه پدافند سایبری کشور

تعاریف مختلفی از هوش مصنوعی (AI) وجود دارد که البته اغلب آنها دارای اشتراکات زیادی‌اند:

-هوش مصنوعی، مطالعه و توسعه سیستم‌های کامپیوتری که می‌توانند رفتار هوشمند انسان را تقلید کنند. هوش مصنوعی برای تشخیص ویژگی‌های شخصیت به همان روشی که مغز انسان انجام می‌دهد، عمل می‌کند.

-هوش مصنوعی، شامل نظریه‌ها و توسعه سیستم‌های کامپیوتری است که قادر به انجام وظایفی هستند که معمولا به هوش انسانی نیاز دارند، مانند ادراک بصری، تشخیص گفتار، تصمیم‌گیری و ترجمه بین زبان‌ها.

-هوش مصنوعی، هوش ماشین‌ها یا نرم‌افزارهاست که برخلاف هوش انسان‌ها یا حیوانات است. این موضوع رشته مطالعاتی در علوم کامپیوتر است که ماشین‌های هوشمند را توسعه و مطالعه می‌کند. اصطلاح هوش مصنوعی ممکن

است به خود ماشین‌های هوشمند نیز اشاره داشته باشد. در ابتدا هوش مصنوعی (AI) به‌عنوان مفهومی برای تقلید از مغز انسان و برای بررسی مشکلات دنیای واقعی با رویکرد انسانی کل‌نگر معرفی شد. می‌توان آن را ترکیبی از فناوری اطلاعات و هوش فیزیولوژیکی دانست که می‌تواند به‌صورت محاسباتی برای رسیدن به اهداف مورداستفاده قرار گیرد. هوش مصنوعی امکان استفاده و پردازش حجم زیادی از داده‌های ذخیره‌شده را به‌صورت هوشمند و امکان ایجاد ابزارهای کاربردی را فراهم می‌کند. این هوش برای ارائه برنامه‌های هوشمند در زمینه‌های مختلف مانند دفاع، مراقبت‌های بهداشتی و اکتشاف فضا و... مورداستفاده قرار گرفته است. سازمان‌ها برای ارائه امنیت اطلاعات بهتر در برابر مهاجمان ماهر از هوش مصنوعی در امنیت سایبری استفاده می‌کنند. این هوش به خودکارسازی فرایندهای پیچیده برای شناسایی حملات و واکنش به نقض سیستم‌های اطلاعاتی کمک می‌کند. این نوع برنامه‌ها با بهره‌گیری از هوش مصنوعی در حال توسعه‌اند و پیشرفته‌تر و جامع‌تر می‌شوند. یادگیری ماشینی حوزه اصلی هوش مصنوعی است و به فناوری‌هایی اشاره دارد که ابزاری برای آموزش رایانه‌ها جهت یادگیری و تطبیق از طریق تجربه فراهم می‌کنند. این مؤلفه فناورانه شناخت انسان را تحریک می‌کند، مانند یادگیری از تجربه و الگوها به‌جای استدلال (علت و معلول).

مزایای استفاده از هوش مصنوعی در حوزه پدافند سایبری

مقرون به صرفه بودن: کنار هم قرار دادن cybersecurity و AI به جمع‌آوری سریع‌تر داده منجر می‌شود، درنتیجه مقابله با تهدیدها، به‌صورت پویاتر و مؤثرتر انجام خواهد گرفت. ضمن اینکه نیاز متخصصان امنیت به انجام کارهای دستی و وقت‌گیر را از بین می‌برد، بنابراین آنها می‌توانند تمرکز بیشتری روی فعالیت‌های استراتژیک داشته باشند و ارزش کسب‌وکارشان را بالا ببرند.

کاهش خطاهای انسانی: یکی از نقاط ضعف رایج در روش‌های قدیمی تأمین امنیت، نیاز به مداخله انسانی بود که گاهی خطاهای صورت گرفته، منجر به خسارت‌های مالی هنگفتی می‌شد. اما در حال حاضر هوش مصنوعی، فاکتور انسانی را از اکثر فرایندهای امنیتی حذف کرده است. قطعا این رویکرد، بسیار مؤثرتر و کارآمدتر بوده، زیرا منابع انسانی را می‌توان در قسمت‌هایی به کار گرفت که بیشتر موردنیاز است.

یادگیری مداوم در شبکه زیرساخت: هوش مصنوعی به‌طور مداوم با داده‌های جدید در حال به‌روزرسانی و learning است، بنابراین قابلیت‌های AI در حال تکامل و بهبود است. تکنیک‌هایی مانند deep learning و ML به هوش مصنوعی این امکان را می‌دهند که علاوه بر شناسایی الگوها، یک خط مبنایی براساس فعالیت‌های منظم ایجاد و هر فعالیت مشکوکی را شناسایی کند که از آن مبنا منحرف شود. توانایی این هوش در یادگیری مداوم، تأثیر بسزایی در دشوار شدن مراحل کار هکرها دارد.

کشف تهدیدهای ناشناخته (مانند Zero Days، APT و...): با ابداع بردارهای جدید و پیچیده حملات توسط مهاجمان سایبری، سازمان‌ها در برابر تهدیدهای ناشناخته، آسیب‌پذیرتر می‌شوند، اما AI توانایی ارائه راهکار برای آسیب‌پذیری‌هایی را دارد که هنوز توسط ارائه‌دهندگان نرم‌افزار، شناسایی یا اصلاح نشده‌اند.

پشتیبانی و تحلیل حجم وسیع داده‌ها: سیستم‌های مبتنی بر هوش مصنوعی می‌توانند حجم وسیعی از داده‌ها را مدیریت کنند که متخصصان امنیت قادر به انجام آن نیستند. به‌این‌ترتیب سازمان‌ها می‌توانند به‌صورت خودکار، تهدیدهای جدید را در میان حجم فراوانی از داده‌ها و ترافیک شبکه تشخیص دهند که ممکن است توسط سیستم‌های قدیمی شناسایی نشوند.

بهبود مدیریت و برطرف‌سازی آسیب‌پذیری‌ها به کمک هوش مصنوعی: هوش مصنوعی به سازمان‌ها این توانایی را می‌دهد که علاوه بر کشف تهدیدهای جدید، بتوانند آسیب‌پذیری‌ها را بهتر مدیریت کنند. درحقیقت «توان ارزیابی مؤثرتر»، «بهبود قدرت حل مسئله» و همین‌طور «قابلیت تصمیم‌گیری بهتری» را در اختیار آنها قرار می‌دهد. ضمن اینکه نقاط ضعف شبکه‌ها و سیستم‌ها را شناسایی

کـرده تا سـازمان‌ها همواره روی مهم‌تریـن وظایف امنیتی خود متمرکز شوند.

نظارت بر ترافیک شبکه با هوش مصنوعی: حجم عظیمی از تبادل داده بین شرکت‌ها و مشتریان از طریق شبکه سازمانی وجود دارد. هوش مصنوعی به هکرها و هرکسی توجه دارد که مایل به دسترسی غیرمجاز به این اطلاعات خصوصی است و از آنها جلوگیری می‌کند. از سوی دیگر متخصصان امنیـت فنـاوری اطلاعات نمی‌توانند به‌طور مسـتقل این ترافیـک را ارزیابـی کنند که هوش مصنوعی به‌تنهایی این موضوع را حل کرده است.

کاهش فرایند تکراری با هوش مصنوعی: مجرمان سـایبری همیشه به‌دنبال روش‌های جدید برای نفوذ به شبکه‌های شرکت‌ها و سرقت اطلاعات ارزشمند آنها هستند. ما تمایل داریم از همان اقدامات امنیتی اساسی روزانه استفاده کنیم. اگر متخصصان امنیت انسانی خسته شوند، ممکن است شبکه شما در معرض مهاجمان قرار گیرد. هوش مصنوعی در کاهش فرایندهای خسته‌کننده نقش دارد.

بهبـود وضعیت کلـی امنیت: مدیریت طیف گسـترده‌ای از تهدیدهـای اعـم از phishing، denial-of-service (DoS) و باج‌افزارهـا و... دشـوار و زمانبـر اسـت، امـا مدیریتی که با هوش مصنوعی همراه باشد، به سازمان‌ها قدرت می‌دهد انواع مختلفی از حملات را در لحظه شناسایی و مدیریت کنند.

تصمیم‌گیری بهتر و سریع‌تر: مسلما تشخیص تهدیدها، از ضروری‌ترین المان‌های امنیت شبکه است و امنیت سایبری که مبتنی بر هوش مصنوعی باشد، می‌تواند به تشخیص سریع و در لحظه بینجامد. هوش مصنوعی در امنیت سایبری به سازمان‌ها کمک می‌کند نقاط ضعف احتمالی را در استراتژی‌های امنیتی خود شناسایی کنند. به‌این‌ترتیب قادر خواهند بود روش‌های مناسب‌تری را برگزیده تا سطح امنیت و پدافند خود را بهبود بخشند.

تهدیدهای هوش مصنوعی

توسعه تهدیدهای سایبری پیچیده‌تر

یکـی از بزرگ‌تریـن چالش‌هـا، پتانسـیل هکرهـا بـرای

استفاده از هوش مصنوعی برای توسعه تهدیدهای سایبری پیچیده‌تر است، به‌عنوان مثال هوش مصنوعی می‌تواند برای تولید ایمیل‌های فیشینگ واقع‌بینانه، استقرار بدافزار یا ایجاد ویدئوهای عمیق جعلی متقاعدکننده استفاده شود. همانطور که هوش مصنوعی پیشرفته‌تر می‌شود، این احتمال وجود دارد که هکرها راه‌های جدید و خلاقانه‌ای برای استفاده از آن به نفع خود پیدا کنند.

بایاس

یکی دیگر از چالش‌های مرتبط با استفاده از هوش مصنوعی در امنیت سایبری، احتمال بایاس است. سیستم‌های این هوش فقط به اندازه داده‌هایی هستند که روی آنها آموزش دیده‌اند و اگر این داده‌ها مغرضانه یا ناقص باشند، سیستم هوش مصنوعی نتایج مغرضانه‌ای ایجاد می‌کند. این امر می‌تواند به‌ویژه در زمینه‌هایی مانند تشخیص چهره مشکل‌ساز باشد که در آن بایاس به شناسایی نادرست و نتایج تبعیض‌آمیز می‌تواند منجر شود.

پتانسیل سیستم‌های هوش مصنوعی برای تصمیم‌گیری بدون نظارت انسان

یکی دیگر از نگرانی‌های هوش مصنوعی در امنیت سایبری، پتانسیل سیستم‌های این هوش برای تصمیم‌گیری بدون نظارت انسان است. درحالی‌که اتوماسیون می‌تواند در برخی زمینه‌ها مفید باشد، مهم است که اطمینان حاصل شود انسان‌ها همچنان در فرایند تصمیم‌گیری دخیلند. این امر به‌ویژه در مورد تصمیمات پرمخاطره مهم است، مانند اینکه آیا حمله سایبری در پاسخ به یک تهدید درک شده انجام شود یا خیر؟

یادگیری ماشینی و هوش مصنوعی می‌توانند به محافظت دربرابر حملات سایبری کمک کنند، اما هکرها می‌توانند با هدف قرار دادن داده‌هایی که روی آنها آموزش می‌دهند و پرچم‌های هشداری که درپی آن هستند، الگوریتم‌های امنیتی را خنثی کنند. هکرها همچنین می‌توانند از هوش مصنوعی برای شکستن سیستم‌های دفاعی و توسعه بدافزارهای جهش‌یافته استفاده کنند که ساختار آن را تغییر

می‌دهد تا از شناسایی جلوگیری کند. بدون حجم عظیمی از داده‌ها و رویدادها، سیستم‌های هوش مصنوعی نتایج نادرست و مثبت کاذب ارائه می‌دهند. اگر دستکاری داده‌ها شناسایی نشود، سازمان‌ها برای بازیابی داده‌های صحیحی- که سیستم‌های هوش مصنوعی آنها را تغذیه می‌کنند- با عواقب بالقوه فاجعه‌بار مبارزه خواهند کرد.

مثبت کاذب

یکی از مهم‌ترین معایب هوش مصنوعی در امنیت سایبری، پتانسیل مثبت کاذب است. سیستم‌های امنیتی مبتنی بر هوش مصنوعی به الگوریتم‌های یادگیری ماشینی متکی هستند که از داده‌های تاریخی یاد می‌گیرند. با این حال هنگامی که سیستم با تهدیدهای جدید و ناشناخته‌ای مواجه می‌شود که با الگوهای موجود مطابقت ندارند، این می‌تواند به نتایج مثبت کاذب منجر شود. مثبت کاذب می‌تواند به خستگی هشدار منجر شود، جایی که تیم‌های امنیتی تحت فشار تعداد زیادی هشدار نادرست قرار می‌گیرند و ممکن است تهدیدهای واقعی را از دست بدهند.

شکاف مهارت‌های امنیت سایبری

یکی دیگر از معایب هوش مصنوعی در امنیت سایبری، شکاف مهارتی است که در حال حاضر در این صنعت وجود دارد. سیستم‌های امنیتی مبتنی بر هوش مصنوعی به متخصصان ماهری نیاز دارند که بتوانند این فناوری را توسعه، پیاده‌سازی و مدیریت کنند. با این حال اکنون کمبود متخصصان با مهارت‌ها و تجربه لازم برای کار با این هوش در امنیت سایبری وجود دارد.

هزینه

پیاده‌سازی سیستم‌های امنیتی مبتنی بر هوش مصنوعی می‌تواند گران باشد، به خصوص برای سازمان‌های کوچک‌تر با بودجه محدود. این فناوری به سخت‌افزار، نرم‌افزار و متخصصان ماهر برای توسعه و نگهداری سیستم‌ها نیاز دارد.

استفاده هکرها از هوش مصنوعی

هکرها می‌توانند از هوش مصنوعی برای توسعه حملات پیشرفته‌تر و فرار از شناسایی توسط ابزارهای امنیتی مبتنی بر این هوش استفاده کنند. به‌طور مشابه، درحالی‌که فاز عصبی می‌تواند به شناسایی آسیب‌پذیری‌ها کمک کند، می‌تواند توسط هکرها برای جمع‌آوری اطلاعات در مورد نقاط ضعف یک سیستم هدف نیز استفاده شود.

سازمان‌ها باید مزایا و معایب هوش مصنوعی را در امنیت سایبری به‌دقت درنظر بگیرند و مزایا را در مقابل هزینه‌ها و خطرات آن بسنجید. پیاده‌سازی سیستم‌های امنیتی مبتنی بر هوش مصنوعی نیازمند استراتژی امنیتی جامع است که شامل سایر فناوری‌ها و تخصص انسانی برای ارائه یک دفاع لایه‌ای در برابر تهدیدها در حال تکامل است. به‌طور خلاصه، درحالی‌که هوش مصنوعی یک فناوری امیدوارکننده در فضای امنیت سایبری است، نوشدارویی برای همه چالش‌های امنیتی نیست و سازمان‌ها باید در رویکرد خود به امنیت سایبری هوشیار باشند.

هوش مصنوعی و امنیت و پدافند سایبری

هوش مصنوعی در امنیت سایبری برای تجزیه‌وتحلیل سریع میلیون‌ها رویداد و شناسایی انواع مختلفی از تهدیدها استفاده می‌شود - از بدافزاری که از آسیب‌پذیری‌های روز صفر سوءاستفاده می‌کند تا شناسایی رفتار خطرناکی که ممکن است منجر به حمله فیشینگ یا دانلود کدهای مخرب شود. این فناوری سیستمی خودآموز است که به‌طور خودکار و مداوم داده‌ها را از سراسر سیستم‌های اطلاعاتی شرکت شما جمع‌آوری می‌کند، سپس این داده‌ها تجزیه‌وتحلیل و برای انجام همبستگی الگوها در بین میلیون‌ها تا میلیاردها سیگنال مرتبط با سطح حمله سازمانی برای شناسایی انواع جدید حملات استفاده می‌شوند. با توجه به حملات سایبری و گسترش روزافزون ابزارهای امروزی، تجزیه‌وتحلیل و حل وضعیت امنیت سایبری دیگر مشکلی در مقیاس انسانی نیست. ابزارهای مبتنی بر هوش مصنوعی (AI) برای امنیت سایبری برای کمک به تیم‌های امنیت اطلاعات با ارائه نظارت لحظه‌ای

بر سطح حمله، بهبود تشخیص تهدیدهای امنیتی و اقدام فوری، به تیم‌های امنیت اطلاعات کمک می‌کنند تا ریسک نقض را کاهش دهند. با توجه به مزایای آن، سیستم‌های مدیریت وضعیت امنیت سایبری مبتنی بر هوش مصنوعی درحال افزایش محبوبیتند، زیرا سازمان‌های بیشتری توانایی خود را برای خودکارسازی تشخیص تهدید و پیش‌بینی حملات سایبری با دقت بی‌نظیر تشخیص می‌دهند.

هوش مصنوعی در امنیت سایبری فرایند تجزیه‌وتحلیل مقادیر متعددی از داده‌های ریسک و رابطه بین تهدیدها در سیستم‌های اطلاعاتی شرکت شما برای شناسایی انواع جدید حملات است. نتیجه سطوح جدیدی از اطلاعات است که تیم‌های انسانی را در دسته‌های مختلف امنیت سایبری، ازجمله موجودی دارایی‌های فناوری اطلاعات، قرارگرفتن در معرض تهدید، اثربخشی کنترل‌ها، پیش‌بینی خطر نقض، پاسخ به حادثه و بهبود ارتباطات پیرامون امنیت سایبری درون سازمان تغذیه می‌کند. فناوری‌های هوش مصنوعی با توانایی آنها در تجزیه‌وتحلیل سریع میلیون‌ها رویداد و شناسایی انواع مختلف تهدیدها، می‌توانند به تیم‌های امنیتی کمک کنند تا خطر نقض را کاهش دهند و وضعیت امنیتی خود را به‌طور کارآمد و مؤثر بهبود بخشند.

هوش مصنوعی و علم داده برای شناسایی حملات سایبری و جلوگیری از گسترش آنها نقش اساسی دارد. کارکردهای حائز اهمیت هوش مصنوعی در این زمینه عبارتند از:

- **امنیت داده**
- **امنیت شبکه**
- **امنیت نقطه پایانی (Endpoint)**
- **امنیت ایمیل**
- **مدیریت هویت کاربران**
- **امنیت ابری**
- **امنیت زیرساخت‌ها**
- **امنیت برنامه**

حملات سایبری علیه سازمان‌ها می‌تواند به اشکال مختلفی انجام شود که ممکن است از یک اقدام واحد یا ترکیبی از مراحل مجزا درکنار هم تشکیل شود. چنین اعمالی ممکن است یک بهره‌برداری پیچیده از کدگذاری یا استفاده ساده از مهندسی اجتماعی برای افشای یا دسترسی به اطلاعات محرمانه باشد. هوش مصنوعی نه‌تنها شامل تهدیدها و عوامل خطر می‌شود، بلکه می‌تواند به‌عنوان یک حل‌کننده مشکلات نیز عمل کند. این هوش و پردازش اطلاعات شناختی هستند و برای شناسایی، دفاع دربرابر و بررسی حملات سایبری استفاده می‌شود. راه‌حل‌های مدرن امنیت اطلاعات یا ساخته دست انسان یا ماشینند؛ راه‌حل‌های به اصطلاح تحلیلی مبتنی بر قوانین ایجادشده توسط کارشناسان امنیت فناوری اطلاعاتند که حملاتی را که با قوانین تعیین‌شده مطابقت ندارند، نادیده می‌گیرند. رویکردهای مبتنی بر یادگیری ماشینی بر شناسایی ناهنجاری‌هایی تکیه می‌کنند که می‌توانند نتایج مثبت کاذب را شناسایی کنند، احساس بی‌اعتمادی نسبت به سیستم ایجاد می‌کنند، بنابراین نیاز به تلاش انسانی برای بررسی موارد دارند. برای مدیریت امنیت سایبری حجم زیادی از داده‌ها، راه‌حل‌های هوش مصنوعی مؤثری موردنیاز است. می‌توان از آنها برای بهبود آگاهی موقعیتی و اجرای اقدامات حفاظتی مؤثر استفاده کرد. این صنعت انواع راه‌حل‌های امنیت سایبری مبتنی بر هوش مصنوعی را توسعه داده است که در بخش بعدی ارائه می‌شود.

شناسایی زودهنگام تهدیدهای سایبری با استفاده از هوش مصنوعی

اگر هکری بتواند به سامانه یا زیرساختی نفوذ کند، تمامی گره‌های شبکه به یک هدف ساده تبدیل می‌شوند. پیچیده‌ترین و سخت‌ترین فرایندی که شرکت‌های فعال در زمینه امنیت سایبری با آن روبه‌رو هستند، شناسایی زودهنگام تهدیدهاست. شناسایی زودهنگام این فرصت را فراهم می‌کند تا درک کنیم چه درخواست‌هایی برای برقراری ارتباط با سامانه‌ها معتبر است و چه فعالیت‌های همچون ارسال و دریافت حجم گسترده‌ای از داده‌ها توسط کارمندان یک سازمان مشکوک به‌نظر می‌رسد. شناسایی چنین فرایندی برای متخصصان امنیت سایبری فرایند

دشـواری اسـت، به‌ویـژه در ارتبـاط با شـرکت‌های بزرگی کـه روزانـه تراکنش‌هـای زیـادی انجام می‌دهنـد و برخی کارمنـدان آنها نسـبت به پروتکل‌هـای امنیتی بی‌تفاوت هسـتند. در چنیـن مواقعـی یادگیری ماشـین می‌تواند به یاری متخصصان مجرب بشتابد. یک سامانه شناسایی هوش‌محور می‌تواند با نظارت بر ارتباطات خروجی و ورودی و تمامی درخواست‌های صادرشده توسط سامانه‌ها نظارت دقیقی بر فعالیت‌های مشکوک اعمال کند.

بدافزارهای مبتنی بر هوش مصنوعی

ظهـور بدافزارهای heuristics و adaptive را می‌توان تغییری بزرگ در صنعت بدافزار محسـوب کرد، به‌طوری‌که نیاز به هوش مصنوعـی را ایجـاد کرد. حجـم بدافزارها از تعدادی که به‌صورت دسـتی مدیریت می‌شـد، بلافاصله به رشـد تصاعـدی رسـید، بنابراین الزام برگزیـدن هوش مصنوعی و Machine learning به منظـور پشـتیبانی از تحلیلگـران بدافزار به وجود آمد.

از گذشـته بدافزارها تهدیدی مهم برای امنیت سازمان‌ها بوده‌انـد و اکنـون آنها به سـرعت درحـال تکاملند. یکی از مهم‌ترین پیشرفت‌های هوش مصنوعی در امنیت سایبری، شناسـایی دقیـق بدافزارهـا بـوده اسـت. سیسـتم‌های تشـخیص تهدید امنیـت سـایبری هوش مصنوعی برای پیـدا کردن برنامه‌های بدافـزاری مفیدند و برای جلوگیری از شناسایی می‌توانند کدهای خود را تغییر دهند. (مانند بدافزارهای چندشکلی و دگرگونی)

بدافزارهای چندشـکلی گروهی از برنامه‌های مخربند که دائما قسمتی از کدهای خود را تغییر می‌دهند و سپس از رمزگـذاری (برای پنهان کردن کد) برای فرار از نرم‌افزارهای ضدبدافـزار بهـره می‌برنـد. ایـن بدافزارهـای سـایبری از موتورهای جهش برای اصلاح کدشـان اسـتفاده می‌کنند تا شناسـایی خود توسـط سیسـتم‌های تشخیص تهدید سایبری را دشوار کنند. متأسفانه تعداد این نوع بدافزارهای مخرب افزایش یافته‌اند. براسـاس تحقیقات Webroot در میان نرم‌افزارهای مخربی که آنها تجزیه‌وتحلیل می‌کنند، ۹۴٪ از آنها ماهیت چندشکلی دارند.

بدافزارهـای دگرگونی گروهی از برنامه‌های مخرب مشـابه چندشـکلی هسـتند که کدهای خود را تغییر می‌دهند تا شناسایی نشوند، همچنین شناسایی بدافزارهای دگرگونی توسط سیستم‌های تشخیص تهدید سایبری سخت‌تر از بدافزارهای چندشـکلی اسـت. تفاوت اصلی بین بدافزار دگرگونی و چندشکلی این است که اولی کدهای منبع خود را به‌طور کامل تغییر می‌دهد، اما دومی برخی قسمت‌های کد خود را نگه می‌دارد و فقط برخی دیگر را اصلاح می‌کند. شناسایی بدافزارهای دگرگونی با استفاده از ابزارهای سنتی امنیت سـایبری بسـیار دشـوار اسـت. از این رو یادگیری و قابلیت‌هـای تطبیقـی سیسـتم‌های امنیـت سـایبری هوش مصنوعی درحال تکامل است.

شـواهد زیـادی مبنی‌بـر اسـتفاده مهاجمـان سـایبری از هوش مصنوعـی در ایجاد گونه‌های جدید بدافزارها وجود ندارد، هرچند از فاکتورهای «هوش مصنوعی» و Machine learning در سایر زمینه‌ها مانند نمونه‌های ذیل استفاده می‌شود تا اقدامات امنیتی نادیده گرفته شود.

- تولید تصاویر و ویدئوهای deep fake برای نادیده گرفتن اقدامـات امنیتـی. این امر به خصوص برای سـایت‌های رسـانه‌ای اجتماعـی به‌منظور ایجاد هویت جعلی بسـیار رایج است.
- کشـف CAPTCHAهـا به‌منظـور دور زدن اقدامـات حفاظتی احراز هویت
- جمـع‌آوری اطلاعـات از سـازمان‌ها به‌منظـور ایجـاد حملات
- مدل‌سـازی الگـوی رفتـاری کاربـر بـرای جلوگیـری از تهدیدهای درون‌زا (Insider Threats)

برخی حملات سـایبری از طریق سـرقت اطلاعات احراز هویت کارمندان انجام می‌شـوند. در چنین شـرایطی تنها کاری کـه هکـر بایـد انجام دهـد ورود به شـبکه بر مبنای اطلاعات لاگین کاربر و در ادامه افزایش سطح دسترسی‌ها از کاربر عادی به کاربر یا مدیر ارشد است. تشخیص چنین حمله‌ای برای ضدویروس‌های عادی فرایند دشواری است، زیـرا ورود با اطلاعات کاربر عادی انجام می‌شـود و حمله سایبری ممکن است بدون اطلاع انجام شود. الگوریتم‌های

یادگیری ماشین بر مبنای مدل‌سازی الگوی رفتاری کاربر می‌توانند به متخصصان امنیتی کمک کنند. الگوریتم‌های یادگیری ماشین را می‌توان به‌گونه‌ای آموزش داد تا رفتار هر کاربر همچون زمان ورود و خروجش را شناسایی کنند. در چنین شرایطی هر زمان رفتار خارج از عرفی انجام شود، الگوریتم یادگیری ماشین می‌تواند آن را شناسایی و به تیم امنیت سایبری هشدار دهد که اتفاقی غیرمعمول در حال انجام است.

مدیریت آسیب‌پذیری‌ها

با استفاده هرچه بیشتر مهاجمان سایبری از روش‌ها و تکنیک‌های پیچیده‌تر، آسیب‌پذیری‌های جدیدتری نیز گزارش می‌شود، درنتیجه سازمان‌ها درتلاش برای مدیریت حجم فراوانی از آسیب‌پذیری‌های جدیدند و سیستم‌های قدیمی آنها نمی‌توانند در لحظه مانع از این حملات پرریسک شوند.

نظارت بر ایمیل

برای پیشگیری از حملات سایبری مخرب مانند فیشینگ، نظارت بر حساب‌های ایمیل رسمی کارمندان یک شرکت مهم است. حملات فیشینگ می‌توانند با ارسال ایمیل‌های جعلی برای کارمندان و درخواست اطلاعات خصوصی ازجمله اطلاعات حساس شغلی، اطلاعات بانکی و کارت اعتباری آنها، گذرواژه‌های شرکت و نمونه‌های مشابه انجام شود. برای پیشگیری از بروز چنین اتفاقات ناگواری می‌توان از نرم‌افزار امنیت سایبری همراه با یادگیری ماشین استفاده کرد. با نظارت بر ایمیل‌های کارمندان امکان شناسایی تله‌های فیشینگ فراهم می‌شود. علاوه‌بر این می‌توان از پردازش زبان طبیعی برای پویش ایمیل‌ها استفاده کرد و برخی الگوها و عبارات در متن ایمیل‌ها که ممکن است نشان‌دهنده تلاش فیشینگ در ایمیل باشند را شناسایی کرد.

کاربردهای هوش مصنوعی در امنیت فیزیکی

امنیت فیزیکی به مجموعه اقدامات امنیتی اطلاق می‌شود که در راستای محافظت از دارایی‌های فیزیکی و افراد در مقابل آسیب‌هایی چون سرقت، جاسوسی یا حملات تروریستی فعالیت می‌کند. در امنیت فیزیکی از تکنیک‌های مختلفی چون نظارت تصویری، حراست فیزیکی، پروتکل‌ها و انواع قفل‌های دسترسی استفاده می‌شود. ظهور هوش مصنوعی با تأکید بر قابلیت‌های بینایی ماشین، تشخیص گفتار و پردازش زبان طبیعی توانسته دقت فعالیت‌های انجام‌شده در این حوزه را به میزان قابل توجهی بالا ببرد، همچنین مواردی از قبیل افزایش سرعت واکنش دربرابر تهدیدها و آسیب‌های امنیتی و کاهش نیاز به نیروی انسانی از دیگر مزایای استفاده از هوش مصنوعی در این زمینه است.

نظارت هوشمند

دوربین‌های نظارتی هوشمند به کمک فناوری بینایی ماشین، ضمن شناسایی افراد، رفتار و حرکت‌های آنها را پردازش کرده و با استخراج الگوهای رفتاری، رفتارهای مشکوک را تشخیص و به نگهبان، نیروی انتظامی یا مالکان هشدار می‌دهد. از این کارکرد در موارد مختلفی ازجمله خانه‌های هوشمند، مراکز تجاری، بانک‌ها، سازمان‌های مختلف و... استفاده می‌شود.

کنترل افراد در حین ورود

کنترل افراد در حین ورود غالبا از طریق بررسی کارت شناسایی توسط نگهبان انجام می‌گیرد که در خیلی از اوقات به ازدحام و آشفتگی منجر می‌شود، همچنین مواردی از قبیل تراکم جمعیت، عوامل محیطی (مانند دما، آلودگی صوتی و...) یا خستگی‌های فردی عملکرد این کنترل‌های دستی را به شدت کاهش می‌داد. هوش مصنوعی به وسیله کنترل مشخصات بیومتریک به‌ویژه تشخیص چهره، انجام این فعالیت را بسیار آسان نکرده و دقت کنترل را نیز به طور قابل توجهی افزایش داده است. سیستم بینایی ماشین با پردازش تعداد زیادی چهره در دقیقه، افراد را شناسایی و با توجه به هویت آنها اجازه ورود را صادر می‌کند.

در این راستا قفل‌های هوشمندی نیز ارائه شده که پس از

شناسایی افراد از طریق چهره، صدا، اثرانگشت یا کارت RFID به طور اتومات باز می‌شود. این قفل‌های هوشمند با استفاده از قابلیت حوزه اینترنت اشیا، با مالکان یا افراد مسئول در ارتباطند و امکان باز و بسته شدن در از راه دور را نیز فراهم می‌کند، همچنین می‌توان از دستیارهای صوتی مانند Alexa آمازون برای این منظور استفاده کرد.

امنیت داده

سازمان‌ها برای به حداقل رساندن صدمات ناشی از حملات سایبری و جلوگیری از وقوع حوادث احتمالی و همچنین حفاظت از داده‌ها از فناوری‌های نوینی مانند هوش مصنوعی استفاده می‌کنند. ابزارهای هوش مصنوعی می‌توانند داده‌ها را مورد بررسی قرار دهند و داده‌های ناهنجار را تشخیص دهند که از دید انسان پنهان مانده است.

شناسایی و جلوگیری از نشت داده

نشت داده ممکن است از داخل یا خارج از سازمان اتفاق افتد که در بسیاری از مواقع آسیب جدی به اطلاعات و دانش سازمان‌ها وارد می‌کند. این امر می‌تواند به دلیل اتصال کاربران غیرمجاز به سیستم، سطح دسترسی‌های نادرست به اطلاعات یا معماری اشتباه شبکه باشد. سیستم‌های مجهز به هوش مصنوعی با شناسایی، نظارت و مراقبت از اطلاعات موجود در حافظه و همچنین مراقبت از داده‌هایی که در شبکه‌ها در حال جابه‌جایی هستند، امنیت داده‌ها را افزایش می‌دهد و در صورت وجود رفتار غیرعادی، به طور خودکار، هشدار می‌دهد و از ادامه آن رفتار جلوگیری می‌کند.

امنیت شبکه

با گسترده شدن شبکه‌های کامپیوتری، ایجاد امنیت در شبکه از اهمیت بسزایی برخوردار است. متأسفانه افراد سودجو با دسترسی به اطلاعات مهم مراکز خاص یا اطلاعات افراد دیگر به قصد اعمال نفوذ، فشار یا ایجاد بی‌نظمی در سیستم‌ها، حمله به شبکه و سیستم‌ها را در پیش می‌گیرند. دو مدل یادگیری با ناظر و یادگیری

بدون‌ناظر در حوزه هوش مصنوعی توانستند تأثیر بسزایی در تأمین امنیت شبکه بگذارند. مدل‌های یادگیری ماشین با ناظر براساس داده‌های برچسب‌دار، آموزش می‌بینند که مسائل طبقه‌بندی نیز در این گروه قرار می‌گیرند. در این مسائل، داده‌های ورودی براساس الگوی نهفته در آنها در یک دسته مشخص جای می‌گیرند، اما در یادگیری بدون‌ناظر به توسعه سیستم‌هایی پرداخته می‌شود که تنها با یافتن شباهت بین داده‌های بدون برچسب، آنها را گروه‌بندی می‌کند. با توجه به اینکه داده‌ها برای این مدل‌ها همگی یکسان به نظر می‌رسند (بدون برچسب)، هدف این نوع از الگوریتم‌ها درک رابطه بین داده‌ها و درنهایت گروه‌بندی آنهاست. خوشه‌بندی یکی از نمونه‌های رایج این نوع از مدل‌هاست. در ادامه کاربردهای هوش مصنوعی در امنیت شبکه شرح داده می‌شود.

تشخیص تهاجم

سیستم تشخیص تهاجم (نفوذ) یک ابزار مؤثر جهت شناسایی و تشخیص هرگونه استفاده غیرمجاز، سوءاستفاده یا آسیب‌رسانی در شبکه را برعهده دارد. برای ایجاد امنیت کامل در یک سیستم کامپیوتری، علاوه بر دیوارهای آتش و دیگر تجهیزات جلوگیری از نفوذ، سیستم‌های دیگری نیز نیاز است تا بتوان در صورت عبور نفوذگر از دیواره آتش، آنتی‌ویروس و سایر تجهیزات امنیتی، آنها را تشخیص داده و چاره‌ای برای مقابله با آن تعبیه کرد. به‌دلیل ماهیت غیرالگوریتمی روش‌های نفوذ در شبکه‌های کامپیوتری، راهکارهای مطرح‌شده برای مقابله با ناهنجاری‌ها نیز باید دارای ماهیت غیرالگوریتمی باشد. هوش مصنوعی به‌ویژه شبکه عصبی که جزء سیستم‌های یادگیرنده محسوب می‌شود، توانسته در زمینه شناسایی و جلوگیری از این ناهنجاری‌ها تأثیر بسزایی بگذارد. به‌طور سنتی فعالیت شناسایی نفوذ از طریق معرفی سیستم‌هایی معروف به سیستم‌های تشخیص نفوذ (IDS) مدیریت می‌شود. این سیستم‌ها به دو دسته سیستم تشخیص نفوذ تحت شبکه و سیستم‌های تشخیص نفوذ میزبان تقسیم

می‌شوند که براساس عواملی از قبیل نوع و تعداد فرایندهای درحال اجرا، رفتار کاربران، ماژول‌های سیستم عامل هنگام راه‌اندازی سیستم یا الگوی مصرف ترافیک به نظارت یا کنترل شبکه‌های داخلی یا خارجی می‌پردازند. با معرفی تکنیک‌های هوش مصنوعی در زمینه امنیت سایبری، نوع سومی تحت عنوان «سیستم تشخیص نفوذ مبتنی بر ناهنجاری» مطرح شد. این دسته با استفاده از الگوریتم‌های یادگیری با ناظر یا بدون ناظر، یادگیری تقویتی و حتی الگوریتم‌های خوشه‌بندی حوزه داده‌کاوی، رویدادهایی را به‌عنوان ناهنجاری شناسایی می‌کند که خارج از رفتار عادی سیستم اتفاق می‌افتد.

شناسایی بات‌نت‌ها برای جلوگیری از حملات DDOS

یکی از رایج‌ترین مشکلات در تشخیص ناهنجاری شبکه، مربوط به بات‌نت‌هاست. با توجه به خطر چنین شبکه‌های مخفی، شناسایی بات‌نت‌ها جهت جلوگیری از فرسودگی شبکه و مصرف بیهوده منابع محاسباتی و برای جلوگیری از انتشار اطلاعات حساس (نشت داده‌ها) به خارج از شرکت ازجمله فعالیت‌های ضروری جهت برقراری امنیت داده‌ها و اطلاعات در سطح شبکه است. بات‌نت‌ها از مجموعه‌ای از کامپیوترها یا سیستم‌های آلوده تشکیل شده‌اند که توسط یک بدافزار هدایت می‌شوند. افرادی که بدافزارها را ایجاد کرده‌اند، می‌توانند به جای اینکه به یک کامپیوتر آلوده به‌صورت مستقیم متصل شوند، از بات‌نت‌ها برای مدیریت خودکار حجم زیادی از این کامپیوترهای آلوده استفاده کنند که از طریق یک کانال فرمان و کنترل (C&C) به یکدیگر وصل شده‌اند. یکی از مشکلات کشف بات‌نت‌ها شباهت زیاد ترافیک بات‌نت با ترافیک واقعی شبکه است، بنابراین به‌راحتی و با استفاده از روش‌های سنتی نمی‌توان آنها را شناسایی کرد. الگوریتم‌های یادگیری ماشین در دو نوع با ناظر و بدون ناظر یکی از ابزارهای هوش مصنوعی در شناسایی بات‌نت‌ها هستند. شناسایی بات‌نت‌ها نمونه‌ای از مسائل طبقه‌بندی است که با هدف تعیین کلاس، یک بسته یا توالی بسته‌ها به ترافیک بات‌نت‌ها یا ترافیک معمولی مورد بررسی قرار می‌گیرند. از طرف دیگر جهت گروه‌بندی ترافیک با توجه به ویژگی‌های مشابه و شناسایی ترافیک‌های مشکوک می‌توان از مدل‌های یادگیری ماشین بدون ناظر استفاده کرد.

امنیت نقطه پایانی (Endpoint)

یکی از کاربردهای هوش مصنوعی در امنیت سایبری، تأمین امنیت نقطه امنیت پایانی است. امنیت نقطه پایانی، یک رویکرد امنیتی است که روی حفاظت از امنیت رایانه‌های شخصی، تلفن، تبلت‌ها یا دیگر دستگاه‌های فعال در شبکه تمرکز می‌کند. بدافزارها از تهدیدهای سایبری در زمینه امنیت نقطه پایانی‌اند. بدافزار برنامه‌ای است که برای آلوده کردن و آسیب رساندن به سیستم میزبان استفاده می‌شود. ویروس یکی از شناخته‌شده‌ترین بدافزارها محسوب می‌شود. انواع دیگری از بدافزارها وجود دارند که می‌توان به تروجان، کرم، جاسوس‌افزار، آگهی‌افزار و باج‌افزار اشاره کرد. امروزه بدافزارها با سرعت سرسام‌آوری درحال آلوده کردن کامپیوترها و دستگاه‌های قابل حملند. با افزایش تقریبا نمایی تعداد تهدیدهای مرتبط با انتشار روزانه بدافزارهای جدید، عملا مقابله با بدافزارها و تجزیه‌وتحلیل مداوم آنها توسط اپراتورهای انسانی، امری غیرممکن است. بنابراین لازم است الگوریتم‌هایی معرفی شوند که حداقل شناسایی آن را به‌طور اتومات انجام دهند. در گذشته شناسایی انواع بدافزارها از طریق روش‌های تجزیه‌وتحلیل استاتیک و به‌صورت دستی توسط تحلیلگران بدافزارها انجام شده است. با معرفی الگوریتم‌های هوش مصنوعی، روند تجزیه‌وتحلیل بدافزارها بهبود یافته و کارآمدتر شده است، زیرا تحلیلگران انسان‌ها را از انجام فعالیت‌های سخت و تکراری آزاد می‌کنند و به آنها اجازه می‌دهند تا در جنبه‌های غیرمعمول تجزیه‌وتحلیل تمرکز کنند. نکته حائز اهمیتی که در زمینه شناسایی بدافزارها وجود دارد، شناسایی و دسته‌بندی آنها براساس شباهت‌های موجود در رفتارشان است. در این زمینه می‌توان از الگوریتم‌های خوشه‌بندی فناوری داده‌کاوی، درخت تصمیم، زنجیره‌های پنهان مارکوف یا یادگیری عمیق هوش مصنوعی بهره برد.

شناسایی هرزنامه (Spam)

هرزنامه یا اسپم به پیام الکترونیکی اطلاق می‌شود که بدون درخواست گیرنده و برای افراد بی‌شمار فرستاده می‌شود. هرزنامه به‌نوعی سوءاستفاده از سامانه انتقال پیام است. جهت شناسایی هرزنامه، استراتژی‌های هوش مصنوعی متفاوتی وجود دارد که یکی از رایج‌ترین و ساده‌ترین آنها شبکه‌های عصبی است. از قابلیت‌های دیگری همچون «ماشین‌های بردار پشتیبان» (به‌ویژه برای اسپم‌های تصویری)، شبکه‌های بیز، همچنین استفاده از فناوری‌های پردازش زبان طبیعی می‌توان در این زمینه استفاده کرد.

شناسایی حملات فیشینگ

حملات فیشینگ، از چالش‌های اصلی ارائه خدمات آنلاین به‌ویژه در زمینه تجارت الکترونیک است. فیشینگ، تکنیک مهندسی اجتماعی محسوب می‌شود که با فریب کاربران اینترنتی به منظور سرقت اطلاعات حساس و محرمانه آنها مانند اطلاعات حساب کاربری، رمز عبور یا شماره کارت اعتباری انجام می‌شود. یکی از این روش‌ها ایجاد صفحات تقلبی و ارجاع دادن کاربرها به آن صفحات است. کاربران نیز به‌دلیل طراحی مشابه این صفحات با صفحات اصلی به آنها اعتماد و اطلاعات شخصی خود را در صفحات تقلبی وارد می‌کنند. حملات فیشینگ به‌طورمعمول دارای مجموعه‌ای از الگوهای پنهان است که کشف این الگوها توسط تکنیک‌های داده‌کاوی و یادگیری ماشین می‌تواند به شناسایی این‌گونه از حملات کمک کند.

مدیریت هویت کاربران (مقابله با حساب‌های جعلی)

مقابله با حساب کاربری جعلی از جمله فعالیت‌های مستلزم نظارت است، زیرا گسترش حساب‌های جعلی باعث فراهم کردن بستری ناامن برای انجام فعالیت‌های نامناسب از جمله فریب کاربران قانونی و سوءاستفاده از حساب کاربری آنها می‌شود. نظارت بر حساب کاربری شبکه‌های اجتماعی مانند فیس‌بوک و توییتر- که روزانه تعداد زیادی حساب کاربری ایجاد می‌شود- کاری دشوار و زمانبر است که با گسترش کاربردهای هوش مصنوعی در امنیت، این فعالیت با دقت بالا و زمان کم قابل انجام است. به‌عنوان نمونه، فیس‌بوک با به‌کارگیری سیستم جدیدی مبتنی بر یادگیری ماشین موسوم به Deep Entity Classification به شناسایی حساب‌های جعلی می‌پردازد و از فعالیت آنها جلوگیری می‌کند. این الگوریتم ۲۰ هزار ویژگی متعلق به هر حساب و افراد وابسته به آن حساب را در نظر می‌گیرد و اصل بودن آن را بررسی می‌کند. انجام این عمل به‌صورت دستی توسط انسان، کاری تقریبا غیرممکن است.

مدیریت هویت کاربران (حفاظت از حساب‌ها و اطلاعات کاربران)

حفاظت از حساب‌های کاربری برای هر سازمانی به‌خصوص در شرایطی که دارای مسئولیت‌های قانونی در قبال اشخاص ثالث است، یک مأموریت حساس به‌شمار می‌رود. این امر با گسترش حساب‌های جعلی جهت سرقت اطلاعات محرمانه و حساس یا ایجاد تشنج و بیان مطالب محرک و توهین‌آمیز در فضای سایبری بحرانی‌تر شده است. یکی از نقاط ضعف در محافظت از حساب کاربران، محافظت ضعیف از رمز عبور آنهاست. هرچند امروزه در راستای افزایش امنیت حساب‌های کاربران، راهکارهایی ازجمله ارسال پیام یا ایمیل به کاربر درحین اتصال سیستم دیگری به حساب مربوطه مطرح شده است. بااین حال این فعالیت‌ها واکنشی هستند که با شناسایی دسترسی‌های غیرمجاز، سیستم در قالب هشدار، واکنشی را نشان می‌دهد و باعث بسته یا معلق شدن حساب کاربر می‌شود. این سیستم‌های هشدار واکنشی معمولا با مجموعه‌ای از محرک‌های پیش‌فرض و مرتبط با رویدادها فعال می‌شوند که برای تمامی کاربران یکسانند. به‌عبارت دیگر این سیستم‌ها در شناسایی رفتار کاربران تلاشی نکرده تا بتوانند براساس الگوی رفتاری هر فرد عمل کنند. علاوه بر این، سیستم‌های واکنشی، آینده را مشابه با گذشته در نظر می‌گیرند و توانایی سازگاری سریع با تغییرات را ندارند. در این راستا، اتخاذ یک رویکرد پیشگیرانه برای حفاظت حساب و اطلاعات کاربران

می‌تواند مثمرثمر واقع شود. در اینجاست که هوش مصنوعی با استفاده از روش‌های مختلف داده‌کاوی و یادگیری ماشین جهت بهره‌برداری از داده‌های ساختاریافته یا غیرساختاری استخراج شده از منابع ناهمگون سازمان به کار می‌آید. هوش مصنوعی با شروع تجزیه‌وتحلیل داده‌های گذشته قادر به نشان دادن الگوهای نهفته، برآورد رفتارهای آینده کاربران و شناسایی به موقع تلاش‌های احتمالی برای کلاهبرداری است.

نظارت بر فعالیت کاربران

نظارت بر فعالیت کاربران جهت جلوگیری از فعالیت‌های نامناسب در فضای دیجیتال به خصوص در شبکه‌های اجتماعی یکی از رایج‌ترین کاربردهای هوش مصنوعی در امنیت سایبری است. در این زمینه می‌توان براساس رفتار و عملکرد هر کاربر، اعتباری به وی اختصاص داد که در صورت پایین بودن این اعتبار از یک حد تعریف شده، از ادامه فعالیت آن جلوگیری شود. این امر می‌تواند از طریق اعمال یک سیستم هشدار در زمان مشاهده رفتار غیرنرمال یا فعالیت‌های بیش‌ازحد زیاد یا نامنظم نیز کنترل شود. برای این منظور، غالبا از الگوریتم‌های یادگیری با ناظر یا خوشه‌بندی جهت طبقه‌بندی رفتار کاربر استفاده می‌شود. علاوه بر این با استفاده از داده‌کاوی و با توجه به الگوی رفتاری کاربر میزان اعتبار و رفتار آینده او قابل پیش‌بینی خواهد بود.

احراز هویت

احراز هویت فرایندی است که طی آن درستی هویت یک فرد، شناسایی و تأیید می‌شود، بنابراین زمانی که کاربر بخواهد وارد سیستم شده یا به منبعی دسترسی پیدا کند، ابتدا باید خود را اثبات کند. احراز هویت به صورت روش‌های متفاوتی از قبیل سؤال‌های امنیتی، رمزهای عبور، توکن‌ها، دستگاه‌های فیزیکی و ویژگی‌های بیومتریک انجام می‌گیرد. درحال حاضر احراز هویت از طریق ویژگی‌های بیومتریک بسیار مطرح شده است. منظور از ویژگی‌های بیومتریک در احراز هویت، ویژگی‌های فیزیکی منحصربه‌فرد مانند عنبیه چشم، چهره، اثرانگشت و صداست که از طریق آن می‌توان افراد را شناسایی و ردیابی کرد. هوش مصنوعی با استفاده از فناوری بینایی ماشین و تشخیص گفتار، تحول شگرفی در این زمینه ایجاد کرده که می‌تواند با تلفیق با علم داده‌کاوی، الگوهای رفتاری مانند نحوه تایپ مطالب و دست‌خط یا الگوی امضا کردن را نیز شناسایی کند و از آن برای صحه‌گذاری هویت افراد بهره ببرد. علاوه‌بر این از قابلیت‌های دیگر سیستم‌های هوشمند می‌توان به موارد زیر اشاره کرد:

- عکس سلفی را با مدارک شناسایی اسکن‌شده مطابقت می‌دهد و میزان شباهت آن را می‌سنجد.
- حرکات لب و دهان فرد را تحلیل و ژست حرکتی خواسته‌شده از کاربر را راستی‌آزمایی می‌کند.
- با بررسی خوانش جملاتی توسط کاربر به زنده بودن، سن، جنسیت و احساسات فرد پی می‌برد.

تشخیص فریب احراز هویت

با پیشرفت تکنولوژی، علاوه‌بر ایجاد راهکارهایی جهت تأمین امنیت بیشتر در فضای دیجیتال، می‌توان ادعا کرد به همان میزان حملات و تقلب‌های سایبری نیز پیچیده‌تر و پیشرفته‌تر شده است. جعل در تصاویر در حوزه Anti-Spoofing شامل موارد متفاوتی ازجمله جعل در صحبت کردن و عدم رعایت الگوی موردنظر در صحبت است. با ظهور فناوری دیپ‌فیک و مدل‌هایی مانند مدل‌های مولد تخاصمی می‌توان تصاویری از افراد ایجاد کرد که هرگز حضور فیزیکی نداشته‌اند و سیستم‌های مربوط به احراز هویت را فریب داد. در این راستا فرایندی تحت‌عنوان صحت‌سنجی یا تشخیص زنده‌بودن مطرح شده که عبارت است از مجموعه‌ای از عملیات که تصاویر ویدئویی را مورد پردازش قرار داده و تشخیص می‌دهد که ویدئوی دریافت‌شده از فرد جعلی نبوده و مورد دستکاری عامدانه قرار نگرفته است. این مورد یکی از جالب‌ترین کاربردهای هوش مصنوعی در امنیت سایبری است که به‌نوعی این فناوری را در مقابل خود قرار می‌دهد.

امنیت ابری

سرورهای ابری نوعی سرور مجازی است که کاربران به‌جای خرید یا اجاره سرورهای فیزیکی، بخشی از فضای این سرورهای مجازی را اجاره می‌کنند. امنیت ابری شامل تمام راه‌حل‌های تکنولوژیکی، سیاست‌های سازمانی و کنترل‌های استفاده شده که برای اطمینان از امنیت پلتفرم‌های ابری به‌کار می‌روند. هدف از امنیت ابری، اطمینان از ایمنی داده‌ها و همچنین معماری سرورهای ابری است. با توجه به رشد چشمگیر داده‌ها در سرویس‌های ابری، ظهور پلتفرم‌های ابری مجهز به هوش‌مصنوعی، فعالیت‌های حفظ و پردازش داده‌ها را تسهیل می‌کند. به بیانی دیگر با توجه به قابلیت‌های هوش‌مصنوعی به‌ویژه الگوریتم‌های یادگیری ماشین در جمع‌آوری و تجزیه‌وتحلیل حجم زیادی از داده‌ها، شناسایی الگوها و یادگیری در این زمینه تجهیز سرورهای ابری به هوش‌مصنوعی بسیار مثمرثمر واقع شده است. همچنین هوش‌مصنوعی درکنار حوزه داده‌کاوی به پیش‌بینی تهدیدهای محتمل ازجمله شناسایی و خنثی‌سازی حملات سایبری، جلوگیری از نشت داده‌ها، کشف نقاط آسیب‌پذیر، نظارت در لحظه و ارائه هشدار در صورت نیاز می‌پردازد و می‌تواند در تأمین امنیت سرورهای ابری به‌طور قابل‌ملاحظه‌ای اثربخش عمل کند.

امنیت زیرساخت‌ها

امروزه حملات سایبری به زیرساخت‌های حساس افزایش پیدا کرده و روزبه‌روز جلوگیری از آنها سخت‌تر شده است. به‌طوری‌که نیاز به هوش‌مصنوعی کاملا حس می‌شود. هوش‌مصنوعی می‌تواند از زیرساخت‌های حساس در مقابل حملات سایبری محافظت کند و مانع آسیب رسیدن به اطلاعات سازمان‌ها یا حتی عموم مردم شود. به‌عبارت‌دیگر، هوش‌مصنوعی با ارائه راهکارهای امنیتی برای هر قسمت از زیرساخت‌های فناوری اطلاعات می‌تواند امنیت آنها را تا مقدار زیادی تأمین کند.

امنیت Application

تأمین امنیت برنامه یکی دیگر از کاربردهای هوش‌مصنوعی در امنیت سایبری، شامل ملاحظات امنیتی برای مواردی از قبیل برنامه‌های وب، برنامه‌های کاربردی کلاینت و موبایل است که درطول توسعه، طراحی برنامه و پس از استقرار آن اتفاق می‌افتد. به‌طورکلی برنامه‌ها در همه مکان‌ها قابلیت اجرا شدن دارند و دائما درحال تغییرند. به همین دلیل تأمین امنیت آنها دشوار است. هدف از امنیت برنامه، جلوگیری از سرقت یا ربودن داده‌ها یا کدهای موجود در برنامه است. نقض امنیت سایبری در لایه برنامه می‌تواند به دلایل مختلف از قبیل کدنویسی ضعیف، انجام کم تست و رشد سریع و چشمگیر فناوری جدید مانند سرورهای ابری باشد که این لایه را در مقابل حمله مهاجمان آسیب‌پذیر کرده است. بااین‌حال حوزه‌های مختلف هوش‌مصنوعی ازجمله سیستم‌های خبره و یادگیری ماشین توانسته‌اند در بهبود تجزیه‌وتحلیل و پیش‌بینی حملات امنیتی، شناسایی نقاط آسیب‌پذیر برنامه و ارائه گزینه‌های اصلاحی جهت رفع عیوب کدگذاری تأثیرات قابل‌توجهی بگذارند. به‌عنوان نمونه مایکروسافت با تکیه‌بر هوش‌مصنوعی ابزاری ارائه کرده که به توسعه‌دهندگان کمک می‌کند ایرادهای کدهای‌شان را با دقت ۹۹ درصد شناسایی کنند. این کار باعث می‌شود بخش بزرگی از امنیت برنامه در همان ابتدا و در مرحله طراحی و توسعه تأمین شود.

روندهای آینده در حوزه پدافند سایبری

بررسی‌ها نشان می‌دهد فناوری‌های نوظهور و اینترنت آینده منشأ تحولات عظیمی خواهد بود و تأثیرات زیادی بر جوامع، کسب‌وکارها و سازمان‌ها خواهد داشت. میزان این تأثیرات به‌گونه‌ای است که می‌توان از آن به انقلاب بعدی در حوزه سایبر یاد کرد. اینترنت اشیا، هوش‌مصنوعی زنجیره بلوکی و تلفیق آنها با یکدیگر آگاهی بیشتر بشر از دنیای اطراف و تأثیر رفتارش بر دنیا را دربی دارد. شبکه اشیاامکان

ارتباط بین دستگاه‌های مختلف را فراهم می‌سازد. جامعه به‌طور روزافزونی به فضای سایبر و اینترنت آینده متکی خواهد شد، همان‌گونه که اینک به الکتریسیته متکی است، زیرا اینترنت آینده زندگی روزمره را پی‌ریزی و اصلاح می‌کند. کسب‌وکارها، تجارت، خدمات دولتی، امور اجتماعی، سرگرمی و پزشکی، همگی وابسته به فضای سایبری‌اند و این وابستگی هر روز وسیع‌تر و عمیق‌تر می‌شود.

فضای سایبر پیامدها و تأثیرات گوناگونی بر جوامع و شیوه حکومت‌ها، سازمان‌ها، کسب‌وکارها، فرهنگ‌ها، افراد و سبک زندگی آنها و بخش‌های دفاعی امنیتی خواهد داشت و مدل‌های نوین کسب‌وکاری شکل خواهد گرفت. این فضا سرشار از فرصت‌ها و تهدیدهای نوینی در ابعاد مختلف سیاسی-امنیتی، فرهنگی و اجتماعی، اقتصادی و فناورانه خواهد بود. با توسعه اینترنت و فناوری‌های نوین فضای سایبر تهدیدها و مخاطرات گوناگون فضای سایبر نیز افزایش پیدا می‌کند و لزوم مواجهه و پدافند فعال و هوشمندانه ضروری و اجتناب‌ناپذیر خواهد بود.

با رشد و گسترش استفاده از ارتباطات و فناوری اطلاعات در زیرساخت‌های حیاتی و همچنین همه‌گیر شدن بهره‌برداری از زیرساخت‌های نرم‌افزاری و نرم‌افزارهای کاربردی در ایجاد، مدیریت، تعمیر و نگهداری زیرساخت‌های حیاتی و به‌تبع آن لزوم شبکه‌ای شدن این زیرساخت‌ها برای کارایی بیشتر و کاهش هزینه‌ها تهدیدها، آسیب‌پذیری‌ها و مخاطرات این زیرساخت‌ها به‌طور فزاینده‌ای افزایش یافته است. از دیگر عوامل مهم این افزایش سطح تهدیدها و مخاطرات را می‌توان در موارد زیر یافت:

- **استفاده روزافزون از سامانه‌های کنترل متمرکز و جمع‌آوری داده‌ها**
- **استفاده از سامانه‌های مرتبط با فناوری محاسبات ابری**
- **استفاده از نرم‌افزارهای کاربردی با قابلیت کار با داده‌های حجیم**
- **هوشمند سازی زیرساخت‌های حیاتی**

همواره تهدیدهای بی‌شماری ضد زیرساخت‌های حیاتی از سوی کارمندان ناراضی در داخل شرکت (کشور)، سارقان اطلاعات، تبهکاران سازمان‌یافته، جاسوسان صنعتی و به‌طور فزاینده‌ای توسط دولت‌ها یا گروه‌های تحت حمایت آنها درحال وقوع است و مدام بر شدت آنها هم افزوده می‌شود. البته باید توجه داشت با رشد فناوری اطلاعات و بهره‌گیری گسترده از آن در زیرساخت‌های حیاتی، بیشتر تهدیدهایی که متوجه زیرساخت‌ها هستند، تهدیدها و حملات سایبری‌اند، زیرا ردیابی‌شان و دفاع دربرابر آنها مشکل‌تر از تهدیدهای فیزیکی است. تهدید سایبری یکی از جدی‌ترین چالش‌های فرا روی زیرساخت‌های حیاتی ملی کشورهاست که می‌تواند امنیت ملی و اقتصادی دولت‌ها و جوامع را به‌شدت تحت‌تأثیر قرار دهد. آسیب‌پذیری‌های جدید که در سطوح متعدد و متنوعی می‌توان از آنها بهره‌برداری کرد، در اثر تلاقی و تداخل فزاینده زیرساخت‌های حساس سنتی یک کشور (برای مثال یک زیرساخت حیاتی مانند سیستم‌های توزیع انرژی یا خدمات فوریتی) با زیرساخت‌های اطلاعاتی نوظهور امروزی (که در معرض حمله‌های الکترونیک است) پدید می‌آیند.

به‌طورکلی تهدیدها علیه زیرساخت‌های حیاتی با تهدیدهای دیگر زیرساخت‌ها تفاوت‌های بنیادی دارد. تهدیدهای زیرساخت‌های دیگر ساده، فرصت‌طلب و عمومی هستند. به‌عبارت‌دیگر این‌گونه از تهدیدها برای تمام افراد، زیرساخت‌ها و مراکز به یک ترتیب است و مکانیسم شناسایی و حفاظت از آنها نسبتاً آسان است. در طرف دیگر تهدیدها علیه زیرساخت‌های حیاتی، بسیار پیچیده، هدف محور، ماندگار و منعطف است. به‌عبارت‌دیگر دشمنان برای ضربه به زیرساخت حیاتی، از مدت‌ها پیش اقدامات اطلاعاتی و فنی انجام می‌دهند تا بدافزار یا دقیق‌تر سلاح سایبری را تولید کنند که مکانیسم تشخیص آن بسیار پیچیده باشد و فقط روی اهدافی خاص آن هم به‌صورت ماندگار و منعطف عمل کند و در دیگر شبکه‌ها اقدامی نداشته باشد. استاکس‌نت نمونه‌ای از این نوع سلاح‌های سایبری است که بسیار پیچیده و خاص منظوره تولید شده بود.

دسته‌بندی انواع تهدیدها و حملات سایبری جدید

Zero-day

تهدیدهای سایبری است که هنوز هیچ‌کس به‌غیراز افراد نفوذگر از وجود آن خبر ندارد و این آسیب‌پذیری برای تجهیزات امنیتی شبکه‌ای قابل شناسایی نیست.

Botnet

Botnet ها تهدیدهایی هستند که به‌صورت زیر عمل می‌کنند.

- شبکه‌ای از کامپیوترهای هک‌شده هستند.
- کنترل بات‌ها از طریق IRC صورت می‌پذیرد.
- به‌صورت رویات عمل می‌کنند.
- کنترل مرکزی توسط C&C انجام می‌شود.

APT (Advanced Persistent Technique)

Advanced: بهره‌گیری از فناوری بسیار پیشرفته و استفاده از آسیب‌پذیری‌های شناخته و ناشناخته

Persistent: مداوم و مرتب درحال تغییرند (Polymorphic)، پویا و گریز از دفاع نوع (Signature (AV, IDS, ...

Threats: دنبال هدف خاصی هستند و فرصت‌طلب نیستند.

AET (Advanced Evasion Threat)

امروزه استفاده از تکنیک‌های Evasion برای اهداف خاص، به‌شدت افزایش یافته است. این تکنیک‌ها منطبق بر اصول زیر است:

- کدهای AET به‌خودی خود ممکن است تهدید جدی تلقی نشوند، ولی برای یک حمله همه‌جانبه طرح‌ریزی شده باشند.
- مبتنی بر ترکیب تکنیک‌ها و روش‌های متعدد حمله جهت خلق یک روش جدید و منحصربه‌فرد حمله سایبری جهت گریز از لایه‌های متنوع دفاعی
- به‌عبارت دیگر کدهای AET می‌توانند به‌عنوان بی‌اثرکننده لایه‌های متعدد امنیتی یک سازمان به‌کار روند.
- روش مورد استفاده حمله‌کنندگان بسیار حرفه‌ای در تهاجمات وسیع
- بسیار پویا و غیرقابل تشخیص توسط لایه‌های متعدد امنیتی

دیپلماسی سایبری فعال

امیر دریادار دوم عطاالله مقدمی خمامی
معاون هماهنگ کننده قرارگاه پدافند سایبری کشور و معاون حقوق سایبری

درحال حاضر با توجه به رشد روزافزون فناوری اطلاعات و ارتباطات و اینترنت و به‌دلیل تأثیر فزاینده آنها، دیپلماسی سایبری و روابط بین‌الملل به یکی از ارکان و ابزار کلیدی و مهم برای حل مسائل جهانی و ارتقای همکاری‌ها مهم در کشورها تبدیل شده‌اند.

دیپلماسی سایبری فعال به مجموعه‌ای از اقدامات، فرایندها، راهبردها و تعاملات بین کشورها و نهادهای بین‌المللی اطلاق می‌شود که هدف آن ایجاد و حفظ روابط مثبت و سازنده در سطح جهانی است. این دیپلماسی به‌ویژه در دنیای امروز که با چالش‌ها و پیچیدگی‌های جدیدی در حوزه فضای سایبر روبه‌رو است، از اهمیت فوق‌العاده‌ای برخوردار بوده و نقش بسیار مهمی در تسهیل مذاکرات و همکاری‌های بین‌المللی ایفا می‌کند تا کشورها بتوانند منافع خود

را در سطح جهانی با تلاش‌های دیپلماتیک برای حل‌وفصل اختلافات، ارتقای همکاری‌های چندجانبه و پیشبرد منافع ملی خود و صلح و ثبات بین‌المللی تأمین کنند.

چالش‌های سایبری در حوزه دیپلماسی و روابط بین‌المللی:

تأمین امنیت و دفاع از منافع ملی در فضای سایبر جمهوری اسلامی ایران با چالش‌های متعددی مواجه است. این چالش‌ها می‌توانند مانع از ایجاد همکاری‌های مؤثر و کاهش تهدیدهای سایبری شوند. در ادامه به برخی از مهم‌ترین چالش‌های مؤثر در این زمینه اشاره می‌شود:

۱ تنوع تهدیدهای سایبری

تهدیدهای سایبری به‌سرعت درحال تحولند و شامل انواع مختلفی از حملات، مانند حملات پیچیده سایبری دولتی، سازمان‌یافته و تروریستی سایبری می‌شوند. این تنوع، شناسایی و پاسخگویی به تهدیدها را پیچیده می‌کند.

۲ کمبود شفافیت و اعتماد

نبود شفافیت در رفتار کشورها در فضای سایبر و عدم اعتماد به یکدیگر می‌تواند مانع از همکاری‌های بین‌المللی مؤثر شود. کشورها ممکن است نگران باشند که اطلاعات یا فناوری‌های خود را به دیگران ارائه دهند و درعوض دچار حملات یا سوءاستفاده شوند.

۳ نبود استانداردهای جهانی

نبود توافقات و استانداردهای جهانی مشخص در زمینه امنیت سایبری، به عدم هماهنگی بین کشورها و کاهش کارایی همکاری‌ها منجر می‌شود. هر کشور ممکن است رویکردهای متفاوتی نسبت به امنیت سایبری داشته باشد که می‌تواند به تنش‌ها و سوءتفاهم‌ها منجر شود.

۴ فناوری‌های نوین و چالش‌های ناشی از آن

ظهور فناوری‌های نوین مانند هوش مصنوعی، کوانتوم، رایانش ابری، اینترنت اشیا (IoT)، اینترنت اشیای صنعتی (IIoT)، بلاک‌چین و...، چالش‌های جدید و جدی را در زمینه امنیت سایبری ایجاد کرده‌اند. این تکنولوژی‌ها می‌توانند به تهدیدهای جدیدی تبدیل شوند که نیاز به همکاری و پاسخگویی مشترک دارند.

۵ عدم توانمندی‌های فنی

بسیاری از کشورها- به‌ویژه کشورهای درحال توسعه- ممکن است ازنظر فنی و فناوری در زمینه امنیت سایبری محدودیت‌هایی داشته باشند. این کمبود می‌تواند مانع از توانمندی آنها در پاسخ به تهدیدها و مشارکت در همکاری‌های بین‌المللی شود.

۶ حملات سایبری و پاسخ‌های نامتقارن

حملات سایبری معمولا نامتقارنند و کشورها ممکن است در پاسخ به حملات با چالش‌هایی مواجه شوند. این موضوع می‌تواند به تضعیف امنیت ملی و بی‌ثباتی در منطقه منجر شود.

۷ تبعیض در دسترسی به فناوری

دسترسی نابرابر به فناوری‌های پیشرفته و اطلاعات بین کشورها می‌تواند به نابرابری‌های فزاینده‌ای در توانمندی‌های امنیت سایبری منجر شود و به تعمیق شکاف‌های دیجیتال کمک کند.

۸ مسائل حقوق بشری و حریم خصوصی

نگرانی‌های مربوط به حقوق بشر و حریم خصوصی در فضای سایبر می‌تواند بر سیاست‌های امنیتی کشورها تأثیر بگذارد. کشورها ممکن است درتلاش برای تأمین امنیت، به نقض حقوق بشر و حریم خصوصی متهم شوند که می‌تواند به تضعیف همکاری‌ها منجر شود.

۹ تأثیرات اقتصادی و تجاری

نگرانی‌های اقتصادی و تجاری ممکن است بر تعاملات سایبری تأثیرگذار باشند. کشورها ممکن است به‌دلیل فشارهای اقتصادی، از همکاری در زمینه امنیت سایبری خودداری کنند یا به‌دنبال منافع اقتصادی خود باشند.

۱۰ اختلافات سیاسی و ژئوپلیتیکی

تنش‌های سیاسی و اختلافات ژئوپلیتیکی می‌توانند بر تعاملات سایبری تأثیر منفی بگذارند. کشورها ممکن است به‌دلیل تعارضات سیاسی، از همکاری در زمینه امنیت سایبری خودداری کنند. چالش‌های مطروحه یادشده در تأمین امنیت و دفاع از منافع ملی در فضای سایبر، نیاز به رویکردهای جامع و همکاری‌های مؤثر بین‌المللی را برجسته می‌کند، لذا لازم است کشورها از جمله جمهوری اسلامی ایران با درک این چالش‌ها، راهبردها و سیاست‌های مناسبی را برای مقابله با تهدیدهای سایبری و تقویت امنیت و دفاع ملی خود تدوین کنند.

انواع دیپلماسی سایبری:

با توجه به چالش‌ها و تهدیدهای سایبری، استفاده از انواع مختلف دیپلماسی سایبری می‌تواند به کشورها کمک کند تا منافع ملی خود را در دنیای دیجیتال تأمین کنند و به امنیت و ثبات جهانی نیز یاری برسانند. انواع دیپلماسی سایبری موارد زیر را شامل می‌شود:

۱ دیپلماسی امنیت دفاعی سایبری- تمرکز بر همکاری‌های بین‌المللی برای مقابله با تهدیدهای سایبری و ارتقای امنیت اطلاعات. این نوع دیپلماسی شامل توافقات و همکاری‌های دو یا چندجانبه برای بهبود امنیت و دفاع از زیرساخت‌های سایبری است.

۲ دیپلماسی پیشگیرانه- استفاده از ابزارهای دیجیتال برای پیشگیری از بحران‌ها و تنش‌های بین‌المللی از طریق ارتباطات و تبادل اطلاعات به‌موقع. این نوع دیپلماسی می‌تواند شامل استفاده از

فناوری‌های جدید برای نظارت بر شرایط و پیش‌بینی تنش‌ها باشد.

۳ دیپلماسی سایبری چندجانبه- همکاری میان چندین کشور و نهادهای بین‌المللی در زمینه مسائل سایبری، مانند تلاش برای تدوین استانداردهای جهانی برای امنیت سایبری و تبادل بهترین شیوه‌ها

۴ دیپلماسی اطلاعات- ترویج و انتقال اطلاعات مرتبط با سیاست‌ها و رویدادهای بین‌المللی از طریق رسانه‌های دیجیتال و شبکه‌های اجتماعی. این نوع دیپلماسی به شکل‌گیری نگرش‌های عمومی و آگاهی از مسائل جهانی کمک می‌کند.

۵ دیپلماسی عمومی سایبری- استفاده از رسانه‌های اجتماعی و پلتفرم‌های دیجیتال برای ایجاد تصویری مثبت از یک کشور در فضای مجازی و تعامل با شهروندان کشورهای دیگر. این نوع دیپلماسی می‌تواند به تقویت روابط مردم و کاهش تنش‌ها کمک کند.

۶ دیپلماسی اقتصادی سایبری- ایجاد و تقویت روابط تجاری و اقتصادی از طریق پلتفرم‌های دیجیتال و تجارت الکترونیک. این نوع دیپلماسی می‌تواند شامل توافقات در زمینه تجارت الکترونیکی و همکاری‌های فناورانه باشد.

۷ دیپلماسی فرهنگی سایبری- ترویج فرهنگ و هنر کشورها از طریق پلتفرم‌های آنلاین، مانند وبینارها، نمایشگاه‌های مجازی و برنامه‌های آموزشی آنلاین. این نوع دیپلماسی به تبادل فرهنگی و ایجاد درک متقابل کمک می‌کند.

۸ دیپلماسی انسانی سایبری- استفاده از فناوری‌های دیجیتال برای ترویج حقوق بشر و کمک به جوامع

آسیب‌پذیر در مواجهه با بحران‌ها. این نوع دیپلماسی می‌تواند شامل اطلاع‌رسانی در مورد نقض حقوق بشر و تلاش برای حمایت از قربانیان باشد.

رویکرد جمهوری اسلامی ایران با چالش‌ها و اتخاذ راهبردهای جامع امنیت و دفاعی سایبری:

رویکرد کشورمان در تعاملات بین‌المللی سایبری به‌منظور تأمین امنیت و دفاع از منافع ملی در فضای سایبر باید شامل مجموعه‌ای از راهبردها و اقداماتی باشد که به‌گونه‌ای مؤثر بتواند به چالش‌های موجود پاسخ دهد.

تأمین امنیت و دفاع از منافع ملی در فضای سایبری در تعاملات بین‌المللی نیازمند تدوین و اجرای راهبردهای مؤثر است که بتواند به تقویت همکاری‌ها، ارتقای امنیت و دفاع سایبری و به کاهش تهدیدها و حملات سایبری جمهوری اسلامی ایران کمک کند، همچنین این اقدامات با در نظر گرفتن راهبردهای ملی و به‌صورت هماهنگ با سایر کشورهای دوست و همسو می‌توانند به تقویت امنیت و دفاع ملی و جهانی در دنیای دیجیتال کمک کنند. در ادامه به برخی از مهم‌ترین این راهبردها اشاره می‌کنیم:

۱ تقویت همکاری‌های بین‌المللی

ایجاد و تقویت همکاری‌های دوجانبه و چندجانبه با سایر کشورها به‌ویژه کشورهای دوست و همسو و سازمان‌های بین‌المللی در زمینه امنیت سایبری از طریق توافقات رسمی، مشارکت در کنفرانس‌ها و تشکیل گروه‌های کاری مشترک به‌منظور اشتراک‌گذاری اطلاعات، تجربیات و بهترین شیوه‌ها در حوزه امنیت سایبری. این نوع همکاری می‌تواند شامل تبادل اطلاعات در مورد تهدیدهای سایبری و آموزش نیروهای امنیتی باشد.

۲ ایجاد چهارچوب‌های قانونی و حقوقی

تدوین و تقویت چهارچوب‌های قانونی و حقوقی در زمینه امنیت سایبری به‌منظور تنظیم رفتار کشورهای دیگر و جلوگیری از جرائم سایبری. این چهارچوب‌ها باید به‌صورت بین‌المللی معتبر و قابل قبول باشند.

۳ تقویت و مقاوم‌سازی زیرساخت‌های حیاتی، حساس و مهم سایبری

سرمایه‌گذاری در بهبود و مقاوم‌سازی زیرساخت‌های سایبری به‌منظور افزایش مقاومت و تاب‌آوری دربرابر حملات سایبری. این زیرساخت‌ها با استفاده از فناوری‌های نوین و روش‌های پیشرفته باید به‌گونه‌ای طراحی شوند که قادر به مقابله با تهدیدهای پیشرفته باشند.

۴ ترویج دیپلماسی سایبری مثبت

ایجاد تصاویری مثبت از کشور در عرصه سایبر با ترویج همکاری‌های سازنده و تعهد به امنیت و ثبات جهانی. این شامل حمایت از ابتکارات جهانی در زمینه امنیت سایبری و ارتقای حقوق بشر در فضای دیجیتال است.

۵ پاسخ‌های سریع و مؤثر به حملات سایبری

تشکیل تیم‌های واکنش سریع به حملات سایبری و تدوین پروتکل‌های مشخص برای مدیریت بحران‌های سایبری. این پاسخ‌ها باید سریع و مؤثر باشند تا خسارات ناشی از حملات کاهش یابد.

۶ توسعه فناوری‌های نوین

تشویق به تحقیق و توسعه در زمینه فناوری‌های نوین که به تقویت امنیت و دفاع سایبری کمک می‌کنند. استفاده از فناوری‌هایی مانند هوش مصنوعی و بلاک‌چین می‌توانند به افزایش امنیت و پیشگیری از تهدیدها و حملات سایبری کمک کنند.

۷ آموزش و توانمندسازی منابع انسانی

سرمایه‌گذاری در آموزش و توانمندسازی متخصصان امنیت سایبری از طریق برگزاری دوره‌های آموزشی، کارگاه‌ها و برنامه‌های تبادل دانش. این اقدام به ارتقای

مهارت‌ها و توانایی‌های نیروی انسانی در حوزه امنیت سایبری کمک می‌کند.

۸ برقراری تفاهمنامه‌ها و توافقات امنیتی و دفاعی

امضای تفاهمنامه‌ها و توافقات امنیتی و دفاعی با کشورهای دیگر برای همکاری در زمینه امنیت و دفاعی سایبری و تبادل اطلاعات مرتبط با تهدیدها. این توافقات می‌توانند به ایجاد چهارچوبی برای همکاری مؤثر در زمینه امنیت و دفاعی سایبری کمک کنند.

۹ تشکیل ائتلاف‌های بین‌المللی

تشکیل ائتلاف‌های بین‌المللی برای همکاری در زمینه امنیت و دفاعی سایبری و مقابله با تهدیدهای مشترک. این ائتلاف‌ها می‌توانند شامل کشورهای مختلف به‌ویژه کشورهای دوست و همسو و سازمان‌های بین‌المللی باشند.

۱۰ تحلیل و ارزیابی مستمر تهدیدها

برقراری سامانه‌های نظارتی و ارزیابی مستمر تهدیدهای سایبری به‌منظور شناسایی و پاسخ به تهدیدهای جدید و پیشرفته. این تحلیل‌ها باید به‌طور منظم انجام شوند تا کشورمان بتواند به‌روز باشد.

۱۱ توجه به مسائل حقوق بشری و حریم خصوصی

تضمین اینکه سیاست‌های امنیت و دفاعی سایبری با حقوق بشر و حریم خصوصی همراستا باشند. این موضوع می‌تواند به افزایش اعتماد کشورها و شهروندان به سیاست‌های امنیت و دفاعی سایبری کمک کند.

۱۲ ایجاد دیپلماسی سایبری در سیاست خارجی

ادغام دیپلماسی سایبری در سیاست‌های خارجی جمهوری اسلامی ایران به‌منظور تأمین منافع ملی و ایجاد روابط مثبت با سایر کشورها، به‌ویژه کشورهای دوست و همسو در زمینه امنیت و دفاعی سایبری.

جمع‌بندی:

تأمین امنیت و دفاع از منافع ملی در فضای سایبری چالشی پیچیده و چندبعدی است که نیازمند رویکردهای جامع و همکاری‌های بین‌المللی مؤثر است. با توجه به تحولات سریع فناوری و افزایش تهدیدها و حملات سایبری، کشورمان باید راهبردها و سیاست‌های معتبری را در زمینه‌های تدوین راهبردهای جامع امنیت و دفاع سایبری، تقویت همکاری‌های بین‌المللی به‌ویژه با کشورهای دوست و همسو، ایجاد چهارچوب‌های قانونی و حقوقی، آموزش و توانمندسازی منابع انسانی، تقویت و مقاوم‌سازی زیرساخت‌های حیاتی، حساس و مهم سایبری، ترویج دیپلماسی سایبری مثبت، پاسخ‌های سریع و مؤثر به حملات سایبری و... و ایجاد دیپلماسی سایبری در سیاست خارجی تدوین و اجرا کنند.

نتیجه:

با توجه به چالش‌های متعددی که در زمینه امنیت و دفاع سایبری در کشور وجود دارد، جمهوری اسلامی ایران باید از طریق رویکردهای جامع و همکاری‌های بین‌المللی، به‌دنبال ایجاد فضای سایبری امن و پایدار در کشور باشد. این اقدامات نه‌تنها به تأمین امنیت و دفاع ملی کمک می‌کند، بلکه به تقویت امنیت جهانی و ایجاد ثبات در دنیای دیجیتال نیز منجر خواهد شد. درنهایت تنها از طریق هماهنگی و همکاری‌های مؤثر مسئولان و مقامات ارشد ذی‌نقش و ذی‌ربط امنیت و دفاع سایبری کشور با استفاده از تمامی ظرفیت‌ها و قابلیت‌های سایبری کشوری و لشکری و همچنین از ظرفیت‌ها، قابلیت‌های دیپلماسی امنیت و دفاع سایبری فعال، مقتدر و عزتمند با کشورهای دوست و همسو می‌توان به چالش‌های سایبری فرارو پاسخ داد و از منافع ملی و جهانی در برابر تهدیدها و حملات سایبری محافظت کرد.

هوش تهدید سایبری
ضرورتی جدید و زیربنایی اساسی در ساختار دفاع سایبری کشور

مصطفی طوقانیان
معاون جمع آوری و برآورد تهدیدات سایبری

باتوجه به حجم بالای ابزارها ، روش ها و آسیب پذیریهای مورد استفاده مهاجمین سایبری، استفاده از هوش تهدید سایبری (CTI[1]) به یک الزام اساسی در ساختار سایبری کشورتبدیل گردیده است که می تواند زیربنای جدیدی برای دفاع سایبری تلقی گردد. تمرکز شرکت های فناور فعال در حوزه امنیت سایبری برای مجهز شدن به هوش تهدیدات در کنار برنامه ریزی های حمایتی ملی در این حوزه (نظیر ارائه خمات میزبانی و فراهم ساختن روندها و زیرساخت های مورد نیاز) می تواند از مهم ترین اقدامات ملی در راستای ارتقاء توان دفاع سایبری تلقی گردد.

در سال های اخیر، رشد قابل توجهی در تعداد و تنوع حملات سایبری مشاهده شده است . مهاجمین سایبری از روش‌های حمله پیچیده و درحال تغییر برای اخذ دسترسی های طولانی مدت و شکست

ساختار دفاعی وغلبه بر مدافعان سایبری استفاده می‌کنند.

مهاجمان از شیوه اشتراک دانش در انجمن ها و جوامع خود برای ایجاد مزیت های فنی و عملیاتی استفاده می کنند. آنها همچنین از آسیب‌پذیری‌ها و ضعف‌های امنیتی در سازمان‌های دولتی، شرکت‌ها و سیستم‌های فردی برای نفوذ سود می‌برند و دسترسی های اخذ شده را به حراج و تبادل می گذارند.

با بکارگیری فناوری‌های جدید در حوزه آفند سایبری، آشکار است که مدل‌ها و ابزارهای دفاع سایبری سنتی، مانند دیواره های آتشین، ضد بدافزارها سیستم‌های تشخیص نفوذ مبتنی بر امضاء وغیره، به تنهایی قادر به همگام شدن با روندهای جاری و مقابله با حملات نیستند.

امنیت سایبری دیگر به عنوان یک موضوع صرفاً فنی دیده نمی شود و به طور گسترده ای (به عنوان یک چالش کلان) در عرصه دفاعی با اشراف اطلاعاتی مرتبط می گردد و صحیح است اگر بگوییم " امروزه امنیت سایبری تابع تصمیمات راهبردی در ایجاد سامانه های هوش تهدید است" .

اصطلاح "هوش تهدید سایبری" نخستین بار در اوایل سال ۲۰۰۴ در ارائه ای با عنوان " Intelligence Led Corporate Security Programs " با طرح این سوال اساسی که "چرا نیاز به راه اندازی یک واحد تحلیل تهدید سایبری وجود دارد؟ " در شانزدهمین رویداد سالانه امنیت کامپیوترو رسیدگی به حوادث در بوداپست- مجارستان مطرح گردید[۲].

از سویی دیگر بررسی ها نشان می دهد خاستگاه سنتی CTI در مطالعات اطلاعاتی (نظامی) است.[۳] چند پژوهشگر در بررسی هایی در سال ۲۰۲۳ اعلام نمودند نظامی‌سازی فزاینده محیط تهدیدات سایبری، علاقه قابل‌توجهی به درک نقش هوش تهدیدات سایبری (CTI) ایجاد کرده است و ادبیات تحقیق در مورد CTI نشان می‌دهد که ریشه‌های سنتی CTI فرآیندی مشتق‌شده از چرخه اطلاعاتی است که در مطالعات اطلاعاتی نظامی به آن ارجاع می‌شود.

براین اساس گفتمان هوش تهدید از حوزه نظامی می آید ، جایی که تصمیم گیرندگان انسانی و کارشناسان اطلاعات را هدایت، جمع آوری، پردازش و به سایر ذینفعان انسانی منتشر می کنند. با اتخاذ CTI، سازمان ها می‌توانند شیوه‌های عمومی سایبری را از «واکنشی و غیر جهت‌دار» به «پیش‌گیرانه، پیش‌بینی‌کننده و پویا» تبدیل کنند.

هوش تهدید که به عنوان هوش تهدید سایبری (CTI) هم شناخته می‌شود، اطلاعاتی است که از طیف وسیعی از منابع در مورد حملات فعلی یا احتمالی علیه یک سازمان جمع‌آوری ، سازمان‌دهی و تحلیل می شود. هوش تهدید به سازمان‌ها کمک می‌کند اطلاعات بیشتری در مورد عوامل تهدید، قابلیت‌ها، زیرساخت و انگیزه‌های آن‌ها داشته باشند.

هوش تهدید به سازمان‌ها اجازه می‌دهد تا زمانی که صحبت از حملات سایبری به میان می‌آید، به جای انفعال، فعال باشند. بدون درک آسیب‌پذیری‌های امنیتی، شاخص‌های تهدید و نحوه اجرای تهدیدها، دفاع موثر در برابر حملات سایبری غیرممکن است. هوش تهدید می‌تواند سریع‌تر از حملات جلوگیری کرده و آن‌ها را مهار کند و به طور بالقوه باعث صرفه‌جویی در هزینه های زیرساختی و کسب و کاری شود.

چرخه بکارگیری هوش تهدید

این چرخه شامل شش مرحله اصلی می‌باشد که به سازمان‌ها کمک می‌کند تا با تهدیدات سایبری به شکلی مؤثرتر مواجه شوند. این مراحل به شکلی منظم و هدفمند به‌کار گرفته می‌شوند تا اطمینان حاصل شود که اطلاعات جمع‌آوری‌شده نه تنها دقیق بلکه عملیاتی و کاربردی هستند. در زیر هر یک از مراحل این چرخه توضیح داده شده است:

۱- برنامه‌ریزی و جهت‌دهی (Planning and Direction):

این مرحله شامل تعریف نیازها و اهداف سازمان برای جمع‌آوری اطلاعات است. تیم‌های امنیتی در این مرحله تعیین می‌کنند که چه نوع تهدیداتی برای سازمان از اهمیت بیشتری برخوردار است و باید بر روی آن‌ها تمرکز شود. این تصمیم‌ها معمولاً براساس خطرات بالقوه، اطلاعات مربوط به صنعت خاص، و نوع زیرساخت‌های دارای اولویت گرفته می‌شود.

۲- جمع‌آوری و دسته‌بندی (Collection and Categorization):

در طی این مرحله اطلاعات مربوط به تهدیدات از منابع مختلف جمع‌آوری می‌شود. این منابع ممکن است شامل اطلاعات عمومی مانند گزارش‌های امنیتی، داده‌های شبکه، تحلیل‌های بدافزار و اطلاعات منتشرشده توسط سازمان‌های امنیتی باشند. در این راستا، می‌توان از منابع متنوع هوش تهدید مانند Logها و رکوردهای داخلی و همچنین اینترنت و دیگر منابع فنی استفاده کرد. هدف از جمع‌آوری این داده‌ها به‌دست آوردن دیدی جامع از وضعیت تهدیدات است.

۳- پردازش (Processing):

در مرحله پردازش داده‌های جمع‌آوری‌شده به شکل قابل تحلیل و بررسی درمی‌آیند. داده‌های خام ممکن است شامل حجم زیادی از اطلاعات نامرتبط یا پراکنده باشند که باید فیلتر و ساختاردهی شوند. این داده‌ها معمولاً به دسته‌هایی مانند تهدیدات داخلی، خارجی، بدافزارهای رایج و روش‌های نفوذ دسته‌بندی می‌شوند.

۴- تحلیل و بررسی (Analysis and Evaluation):

این فاز است که منجر به تمایز «هوش تهدید» از «جمع‌آوری و انتشار ساده اطلاعات» می‌شود. در این فاز، با به‌کارگیری روش‌های تحلیل ساختاری، داده‌های پردازش شده‌ی فاز قبل مورد تجزیه و تحلیل قرار می‌گیرد. در نتیجه‌ی این اقدام، feedهای هوش تهدید سایبری ایجاد می‌شود و تحلیل‌گران به کمک آن‌ها قادر به شناسایی IOCها (Indicators of Compromise) خواهند بود. از جمله IOCهای معمول می‌توان به لینک‌ها، وب‌سایت‌ها، ایمیل‌ها، ضمائم ایمیل و کلیدهای رجیستری مشکوک اشاره داشت

۵- انتشار (Dissemination):

در این مرحله نتایج به دست‌آمده به‌صورت گزارش‌ها یا هشدارهای امنیتی به تیم‌های مختلف در سازمان‌ها منتقل می‌شود. این گزارش‌ها باید به زبان ساده و قابل‌فهم برای تمامی ذی‌نفعان تهیه شوند تا همه اعضای سازمان از مدیران تا کارشناسان فنی بتوانند از این اطلاعات استفاده کنند. قابلیت ردیابی در این فاز به گونه‌ای است که باعث ایجاد تداوم بین چرخه‌ها می‌شود.

۶- بازخورد (Feedback):

آخرین مرحله نیز بازخورد و ارزیابی عملکرد چرخه هوش تهدید است. تیم‌های امنیتی پس از پیاده‌سازی اقدامات امنیتی، بازخوردی از تأثیر آن‌ها و میزان موفقیت در جلوگیری از حملات دریافت می‌کنند. این بازخوردها به بهبود و اصلاح فرآیند هوش تهدید کمک می‌کند و چرخه را به‌روز می‌کند.

انواع هوش تهدید

هوش تهدیدات سایبری عمدتاً به چهار دسته راهبردی، تاکتیکی، فنی و عملیاتی طبقه‌بندی می‌شود.

۱ هوش تهدید راهبردی

هوش تهدید راهبردی یک نمای کلی از چشم‌انداز تهدید سازمان ارائه می‌دهد. این اطلاعات عمدتاً برای متخصصان امنیتی که راهبردهای سازمانی سطح بالا را بر اساس یافته‌های گزارش‌ها هدایت می‌کنند. در حالت ایده‌آل، هوش تهدید راهبردی بینش‌هایی مانند آسیب‌پذیری‌ها و خطرات مرتبط با چشم‌انداز تهدید سازمان را با اقدامات پیشگیرانه، عوامل تهدید، اهداف آنها و شدت حملات احتمالی ارائه می‌دهد.

۲ هوش تهدید تاکتیکی

هوش تهدید تاکتیکی شامل جزئیات بیشتر در مورد عوامل تهدید TTP (تاکتیک، تکنیک و روش‌ها) است و عمدتاً برای تیم امنیتی برای درک عامل‌های حمله است. اطلاعات به آنها بینشی در مورد چگونگی ایجاد یک رویکرد دفاعی برای کاهش این حملات می‌دهد.

۳ هوش تهدید فنی

هوش تهدید فنی بر سرنخ‌ها یا شواهد خاصی از یک حمله تمرکز می‌کند و پایگاهی برای تجزیه و تحلیل چنین حملاتی ایجاد می‌کند. تحلیلگر Threat Intelligence نشانه‌های حمله (IOC) را که شامل آدرس‌های IP گزارش شده، محتوای ایمیل‌های فیشینگ، نمونه‌های بدافزار و URLهای جعلی است، اسکن می‌کند. زمان‌بندی برای اشتراک‌گذاری اطلاعات فنی بسیار حیاتی است زیرا IOCهایی مانند IPهای مخرب یا URLهای جعلی در عرض چند روز منسوخ می‌شوند.

۴ هوش تهدید عملیاتی

اطلاعات تهدید عملیاتی بر دانش درباره حملات متمرکز است. بینش دقیقی در مورد عواملی مانند ماهیت، انگیزه، زمان و نحوه انجام یک حمله ارائه می‌دهد. در حالت ایده‌آل، اطلاعات از اتاق‌های چت هکرها یا بحث آنلاین آنها از طریق نفوذ جمع‌آوری می‌شود که به دست آوردن آن اغلب دشوار است و مستلزم برخورداری از فیدهای خاص و یا اقدامات کنشگرانه در سطح وب تاریک و پایش انجمن‌ها است.

مزایای هوش تهدید

استفاده از هوش تهدید در سازمان‌ها مزایای زیادی به همراه دارد که می‌تواند امنیت سایبری را به‌طور چشمگیری بهبود بخشد. این مزایا به تیم‌های امنیتی کمک می‌کنند تا بهتر با تهدیدات سایبری مقابله کنند و از آسیب‌پذیری‌های سازمانی محافظت نمایند. در ادامه به برخی از مهم‌ترین مزایای هوش تهدید اشاره می‌کنیم:

پیشگیری از حملات سایبری

یکی از اصلی‌ترین مزایای هوش تهدید، توانایی پیش‌بینی و جلوگیری از حملات سایبری قبل از وقوع آن‌ها است. این نوع هوش با ارائه اطلاعات به‌روز درباره تهدیدات فعال و تکنیک‌های مهاجمان به سازمان‌ها کمک می‌کند که تدابیر پیشگیرانه‌ای مانند به‌روزرسانی سیستم‌ها و نرم‌افزارها، اعمال سیاست‌های امنیتی و تنظیم فایروال‌ها را اتخاذ کنند.

کاهش ریسک‌ها و آسیب‌پذیری‌ها

با تجزیه‌وتحلیل تهدیدات و نقاط ضعف موجود، هوش تهدید به شناسایی آسیب‌پذیری‌های موجود در سیستم‌ها و شبکه‌های سازمان کمک می‌کند. این اطلاعات به تیم‌های امنیتی اجازه می‌دهد تا پیش از آن‌که مهاجمان از این نقاط ضعف سوءاستفاده کنند، آن‌ها را شناسایی و رفع کنند.

بهبود تصمیم‌گیری‌های امنیتی

این فناوری به مدیران ارشد و تیم‌های امنیتی سازمان‌ها اطلاعات جامعی درباره روندها و تهدیدات سایبری فعلی ارائه می‌دهد. این داده‌ها به آن‌ها کمک می‌کند تا تصمیمات آگاهانه‌تری در مورد سیاست‌های امنیتی، تخصیص منابع و انتخاب فناوری‌های امنیتی مناسب بگیرند.

واکنش سریع‌تر به تهدیدات

یکی دیگر از مزایای مهم هوش تهدید، افزایش سرعت و دقت در واکنش به تهدیدات است. با دسترسی به اطلاعات لحظه‌ای در مورد تهدیدات و فعالیت‌های مشکوک، تیم‌های امنیتی می‌توانند به سرعت حملات را شناسایی و واکنش مناسبی نشان دهند. این مزیت به کاهش زمان و تأثیر حملات کمک می‌کند.

بهبود همکاری و هماهنگی در سازمان

هوش تهدید اطلاعات دقیقی را در اختیار سازمان ها قرار می‌دهد و به بهبود هماهنگی در مدیریت فضای سایبری کمک می‌کند. این هماهنگی منجر به بهبود روندهای دفاعی و مقابله بهتر با حملات سایبری می‌شود.

ارتقای آموزش و آگاهی امنیتی

هوش تهدید به تیم‌های امنیتی و کارکنان سازمان کمک می‌کند تا با آخرین روش‌ها و تکنیک‌های حملات سایبری آشنا شوند. این آگاهی می‌تواند منجر به ارتقای فرهنگ امنیتی در سازمان و کاهش ریسک‌های امنیتی از طریق رفتارهای آگاهانه و محافظه‌کارانه کاربران شود.

پی‌نوشت:

1- Cyber Threat Intelligence

2- https://www.first.org/global/sigs/cti/curriculum/cti-introduction#:~:text=The%20term%20Cyber%20Threat%20Intelligence,the%20use%20of%20the%20term.

3- https://www.sciencedirect.com/science/article/pii/S0167404823002626#bib0032

ما و امنیت رسانه‌های اجتماعی

علی اکبر خلیلیان
دکتری مدیریت راهبردی فضای سایبر

امنیت رسانه‌های اجتماعی امروزه با تهدیدهای متعددی مواجه است. این تهدیدها به خصوص در صنایع تحت‌نظارت مانند بانکداری، مالی، نظامی، صداوسیما و مراقبت‌های بهداشتی و زیرساخت‌های مهم جنبه‌ای حیاتی است که نمی‌توان نادیده گرفت. استفاده از رسانه‌های اجتماعی هم برای استفاده شخصی و هم برای شبکه‌های حرفه‌ای عمیقا در زندگی ما جاافتاده است. درحالی‌که رسانه‌های اجتماعی مزایای متعددی را ارائه می‌دهند، خطرات امنیتی بالقوه‌ای را نیز به همراه دارند. کارمندان به‌عنوان اولین خط دفاعی دربرابر تهدیدهای سایبری عمل می‌کنند و برای سازمان‌ها ضروری است که آنها را به شیوه‌ها و ابزارهای مؤثر امنیت رسانه‌های اجتماعی برای محافظت از خود آماده کنند. اقدامات ناکافی امنیت رسانه‌های اجتماعی می‌تواند به چالش‌ها و تهدیدهای

بالقوه متعددی منجر شود، ازجمله نقض داده‌ها، جعل هویت و آسیب به اعتبار که به توجه حداکثری و اقدامات پیشگیرانه ما نیازمند است.

در این یادداشت بهترین شیوه‌های امنیت رسانه‌های اجتماعی برای ایمن کردن حساب‌های رسانه‌های اجتماعی و محافظت از حضور دیجیتال افراد گردآوری شده‌اند.

امنیت رسانه‌های اجتماعی چیست؟

امنیت رسانه‌های اجتماعی به اقدامات پیشگیرانه‌ای اطلاق می‌شود که توسط افراد یا سازمان‌ها برای محافظت از داده‌ها، حریم خصوصی و محرمانه بودن آنها و جلوگیری از تهدیدها و خطرات کسب‌وکارها در پلتفرم‌های رسانه‌های اجتماعی انجام می‌شود. این شامل محافظت از اطلاعات شخصی از طریق روش‌های گوناگون مانند اطمینان از پردازش ایمن تأیید اعتبار حساب، بررسی کنترل دسترسی و مجوزهای شخص ثالث و افزایش برنامه‌های آگاهی در مورد روش‌های رایج مهندسی اجتماعی و بهترین شیوه‌ها برای ایمنی برخط است.

چرا امنیت رسانه‌های اجتماعی مهم است؟

رسانه‌های اجتماعی برای محافظت از دارایی‌های دیجیتال، حریم خصوصی و شهرت افراد و سازمان‌ها مهمند. این شامل اجرای طیف وسیعی از اقدامات پیشگیرانه برای کاهش تأثیر بالقوه حملات سایبری، نقض داده‌ها و دسترسی غیرمجاز است.

اقدامات اخیر متا این فوریت را برجسته می‌کند. متا بین ژانویه تا مارس ۲۰۲۴ علیه ۶۳۱ میلیون حساب جعلی اقدام کرد. این عدد خیره‌کننده بر اهمیت شیوه‌های امنیتی قوی رسانه‌های اجتماعی تأکید می‌کند. در اینجا چند دلیل برای اهمیت و حیاتی بودن امنیت رسانه‌های اجتماعی ذکر می‌شود:

۱ از داده‌های مشتری و اطلاعات حساس محافظت می‌کند: رسانه‌های اجتماعی حجم زیادی از داده‌های شخصی را ذخیره می‌کنند. حفاظت از این داده‌ها از دسترسی غیرمجاز، حریم خصوصی را تضمین می‌کند و از سوءاستفاده‌هایی مانند سرقت هویت یا کلاهبرداری مالی جلوگیری می‌کند.

۲ حفظ شهرت برند: امنیت رسانه‌های اجتماعی برای حفظ شهرت آنلاین و حفظ اعتماد و اعتبار برند بسیار مهم است، زیرا کنترل بهتری بر حضور برخط فرد ارائه می‌دهد، از دسترسی غیرمجاز- که می‌تواند منجر به ارسال محتوای نامناسب شود- جلوگیری می‌کند و از اطلاعات حساس مانند مالکیت معنوی محافظت می‌کند که شهرت برند را حفظ می‌کنند.

۳ حملات مهندسی اجتماعی را کاهش می‌دهد: اقدامات امنیتی قوی رسانه‌های اجتماعی به جلوگیری از تهدیدهای سایبری، شناسایی سرقت، کلاهبرداری و تلاش‌های مهندسی اجتماعی ازجمله فیشینگ، بدافزار، جعل هویت و موارد دیگر کمک می‌کند، همچنین به محافظت از کاربران دربرابر فریب خوردن برای افشای اطلاعات حساس و ایجاد محیط برخط امن یاری می‌رساند.

۴ رعایت مقررات: اجرای شیوه‌های امنیتی قوی رسانه‌های اجتماعی، انطباق با مقررات مربوط به حفاظت از داده‌ها و استانداردهای صنعتی مانند GDPR،CCPA و PCI DSS را تضمین می‌کند. این فرایند از داده‌های حساس محافظت و از مجازات قانونی جلوگیری می‌کند و اعتماد و اعتبار مشتری‌تان را افزایش می‌دهد.

بهترین روش‌ها برای امنیت رسانه‌های اجتماعی

بهترین شیوه‌های استفاده از رسانه‌های اجتماعی شامل استراتژی‌های قوی برای حفظ امنیت هنگام استفاده از رسانه‌های اجتماعی است که ایجاد رمزهای عبور قوی

و منحصربه‌فرد و فعال کردن احراز هویت دومرحله‌ای برای محافظت بیشتر را شامل می‌شود. این روش‌ها به محافظت از حساب‌های شما دربرابر دسترسی غیرمجاز کمک می‌کند و امنیت کلی برخط را افزایش می‌دهد. برای کاهش این خطرات، اتخاذ بهترین شیوه‌های امنیتی که هم از افراد و هم از شرکت محافظت می‌کند، بسیار مهم است. در اینجا برخی از بهترین روش‌ها برای امنیت رسانه‌های اجتماعی آورده شده‌اند:

۱ پیاده‌سازی رمزهای عبور قوی

دستورالعمل‌های واضحی برای ایجاد رمز عبور ایجاد کنید. استفاده از رمزهای عبور قوی و منحصربه‌فرد را تشویق و از استفاده از عبارات رایج اجتناب کنید؛ از ترکیبی از اعداد و کاراکترهای خاص برای دور زدن تاکتیک‌های مهندسی اجتماعی استفاده کنید. بر اهمیت به‌روزرسانی منظم رمز عبور برای تقویت دفاع دربرابر تهدیدهای امنیتی درحال تحول تأکید کنید.

۲ فعال کردن احراز هویت دوعاملی

احراز هویت چندعاملی با درخواست فرم‌های تأیید اضافی مانند کد ارسال شده به تلفن یا ایمیل شما علاوه بر رمز عبور، یک لایه امنیتی بیشتر، اضافه می‌کند. این فرایند تضمین می‌کند حتی اگر گذرواژه‌ها درمعرض خطر باشند، هکرها نتوانند بدون احراز هویت اضافی به حساب‌ها دسترسی داشته باشند. اکثر پلتفرم‌های رسانه‌های اجتماعی روش‌های احراز هویت دومرحله‌ای را برای کاهش خطر دسترسی مجاز ارائه می‌دهند. مطمئن شوید آنها را فعال کرده‌اید تا از حساب‌ها و برنامه‌های شما محافظت کنند.

۳ حفظ کردن کنترل دسترسی

از اصل کمترین امتیاز استفاده کنید و دسترسی به نمایه‌ها، ویژگی‌ها و داده‌های رسانه‌های اجتماعی را فقط برای آن دسته از کارمندانی محدود کنید که برای نقش‌های خود به آن نیاز دارند و از رعایت آن اطمینان حاصل کنید و خطر را به حداقل برسانید.

۴ احتیاط در مورد تاکتیک‌های مهندسی اجتماعی

مراقب حملات فیشینگ باشید که شما را فریب می‌دهند تا اطلاعات حساس را فاش کنید. پیوندها یا پیام‌های مشکوک را نادیده نگیرید و گزارش دهید. هرگز رمز عبور، اطلاعات شخصی یا اطلاعات مالی را از طریق رسانه‌های اجتماعی یا کانال‌های ناامن به اشتراک نگذارید. سازمان‌های قانونی از این طریق اطلاعات حساس را درخواست نمی‌کنند. قبل از تعامل با پیوندها یا پیام‌ها، هویت فرستندگان را تأیید کنید، حتی همکاران قابل‌اعتماد یا حساب‌های دوستان و خانواده ممکن است هک شده باشند و پیام‌های آنها بخشی از حمله فیشینگ باشد

۵ اجرای استراتژی نظارت بر رسانه‌های اجتماعی

فعالیت رسانه‌های اجتماعی را در همه سکوها به‌طور مداوم رصد کنید تا تهدیدهای امنیتی بالقوه را شناسایی و زمینه‌های بهبود را شناسایی کنید.

۶ افزایش آگاهی امنیتی درمیان کارکنان

کارمندان خود را در مورد شناسایی تلاش‌های فیشینگ، سایت‌های مشکوک و تاکتیک‌های مهندسی اجتماعی از طریق جلسات آموزشی منظم آموزش دهید و تشویق به یادگیری کنید. دستورالعمل‌های جامع برای استفاده از رسانه‌های اجتماعی، مدیریت رمز عبور و مدیریت داده‌ها را اجرا کنید.

۷ استفاده از ابزارهای اتوماسیون امنیتی

از ابزارهای اتوماسیون برای نظارت مستمر حساب‌های رسانه‌های اجتماعی در زمان واقعی و علامت‌گذاری هرگونه فعالیت غیرمنطبق یا تهدیدهای امنیتی بالقوه استفاده کنید. پیاده‌سازی سیستم‌های خودکار به شما کمک می‌کند تمام تعاملات و تغییرات رسانه‌های اجتماعی را ردیابی کنید، همچنین مسیر حسابرسی واضحی را برای بررسی‌های امنیتی و بررسی‌های حادثه ارائه می‌دهد.

لزوم نهادینه کردن مباحث امنیتی در چرخه توسعه محصول

امیرحسین قاسمی
مدیر تیم امنیت سایبری گروه اسنپ

بهبود و ارتقای تمهیدات امنیتی مسیری بی‌پایان و نیازمند تفکر پویا و پیوسته درباره راهکارهای امنیتی و پیش‌بینی روندهاست. این مسیر تنها با پذیرش و درک عمیق از روش‌های حمله و آسیب‌پذیری‌های مختلف، آگاهی‌رسانی و آموزش کارکنان، به‌روزرسانی سیستم‌ها و نرم‌افزارها، استفاده از تکنولوژی‌های روز و تشکیل تیم‌های متخصص امنیت سایبری طی می‌شود.

تیم امنیت سایبری گروه اسنپ تلاش می‌کند چهار اصل راهبری، حکمرانی شرکتی، فرایندها و ابزارها و آگاهی‌رسانی و آموزش را در اولویت قرار دهد. در بخش راهبری، حفاظت از داده‌ها و حریم خصوصی یکی از اولویت‌های اصلی راهبران اجرایی محسوب می‌شود. بر همین اساس، مدیران ارشد درتمامی گروه‌ها نیازمندی‌های امنیتی را تأمین و

ریسک‌های مرتبط را مدیریت می‌کنند. در بخش حکمرانی شرکتی، استراتژی جامع امنیت سایبری با عملیات و فرایندهای سازمانی یکپارچه شده است. این رویکرد شدت اثرگذاری تهدیدها و حملات سایبری را بر کسب‌وکار به حداقل می‌رساند؛ چراکه سازوکارهای لازم برای پاسخگویی سریع و مؤثر به حوادث امنیت اطلاعات از پیش تعیین شده است. درحال‌حاضر در بخش فرایندها و ابزارها، امنیت در همه مراحل چرخه توسعه محصولات ادغام و نهادینه شده است.

برای تحقق این امر تمامی توسعه‌دهندگان در شرکت‌های زیرمجموعه گروه اسنپ از راهنمایی و مشاوره مهندسان امنیت سایبری بهره می‌برند. در بخش آگاهی‌رسانی و آموزش، تیم امنیت سایبری آگاهی‌رسانی و آموزش را براساس خلأهای امنیت اطلاعات، تجربیات شرکت‌های فعال در اکوسیستم فناوری و نیز تغییرات حوزه سایبری پایه‌ریزی می‌کند.

همچنین تیم ارزیابی امنیت (Red Team) به‌صورت مداوم و با بهره‌گیری از روش‌های پیشرفته امنیتی، همه راهکارها را مورد آزمون قرار می‌دهد تا نقاط ضعف احتمالی شناسایی و رفع شوند. این تلاش‌ها در راستای افزایش امنیت و اطمینان کاربران از محصولات و خدمات ما صورت می‌گیرد و تیم امنیت دفاعی (Blue Team) به‌صورت مستمر بر امنیت سامانه‌ها نظارت کرده و با پیاده‌سازی راهکارهای پیشگیرانه، از نفوذ و تهدیدات امنیتی جلوگیری می‌کند. هدف این تیم حفاظت از داده‌ها و زیرساخت‌های حیاتی و تضمین امنیت کاربران است.

چهارچوب توسعه امن نرم‌افزار در گروه اسنپ

امنیت نرم‌افزار با استفاده از چهارچوبی به نام رادار (RADAR) پیاده‌سازی شده است. رادار به تیم امنیت سایبری این امکان را می‌دهد که تست‌های امنیتی را در محیط CI/CD با استفاده از مجموعه‌ای از ابزارها- ازجمله SBOM، SCA، SAST، تشخیص رمزهای عبور، اسکن زیرساخت‌های کدشده (IaC)، اسکن کانتینرها و DAST- ادغام کنند. با ادغام این ابزارها در فرایند توسعه، آسیب‌پذیری‌های امنیتی بالقوه را پیش از سوءاستفاده می‌توان شناسایی و رفع کرد. رادار ۱۸۲ محصول و ۴۵ گروه را پوشش می‌دهد و به‌گونه‌ای طراحی‌شده که برای همه توسعه‌دهندگان آسان و در دسترس باشد.

برنامه‌های اجراشده برای حفظ حریم خصوصی افراد در اسنپ

در ادامه به برخی برنامه‌های اجراشده اسنپ درخصوص حفظ حریم خصوصی افراد- که در مواردی هنوز نیز درحال اجرا بوده و ادامه دارد- به‌صورت تیتروار اشاره خواهم کرد:

۱. امکان حذف حساب کاربری در بیشتر سرویس‌های سوپراپ اسنپ

۲. حذف داده‌های پزشکی کاربران اسنپ‌دکتر پس از ۲۴ ساعت

۳. رمزنگاری داده‌های حساس کاربران در پایگاه‌های داده

۴. جمع‌آوری و نگهداری حداقلی اطلاعات موردنیاز به‌منظور کاهش ریسک‌های امنیتی و حریم خصوصی

۵. حسابرسی امنیتی (Cyber Security Audit) به‌عنوان فرایندی برای ارزیابی و بررسی سیستم‌ها، فرایندها و کنترل‌های امنیتی به‌منظور شناسایی نقاط ضعف و اطمینان از انطباق با استانداردهای امنیتی.

مسابقات امنیت سایبری گروه اسنپ

برنامه باگ‌بانتی یا مسابقات ارزیابی امنیتی و شناسایی باگ، برای تقویت ساختار امنیت داده،

از اواخر ۱۳۹۸ در گروه اسنپ شروع شد و در ۱۴۰۲ گسترش پیدا کرد. در برنامه باگ‌بانتی گروه اسنپ، چهارسطح از متوسط تا حیاتی تعریف شده است. اهمیت برنامه‌های باگ‌بانتی در دوران بحران به‌طور قابل‌توجهی افزایش پیدا می‌کند. بحران‌های سایبری مانند حملات گسترده یا شناسایی آسیب‌پذیری‌های حیاتی می‌توانند تبعات جدی برای شرکت‌ها و سازمان‌ها داشته باشند. در چنین شرایطی برنامه‌های باگ‌بانتی نقش حیاتی در شناسایی و رفع سریع آسیب‌پذیری‌ها ایفا می‌کنند. این برنامه‌ها با بهره‌گیری از توانایی هکرهای اخلاقی (white hat hackers) که تخصص و دانش عمیقی در زمینه امنیت سایبری دارند، می‌توانند نقاط ضعف سیستم‌ها را پیش از سوءاستفاده هکرهای مخرب کشف کنند. این فرایند باعث می‌شود شرکت‌ها بتوانند به‌سرعت واکنش نشان دهند و از بروز خسارات بیشتر جلوگیری کنند.

اسنپ همچنین اولین رویداد باگ‌بانتی خصوصی را در شهریور ۱۴۰۳ برگزار کرد. در این رویداد خصوصی بهترین هکرهای کلاه‌سفید کشور به رقابتی ۴۸ ساعته دعوت شدند تا آسیب‌پذیری‌ها و باگ‌های امنیتی سرویس‌های اسنپ را پیدا کنند و گزارش دهند. در پایان این رویداد ۱۷۳ گزارش به‌دست ما رسید که ۲۸ مورد از آنها معتبر بود. برنده‌های این رقابت جوایزی را بدون درنظرگرفتن جایگاه و رتبه آنها و براساس میزان آسیب‌پذیری معتبری- که گزارش شده بود- دریافت کردند. درمجموع ۲۵۰ میلیون تومان جایزه در این رویداد به ۱۰ تیم اهدا شد.

با توجه به تجربه‌ای که تیم امنیت سایبری اسنپ از اواخر سال ۱۳۹۸ در بحث اجرای برنامه باگ‌بانتی داشته، این رویکرد می‌تواند به‌طور مؤثری به بهبود امنیت و عبور از دوران بحران کمک کند. شرکت‌هایی که از برنامه‌های باگ‌بانتی استفاده می‌کنند، نه‌تنها امنیت سیستم‌های خود را افزایش

می‌دهند، بلکه از اعتماد بیشتر کاربران و مشتریان نیز بهره‌مند می‌شوند، همچنین اولین دوره مسابقات فتح پرچم (CTF) گروه اسنپ ۳ اسفند ۱۴۰۲ برگزار شد. در این رقابت چالش‌هایی در زمینه وب، مهندسی معکوس، رمزنگاری پیشرفته (کریپتوگرافی)، جرم‌شناسی (فارنزیک) و نفوذ به برنامه‌های کاربردی (اکسپلویت) طراحی‌شده بود. مسابقه فتح پرچم با هدف به‌چالش کشیدن مهارت‌های علاقه‌مندان حوزه امنیت سایبری، کشف رویکردهای نوآورانه برای حل مسئله و ارتباط‌سازی اجرا شد.

در پایان لازم به یادآوری است مباحث مربوط به امنیت سایبری و حفاظت از اطلاعات کاربران به‌سرعت درحال تغییر و نیازمند به‌روزرسانی مداوم و پیوسته است. به‌روز نگه داشتن دانش، مهارت و ابزارها در این بخش می‌تواند برگ برنده حفظ امنیت سایبری برای هر سازمان یا کسب‌وکاری باشد.

در بخش حکمرانی شرکتی، استراتژی جامع امنیت سایبری باعملیات‌وفرایندهای سازمانی یکپارچه شده است. این رویکرد شدت اثرگذاری تهدیدها و حملات سایبری را برکسب‌وکار به حداقل می‌رساند؛ چراکه سازوکارهای لازم برای پاسخگویی سریع ومؤثر به حوادث امنیت اطلاعات ازپیش تعیین شده است. درحال حاضر در بخش فرایندها و ابزارها، امنیت در همه مراحل چرخه توسعه محصولات ادغام و نهادینه شده است

درباره امنیت و حریم خصوصی کاربران در دیوار

پویا رضایی
راهبر ارشد فنی دیوار

ما در دیوار برای حفاظت از حریم خصوصی کاربران‌مان مجموعه‌ای از بهسازی‌ها و به‌روزرسانی‌ها را به‌اجرا گذاشته‌ایم که امنیت داده‌های کاربران را بهبود می‌بخشد. البته ما فرایند ایمن‌سازی را کاری همیشگی و به‌هم‌پیوسته با کار مهندسی می‌دانیم و می‌کوشیم گام‌به‌گام در این راه پیشرفت کنیم. هرچند هنوز کاستی‌های بسیاری وجود دارد، اما تلاش ما بر بهبود پایدار و همیشگی است. برخی بهسازی‌ها که در ادامه این نوشته آمده، هنوز در دست انجام است.

درکنار فرایند امن‌سازی، ما آغاز به گمنام‌سازی داده‌های تحلیلی کرده‌ایم؛ به‌گونه‌ای که پیگیری هویت کاربران، حتی برای مهندسان و بررسی‌کنندگان داخلی نیز امکان‌پذیر نباشد. ما این گمنام‌سازی را از داده‌های جست‌وجو و کلیک‌های کاربران آغاز کرده‌ایم. ازنظر ما در دیوار فرایند امن‌سازی یک

فرایند پیشگیرانه است که هرچند واجب است، اما هیچ‌گاه به‌طورکامل امنیت داده‌های کاربران را تضمین نمی‌کند. در اینجاست که هر کسب‌وکاری در دوراهی قرار می‌گیرد؛ نگهداری داده‌های ارزشمند و بیشتر از کاربران برای پیشرفت و گسترش خود یا نگه نداشتن چنین داده‌هایی و تضمین بیشتر امنیت داده‌های شخصی کاربران. در دیوار تلاش کرده‌ایم نقطه بهینه این تعادل را پیدا و داده‌ها را به‌صورت گمنام نگهداری کنیم، همچنین دیوار درحال افزودن امکان «حق فراموش‌شدن» برای کاربران است تا پس از گذشت زمان قانونی، پیوند هویت کاربر با داده‌های عملکردی به‌طور کامل پاک شود.

با افزودن امکان حذف حساب کاربری، کاربران دیوار می‌توانند تمامی داده‌های مرتبط با خود را به‌صورت همیشگی حذف کنند و در صورت ورود دوباره، همچون یک کاربر جدید شناخته شوند، همچنین امکان مدیریت دستگاه‌های متصل به حساب کاربری به‌زودی فراهم می‌شود تا کاربران بتوانند دستگاه‌های مشکوک یا ناخواسته را غیرفعال کنند. دیوار با اجرای این تغییرات درتلاش است به‌سمت ایجاد محیطی امن‌تر و قابل‌اعتمادتر برای کاربران خود حرکت کند. ما امیدواریم ازاین‌پس نیز با یادگیری از تجربیات به‌دست‌آمده، تغییرات بیشتری در جهت پاسداشت حریم خصوصی و امنیت کاربران اعمال کنیم.

گفت‌وگو

ابوالحسن فیروزآبادی، دبیر شورای عالی فضای مجازی
ورئیس سابق مرکز ملی فضای مجازی

باید در فضای سایبری جهانی همزیستی داشته باشیم

سیاستگذاران حوزه فضای مجازی کشور بر این باورند که یکی از راه‌های برقراری امنیت سایبری کشور ایجاد تعامل با جهان است. همچنین از منظر آنها راه شناخت فضای سایبری تعامل و به میان آوردن آن در زندگی روزمره افراد است، یعنی الزام شناساندن این حوزه و رشد در برقراری آن را شناخت این حوزه می دانند، مثلا همان طور که در فضای فیزیولوژیکی با انواع بیماری ها و تهدیدهای انسان آشناییم. در این حوزه باید طبق برنامه ریزی، نهادهای تخصصی آسیب ها و فرصت ها را مغتنم شمرد.

ابوالحسن فیروزآبادی، دبیر شورای عالی فضای مجازی و رئیس سابق مرکز ملی فضای مجازی بر این باور است که رشد در حوزه امنیت سایبر باید مانند رشد در سطوح مختلف اجتماع مانند درمان یا بهداشت باشد، همچنین وی از الزامات رشد در امنیت سایبری را تربیت افراد متخصص در این حوزه و فعالیت حرفه‌ای نهادهای مرتبط می داند. در ادامه گفت‌وگوی تفصیلی با فیروزآبادی را از نظر می گذرانید.

اهمیت راهبردی امنیت سایبری برای امنیت ملی و

به‌طورکلی اهداف این حوزه را چه می‌دانید؟

حوزه سایبری به این دلیل که تکنولوژی پایه است و تحولات آن بسیار سریعند، اصولا در این فضا و معماری آن به‌دنبال توسعه ارتباطات و افزایش مبادله اطلاعات و تولید اطلاعات است، همچنین پدیده‌ها این محیط را متلاطم می‌کنند. اینکه ما بتوانیم در فضای متلاطم، امنیت صددرصدی را حفظ کنیم، مقدور نیست. به همین دلیل تئوری‌های امنیتی سایبری مبتنی‌بر کاهش تهدیدها و رفع آسیب‌پذیری‌ها هستند، یعنی این تصور که شما در فضای سایبری زندگی و فعالیت و تولید ارزش کنید و ضمن اینکه این فعالیت و تولید ارزش امنیت صددرصدی داشته باشد، تقریبا منتفی است. همان‌طور که در فضای فیزیکی نیز در محیط بیولوژیکی شما نمی‌توانید بگویید فعالیتی که انجام می‌دهم از ویروس‌ها، قارچ‌ها و هر چیزی که برای محیط طبیعی انسان مضرند، در امانید. مهم این است که ما فضایی مناسب را برای زیست فراهم کنیم. هم در فضای فیزیکی و هم در فضای سایبری، لذا در امنیت سایبری دو هدف را مدنظر قرار می‌دهند؛ یکی اینکه از بین بردن و رفع آسیب‌پذیری‌هاست و دیگری کاهش تهدیدهایی که وجود دارند.

به‌نظر شما چالش‌های و فرصت‌های زیرساخت‌های سایبری کشورمان را چیستند و درمجموع چه تهدیدها و فرصت‌هایی پیش روی ماست؟

چالش‌های گوناگونی در رابطه با زیرساخت‌های حیاتی کشور در حوزه امنیت سایبری وجود دارند، یکی اینکه به همان نحوی که اکنون بشر در فضای فیزیکی می‌تواند خطر بهداشتی را ملاحظه کند و در صورت اشکالات برای درمان مراجعه و اقدام کند، در فضای سایبری نیز دیدن تهدیدها و آسیب‌پذیری‌ها ناملموسند، بنابراین باید سطح دانش خودمان را در فضای سایبری بالا ببریم، مانند زمانی که در فضای فیزیکی سطح دانش اجتماعی، فیزیولوژیکی یا بهداشتی را بالا می‌بریم تا بتوانیم امنیت افراد جامعه را تضمین کنیم. در فضای سایبری نیز باید زمان صرف آموزش، ترویج، توجیه و محسوس کردن خطرات ناملموس و نامحسوس شود. دومین کار این است که بتوانیم نهادهای مناسبی را در کشور فراهم کنیم، درست همان‌طور که در فضای فیزیکی برای درمان نهادهای مناسبی داریم- از داروخانه گرفته تا کلینیک و پاراکلینیک و پزشکانی با تخصص‌های مختلف- که همه مجموعه‌ای را تشکیل می‌دهند تا اکوسیستم و زیست‌بوم سالمی را برای شهروندان تشکیل دهند. متأسفانه در فضای مجازی این ساختارها شکل نگرفته‌اند. این افراد تربیت نشده‌اند و آن زنجیره ارزشی که مثلا ما در نظام درمان و بهداشتی کشور و در نظام حفظ محیط زیست داریم، در فضای سایبری همه این نهادها و همه این فرایندها شکل نگرفته‌اند و همه آدم‌هایی که برای تصدی محیط نیاز است، آموزش‌های لازم را ندیده‌اند. این زیست‌بوم مجازی نیز درحال شکل گرفتن است و این درحالی است که این فضا، فضای به‌شدت متلاطمی است که از تحولات تکنولوژی و توسعه شبه‌انفجاری فضای سایبری ناشی شده‌اند.

به نظر شما در این میان چه نتیجه‌ای باید حاصل می‌شد؟ یعنی دقیقا در فضای امنیت سایبری به چه چیزی باید می‌رسیدیم؟

یکی از مشکلاتی که وجود دارد، این است که به‌طور سنتی در دیدگاه‌مان نهادینه شده که امنیت وظیفه حکومت‌هاست. در فضای سایبری این مقوله که مطلق امنیت سایبری به‌طورکلی برعهده حکومت است، به‌شدت زیرسؤال است. فضای سایبری فضای اجتماعی است و حفظ محیط زیست همان‌طور که بدون کمک شهروندان و فعالیت شرکت‌ها و ان جی اوها امکان‌پذیر نیست، در فضای سایبری نیز حفظ امنیت سایبری و داشتن فضای سایبری سالم برای فعالیت کردن، بدون مشارکت مدنی و بخش خصوصی و سایر بخش‌های اجتماعی مقدور نیست. یکی از مشکلاتی که ما در حوزه امنیت سایبری داریم، متأسفانه

این است که از این ظرفیت به‌طور مناسب استفاده نمی‌کنیم. بخشی از امنیت سایبری توسط دستگاه‌ها، سخت‌افزارها و نرم‌افزارهای وارداتی صورت می‌گیرد و عموما سعی می‌کنیم این امر را در چهارچوب دولت و حکومت منحصر کنیم. نمی‌گویم از ترویج آن از بخش خصوصی و سایر بخش‌های اجتماعی جلوگیری می‌شود، اما توجه کافی برای توسعه آن رخ نمی‌دهد. به نظر من در این زمینه باید در نظام آموزشی، رسانه‌ای و فعالیت‌های اجتماعی خود به‌طورجدی به بحث حفظ امنیت سایبری و داشتن فضایی امن توجه کنیم و برای رسیدن به آن، تلاش گسترده‌ای به عمل بیاید.

رویکرد ایران در تعاملات بین‌المللی سایبری و دیپلماسی برای دفاع از امنیت ملی در فضای سایبری را چگونه ارزیابی می‌کنید و اساسا به نظر شما این موضوع باید در عرصه بین‌الملل به چه صورت باشد؟

فضای سایبری فضایی جهانی است و ما در فضای جهانی هم باید نوعی همزیستی داشته باشیم و قرارمان را بر همزیستی بگذاریم. اگر قرارمان بر همزیستی گذاشته شود، آن‌وقت بحث امنیت سایبری می‌تواند مقوله جدی و درستی باشد. اگر بنایمان را بر آنارشیسم و عدم همکاری در فضای سایبری درحال تلاطم قرار دهیم، آنگاه کار حفظ امنیت سایبری در کشور بسیار سخت می‌شود. به همین دلیل تلاش جمهوری اسلامی در سال‌های اخیر این بوده که در نهادهای بین‌المللی مثل سازمان ملل به‌دنبال مصوبات مناسبی در حوزه امنیت سایبری باشد و تلاش کند تا بتواند سطح تعهدات متقابل دولت‌ها را افزایش دهد و راهی پیدا کند که دولت‌ها در پلتفرم‌هایی که جهانی‌اند، مسئولیت‌پذیری داشته باشند. همچنین تلاش شده کشورهای جهان سوم و درحال توسعه را- تا آنجا که مقدور بوده است- با خود همراه کند تا بتوانیم به اسناد بین‌المللی مناسب برای ایجاد نوعی تعاملات همزیستی در سطح بین‌المللی در میان فعالان فضای سایبری برسیم. این کار لاجرم باید صورت بگیرد، چون بخش بزرگی از تهدیدهای سایبری از خارج از مرزهای ما اعمال شده و بخش بزرگی از امنیتی که ما درپی برقراری آن در جامعه‌ایم، بدون همکاری سایر دولت‌ها و شرکت‌هایی امکان‌پذیر نیست که فعالیت جهانی دارند. اگر بتوانیم این فضای همکاری را ترویج کنیم، آن موقع باید امیدوار باشیم بتوانیم فضای سایبری شکوفا و امن را در کشورمان برقرار کنیم. اگر بنای پلتفرم‌ها و شرکت‌های بزرگ جهانی این باشد که با کشورهای درحال توسعه درگیر باشند و تفاهم و تعامل وجود نداشته باشد و این محیط را یک محیط نزاع و جنگ تبدیل کنند، ما آینده تیره‌وتاری را در حوزه امنیت سایبری پیش‌بینی می‌کنیم.

پیش‌بینی شما از آینده حوزه امنیت سایبری چیست؟

من معتقدم چون اقتصاد بزرگی در این فضا درحال شکل‌گیری است، خواه‌ناخواه آن لجام‌گسیختگی که امروزه در حوزه فعالیت پلتفرم‌ها در دنیا وجود دارد، به‌سمت نظم مشخص‌تر و ضرورت تدوین کنوانسیون‌ها پیش رفته و به‌سمتی حرکت می‌کند که دیپلماسی شرکتی در حوزه فضای سایبری صورت بگیرد - در دیپلماسی شرکتی، روابط شرکت‌ها و دولت‌ها تنظیم شده و در آن توافقاتی صورت می‌گیرد- و به‌صورت کلی پیش‌بینی من این است که به‌سمت نوعی تعادل در اکوسیستم حرکت خواهیم کرد.

درباره اینکه ما بحث امنیت را دولتی می‌دانیم صحبت شد. راهکار شما برای نهادینه‌سازی پدافند و ادبیات سایبری در جامعه و آوردن بخش‌های غیردولتی به پای کار چیست؟

همان‌طور که عرض کردم، در نظام آموزش بخشی از اجتماعی و نهادینه شدن بعضی امور در جامعه برعهده مدارس و نظام آموزشی است. درکنار نظام آموزشی، نظام رسانه‌ای وجود دارد و این دو نقش بسیار بزرگی دارند. به نظر من ما باید از خصلت آموزش اطلاعاتی فضای مجازی استفاده کنیم و بخش قابل توجهی از آموزش در نظام‌های

آموزشی، تربیتی، پرورشی و رسانه‌ای را برای آموزش چگونه زیستن، چگونه فعالیت کردن، چگونه حفظ کردن دارایی و بهره‌برداری از فرصت‌های فضای مجازی قرار دهیم. یکی از وظایف این حکومت و حتی مردم، کمک به ترویج این قضیه است و ما بایستی حتما به نسل Z- که یکی از نگرانی‌ها در مورد آنها این است که ما در فضای مجازی افراد متلاطم داریم تربیت می‌کنیم که اینها افراد متلاطم فیزیکی نیستند و افراد متلاطم مجازی‌اند- توجه کنیم. چه بسا به فضای آموزشی در کشور بروید و ببینید که ما درحال آموزش کودکانی به شدت آرام و بدون تحرکیم و به این صورت است که نوآوری فقط به‌صورت یک کلمه در نظام آموزشی است که دائما تکرار شده، همچنین به‌دنبال این هستیم که این افراد مواد خامی شوند که به خارج از کشور بروند و تحصیل کنند، درحالی‌که لزومی ندارد در نظام خارج از کشور مشغول به تحصیل شوند. شما در نظام آموزشی خود نحوه استفاده از فضای مجازی را به‌شکلی یاد بدهید که آن شخص به مملکت خود، رشد خود، وارد شدن به رقابت جهانی، دفاع از مملکت خود، تعصب و دفاع از هویت‌های خود و ارتقای آنها علاقه داشته باشد. متأسفانه اکنون نظام آموزشی ما فاقد این موارد است و فقط یک گزینه تهدید فضای مجازی وجود دارد و برای اینکه تهدید به ما لطمه دیگری نزند، به‌سمت روش‌هایی می‌رویم که صلاح نیست آنها را گسترش دهیم، چون این جهان ترکیبی از فضای مجازی و حقیقی است و ما باید در فضای مجازی توسعه پیدا کنیم. اتفاقا فضای مجازی یکی از فرصت‌های بزرگ ملی ماست که می‌توانیم در آن عرض‌اندام کنیم و ظهور و بروز داشته باشیم. بحث سوشالیزیشن یا اجتماعی شدن و آموزش دیدن و رشد کردن و نحوه زیست در فضای مجازی بایستی به‌شدت موردتوجه نظام آموزشی و پرورشی ما قرار بگیرد که نظام رسانه‌ای حکومتی و دولتی ما در این حوزه دچار قصور است و به نظر می‌رسد نسبت به واقعیت‌های سایبری جهان بی‌توجه است. درواقع نگاه این نظام به فضای سایبری، همیشه به گذشته و نهایتا حال بوده و نگاهی به آینده نداشته و آن را به توکل واگذار می‌کند.

فضای سایبری فضایی جهانی است و ما در فضای جهانی هم باید نوعی همزیستی داشته باشیم و قرارمان را بر همزیستی بگذاریم. اگر قرارمان بر همزیستی گذاشته شود، آن‌وقت بحث امنیت سایبری می‌تواند مقوله جدی و درستی باشد. اگر بنایمان را بر آنارشیسم و عدم همکاری در فضای سایبری درحال تلاطم قرار دهیم، آنگاه کار حفظ امنیت سایبری در کشور بسیار سخت می‌شود. به همین دلیل تلاش جمهوری اسلامی در سال‌های اخیر این بوده که در نهادهای بین‌المللی مثل سازمان ملل به‌دنبال مصوبات مناسبی در حوزه امنیت سایبری باشد و تلاش کند تا بتواند سطح تعهدات متقابل دولت‌ها را افزایش دهد و راهی پیدا کند که دولت‌ها در پلتفرم‌هایی که جهانی‌اند، مسئولیت‌پذیری داشته باشند

دکترجواد غریبی، معاون آموزش و پژوهش
قرارگاه پدافند سایبری کشور

بیش از ۲۵ هزار نفر آموزش تخصصی دیدند

نهادینه‌سازی فرهنگ سایبری و آموزش در سطوح مختلف برای آشنایی با این فضا موضوعی است که از بدو تأسیس سازمان پدافند غیرعامل در دستور کار قرار گرفته است. تعریف کردن رشته‌های درسی امری است که در راستای آموزش و البته بومی‌سازی پدافند سایبری صورت گرفته و جدای از آن کتاب‌هایی نیز در سطوح مختلف برای آشنایی مردم با پدافند سایبری منتشر شده است. جواد غریبی، معاون آموزش و پژوهش قرارگاه پدافند سایبری در این گفت‌وگو به جزئیات بیشتری از فعالیت آموزشی قرارگاه پدافند سایبری پرداخته است که در ادامه ازنظر می‌گذارید.

معاونت قرارگاه پدافند سایبری چه وظایفی را برعهده دارد؟

یکی از معاونت‌های مهم قرارگاه پدافند سایبری معاونت آموزش و پژوهش است. این معاونت تلاش دارد نسبت به تولید محتوای علمی و فرهنگی و برنامه‌ریزی آموزش‌های لازم در سطوح مختلف اقدامات لازم را به‌عمل آورد. با توجه به مأموریتی که

این معاونت برعهده دارد، دوره‌های آموزشی را در سطح زیرساخت‌های کشور برگزار می‌کند. در این دوره‌ها زیرساخت‌های حیاتی و حساس کشور معرفی می‌شوند و برنامه‌ریزی‌های این زیرساخت‌ها طی سال‌های مختلف انجام می‌شود. از اهداف مهم این دوره‌ها ایجاد محتواهای آموزشی مناسب است. برای تولید این محتواها از استادان دانشگاه‌ها و کارشناسان مجرب بهره گرفته می‌شود تا مطالب باکیفیت بالا تولید شوند. طی چندسالی که پدافند سایبری شروع به کار کرده، معاونت آموزش و پژوهش در سازمان پدافند غیرعامل، کتاب‌های بسیاری در سطوح مختلف با موضوع آموزش پدافند سایبری تألیف و ترجمه کرده است. یکی از آثار بسیار ارزشمند تألیف کتاب‌های پنج جلدی محتوای دوره‌های آموزشی کوتاه‌مدت (عرضی) پدافند سایبری در پنج سطح، طبقه‌بندی شده‌اند که پایین‌ترین سطح آن، سطح عمومی است. ما برنامه‌هایی آموزشی بسیاری برای مدارس کشور و فرهنگیان عزیز ارائه داده‌ایم؛ حوزه‌هایی مانند شبکه‌های اجتماعی، IT، حوزه‌های بانکی و Wi-Fi با مسائلی که مردم با آنها روبه‌رو هستند، راهکارهای مناسبی را به مردم معرفی می‌کند. محتوای آموزش مجازی و فایل pdf این کتاب از طریق وبگاه pdrc.ir در اختیار همه مردم قرار داده شده که از طریق این وبگاه بتوانند از مطالب و راهکارها استفاده کنند. سطح دوم، سطح مقدماتی است که در این کتاب با یک سطح بالاتر، آسیب‌پذیری‌ها را در این حوزه‌ها معرفی می‌کند و راهکارهای مناسبی را ارائه می‌دهد. ما برای این دو سطح از سال ۹۸ دوره‌های آموزشی ازجمله آموزش مجازی برای دانش آموزان و معلمان عزیز تدارک دیده‌ایم و در این خصوص با آموزش‌وپرورش هم تفاهمنامه‌ای امضا شده است. سطح سوم این کتاب‌ها دوره تخصصی هستند. درواقع کتاب‌های تخصصی در دو سطحند؛ دوره فنی پدافند سایبری و دوره تخصص پدافند سایبری که هر دو سطح برای کسانی مناسب است که در زیرساخت‌های حیاتی، حساس و مهم کشور (مانند صداوسیما، حمل‌ونقل، حوزه انرژی (نفتی، گازی و نیرو) و سایر حوزه‌های حیاتی کشور) کار می‌کنند. درحال‌حاضر این دوره‌ها جمع‌بندی شده و سرفصل‌هایش تهیه شده‌اند. درواقع این کتاب‌ها تألیف شده و مطالب آن هم قبلاً آماده شده است.

همچنین دوره‌های مختلفی طی این سال‌ها برگزار کرده‌ایم. سال ۹۸ نزدیک به ۳۰ دوره در استان‌های کشور برای زیرساخت‌های کشور برگزار کرده‌ایم. این دوره‌ها در سطح فنی و تخصصی پدافند سایبری به‌صورت حضوری برگزار شده‌اند. مدیران کل پدافند غیرعامل در استان‌ها با استانداری‌ها و با بخش‌های زیرساختی هماهنگ شده‌اند. در دوره شیوع کرونا، این دوره‌ها به‌صورت آموزش مجازی و ویدئوکنفرانس اجرا شدند. برای بسیاری از زیرساخت حیاتی و حساس کشور حوزه حمل‌ونقل، حوزه انرژی، بانک و سایر بخش‌ها، این دوره‌ها را به‌صورت مجازی برگزار کرده‌ایم. درواقع در برنامه آموزشی، ما هرسال دوره‌های تخصصی پدافند سایبری برای زیرساخت‌های کشورمان برگزار می‌کنیم. بخشی از این دوره‌ها با همکاری شرکت‌های دانش‌بنیان- که گواهینامه اجرای دوره در زیرساخت‌های حیاتی و حساس را از سازمان پدافند غیرعامل دریافت کرده‌اند- در چندسال اخیر به‌صورت تولید محتوای آموزشی مجازی برگزار شده‌اند را در ادامه آنها مرور می‌کنیم:

۱ اجرای دوره آموزش تخصصی پدافند سایبری (سطح ۱ و ۲- ۱۲ساعت) مجموعا ۲۵۵۰۰ نفر از زیرساخت‌های حیاتی، حساس و مهم کشور

۲ اجرای اولین دوره آموزش مجازی تخصصی پدافند سایبری (۱۲ ساعت) در اسفندماه سال ۱۳۹۹ (با گرامیداشت یاد سردار دکتر علی‌اصغر زارعی) تعداد شرکت‌کننده‌ها در این دوره آموزشی ۸هزار نفر از زیرساخت‌های کشور

۳ اجرای دوره آموزش مجازی تخصصی پدافند سایبری به‌صورت آنلاین برخط (۱۶ ساعت) تعداد شرکت‌کننده‌ها در این دوره‌های آموزشی ۱۳۵۰۰ نفر از زیرساخت‌های کشور (با همکاری شرکت پردیس شریف)

۴ اجرای دوره آموزش مجازی تخصصی پدافند سایبری سطح ۳ برگزار شد (۲۴ ساعت آموزش). تعداد شرکت‌کنندگان در این چهار دوره، ۱۳هزار نفر (با همکاری شرکت رستار نوین رایا)

۵ اجرای دوره آموزش مجازی تخصصی پدافند سایبری سطح ۴ برگزار شد (۲۴ ساعت آموزش). تعداد شرکت‌کنندگان در این دو دوره، دوهزار نفر (با همکاری شرکت رستار نوین رایا)

سطح پنج این کتاب، مدیریت راهبردی پدافند سایبری است. این کتاب برای مدیران زیرساخت‌های کشور است که بتوانند با ادبیات پدافند سایبری آشنا شوند. این کتاب‌ها و کتاب‌های دیگری را که ما در این حوزه چاپ کرده‌ایم در ادامه معرفی می‌کنیم.

تاکنون چه کتاب‌هایی چاپ شده‌اند؟

کتاب‌های پنج جلدی دوره‌های آموزشی کوتاه‌مدت و عرضی پدافند سایبری، تروریسم سایبری، امنیت سایبری راهبردی، شبکه‌های سیستم کنترل مقاوم، حقوق بین‌الملل مدرن و جنگ سایبری در فضای مجازی و سایر کتاب‌های امن‌سازی اضطراری پروتکل opc، شهر هوشمند، پایداری، تاب‌آوری و امنیت شهر هوشمند، مدل بلوغ شهر هوشمند ترجمه و چاپ کتاب تالین ۱ و ۲، ترجمه و چاپ کتاب تهدیدات سایبری و... .

برنامه‌های آموزشی قرارگاه پدافند سایبری در سال جدید چیست؟

از اول سال ۹۹- با توجه به اینکه بحث بیماری کرونا پیش آمد- برنامه‌ها را وارد حوزه آموزش‌های

برنامه‌های آموزشی به این صورت است که برای زیرساخت‌ها یک برنامه آموزشی ۱۲ ساعته اجرا می‌کنیم. سرفصل‌های این دوره‌های آموزشی از این قرارند؛ اولین سرفصل، کلیات اصول پدافند سایبری است. ادبیات پدافند سایبری مهم‌ترین بخش این دوره‌هاست که برگزار می‌کنیم. مصون‌سازی زیرساخت‌های سایبری کشور به‌تنهایی یک دوره هشت‌ساعته است که به‌صورت مجازی در سازمان پدافند غیرعامل ضبط شده است. علاوه‌بر این، ما از چند شرکت آموزشی خارج از سازمان نیز حمایت می‌کنیم و محتوای آموزشی را در اختیار آنها قرار می‌دهیم. محتوا و استادان هم از قرارگاه پدافند سایبری معرفی می‌شوند

مجازی کردیم. تاکنون چند دوره برای بانک‌ها اجرا کرده‌ایم. برنامه‌های آموزشی به این صورت است که برای زیرساخت‌ها یک برنامه آموزشی ۱۲ ساعته اجرا می‌کنیم. سرفصل‌های این دوره‌های آموزشی از این قرارند؛ اولین سرفصل، کلیات اصول پدافند سایبری است. ادبیات پدافند سایبری مهم‌ترین بخش این دوره‌هاست که برگزار می‌کنیم. مصون‌سازی زیرساخت‌های سایبری کشور به‌تنهایی یک دوره هشت‌ساعته است که به‌صورت مجازی در سازمان پدافند غیرعامل ضبط شده است. علاوه‌بر این، ما از چند شرکت آموزشی خارج از سازمان نیز حمایت می‌کنیم و محتوای آموزشی را در اختیار آنها قرار می‌دهیم. محتوا و استادان هم از قرارگاه پدافند سایبری معرفی می‌شوند. استادان را در دوره ۳۲ ساعته تربیت مربی پدافند سایبری آموزش داده‌ایم که سرفصل‌هایش قبلا تدوین شده است. در سال‌های مختلف در کل استان‌های کشور به‌خصوص در تهران، این استادان را تربیت کرده‌ایم و از مرکز مطالعات نیز کارت تربیت مربی دریافت کرده‌اند. موضوع بعدی مصون‌سازی زیرساخت‌های حیاتی کشور چند بخش دارد؛ اولین بخش، متدولوژی احصای آسیب‌پذیری‌هاست. ما باید آسیب‌پذیری‌های زیرساخت‌های کشور را بشناسیم و هم‌ادبیات شویم. بعد از شناسایی آنها لازم است فرایند مصون‌سازی را شروع کنیم. یکی از مهم‌ترین متدولوژی‌ها در این زمینه دفاع در عمق است که این یکی از بخش‌های مهم ادبیات پدافند سایبری است و از تجربیات استادان قرارگاه پدافند سایبری استفاده می‌کند و تدریس می‌شود. بخش بعدی متدولوژی تاب‌آوری و بازدارندگی سایبری است که در این موضوع یک دوره چهارساعته برگزار می‌کنیم. بخش بعدی- که یکی از مأموریت مهم قرارگاه پدافند است- رزمایش و تمرین سایبری است که برای آن دوره‌های آموزشی مختلف برگزار کرده‌ایم. در سال ۱۴۰۲ برای بسیاری از بخش‌های مختلف کشور به‌خصوص در

موضوع مصون‌سازی زیرساخت‌های حیاتی کشور چند بخش دارد؛ اولین بخش، متدولوژی احصای آسیب‌پذیری‌هاست. ما باید آسیب‌پذیری‌های زیرساخت‌های کشور را بشناسیم و هم‌ادبیات شویم. بعد از شناسایی آنها لازم است فرایند مصون‌سازی را شروع کنیم. یکی از مهم‌ترین متدولوژی‌ها در این زمینه دفاع در عمق است که این یکی از بخش‌های مهم ادبیات پدافند سایبری است و از تجربیات استادان قرارگاه پدافند سایبری استفاده می‌کند و تدریس می‌شود. بخش بعدی متدولوژی تاب‌آوری و بازدارندگی سایبری است که در این موضوع یک دوره چهارساعته برگزار می‌کنیم. بخش بعدی- که یکی از مأموریت مهم قرارگاه پدافند است- رزمایش و تمرین سایبری است که برای آن دوره‌های آموزشی مختلف برگزار کرده‌ایم

حوزه‌های حمل‌ونقل، هواپیمایی، راه‌آهن، حوزه انرژی و سایر حوزه‌ها (قوه قضائیه و ثبت‌اسناد) دوره آموزشی برگزار کرده‌ایم و امسال هم این دوره‌ها به‌صورت آموزش مجازی درحال برگزاری هستند. یک‌سری دوره‌ها را سازمان‌ها از ما درخواست می‌کنند و دوره‌هایی را برای آنها درنظر می‌گیریم که به‌صورت آموزش مجازی برگزار می‌شوند. بحث بعدی، طرح کاهش آسیب‌پذیری و مصون‌سازی قرارداد پدافند سایبری است. یک‌سری اسناد امن‌سازی است که ما معرفی می‌کنیم. از این اسناد در حوزه پاسخ به شرایط اضطراری سایبری استفاده می‌کنند. این اسناد در حوزه‌های بانکی، نفتی، هواپیمایی و حمل‌ونقل آماده شده و در اختیار زیرساخت‌ها قرار گرفته‌اند.

سال گذشته همه این کتاب‌ها را چاپ کرده‌ایم و در اختیار استان‌ها و همه زیرساخت‌ها قرار داده‌ایم. امسال نیز چند همایش داریم که ان‌شاءالله اجرا می‌کنیم. بحث مهم دیگر برگزاری همایش‌هاست. ما قصد داریم در این همایش‌ها استادانی را معرفی کنیم که مقالات و طرح‌های جدید دارند. بحث‌های آموزشی که در این همایش‌ها معرفی می‌شود، فناوری‌های نوین سایبری ازجمله IOT، اینترنت اشیا و اینترنت اشیای صنعتی و هوشمندسازی است، همچنین پردازش کوانتومی و هوش‌مصنوعی بحث‌های جدیدی‌اند که در این همایش‌ها بیشتر این موضوعات را معرفی می‌کنیم.

قرارگاه پدافند سایبری چه اقداماتی را برای بومی کردن دانش سایبری انجام داده است؟

کتاب پنج‌جلدی که با استادان داخلی کشورمان تألیف کردیم، درواقع پایه علمی است، یعنی فقط این‌طور نبوده که ترجمه کرده باشیم. به این طریق بسیاری از کتاب‌ها را تألیف کرده‌ایم. یکی از کارهای مهم این است که ما نخبگان را شناسایی می‌کنیم و از استادانی که در این حوزه کتاب تألیف می‌کنند، حمایت می‌کنیم. استادان برخی دانشگاه‌های کشور، ازجمله دانشگاه مالک اشتر، دانشگاه امام حسین(ع)، دانشگاه عالی دفاع ملی، دانشگاه فارابی و بسیاری از دانشگاه‌های دیگر که در حوزه‌های پدافند سایبری با ما همکاری دارند، در این حوزه به ما کمک شایانی می‌کنند. در این دانشگاه‌ها، دوره‌های آموزشی طولی مانند دوره دکترای مدیریت راهبردی فضای سایبری گرایش دفاع سایبری و کارشناسی ارشد دفاع سایبری ایجاد کرده‌ایم که چند دوره فارغ‌التحصیل نیز داشته‌ایم. این دانشجویان که در داخل کشور تربیت شده‌اند، کسانی هستند که در زیرساخت‌های کشور فعالیت می‌کنند و دانش بومی را آموزش دیده‌اند. استادانی که به اینها آموزش داده‌اند بی‌شک از نخبگان کشورند. قرارگاه پدافند سایبری کار بسیار شایسته‌ای که انجام می‌دهد، این است که از مقالات و تألیف‌ها و... حمایت می‌کند. ما نخبگان این حوزه را شناسایی می‌کنیم و با بسیاری از شرکت‌هایی- که در این حوزه فعالیت‌های بومی‌سازی را پیش می‌برند- همکاری و از آنها حمایت می‌کنیم. بسیاری از دوره‌های آموزشی را به آنان واگذار می‌کنیم که این شرکت‌های متخصص، دوره‌ها را اجرا کنند تا علاوه‌بر استفاده از زیرساخت‌های این شرکت‌ها از علم و دانش بالای آنها بهره ببرند، همچنین طی چندسال در یک مجله آموزشی در حوزه آموزش با دانشگاه امیرکبیر همکاری کرده‌ایم. گفتنی است که با دانشگاه شریف در دوره‌های آموزشی در تعامل و همکاری هستیم، حتی در نمایشگاه‌های پدافند سایبری که هرسال اجرا می‌شود، استادان دانشگاه و کارهایی که در این حوزه انجام دادند (شامل محصولات، دوره‌های آموزشی و تألیفات آنها) معرفی می‌شوند.

نخبگان چطور می‌توانند با سازمان پدافند ارتباط بگیرند و طرح و ایده ارائه کنند؟

یکی از کانال‌های ارتباطی، مرکز مطالعات و انجمن پدافند غیرعامل که اکثرا نخبگان کشور عضوند. ایجاد انجمن پدافند سایبری، یکی از اهداف مهم در این خصوص است که ما درحال پیگیری آن هستیم

و همچنین رئیس محترم سازمان توجه ویژه نسبت به این موضوع دارند تا ان‌شاءالله در سال آینده این موضوع به نتیجه برسد. اکنون روی این موضوع کار می‌کنیم که نخبگان کشور و کسانی که ایده‌ای دارند، بتوانند در این انجمن عضو شوند، ایده بدهند و ما هم حمایت کنیم. هرسال در هفته پدافند غیرعامل نمایشگاه‌های محصولات بومی پدافند سایبری برگزار می‌شود و همایش‌هایی ملی پدافند سایبری نیز داریم و به همه نخبگان کشور اطلاع‌رسانی می‌کنیم. در دانشگاه عالی دفاع ملی در دوره دکتری در سه گرایش به خصوص گرایش دفاع سایبری، اکثر استادان تدریس می‌کنند و مهم‌ترین بخشی هم که خدمت شما عرض کردم مرکز مطالعات سازمان پدافند غیرعامل است که همه نخبگان می‌توانند از طریق این مرکز با معاونت آموزش قرارگاه پدافند سایبری ارتباط برقرار کنند و ما نیز حمایت می‌کنیم. این همکاری می‌تواند در حوزه ایده‌پردازی یا تألیفات باشد که حمایت ما ایجاد امکانات و پشتیبانی مالی خواهد بود.

در دانشگاه‌ها در حوزه پدافند سایبری ضعف‌هایی داریم، برای جبران آن باید چه کارهایی انجام شوند و انجام شده‌اند؟

دانشگاه‌های مهمی ازجمله دانشگاه امام حسین(ع)، دانشگاه مالک اشتر و دانشگاه عالی دفاع ملی را داریم که چندسال است در این حوزه فعالیت می‌کنند، همچنین چند گرایش جدید در رشته‌های حوزه کارشناسی ارشد و دکترا داریم که درحال تدوین آنها هستیم. درواقع بخش‌هایی از برنامه‌هایشان نیز انجام شده؛ یکی از رشته‌های کارشناسی ارشد، مهندسی پدافند غیرعامل گرایش پدافند سایبری صنعتی است که درحال حاضر این رشته تدوین شده و بعد از مراحل تصویب در دانشگاه امام حسین(ع) از بین کارشناسان حوزه امنیت در زیرساخت‌های حیاتی و حساس کشور دانشجو جذب می‌کنیم. در آینده برنامه ما این است گرایش‌هایی که در دانشگاه‌های معین سازمان درحال اجرا هستند در دانشگاه‌های دیگر کشورمان هم این رشته‌ها گسترش پیدا کنند.

در دانشگاه‌های سراسری و دانشگاه آزاد می‌خواهیم یک‌سری رشته در حوزه کارشناسی ارشد پدافند سایبری ایجاد کنیم. در دانشگاه گیلان رشته کارشناسی ارشد حفاظت از زیرساخت‌های سایبری با همکاری معاونت محترم سازمان پدافند غیرعامل و قرارگاه پدافند سایبری طراحی و تدوین و مراحل تصویب هم طی شده و آماده است از بهمن‌ماه ۱۴۰۳ دانشجو پذیرش کند. امسال چند دانشگاه با ما تفاهمنامه امضا می‌کنند که بتوانیم این رشته‌ها را ایجاد کنیم. رشته‌های کارشناسی ارشد اطلاعات و عملیات سایبری و کارشناسی ارشد حقوق بین‌الملل سایبری- که رشته جدید است- را قصد داریم در دانشگاه‌های مختلف ایجاد کنیم. بعد از دوره دکترا، دکترای آینده‌پژوهی پدافند سایبری است که می‌خواهیم آن را نیز ایجاد کنیم. رشته‌های کنترل صنعتی شبکه‌های جنگ الکترونیک و رشته‌های شبکه‌های ارتباطی چندین رشته‌اند که روی آن کار می‌کنیم که ان‌شاءالله تا سال آینده در چند دانشگاه- غیر از چند دانشگاهی که نام بردم- ایجاد می‌کنیم. قصد ما این است که همه دانشجوهایی که در گرایش‌های مختلف کارشناسی را دریافت کرده‌اند، بتوانند در این رشته‌ها شرکت کنند که فقط مختص به افرادی نباشند که در حوزه‌های زیرساخت کار می‌کنند.

در ادامه به دو نمونه از فعالیت‌های حوزه فرهنگی در این حوزه اشاره می‌کنم؛

- آماده کردن ۳۰ مستند، موشن‌گرافی و فیلم‌های کوتاه در حوزه آموزش و فرهنگ‌سازی پدافند سایبری، تهیه محتوای آموزشی و ضبط آنها برای اجرای دوره پدافند سایبری و ارائه آن به وزارت آموزش‌وپرورش کشور و کمک در اجرای آن برای معلمان عزیز (به‌صورت ضمن خدمت).
- صدور گواهی‌نامه به ۱۵ شرکت خصوصی و دانشگاهی در حوزه پدافند سایبری جهت اجرای دوره‌های آموزشی تخصصی پدافند سایبری.

دکترسیدمحمود محمدی، کارشناس حوزه هوش‌مصنوعی و پدافند سایبری

هوش‌مصنوعی فرصت‌ها و تهدیدها

وارد شدن به عصر هوش‌مصنوعی منجر شده تحلیل‌ها و گزاره‌های مختلفی در مورد این فناوری پیشرفته در جهان مطرح شود. طبیعی است ورود فناوری جدید می‌تواند در پیشرفت و افزایش سرعت کار در حوزه‌های مرتبط مؤثر باشد، اما از طرفی نگرانی‌هایی هم در مورد این فناوری پیشران وجود دارد. بخشی از نگرانی، تهدیدها در حوزه امنیت سایبری است و بر این اساس باید مؤلفه‌هایی را موردتوجه قرار داد. برای بررسی فرصت‌ها و تهدیدهای هوش‌مصنوعی با دکتر سیدمحمود محمدی، کارشناس حوزه هوش‌مصنوعی و پدافند سایبری گفت‌وگو کردیم که در ادامه از نظر می‌گذرانید.

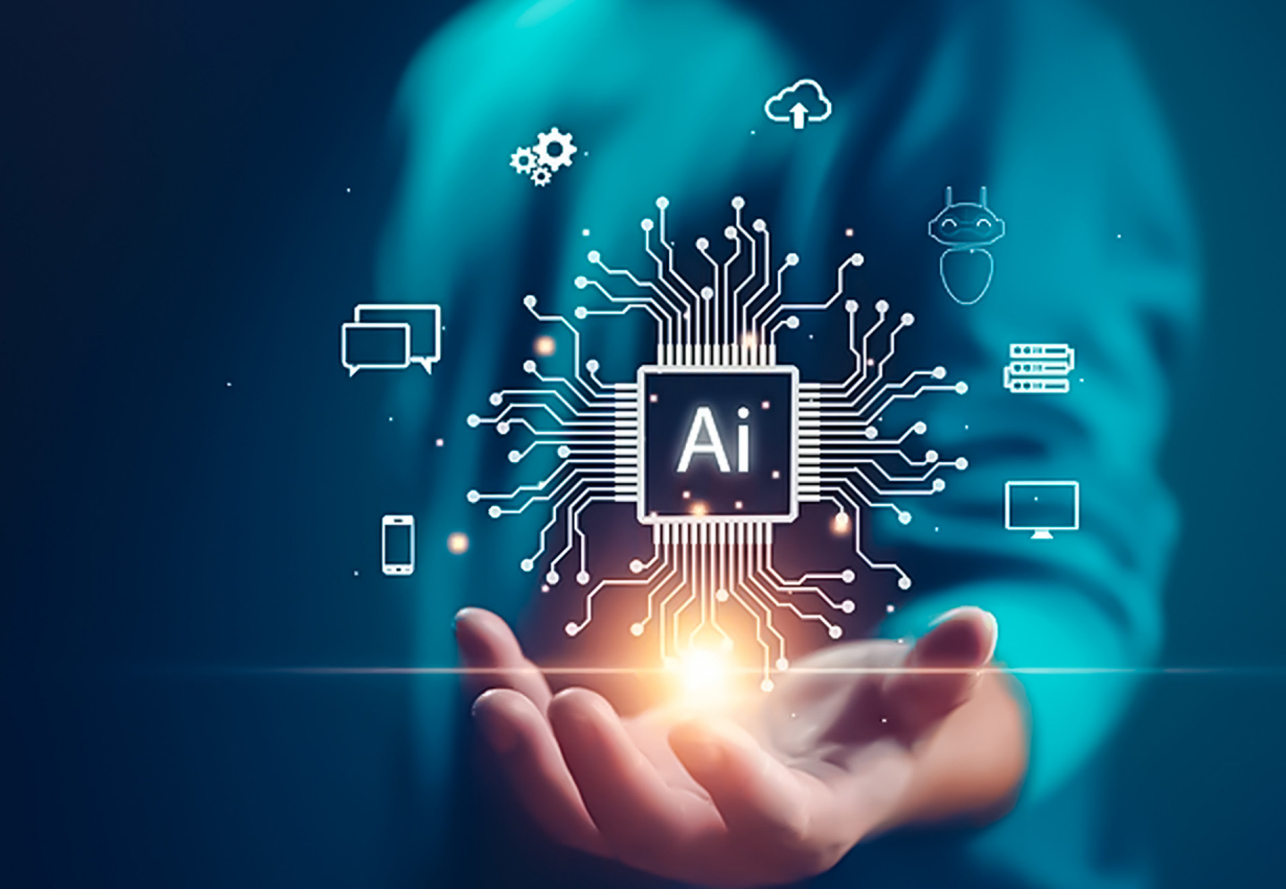
فرصت‌های فناوری‌های پیشران مثل هوش‌مصنوعی در کشور ما چیست؟

در این حوزه بحث شناسایی تهدیدهای پیشرفته را مدنظر داریم. فناوری هوش‌مصنوعی چندسالی است وارد ادبیات کشور ما شده و در صنعت و فناوری‌ها نقش ایفا می‌کند و گاهی کارهایی انجام می‌دهد که می‌توانند

تاثیرگذار باشند. یکی از این حوزه‌ها امنیت و پدافند سایبری است که درحال‌حاضر برای ما مهم، اساسی و قابل‌توجه است؛ چراکه به‌راحتی می‌توانند با این موضوع در حوزه امنیت و سایبری نفوذ کنند و چالش‌هایی را برای ما در حوزه سایبری به وجود آورند، کمااینکه برخی از اینها منجر به مختل کردن سیستم‌های زیرساختی ما می‌شود و گاهی نیز با هک و نفوذ داده‌های ما را به‌سرقت می‌برند یا از آن سوءاستفاده می‌کنند. فناوری هوش‌مصنوعی با ورود به این حوزه، فرصت‌هایی را برای ما ایجاد کرده، ازجمله بحث شناسایی تهدیدها پیشرفته، یعنی الگوهای حمله یا الگوهای غیرعادی را- که در داده‌ها و رفتار شبکه ممکن است به وجود آید- می‌توانند شناسایی کنند، چون شاید شناسایی برخی الگوها توسط انسان زمانبر باشد و گاهی زمانی اتفاق می‌افتد که حمله صورت گرفته و شاید فرصت را نتوان به‌درستی مدیریت کرد. فناوری هوش‌مصنوعی تهدیدهای پیشرفته و الگوهای غیرعادی را شناسایی می‌کند، همچنین به این الگوها در کمترین فرصت پاسخی سریع می‌دهد. موضوع بعدی در بحث فرصت‌ها تحلیل داده‌های بزرگ است. هرچه تعداد داده بیشتر و به حجم‌شان افزوده شود، قابلیت تحلیل آنها کمتر می‌شود. تنها ماشین می‌تواند الگوها را تحلیل کند، البته آن هم از الگوریتم‌های ماشین یا موضوعاتی است که از این نمونه استفاده و داده‌ها را تجزیه‌وتحلیل می‌کند و الگوها یا اطلاعات ارزشمند را در حوزه تهدیدها به‌دست می‌آورد. فناوری هوش‌مصنوعی نیز می‌تواند در کمترین زمان این کار را انجام دهد و به حوزه امنیت و پدافند سایبری کمک شایانی کند. موضوع بعدی، خودکارسازی فرایندهای امنیتی است. برای جلوگیری از نفوذ و اینکه رخدادها و اقداماتی را مدیریت کنیم که می‌تواند در حوزه امنیت سایبری اتفاق بیفتد و پاسخی به‌موقع به این حملات بدهیم، باز هم فناوری هوش‌مصنوعی به یاری‌مان می‌آید. مورد دیگر پیشگیری از این حملات است. حملاتی را که ممکن است قبلا صورت گرفته باشد و الگوهایی که شناسایی کرده‌ایم با استفاده از الگوریتم‌های یادگیری ماشین تحلیل و برای سیستم پیش‌بینی می‌کنیم. آخرین موضوع بحث مدیریت امنیت در زمان واقعی است. ما می‌توانیم براساس حداقل زمان این تهدیدها را شناسایی و مدیریت کنیم که در کوتاه‌ترین زمان بتوانیم نسبت به آن عکس‌العمل نشان دهیم.

در حوزه هوش‌مصنوعی چه تهدیدهایی باید موردتوجه قرار گیرند؟

هر فناوری قطعا فرصت‌ها و تهدیدهایی دارد؛ یکی از تهدیدهایی که برای هوش‌مصنوعی متصوریم استفاده از آن توسط مهاجمان است، اما به‌عنوان فرصت هم دشمن و هم افرادی که می‌خواهند به زیرساخت‌های ما حمله کنند و امنیت سایبری‌مان را تحت‌تأثیر قرار دهند و هم آن مهاجم، در حوزه امنیت و پدافند سایبری، می‌توانند- به‌عنوان هکر- از این فناوری استفاده کنند و ضعف‌ها و آسیب‌پذیری‌های ما را با این هوش کشف کنند و از آن نقطه به ما خسارت بزنند. همین موضوع به‌مثابه تهدید است. مورد دیگر در این بحث، ایجاد داده‌های نادرست است؛ بانفوذ و رسوخ برخی داده‌ها به داده‌های اصلی کارایی سیستم ما با اشکال مواجه می‌شود و در امنیت و پدافند سایبری ما اختلال ایجاد خواهد شد. موضوع بعدی در این حوزه، پیچیدگی و عیب‌یابی است. الگوریتم‌های هوش‌مصنوعی و یادگیری ماشین ممکن است پیچیده باشند و عیب‌یابی‌شان مشکل باشد، حتی شاید نتوانیم به‌راحتی با نیروی انسانی به آنها رسیدگی کنیم و همین پیچیدگی نوعی تهدید به‌شمار می‌آید که لازم است در ادامه ارزیابی درستی از سیستم دفاعی و پدافندی خود داشته باشیم. از موضوعاتی که به‌عنوان تهدید مطرح می‌شود، بحث حریم خصوصی است. دیتاهایی که برای آموزش استفاده می‌شوند گاهی ممکن است دیتاهای شخصی باشند که این امر می‌تواند چالش‌هایی را ایجاد کند. موضوع آخر بحث وابستگی کامل به تکنولوژی است که هرچند ممکن است برای ما فرصت باشد، در جایی دیگر می‌تواند تهدید مدنظر سیستم ما باشد و برایمان تهدید تلقی شود؛ چراکه سیستم در حوزه زیرساختی اعم از برق و



پردازش‌های بالاازجمله سی‌پی‌یو و... آسیب‌پذیر است و این نشان‌دهنده اتصال کامل به فناوری است. ما از تکنولوژی‌ها استفاده می‌کنیم، بی‌آنکه راه جایگزینی برایشان در نظر گرفته باشیم و همین امر فرصت‌ها را به تهدیدها بدل می‌کند. با این تفاصیل در حوزه امنیت و پدافند سایبری به‌صورت اجمالی و کلی اینطور نتیجه می‌گیریم که اگر این فرصت‌ها و تهدیدها به‌درستی مدیریت شوند، چنین فناوری‌ای به حوزه دفاع و امنیت سایبری ما کمک شایانی خواهد کرد.

در کشور ما راهکارهای مدیریت بحران فضای سایبری تا چه میزان به‌روز و کارآمد است؟

در حوزه مدیریت سایبری کارهای بسیاری انجام می‌شود که در مواقع بحران حوزه سایبری خود را به‌خوبی مدیریت کنیم، اما همان‌طور که بیان کردم از این فناوری جدید استفاده می‌کنیم. اگر فردی وارد مدیریت سایبری کشور شود، مزایای فراوانی برایش به‌همراه خواهد داشت، ولی چالش اساسی ما بحث نیروی انسانی است که در این حوزه به اندازه کافی نیروی متخصص و کارآمد نداریم. موضوع بعدی این است که گاهی ممکن است سیستم‌های ما انسان‌محور باشند. اگر این فناوری‌های نوظهور مثل هوش مصنوعی را در این فناوری‌های امنیت و پدافند و حملات سایبری نفوذ دهیم، می‌توان گفت به حدی از بلوغ رسیده‌ایم. هرچند هنوز جا دارد در شرایط بحرانی سیستم امنیت سایبری خوبی داشته باشیم که هیچ ضعف و ایرادی نداشته باشد.

به نظر شما چه نارسایی‌ها و نقدهای عمده‌ای بر این فضا وارد است؟

انسان‌محوری یکی از مشکلات است که باید از آن عبور و فناورمحور به این حوزه نگاه کنیم، همچنین فناوری‌های جدید و نوظهور را در این حوزه دخالت دهیم، چون می‌تواند سرعت و عکس‌العمل‌مان را برای رسیدن به نتیجه درست و مطلوب بهتر کند و سیستم‌های دفاعی‌مان را در مقابل حملات و موضوعاتی که علیه امنیت سایبری ما انجام می‌شود، محکم‌تر کند.

چند درصد از فضای مدیریت بحران به‌واسطه نیروی انسانی توسعه پیدا کرده و چه میزان وابسته به پیشرفت‌های تکنولوژی است؟

در سال‌های اخیر کارهای خوبی در این حوزه انجام شده، به خصوص از وقتی فناوری هوش مصنوعی آمده است، اما آمار دقیقی در این زمینه وجود ندارد. به نظر می‌آید نهایتا ۴۰ درصد از فناوری استفاده می‌کنیم و ۶۰ درصد هنوز بر نیروی انسانی متکی هستیم و همچنان نیروی فردی در حوزه زیرساختی و سایبری ما نقش اساسی را ایفا می‌کند. در این زمینه نمی‌گویم نقش انسان را به صفر برسانیم، بلکه اگر نقش انسان را کمتر کنیم و در حد ناظر و مدیر نگه داریم- نه به‌عنوان عامل اجرایی- بهتر خواهد بود. تکنولوژی و فناوری عامل اجرایی باشد و انسان بتواند آن را مدیریت کند. درنهایت فرد متخصص و متبحر باید خروجی بگیرد، اما باید امور اجرایی و ملزومات تحلیلی و نقاط ضعف سیستم را ماشین انجام دهد؛ چراکه دقیق‌تر، سریع‌تر و در زمان کمتری این کار را انجام می‌دهد.

در حوزه مدیریت سایبری کارهای بسیاری انجام می‌شود که در مواقع بحران حوزه سایبری خود را به‌خوبی مدیریت کنیم، اما همان‌طور که بیان کردم از این فناوری جدید استفاده می‌کنیم. اگر فردی وارد مدیریت سایبری کشور شود، مزایای فراوانی برایش به‌همراه خواهد داشت، ولی چالش اساسی ما بحث نیروی انسانی است که در این حوزه به اندازه کافی نیروی متخصص و کارآمد نداریم

دکتر محمدمهدی احمدیان، مدیرعامل شرکت دانش‌بنیان پیشگامان امن و کارشناس حوزه صنعت و پدافند

صنعت و پدافند سایبری

تقویت زیرساخت‌های صنعتی برای مقابله با امنیت سایبری، از موضوعات قابل توجه در حوزه پدافند سایبری است. تقویت آن می‌تواند تنش‌های سایبری ما را در مقابل هکرها و حملات آن بیمه کند. دکتر محمدمهدی احمدیان، مدیرعامل شرکت دانش‌بنیان پیشگامان امن و کارشناس حوزه صنعت و پدافند به چالش‌ها و موضوعات مهم در حوزه صنعت در پدافند سایبری اشاره کرده که در ادامه از نظر می‌گذرانید.

شرکت دانش‌بنیان شما چه اقداماتی را در حوزه پدافند با محوریت صنعت انجام داده است؟

دو دهه است که ما در زیرساخت‌های ویژه، حیاتی، حساس، مهم و قابل حفاظت صنایع مختلف را در کشور داریم. حوزه کاری ما شرکت امان صنعتی است، یعنی با صنایع کار داریم. آنچه درباره پدافند غیرعامل و امنیت سایبری مطرح می‌کنم با محوریت حوزه صنایع کشور است و زیرساخت‌ها را در قالب صنایع نفت، گاز، پالایش، پتروشیمی، آب و فاضلاب، برق، منابع آب، فولاد، مس، سنگ آهن، خودروسازی، داروسازی، صنایع غذایی و... پوشش می‌دهد. برخی از این صنایع

همچون صنعت برق، خود زیرشاخه‌ها و حوزه‌هایی دارد، صنعت نفت نیز همین‌طور است. در حوزه برق، تولید برق، انتقال، توزیع و... و در حوزه منابع آب نیروگاه برقابی، آب منطقه‌ای و... راداریم. اگر به هریک از اینها ورود کنیم، مسئله پدافند غیرعامل و امنیت سایبری با توجه به تهدیدها و حملات سایبری که وجود دارد، در این دو دهه مورد توجه قرار گرفته است. ممکن است برخی از مردم در کشور ما و با توجه به اتفاقاتی که اخیرا افتاده قدری بیشتر با این مسئله آشنا شده باشند. اتفاقاتی که ۲۷ و ۲۸ شهریور سال جاری در انفجارها و تجهیزات الکترونیکی در لبنان داشتیم، مسئله سایبری را پررنگ‌تر کرده‌اند. تنش‌های سایبری بعد از آن اینچنین بود ولیکن نکته این است که مسئله حملات سایبری و خرابکاری‌های صنعتی و الکترونیکی که در حوزه پدافند غیرعامل به آن پرداخته می‌شود، موضوع چندان جدیدی نیست. در فضای عمومی تقریبا از ۱۹۸۲ میلادی اولین حملات سایبری و خرابکاری صنعتی در دنیا در فضای عمومی منتشر شد. چه اتفاقی افتاد؟ دو انفجار بسیار گسترده را در خطوط گاز سیبری رخ داد. ما جرا به اینجا برمی‌گشت که در زمان جنگ سرد در شوروی (روسیه فعلی) برای مانیتورینگ و کنترل سامانه‌های خطوط لوله که از سامانه‌های قدیمی به سامانه‌های جدیدتر حرکت می‌کرد و قرار بود سامانه‌های جدیدتری به کار گرفته شود، آنها سامانه‌هایی نبودند که در روسیه وجود داشته باشد و باید از سامانه و فناوری‌ها و سازندگان غربی استفاده می‌کردند. آن زمان جنگ سرد بود و آمریکا نهایت سوءاستفاده را کرد و با اطلاع از این پروژه‌ها در خطوط گاز سیبری که حساسیت بسیار بالای ملی را داشت، یک سری بدافزار را در این سامانه‌های نرم‌افزاری وارد کرد، به این صورت که در آن فناوری‌ها و تجهیزاتی که برای سیبری ارسال می‌شد، دستکاری و خرابکاری صنعتی انجام داد؛ در حالت عادی سامانه‌ها خوب کار می‌کردند و مجموعه آنها بیش از ۱۰ میلیون بار به شکل نرمال کار خود را انجام داده بودند و مشکلی نداشتند. اما سال ۱۹۸۲ که زمان ارسال فرمان برای این انفجارها بود، دو انفجار تقریبا معادل سه هزار TNT حدود یک بمب هسته‌ای کوچک و حجم انفجارها خیلی بیشتر بود و خسارات زیادی نیز وارد کرد. الان که در سال ۲۰۲۴ هستیم، همچنان این اتفاقات وجود دارد. حالا که از شوروی و روسیه گفتم، مثالی هم از آمریکا بزنم. در آمریکا بحث‌های سایبری و پدافندی سال‌های سال وجود داشت تا اینکه در سال ۲۰۰۱، از دو منظر حادثه معروف ۱۱ سپتامبر و همچنین حملات سایبری گسترده به شبکه برق آمریکا، باعث شد نظارت امنیت داخلی آمریکا برنامه ویژه‌ای را برای پدافند و امنیت سایبری زیرساخت‌های حیاتی پیش ببرد. این مقدمه را بیان کردم تا به کشور ایران برسیم. موضوعی که در مورد حملات سایبری و انفجار پیجرها رخ داد موضوع جدیدی نیست و بیش از دو دهه است که در دنیا مطرح می‌شود. در کشور ما همه مستحضرید که از سال ۱۳۸۲ موضوع پدافند غیرعامل با تأسیس سازمان پدافند غیرعامل به دستور مقام معظم رهبری جدیت یافت. ۱۳۹۰ با توجه به حساسیت موضوع و اتفاقاتی که در ماجرای استاکس‌نت و خسارت آن در کشور داشتیم، قرارگاه سایبری در سازمان پدافند غیرعامل شکل گرفت و موضوع پدافند سایبری از اینجا در کشور با جدیت بیشتری از منظر پدافندی مورد بررسی و توجه قرار گرفت. اگر یک سال قبل را در کشور مرور کنیم، سال ۱۳۸۹ قبل از تشکیل قرارگاه سایبری خط مشی‌های کلی نظام در امور پدافند غیرعامل و ابلاغیه مقام معظم رهبری در خط مشی‌های نظام دیده شدند. در یکی از بحث‌های این خط مشی‌ها مقابله با تهدیدهای نرم‌افزاری و الکترونیکی و سایر تهدیدهای جدید دشمن به منظور حفظ و صیانت از شبکه‌های اطلاعاتی، اطلاع‌رسانی، مخابراتی و رایانه‌ای تصریح شده است. این موضوعی نیست که بگوییم جدید است.

برای تقویت پدافند و امنیت سایبری در کشور چه اقداماتی را می‌توان انجام داد؟

مقوله پدافند سایبری و امنیت سایبری یک پازل است، یعنی قطعات مختلفی دارد که اگر کنار هم قرار بگیرند تصویری که ارائه می‌شود تصویر کاملی است، اما اگر هریک از تکه‌های پازل یا این ذی‌نفعان به درستی در کنار هم قرار نگیرد، ضعف‌هایی را در کشور به وجود می‌آورند و منجر می‌شوند، مهاجمان و دشمنان بتوانند از این ضعف‌ها استفاده کنند و به تجهیزات ملی، زیرساخت‌های ویژه، حیاتی و مهم آسیب بزنند. یکی از

این موضوعات، بحث آموزش و فرهنگ‌سازی است. تقریبا دو مسئله داریم که یکی انبوهی از تهدیدها و آسیب‌پذیری‌هایی است که برای زیرساخت‌های ما در کشور متصور است و زحمات زیادی در این سال‌ها در کشور کشیده شده که بخشی از این موارد پوشش داده شود، ولی با توجه به حساسیت موضوع و اینکه ما سیبل حملات سایبری هستیم، طبیعتا بیش از پیش باید به آن توجه کنیم. از یک سو ضعف‌هایی داریم. بحث آموزش و فرهنگ‌سازی کمک می‌کند این مسائل را ارتقا دهیم. منابع و نیروهای انسانی- چه نفراتی که به شکل رسمی در زیرساخت‌ها هستند و چه به شکل پیمانی اعم از مشاوران و پیمانکاران مختلف- هریک از بازیگرانی که در بخش صنایع کشور در حوزه پروژه‌های مختلف شامل طراحی، اجرا و بهره‌برداری هستند، می‌بایست این آموزش‌ها را ببینند؛ چراکه باید بتوانیم وضعیت موجود را ارتقا دهیم. مسئله دیگری وجود دارد که آن هم بحث پروژه‌های جدید، افزایش ناامنی‌های سایبری به علت پروژه‌های تحول دیجیتال، پروژه‌های هوشمندسازی و... است. ما ناگزیریم به سمت اینها برویم. بحث تحول دیجیتال، هوشمندسازی، اینترنت اشیای صنعتی، داده‌های حجیم، فناوری‌هایی نظیر مجازی‌سازی و هوش مصنوعی و مفاهیمی که در سایبر فیزیک مطرح است، نظیر شهرهای هوشمند، خودروهای هوشمند، منازل هوشمند و تهدیدهای نوینی که به همراه دارند، مسائلی هستند که نمی‌توان از آنها فاصله گرفت. تکنولوژی تحول دیجیتال چیزی نیست که ما بخواهیم آن را کنار بگذاریم، چون از دیدگاه اقتصاد مهندسی تحول دیجیتال و هوشمندسازی شاخص‌های عملکردی و کارایی را بسیار بهبود می‌بخشد. در بخش تولید می‌بینیم که پروژه‌های مختلفی نظیر هوشمندسازی، پروژه‌های مانیتورینگ، پروژه‌های نظارت و... در حوزه صنعتی وجود دارند. در این حوزه یک هرم و مدل مرجع داریم که به آن هرم اتوماسیون صنعتی می‌گوییم. این هرم پنج سطح دارد که از سطح صفر، سطح فیزیکی شروع می‌شود، حسگرها و عملگرها، سیستم کنترل صنعتی ما در این سطح یک، سرپرستی ما در سطح دو است که اینها در کشور پیاده شده‌اند. اما نکته این است که در بحث تحول دیجیتال و هوشمندسازی دو لایه بالاتر این هرم اتوماسیون صنعتی مطرح می‌شوند که سطوح سه و چهارند، یعنی لایه برنامه‌ریزی مثل پروژه‌های NEF و سطح مدیریت مثل پروژه‌های ERP مواردی‌اند که شاخص‌های عملکردی و بهینه‌سازی را بسیار بالا می‌برند؛ تولید صنایع را افزایش و میزان هزینه‌های تعمیر و نگهداری را کاهش می‌دهند، همچنین میزان مصرف انرژی را در صنایع به شکل قابل توجه بهبود می‌بخشند. اینها باعث می‌شوند صنایع و زیرساخت‌های ویژه، حیاتی، مهم و قابل حفاظت ناگزیر به سمت تکنولوژی پیش بروند. اما اگر قبل از ورود تجهیزات و فناوری‌های جدید در بخش‌های گوناگون از جمله اینترنت اشیای صنعتی و مجازی‌سازی- چه در لایه سرپرستی سیستم‌های صنعتی و چه در لایه سیستم‌های کنترلی در شبکه‌های صنعتی- آموزش و آگاهی‌رسانی را به همان میزان افزایش ندهیم و پیش از آن ارزیابی امنیتی را انجام ندهیم، اتفاقاتی که برای پیجرها و تجهیزات الکترونیکی در لبنان افتاد، متأسفانه در کشور ما نیز رخ می‌دهند. بنابراین باید کمک کنیم، آموزش دهیم، تأمین محتوا کنیم و این مطالب را ارائه دهیم.

در حوزه آموزش پدافند سایبری چه اقداماتی لازم است انجام شود؟

آنچه می‌گویم براساس تجربه اندک ما در این مدت در شرکت پیشگامان امن به عنوان شرکت دانش‌بنیان و پیشگام در حوزه امنیت سایبری کشور است که اولین مجوز امنیتی را از سازمان پدافند غیرعامل گرفته‌ایم. بالغ بر ۱۱ هزار نفر در زیرساخت‌های مهم صنعتی کشور آموزش داده‌ایم که با بالاترین میزان سطح رضایت همراه بوده است. دوره‌های آموزشی تئوری و عملی هم داشته‌ایم. کارهایی که در کشور در تیم‌های مشابه ما انجام می‌دهند، در قالب همکاری با سازمان محترم پدافند غیرعامل است. اما علاوه بر این نیاز داریم در قالب تقویت نظام آموزشی کشور در حوزه پدافند سایبری اقداماتی را انجام دهیم. اینها مهم‌ترین بخش نظام آموزشی دانشگاه‌های ما هستند. کارهای ارزشمندی در این چند سال انجام شده و ما هم در دانشگاه صنعتی امیرکبیر در مرکز پژوهشی آفاق با همکاری با سازمان پدافند در حال برنامه‌ریزی برای افزایش دوره‌ها و ارائه دوره‌های تخصصی این حوزه‌ایم. ان شاء الله با حمایت مسئولان بتوانیم

مجوزهای لازم را بگیریم و این کار را در اسرع وقت همانطور که در شرکت دانش‌بنیان انجام می‌دادیم، در دانشگاه امیرکبیر درکنار بحث دانشگاه‌های دیگر به نحو احسن انجام دهیم. دانشگاه صنعتی امیرکبیر قطب امنیت سایبری و اطلاعاتی کشور بوده و ما نیز جزء فارغ‌التحصیلان همین حوزه‌ایم. به این نکته نیز اشاره کنم که در زمینه آموزش صحبت می‌کنیم، هریک از این آیتم‌هایی که خدمت شما توضیح می‌دهم، در اسناد سازمان پدافند دیده شده است، به‌عنوان مثال در سال ۱۳۸۹ در خط مشی‌های کلی نظام در امور پدافند غیرعامل در این سند بحث فرهنگ‌سازی و آموزش را می‌بینیم که چه به شکل تخصصی و چه در بحث عمومی مطرح شده است.

در حوزه آموزش و فرهنگ‌سازی پدافند سایبری بهترین و مفیدترین فعالیت چیست؟

ما نه‌تنها ایران- در واحد تحقیق و پژوهش شرکت پیشگامان امن- بلکه کشورهای پیشگام را هم رصد می‌کنیم؛ در برخی کشورها صرفا الگوبرداری در حوزه آموزش از مدل‌های غربی است، برای مثال یک موسسه برنامه آموزشی را برگزار می‌کند و ما همان را کپی می‌کنیم. دوره‌های دیگر از مؤسسات معتبر دیگر کپی‌برداری و در کشور ارائه می‌شوند. حتی کپی دوره‌های مطرح دنیا در کشور ایران با توجه به اینکه فرهنگ و صنایع ما متفاوتند و هستی‌شناسی کشور متفاوت است لزوما مدل خوبی برای افزایش بهره‌وری نیست. توصیه اول ما این است. کاری که در شرکت دانش‌بنیان یا مجموعه آفاق دانشگاه امیرکبیر انجام می‌دهیم، این است که دوره‌هایی را تهیه می‌کنیم که برای نمونه، ۱۱ هزار نفر در آن آموزش می‌بینند. در بسیاری از موارد تولید محتواهایی در کشور انجام داده‌ایم، یعنی چنین نبوده که استاندارد خارجی را برداریم و بگوییم این را آموزش می‌دهیم یا یک دوره خارجی را برداریم و آموزش دهیم. دوره سبز ۴۱۰ دوره‌ای است که در امنیت صنعتی بسیار برگزار می‌کنند و هیچ خروجی‌ای ندارد. برای کشور مو شرایط صنعتی‌مان دوره اثربخشی نیست. اگرچه برای ما بسیار هزینه‌بر بوده‌اند، ما این دوره‌ها را سفارشی‌سازی کرده‌ایم. در کشور ما که به آموزش بهای چندانی داده نمی‌شود- این را به‌عنوان یک دغدغه عرض می‌کنم- مخصوصا در سال‌های

تحول دیجیتال، هوشمندسازی، اینترنت اشیای صنعتی، داده‌های حجیم، فناوری‌هایی نظیر مجازی‌سازی و هوش مصنوعی و مفاهیمی که در سایبر فیزیک مطرح است، نظیر شهرهای هوشمند، خودروهای هوشمند، منازل هوشمند و تهدیدهای نوینی که به همراه دارند، مسائلی هستند که نمی‌توان از آنها فاصله گرفت. تکنولوژی تحول دیجیتال چیزی نیست که ما بخواهیم آن را کنار بگذاریم، چون از دیدگاه اقتصاد مهندسی تحول دیجیتال و هوشمندسازی شاخص‌های عملکردی و کارایی را بسیار بهبود می‌بخشد

گذشته، گاهی به‌عنوان کارشناسان این حوزه وارد صنایع می‌شویم و می‌بینیم، یک دوره امنیت صنعتی را ازنظر بودجه، صنعت یا صنایع کشور با دوره‌ای همچون ICDEL مقایسه می‌کنند. اگر ما در کشور برای این دوره‌ها دوهزار مدرس داریم، برای دوره‌های امنیت صنعتی این مدرسان انگشت شمارند. اگر انگیزه برای مدرسان یا مجموعه‌ها وجود نداشته نباشد نمی‌توانند تأمین محتوا انجام دهند و مسئله اصلی کمبود بودجه است. مدرس یا تیمی حاصل تجارب خود را در قالب یک دوره سفارشی‌سازی شده - که حتی خارج از کشور نیز نیست- تأمین محتوا می‌کند. انتظار دارد وقتی صنایع این دوره را برگزار می‌کنند قیمت دوره را با یک دوره ICDEL مقایسه کنند. یکی از معضلات ما در کشور این است که چون به آموزش خیلی بها داده نمی‌شود، هزینه‌های برگزاری آموزش کم است. درصورتی‌که اگر با هزینه‌های آموزش در کشورهای پیشرفته مقایسه کنیم، می‌بینیم مدرس و تیم‌هایی که آموزش کار می‌کنند دغدغه مالی روی مطالب ندارند و اگر مجموعه‌ای همچون ما مطالبی را تدریس می‌کند، متأسفانه خیلی از مجموعه‌های دیگر که پیشگام نیستند، صرفا بدون رعایت حق کپی‌رایت اسناد آموزشی تمایل دارند اسناد را به‌دست بیاورند و کپی-پیست کنند. بدون اینکه مالکیت معنوی مرجع خود را رعایت کنند. این یکی از مشکلاتی است که باعث می‌شود مجموعه‌ای مثل ما از جایی به بعد انگیزه برایش ایجاد نشود که محتوا تولید کند تا آموزش‌های تخصصی پیشرفته صنعتی انجام شود. بنابراین تأمین محتوا، یعنی سفارشی‌سازی محتوا، تولید محتوای بومی اثربخش و غنی از کمبودهای این حوزه نیازمند پشتوانه و حمایت مالی است. اینکه سازمان یا مجموعه‌ای حمایت کند و بودجه‌ای را تخصیص دهد تا چنین محتواهایی در کشور تولید و منتشر شوند. اگر این اتفاق نمی‌افتد باید هزینه و رقم این آموزش‌ها به‌نحوی باشد که مجموعه‌ها انگیزه پیدا کنند که برای این آموزش‌ها و انتقال تجارب وقت بگذارند. بخشی از مسئولیت اجتماعی و زکات علم در شرکت و چه مجموعه‌های دیگر این مسئله را رعایت می‌کنند، ولی به بودجه و حمایتی نیاز دارد که بتوان کارهای بهتری انجام داد.

به نظر شما در حوزه مدیریت بحران پدافند سایبری با چه چالش‌هایی مواجهیم؟

در یک دهه اخیر در صنایع و زیرساخت‌های کشور حملات متعددی را تجربه کرده‌ایم و بخشی از این حملات خساراتی را به بار آورده‌اند. نکته‌ای که در برخی از این حملات دیده‌ایم این است که متأسفانه زمانی که حمله سایبری اتفاق می‌افتد، صنعت یا سازمان سردرگم است، چون تجربه رزمایش نداشته و تجربه این را ندارد که اگر یک حمله سایبری اتفاق افتاد چه باید کار کرد؟ سندی هم تهیه نشده است. البته استاندارد داریم. در این مقوله دو سند طرح تداوم کسب‌وکار و سند طرح بازیابی از اقدامات ملی است که هر سازمان یا صنعتی الان باید این را داشته باشد. این اسناد کمک می‌کند زمانی که یک حمله اتفاق می‌افتد، مجموعه‌ها و صنعت سردرگم نشود که چه نفراتی چه وظیفه‌ای را دارند و فرمانده میدان کیست؟ چه تجهیزاتی را باید الان استفاده کنند؟ چه تیم‌هایی باید خدمات ارائه کنند؟ وقتی این موارد را نداشته باشیم، ابعاد و خسارات حمله گسترش می‌یابد. این موضوع جدیدی نیست. به نظام عملیات پدافند سایبری کشور ارجاع می‌دهم که ابلاغیه سال ۱۳۸۹ و سند قبلی است که اشاره کردم و خط مشی‌های کلی نظام در پدافند غیرعامل است. در آن نیز تصریح شده که تأکید بر تداوم فعالیت‌های ضروری، ارتقای پایداری ملی و تشکیل مدیریت بحران، مسائلی هستند که در این پازل اسناد و خط مشی تصریح شده است. اما مسئله ما این است که تکه‌های پازل کامل نیست و باعث شده در حوزه سایبری ضعف‌هایی داشته باشیم، یعنی خط مشی و نظام عملیاتی مشخص است، اما در مرحله اجرا وقتی اتفاقاتی می‌افتد صنایع و سازمان‌های ما سردرگم می‌شوند. به تعبیری با مسائل پیش‌پاافتاده‌ای در زمان بحران روبه‌رو هستند که مرا یاد این بیت شعر می‌اندازد که «هفت شهر عشق را عطار گشت، ما هنوز اندر خم یک کوچه‌ایم.» واقعیت همین است که در برخی موارد کم‌وکاستی‌هایی هست که تنظیم اسناد باعث می‌شود جلوی خسارت را بگیریم یا آن را کاهش دهیم. ما به عنوان شرکت پیشگامان امن یا دانشگاه امیرکبیر در خیلی از پروژه‌ها، مشاور صنایع حیاتی کشوریم. نکته این

است که به مدیران ارشد و مدیران عامل و روسای سازمان‌ها به‌صورت مزاح عرض می‌کنم، در برخی سازمان‌ها طرح تداوم کسب‌وکار در مقابل مهاجمان و هکرها نداریم! هکر می‌داند اگر برنامه اول را انجام دهد، جواب نداد برنامه دوم چیست. برنامه سوم چیست، یعنی دقیقا برای اجرا و گسترش حمله خود برنامه دارد. متأسفانه در صنایع کشور در خیلی از موارد این مسئله وجود ندارد.

در حوزه استاندارد و بومی‌سازی پدافند سایبری با چه چالش‌هایی مواجهیم؟

با دو مقوله و چالش مهم روبه‌روییم؛ یکی بحث بومی‌سازی و استانداردسازی پدافند سایبری به‌همراه نوآوری و خلاقیت در پدافند سایبری است. این نکته را هم تصریح کنم به‌عنوان کارشناس در ۱۰ سالی که در سازمان‌های کشور کار کرده‌ام، چه در بخش صنایع و چه در بخش دانشگاه صنعتی امیرکبیر بر این باورم که استفاده از استانداردهای بین‌المللی معتبر قطعا بسیار ارزشمند است. این استانداردها و اسنادی نظیر این، اگرچه بسیار ارزشمند است، ولی وابستگی به اسناد بین‌المللی و صرفا کپی از آنها پرریسک است، یعنی برای کشور مخاطره زیادی به‌همراه دارد. در خیلی از سازمان‌ها اسناد را کپی-پیست می‌کنند یا مشاورانی سند خارجی را برمی‌دارند و می‌خواهند در کشور همان را پیاده کنند که قطعا شدنی نیست. اگر بخواهید راهکار یا پدافند سایبری در کشور را پیش ببرید، به نحو شایسته‌ای باید بومی‌سازی شود. مدارک و اسنادی در شرکت پیشگامان امن داریم که اگر نیاز باشد می‌توانیم این مصادیق را ارائه دهیم و قابل راستی‌آزمایی است. درباره تحقیق و پژوهش به دستاوردهایی رسیده‌ایم که نشان می‌دهد این استانداردها به‌ظاهر خوب خارجی- که هم خوب است عمدی یا سهوی ضعف‌هایی دارد، یعنی همه چیز را پوشش نمی‌دهد، بنابراین خیلی از این استانداردها کف ماجراست، نه سقف آن! این امر می‌طلبد که حتما کار را جدی انجام دهیم. بخشی از این کار را در حد بضاعت اندک در شرکت انجام داده‌ایم و اسناد و متدولوژی‌هایی

> استفاده از استانداردهای بین‌المللی معتبر قطعا بسیار ارزشمند است. ولی وابستگی به اسناد بین‌المللی و صرفا کپی از آنها پرریسک است، یعنی برای کشور مخاطره زیادی به‌همراه دارد. در خیلی از سازمان‌ها اسناد را کپی-پیست می‌کنند یا مشاورانی سند خارجی را برمی‌دارند و می‌خواهند در کشور همان را پیاده کنند که قطعا شدنی نیست. اگر بخواهید راهکار یا پدافند سایبری در کشور را پیش ببرید، به نحو شایسته‌ای باید بومی‌سازی شود

را تنظیم کرده‌ایم که توانسته‌ایم از معاونت علمی و پژوهشی ریاست جمهوری نیز لوح دانش‌بنیانی بگیریم. راهکارهایی را در پیشگیری یا مقابله با حملات هدفمندی نظیر استاکس‌نت پیش‌بینی کرده‌ایم یا حملاتی که در چهار، پنج سال اخیر در صنایع معدنی و فولادی کشور اتفاق افتاد، راهکارهایی است که در بخش طراحی ایده‌ها پیاده کرده‌ایم و طرح ما آماده شده است. طرح در قالب شرکت دانش‌بنیان و دانشگاه امیرکبیر بوده که توانسته دستاوردهای ملی داشته باشد. دعوتنامه‌های بین‌المللی را جهت ارائه طرح داشته‌ایم و دعوت شده‌ایم و برخی را هم ارائه داده‌ایم. از دو جشنواره نیز در دو وزارتخانه کشور رتبه اول را در این بخش کسب کرده‌ایم. سال گذشته به لطف خدا در کل گروه فنی مهندسی در کشور در رساله‌ای با همین موضوع توانستیم رتبه اول را کسب کنیم. نوآوری و خلاقیت‌هایی وجود داشته که اینها در مرحله طرح تأییدیه‌های لازم را گرفته و رتبه‌های برتر را کسب کرده‌اند، ولی یک طرح از زمانی که وقت گذاشته می‌شود و تیم‌های مختلف روی آن کار می‌کنند و تست‌های اولیه را انجام می‌دهند تا بخواهد وارد اجرا شود، تغییرات عمده‌ای می‌یابد، به‌عنوان‌مثال همین طرحی که عرض کردم می‌تواند حملات سایبری هدفمند را به چالش بکشد، اما این‌گونه طرح‌ها حتی بعد از اینکه تأییدیه‌ها را می‌گیرند و به این مراحل می‌رسند بدون حمایت دستگاه‌های ذی‌صلاح، صنایع و تحقیق یک‌سری بودجه‌هایی که در مرحله طراحی یا در قالب تیم فنی تخصصی اجرا و تبدیل به محصول یا تبدیل به یک‌سری خدمات ارزشمند در کشور شوند، با مشکلاتی همراهند، چون پشتوانه نیست، حمایت ملی هم نیاز دارند تا تأمین اعتبار انجام شود و بعد بتوانیم طرح‌هایی که تأییدیه لازم را گرفته‌اند و طرح‌هایی را در بخش نوآوری و خلاقیت ارائه دهیم که دعوتنامه‌های بین‌المللی را برای آن داریم، یعنی خارج از کشور مجموعه‌ای است که علاقه‌مندند این موارد در اختیار آنها قرار گیرد، ولی اولویت ما کشور ایران است و تمام تلاش‌مان در شرکت دانش‌بنیان این است که این مطالب و دستاوردها را در اختیار کشور خودمان قرار دهیم.

راهکارهایی را در پیشگیری یا مقابله با حملات هدفمندی نظیر استاکس‌نت پیش‌بینی کرده‌ایم یا حملاتی که در چهار، پنج سال اخیر در صنایع معدنی و فولادی کشور اتفاق افتاد، راهکارهایی است که در بخش طراحی ایده‌ها پیاده کرده‌ایم و طرح ما آماده شده است. طرح در قالب شرکت دانش‌بنیان و دانشگاه امیرکبیر بوده که توانسته دستاوردهای ملی داشته باشد. دعوتنامه‌های بین‌المللی را جهت ارائه طرح داشته‌ایم و دعوت شده‌ایم و برخی را هم ارائه داده‌ایم. از دو جشنواره نیز در دو وزارتخانه کشور رتبه اول را در این بخش کسب کرده‌ایم. سال گذشته به لطف خدا در کل گروه فنی مهندسی در کشور در رساله‌ای با همین موضوع توانستیم رتبه اول را کسب کنیم. نوآوری و خلاقیت‌هایی وجود داشته که اینها در مرحله طرح تأییدیه‌های لازم را گرفته و رتبه‌های برتر را کسب کرده‌اند

در حوزه مشارکت بخش‌های دولتی و غیردولتی در بخش‌های دانش‌بنیان با چه چالش‌هایی روبه‌روییم؟

این را به‌عنوان مدیرعامل شرکت دانش‌بنیان بیان می‌کنم که در سال ۱۴۰۳ مزین به نام جهش تولید و مشارکت مردمی شده است. می‌طلبد مردم بیشتر مشارکت کنند. بخشی از این مردم شرکت‌های خصوصی دانش‌بنیان نظیر شرکت ما هستند، قطعا نهادهای مختلف حمایت‌های ارزشمندی کرده‌اند، شکی در این نیست. در خیلی از موضوعات اولین شرکت در کشور در حوزه کاری خود بوده‌ایم. طبیعتا بخشی از ظرفیت ما این بوده که از ظرفیت معاونت علمی استفاده و نیروهایی را جذب کنیم و به کمک آنها- که نیروهای نخبه و برتر دانشگاه‌های کشورند- خدمات را به صنایع کشور ارائه دهیم که بسیار نیاز است. نیروی انسانی تربیت کنیم، یعنی نخبگان در قالب نیروی نخبه وظیفه که درحال سپری دوره سربازی خود هستند، تربیت شوند تا به زیرساخت‌های حیاتی کشور خدمات ارائه دهند. متأسفانه در برخی سازمان‌های ذی‌ربط در فرایند جذب نیروهای نخبه کم‌لطفی می‌بینیم؛ وظیفه ما به‌عنوان شرکت دانش‌بنیان اول این است که باید وقت بگذاریم، بازاریابی کنیم، جلساتی با دانشگاه‌ها و نخبگان کشور برگزار کنیم تا بتوانیم این افراد را به‌سمت امنیت سایبری صنعتی جذب کنیم. این کار را امان انجام داده است. با مشقت بسیار این افراد را شناسایی می‌کنیم و به شرکت می‌آوریم که می‌خواهیم برای شما پروژه نخبه وظیفه اجرا کنیم، یعنی سربازی خود را در شرکت دانش‌بنیان می‌گذرانید. بعد از اینکه دوره سخت شناسایی نفرات را گذراندیم و این افراد را جذب کردیم باید به یک‌سری دستگاه‌های ذی‌صلاح معرفی شوند که فرایند معرفی آنها به سازمان نظام‌وظیفه اتفاق بیفتد و پروژه و طرح‌شان در شرکت امان تعریف شود. کم‌لطفی‌ای که متأسفانه دیدیم این است که به‌عنوان شرکت دانش‌بنیان وقت می‌گذاریم و نفرات را شناسایی می‌کنیم و به آنها انگیزه می‌دهیم و بعد معرفی می‌کنیم. دستگاه ذی‌صلاح وقتی جلسه خصوصی با نفرات می‌گذارد آنها را از شرکت‌های خصوصی می‌گیرد و می‌گوید در فلان شرکت دولتی بروید یا به بخش نظامی یا فلان شرکت‌هایی که ارتباط بیشتری با آن دستگاه دارند، بروید. کم‌لطفی‌ای که بارها در یکی، دو سال اخیر در شرکت دیدیم و به‌عنوان دغدغه ملی مطرح می‌شود این است. اگر در سال جهش تولید با مشارکت مردمی می‌خواهیم شرکت‌های دانش‌بنیان بتوانند از این ظرفیت استفاده کنند، این کم‌لطفی است که یک شرکت نیروی نخبه خود را معرفی می‌کند و اینجا رقابت دستگاهی می‌شود که به آن اعتماد و نیروی خود را به آن معرفی کرده‌ایم و به برخی شرکت‌های دیگر- که حتی رقیب ما هستند- معرفی می‌کنند. شرکت‌های خصولتی که رانت دولتی دارند. این نخبگان را به این مجموعه‌ها معرفی می‌کنند و این به ما ضربه می‌زند. مجموعه‌های دولتی چون چابکی لازم را ندارند، این افراد پرت می‌شوند، یعنی ما خروجی‌هایی را دیده‌ایم که نیرو می‌توانست در بخش خصوصی تربیت شود و به کشور خدمت کند، آن هم در همین حوزه که نیاز جدی است- یعنی پدافند سایبری صنعتی- اما وارد حوزه دیگری می‌شود و تربیت نیروی انسانی از بین می‌رود و در این حوزه دو سال با مشکل روبه‌رو هستیم.

نقش فرصت‌ها و تهدیدهای فناوری پیشران مثل هوش مصنوعی در این حوزه چیست؟

تکنولوژی و فناوری و هوشمندسازی که یکی از آنها هوش مصنوعی است، شمشیر دولبه‌اند، به این معنی که اگر به‌نحو دقیق و درست از اینها استفاده کنیم و قبل از ورود تکنولوژی فرهنگ‌سازی و آموزش را انجام دهیم. استانداردها را تدوین و تیم‌های اجرایی را تربیت کنیم و این مسیر را پیش ببریم، اینها تبدیل به فرصت می‌شوند. اگر خوب استفاده نکنیم قطعا تبدیل به تهدید می‌شوند. در بحث هوش مصنوعی مؤلفه‌ها و الگوریتم‌ها و روش‌های مختلفی در بحث ماشین و شبکه‌های یادگیری داریم که معمولا در حوزه امنیت سایبری در بخش تصمیم‌گیری وقتی اتفاقی می‌افتد، رویداد جمع‌آوری می‌شود که با حجم داده‌های عظیم روبه‌رو هستیم، طبیعتا از این تکنیک‌ها استفاده می‌کنیم که تکنیک‌های مختلف هوش مصنوعی است، مثل یادگیری عمیق، برای اینکه بتوانیم در سریع‌ترین زمان تصمیم‌گیری را انجام دهیم و پاسخگویی سریع و خودکاری را نسبت به آن حادثه داشته باشیم. یکی از کاربردهای هوش مصنوعی این است که در امنیت سایبری و

پدافند سایبری استفاده شود. حوزه دیگر دسته‌بندی اطلاعات است. ما با حجم عظیمی از اطلاعات در زیرساخت‌ها روبه‌رو هستیم که قطعا بدون استفاده از تکنیک‌های هوش مصنوعی و منابعی که بتواند تکنیک‌های هوش مصنوعی را پیاده کند دسته‌بندی اطلاعات رخداد تا قبل از اینکه حمله‌ای اتفاق افتد یا بعد از آن برای مواجهه با گسترش حمله و پاسخگویی به حمله نیاز اساسی است. این فرصتی است که می‌توان از این تکنولوژی استفاده کرد. نکته منفی ماجرا کجاست؟ این است که مهاجمان نیز از این تکنیک‌ها استفاده می‌کنند. به‌تعبیری با افزایش تکنیک‌های هوش مصنوعی و به‌کارگیری آن توسط گروه‌های حملات سایبری که پشت آن دولت‌ها هستند، مانند حملاتی که در این سه، چهارسال در حوزه نفت و گاز و معادن و پخش فرآورده‌های نفتی اتفاق افتاد، با افزایش تعداد حملات، افزایش پیچیدگی و عمق حملات روبه‌رو می‌شویم. براساس اطلاعات موثق بیان می‌کنم، بدافزارهایی که به یک زیرساخت حمله می‌کنند به شکل عمومی نوشته می‌شوند و به ساختار آسیب می‌زنند، تیم امنیتی در عرض ۲۰ دقیقه تا ۱۰ ساعت می‌تواند آن بدافزار را تحلیل کند و درباره‌اش راهکار ارائه دهند. اما تحلیل حمله‌ای همچون استاکس نت که سال ۱۳۸۸ تا ۱۳۹۰ در کشور آسیب زد، برای تیم‌های امنیتی حدود سه ماه طول کشید که نشان می‌دهد طراحی یک بدافزار مثل آن، حتما چندین سال طول کشیده است. این زمانی بود که تکنولوژی‌های هوش مصنوعی فراگیر نشده بود. با افزایش تکنیک‌ها و به‌کارگیری آنها طراحی و پیاده‌سازی و گسترش این حملات چندین برابر تسریع می‌شود. پیچیدگی آن بالاتر می‌رود و عمق حملات بیشتر می‌شود. همچنین اگر نتوانیم از این تهدیدها که هکرها در بخش تهاجمی استفاده می‌کنند، در بخش دفاعی و پدافندی استفاده کنیم، طبیعتا به شدت تحت آسیب خواهیم بود؛ چراکه مهاجم ابزاری دارد که مدافع ندارد و این نبردی می‌شود که باید قبل از اینکه مهاجمان استفاده بیشتری از این ابزارها کنند- که همین الان هم استفاده می‌کنند- به این سمت برویم و از تکنولوژی‌هایی نظیر هوش مصنوعی در دو بخش تصمیم‌گیری و پاسخگویی سریع و خودکار و همچنین دسته‌بندی اطلاعات زیرساخت‌های صنعتی و سازمانی، با هدف پدافند غیرعامل سایبری استفاده کنیم.

با افزایش تکنیک‌ها و به‌کارگیری آنها طراحی و پیاده‌سازی و گسترش این حملات چندین برابر تسریع می‌شود. پیچیدگی آن بالاتر می‌رود و عمق حملات بیشتر می‌شود. همچنین اگر نتوانیم از این تهدیدها که هکرها در بخش تهاجمی استفاده می‌کنند، در بخش دفاعی و پدافندی استفاده کنیم، طبیعتا به شدت تحت آسیب خواهیم بود؛ چراکه مهاجم ابزاری دارد که مدافع ندارد و این نبردی می‌شود که باید قبل از اینکه مهاجمان استفاده بیشتری از این ابزارها کنند- که همین الان هم استفاده می‌کنند- به این سمت برویم و از تکنولوژی‌هایی نظیر هوش مصنوعی در دو بخش تصمیم‌گیری و پاسخگویی سریع و خودکار و همچنین دسته‌بندی اطلاعات زیرساخت‌های صنعتی و سازمانی، با هدف پدافند غیرعامل سایبری استفاده کنیم

دکتر داود ادیب، رئیس کانون هماهنگی فاوا

امنیت سایبری در گرو زیرساخت بومی

زندگی در عصر تکنولوژی الزامات خود را دارد. آنچه در این فضا اهمیتی دوچندان پیدا می‌کند، تقویت امنیت سایبری است؛ چراکه دشمن با استفاده از این فضا هم به‌راحتی به اطلاعات و اسناد محرمانه کشور دسترسی پیدا می‌کند، هم افکار عمومی جامعه را هدایت می‌کند. به این منظور، تقویت زیرساخت‌های سایبری بیش از گذشته اهمیت دارد، اما سؤال این است که الزامات تقویت امنیت سایبری چیست؟ برای پاسخ به این سؤال با دکتر داود ادیب، رئیس کانون هماهنگی فاوا گفت‌وگو کردیم که در ادامه از نظر می‌گذرانید.

به نظر شما اهمیت راهبردی پدافند سایبری برای امنیت ملی ایران و معرفی اهداف کلان و راهبردهای این حوزه چیست؟

پدافند در تعریف کلی مجموعه‌ای از اقدامات جامع و هماهنگ، شامل دفع، خنثی کردن و کاهش تأثیر اقدام‌های تهاجمی دشمن و جلوگیری از دستیابی بیگانگان به برنامه‌ها و هدف‌هایش است که مشتمل بر دو بخش پدافند عامل و غیرعامل است. اهمیت و

اهداف راهبردی کلان پدافند غیرعامل حفظ سرمایه ملی، کاهش آسیب‌پذیری، افزایش آستانه مقاومت مردم، حفظ تمامیت ارضی امنیت ملی و استقلال کشور، افزایش قابلیت سامانه‌های شناسایی، تقویت نیروی بازدارندگی و صرفه‌جویی منطقی و همه‌جانبه در هزینه‌های تسلیحاتی و نیروی انسانی است. پدافند سایبری را به‌عنوان یکی از ارکان اصلی پدافند غیرعامل می‌توان مجموعه‌ای از اقدامات غیرنظامی، فنی و مدیریتی دانست که برای مقابله با تهدیدهای سایبری در مراکز مهم، حساس و حیاتی کشور به کار گرفته می‌شود تا ضمن جلوگیری از به‌سرقت رفتن اطلاعات حساس و محرمانه کشور موجب تأمین امنیت سایبری زیرساخت‌ها، شبکه‌های الکترونیکی و سامانه‌های داخلی و سازمانی شود که برای خدمات‌رسانی به مردم و درنهایت حفظ تاب‌آوری و پایداری تشکیل شده است.

بررسی ساختارها و الزامات نظام جامع بومی پدافند سایبری مطابق با راهبردهای سند، از طراحی تا پیاده‌سازی و نظارت را چطور ارزیابی می‌کنید و تا نقطه مطلوب چقدر فاصله داریم؟

سند راهبردی پدافند سایبری کشور براساس چشم‌انداز جمهوری اسلامی ایران در افق ۱۴۰۴ که بیان می‌کند جامعه ایرانی در افق چشم‌انداز ۱۴۰۴ «با قدرت بازدارندگی مؤثر دربرابر تهدیدهای سایبری دشمن مبتنی‌بر نظام پدافند سایبری هوشمندانه، انحصاری، ابتکاری، عمیق، لایه‌به‌لایه، بومی و پیشگیرانه، شبکه‌ای گسترش یافته و سلسله مراتبی، چابک و منعطف، نظام دفاع حقوقی و قانونی جامع ملی در حوزه پدافند سایبری، دانش و فناوری و صنعت پیشرفته بومی، منابع انسانی نخبه، خبره، توانمند، متعهد و مبتکر، فرماندهی و کنترل جامع، مقتدر و هوشمند، دارای جایگاه ممتاز جهانی در پدافند سایبری» خواهد بود، پایه‌گذاری شده است و به‌نظر می‌رسد سندی کامل و تقریبا بدون نقص باشد ولیکن این یک واقعیت است که ماهیت فضای سایبری موضوعی مرکب و

طبیعتا برخی اقدامات و فعالیت‌های پیشگیرانه می‌تواند از وقوع تهدیدها و حملات سایبری جلوگیری کند. به این صورت که با تمرکز بر آسیب‌پذیری در بخش‌های مختلف یک شبکه یا زنجیره‌ای از ارتباطات و علی‌الخصوص سامانه‌های زیرساختی وارتباطی اقداماتی را می‌توان انجام داد که در صورت حملات سایبری تلفات را به حداقل رساند. امروزه اصلی‌ترین فعالیت‌های واحدهای امنیتی در سازمان‌ها بر روش‌های پیشگیری و کاهش میزان آسیب‌پذیری متمرکزند

پیچیده است. یکی از این موارد «گسترده بودن» آن است، یعنی اینکه به همان میزان که فضای مجازی گسترده است تهدیدهای آن نیز گسترده است. موضوع بعدی «متنوع بودن» تهدیدهای سایبری است و این امر به این دلیل است که به جهت گسترده بودن جوامع در فضای مجازی، مدل‌های مختلف تهدید در این فضای پهناور به‌وجود آمده و سازمان‌های مستقل با هکرهای مختلف انواع مجزایی از تهدیدها را تحمیل می‌کنند. موضوع دیگر «نهفته بودن» تهدیدهاست، به این صورت که غالبا تهدید بالقوه، ویژگی ذاتی فضای سایبری است، لذا به‌راحتی نمی‌توان آن را به‌طور کامل کشف و نمایان کرد. این تهدیدها گاهی در زمان تولید یا عبور کالاها از زنجیره تأمین در آنها تعبیه می‌شوند. در روزهای اخیر نمونه‌هایی از این اقدام‌ها را در تجهیزات الکترونیکی و ارتباطی مشاهده بوده‌ایم. به همین منظور این استنباط وجود دارد که نقطه مطلوب هیچ‌گاه در پدافند سایبری وجود ندارد و به نظر می‌رسد خوش‌خیالی و اطمینان از نقطه مطلوب ممکن است تبعات جبران‌ناپذیری را به وجود آورد.

چالش‌ها و فرصت‌های مصون‌سازی زیرساخت‌های حیاتی سایبری کشور با تأکید بر پیشگیری از تهدیدها و ایجاد بازدارندگی را چطور ارزیابی می‌کنید؟

طبیعتا برخی اقدامات و فعالیت‌های پیشگیرانه می‌تواند از وقوع تهدیدها و حملات سایبری جلوگیری کند. به این صورت که با تمرکز بر آسیب‌پذیری در بخش‌های مختلف یک شبکه یا زنجیره‌ای از ارتباطات و علی‌الخصوص سامانه‌های زیرساختی و ارتباطی اقداماتی را می‌توان انجام داد که در صورت حملات سایبری تلفات را به‌حداقل رساند. امروزه اصلی‌ترین فعالیت‌های واحدهای امنیتی در سازمان‌ها بر روش‌های پیشگیری و کاهش میزان آسیب‌پذیری متمرکزند. علت این موضوع آن است که اساسا تمرکز روی قبل از وقوع حمله و حادثه می‌تواند موجب کاهش

صدمات شود و تجربه نشان داده معمولا هزینه‌های پیشگیری بسیار کمتر از هزینه رفع آسیب‌های عمده و کلان است.

فناوری‌های بومی‌شده در حوزه پدافند سایبری و نقش آنها در مقاوم‌سازی و خوداتکایی زیرساخت‌های کشور چیست ؟

یکی از موضوعات پیشگیرانه در پدافند سایبری استفاده از تجهیزات زیرساختی بومی و عدم استفاده از تجهیزات خارجی و نامطمئن در شبکه‌های زیرساختی مهم، حساس و حیاتی کشور است. اتفاقات روزهای اخیر در حمله سایبری به دستگاه‌های مخابراتی و ارتباطی در کشور لبنان نشانگر این موضوع است که وابستگی به کشورهای بیگانه در حوزه تجهیزات زیرساختی و علی‌الخصوص ارتباطی به چه میزان می‌تواند آسیب‌پذیری را افزایش دهد. در همین راستا می‌توان ادعا کرد کشورهایی که دارای شبکه‌های زیرساختی بومی‌اند، نفوذ بسیار کمتری را در حملات سایبری دارند و این کشورها دارای قدرت مقابله به‌مثل قوی‌تری نیز هستند.

ابزارها و تکنیک‌های مورداستفاده در رصد، پایش و مدیریت تهدیدهای سایبری، مطابق با راهبردهای تعیین‌شده در سند تا چه حد موفق بوده‌اند و چه مواهب و چالش‌هایی داشته‌اند؟

این که ابزارها و تکنیک‌های مورداستفاده در رصد، پایش و مدیریت تهدیدهای سایبری، مطابق با راهبردهای تعیین‌شده در سند تا چه حد موفق بوده، نیازمند آمار مراجع ذی‌صلاح مرتبطند ولیکن درکنار این موضوع به‌نظر می‌رسد امروزه با رشد فناوری‌های نوین باید از ابزارها و تکنیک‌های رصد، پیشگیری و پایش توسعه‌یافته با هوش‌مصنوعی در این زمینه استفاده کرد. ابزارهای پیشگیرانه مبتنی‌بر هوش‌مصنوعی قادرند با سرعت و دقت بالا، داده‌های

بزرگ و پیچیده را تجزیه‌وتحلیل و تفسیر کنند. استفاده از ابزارهای پیشگیرانه هوش‌مصنوعی در سیستم‌های امنیتی امکان شناسایی سریع‌تر الگوهای مشکوک را مقدور می‌کنند و از وقوع حملات سایبری جلوگیری به‌عمل می‌آورند. به‌عبارتی استفاده از رویکردهای هوش‌مصنوعی در امنیت سایبری، بهره‌وری بیشتر و افزایش کارایی در مقابله با تهدیدها و درکنار اینها، کاهش زمان پاسخ به تهدیدها، به‌روزرسانی دائمی الگوریتم‌ها، تعیین سطح و اولویت‌بندی حملات، کاهش خطاهای انسانی را به‌همراه می‌آورد.

راهبردهای دیپلماسی سایبری و نحوه تعامل با دیگر کشورها در زمینه امنیت سایبری و پدافند غیرعامل چیست و چطور پیش می‌رود؟

اصولا مقابله با حملات سایبری نیازمند راهبرد عملیاتی منسجم در سطح جهانی است و همان‌طور که در حوزه پلیس، امروزه نقش پلیس اینترپل در برخی مواقع اثربخشی مناسب خود را نشان داده، لزوم پلیس سایبری بین‌المللی- البته با رهبری بی‌طرفانه و بدون جهت‌گیری خاص- می‌تواند مورد اعتماد جامعه جهانی باشد. همچنین در این راستا عضویت، همکاری و حضور فعال در مجامع بین‌المللی رسمی حوزه فاوا و ایجاد سازوکارهای قانونی و حقوقی بین‌المللی لازم جهت پیگیری در صورت تعرض به زیرساخت‌های کشورها، امری است که در برنامه‌های راهبردی دیپلماسی سایبری و نحوه تعامل با دیگر کشورها، می‌تواند موردتوجه قرار گیرد.

اصولا مقابله با حملات سایبری نیازمند راهبرد عملیاتی منسجم در سطح جهانی است و همان‌طور که در حوزه پلیس، امروزه نقش پلیس اینترپل در برخی مواقع اثربخشی مناسب خود را نشان داده، لزوم پلیس سایبری بین‌المللی- البته با رهبری بی‌طرفانه و بدون جهت‌گیری خاص- می‌تواند مورد اعتماد جامعه جهانی باشد

راهکارها و برنامه‌های آموزشی برای نهادینه‌سازی فرهنگ پدافند سایبری در بین عموم مردم و نخبگان، به‌ویژه در نظام آموزشی کشور بروز و ظهور دارد. آیا ارزیابی‌ای هم نسبت به آنها وجود دارد؟

در سال‌های اخیر برنامه‌های اطلاع‌رسانی و آگاهی‌بخشی قابل‌توجهی- چه از طریق نظام آموزشی کشور و چه از طریق رسانه‌ها- صورت پذیرفته و

طبیعتا پیشرفت خوبی را در فرهنگ‌سازی در این حوزه داشته‌ایم. در این راستا پیشنهاد می‌شود به جهت اهمیت موضوع امنیت، نهادینه‌سازی فرهنگ پدافند سایبری از سطح دبستان شروع شود. همچنین تدوین واحدهای درسی مرتبط با موضوعات امنیتی در دوره‌های ابتدایی و سطوح دبیرستانی ضروری است و اجرای برنامه ارتقای سطح دانش امنیت و مهارت‌های عمومی در به‌کارگیری امن فناوری‌های نوین ارتباطی و اطلاعاتی و ارتقای دانش و سواد رسانه‌ای نیز همراستا با این رویکرد در صنایع مختلف و سازمان‌ها، نکاتی هستند که می‌بایست به آنها توجه ویژه کرد.

ازنظر شما اهمیت سرمایه‌های انسانی و روش‌های مدیریت بحران در مواجهه با تهدیدهای سایبری چیست و سازمان در این زمینه چه وضعیتی دارد؟

اگر در دنیای امروز در خصوص پیشگیری و بازدارندگی صحبت می‌کنیم و می‌خواهیم در این خصوص برنامه‌ریزی کنیم، می‌بایست همه مؤلفه‌ها را درنظر بگیریم و اقدامات موزون و پایدار را در برنامه‌های مرتبط با پیاده‌سازی سیاست‌های امنیت سایبری و ازجمله سرمایه‌های اجتماعی را مدنظر قرار دهیم. امروز امنیت موضوعی تک‌ساحتی نیست و مؤلفه‌های فراوانی دارد.

در جنگ ایران و عراق شاهد بودیم که علی‌رغم برتری نظامی و اقتصادی طرف مقابل به‌واسطه کمک‌های کشورهای مختلف اتفاقی غیرمعمول صورت پذیرفت. در آن زمان افزایش کارکرد روحیه جمع‌گرایی و نفی روحیه فردگرایی در جامعه ما، ضمن آنکه شکل جدیدی از روابط اجتماعی را به وجود آورد، شکاف‌های قومی و مذهبی را در آن دهه کمتر کرد و با تقویت سرمایه اجتماعی، عزم ملی را برای مقاومتی بزرگ به‌وجود آورد. این موضوع در کشور اثبات شده و می‌تواند اهمیت سرمایه‌های انسانی و روش‌های مدیریت بحران در مواجهه با تهدیدهای سایبری را در دورانی که در آن به سر می‌بریم، حتی در موضوعات غیرنظامی تبیین کند.

در جنگ ایران و عراق شاهد بودیم که علی‌رغم برتری نظامی و اقتصادی طرف مقابل به‌واسطه کمک‌های کشورهای مختلف اتفاقی غیرمعمول صورت پذیرفت. در آن زمان افزایش کارکرد روحیه جمع‌گرایی و نفی روحیه فردگرایی در جامعه ما، ضمن آنکه شکل جدیدی از روابط اجتماعی را به وجود آورد، شکاف‌های قومی و مذهبی را در آن دهه کمتر کرد و با تقویت سرمایه اجتماعی، عزم ملی را برای مقاومتی بزرگ به‌وجود آورد. این موضوع در کشور اثبات شده و می‌تواند اهمیت سرمایه‌های انسانی و روش‌های مدیریت بحران در مواجهه با تهدیدهای سایبری را در دورانی که در آن به سر می‌بریم، حتی در موضوعات غیرنظامی تبیین کند

سیناشادمان
مشاورسازمان صنایع کوچک

برای مدیریت بحران ابتدا باید تهدیدهای بالقوه داخلی و خارجی را شناسایی کرد

در حوزه امنیت سایبری یکی از موضوعات اصلی، تقویت زیرساخت‌های صنعتی و تجاری برای در امان ماندن از حملات احتمالی هکرهاست. طبیعی است که تقویت این زیرساخت‌ها الزامات و بایسته‌هایی دارد که در طول این سال‌ها برخی از آنها محقق شده‌اند، اما همچنان نیاز به تقویت این زیرساخت‌ها برای افزایش امنیت سایبری احساس می‌شود. سینا شادمان، مشاور سازمان صنایع کوچک در گفت‌وگویی که با ما داشته الزامات و بایسته‌های امنیت سایبری را بررسی کرده که در ادامه ازنظر می‌گذرانید.

از نظر شما اهمیت راهبردی پدافند سایبری برای امنیت ملی ایران و معرفی اهداف کلان و راهبردهای این حوزه چیست؟

پدافند سایبری در حوزه تجارت و صنعت برای امنیت ملی ایران از اهمیت راهبردی بالایی برخوردار است. با توجه به جهانی شدن اقتصاد و دیجیتالی شدن بسیاری از زیرساخت‌های تجاری و صنعتی، هرگونه حمله سایبری می‌تواند به اختلالات عمده‌ای در عملکرد اقتصادی و تولیدی کشور منجر شود. در این زمینه پدافند سایبری نه تنها به حفظ

یکپارچگی و امنیت سیستم‌های اطلاعاتی کمک می‌کند، بلکه در حفاظت از دارایی‌های ملی، ایجاد ثبات اقتصادی و حفظ امنیت اجتماعی نیز نقش کلیدی ایفا می‌کند.

حفاظت از زیرساخت‌های حیاتی، تضمین تداوم فعالیت‌های اقتصادی و تجاری، حفاظت از اطلاعات و دارایی‌های استراتژیک، حفظ اعتماد عمومی و پایداری اجتماعی اهمیت راهبردی پدافند سایبری در حوزه تجارت و صنعت است. در این راستا تدوین قوانین و مقررات محکم برای حفاظت از سیستم‌های سایبری و الزام شرکت‌ها و نهادهای صنعتی به رعایت استانداردهای امنیتی از راهبردهای کلان است. دولت می‌تواند با ایجاد چهارچوب‌های قانونی مشخص، صنایع را ملزم به رعایت تدابیر امنیتی کند، همچنین استفاده از فناوری‌های پیشرفته مانند هوش مصنوعی و ماشین لرنینگ برای شناسایی الگوهای حمله و مقابله با آنها و نیز شبیه‌سازی‌های دوره‌ای برای تست آمادگی سازمان‌ها در برابر تهدیدهای سایبری از راهبردهای بسیار مهم در پدافند سایبری حوزه تجارت است.

چالش‌ها و فرصت‌های مصون‌سازی زیرساخت‌های حیاتی سایبری کشور، با تأکید بر پیشگیری از تهدیدها و ایجاد بازدارندگی را چطور ارزیابی می‌کنید؟

مصون‌سازی زیرساخت‌های حیاتی سایبری در حوزه تجارت و صنعت کشور، با توجه به پیچیدگی‌های فناوری، تعدد سازمان‌های متولی و وجود سامانه‌های بی‌شمار تجاری، کمبود نیروی متخصص و افزایش تهدیدهای سایبری از مهم‌ترین چالش‌های پیش‌روی کشور است. از این رو توسعه فناوری‌های بومی توسط شرکت‌های خصوصی در حوزه‌های کلیدی مانند رمزنگاری، هوش مصنوعی برای شناسایی تهدیدها و نرم‌افزارهای مدیریت می‌تواند به تقویت پدافند سایبری کشور کمک کند. برای پیشگیری از این تهدیدها می‌بایست برنامه مدونی جهت ارزیابی مداوم ریسک‌ها و تهدیدها، توسعه تیم‌ها و سیستم‌های نظارتی و واکنش سریع و افزایش تاب‌آوری سیستم‌ها -از جمله بهبود فرایندهای بازیابی اطلاعات و پشتیبان‌گیری مداوم- تدارک دید.

از نظر شما اهمیت سرمایه‌های انسانی و روش‌های مدیریت بحران در مواجهه با تهدیدهای سایبری چیست و سازمان در این زمینه چه وضعیتی دارد؟

سرمایه‌های انسانی در مقابله با تهدیدهای سایبری در حوزه تجارت و صنعت نقش حیاتی دارند. همان‌طور که تکنولوژی‌های پیشرفته‌تر برای مقابله با حملات سایبری توسعه می‌یابند، به نیروهای متخصص و ماهر برای مدیریت و اجرای این فناوری‌ها نیاز است. با توجه به اینکه حملات سایبری حوزه تجارت هر ثانیه میلیون‌ها دلار به کشور آسیب می‌زند وجود نیروهای متخصص در زمینه امنیت سایبری و همچنین وجود تیم‌های واکنش سریع به حوادث سایبری (CSIRT) در سازمان‌های متولی تجارت و شرکت‌های بزرگ ضروری است.

سازمان پدافند غیرعامل با تدوین سیاست‌ها و مقررات، آموزش و توانمندسازی و همکاری با بخش خصوصی در جهت مقاوم‌سازی زیرساخت‌های حیاتی کشور در برابر تهدیدهای سایبری اقدام می‌کند، با این حال تا رسیدن به نقطه مطلوب فاصله داریم.

استراتژی‌های مدیریت بحران و آمادگی در برابر تهدیدهای سایبری به منظور حفظ تداوم خدمات رسانی زیرساخت‌های حیاتی را بیان بفرمایید.

برای مدیریت بحران ابتدا باید تهدیدهای بالقوه در زمینه داخلی و خارجی توسط افراد فعال حوزه تجارت شناسایی شوند، از جمله تهدیدهای سایبری، قطع زیرساخت‌ها و ناپایداری‌های اقتصادی. در ایران تعدد سامانه‌ها و سازمان‌های متولی تجارت و صنعت بزرگ‌ترین چالش در مواقع بروز بحران‌های سایبری است، از جمله سامانه جامع تجارت، سامانه انبارها، تجارت فرامرزی، بورس کالا و بارنامه که با قطع دسترسی به اینترنت یا حملات سایبری به هرکدام از آنها بحران بزرگی در زمینه صنعتی و تجاری رخ خواهد داد. از این رو توصیه می‌کنم که به جای الکترونیکی کردن اخذ مجوز و مراحل تجاری، نسبت به ساده‌سازی و کاهش فرایندهای تجاری برنامه‌ریزی صورت گیرد. با این حال در شرایط کنونی، برای مدیریت این بحران می‌بایست اطلاعات این سامانه‌ها

به‌صورت مرتب پشتیبان‌گیری شوند و برنامه‌های دقیق بازیابی این سامانه‌ها را در زمان حملات سایبری تدوین کرد. این برنامه‌ها شامل روش‌هایی برای ایجاد دسترسی و بازگرداندن سریع اطلاعات و بازیابی داده‌های مهمند، همچنین پیشنهاد می‌کنم از فناوری‌های پیشرفته امنیت نظیر سرورهای غیرمتمرکز (Decentralizedservers) و فناوری‌های رمزنگاری و احراز هویت چندعاملی استفاده شود.

یکی از بزرگ‌ترین تهدیدهای صنعتی و تجاری وابستگی به تأمین‌کننده خاص نظیر پتروشیمی و صنایع فولاد است که با حملات سایبری احتمال اختلال در ارائه خدمات در آنها وجود دارد. تنوع‌بخشی به تأمین‌کنندگان داخلی و خارجی از نظر مواد اولیه و تجهیزات می‌تواند در مواجهه با بحران‌های سایبری مؤثر باشد، همچنین سیستم ارتباطی مؤثر برای اطلاع‌رسانی به ذی‌نفعان در زمان بحران باید وجود داشته باشد. این سیستم باید شامل راه ارتباطی برای اطلاع‌رسانی سریع به واحدهای صنعتی و صنفی و تأمین‌کنندگان باشد تا از بروز هرگونه التهاب جلوگیری شود.

نقش و اهمیت مشارکت بخش‌های مختلف جامعه از جمله بخش‌های دولتی، غیردولتی و مردم در تقویت پدافند سایبری چیست؟

مشارکت هماهنگ و فعال بخش‌های دولتی، غیردولتی و مردم در تقویت پدافند سایبری می‌تواند به‌طور چشمگیری امنیت سایبری در حوزه تجارت و صنعت را افزایش دهد. هریک از این بخش‌ها نقشی کلیدی در ایجاد یک اکوسیستم امنیتی قوی در حوزه تجارت و صنعت دارند. در این راستا دولت با تدوین سیاست و سرمایه‌گذاری در زیرساخت و آموزش و بخش خصوصی با گزارش‌دهی، تحقیق و توسعه و شناسایی تهدیدها می‌تواند به مقابله با تهدیدهای سایبری کمک و از منافع ملی و اقتصادی حفاظت کند.

روندهای آینده در حوزه پدافند سایبری و پیش‌بینی چالش‌ها و فرصت‌های پیش‌رو در این زمینه چیست؟

پدافند سایبری در حوزه تجارت و صنعت، با توجه به رشد سریع تجارت الکترونیکی به یکی از مهم‌ترین اولویت‌ها برای

سازمان‌ها و شرکت‌ها تبدیل شده است. در آینده نزدیک هوش مصنوعی (AI) و ماشین لرنینگ (ML) نقش مهمی در تشخیص تهدیدهای سایبری دارند. این فناوری‌ها قادر به شناسایی الگوهای غیرمعمول در شبکه‌ها و پیش‌بینی حملات بالقوه قبل از وقوع آنها هستند و یکی از چالش‌های پیش رو توسعه و به‌کارگیری آنها در امنیت سامانه‌ها و نرم‌افزارهای تجاری است، همچنین با افزایش استفاده از دستگاه‌های متصل به اینترنت در کارخانه‌ها و صنعت، امنیت در اینترنت اشیا به یکی از مسائل مهم تبدیل می‌شود. این دستگاه‌ها ممکن است آسیب‌پذیری‌های بیشتری داشته باشند و به‌عنوان نقاط ورود برای حملات سایبری مورد استفاده قرار گیرند، به‌همین دلیل امنیت در اینترنت اشیا (IoT) از چالش‌های مهم پیش رو در تجارت و صنعت است. با این حال با افزایش تهدیدها در سطح جهان، شرکت‌ها برای محافظت از سیستم‌هایشان بیشتر به متخصصان نیاز دارند که کشور می‌تواند به دید فرصت به آنها بنگرد و با سرمایه‌گذاری و برنامه‌ریزی بلندمدت در تربیت متخصصان این حوزه از فرصت پیش رو بهره‌برداری اقتصادی کند.

فرصت‌ها و تهدیدهای فناوری‌های پیشران مثل هوش مصنوعی در امنیت و پدافند سایبری را چطور توصیف و ارزیابی می‌کنید و چه آمادگی‌هایی در این زمینه داریم؟

در حوزه تجارت و صنعت، هوش مصنوعی می‌تواند به بهینه‌سازی زنجیره تأمین کمک کند، از پیش‌بینی تقاضا گرفته تا مدیریت موجودی و شبیه‌سازی و شناخت الگوی رفتاری بازار در زمان بحران که باعث می‌شوند بتوان اقدامات لازم را برای مواجهه با بحران‌های سایبری برنامه‌ریزی کرد، همچنین در تحلیل بازار، افزایش امنیت اطلاعات تجاری و توسعه صنعت، هوش مصنوعی در آینده نقش بی‌بدیلی ایفا خواهد کرد. با این حال احتمال استفاده از هوش مصنوعی در حملات پیچیده‌تر و هدفمند علیه زیرساخت‌های تجاری وجود دارد که باید نسبت به سرمایه‌گذاری در فناوری‌های امنیت سایبری و به‌روزکردن سیستم‌ها به منظور پیشگیری از این حملات اقدام کرد.

محمدجعفر نعناکار، معاون اسبق حقوقی وزارت ارتباطات و فناوری اطلاعات

نیاز به اصلاح و تکمیل قوانین امنیت سایبری

در ارتباط با تهدیدهای موجود در فضای سایبری، آمادگی ایران برای مقابله با این تهدیدها و همچنین ابعاد مختلف این آمادگی در زمینه‌های گوناگون گفت‌وگویی با محمدجعفر نعناکار، معاون اسبق حقوقی وزارت ارتباطات و فناوری اطلاعات داشتیم تا از زوایای مختلف به این مسئله بپردازیم و ضمن فهم وضعیت موجود، چشم‌اندازی ناظر به تجربیات زیسته سایر کشورها نسبت به وضعیت مطلوب داشته باشیم. او در این گفت‌وگو ضمن توصیف وضعیت و نسبت شرایط موجود کشور در مواجهه با تهدیدهای سایبری و همچنین تجربه سایر کشورها، تصویری ارائه داد که می‌تواند استنباط و فهم درستی به مخاطبان و تصمیم‌گیران بدهد. مشروح این گفت‌وگو را از نظر می‌گذرانید.

۱ برای شروع می‌خواستیم از شما بپرسیم جنس تهدیدهای فضای سایبری، آن چیزی که امروزه با آن مواجهیم در قیاس با قبل چه تغییراتی داشته و آیا رویکردها، تصمیمات و مراقبت‌های ما نیز همراستا با این تغییرات به‌روز و کارآمد شده است؟

تهدیدهای سایبری که در گذشته به‌طور عمده شامل نفوذ به سامانه‌های کوچک و سرقت اطلاعات ساده بود، اکنون به سطوح پیچیده‌تر و چندلایه‌ای تبدیل شده‌اند. حملات پیشرفته مداوم (APT)، جاسوسی سایبری، سرقت مالکیت معنوی، حملات به زیرساخت‌های حیاتی (نظیر برق، آب، شبکه‌های بانکی و ارتباطی) و حملات باج‌افزار بخشی از تهدیدهای جدید محسوب می‌شوند. در گذشته، هدف اصلی مهاجمان اغلب مالی و اطلاعاتی بود، اما امروزه شاهد استفاده از حملات سایبری به‌عنوان ابزار سیاسی و حتی جنگ‌های سایبری میان کشورها هستیم؛ ازنظر حقوقی، کشورها موظف به بازنگری و اصلاح قوانین مرتبط با امنیت سایبری‌اند. در بسیاری از کشورها قوانین قدیمی و ناکارآمد برای مقابله با تهدیدهای نوین هنوز به‌کار می‌روند، درحالی‌که تکنولوژی به‌سرعت تغییر می‌کند، برای مثال به اصلاح قوانین مرتبط با جرم‌انگاری حملات سایبری، تقویت چهارچوب‌های قانونی برای حفاظت از داده‌ها و حریم خصوصی و همچنین ایجاد سازوکارهای بین‌المللی برای مبارزه با جرائم سایبری نیازمندیم. قوانین مربوط به کنوانسیون بوداپست از مهم‌ترین تلاش‌ها در این زمینه است که کشورهای مختلف را به همکاری بین‌المللی برای مقابله با جرائم سایبری ترغیب می‌کند، اما برخی کشورها هنوز به این کنوانسیون نپیوسته‌اند یا قوانین داخلی‌شان به‌طور کامل با این کنوانسیون همراستا نیست.

۲ به‌عنوان یک متخصص و فردی که در حوزه‌های فناورانه فعالیت داشتید و دارید. اهم تهدیدها در این حوزه را چه چیزهایی می‌دانید و سرعت تحولات در تهدیدها چه تأثیری بر روند رشد و پیشرفت حوزه‌های فناورانه در داخل ایران دارد؟

تهدیدهای فناورانه در ایران شامل سرقت اطلاعات بانکی، حملات به شبکه‌های دولتی و کسب‌وکارهای اینترنتی، حملات باج‌افزار و نفوذ به زیرساخت‌های حیاتی است. این تهدیدها از سوی هکرهای داخلی و خارجی صورت می‌گیرد و موجب ایجاد خسارات مالی، حقوقی و حتی اجتماعی می‌شود؛ از منظر حقوقی، نیاز به چهارچوب‌های قانونی برای مقابله با این تهدیدها به‌ویژه در حوزه حفاظت از اطلاعات کاربران بسیار ضروری است. تاکنون ایران قوانین پراکنده‌ای مانند قانون جرائم رایانه‌ای را برای مقابله با تهدیدهای سایبری تدوین کرده است، اما با توجه به پیشرفت فناوری و گسترش تهدیدهای سایبری، این قوانین به‌روز نیستند و نیاز به اصلاح و تکمیل دارند. یکی از چالش‌های اصلی، عدم تطابق قوانین داخلی با استانداردهای بین‌المللی و کنوانسیون‌های مرتبط است. به‌علاوه توسعه فناوری‌های جدید نظیر اینترنت اشیا (IoT) و هوش مصنوعی نیز به قوانین و مقررات جدید نیاز دارد تا به‌طور مؤثری از تهدیدهای نوظهور جلوگیری شود؛ سرعت تحولات در تهدیدهای سایبری، رشد و پیشرفت داخلی را نیز تحت تأثیر قرار می‌دهد. کشورهایی که نتوانند قوانین خود را به‌روز کنند و نهادهای اجرایی کارآمدی برای مقابله با تهدیدها ایجاد نکنند، با مشکلات جدی در جذب سرمایه‌گذاری‌های فناورانه مواجه خواهند شد. از سوی دیگر حقوق مالکیت فکری و تجاری تحت تأثیر این تهدیدها قرار می‌گیرند و اگر کشورها نتوانند از داده‌ها و اطلاعات تجاری محافظت کنند، احتمال از دست رفتن فرصت‌های کسب‌وکار و نوآوری افزایش می‌یابد.

۳ مدل مواجهه نهادهای مسئول در حوزه تأمین امنیت فضای فناوری کشور، اعم از شبکه‌های بانکی، کسب‌وکارها و زیرساخت‌ها را چطور ارزیابی می‌کنید؟

مدل مواجهه نهادهای مسئول در ایران با تهدیدهای سایبری همچنان به تقویت نیاز دارد. از یک‌سو نهادهایی نظیر پلیس فتا، مرکز ماهر و دستگاه‌های اجرایی مربوطه تلاش‌هایی برای افزایش امنیت فضای سایبری انجام داده‌اند، اما عدم هماهنگی کامل میان نهادهای اجرایی و نبود رویکرد جامع و فراگیر برای مقابله با تهدیدها موجب شده اقدامات به‌طور پراکنده و ناکافی انجام شود؛ از منظر حقوقی نیاز است نهادهای مسئول به‌ویژه در حوزه زیرساخت‌های حیاتی نظیر بانک‌ها، شبکه‌های ارتباطی و دولتی، ملزم به اجرای پروتکل‌های امنیتی سفت‌وسخت‌تری شوند. نهادهای دولتی باید تحت قانون مسئولیت حفاظت از زیرساخت‌های حیاتی قرار گیرند و به‌صورت قانونی موظف شوند از آخرین استانداردهای امنیتی استفاده کنند، همچنین به تصویب قوانین جدیدی برای حمایت از شرکت‌ها و کسب‌وکارها

دربرابـر تهدیدهـای سـایبری نیاز اسـت، به‌گونـه‌ای که بتواند مسئولیت نهادهای مختلف را به‌صورت شفاف مشخص کند.

۴ مقایسـه تطبیقی در این حوزه داشـته‌اید؟ تجربه سـایر کشـورها در این زمینه و در مواجهه با تهدیدهای این فضا با ایران چه تفاوت‌ها و قرابت‌هایی دارند؟

در مقایسه با کشورهای پیشرفته، ایران هنوز در مراحل ابتدایی مدیریـت تهدیدهـای سـایبری قـرار دارد. کشـورهایی نظیـر ایالات‌متحده و اتحادیه اروپا قوانین سفت‌وسختی برای مقابله باتهدیدهای سایبری دارند. در این کشورها تلاش‌های گسترده‌ای برای تدوین قوانین جامع برای حفاظت از اطلاعات، مسئولیت شـرکت‌های ارائه‌دهنده خدمـات اینترنتی و همچنین حفظ حقوق کاربران صورت گرفته است. به‌عنوان نمونه قانون عمومی حفاظـت از داده‌هـای اتحادیـه اروپـا (GDPR) از جامع‌ترین و مؤثرتریـن قوانین در زمینه حفاظت از داده‌های کاربران اسـت. از سـوی دیگر ایران با کمبودهای قانونی مواجه اسـت و قوانین موجود به‌روز نشـده‌اند. ازلحاظ حقوقی برای ایران مهم اسـت که به اسـتانداردهای بین‌المللی نزدیک شـود و با پیوسـتن به کنوانسیون‌هایی نظیر کنوانسیون بوداپست، همکاری بین‌المللی خود را در زمینه مقابله با جرائم سایبری تقویت کند.

۵ با وجود توسـعه و نفوذ هوش مصنوعی در سـاختارها و حوزه‌های مختلف، آیا اسناد و برنامه‌ریزی‌هایی برای مواجهه با فرصت‌ها و تهدیدهای هوش مصنوعی داریم؟ پیشـنهاد شما برای این مواجهه چیست؟

هوش مصنوعـی به‌عنوان یکی از حوزه‌های نوظهور، فرصت‌های بی‌شماری در زمینه‌های اقتصادی و اجتماعی ایجاد کرده‌است، امـا به‌طور هم‌زمـان تهدیدهای جدی نیز به همـراه دارد، ازجمله تهدیدهـای هوش مصنوعی می‌تـوان به اسـتفاده از این فناوری در حملات سـایبری، جاسوسـی صنعتی و حتی نقض حقوق خصوصی افراد اشاره کرد. استفاده از الگوریتم‌های هوش مصنوعی بـرای تحلیـل داده‌های شـخصی ممکن اسـت بـه نقض حریم خصوصی منجر شود؛ در ایران به‌رغم پیشرفت‌های فناورانه، اسناد و قوانین جامعی برای مواجهه با این تهدیدها وجود ندارند. از منظر حقوقـی به تدوین قوانین مرتبط با اسـتفاده از هوش مصنوعی در حوزه‌های مختلف ازجمله امنیت سـایبری، حفاظت از داده‌ها و حریم خصوصی نیاز اسـت. پیشـنهاد می‌شـود دولت ایران از تجربیات کشورهای پیشرفته در این زمینه استفاده کند و چهارچوب حقوقی جامعی برای مدیریت هوش مصنوعی تدوین کند.

۶ در حوزه فنی و لجسـتیکی برای اقدامی منسـجم و کارا جهـت مواجهـه بـا تهدیدهای سـایبری به چـه اقدامات و توانمندی‌هایی نیازمندیم تا شاهد خرابکاری‌ها و حملات سایبری در این حوزه نباشیم؟

بـرای مقابلـه مؤثـر با تهدیدهـای سـایبری به اقدامـات فنی و لجسـتیکی فراگیر نیاز اسـت، ازجمله این اقدامـات می‌توان به اسـتفاده از سیسـتم‌های پیشرفته تشـخیص نفوذ، تحلیل تهدیدها به‌کمک هوش مصنوعی و بلاک‌چین و همچنین تربیت نیروی انسانی متخصص اشاره کرد. به‌علاوه نهادهای دولتی و خصوصـی باید به‌صورت قانونی به اتخاذ پروتکل‌های امنیتی قوی و گزارش‌دهی منظم در زمینه امنیت سایبری موظف شوند.

۷ از منظـر حقوقـی برای صیانت از مردم به‌عنوان کاربران و همچنیـن ارائه‌دهنـدگان چـه تکالیفی برعهـده نهادهای حاکمیتی است و در مقابل چه تکالیف و الزاماتی می‌بایست از سوی خدمات‌دهندگان و... در این حوزه رعایت شوند؟

ازنظر حقوقـی نهادهای حاکمیتی موظفند چهارچوب قانونی شـفافی بـرای حفاظـت از اطلاعـات کاربـران و همچنیـن زیرسـاخت‌های حیاتی کشـور ایجـاد کنند. ایـن نهادها باید قوانینی تدوین کنند که مسـئولیت ارائه‌دهنـدگان خدمات را به‌صـورت دقیق مشـخص کند و به کاربران امـکان دهد که در صـورت نقض حریـم خصوصی یـا امنیت اطلاعات‌شـان، از حقـوق خود دفاع کنند. همچنیـن نهادهای دولتی باید به‌طور مستمر بر عملکرد شرکت‌ها و سازمان‌ها نظارت داشته باشند و در صورت نیاز اقدام به اعمال تحریم‌ها یا جریمه‌های سنگین کنند. درنهایت ارائه‌دهندگان خدمات نیز باید به قوانین داخلی و بین‌المللـی پایبند باشـند و مسـئولیت‌های خـود را در قبال حفاظـت از اطلاعـات کاربـران به‌طـور دقیق انجـام دهند. در غیـر این صـورت کاربران باید امکان پیگیری قانونی و دریافت خسارت را داشته باشند.

ترجمه

حفظ امنیت سایبری در زیرساخت‌های حیاتی:

حفاظت از شبکه‌های برق و هوشمند

Kehinde Ayano[1] Indiana Wesleyan University - September 30, 2024

زیرساخت‌هایی مانند سیستم آب، سیستم تأمین انرژی، شبکه‌های مخابراتی و نیروگاه‌ها از سرمایه‌های حیاتی هر کشور به‌شمار می‌روند که تخریب و ناتوانی این سیستم‌ها بر امنیت، اقتصاد، سلامت و رفاه کلی و موجودیت هر کشور تأثیر منفی می‌گذارد. ادغام جنگ دیجیتال و سایبری در جنگ سنتی، نیاز به ایمن‌سازی کافی این زیرساخت‌های حیاتی را ضروری می‌سازد، زیرا این زیرساخت‌ها به هدف اصلی بازیگران دولتی در صورت درگیری و جنگ تبدیل می‌شوند. اکثر سیستم‌های زیرساختی در جامعه مدرن با الکتریسیته هدایت می‌شوند که برق و شبکه‌های هوشمند را بسیار حیاتی می‌سازد، زیرا تقریبا زیرساخت‌های حیاتی دیگر را زیربنا می‌دهند؛ یک حمله موفقیت‌آمیز به این زیرساخت، تأثیر آبشاری بر سایر زیرساخت‌های حیاتی خواهد داشت. این مقاله به بررسی تکامل شبکه‌های برق، چشم‌انداز تهدید و آسیب‌پذیری‌ها در شبکه‌های برق و هوشمند می‌پردازد. همچنین مطالعات موردی در دنیای واقعی حملات سایبری به شبکه‌های برق و هوشمند را بررسی می‌کند و حوادث را تحلیل می‌کند و با استراتژی‌های امنیتی و بهترین شیوه‌ها برای حفاظت از برق و شبکه‌های هوشمند نتیجه‌گیری می‌کند.

تکامل برق و شبکه‌های هوشمند

سیستم‌های برق سنتی - که به‌عنوان شبکه‌های برق نیز شناخته می‌شوند - سیستمی یک‌طرفه برای توزیع برق از تولیدکنندگان به مصرف‌کنندگانند و برای عملکرد کسب‌وکار، جامعه و دولت به‌طورکلی حیاتی‌اند. آنها به‌صورت دستی با ظرفیت محدود برای ادغام با انرژی‌های تجدیدپذیر کنترل می‌شوند. پیشرفت در فناوری و تکامل دیجیتال منجر به توسعه نسخه‌های مدرن سیستم قدرت سنتی می‌شود که از فناوری‌های دیجیتال برای نظارت، مدیریت، هماهنگ‌سازی و انتقال انرژی از منابع متعدد جهت پاسخگویی به نیازهای مختلف مصرف‌کنندگان استفاده می‌کند. این شبکه‌های هوشمند، برخلاف شبکه‌های برق، سیستم‌های ارتباطی دوطرفه با کنترل خودکار و نظارت زمان واقعی‌اند و امکان ادغام آسان انرژی‌های تجدیدپذیر را فراهم می‌کنند که قابلیت اطمینان و کارایی سیستم‌های قدرت الکتریکی را بهبود می‌بخشد.

اجزای شبکه‌های ارتباطی هوشمند

برخی اجزای اصلی شبکه ارتباطی شبکه هوشمند شامل موارد زیرند که امکان برقراری ارتباط دوطرفه یکپارچه بین شرکت‌ها و مصرف‌کنندگان را فراهم می‌کند:

۱ مرکز کنترل: این مرکز برای نظارت و مدیریت کل شبکه است. داده‌ها را از تمام اجزای دیگر می‌پذیرد و سیگنال‌های کنترلی را برای مدیریت عملیات شبکه ارسال می‌کند.

۲ پست: ولتاژ بالا را از شبکه انتقال به سطوح پایین مناسب برای توزیع تبدیل می‌کند. پست‌های شبکه هوشمند مجهز به حسگرها و دستگاه‌هایی‌اند که می‌توانند اطلاعات مربوط به کیفیت توان، وضعیت بار و وضعیت تجهیزات را به مرکز کنترل ارسال کنند.

۳ کنتور هوشمند: کنتور هوشمند مصرف را، هم با مصرف‌کننده و هم با شرکت برق در زمان واقعی اندازه‌گیری کرده و کنترل می‌کند.

۴ زیرساخت اندازه‌گیری پیشرفته: ارتباطات بین کنتورهای هوشمند و تأسیسات را تسهیل و داده‌های کنتور هوشمند را به مرکز کنترل و سایر اجزای شبکه ارسال می‌کند.

اجزای ذکرشده و بسیاری موارد دیگر، شبکه‌های هوشمند را به شبکه ارتباطی کاملا دیجیتالی تبدیل می‌کند که قابلیت اطمینان و کارایی سیستم قدرت الکتریکی را بهبود می‌بخشد. با این حال، ادغام فناوری دیجیتال در شبکه‌های هوشمند، آسیب‌پذیری‌ها و تهدیدات امنیت سایبری جدیدی را نیز معرفی می‌کند که برای عملیات قوی باید برطرف شوند. اطمینان از ایمن بودن شبکه‌های برق و هوشمند برای کسب‌وکار، سازمان و دولت بسیار مهم است، زیرا نتیجه این حملات می‌تواند فاجعه‌بار و تهدیدکننده زندگی باشد.

چشم‌انداز تهدیدها در برق و شبکه‌های هوشمند

۱ بدافزار: اینها نرم‌افزارهای مخربی‌اند که برای ایجاد اختلال در آسیب و دسترسی به سیستم طراحی شده‌اند. این شامل تروجان‌ها، ویروس‌ها، باج‌افزارها و بسیاری دیگر می‌شود. بدافزار از آسیب‌پذیری‌های شناخته‌شده و روز صفر در نرم‌افزار، سخت‌افزار و پروتکل‌های شبکه مورد استفاده در سیستم‌های قدرت سوءاستفاده می‌کند و می‌تواند سیستم‌های کنترل نظارتی و جمع‌آوری داده‌های DCS، SCADA و سایر فناوری‌های عملیاتی را غیرفعال یا مختل کند.

۲ فیشینگ: این نوعی از حمله است که به موجب آن مهاجم با تظاهر به موجودیت قانونی، اطلاعات حساسی مانند نام کاربری و رمز عبور را پنهان و تلاش می‌کند اطلاعات حساس را به دست آورد.

۳ نفوذ شبکه: سیستم‌های ارتباطی شبکه برق و شبکه‌های هوشمند می‌توانند از طریق تنظیمات امنیتی ضعیف مانند رمز عبور پیش‌فرض، دسترسی از راه دور ناامن یا سیستم‌های وصله‌نشده و سایر آسیب‌پذیری‌ها برای به دست آوردن کنترل روی سیستم، نفوذ کنند.

۴ تهدیدهای پایدار پیشرفته (APT): این حمله سایبری طولانی‌مدت و هدفمند است که در آن بازیگران دولتی یا مجرمان سایبری بسیار ماهر به یک شبکه دسترسی پیدا می‌کنند و شناسایی نمی‌شوند.

آسیب‌پذیری در برق و شبکه‌های هوشمند

سطح حمله در شبکه‌های هوشمند به دلیل شبکه پیچیده دستگاه‌ها که شامل حسگرها، کنتورهای هوشمند، سوئیچ‌های هوشمند، شبکه‌های ارتباطی و سیستم‌های کنترلی‌اند، به‌طور قابل توجهی گسترش یافته که هریک از این اجزا هدف حملات سایبری‌اند. افزایش اتصال و تبادل داده در مرکز کنترل و سایر اجزای شبکه‌های هوشمند، آن را در برابر حملات آسیب‌پذیرتر می‌کند، بنابراین برای حفظ انعطاف‌پذیری و امنیت شبکه‌های هوشمند، درک و رسیدگی به آسیب‌پذیری‌های ذاتی در سیستم‌های شبکه‌های هوشمند بسیار مهم است.

این آسیب‌پذیری‌ها شامل موارد زیر است:

۱ سیستم‌های قدیمی: استفاده مداوم از سیستم‌های قدیمی که به دلیل محدودیت‌های خاص در یک سازمان، فناوری‌های قدیمی‌اند، خطرات قابل توجهی برای امنیت چنین سیستم‌هایی ایجاد می‌کند. دلیلش این است که چنین سیستم‌هایی ممکن است دیگر برای به‌روزرسانی وصله نشوند و همچنین ممکن است قابلیت نظارت محدودی داشته باشند.

۲ شبکه‌های به‌هم‌پیوسته: اتصال گسترده دستگاه‌ها و افزایش اتصال سیستم‌های ارتباطی شبکه‌های هوشمند در صورت عدم ایمن‌سازی مناسب، آنها را در برابر حمله بسیار آسیب‌پذیر می‌کند.

۳ دسترسی از راه دور: مدیریت و نظارت بر سیستم شبکه‌ها معمولا از طریق دسترسی از راه دور انجام می‌شود. آسیب‌پذیری‌ها در اتصال دسترسی از راه دور ممکن است توسط مهاجمان برای دسترسی به سیستم مورد سوءاستفاده قرار گیرند.

۴ ریسک زنجیره تأمین: شبکه‌های هوشمند به شدت به زنجیره تأمین پیچیده قطعات سخت‌افزاری و نرم‌افزاری متکی‌اند که عمدتا با تولیدکنندگان و تأمین‌کنندگان قرارداد بسته شده است. اقدامات امنیتی چنین فروشندگان شخص ثالث، اگر قوی نباشد، ممکن است در صورت ادغام در شبکه‌های برق و هوشمند، خطرات قابل توجهی ایجاد کند. مهاجمان همچنین می‌توانند چرخه عمر توسعه نرم‌افزار را با به خطر انداختن

به‌روزرسانی‌های نرم‌افزار و نرم‌افزار قانونی هدف قرار دهند که به‌نوبه خود سیستمی را که در آن مستقرشده‌اند دربرابر حمله آسیب‌پذیر می‌کند. نمونه‌ای از چنین آسیب‌پذیری‌های زنجیره تأمین، حمله SolarWinds است که در آن بدافزار به به‌روزرسانی معمول نرم‌افزار تزریق می‌شود.

۵ عامل انسانی: عامل انسانی یکی از رایج‌ترین آسیب‌پذیری‌ها در چهارچوب امنیت سایبری است. خطا و سهل‌انگاری یا سوءنیت کارکنان علی‌رغم دفاع‌های فناورانه محکم منجر به سازش سیستم شده است. این سازش به‌دلیل آموزش و آگاهی ناکافی، شیوه‌های نامناسب رمز عبور و تهدیدات داخلی است.

نمونه‌های دنیای واقعی از حملات سایبری به برق و شبکه‌های هوشمند

باتوجه به تکامل دیجیتالی سیستم‌های قدرت الکتریکی، برق و شبکه‌های هوشمند به‌طور فزاینده‌ای در حال تبدیل شدن به زمین صفر برای جنگ سایبری‌اند. در طول دو دهه گذشته، حملات متعددی علیه شبکه‌های هوشمند انجام شده که منجر به قطع و خسارات مالی ناشی از پرداخت باج هنگفت شده است. نمونه‌ای از آن حمله به شبکه برق اوکراین در سال ۲۰۱۵ است که در آن بدافزار BlackEnergy برای به خطر انداختن سه سیستم توزیع اوکراینی با استفاده از ایمیل‌های فیشینگ استفاده شد. مهاجم به سیستم‌های کنترل نظارت و جمع‌آوری داده‌ها (SCADA) دسترسی پیدا کرد و قطع‌کننده مدار را از راه دور به خطر انداخت و UPS و پشتیبان‌گیری را غیرفعال کرد. همچنین در سال ۲۰۱۶، ایستگاه انتقال اوکراین مورد هدف بدافزاری به نام Industroyer قرار گرفت که سیستم کنترل صنعتی را به خطر انداخت و توزیع برق را برای حدود یک ساعت مختل کرد. در ایالات متحده، آژانس‌های برق شهرداری فلوریدا نیز در ژوئن ۲۰۲۱ با استفاده از فیشینگ و آسیب‌پذیری‌های راه دور به‌عنوان بردارهای حمله هدف قرار گرفتند. درحالی‌که مهاجمان سطحی از دسترسی را به‌دست آوردند، حمله قبل از این کاهش یافت که بتواند اثر فاجعه‌باری ایجاد کند. این موارد بر اهمیت استراتژی‌های امنیتی و بهترین شیوه‌ها در مدیریت برق و شبکه‌های هوشمند تأکید می‌کنند.

استراتژی‌های امنیتی و بهترین روش‌ها برای مدیریت برق و شبکه‌های هوشمند

در سال‌های اخیر حملات سایبری به شبکه‌های برق و شبکه‌های هوشمند مکرر و پیچیده‌تر شده‌اند و می‌توانند پیامدهای مخربی از جمله خاموشی، خسارات اقتصادی، اختلال در زیرساخت‌های حیاتی و سرقت داده‌های حساس داشته باشند، بنابراین برای محافظت از این زیرساخت حیاتی دربرابر حمله، نیاز به ایجاد استراتژی‌های امنیتی مناسب و بهترین شیوه‌هاست. برخی استراتژی‌های امنیتی و بهترین شیوه‌ها برای برق و شبکه‌های هوشمند در زیر مورد بحث قرار می‌گیرند.

۱ ارزیابی و مدیریت ریسک: ارزیابی و مدیریت ریسک در امنیت شبکه‌های برق و هوشمند نقش حیاتی بازی می‌کنند، زیرا به شناسایی و کاهش آسیب‌پذیری‌ها و به واکنش دربرابر حوادث کمک می‌کنند. اجرای ارزیابی و مدیریت ریسک با استفاده از گزارش بین‌سازمانی NIST (IR) 7628 ویرایش[1] که چهارچوبی جامع برای ایمن کردن سیستم‌های شبکه هوشمند ارائه می‌دهد، در ایمن‌سازی این زیرساخت حیاتی کمک فراوانی خواهد کرد.

۲ دفاع در عمق: اجرای رویکرد امنیتی لایه‌ای با استفاده از کنترل‌ها و پروتکل‌های امنیتی مختلف (دیوارهای آتش، رمزگذاری، SIEM، IPS، IDS، کنترل‌های دسترسی) وضعیت امنیتی سیستم‌های شبکه هوشمند را افزایش می‌دهد.

۳ ارزیابی آسیب‌پذیری و تست نفوذ: تشخیص ضعف ذاتی در سیستم‌های شبکه هوشمند پیش از اینکه مهاجم از طریق سیستم، آسیبی فراگیر به آن وارد کند. ارزیابی توانایی و شبیه‌سازی حمله واقعی برای کشف آسیب‌پذیری‌هایی که پنهانند و توسط اسکن خودکار کشف نشده باقی می‌مانند، این امکان را فراهم می‌کند که چنین نقص‌های امنیتی‌ای در سیستم قبل از سوءاستفاده توسط مهاجمان تشدید شوند.

۴ مدیریت پچ: جدا از اطمینان از قابلیت اطمینان سیستم، مدیریت پچ مؤثر سطح حمله را نیز کاهش می‌دهد. پرداختن فعالانه به آسیب‌پذیری‌ها در شبکه هوشمند از طریق مدیریت وصله‌های مؤثر مقرون به صرفه‌تر از کاهش واکنشی اثر ناشی از نقض‌های امنیتی است.

۵ تقسیم‌بندی شبکه: تقسیم‌بندی سیستم شبکه‌های ارتباطی یک سیستم شبکه هوشمند، حرکت جانبی را مهار می‌کند و مانع از دسترسی مهاجم به کل سیستم در صورت رخنه می‌شود و در نتیجه تأثیر حمله را به حداقل می‌رساند، همچنین به اصلاح کمک می‌کند، زیرا تمرکز می‌تواند فقط روی بخش آسیب دیده باشد.

۶ برنامه‌های آموزش و آگاهی کارکنان: اهمیت آموزش و آگاهی کارکنان را نمی‌توان بیش از حد مورد تأکید قرار داد، زیرا تحقیقات نشان داده انسان‌ها حلقه مفقوده زنجیره امنیت سایبری‌اند و به‌شدت در معرض مهندسی اجتماعی، فیشینگ، تهدیدات داخلی و مستعد ارتکاب خطا هستند. آموزش و آگاهی به کارکنان کمک می‌کند بهداشت سایبری خوبی داشته باشند و ساختار امنیت سایبری قوی را پرورش دهند.

نتیجه‌گیری

با این تفاصیل، امنیت شبکه‌های برق و هوشمند به رویکرد چندبعدی نیاز دارد که اجرای کنترل‌های امنیتی را که مدیریت، فیزیکی، فنی و مدیریتی‌اند و ارزیابی و مدیریت ریسک فعال و آموزش و بازآموزی مستمر عناصر انسانی را ترکیب می‌کند. قرار دادن امنیت سایبری در اولویت اصلی و تقویت فرهنگ امنیت سایبری از این زیرساخت حیاتی در برابر حملات محافظت می‌کند.

پی‌نوشت:

۱- استادیار کامپیوتر و علوم اطلاعات در دانشگاه ایندیانا و سلیان ایندیاناست. او همچنین متخصص امنیت سیستم‌های اطلاعاتی است.

مبارزه با حملات سایبری از طریق اطلاعات تهدیدآمیز

Deboleena DuttaJune

در دنیای دیجیتالی امروزی سازمان‌ها با مجموعه‌ای از تهدیدهای سایبری رو به رشد مواجهند؛ از بدافزارهای پیچیده گرفته تا حملات فیشینگ هدفمند. به همین دلیل چشم‌انداز امنیت سایبری به‌طور مداوم درحال تغییر است و چالش‌های مهمی را برای مشاغل در هر اندازه‌ای ایجاد می‌کند. در پاسخ، تقاضا برای راه‌حل‌های اطلاعاتی تهدید مؤثر هرگز بالاتر نبوده است. حوزه اطلاعاتی «تهدید» به‌عنوان یکی از اجزای حیاتی استراتژی‌های امنیت سایبری پدیدار شده است و سازمان‌ها را در مورد تهدیدها و آسیب‌پذیری‌های بالقوه پیش از بهره‌برداری از آنها مطلع می‌کند، اما پیمایش در این صنعت پیچیده می‌تواند دلهره‌آور باشد، زیرا طیف گسترده‌ای از فروشندگان راه‌حل‌ها و خدمات مختلفی را ارائه می‌دهند. در اینجا پویایی بازار اطلاعات تهدید، بازیگران کلیدی آن و عواملی را بررسی می‌کنیم که باعث رشد آن می‌شوند.

درک هوش تهدید

هوش تهدید شامل جمع‌آوری، تجزیه‌وتحلیل و انتشار اطلاعات در مورد تهدیدهای بالقوه امنیت سایبری است. این اطلاعات

می‌تواند از منابع مختلفی از جمله محققان امنیتی، سازمان‌های دولتی و سازمان‌های بخش خصوصی به دست آیند. اطلاعات تهدید معمولا به سه نوع اصلی طبقه‌بندی می‌شود: استراتژیک، عملیاتی و تاکتیکی.

۱ هوش استراتژیک بینش‌های سطح بالایی را در مورد روندهای بلندمدت و تهدیدهای نوظهور فراهم می‌کند.

۲ هوش عملیاتی بر تهدیدها و آسیب‌پذیری‌های فعلی مرتبط با محیط خاص یک سازمان تمرکز دارد.

۳ اطلاعات تاکتیکی جزئیات دقیقی را در مورد تهدیدهای خاص ارائه می‌دهد، مانند شاخص‌های سازش (IOC) یا امضای بدافزار.

هوش تهدید چگونه مؤثر است؟

اطلاعات تهدید، بینش‌های ارزشمندی را در مورد تهدیدهای سایبری بالقوه ارائه و به افراد امکان می‌دهد تصمیماتی آگاهانه برای محافظت از دارایی‌های سازمان خود بگیرند. با تجزیه‌وتحلیل داده‌های اطلاعاتی تهدید، تهدیدهای نوظهور را می‌توان شناسایی کرد. پرسنل می‌توانند بردارهای حمله را درک و اقدامات امنیتی را به‌طور مؤثر اولویت‌بندی کنند. این رویکرد پیشگیرانه به تقویت وضعیت امنیتی سازمان و کاهش خطرات قبل از تبدیل شدن به حوادث بزرگ کمک می‌کند.

دامنه اطلاعات تهدید- برنامه‌های کاربردی

برنامه‌های کاربردی برای هوش تهدید متنوع‌اند و طیف گسترده‌ای از موارد استفاده را در صنایع مختلف دربرمی‌گیرند. برخی از کاربردهای کلیدی موجود در بازار اطلاعات تهدید عبارتند از:

۱ **شناسایی پیشگیرانه تهدید:** سازمان‌ها می‌توانند تهدیدهای سایبری احتمالی را قبل از اینکه به حملات گسترده تبدیل شوند، به‌لطف اطلاعات تهدید، شناسایی و پیش‌بینی کنند. سازمان‌ها می‌توانند با شناسایی فعال و خنثی کردن تهدیدها در مراحل اولیه از طریق نظارت مستمر برای شاخص‌های سازش (IOC) و توسعه روندهای تهدید، خطر نقض داده‌ها و به خطر افتادن سیستم را کاهش دهند.

۲ **تشخیص و پیشگیری از تقلب:** اطلاعات تهدید همچنین در شناسایی و توقف فعالیت‌های کلاهبرداری از جمله سرقت هویت، کلاهبرداری مالی و طرح‌های فیشینگ مفیدند. سازمان‌ها می‌توانند فعالیت‌های مشکوک حاکی از تقلب را شناسایی کنند و با بررسی روندها و ناهنجاری‌ها در رفتار کاربر، داده‌های تراکنش و کانال‌های ارتباطی، اقداماتی پیشگیرانه را برای کاهش خطر زیان‌های پولی و آسیب‌های اعتباری انجام دهند.

۳ **واکنش و کاهش حادثه:** اطلاعات تهدید بینش‌های مهمی را ارائه می‌دهد که واکنش حادثه و اقدامات کاهش دهنده را در مورد حادثه یا نقض امنیتی سرعت می‌بخشد. سازمان‌ها می‌توانند به سرعت وسعت و شدت حمله را ارزیابی کنند، تاکتیک‌ها، روش‌ها و رویه‌ها (TTP) مورد استفاده دشمنان را مشخص کنند و با یکپارچه‌سازی داده‌های حادثه با فیدهای اطلاعاتی تهدید، اقدامات اصلاحی متمرکزی را برای حذف تهدید انجام دهند.

۴ **انطباق با مقررات:** توانایی سازمان برای پیروی از قوانین صنعت و قوانین حفاظت از داده‌ها به‌شدت توسط اطلاعات تهدید کمک می‌کند. سازمان‌ها می‌توانند با نشان دادن دقت لازم در شناسایی و کاهش تهدیدهای سایبری از طریق ادغام اطلاعات تهدید در چهارچوب‌های امنیتی خود، معیارهای سختگیرانه نهادهای استاندارد صنعتی و آژانس‌های نظارتی را برآورده کنند.

چشم‌انداز بازار

انتظار می‌رود صنعت اطلاعات تهدید تا پایان سال ۲۰۳۵ به ۵۵ میلیارد دلار برسد و با نرخ رشد مرکب سالانه ۱۶ درصدی ثابت در چند سال گذشته به رشد خود ادامه دهد. صنعت اطلاعات تهدید تا سال ۲۰۲۲ حدود ۱۱ میلیارد دلار تخمین زده شد. برای جلوگیری از افزایش تعداد حملات سایبری در همه سطوح، عمدتا از اطلاعات تهدید استفاده می‌شود. تخمین زده می‌شود که هرروز حدود ۲۲۲۰ حمله سایبری رخ می‌دهد که معادل بیش از ۸۰۰ هزار حمله در سال است.

با توجه به افزایش درگیری سایبری بین مهاجمان و مدافعان، بیشتر سازمان‌ها برادغام اطلاعات تهدید و سایر اقدامات امنیت سایبری تمرکز می‌کنند، درنتیجه شرکت‌ها تشویق می‌شوند با توجه به به‌کارگیری اطلاعات تهدید، گزینه‌های امنیتی سریع‌تر و مؤثرتری ایجاد و در برابر نقض‌ها کار کنند.

نیروهای محرک در پشت رشد بازار

۱ نفوذ روزافزون خدمات اینترنتی: دیجیتالی شدن جهانی به توسعه خدمات اینترنتی منجر شده احتمال تهدیدهای سایبری را افزایش می دهد، بنابراین سیستم های کنترل ایمن مانند هوش تهدید در صنایع مستقر می شوند. تا ژانویه ۲۰۲۳ تقریبا پنج میلیارد کاربر اینترنت در سراسر جهان وجود داشت.

۲ افزایش نقض داده ها و تهدیدهای ابری: ظهور فناوری های دیجیتال تهدیدهای ابری و نقض داده ها را افزایش داده که متعاقبا به هوش تهدید برای مبارزه با سرقت داده نیاز دارد. در ۴۵ درصد موارد، نقض مبتنی بر ابر است. نظرسنجی اخیر نشان داد ۲۷ درصد از شرکت ها با یک رویداد امنیت ابر عمومی مواجه شده اند که نسبت به سال گذشته ۱۰ درصد افزایش داشته است و ۸۰ درصد از مشاغل حداقل یک حادثه امنیت ابری را در سال ۲۰۲۳ تجربه کرده اند.

۳ افزایش سیستم های صنعتی و فناوری های دیجیتال: چشم انداز فناوری به سرعت در حال تحول است که باعث انتقال جهانی در تعدادی از صنعت های عمودی شده، درنتیجه تحول صنعتی و توسعه فناوری های دیجیتال سرعت بیشتری گرفته، درنتیجه سیستم های صنعتی و فناوری های دیجیتال با هم ترکیب شده اند تا یک اکوسیستم واحد را تشکیل دهند. این پتانسیل سودآوری را برای فناوری ارتباطات IIoT و M2M ارائه می دهد. علاوه بر این استفاده از فناوری های دیجیتال در نتیجه کووید-۱۹ حتی بیشتر گسترش یافته است. طبق پیش بینی ها انتظار می رود هزینه های جهانی برای تحول دیجیتال تا سال ۲۰۲۶ به حدود ۳,۴ تریلیون دلار برسد. مجمع جهانی اقتصاد تخمین می زند تا سال ۲۰۲۵، تحول دیجیتال ۱۰۰ تریلیون دلار برای اقتصاد جهانی به ارمغان خواهد آورد. علاوه بر این قرار است تا سال ۲۰۲۵، تعاملات مبتنی بر پلتفرم تقریبا دوسوم از ۱۰۰ تریلیون دلار ارزش دیجیتالی شدن را تسهیل کند.

تحلیل منطقه ای

تجزیه و تحلیل منطقه ای برای بازار اطلاعات تهدید معمولا روندها و عوامل کلیدی مؤثر بر رشد این بخش در مناطق مختلف جغرافیایی را برجسته می کند. در اینجا به تفکیک برخی مناطق مشترک و اهمیت آنها می پردازیم.

۱ آمریکای شمالی: این کشور، دارای بازاری پیشرو در این حوزه است و آن هم به‌دلیل حضور شرکت‌های بزرگ امنیت سایبری و پذیرش زودهنگام فناوری‌های امنیتی پیشرفته شکل گرفته‌است. ابتکارات قوی دولت برای مبارزه با تهدیدهای سایبری به رشد بازار کمک می‌کند. سرمایه‌گذاری بالادر فعالیت‌های تحقیق و توسعه که به نوآوری در راه‌حل‌های اطلاعاتی تهدید منجر می‌شود.

۲ اروپا: افزایش نگرانی در مورد تهدیدهای امنیت سایبری به تقاضای بازار دامن می‌زند، به‌عنوان‌مثال آلمان تا حد زیادی از حملات باج‌افزار (۵۲٪) و حملات انکار سرویس (۴۳٪) رنج می‌برد. مقررات سختگیرانه‌ای مانند GDPR (مقررات عمومی حفاظت از داده‌ها) سازمان‌ها را به سرمایه‌گذاری در راه‌حل‌های اطلاعاتی تهدید برای انطباق سوق می‌دهد، یعنی افزایش همکاری بین دولت و نهادهای بخش خصوصی برای افزایش تاب‌آوری سایبری.

۳ آسیا اقیانوسیه: دیجیتالی شدن سریع و توسعه زیرساخت فناوری اطلاعات منجر به افزایش آسیب‌پذیری در برابر تهدیدهای سایبری می‌شود و تقاضا برای راه‌حل‌های اطلاعاتی تهدید را افزایش می‌دهد. افزایش آگاهی شرکت‌ها در مورد اهمیت امنیت سایبری رشد بازار را تقویت می‌کند. در این کشور ما شاهد افزایش سرمایه‌گذاری در امنیت سایبری توسط دولت‌ها و سازمان‌ها برای مقابله با تهدیدهای در حال تحول هستیم.

نتیجه‌گیری

یکی از مهم‌ترین عناصر دنیای دیجیتال که به‌سرعت درحال گسترش است، هوش تهدید است. تا آنجاکه به حملات سایبری مربوط می‌شود، اطلاعات تهدید به سازمان‌ها اجازه می‌دهد به‌جای واکنش‌های تقابلی، فعالانه عمل کنند. محافظت موفقیت‌آمیز در برابر حملات سایبری ممکن نیست، مگر اینکه آسیب‌پذیری‌های امنیتی، شاخص‌های تهدید و نحوه ایجاد تهدیدها را درک کنیم. اطلاعات تهدید می‌تواند به کاهش خطر حملات سایبری، تقویت وضعیت امنیتی و تسهیل توانایی تیم برای واکنش ماهرانه‌تر به موقعیت‌ها کمک کند، زیرا مهاجمان سایبری پیچیده‌تر می‌شوند.

چگونه اتوماسیون می‌تواند به بهینه‌سازی خط‌مشی امنیتی در حوزه سایبری کمک کند؟

Erez Tadmor Tufin

یکی از سؤالات تکراری که از رهبران امنیت شبکه‌ای - سایبری می‌شنویم، این است که «چرا سیاست‌های امنیتی ما بهینه نشده‌اند؟» با این حال پاسخ به این سؤال چندان ساده نیست. برای درک چگونگی حل مشکل، ابتدا باید بفهمید چه چیزی باعث ایجاد آن شده است؟

مسائل رایج سیاست امنیتی

بیایید چک‌لیستی از مسائل رایجی تهیه کنیم که می‌توانند بر پذیرش و پایبندی کلی سیاست امنیتی تأثیر بگذارند:

۱ **حجم:** یکی از مهم‌ترین چالش‌ها از حجم بسیار زیاد کنترل‌های امنیتی شبکه ناشی می‌شود. این کنترل‌ها، مانند فایروال یا گروه امنیتی، هرکدام با صدها تا هزاران قانون دسترسی تزئین شده‌اند. از آنجاکه خود قوانین اغلب در مکان‌های مختلف پراکنده می‌شوند، تنظیمات دشوار می‌شود و تیم‌ها باید تأثیر تغییر یک قانون را بر قانون دیگر در نظر بگیرند.

۲ **فرایندهای بازبینی:** بررسی دوره‌ای قوانین دسترسی، صرف‌نظر از اینکه از شبکه‌های قدیمی، ابر یا محیط‌های لبه محافظت می‌کنند، اغلب نادیده گرفته می‌شوند و

سیاست‌های امنیتی مرتبط با آنها را هم راکد و هم آسیب‌پذیر می‌کنند.

۳ تغییرات خارج از فرایند: مسئله دیگر این است که اعضای تیم گاهی اوقات بدون رعایت هیچ کنترلی، اصلاحاتی در خط مشی انجام می‌دهند. تنظیم یا به‌روزرسانی قوانین خارج از فرایند تأییدشده، نه‌تنها یکپارچگی زیرساخت امنیتی را به‌عنوان یک کل تضعیف می‌کند، بلکه آسیب‌پذیری‌های پیش‌بینی‌نشده را نیز معرفی می‌کند.

۴ تغییرات فوری: در تلاش دیوانه‌وار برای حل سریع مسائل، تغییرات گاهی با عجله و اغلب بدون تأیید یا مستندات لازم اعمال می‌شوند. بسیاری از این تغییرات ماهیت موقتی دارند، اما بازگشت به قوانین اولیه پس از این واقعیت به ندرت اتفاق می‌افتد. اتخاذ رویکرد «کمک نواری» برای تنظیم سیاست امنیتی فقط مشکل بزرگ‌تر را تشدید و ایجاد درهم‌وبرهمی و سیستم را مستعد بهره‌برداری می‌کند، زیرا تغییرات فوری به‌خوبی مستند نشده، برای همیشه فراموش نمی‌شوند یا عواقب ناخواسته‌ای دارند.

۵ مستندسازی: مستندسازی مناسب به‌عنوان کار طاقت‌فرسا درنظر گرفته می‌شود یا به‌شدت ناکافی است یا به فکر بعدی واگذار می‌شود. تیم‌های امنیتی مجبورند با وظیفه شناسایی و اصلاح پیکربندی‌های نادرست یا آسیب‌پذیری‌ها دست‌وپنجه نرم کنند، آن هم اغلب در مواقعی که سرعت بسیار مهم است. فقدان اطلاعات نه‌تنها سرعت آنها را کند می‌کند، بلکه می‌تواند مانع از توانایی آنها در درک دقیق موقعیت شود. انجام ممیزی یا تأیید انطباق با مقررات بدون اطلاعات دقیق و به‌روز شده نیز کابوسی برای تیم‌های امنیتی است.

۶ ترس: ترس غالب از برهم زدن وضعیت موجود، تیم‌ها را از حذف قوانین اضافی یا متضاد بازمی‌دارد. از آنجاکه دانش یا مستندات کمی در مورد قوانین موجود هست، احتمال ایجاد ناخواسته قطع برنامه یا شبکه بسیار زیاد است. تلاش‌های پیشگیرانه برای بهینه‌سازی قوانین اغلب به‌دلیل ترس کنار گذاشته می‌شوند یا به «مشکل فرد بعدی» تبدیل می‌شوند. درحالی‌که ضرب‌المثل «اگر خراب نیست، آن را تعمیر نکنید» می‌گوید انباشته شدن قوانین غیرضروری چهارچوب امنیتی را به هم می‌زند، ناکارآمدی آن را تشدید می‌کند و به اصطلاح در شرکت‌ها را روی مشکلات آینده باز می‌کند.

هریک از اینها می‌تواند علت چالش‌های بهینه‌سازی سیاست امنیتی باشد و منجر به مسائل امنیتی سازمانی شود که به نقض یا حمله منجر می‌شود. حقیقت وضعیت این است که بسیاری از سازمان‌ها چندین مورد از این مسائل را دارند که بر سیاست‌ها و قوانین‌شان تأثیر می‌گذارد. درعین‌حال با بودجه‌های راکد امنیتی و نبرد مداوم سازمان‌ها برای یافتن و حفظ استعدادهای امنیت سایبری، به‌راحتی می‌توان فهمید اگر این مسائل برای مدت طولانی مورد توجه قرار نگیرند، چگونه می‌توانند اثر زیادی داشته باشند؟ همچنین به‌راحتی می‌توان دریافت تیم‌های امنیتی برای غلبه بر این مسائل و ایجاد سیاست امنیتی ناب و کارآمد به کمک نیاز دارند. به همین دلیل استقبال از اتوماسیون بسیار مهم است؛ اتوماسیون برای سازمان‌های امروزی ضروری است. بدون آن، تیم‌ها نمی‌توانند روی بهینه‌سازی واقعی فرایندهای خود کار کنند.

استقبال و بهره‌گیری از اتوماسیون بسیار مهم است، اما اغلب کافی نیست. اتوماسیون امنیتی اغلب به‌عنوان راه‌حلی برای نیاز به استفاده بیشتر از منابع موجود درنظر گرفته می‌شود، درحالی‌که هنوز قادر به مبارزه خوب با مهاجمان است. فقط پیاده‌سازی ابزارهای خودکار کافی نیست، برای رسیدگی واقعی به مشکلات فوق یک بار و برای همیشه برای بهینه‌سازی سیاست‌های امنیتی خود، بهترین شیوه‌های خاصی را دنبال کنید.

بیایید به این مراحل و آنچه برای هرکدام نیاز است، نگاهی بیندازیم:

۱ شناسایی: شناسایی آغاز واقعی اتوماسیون خط مشی امنیتی است. سازمان‌ها باید سیاست‌های امنیتی موجودشان را به دقت فهرست‌بندی کنند و شبکه پیچیده قوانین و کنترل‌ها را باز کنند تا بفهمند چه چیزهایی به هم مرتبط است و مهم‌تر از همه، چرا؟! یک حسابرسی جامع به‌مثابه پایه‌ای عمل می‌کند که تلاش‌های بهینه‌سازی بعدی بر آن بنا می‌شوند. با این اوصاف دید به‌تنهایی کافی نیست تا تاثیرگذار باشد. باید پلتفرم بینش خودکار وجود داشته باشد که بتواند به

شناسایی به‌موقع جنبه‌های مختلف سیاستی کمک کند که نیاز به بهینه‌سازی دارند، برای مثال اتوماسیون می‌تواند قوانین بلااستفاده یا غیرضروری را شناسایی کند که مانع بهینه‌سازی می‌شوند و می‌توانند حذف شوند، اما به‌دلیل عدم استفاده تیم‌ها موردتوجه قرار نمی‌گرفت.

۲ ارزیابی مستمر خط‌مشی: پس از مرحله شناسایی، ارزیابی ضروری می‌شود. شرکت‌ها باید هر خط‌مشی را موردبررسی قرار دهند و ارتباط، اثربخشی و انطباق آن با استانداردهای نظارتی را ارزیابی کنند. دقیقا چه چیزی لازم است، چه چیزی نیست و چه چیزی ازدست‌رفته است؟ این ارزیابی انتقادی آسیب‌پذیری‌ها و ناکارآمدی‌ها را آشکار و راه را برای استراتژی‌های کاهش هدفمند هموار می‌کند و به ایجاد عمل انطباق مداوم یاری می‌رساند. بااین‌حال همه‌چیز عذاب و تاریکی نیست. علاوه بر اینها این فرایند می‌تواند به تیم‌ها کمک کند تا بفهمند چه چیزی به‌خوبی کار می‌کند و باید ادامه یا تکرار شود.

۳ تعریف مناسب خط‌مشی: نرده‌هایی که برای ردیابی دسترسی و تخلفات احتمالی خط‌مشی تنظیم می‌کنید باید دقیق باشند تا اطمینان حاصل شود که همه انحرافات ثبت‌شده و قابل‌رسیدگی‌اند. بدون دقت در تعاریف و قوانین، گرفتن هر چیزی که بالقوه خطرناک است، غیرممکن می‌شود و درنتیجه تلاش‌های بهینه‌سازی را محدودتر می‌کند.

۴ کاهش: کاهش زمانی است که سازمان‌ها برای اصلاح کاستی‌های شناسایی‌شده و تقویت وضعیت امنیتی خود تلاش می‌کنند. اقدامات شامل ساده‌سازی سیاست‌ها، حذف موارد اضافی، حفظ سیاست‌های مؤثر و تقویت دفاع دربرابر تهدیدهای نوظهور است. برای سازمان‌ها مهم است که هوشیار بمانند و درک کنند اقدامات آنها در اینجا پایه و اساس سیاست‌های آینده را ایجاد می‌کند.

۵ ردیابی و گزارش: ردیابی و گزارش پیشرفت به‌همان اندازه حیاتی است. شرکت‌ها باید مکانیسم‌های نظارتی قوی را برای سنجش موفقیت تلاش‌های اتوماسیون شان

به‌کارگیرند و اسناد موردنیاز برای توضیح تصمیم‌ها و بازگرداندن تغییرات- در صورت لزوم- را در اختیار آنها قرار دهند. گزارش شفاف همچنین به اطمینان از پاسخگویی و تسهیل تصمیم‌گیری آگاهانه اکنون و آینده کمک می‌کند. با پایبندی به بهترین شیوه‌ها، یک سازمان می‌تواند خود را در بهترین موقعیت ممکن برای تلاش‌های اتوماسیون قرار دهد تا در سیاست‌های امنیتی واقعا تفاوت ایجاد کند.

نگاهی به آینده

هنگامی‌که یک سازمان اشتباهات خط مشی امنیتی گذشته‌اش را تصحیح و مجموعه‌ای از قوانین و فرایندهای واقعی و کارآمد را ایجاد کرد، نبرد بعدی حفظ آن به همین شکل است. همانطور که هریک از اعضای تیم امنیتی می‌دانند، گفتن این کار آسان‌تر از انجامش است.

برای حفظ کارایی سیاست‌های امنیتی جدید، شرکت‌ها باید فرهنگ پیشگامی را پرورش دهند. ممیزی‌های منظم، بررسی‌های دوره‌ای و شیوه‌های مستندسازی دقیق غیرقابل مذاکره‌اند. علاوه بر این همکاری در داخل سازمان کلیدی است، درنتیجه تغییرات یا مسائل موردنیاز خط مشی را می‌توان بدون ایجاد مجموعه جدیدی از مسائل شناسایی و اصلاح کرد. سازمان‌ها همچنین باید درک کنند که نیازهای سیاست‌ها دائما تغییر خواهند کرد، همانطور که تهدیدات امنیتی نیز رخ می‌دهند. بهینه‌سازی خط مشی امنیتی باید به فرایندی پیوسته تبدیل شود، جایی که فناوری‌های جدید و نیازهای کارکنان با تنظیمات خط مشی تأییدشده شناسایی می‌شوند، نه تغییرات موقت.

با استقبال از اتوماسیون و پیروی از رویکرد سیستماتیک، سازمان‌ها می‌توانند مسائل مربوط به خط مشی‌ها را با اطمینان دنبال کنند. فرهنگ مدیریت سیاست پیشگیرانه و اصلاح مستمر دسترسی لازم برای موفقیت را به کارمندان می‌دهد و تضمین می‌کند دفاع دربرابر تهدیدهای همیشه درحال تحول قوی باقی بماند.

نوآوری‌های متحول‌کننده امنیت سایبری

Samridhi Agarwal

از زمانی که من در زمینه امنیت سایبری شروع به کار کردم، شرکت کردن در کنفرانس RSA آرزوی دیرینه من بود. سفر برای تحقق بخشیدن به این رؤیا، سفری به قصد شرکت در این کنفرانس، در ژانویه آغاز شد، زمانی که من لیست باورنکردنی سخنرانان و مهمانان RSA 2024 را دیدم. زمانی که برای جایزه زنان جوان در حوزه سایبر انتخاب شدم، این اتفاق از رؤیاهایم هم فراتر رفت و این فرصت شگفت‌انگیز را به من داد تا در RSA شرکت کنم، آن هم در سال ۲۰۲۴ با پاس پرس.

بله، یک پاس مطبوعاتی!

برای آماده شدن کنفرانس، در مورد فناوری‌های مختلف مطالعه و تقویمم را برنامه‌ریزی کردم تا از این تجربه حداکثر استفاده را ببرم. بااین‌حال هنگامی‌که وارد شدم، دریافتم که هیچ آمادگی‌ای نمی‌تواند با مقیاس رویداد برابری کند. این نمایشگاه عظیم بود؛ نمایشگاهی با سازمان‌هایی که راه‌اندازی‌هایشان را میزبانی می‌کردند، با ظاهری چشمگیر و افراد شگفت‌انگیز بی‌شماری برای گفت‌وگو. درحالی‌که

همه چیز در کنفرانس جذاب بود، من از کار چند سازمان در عرصه سایبری به‌طور ویژه لذت بردم و دوست داشتم درباره تلاش‌های پیشگامانه‌ای بیشتر بدانم که تیم‌هایشان در این زمینه انجام می‌دهند. از توسعه فناوری‌های امنیتی پیشرفته گرفته تا پیشگامی روش‌های جدید برای حفاظت از زیرساخت‌های دیجیتال، این سازمان‌ها در خط مقدم امن‌تر کردن زندگی دیجیتالی ما هستند. در این گزارش مختصر، به برخی از افراد شگفت‌انگیزی می‌پردازم که با آنها صحبت کردم و سازمان‌هایی که آنان نمایندگی می‌کنند.

HORIZON3.ai انقلابی در تست نفوذ با nodezero

در گفت‌وگو با اسنهال آنتانی، بنیانگذار و مدیرعامل HORIZON3.ai بررسی کردیم که چگونه سازمان‌ها دائما در معرض تهدید حملات پیچیده مانند باج‌افزارها و سایر عوامل مخربند. روش‌های سنتی تست نفوذ اگرچه مؤثرند، اغلب همراه با کار فشرده، پرهزینه و زمانبرند و ادامه دادن به آنها را برای کسب‌وکارها چالش‌برانگیز می‌سازند. HORIZON3.ai با راه‌حل پیشگامانه‌اش به این مسئله حیاتی می‌پردازد.

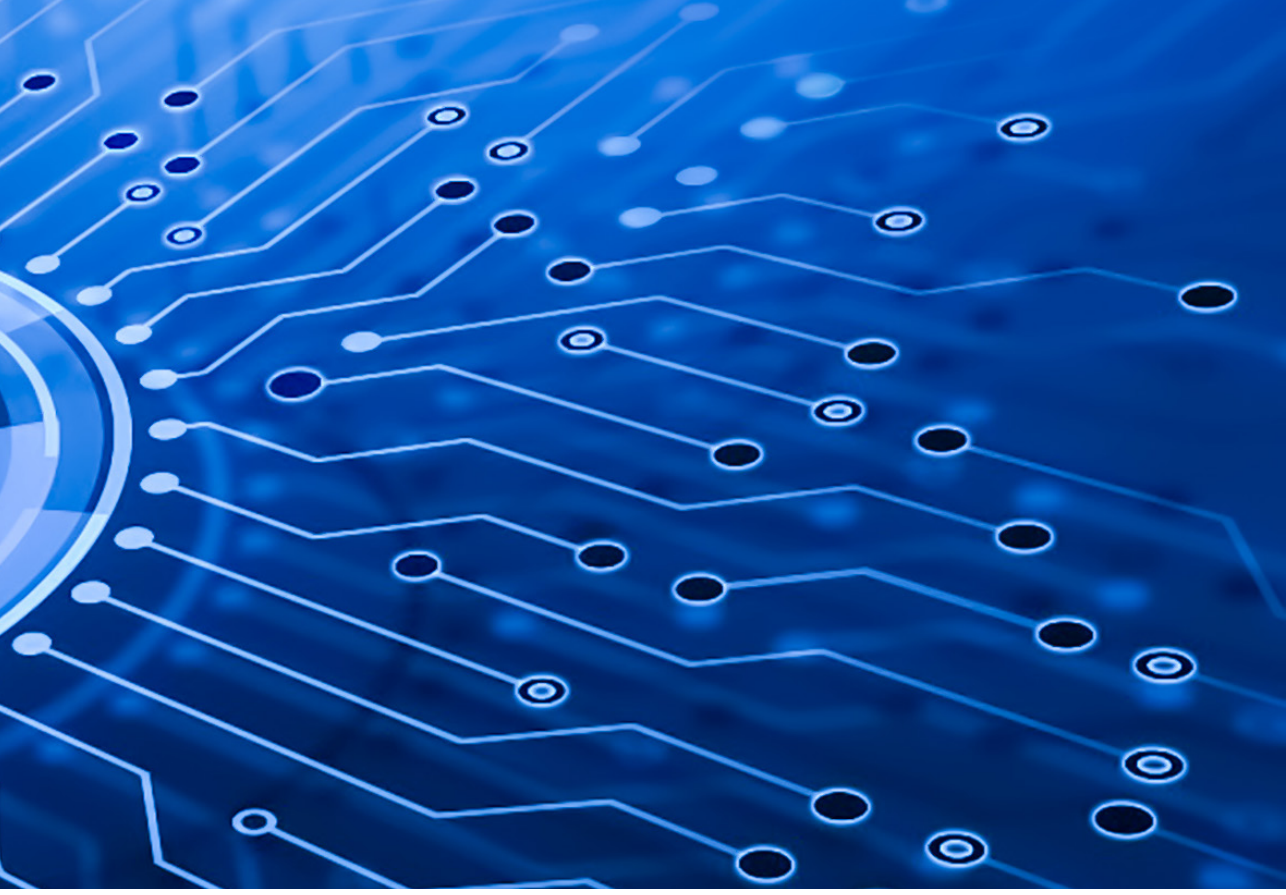
NodeZero پلتفرم تست نفوذ خودکار است که تخصص انسانی را با اتوماسیون ماشین ترکیب می‌کند. این پلتفرم بسیاری از جنبه‌های زمانبر تست نفوذ را خودکار می‌کند و به متخصصان انسانی اجازه می‌دهد روی وظایف و تحلیل‌های پیچیده‌تر تمرکز کنند. مضاف بر اینکه گزارش‌هایی دقیق را همراه با اطلاعات اصلاحی ارائه می‌دهد که رسیدگی به آسیب‌پذیری‌ها و پیروی از استانداردهای صنعت را برای سازمان‌ها آسان‌تر می‌کند و به‌وضوح توالی وقایعی را توضیح می‌دهد که منجر به تأثیرات حیاتی می‌شوند، همچنین اثبات بهره‌برداری و توضیحات مفصلی از اصلاحات لازم را ارائه می‌دهند. یکی از ویژگی‌های داشبورد- که به‌طور خاص آن را دوست داشتم- طراحی‌اش است که برای کاربران در همه سطوح مهارت، از متخصصان فناوری اطلاعات اولیه گرفته تا آزمایش‌کننده‌های باتجربه ارائه می‌شود. NodeZero تست نفوذ را در دسترس و کارآمد می‌کند.

اسنهال آنتانی گفت: «ما راه‌حل دیگری برای هوش‌مصنوعی نمی‌سازیم. این سیستم مستقلی است که رویکرد تیمی انسان و ماشین را مجسم می‌کند. این پلتفرم شفافیت و دید را در عملیات‌های درحال انجام ارائه و به مشتریان امکان می‌دهد ماژول‌های درحال اجرا، مشکلات کشف‌شده و اتصالات شبکه را در زمان واقعی نظارت کنند.»

پلتفرم HORIZON3.ai در رویکرد سازمان‌ها به امنیت سایبری، انقلابی ایجاد کرده است. با ارائه آزمایش‌های نفوذ مستمر و مستقل، به سازمان‌ها کمک می‌کند به‌طور فعال آسیب‌پذیری‌ها را شناسایی و برطرف کنند و از دفاعی قوی دربرابر تهدیدات سایبری پیچیده اطمینان حاصل کنند. با ویژگی‌های نوآورانه و طراحی کاربرپسند، تعیین معیارهای جدید در صنعت امنیت سایبری، سازمان‌ها را قادر می‌سازد به‌شکل مؤثری دارایی‌های دیجیتال خود را ایمن کنند.

مشتریان Horizon3.ai را به‌دلیل تأثیر تحول‌آفرین NodeZero بر استراتژی‌های امنیت سایبری خود تحسین کرده‌اند. یک متخصص ارشد امنیت و ریسک فناوری اطلاعات به اشتراک گذاشت: «این پلتفرم به سازمان ما توانایی‌ای را داده که آزمایش نفوذ را به روشی قابل‌اعتماد، تکرارپذیر و مقرون‌به‌صرفه انجام دهد. بینش‌هایی که از این پلتفرم به‌دست می‌آوریم در تقویت وضعیت امنیتی ما بسیار ارزشمند است.»

به‌طورکلی هدف ایجاد انقلابی در فرایند تست نفوذ داخلی با ارائه راه‌حلی کارآمدتر، دقیق‌تر و مطمئن‌تر است که تخصص انسانی را با اتوماسیون ماشین ترکیب می‌کند، درحالی‌که سطح حمله را به حداقل



می‌رساند و برای اصلاح به مشتریان گزارش‌های دقیق و عملی ارائه می‌دهد.

امنیت: RAD انقلابی در امنیت ابری با رویکرد پیشگیرانه

در گفت‌وگو با بروک موتا، مدیرعامل و یکی از بنیانگذاران RAD Security ما به این موضوع پرداختیم که چگونه RAD Security درحال تغییر تشخیص و پاسخ به رخنه ابری است. این شرکت به‌عنوان موسسه‌ای در جهت تشخیص و پاسخ مبتنی‌بر ابر رفتاری، منبع نهایی حقیقت را برای رخنه‌های ابری با اثرانگشت رفتاری فراهم می‌کند، یعنی به‌طور فعالانه از محیط‌های منحصربه‌فرد اثرانگشت می‌گیرد و امکان شناسایی حملات جدید را در زمان واقعی فراهم می‌کند.

رویکردهای سنتی برای امنیت ابری اغلب بر شناسایی میلیون‌ها امضای حمله احتمالی تکیه می‌کنند که هم زمانبر و هم ناکارآمد است. RAD Security با مشاهده رفتار خوب شناخته‌شده و علامت‌گذاری هرگونه انحراف به‌عنوان مورد مشکوک، رویکرد متفاوتی درپیش می‌گیرد، به‌عنوان مثال انگشت‌نگاری sshd با RAD می‌تواند حمله XZ Backdoor را بلافاصله شناسایی کند.

RAD Security راه‌حل جامع سه در یک را ارائه می‌دهد، آن هم با تمرکز بر مناطق حیاتی که امروزه توسط مهاجمان هدف قرار می‌گیرند؛ زیرساخت‌های بومی ابر، هویت و زنجیره تأمین نرم‌افزار. این رویکرد کل‌نگر سازمان‌ها را قادر می‌سازد اثرانگشت زمان اجرا را در خطوط لوله زنجیره تأمین خود تعبیه و حملات جدید را درطول زمان اجرا شناسایی و افراد مخرب خود را پیدا کنند و برنامه‌های امنیتی Shift-Let شان را تقویت کنند. همانطور که بروک موتا تأکید کرد ایمن‌سازی محیط‌های بومی ابری به حیاتی‌ترین وظیفه برای CISO تبدیل شده است،

زیرا این محیط‌ها زیربنای پیشرفت‌های عظیم در هوش‌مصنوعی (AI) هستند. برای ایمن‌سازی هوش‌مصنوعی، ایمن‌سازی محیط‌های اصلی ابری ازجمله کانتینرها و Kubernetes ضروری است. آمار قانع‌کننده است؛ ۷۰٪ از تیم‌ها درحال حاضر از کانتینرها در تولید بهره می‌برند و تحلیلگران پیش‌بینی می‌کنند تا سال ۲۰۲۵، ۹۵٪ از برنامه‌های جدید با استفاده از بارهای کاری بومی ابری ساخته خواهند شد.

مشتریان RAD Security این پلتفرم را به‌دلیل تأثیر متحول‌کننده‌اش بر استراتژی‌های امنیت ابری خود تحسین کرده‌اند. زمانی که بروک موتا نیز بر اهمیت تنوع و گنجاندن در امنیت سایبری تأکید کرد، شخصا جذب آن شدم و فرهنگ حمایت از زنان در این زمینه را تحسین کردم. RAD Security با ارائه رویکرد پیشگیرانه برای امنیت ابری خود را متمایز و سازمان‌ها را قادر می‌کند تا حملات را در صورت وقوع- به‌جای تکیه بر روش‌های شناسایی واکنشی و مبتنی‌بر امضا- شناسایی و به آنها پاسخ دهند.

Zentera Systems: پیشگام امنیت و اعتماد برای شرکت‌های مدرن

در چشم‌انداز دیجیتال امروزی، جایی که محیط‌های سنتی شبکه به‌طور فزاینده‌ای متخلخل شده‌اند، شرکت‌ها با چالش دلهره‌آوری روبه‌رو هستند؛ ایمن کردن دارایی‌ها و داده‌های حیاتی خود دربرابر تهدیدات سایبری پیچیده. هکرها می‌توانند از راه‌های مختلف به محیط شرکت نفوذ کنند و وقتی وارد می‌شوند، زمان کافی برای مطالعه سازمان و ایجاد حملات سفارشی دارند که دفاع دربرابر آنها دشوار است. عواقب حمله سایبری موفقیت‌آمیز می‌تواند ویرانگر باشد، با هزینه‌هایی که اغلب بیش از ۱۰۰ میلیون دلار برای جبران حمله‌ای بیشتر می‌شود که در یک آخر هفته رخ می‌دهد.

Zentera Systems راه‌حل تغییردهنده بازی برای این مشکل ارائه می‌دهد.

CoIP Zero Trust Fabric: همانطور که با جاوشین لی، رئیس و مدیرعامل شرکت صحبت شد، این راه‌حل مشخصات NIST SP800-207 را برای معماری Zero Trust پیاده‌سازی می‌کند و به‌طور مؤثری از دارایی‌ها و داده‌ها دربرابر باج افزار، حملات جانبی، تهدیدات داخلی و نشت داده‌ها دفاع می‌کند.

CoIP Zero Trust Fabric یک‌لایه جدید از محافظت‌های ضدهوا را در اطراف دارایی‌ها و داده‌های حیاتی به‌کار می‌گیرد و اطمینان می‌دهد هر دسترسی به شبکه شناخته‌شده و مجاز است. این رویکرد فعالانه با حفاظت از امنیت سایبری مؤثر، رفع محدودیت‌های فایروال‌های شبکه سنتی، ابزارهای تشخیص تهدید و نظارت و تهدیدهای دارایی‌های حیاتی را خنثی می‌کند. آنچه Zentera را متمایز می‌کند سرعت و سادگی بی‌نظیر و چابکی باورنکردنی آن در به‌کارگیری امنیت Zero Trust است. همانطور که جاوشین لی تأکید می‌کند «پلتفرم CoIP ما شبکه، امنیت و اتصال چند ابری برنده جایزه Zero Trust را فراهم می‌کند که در بالای هر زیرساخت در هر محیط پراکنده‌ای قرار می‌گیرد و به مشتریان اجازه می‌دهد در کمتر از یک روز راه‌اندازی و کار کنند.»

Zentera Systems به رهبری در راه‌حل‌های اتصال ایمن و چابک برای شرکت‌های دیجیتالی تبدیل شده است.

یک تجربه مهم در کنفرانس RSA 2024

به‌طور خلاصه، کنفرانس RSA 2024 شگفت‌انگیز بود. من نمی‌توانم به‌اندازه کافی از مجله دفاع سایبری برای این فرصت باورنکردنی تشکر کنم. این واقعا مانند جشنواره‌ای بود که در آن همه با یک هدف مشترک متحد شده بودند؛ ایمن کردن فضای دیجیتال ما و پیش بردن مرزهای فناوری. از دیدن تلاش‌های جمعی بسیاری از ذهن‌های درخشان برای تبدیل هفته RSA به یک موفقیت مطلق، شگفت‌زده شدم. از راه‌اندازی محصولات پیشگامانه گرفته تا جلسات روشن‌فکرانه و رویدادهای شبکه‌ای جذاب، به‌سادگی شگفت‌انگیز بود. الهام‌بخش بود که از نزدیک شاهد اشتیاق، خلاقیت و عزم تزلزل‌ناپذیر رهبران صنعت و نوآورانی باشم که خستگی‌ناپذیر برای تقویت دفاع دیجیتال ما تلاش می‌کنند. من کنفرانس را با احساسی تازه از هیجان و خوش‌بینی نسبت به امکانات بی‌حدوحصری ترک کردم که در فضای همیشه درحال تحول امنیت سایبری درپیش است.

اطلاع‌نگاشت

مهم‌ترین نقاط عطف امنیت سایبری جهان در چند سال گذشته

باگسترش اینترنت، شبکه‌ها و دستگاه‌های پیچیده، عبارت مهمی که باید در نظر داشت این است: هرگز امنیت آنلاین را دست کم نگیرید. حوزه فناوری اطلاعات و امنیت سایبری به رشد خود ادامه می‌دهد و ادامه خواهد داد تا از سیستم‌ها در برابر سرقت داده‌ها، حملات سایبری، دسترسی به خطر افتاده و سایر آسیب‌ها محافظت کند. با این حال تنها کسب و کارها و سازمان‌ها نیستند که باید اهمیت امنیت سایبری را تشخیص دهند. تاریخ نشان داده حتی دولت‌ها و نهادهای دولتی نیز از ارتکاب کاستی‌های امنیت سایبری مصون نیستند. تاریخچه امنیت سایبری به دهه ۱۹۷۰ بازمی‌گردد. در این اینفوگرافی، روی برخی از برجسته‌ترین رویدادهای تاریخ امنیت سایبری در چند سال گذشته تمرکز خواهیم کرد.

۲۰۱۱

سال تبلیغاتی مهمی برای شرکت الکترونیکی سونی بود، هرچند که خوب پیش نرفت و سونی به یکی از نمونه‌های حمله سایبری در این دهه تبدیل شد

شبکه پلی‌استیشن (PSN)، یا همان سرویس بازی آنلاین سونی، در آوریل ۲۰۱۱ مورد حمله قرار گرفت. طی این حمله، اطلاعات کاربری ۷۷ میلیون کاربر از جمله نام، رمز عبور، ایمیل و موارد دیگر فاش شد. پلتفرم PSN سونی که قادر به کنترل گسترش نفوذ نبود، به واسطه همین حمله سایبری ۲۳ روز دچار اختلال شد. Sony Online Entertainment (سازنده و ناشر بازی این شرکت) و Qriocity (سرویس استریم سونی) نیز یک ماه تعطیل شدند. سونی نه تنها توسط مقامات در بریتانیا به دلیل رویدادهای فوق ۴۰۰ هزار دلار جریمه شد، بلکه این شرکت مجبور به پرداخت غرامت

۲۰۱۱

شبکه پلی‌استیشن سونی و سونی پیکچرز حملات متعددی را متحمل شدند

به بازیکنان آسیب دیده در قالب کالاهای دیجیتال هم شد! با این حال مشکلات سونی در آن سال هنوز تمام نشده بود که دومین نقض امنیتی را این بار توسط گروه هکرهای LulzSec تجربه کرد. هکرها گفتند اسامی، جزئیات کارت اعتباری و سایر اطلاعاتی که از وب سایت‌های سونی پیکچرز سرقت کرده‌اند، رمزگذاری نشده بوده‌اند. طبق بیانیه مطبوعاتی LulzSec، «سونی بیش از یک میلیون رمز عبور مشتریان خود را به صورت متن ساده ذخیره کرده است ... و این به معنی آن است که فقط باید آنها را دریافت کنید. بدون اینکه نیاز به پیچیدگی خاصی باشد».

۲۰۱۲

نقض داده‌های سیستم‌های پرداخت جهانی

در آوریل ۲۰۱۲، سیستم‌های پرداخت جهانی، با حمله سایبری عظیمی مواجه شد. global payment system از بزرگ‌ترین ارائه دهندگان سیستم پرداخت شخص ثالث است. در ابتدا تخمین زده شد که ۱٫۵ میلیون حساب افشا شده‌اند. با این حال گزارش‌های خبری بیشتر حاکی از آن است که تعداد حساب‌هایی که در این حمله، اطلاعاتشان فاش شده می‌تواند به هفت میلیون برسد. در نتیجه این شرکت هزینه هنگفتی معادل ۹۳٫۹ میلیون دلار را متحمل شد.

۲۰۱۳

حملات سایبری به دولت سنگاپور

Anonymous یکی از نمادین‌ترین گروه‌های هک در جهان از اوایل دهه ۲۰۰۰ بود. این گروه هکری، یک گروه هکتیویست بین‌المللی بود که در سال ۲۰۰۳ شروع به کار کرد و مسئول چندین حمله سایبری پرمخاطب علیه دولت‌ها و سازمان‌های بزرگ را برعهده گرفته بود. این گروه در سال ۲۰۱۳ مجموعه‌ای از حملات سایبری را علیه دولت سنگاپور آغاز کرد. یکی از دلایل این حملات ظاهرا سانسور وب سازمان دولتی سنگاپور بود.

۲۰۱۳

حمله سایبری هماهنگ سالانه #OpIsrael

#OpIsrael حمله «ضد اسرائیل» و سایبری هماهنگ و سالانه است که توسط هکتیویست‌ها نسبت به دولت و وب سایت‌های خصوصی اسرائیل انجام می‌شود. اولین #OpIsrael در سال ۲۰۱۳ توسط Anonymous در آستانه روز یادبود هولوکاست انجام شد.

2013

باوجوداینکه Adobe یکی از شناخته شده‌ترین نام‌ها در نرم‌افزار است، در اکتبر ۲۰۱۳ اعلام کرد سیستم آن به طور گسترده هک شده است. بیش از ۳۸ میلیون کاربر و بیش از ۱۵۲ میلیون رکورد شکسته شده در این حادثه دخیل بودند. برای انجام این هک، عاملان از شیوه‌های رمزگذاری ضعیف Adobe استفاده کردند، اما این همه ماجرا نبود؛ هکرها همچنین توانستند بیش از ۴۰ گیگابایت کد منبع را برای سه برنامه Adobe به دست آورند .ColdFusion ،Acrobat و Builder ادوبی در نهایت به دلیل این حادثه یک میلیون دلار جریمه شد.

2013

ادوارد اسنودن اسناد طبقه‌بندی شده NSA را افاش کرد

ادوارد اسنودن قبلا کارمند سیا (آژانس اطلاعات مرکزی آمریکا) بود اما تا سال ۲۰۱۳ که به دلیل اقدام بسیار بحث برانگیز افشای اطلاعات محرمانه امنیت سایبری از NSA (آژانس امنیت ملی) بدنام شد. در سال ۲۰۱۳، دو خبرگزاری برجسته - واشنگتن پست و گاردین - اسناد به دست آمده اسنودن را منتشر کردند. این نشریات اطلاعات هک شده گسترده‌ای را افشا کردند که توسط NSA انجام شده بود.

2013 و 2014

Yahoo! دچار نقض گسترده داده‌ها می‌شود

در اواخر سال ۲۰۱۴، شرکت اینترنتی پیشگام Yahoo! یکی از بزرگ‌ترین (اگر نگوییم بزرگ‌ترین) نقض داده در تاریخ را تجربه کرد. در این حمله درمجموع ۵۰۰ میلیون کاربر یاهو! در معرض خطر قرار گرفتند. همه اکانت‌ها - نام، رمز عبور، پاسخ به سؤالات امنیتی - به سرقت رفتند. همچنین گزارش جداگانه‌ای وجود دارد که Yahoo! پیش از این در سال ۲۰۱۳ نیز در معرض چنین اتفاقی قرارگرفت. برآورد اولیه اکانت‌های نقض شده در این حادثه خاص یک میلیارد کاربر را شناسایی کرد. بعدا یاهو تأیید کرد تعداد کل کاربران تحت تأثیر این نقض درواقع سه میلیارد بوده‌اند. بدتر آنکه Yahoo! این تخلفات را تا سال ۲۰۱۶ گزارش نکرد. کمیسیون بورس و اوراق بهادار (SEC) یاهو را جریمه کرد؛ ۳۵ میلیون دلار برای گزارش نابهنگام. در ادامه بیش از ۴۰ شکایت دسته جمعی علیه Yahoo! صورت گرفت. این اتفاقات پی درپی همچنین قیمت فروش شرکت را حدود ۳۵۰ میلیون دلار کاهش داد.

2013 و 2014

داده‌های کارت اعتباری Target به سرقت رفت

تا دسامبر ۲۰۱۳، زمانی که داده‌های کارت اعتباری و نقدی متعلق به خریداران تارگت در Rescator - یک فروشگاه جرائم سایبری اوکراینی - ظاهر شد، دنیای امنیت سایبری متوجه شد که اتفاقی بسیار بزرگ در راه است. در طول تعطیلات شکرگزاری نوامبر ۲۰۱۳، سیستم نقطه فروش Target به بدافزار آلوده شد. مشتریانی که بین ۲۷ نوامبر تا ۱۵ دسامبر ۲۰۱۳ خرید کردند، تحت تأثیر این بدافزار قرار گرفتند. به واسطه این اتفاق، داده‌های ۱۱۰ میلیون مصرف‌کننده تارگت، ازجمله داده‌های پین، نام، شماره کارت اعتباری/دبیت و تاریخ انقضا فاش شدند.

2014

سونی ضربه دیگری را با حمله به سونی پیکچرز اینترتینمنت وارد کرد

سه سال پس از تخلفات سونی در سال ۲۰۱۱، سونی ضربه دیگری خورد. گروه Guardians of Peace مدعی شد شبکه Sony Pictures Entertainment را هک کرده است. آنها ۱۰۰ ترابایت داده را دزدیدند که شامل فیلمنامه، ایمیل و اطلاعات شخصی کارکنان سونی بود. سونی مجبور شد پخش برخی فیلم‌های خود را لغو کرده و به کارمندان فعلی و سابقش غرامت پرداخت کند.

2015

نقض داده‌های Experian ۱۵ میلیون رکورد را به خطر انداخت

Experian در سال ۲۰۱۵ از نقض داده‌هایش خبر داد و اطلاعات حساس حدود ۱۵ میلیون نفر را به خطر انداخت که برای سرویس مخابراتی T-Mobile درخواست سیم‌کارت و خطوط اعتباری کرده بودند. Experian یکی از سه دفتر اعتباری ایالات متحده است.

2015

اطلاعات شخصی کاربران اسنپ‌چت افشا شد

در سال ۲۰۱۵، هکرها نام کاربری، شماره تلفن و مکان ۴٫۶ میلیون حساب کاربری اسنپ‌چت را منتشر کردند. این موضوع هزاران کاربر اسنپ‌چت را نگران کرد، به خصوص کسانی که از این برنامه برای به اشتراک‌گذاری تصاویر شخصی خود استفاده می‌کنند. گفته می‌شود به اسنپ‌چت از سوی هکرها برای رفع این آسیب‌پذیری هشدار داده شده است، اما این شرکت اقدامی نکرده است.

2015 تا 2016

ویکی‌لیکس و کمیته ملی دموکرات

گروه‌های جاسوسی سایبری روسی Cozy Bear و Fancy Bear ایمیل‌های کمیته ملی دموکرات (DNC) را هک کردند. چرا آنها این کار را کردند؟ تحلیلگران گفتند این اقدام احتمالا تلاشی برای تأثیرگذاری بر انتخابات ریاست جمهوری ۲۰۱۶ ایالات متحده بوده است. این حملات سایبری ظاهرا بین سال‌های ۲۰۱۵ و ۲۰۱۶ اتفاق افتاده است. هکرها توانستند به شبکه‌های DNC دسترسی پیدا کنند که منجر به نقض گسترده داده‌ها شد. براساس تحقیقات، افراد خاصی ایمیل‌های سرقت شده را در اختیار ویکی‌لیکس قرار دادند. ویکی‌لیکس سپس این اسناد را منتشر کرد. ادعا می‌شود این رویداد یکی از مهم‌ترین افشاگری‌های بدنام در تاریخ اخیر ایالات متحده است.

2015

دفتر مدیریت پرسنل (OPM) متحمل نقض قابل توجه داده شد

در آوریل ۲۰۱۵، دفتر مدیریت پرسنل ایالات متحده (OPM) متوجه شد که هک شده است. این حادثه یکی از مهم‌ترین نقض‌های اطلاعات دولتی در تاریخ ایالات متحده شناخته شد. براساس تحقیقات OPM و یک تیم بین‌سازمانی، «اطلاعات حساس، ازجمله شماره‌های تأمین اجتماعی (SSNs) ۲۱٫۵ میلیون نفر، از پایگاه‌های تحقیقاتی سوابق به سرقت رفته است...» این نقض همچنین شامل یافته‌های مصاحبه‌های انجام شده توسط بازرسان پیشین دولت و تقریبا ۵٫۶ میلیون اثرانگشت بود. گمان می‌رود این هک توسط هکرهای چینی انجام شده باشد. البته که چین هرگونه دخالت در این حمله سایبری را رد کرده است.

2015

هکرهای اشلی مدیسون نشانی ایمیل کاربران را منتشر کردند

گروه هکر The Impact Team در جولای ۲۰۱۵ به وب‌سایت همسریابی اشلی مدیسون نفوذ کرد. این سایت توسط RubyCorp مدیریت می‌شود که قبلا AvidLifeMedia بود. به گفته هکرها، آنها نه‌تنها داده‌های شرکت، بلکه داده‌های ۳۷ میلیون کاربر را نیز گرفته‌اند. هکرها برای اثبات حرف خود، ایمیل مدیرعامل شرکت را منتشر کردند. آنها حتی تهدید کردند اطلاعات کاربران را منتشر خواهند کرد، مگر اینکه سایت بسته شود. اما AvidLifeMedia به این هشدار توجه نکرد.

2017

اولین باج‌افزار در جهان WannaCry

WannaCry | اولین «باج‌افزار» جهان، ۲۳۰ هزار رایانه تحت ویندوز را در ۱۵۰ کشور تحت تأثیر قرارداد.

2016

قوانین عمومی حفاظت از داده‌ها (GDPR) توسط اتحادیه اروپا تصویب شد

این اتفاق، یعنی تصویب قوانین عمومی حفاظت از داده‌ها، نقض امنیتی یا حمله سایبری نیست، با وجود این یک نقطه عطف مهم است. مقررات عمومی از داده‌ها (GDPR) در آوریل ۲۰۱۶ در اتحادیه اروپا تصویب شد. این قوانین به‌طور کامل از اواسط سال ۲۰۱۸ اجرا شده است. یکی از الزامات اولیه GDPR این است که سازمان‌ها ملزم به داشتن یک افسر حفاظت از داده‌ها (DPO) هستند.

2017

NotPetya

باج‌افزار NotPetya بیش از ۱۲۵۰۰ رایانه را تحت تأثیر قرار داد. NotPetya، کسب‌وکارهای جهانی مهمی را ازجمله شرکت‌های کشتیرانی برجسته Maersk و FedEx، شرکت نفت و گاز روسیه Rosneft و تبلیغ‌کننده بریتانیایی WPP را هدف قرار گرفت. درواقع فدرال اکسپرس ادعا کرد در این حمله ۳۰۰ میلیون دلار ضرر کرده است.

2017

Bad Rabbit Masquerades as a Adobe Flash Update

باج‌افزار دیگری که در سال ۲۰۱۷ خبرساز شد، خرگوش بد بود که با تظاهر به یک به‌روزرسانی Adobe Flash، به رایانه‌ها نفوذ کرد. این باج‌افزار، این کار را از طریق وب‌سایت‌های رسانه‌ای در معرض خطر انجام می‌دهد. این نوع باج‌افزار حدود ۲۰۰ هدف را در روسیه و بلغارستان تحت تأثیر قرار داد.

2018

فیس‌بوک درگیر نگرانی‌های حفظ حریم خصوصی است

ازنظر حملات سایبری و نقض اطلاعات، سال ۲۰۱۸ شاهد چندین حادثه قابل توجه بود. غول رسانه‌های اجتماعی، فیس‌بوک، به سرعت به یکی از بحث‌برانگیزترین نمونه‌های نقض اطلاعات تبدیل شد. در سال ۲۰۱۸، این رسانه به دلیل انعقاد قراردادی با تولیدکنندگان لوازم الکترونیکی برای دسترسی به اطلاعات کاربران، تحت تحقیقات پلیس فدرال قرار گرفت. بعدا فیس‌بوک با چندین نقض امنیتی مورد حمله قرار گرفت. یکی از این موارد مربوط به شرکت تحلیلی کمبریج آنالیتیکا بود که به داده‌های بیش از ۸۷ میلیون کاربر دسترسی داشت؛ بسیار بیشتر از ۵۰ میلیون کاربری که در ابتدا گزارش شده بود.

2017

Uber

هکرها ۵۰ میلیون نام، آدرس خانه، شماره تلفن همراه و ایمیل افرادی را به سرقت بردند که کاربران اوبر بودند! همچنین آنها گواهینامه رانندگی و سایر اطلاعات هفت میلیون راننده را نیز داشتند. بدتر از همه، اوبر ۱۰۰ هزار دلار به هکرها پرداخت تا این حمله سایبری و هک بزرگ را پنهان کنند. شرکت شبکه حمل‌ونقل این امر را تا نوامبر ۲۰۱۷ فاش نکرد. این موضوع خشم مشتریان را برانگیخت و باعث شد سناتور آمریکایی لایحه‌ای را ارائه کنند که به موجب آن مدیران شرکت‌هایی که تخلف را پنهان می‌کنند، محکوم به زندان شوند.

2018

جزئیات حساب ۹۲ میلیون کاربر MyHeritage به خطر افتاد

در اواسط سال ۲۰۱۸، وب‌سایت شجره‌شناسی آنلاین MyHeritage اعلام کرد یک نقض امنیتی را تجربه کرده است. هکر به آرشیوی حاوی اطلاعات حساب حداقل ۹۲ میلیون کاربر MyHeritage دسترسی پیدا کرد. خوشبختانه بایگانی فقط حاوی ایمیل‌ها و رمزهای عبور بود، بدون جزئیات حساب مالی یا آزمایش DNA!

2018

حمله سایبری هتل‌های ماریوت

نقض‌های اطلاعاتی می‌توانند برای مدت طولانی قبل از اینکه کشف شوند، خاموش بمانند و این همان چیزی است که در مورد هتل‌های ماریوت رخ داد. زمانی که پایگاه داده هتل‌های استارووود به خطر افتاد، اطلاعات شخصی حدود ۵۰۰ میلیون میهمان ماریوت را فاش کرد. بازرسان دولت ایالات متحده به طور فزاینده‌ای بر این باورند که هکرهای دولتی چین مسئول این نفوذ بوده‌اند. وزارت امور خارجه چین هرگونه اطلاع از این موضوع را رد کرد. این شرکت به دلیل کوتاهی در محافظت از اطلاعات مشتریان با جریمه ۱۲۳ میلیون دلاری مواجه شد که دومین جریمه بزرگی است که توسط قانونگذاران بریتانیا در تابستان ۲۰۱۹ صادر شد.

2018

حمله سایبری بریتیش ایرویز

۱۵ ماه پس از وجود نقض در سیستم بریتیش ایرویز در فرودگاه هیترو، این شرکت هواپیمایی به دلیل حملات سایبری بین آگوست تا سپتامبر ۲۰۱۸ از مشتریان عذرخواهی کرد. حدود ۵۰۰ هزار پرداخت کارتی در این حادثه تحت تأثیر قرار گرفتند. هکرها اسامی، ایمیل ها، آدرس ها و شماره کارت های اعتباری و سایر داده ها را سرقت کردند. بریتیش ایرویز با پرداخت جریمه ۲۳۰ میلیون دلاری GDPR که حدود ۱٫۵ درصد از درآمد سال ۲۰۱۷ آن است تنبیه شد.

2019

نقض در بخش های بهداشتی سنگاپور

سنگاپور پیش از سال ۲۰۱۹ به وسیله دو حمله سایبری آسیب دیده بود. در ماه ژانویه، اطلاعات شخصی ۸۰۸ هزار اهداکننده خون در اینترنت پیدا شد. گزارش شده که داده ها توسط SecurSolutionsGroup، فروشنده اداره علوم بهداشتی سنگاپور (HSA) به اشتباه استفاده شده است. داده های ارسال شده شامل نام، شماره کارت شناسایی، جنسیت، تاریخ سه اهدای اخیر و در برخی موارد گروه خونی، قد و وزن بوده است. ژانویه به پایان نرسیده بود که حادثه دیگری رخ داد. این بار وضعیت اچ آی وی ۱۴۲۰۰ نفر در فضای مجازی به بیرون درز کرد. عامل افشای اطلاعات Mikhy Farrera بود که درنهایت در دادگاه ایالات متحده به دلیل تلاش برای اخاذی از دولت سنگاپور در مورد این اطلاعات مجرم شناخته شد. او از طریق شریک زندگی خود، لرتک سیانگ، پزشک سابق و مدیر واحد ملی بهداشت عمومی وزارت بهداشت، به رجیستری اچ آی وی دسترسی پیدا کرده بود.

2020

توییتر!

شوک دیگری که به دنیا وارد شد، هدف قرار گرفتن حساب های توییتری چندین شخصیت معروف دنیا توسط مجرمان سایبری بود. مهاجمان توانستند با ورود به حساب های آنها بسیاری از دنبال کنندگان شان را فریب دهند و از طریق بیت کوین به کلاهبرداری اقدام کنند.

2021

مایکروسافت!
حملات سایبری گسترده به سرورهای مایکروسافت

در مارس ۲۰۲۱، حمله امنیتی دیگری نیز رخ داد که طی آن دست کم هزاران نفر از مشتریان مایکروسافت اعم از سازمان های تجاری و دولتی هک شدند. ظاهرا این حملات از ژانویه توسط گروه های APT چینی انجام شده اند. دست کم یکی از گروه های APT موسوم به HAFNIUM با استفاده از این آسیب پذیری به سرورهای پیش فرض Exchange و سپس اکانت های ایمیلی دست یافتند و بک دورهایی برای یافتن دسترسی به محیط قربانیان کار گذاشتند. به نقل از کارشناسان سازمان امنیتی Volexity حملات در ژانویه آغاز شد، اما در ماه مارس شدت یافت. به دنبال این موضوع کارشناسان حجم آسیب هایی را بررسی کردند که به سرورهای مشتریان وارد شده بود. شرکت مایکروسافت حملات سایبری به سرورهای Exchange را تأیید کرد و بیان داشت که این حملات با هدف سرقت ایمیل ها و نصب دائمی بدافزار در شبکه های قربانیان بوده است.

2022

اوکراین در بحبوحه جنگ روسیه

زیرساخت های حیاتی اوکراین بار دیگر خود را در تیررس عوامل تهدید قرار داد. در اوایل تهاجم روسیه، محققان ESET از نزدیک با CERT-UA برای اصلاح حمله ای همکاری کردند که شبکه کشور را هدف قرار داده و شامل بدافزار مخربی بود که Sandworm سعی کرده بود علیه پست های برق با ولتاژ بالا مستقر کند. این بدافزار در ترکیب با نسخه جدیدی از نوع مخرب CaddyWiper مورد استفاده قرار گرفت که به احتمال زیاد رد های گروه را پنهان می کند و سرعت حادثه را کاهش می دهد.

2023

بازهم مایکروسافت!
(مایکروسافت CloudEmailBreach)

گمان می رود نفوذ گسترده به اکانت های ایمیل ابری مایکروسافت متعلق به چندین آژانس دولتی ایالات متحده که در ماه ژوئن کشف شد، بر ایمیل های جینا ریموند و وزیر بازرگانی و همچنین نیکلاس برنز سفیر ایالات متحده در چین و مقامات وزارت بازرگانی تأثیر گذاشته است. براساس گزارش ها، در مجموع ۶۰ هزار ایمیل از ۱۰ دپارتمان ایالات متحده به سرقت رفته است. این حادثه سناتور آمریکایی ران وایدن را وادار کرد تحقیقات فدرال را برای تعیین اینکه آیا اقدامات امنیتی ضعیف توسط مایکروسافت منجر به هک شده است یا خیر را پیگیری کند. همچنین منجر به انتقاد بسیاری از مدیران برجسته در صنعت امنیت شد. در ماه سپتامبر مایکروسافت فاش کرد مسائل دیگری را شناسایی کرده که عامل تهدید مرتبط با چین ردیابی شده با عنوان Storm-0558 را قادر می سازد حساب های ایمیل ابری مقامات آمریکایی را مورد تهدید قرار دهد.

درنهایت اما باید دوباره مرور کرد که چرا امنیت سایبری مهم است؟

دهه گذشته، دهه ای پرآشوب در دنیای امنیت سایبری بوده است. همانطور که هکرها به طور فزاینده ای اقدامات پیچیده حمله را توسعه می دهند، شرکت ها در هر اندازه باید آماده دفاع و محافظت از داده های خود در برابر حملات سایبری جدی تر در سال های آینده باشند.

سند راهبردی پدافند سایبری کشور

کمیته دائمی (شـــورای عالـــی) پدافند غیرعامل کشـــور در جلســـه مورخ ۱۳۹۴/۰۲/۲۹ به استناد ماده (۸) اساسنامه سازمان پدافند غیرعامل کشور مصوّب مقام معظم رهبری و فرماندهی کل قوا(مدظله‌العالی)، «سند راهبردی پدافند سایبری کشور» پیشنهادی سازمان پدافند غیرعامل کشور، موضوع بند ۱ ماده ۹ اساسنامه مذکور را بررسی و تصویب نمود.

ماده ۱: تعاریف و اصطلاحات

- فضای سایبری
- سرمایه ملی سایبری
- آسیب‌پذیری سایبری
- تهدید سایبری
- تهاجم سایبری
- جنگ سایبری
- زیست بوم سایبری
- سامانه‌های پایه سایبری
- دیپلماسی پدافند سایبری
- پدافند سایبری
- نظام جامع بومی پدافند سایبری

ماده ۲: چشم‌انداز پدافند سایبری کشور

۱ نظام جامع بومی پدافند سایبری هوشمند، پایدار و مقاوم، انحصاری، ابتکاری، لایه به لایه، شبکه‌ای، چابک و منعطف در سطوح ملی، دستگاهی و استانی

۲ نظـــام مدیریت و کنترل جامع و هوشمند با قابلیت رصد، پایش، تشخیص، هشدار و مدیریت و کنترل بهنگام صحنه عملیات پدافند سایبری

۳ مصونیت در زیرساخت‌های حیاتی، استحکام و پایداری در زیرساخت‌های حساس و امنیت و ایمنی در زیرساخت‌های مهم

۴ سرمایه‌های انسانی مؤمن، متعهد مجرب، آمـــوزش دیده و متخصص در حوزه پدافند سایبری و دارای تفکر بسیجی و روحیه جهادی

۵ نظام دیپلماسی پدافند سایبری فعال، متعامل، مشارکت‌جو و مدافع منافع ملی سایبری

۶ صنعت بومی پدافند سایبری روزآمد، رقابتی و پاسخگو به تهدید، خوداتکا و اقتصادی در تولید سامانه‌های پایه پدافند سایبری با بهره‌گیری از ظرفیت‌های کشور

۷ استانداردها و الگوهای پدافند سایبری بومی، امن، پویا و روزآمد

۸ جایگاه ممتاز علمی و فناورانه در حوزه پدافند سایبری منطقه

۹ توانمندی مدیریت بحران سایبری در راستای تداوم خدمات‌رسانی ضروری

۱۰ نظام نهادینه شده آموزش و فرهنگ سازی پدافند سایبری در متن فرهنگ عمومی و نظام آموزشی کشور

۱۱ مشارکت ظرفیت بخش‌های دولتی، غیردولتی، مردم نهاد و بسیج در پدافند سایبری

۱۲ نظام تولید، حفظ و ارتقاء آمادگی‌های پدافند سایبری در برابر تهدیدات

ماده ۳: ارزش‌های اساسی حاکم بر حوزه پدافند سایبری کشور

- خودباوری و خوداتکایی
- اعتماد سازی
- اطمینان بخشی
- نوآوری و خلاقیت
- اخلاق اسلامی
- نفی سلطه دشمن
- فرهنگ و ارزش‌های اسلامی
- مدیریت جهادی
- تفکر و عمل بسیجی

ماده ۴: اصول حاکم بر حوزه پدافند سایبری کشور

- مصون سازی و پایداری
- وحدت مدیریت
- بازدارندگی
- حفظ آمادگی
- پیش‌بینی در تهدید شناسی
- اقتصادی سازی (رعایت صرفه و صلاح)
- اشراف اطلاعاتی
- دیپلماسی فعال
- اقتدار درون‌زا

ماده ۵: رسالت پدافند سایبری کشور

- پدافند سایبری از سرمایه‌های ملی سایبری و فضای سایبری کشور در برابر تهدیدات و حملات سایبری دشمن

قرارگاه پدافند سایبری کشور رسالت مصون سازی و پایدارسازی سامانه‌های سایبری کشور از طریق رصد، پایش و تشخیص تهدیدات، کشف، مدیریت و کنترل آسیب‌پذیری‌ها، اعلام هشدارهای لازم، اطمینان از پدافند سایبری، تدوین و انتشار نظامات (ملاحظات، مقررات، الزامات و اصول) پدافندی، آموزش و نهادینه‌سازی پدافند سایبری، مدیریت عملیات پدافند سایبری و دفاع حقوقی در برابر تهدیدات و حملات دشمن را بر عهده دارد.

ماده ۶: مأموریت‌های عمده قرارگاه پدافند سایبری کشور

۱. هدایت، راهبری، نظارت و هماهنگی فرماندهی عملیاتی پدافند سایبری از زیرساخت‌های اساسی کشور متناسب با سطح اهمیت

۲. رصد، پایش و تشخیص تهدیدات سایبری دشمن و هشدار و تعیین وضعیت آن

۳. هدایت و راهبری ایجاد توانمندی‌ها و ظرفیت‌های احتیاط راهبردی برتر ساز در حوزه پدافند سایبری

۴. هدایت و راهبری پدافند سایبری هوشمند، چندلایه و اثربخش از سرمایه‌های سایبری کشور

۵. هدایت و راهبری کنترل عملیاتی پدافند سایبری در سطوح ملی، منطقه‌ای و دستگاهی

۶. هدایت و راهبری ایجاد و ارتقاء نظام جامع پدافند سایبری کشور

۷. هدایت و راهبری ایجاد و ارتقاء آمادگی پدافند سایبری در دستگاه‌های اجرایی ملی و استانی، بخش غیردولتی و آحاد جامعه

۸. هدایت و راهبری مصون سازی، پایدارسازی و استحکام زیست بوم سایبری و سرمایه‌های ملی سایبری کشور

۹. نظارت و حصول اطمینان از تولید و به‌کارگیری سامانه‌های پایه و اساسی پدافند سایبری کشور

۱۰. هدایت و راهبری جلب مشارکت ظرفیت‌های بخش‌های دولتی، غیردولتی، مردم و به ویژه بسیج در پدافند سایبری

۱۱. هدایت و راهبری ایجاد و ارتقاء ظرفیت‌های صنعت بومی دفاع سایبری کشور (دولتی و غیردولتی)

۱۲. نهادینه سازی اصول، الزامات و ملاحظات فنی پدافند سایبری در متن برنامه‌ها و طرح‌های توسعه سایبری کشور

۱۳ هدایت و راهبری توسعه و پایدارسازی معماری پدافند سایبری در زیرساخت‌های دارای اهمیت

۱۴ نهادینه سازی آموزه‌های پدافند سایبری در متن برنامه‌های آموزشی و فرهنگ سازی کشور در سطوح مختلف

۱۵ هدایت و راهبری ایجاد و ارتقاء نظام اطلاع‌رسانی و عملیات روانی در فضای سایبری در برابر دشمن

۱۶ هدایت و راهبری آموزش‌های تخصصی تربیت نیروی انسانی متخصص در حوزه پدافند سایبری

۱۷ هدایت و راهبری تولید و مدیریت دانش در حوزه پدافند سایبری

۱۸ هدایت و راهبری دیپلماسی پدافند سایبری

ماده ۷ : اهداف کلان در افق چشم‌انداز پدافند سایبری کشور

- دستیابی به نظام جامع بومی پدافند سایبری
- دستیابی به زیرساخت‌ها و سرمایه‌های ملی مصون سایبری
- دستیابی به زیست بوم سایبری امن، مصون و پایدار
- دستیابی به منابع انسانی توانمند و کارآمد پدافند سایبری
- دستیابی به جایگاه ممتاز علمی و فناوری پدافند سایبری منطقه
- دستیابی به صنعت بومی خوداتکا و پیشرفته پدافند سایبری
- دستیابی به استانداردها و الگوهای پدافند سایبری بومی، امن، پویا و روزآمد
- دستیابی به دیپلماسی فعال پدافند سایبری
- دستیابی به ظرفیت مناسب فرماندهی و کنترل پدافند سایبری
- نهادینه سازی فرهنگ، ادبیات و آموزه‌های پدافند سایبری
- دستیابی به مشارکت ظرفیت‌های بخش‌های دولتی و غیردولتی در حوزه پدافند سایبری
- حفظ و ارتقاء آمادگی‌های پدافندی سایبری در برابر تهدیدات

ماده ۸ : راهبردهای پدافند سایبری کشور

۱ طراحی، پیاده‌سازی و راهبری نظام جامع بومی پدافند سایبری هوشمند، پایدار و مقاوم، انحصاری، ابتکاری، لایه به لایه، پیشگیرانه، شبکه‌ای، چابک و منعطف در سطوح ملی، دستگاهی و استانی

۲ طراحی، پیاده‌سازی و راهبری طرح‌ها و برنامه‌های پدافند سایبری از زیرساخت‌های کشور برای مصون‌سازی زیست بوم سایبری در برابر تهدیدات و تهاجم سایبری متناسب با سطح اهمیت آن‌ها

۳ الزام و همراه سازی سازمان‌های متولی زیرساخت‌های حیاتی و حساس کشور در استفاده از محصولات سایبری امن بومی

۴ به‌کارگیری منابع انسانی متخصص و امین با ساماندهی و ارتقای کمی و کیفی در حوزه پدافند سایبری

۵ تولید و مدیریت دانش و فناوری پدافند سایبری متناسب با تهدیدات

۶ بومی و امن سازی سامانه‌های سایبری مورد استفاده در زیرساخت‌های حیاتی و حساس کشور با تأکید بر ممنوعیت کاربرد سامانه‌های خارجی در آنها (در جهت کاهش وابستگی به فناوری‌ها و محصولات غیربومی)

۷ ساماندهی و تقویت صنعت پدافند سایبری بومی و حمایت از سازمان‌ها و شرکت‌های تولیدکننده دولتی و غیردولتی و محصولات بومی و روزآمد

۸ سازماندهی، حمایت و صیانت از تولید امن داخلی سامانه‌های پایه و اساسی پدافند سایبری کشور

۹ بومی سازی فرایندها، نظام‌ها و استانداردها، پروتکل‌های فنی، رویه‌ها و روال‌های پدافند سایبری

۱۰ طراحی، پیاده‌سازی و راهبری نظام دیپلماسی پدافند سایبری کشور

۱۱ طراحی، پیاده سازی و راهبری سامانه فرماندهی و کنترل پدافند سایبری

۱۲ فرهنگ سازی و آموزش تخصصی و عمومی مسئولین و نخبگان و آحاد جامعه در حوزه پدافند سایبری

۱۳ نهادینه سازی آموزه‌های پدافند سایبری در نظام آموزشی (ابتدایی، متوسطه و دانشگاهی) و نظام آموزش دفاعی کشور

۱۴ بهره‌گیری از قابلیت‌های سازمان بسیج مستضعفین و سازمان‌های مردم نهاد و ظرفیت‌های بخش غیردولتی در پدافند سایبری

۱۵ مدیریت بر ارتقاء ضریب پایداری، مصون سازی، ارتقاء توان بازدارندگی زیرساخت‌های حیاتی و حساس کشور در برابر تهدیدات و حملات سایبری

۱۶ حفاظت و تأمین امنیت هوشمندانه سایبری از زیرساخت‌ها و طرح‌ها متناسب با سطح اهمیت آنها

۱۷ استفاده هوشمندانه (توجه به فرصت‌ها و تهدیدات فناوری‌ها) از سامانه‌های جدید سایبری در زیرساخت‌های دارای اهمیت

۱۸ مشارکت در تدوین راهبردها علیه تهدیدات مشترک نظامی و سایبری

۱۹ راهبری، هدایت، ایجاد هماهنگی و هم‌افزایی راهبرد محور پدافند سایبری در کلیه دستگاه‌های اجرایی

۲۰ طراحی و پیاده‌سازی و راهبری نظام جامع رصد، پایش، تشخیص و هشدار در مقابل تهدیدات سایبری دشمن

نظام آمادگی و رزمایش دستگاه‌های اجرایی در برابر تهدیدات

چهل و پنجمین جلسه کمیته دائمی (شورای عالی) پدافند غیرعامل کشور به استناد ماده ۸ اساسنامه سازمان پدافند غیرعامل کشور مصوّب مقام معظّم رهبری و فرماندهی کلّ قوا (مد ظله العالی) در تاریخ ۱۳۹۹/۰۶/۲۵ تشکیل و نظام آمادگی و رزمایش دستگاه‌های اجرایی در برابر تهدیدات موضوع مادّه نه اساسنامه، پیشنهادی آن سازمان را بررسی و به شرح زیر تصویب نمود:

نظام آمادگی و رزمایش دستگاه‌های اجرایی در برابر تهدیدات

ماده ۱: تعاریف و اختصارات

مربوط به اصطلاحات و واژگان به‌کار رفته در این سند است که با مراجعه به اصل سند آن را مطالعه نمایید.

ماده ۲: اسناد بالادستی

- رهنمودها، احکام، منویّات و تدابیر مقام معظّم رهبری (مدظله‌العالی)
- سیاست‌های کلی نظام در موضوع پدافند غیرعامل ابلاغی مقام معظّم رهبری (مدظله‌العالی)
- قانون احکام دائمی برنامه‌های توسعه کشور
- قانون برنامه پنج‌ساله ششم توسعه جمهوری اسلامی ایران
- اساسنامه سازمان پدافند غیرعامل کشور
- سند راهبردی پدافند غیرعامل کشور
- سند تقسیم کار ستادکل نیروهای مسلح و قرارگاه مرکزی خاتم الانبیاء(ص) برای شرایط جنگ (بخش پدافند غیرعامل)

ماده ۳: دامنه شمول

دستگاه‌های اجرایی موضوع ماده۵ قانون مدیریت خدمات کشوری، نیروهای مسلح و آحاد مردم مشمول این نظام‌نامه می‌باشند.

ماده ۴: هدف

ارزیابی آمادگی دستگاه‌های اجرایی موضوع ماده۳ این نظام‌نامه در برابر حوادث، تهدیدات و اقدامات خصمانه دشمن در راستای ارتقاء پایداری، تاب‌آوری و تداوم کارکردهای ضروری کشور و صیانت از مردم با تاکید بر اجرای رزمایش‌های پدافند غیرعامل

ماده ۵: منظور

- ارتقای آمادگی‌های سازمانی، مدیریتی، تجهیزاتی، نیروی انسانی و برنامه‌ای در تمام ابعاد (بخشی، گروهی، موضوعی)
- الزام دستگاه‌های اجرایی مشمول این نظام‌نامه به تدوین طرح‌های پاسخ به تهدیدات و حوادث
- شناسایی آسیب‌پذیری‌ها و نقاط ضعف و اقدام برای رفع آنها با اصلاح و به‌روزرسانی طرح‌ها و دستورالعمل‌های آمادگی
- ارزیابی میزان اثربخشی و کارایی برنامه آمادگی مقابله دستگاه‌های اجرایی برای شرایط بحران ناشی از جنگ

ماده ۶: تهدیدات محتمل

الف) تهدیدات شیمیایی ب) تهدیدات پرتوی
ج) تهدیدات زیستی د) تهدیدات سایبری/
الکترونیک و الکترومغناطیس ه) تهدیدات نظامی و
امنیّتی و) تهدیدات ترکیبی

ماده ۷: چرخه آمادگی

گام‌های چرخه آمادگی عبارتند از؛
۱) طراحی ۲) سازماندهی ۳) آموزش ۴) تجهیز
۵) تمرین ۶) رزمایش (اجرا) ۷) ارزیابی و
مستندسازی ۸) بازخورد و اصلاح
۹) به‌روزرسانی طرح‌ها

ماده ۸: گام‌های رزمایش

۱) تهیه برنامه و تعیین اعتبارات رزمایش
۲) برآورد تهدیدات و تعیین سناریو پایه
۳) طراحی (طرح پاسخ)
۴) بررسی، تائید و تصویب طرح رزمایش
۵) آموزش عمومی و تخصّصی نیروهای رزمایش
۶) تجهیز ابزار و تجهیزات طرح رزمایش
۷) تمرین و مهارت افزایی
۸) اجرای رزمایش میدانی
۹) نظارت، ارزیابی و بازخورد
۱۰) اصلاح و تکمیل و به‌روزرسانی طرح ها

ماده ۹: الزامات آمادگی و اجرای رزمایش

۱) مدیریت و فرماندهی
۲) سازماندهی
۳) طرح‌ریزی
۴) زیرساخت
۵) تجهیزات
۶) مهارت
۷) هماهنگی و ارتباطات
۸) نظارت، ارزیابی و مستندسازی
۹) بودجه و اعتبارات

ماده ۱۰: نقش‌ها و مسئولیت‌ها

مسئولیت اجرا، هدایت و راهبری، نظارت و ارزیابی و تصویب طرح‌های رزمایش در سطوح مختلف آن، برابر جدول زیر تعیین می‌گردد؛

سطوح رزمایش	مسئولیت اجرا	تصویب طرح	هدایت و راهبری	نظارت و ارزیابی
فراملی	دولت/ دستگاه اجرایی	شورای عالی امنیت ملی	سازمان	کمیته دائمی
ملی	دولت/ دستگاه اجرایی	کمیته دائمی	سازمان	کمیته دائمی/ دستگاه اجرایی
منطقه ای	وزارت کشور/ سازمان	سازمان/کمیته دائمی	سازمان	سازمان/ وزارت کشور
استانی	استاندار	سازمان	استاندار	سازمان
دستگاهی	رئیس دستگاه اجرایی	سازمان	سازمان/ دستگاه اجرایی	سازمان/ استانداری/ وزارت کشور
محلی	مسئول دستگاه استانی	استاندار	فرماندار/ شهردار	سازمان/ مدیرکل پدافند استان
مشترک	دستگاه اجرایی/ سازمان	کمیته دائمی/ سازمان	کمیته دائمی/ سازمان	سازمان

ماده ۱۱: تکالیف و وظایف

۱ دستگاه‌های اجرایی مشمول این نظام‌نامه که دارای زیرساخت‌ها و مراکز ویژه، حیاتی، حساس، مهم و قابل حفاظت هستند به‌طور سالانه موظّف به اجرای حداقل یک رزمایش تخصّصی پدافند غیرعامل در هریک از انواع ستادی (دورمیزی) و میدانی هستند.

۲ استانداران و دستگاه‌های اجرایی استانی موظّفند نسبت به انجام رزمایش‌های پدافند شیمیایی، پدافند پرتوی، پدافند زیستی و پدافند مردم محور به صورت سالانه - حداقل یکبار- برابر چرخه رزمایش و آمادگی اقدام نمایند.

۳ دستگاه‌های اجرایی موظفند تقویم رزمایش‌های سالانه پدافند غیرعامل خود را به سازمان ارسال نمایند، رزمایش‌های سالانه پدافند غیرعامل در سطوح ملی و منطقه‌ای برای مراکز ویژه، حیاتی و حساس، پس از تصویب در کمیته دائمی جهت اجرا به دستگاه‌های اجرایی ابلاغ می‌گردد. تبصره: تقویم رزمایش‌های سالانه پدافند غیرعامل در سایر سطوح و مراکز توسط سازمان تصویب و ابلاغ می‌گردد.

۴ سازمان ضمن ارزیابی، هدایت و کنترل رزمایش‌های پدافند غیرعامل در کشور، گزارشی از میزان آمادگی دستگاه‌های اجرایی در برابر تهدیدات و تعیین نقاط ضعف و قوت آنها بصورت نوبه‌ای به کمیته دائمی، ستاد کل نیروهای مسلح و شورای عالی امنیّت ملی ارسال کرده و برنامه‌ی اجرایی رفع اشکالات و نواقص را به دستگاه اجرایی ذی‌ربط ارائه نماید. گزارش میزان آمادگی استان‌ها و شهرستان‌ها و دستگاه‌های اجرایی مستقر در آنها، به روسای کمیته پدافند غیرعامل استان و دستگاه اجرایی نیز ارائه می‌گردد.

۵ سازمان موظف است دستورالعمل‌ها و ضوابط اجرایی رزمایش‌های پدافند غیرعامل در انواع و سطوح مختلف و شیوه‌نامه طراحی و سناریونویسی رزمایش‌های تخصّصی پدافند غیرعامل را تدوین و ابلاغ کند.

۶ سازمان موظّف است با همکاری دستگاه‌های اجرایی ملی و استانی، رزمایش فراملی در زیرساخت‌های مشترک با کشورهای همسایه را طرح‌ریزی نماید؛ رزمایش‌های فراملی در قالب همکاری‌های مشترک آمادگی و مقابله با تهدیدات و حوادث شیمیایی، پرتوی، میکروبی و زیستی در چارچوب سیاست‌های دفاعی با تصویب شورای عالی امنیّت ملی و نظارت کمیته دائمی، توسط سازمان هدایت، طرح‌ریزی، آموزش و ارزیابی می‌گردد. تبصره: وزارت امور خارجه موظف است نسبت به ایجاد هماهنگی با کشورهای مشارکت‌کننده اقدام نموده و همکاری و مشارکت لازم را با سازمان در اجرای رزمایش‌های فراملی به انجام رساند.

۷ وزارت دفاع و پشتیبانی نیروهای مسلح - سازمان پژوهش‌های نوین دفاعی (سپند)- به‌عنوان مرکز اقدام و عمل کلی قرارگاه‌های تخصّصی پدافند غیرعامل (پدافند پرتوی، پدافند شیمیایی، پدافند زیستی) موظّف است از توانمندی‌ها و ظرفیّت‌های تولید تجهیزات و لوازم موردنیاز متناسب با طرح‌های آمادگی و رزمایش، پشتیبانی و حمایت نماید.

۸ وزارت بهداشت، درمان و آموزش پزشکی موظّف به ارتقاء آمادگی زیرساخت‌های بهداشتی و درمانی کشور و افزایش توانمندی و تاب‌آوری شبکه تجهیزاتی و نیروی انسانی برای مقابله و پاسخ درچارچوب طرح‌های مصوّب آمادگی و رزمایش، متناسب با انواع تهدیدات و مخاطرات شیمیایی، زیستی و پرتوی می‌باشد.

۹ وزارت جهاد کشاورزی موظّف به ارزیابی زیرساخت‌های رصد و پایش تهدیدات حوزه ماموریت خود، ارتقاء آمادگی تجهیزاتی و نیروی انسانی، افزایش پایداری و تداوم کارکردهای اساسی درچارچوب طرح‌های مقابله و پاسخ، تداوم کارکرد، حفاظت از زیرساخت، صیانت از مردم و سایر طرح‌ها در حوزه‌های غذا، دام و نباتات با اجرای رزمایش‌های تخصّصی پدافند غیرعامل می‌باشد.

۱۰ وزارت راه و شهرسازی موظّف به ایجاد زیرساخت‌ها و تجهیزات لازم در حوزه‌های حمل و نقل، هواشناسی و مانند آن به منظور ارتقاء آمادگی‌ها در اجرای رزمایش‌های پدافند غیرعامل حوزه‌های پرتوی، شیمیایی، زیستی و نظامی درچارچوب طرح‌های پاسخ و تداوم کارکرد قرارگاه‌های تخصّصی می‌باشد.

۱۱ سازمان بسیج مستضعفین موظّف است نسبت به سازماندهی ساختارهای پدافند شیمیایی، زیستی، پرتوی، مردم محور و تامین تجهیزات لازم در سازمان بسیج اقدام کند و ظرفیّت‌های نیروی بسیج در دستگاه‌های اجرایی و سایر اقشار را در چارچوب طرح‌های آمادگی و رزمایش پدافند غیرعامل، سازماندهی و آموزش داده و در رزمایش‌ها به صورت فعّال شرکت نماید.

۱۲ نیروی انتظامی جمهوری اسلامی ایران (ناجا) موظّف است با ایجاد زیرساخت‌های لازم و تامین تجهیزات موردنیاز، آمادگی‌های کافی برای مقابله با تهدیدات و مخاطرات شیمیایی، پرتوی و زیستی درچارچوب طرح‌های آمادگی و پاسخ ایجاد نموده و با آموزش‌ها و تمرینات لازم و تخصّصی در رزمایش‌های پدافند غیرعامل مشارکت و همکاری نماید.

۱۳ سازمان صدا و سیما و مراکز استانی تابعه، ضمن ارتقاء آمادگی‌های درون سازمانی در برابر تهدیدات، مسئول آگاهی‌بخشی، اطلاع‌رسانی و اجرای آموزش‌های عمومی موردنیاز و مناسب برای اجرای رزمایش در جامعه مخاطب پیرامون محیط رزمایش هستند.
راه‌اندازی رادیو رزمایش جهت آموزش محدود پدافند غیرعامل در حوزه‌های تخصّصی (شیمیایی، پرتوی و زیستی) و توجیه افکار عمومی در اجرای رزمایش‌ها ضرورت داشته و مورد تاکید است.

۱۴ استانداران موظّفند درچارچوب برنامه‌های امنیّتی- دفاعی استان نسبت به سازماندهی قرارگاه‌های استانی پدافند شیمیایی، پرتوی، زیستی، سایبری و مردم‌محور و تهیّه طرح‌های پاسخ، تداوم کارکردها، حفاظت از زیرساخت‌ها، صیانت از مردم و برنامه‌های آمادگی و رزمایش استانی اقدام نمایند.
وزارت کشور مسئول سیاست‌گذاری امنیّتی، هدایت و پشتیبانی استان‌ها در اجرای رزمایش‌ها بوده و هماهنگی بین استان‌ها در رزمایش‌های ملی و منطقه‌ای را ایجاد نماید.

۱۵ دستگاه‌های اجرایی و نهادهای عمومی موظّفند در حوزه وظایف و ماموریت‌های قانونی خود، نسبت به ارتقاء آمادگی درون سازمانی با اجرای طرح‌های پاسخ، تداوم کارکردها، حفاظت از زیرساخت‌ها و صیانت از مردم درچارچوب دستورالعمل‌های سازمان عمل نمایند و با طرح‌ریزی و برنامه‌ریزی سالانه، رزمایش‌های پدافند غیرعامل را اجرا کرده و نسبت به اصلاح و رفع اشکالات و نواقص کشف شده از رزمایش‌ها در قالب برنامه‌های جاری و سالانه اقدام و گزارش اجرای آن را به سازمان ارائه کنند.

۱۶ دستگاه‌های اجرایی موظفند هرگونه قصور و کوتاهی در مصون‌سازی و ایجاد آمادگی و مقابله با تهدیدات و انجام رزمایش‌های پدافند غیرعامل در قالب این نظام‌نامه در زیرساخت‌ها و مراکز حیاتی و حساس و مهم که احتمال وقوع مخاطرات امنیّتی در آن وجود دارد به سازمان پدافند غیرعامل گزارش نمایند.

۱۷ سازمان پدافند غیرعامل مکلّف است به‌عنوان راهبر، هادی و ناظر اجرای مقرّرات و ضوابط پدافند غیرعامل گزارش تخلّفات صورت گرفته را به مراجع قضایی ذی‌ربط اعلام نماید.

۱۸ قـوه قضاییـه هرگونـه کوتاهی در انجام اقدامات ایجاد و حفظ آمادگی دسـتگاه‌ها که منجر به ایجاد مخاطرات امنیّتی می‌گردد، به تشخیص سازمان، پیگیری قضایی نموده و وفق مقرّرات و قوانین امنیّتی و دفاعی اقدام کند.

۱۹ سـازمان بازرسـی کل کشور اجرای برنامه رزمایش سالانه دسـتگاه‌های اجرایی را در برنامه‌های بازرسی برنامه‌ریزی شده سالانه درج نموده و نتایج آن را به سازمان و کمیته دائمی گزارش نماید.

۲۰ رزمایش‌های مشترک در قالب برنامه سالانه رزمایش‌های پدافند غیرعامل کشور با پیشنهاد سازمان یا دستگاه‌های اجرایی به تصویب رئیس ستاد کل نیروهای مسلح و کمیته دائمی می‌رسد و با هماهنگی کامل فیمابین حوزه‌های لشکری و کشوری اجرا می‌شوند.

ماده ۱۲

سازمان با همکاری دستگاه‌های اجرایی ذی‌ربط، اسناد تفصیلی، دستورالعمل‌ها و طرح‌هـای عملیاتـی موردنیـاز بـرای پیاده‌سازی سـایر گام‌های آمادگی این نظـام را تهیه و به دسـتگاه‌های اجرایی ابلاغ می‌نماید.

ماده ۱۳

سازمان مسئول نظارت بر حسن اجرای این نظام‌نامه بوده و هر نوع اصلاح و بازنگری برای آن، با پیشنهاد سازمان به تصویب کمیته دائمی می‌رسد.

ماده ۱۴

این تصویب‌نامه در چهارده ماده و شصت و سه بند و سه تبصره در چهل و پنجمین جلسه کمیته دائمی به تاریخ بیست و پنجم شهریورماه سال یکهزار و سیصد ونود و نه هجری شمسی به تصویب رسید.

نظام عملیاتی پدافند سایبری کشور

به استناد ماده ۸ اساسنامه سازمان پدافند غیرعامل کشور مصوّب مقام معظّم رهبری و فرماندهی کلّ قوا (مدظله‌العالی) در تاریخ ۱۳۹۸/۰۲/۳۱ سی و چهارمین جلسه کمیته دائمی (شورای عالی) پدافند غیرعامل کشور تشکیل و نظام عملیاتی پدافند سایبری کشور موضوع مادّه نه اساسنامه، پیشنهادی آن سازمان را بررسی و تصویب نمود.

نظام عملیاتی پدافند سایبری کشور

ماده ۱: تعاریف و اختصارات

مربوط به اصطلاحات و واژگان به‌کار رفته در این سند است که با مراجعه به اصل سند آن را مطالعه نمایید.

ماده ۲: اسناد بالادستی

- فرامین، تدابیر و رهنمودهای مقام معظم رهبری (مدظله‌العالی)
- سیاست‌های کلی نظام در حوزه پدافند غیرعامل
- قانون برنامه ششم توسعه کشور (مواد ۱۰۶، ۱۰۷ و ۱۰۹)
- اساسنامه سازمان پدافند غیرعامل کشور
- تدابیر مقام معظم رهبری (مد ظله العالی) در هیئت عالی سایبری
- سند راهبردی پدافند غیرعامل کشور
- سند راهبردی پدافند سایبری کشور

ماده ۳: قلمرو

الف) زیرساخت‌های فضای سایبری کشور
ب) دارایی‌ها و سرمایه‌های ملی سایبری و وابسته به سایبر در زیرساخت‌های ویژه، حیاتی، حساس و مهم

ماده ۴: هدف

تدوین نظام عملیاتی پدافند سایبری کشور و تعریف عناصر اصلی مشارکت‌کننده در عملیات پدافند سایبری در برابر تهاجم دشمنان و تعیین روابط، نقش‌ها و وظائف آنها درجهت هماهنگی و هم‌افزائی و اثربخشی هرچه بیشتر بین کنشگران در عملیات پدافند سایبری.

ماده ۵: اصول عملیاتی پدافند سایبری کشور

۱) صیانت ۲) ممانعت ۳) مانایی ۴) یکپارچگی ۵) مشارکت و هم‌افزایی ۶) دفاع جمعی ۷) آمادگی ۸) انطباق‌پذیری ۹) تاب‌آوری ۱۰) آگاهی وضعیتی ۱۱) آینده‌نگری (پیش‌بینی) ۱۲) پیش‌کنش‌گری

۱) پرهیز از هرگونه غافلگیری
۲) تناسب اقدام‌های پدافند سایبری، با ویژگی‌های کلیدی اهمیت سرمایه سایبری، تهدید سایبری، آسیب‌پذیری سایبری، مخاطره‌سایبری، تهاجم سایبری دشمن و پیامدهای سایبری، شناختی و فیزیکی ناشی از جنگ سایبری
۳) اتکاء به توان داخلی، محصولات بومی و به‌ویژه معماری پدافندی اختصاصی (بومی)
۴) عدم اعتماد به سامانه‌ها و خدمات خارجی
۵) تمرکز بر عملیات پدافند سایبری بر اساس اولویت پیش‌بینانه، پیش‌گیرانه، پیش‌کنشگرانه، واکنش‌گرایانه و منفعلانه
۶) صیانت از دارایی‌های معنوی و افکار عمومی، دارایی‌های شبکه‌ای - جزیره‌ای، سامانه‌های کنترل صنعتی و دارایی‌های سایبری
۷) تمرکز بر مواجهه با عملیات ترکیبی دشمن از طریق فضای سایبر بر اساس اولویت مواجهه با عملیات ترکیبی سایبری - اجتماعی، سایبری - فیزیکی و سایبری - سایبری
۸) کاهش حداکثری و مداوم آسیب‌پذیری، تهدید، خطای پیش‌بینی، زمان تشخیص و واکنش
۹) افزایش حداکثری و مداوم زمان دسترسی و دستیابی دشمن به آسیب‌پذیری سایبری، سرعت پیش‌بینی، تداوم کارکردهای ضروری و دقّت پاسخ

ماده۶: سیاست‌های عملیاتی پدافند سایبری

عملیات پدافند سایبری، در عمق فضای سایبر خودی، در هشت لایه، شامل لایه‌های شبکه، ارتباطات (خطوط ارتباطی)، سامانه اطلاعاتی، سیستم عامل، کاربرد، تجهیزات انتهایی، محتوا (داده) و دسترسی فیزیکی به مورد اجرا گذاشته می‌شود.

ماده۹: لایه‌های عملیات پدافند سایبری

عملیات پدافند سایبری، در چهار محدوده زمانی پیش از جنگ سایبری، در آستانه جنگ سایبری، حین جنگ سایبری و پس از جنگ سایبری اجرا می‌شود و به ترتیب معادل عملیات پدافند سایبری پیش‌گیرانه، پیش‌کنشگرانه، واکنش‌گرایانه و منفعلانه است. تمرکز اصلی نظام عملیاتی پدافند سایبری، بر مأموریت‌های پیش‌گیرانه در محدوده‌ی زمانی پیش از جنگ سایبری است و عملیات چهارگانه پدافند سایبری بر اساس اصل آینده‌نگری (پیش‌بینی) باید الزاما توسط عملیات پیش‌بینانه پشتیبانی شوند.

ماده۷: زمان اجرای عملیات پدافند سایبری

- عملیات پدافند سایبری زیرساختی، در مقابل تهاجم سایبری علیه یک دارایی حیاتی یا حساس سایبری یا وابسته به سایبر با نقش و کارکرد زیرساختی و قدرت تولید مخاطرات محلی انجام و درگیری سایبری نامیده می‌شود.
- عملیات پدافند سایبری حوزه‌ای، در مقابل تهاجم سایبری گسترده علیه یک دارایی حیاتی یا حساس سایبری یا وابسته به سایبر برخوردار از نقش و کارکرد حوزه‌ای و قدرت تولید مخاطرات عمده انجام و نبرد سایبری نامیده می‌شود.
- عملیات پدافند سایبری ملی، در مقابل تهاجم سایبری گسترده علیه مجموعه‌ای از چند دارایی حیاتی یا حساس سایبری یا وابسته به سایبر است که مجموعا نقش و کارکرد ملی و قدرت تولید مخاطرات فاجعه‌بار انجام و جنگ سایبری نامیده می‌شود.
- عملیات پدافند سایبری- شناختی ملی در مقابل تهاجم سایبری هم‌زمان با تهاجم شناختی گسترده علیه افکار و باورهای جامعه در یا ازطریق فضای سایبر کشور انجام و جنگ ترکیبی سایبری-شناختی نامیده می‌شود.
- عملیات پدافند سایبری تمام عیار که در مقابل جنگ ترکیبی سایبری-شناختی هم‌زمان با جنگ فیزیکی (غیرسایبری) علیه کشور انجام و جنگ تمام عیار نامیده می‌شود.

ماده۸: سطوح عملیات پدافند سایبری

وضعیت سایبری، شامل چهار وضعیت با عناوین سفید، زرد، نارنجی و قرمز است که به‌ترتیب معادل احساس امنیت، احساس تهدید، احساس جنگ قریب‌الوقوع و وقوع جنگ در فضای سایبر یا ازطریق این فضا می‌باشد.

ماده ۱۰: وضعیت های عملیات پدافند سایبری

- اشراف اطلاعاتی بر فضای سایبر و قابلیت ها، توانایی و آمادگی عملیات سایبری دشمن و پدافند سایبری خودی
- آمادگی عملیاتی قابلیت ها و نیروهای پدافند سایبری
- مصونیّت دارایی های حیاتی و حساس سایبری و وابسته به سایبر در مقابل هر نوع تهدید سایبری
- تاب‌آوری و تداوم کارکردهای ضروری دارایی های حیاتی و حساس سایبری و وابسته به سایبر در مقابل جنگ سایبری
- برتری عملیاتی نیروهای پدافند سایبری خودی بر دشمن
- ابقاء (ترمیم) و ارتقاء قدرت پدافندی سایبری

ماده ۱۲: اهداف عملیاتی پدافند سایبری کشور

- تهیه برآورد اطلاعاتی از تهدیدات سایبری دشمن و به‌روزرسانی آن
- شناسایی و تهیه برآورد از آسیب‌پذیری های سایبری، نقاط ضعف قابلیت های پدافند سایبری و مخاطرات سایبری، فیزیکی و شناختی ناشی از آنها
- صیانت همه‌جانبه، چندلایه و تطبیق‌پذیر از دارایی های حیاتی و حساس سایبری و وابسته به سایبر کشور در مقابل تهدیدات سایبری دشمن
- آگاهی‌رسانی، هشداردهی، آموزش، تمرین و آزمون هماهنگی و آمادگی قابلیت ها و نیروهای پدافند سایبری
- ممانعت از انجام، تشخیص، انتساب و دفع تجاوز سایبری و کنترل پیامدهای آن
- پاسخ متناسب و/یا تنبیهی به تجاوز سایبری دشمن با هماهنگی نظام آفند سایبری
- بازیابی پیامدهای تجاوز سایبری و افزایش آمادگی پدافند سایبری
- اقناع افکار عمومی خودی، بیطرف و دشمن درخصوص محکومیت جنگ سایبری و ثبت ادله قانونی اثبات تجاوز سایبری و دیپلماسی سایبری
- دفاع جمعی با همکاری کشورهای همسو در برابر تهدیدات ائتلافی سایبری

ماده ۱۱: مأموریت های عملیاتی پدافند سایبری

الف: اشراف اطلاعاتی

۱) رصد، پایش، برآورد اطلاعاتی و اشتراک‌گذاری اطلاعات وضعیت تهدید سایبری و مخاطرات احتمالی ناشی از آن

۲) رصد، پایش، برآورد عملیاتی و اشتراک‌گذاری اطلاعات وضعیت خودی

ماده ۱۳: تدبیر عملیاتی
(چگونگی اقدام عملیات پدافند سایبری)

ب : آمادگی عملیاتی

۳) تعیین وضعیت سایبری و عملیاتی، آگاهی‌رسانی و صدور هشدار سایبری

۴) توسعه تشکیلات، فرایندها، نیروی انسانی و فناوری‌های پدافند سایبری در سطوح زیرساختی، حوزه‌ای و ملی

۵) ارتقاء مهارت، تخصص و توانایی عملیاتی نیروهای پدافند سایبری

۶) ارتقاء تجارب و آمادگی عملیاتی نیروهای پدافند سایبری با هماهنگی و مشارکت نیروهای آفند سایبری

پ : مصونیّت دارایی‌های حیاتی و حساس در مقابل هر نوع تهدید سایبری

۷) شناخت، احصاء ویژگی‌ها، ارزش‌گذاری و طبقه‌بندی دارایی‌های سایبری و وابسته به سایبر

۸) صیانت همه‌جانبه از دارایی‌های حیاتی و حساس سایبری و وابسته به سایبر در مقابل هر نوع تهدید سایبری

۹) رفع یا کاهش آسیب‌پذیری‌های سایبری، با بهره‌گیری از محصولات بومی، سازوکار اعتبارسنجی و وصله‌زنی آسیب‌پذیری

ت : تاب‌آوری و تداوم کارکردهای ضروری دارایی‌های سایبری و وابسته به سایبر در مقابل جنگ سایبری

۱۰) یکپارچه‌سازی، تقویت تعامل و تعمیق همکاری و مشارکت نیروهای پدافند سایبری برای افزایش انسجام و مقاومت در جنگ سایبری

۱۱) بهره‌گیری از سازوکارهای پدافند سایبری همه‌جانبه و لایه‌ای، جهت اجرای مأموریت‌های پدافند سایبری

۱۲) تطبیق دادن مکانیزم‌ها و سازوکارهای پدافندی سایبری، در مقابل جنگ سایبری

۱۳) اشتراک‌گذاری اطلاعات و تبادل تجارب برتر جهت تشخیص و واکنش سریع و مؤثر به جنگ سایبری و پیامدهای آن

ث : برتری عملیاتی نیروهای پدافند سایبری خودی بر دشمن

۱۴) کنترل تنش سایبری (کاهش شدّت، احتمال وقوع و اثر مخاطره سایبری) با مدیریت مخاطرات سایبری

۱۵) اقناع افکار عمومی خودی در خصوص محکومیت جنگ سایبری قریب‌الوقوع دشمن و مشروعیت پاسخ خودی

۱۶) تأثیرگذاری بر افکار عمومی بی‌طرف و دشمن جهت نفی مشروعیت جنگ سایبری قریب‌الوقوع و مشروعیت پاسخ خودی

۱۷) نمایش قدرت سایبری، بزرگ‌نمایی پیامدهای اقدام متقابل و تهدید به استفاده از قدرت نظامی در پاسخ به تجاوز سایبری

۱۸) یکپارچه‌سازی سلاح‌های پدافندی در مأموریت‌های پدافند سایبری

۱۹) شناسایی متجاوز و منشأ تجاوز سایبری، انتساب تجاوز سایبری به دشمن و مستندسازی ادلّه قانونی تجاوز سایبری

۲۰) ممانعت از تداوم تجاوز سایبری یا مقابله و دفع تجاوز سایبری دشمن از طریق ریشه‌کنی منشأ جنگ سایبری یا ضدحمله محدود به متجاوز سایبری

۲۱) محدودسازی، قرنطینه، کنترل و پاک‌سازی پیامدهای جنگ سایبری

۲۲) پاسخ محدود تلافی‌جویانه به متجاوز سایبری یا پدافند فعال سایبری

۲۳) هماهنگی پاسخ تهاجمی سایبری و یا غیرسایبری به متجاوز سایبری

ج: ابقاء (ترمیم) و ارتقاء قدرت پدافندی سایبری

۲۴) بازیابی، ترمیم و ریشه‌کنی پیامدهای جنگ سایبری و ابقاء کارکردهای دارایی‌های حیاتی و حساس

۲۵) استیفای حقوق قانونی کشور از طریق محکومیت سیاسی و حقوقی تجاوز سایبری در مراجع و محاکم بین‌المللی

۲۶) ابقاء و ارتقاء قابلیت‌ها، توانایی و آمادگی عملیاتی غیرعامل و فعّال پدافند سایبری

الف: کنشگران نقش راهبر

دستگاه‌های راهبر مأموریت‌های عملیاتی پدافند سایبری، عبارتند از شورای عالی امنیت ملی، شورای عالی فضای مجازی، ستاد کل نیروهای مسلح و قرارگاه مرکزی خاتم‌الانبیاء (ص)

ب: کنشگران نقش مجری

دستگاه‌های مجری مأموریت‌های عملیاتی پدافند سایبری، عبارتند از ستاد کل نیروهای مسلح، قرارگاه مرکزی خاتم‌الانبیاء (ص)، قرارگاه پدافند سایبری، یگان سایبری سپاه پاسداران انقلاب اسلامی، یگان سایبری ارتش جمهوری اسلامی، پلیس فتا، یگان سایبری بسیج، وزارت اطلاعات/مرکز مدیریت راهبردی افتا، وزارت ارتباطات و فناوری اطلاعات و سایر دستگاه‌های اجرایی.

پ: کنشگران نقش پشتیبان

دستگاه‌های پشتیبان مأموریت‌های عملیاتی پدافند سایبری، عبارتند از مجلس شورای اسلامی، قوه قضائیه، سازمان صدا و سیمای جمهوری اسلامی، وزارت دفاع و پشتیبانی نیروهای مسلح، وزارت امور خارجه، وزارت علوم، تحقیقات و فناوری و قابلیت‌های پدافند سایبری بخش دولتی و غیردولتی از جمله مراکز آپا و آزمایشگاه‌های ارزیابی و اعتبارسنجی.

ت: کنشگران نقش همکار

دستگاه‌های همکار در اجرای مأموریت‌های عملیاتی پدافند سایبری، عبارتند از وزارت علوم، تحقیقات و فناوری، سازمان صدا و سیمای جمهوری اسلامی، حوزه‌های علمیه، رسانه‌ها و سایر دستگاه‌های اجرایی حسب مورد.

ماده ۱۴: نقش‌های کنشگران:

۱) شورایعالی امنیت ملی: اعلام شروع و خاتمه جنگ سایبری، تعیین وضعیت نارنجی و قرمز (جنگ سایبری) به پیشنهاد قرارگاه مرکزی حضرت خاتم‌الانبیاء (ص) را به عهده دارد.

۲) ستاد کل نیروهای مسلح: در شرایط سفید و زرد هدایت و راهبری قرارگاه پدافند سایبری کشور را به عهده دارد.

۳) قرارگاه مرکزی حضرت خاتم‌الانبیاء (ص): در شرایط قرمز و نارنجی هدایت و راهبری (کنترل عملیاتی) قرارگاه پدافند سایبری کشور را به عهده دارد.

۴) قرارگاه پدافند سایبری کشور:

- فرماندهی، طرح‌ریزی عملیاتی، هدایت، راهبری و مدیریت سطح ملی پدافند سایبری در وضعیت نارنجی و قرمز
- راهبری و نظارت بر مصون سازی زیرساخت‌های حیاتی، حساس، مهم
- پایش، رصد و تشخیص تهدیدات و کشف آسیب‌پذیری‌ها در فضای سایبری
- هدایت، راهبری و نظارت بر طرح ریزی، آموزش، تمرین، رزمایش و آمادگی سایبری
- طبقه بندی و سطح بندی زیرساخت‌های سایبری و وابسته به سایبر به حیاتی، حساس و مهم ازمنظر نقش و کارکرد و میزان وابستگی به فضای سایبر و پیامدهای حدف آن
- هدایت و راهبری دفاع جمعی سایبری و دفاع حقوقی سایبری

ماده ۱۵: وظایف کنشگران (پیوست)

۵) مرکز ملی فضای مجازی:

- هماهنگی دستگاه‌های کشوری برای ایجاد و ارزیابی آمادگی و اجرای عملیات پدافند سایبری
- پیگیری و نظارت بر اجرای نظامات، دستورالعمل‌ها و طرح‌های عملیات پدافند سایبری

۶) سپاه پاسداران انقلاب اسلامی/ فرماندهی سایبرالکترونیک و بسیج سپاه:

- تهیه طرح‌ها و انجام اقدامات عامل، پیش‌کنشانه و پیش‌دستانه و دفاع فعال
- آماده‌سازی و عملیاتی سازی ظرفیت‌های لازم برای واکنش سریع به جنگ سایبری
- خنثی سازی اقدامات ضدامنیتی دشمن و آشوبگران در فضای سایبری

۷) وزارت دفاع و پشتیبانی نیروهای مسلح:

- انجام عملیات امداد و نجات سایبری در زیرساخت‌های حیاتی، حساس و مهم کشور
- جمع‌آوری ادله مثبته و جرم‌شناسی رقومی در زیرساخت‌های حیاتی، حساس و مهم کشور
- رصد تهدیدات دشمن و ارسال گزارش تهدیدات و حملات احتمالی سایبری به زیرساخت‌های حیاتی، حساس و مهم کشور
- انجام رزمایش و ارزیابی مستمر آمادگی عملیاتی در زیرساخت‌های کشور
- طراحی، تولید و عملیاتی سازی تجهیزات پایه پدافند سایبری مورد نیاز در اسرع وقت.
- پایش و رصد اتحادها و معاهدات دفاعی سایبری و اتخاذ رویکرد مناسب با نیاز قرارگاه پدافند سایبری کشور.
- کمک و پشتیبانی در ظرفیت‌سازی و تربیت نیروی انسانی در قالب اطلاع‌رسانی و مهارت‌آموزی

۸) وزارت اطلاعات / مرکز مدیریت راهبردی افتا:

- تبادل اطلاعات در مورد تهدیدات سایبری با قرارگاه پدافند سایبری
- تعامل امنیتی-عملیاتی با قرارگاه پدافند سایبری در مورد برنامه‌ها و آسیب‌پذیری‌های سایبری کشور
- کمک به قرارگاه پدافند سایبری در پاسخگویی به شرایط اضطراری سایبری در وضعیت‌های نارنجی و قرمز
- همکاری در مدیریت صحنه رخدادهای سایبری در شرایط دفاع سایبری (وضعیت نارنجی و قرمز) و ارسال گزارش به قرارگاه پدافند سایبری

۹) وزارت امور خارجه

- هماهنگی، همکاری، پشتیبانی و دفاع حقوقی از اقدامات عملیاتی پدافند سایبری در مجامع و مراجع بین‌المللی
- اقناع افکار عمومی کشورهای بیطرف و همسو درخصوص محکومیت جنگ سایبری
- ثبت ادله قانونی اثبات تجاوز سایبری، دیپلماسی سایبری، پشتیبانی و دفاع حقوقی از اقدامات عملیاتی پدافند سایبری در مجامع و مراجع بین‌المللی
- هماهنگی و پشتیبانی از دفاع جمعی با همکاری کشورهای همسو در برابر تهدیدات ائتلافی سایبری

۱۰) نیروی انتظامی-پلیس فتا:

- اقدام مقابله‌ای به‌موقع با جرائم سازمان یافته سایبری
- ارسال گزارشات رصد و پایش تهدیدات و حملات سایبری احتمالی جرایم سازمان یافته در حوزه زیرساخت های حیاتی، حساس و مهم و سرمایه های ملی سایبری به قرارگاه پدافند سایبری کشور (به صورت سیستمی)
- کمک به قرارگاه پدافند سایبری کشور در پاسخگویی به شرایط اضطراری سایبری در وضعیت های نارنجی و قرمز
- کمک به دفاع حقوقی و انجام اقدامات فارنزیک

۱۱) وزارت ارتباطات و فناوری اطلاعات

- طبقه‌بندی دارایی های سایبری کشور
- صیانت و پدافند از مرزهای سایبری کشور با هماهنگی کامل قرارگاه پدافند سایبری (مرزبانی رقومی «سایبر»)
- تداوم کارکرد زیرساختی در شبکه ملی و ارتقا پایداری آن
- پایش، رصد و کشف آسیب پذیری در زیرساخت های ارتباطی در دسترس
- حیطه‌بندی، مدیریت صحنه و فراهم آوردن امکان مدیریت منطقه‌ای و تمرکز بر دفاع در لایه G.W (دروازه ورودی)
- تشخیص، محدودسازی و جلوگیری از انواع حملات سایبری از جمله حملات منع سرویس توزیع شده
- ایجاد و بهره‌برداری ارتباط ویژه با گروه های واکنش سریع (CERT) بین المللی
- آماده‌سازی مسیرهای جایگزین مخابراتی، ارتباطی و اینترنت (امکان اتصال و انفصال شبکه های خارجی متصل به شبکه ملی اطلاعات)
- انجام عملیات امداد و نجات در زیرساخت های ارتباطی کشور (نظیر واکنش سریع به حملات)
- جمع‌آوری ادلّه مثبته و جرم‌شناسی رقومی در زیرساخت های تحت کنترل و نظارت.
- در اختیار گذاشتن داشبورد رصد و پایش زیرساخت های کشور از طریق برقراری ارتباط اختصاصی مرکز و قرارگاه پدافند سایبری کشور
- ارسال گزارشات تهدیدات و حملات سایبری احتمالی دشمن به زیرساخت های حیاتی، حساس و مهم و سرمایه های ملی سایبری به قرارگاه پدافند سایبری
- کمک به قرارگاه پدافند سایبری در پاسخگویی به شرایط اضطراری سایبری در وضعیت های عملیاتی
- ارزیابی آمادگی های عملیاتی در شبکه ملی اطلاعات با انجام رزمایش های مستمر

۱۲) دستگاه‌های اجرائی:

- صیانت همه جانبه از دارایی های حیاتی و حساس سایبری و وابسته به سایبر ذی ربط در مقابل هر نوع تهدید سایبری
- مصون سازی، رفع یا کاهش آسیب پذیری های سایبری، با بهره‌گیری از محصولات بومی، سازوکار اعتبارسنجی و وصله زنی آسیب پذیری
- تاب‌آوری و تداوم کارکرد های ضروری دارایی های سایبری و وابسته به سایبر در زیرساخت های ذی ربط در مقابل جنگ سایبری
- حیطه‌بندی، مدیریت صحنه و فراهم آوردن امکان مدیریت منطقه‌ای و محلی
- آماده‌سازی مسیرهای جایگزین مخابراتی، ارتباطی و اینترنت
- ارزیابی آمادگی های عملیاتی در زیرساخت های ذی ربط با انجام رزمایش های مستمر

ماده ۱۶: دستورات هماهنگی:

۱) مسئولیت انجام عملیات پدافند سایبری (پایش و رصد، مصون سازی، پیشگیری ومقابله با حوادث) مربوط به هر دستگاه با هدایت و راهبری قرارگاه پدافند سایبری کشور بر عهده بالاترین مقام آن دستگاه می باشد.

۲) عملیات پدافند سایبری در دارایی های حیاتی، حساس و مهم تا پایین ترین سطح مورد نیاز با هماهنگی، هدایت و راهبری قرارگاه پدافند سایبری کشور توسط مسئولین دارایی ها تداوم می یابد.

۳) ضابطین قضایی و انتظامی وضعیت سفید و زرد پلیس فتا، و وضعیت نارنجی و قرمز قرارگاه پدافند سایبری کشور می باشند.

۴) قوه قضائیه (دادستانی کل کشور) در وضعیت های وضعیت سفید، زرد، نارنجی و قرمز، عملیات پدافند سایبری را پشتیبانی و حمایت قضایی می نماید.

ماده ۱۷

قرارگاه پدافند سایبری، اصول و قواعد، سند تفصیلی نظام عملیاتی پدافند سایبری کشور (حاوی جزئیات کافی برای قابل درک و قابل اجرا نمودن نظام عملیاتی پدافند سایبری، برای هر یک از ارکان این نظام، طرح های عملیاتی مربوط به هر یک از مأموریت های عملیاتی پدافند سایبری، چارچوب ها و قواره ها و دستورالعمل های عملیاتی و فنی مورد نیاز اجرایی نمودن نظام عملیات پدافند سایبری را در چارچوب و مبتنی بر نظام عملیات پدافند سایبری تهیه، تدوین و به مسئولین و کنشگران نظام مذکور ابلاغ می نماید.

ماده ۱۸

سازمان پدافند غیرعامل کشور با تشکیل کمیته عالی راهبری و نظارت مرکب از نمایندگان تام الاختیار کنشگران نظام عملیات پدافند سایبری، مسئول هدایت، راهبری و نظارت بر اجرای این نظام است و آمادگی کشور در تمام سطوح، لایه ها، جنبه ها و زمان اجرای عملیات پدافند سایبری را با انجام رزمایش ارزیابی نموده و به کنشگران راهبر و کمیته دائمی گزارش می نماید.

ماده ۱۹

نظام عملیاتی پدافند سایبری کشور در نوزده مادّه و یکصد و بیست و شش بند در سی و چهارمین جلسه کمیته دائمی به تصویب رسید.

۱۳) مشاورین/ همکاران (آپا، شرکت های مشاور، بخش خصوصی و...):

در تمام وضعیت های عملیاتی پدافند سایبری شرکت ها، موسسات، و دانشگاه ها برای عمل کلی و پشتیبانی های عمومی، تخصصی و آموزشی در کنترل عملیاتی قرارگاه پدافند سایبری اقدام می نمایند.

۱۴) قوه قضاییه

سازوکار رسیدگی به موقع به جرایم را ایجاد و به تناسب با سطوح، جنبه ها، لایه ها و محدوده های زمان عملیات پدافند سایبری در تمام وضعیت ها عملیات پدافند سایبری را از منظر قضایی نظارت، رسیدگی، پشتیبانی و حمایت قضایی می نماید.

مقام معظم رهبری و فرماندهی کل قوا (مدظله العالی)

« این را در درجه اول مدیران کشور باید درک و احساس کنند، اگر چنانچه مدیران ارشد کشور اهمیت پدافند غیر عامل را درک نکنند و پدافند غیرعامل آنچنان که باید و شاید در کشور توسعه پیدا نکند و اعمال نشود، ما در معرض تهدیدهایی قرار می گیریم که بعضی از آنها قابل جبران نیست، اصرار دارم که مسئولین همه بخش های مختلف کشور، همکاری کامل و لازم را با پدافند غیرعامل بکنند. ...اگر بناست این بی توجهی ادامه پیدا کند قطعا ضربه خواهیم خورد؛ این یک طرف قضیه است، طرف دیگر قضیه شما [مسئولین پدافند غیرعامل] هستید؛ شما باید کار را با جدیّت و اقتضائاتش دنبال کنید؛ یکی از این اقتضائات این است که کار را کاملاً علمی، دقیق و همه جانبه ببینید و صلاحیت های لازم را برای آن کسب کنید. » « کارگروه (کمیته) دائمی پدافند غیرعامل کشور به ریاست رئیس ستاد کل نیروهای مسلح بالاترین مرجع تصمیم‌گیری در حوزه پدافند غیرعامل کشور است که تصمیمات آن با ابلاغ رئیس کارگروه مزبور، برای همه دستگاه‌های لشکری، کشوری، بخش دولتی و عمومی غیردولتی لازم‌الاجراست.... »

قانون تشکیل سازمان پدافند غیرعامل کشور (۱۴۰۲/۰۶/۱۲)

تصویب‌نامه

به استناد تبصره۱ قانون تشکیل سازمان پدافند غیرعامل کشور- مصوب مجلس شورای اسلامی- و ماده۸ اساسنامه این سازمان- مصوّب مقام معظّم رهبری- هفتاد و هفتمین جلسه کارگروه (کمیته) دائمی پدافند غیرعامل کشور در تاریخ ۱۴۰۲/۰۶/۲۸ تشکیل گردید و پیشنهاد آن سازمان با موضوع دستورالعمل عملیاتی پدافند سایبری زیرساخت‌های صنعتی کشور را بررسی و تصویب نمود.

دستورالعمل عملیاتی پدافند سایبری زیرساخت‌های صنعتی کشور

ماده۱: تعاریف و اختصارات

در اصل سند قابل رویت است.

ماده ۲: اسناد بالادستی

۱) فرامین، تدابیر، سیاست‌ها و منویات مقام معظّم رهبری در حوزه امنیت و دفاع و پدافند غیرعامل
۲) اساسنامه سازمان پدافند غیرعامل کشور- ابلاغی مقام معظم رهبری
۳) قانون تشکیل سازمان پدافند غیرعامل کشور- مصوب مجلس شورای اسلامی
۴) قانون احکام دائمی برنامه‌های توسعه کشور- ماده۵۸
۵) بند پ ماده ۱۰۷ و ماده ۱۰۹ قانون برنامه ششم توسعه
۶) نظام عملیاتی پدافند سایبری کشور

ماده ۳: هدف از تدوین سند

تعیین سازوکار، روش‌ها و الزامات پدافند سایبری از زیرساخت‌های صنعتی بصورت هماهنگ، همسو و هم‌افزا

۱) ایجاد امنیت و مصونیت، تاب‌آوری و استمرار کارکردهای ضروری و قابلیت برگشت‌پذیری در زیرساخت صنعتی و فناوری‌های عملیاتی
۲) ارتقای آمادگی به منظور پاسخ پدافند غیرعاملی به جنگ سایبری علیه زیرساخت‌های صنعتی
۳) آگاه‌سازی متولیان زیرساخت‌های صنعتی سایبری از تهدیدات، آسیب‌پذیری‌ها و مخاطرات سامانه‌های کنترل صنعتی و فناوری عملیاتی
۴) آگاه‌سازی صاحبان زیرساخت‌های صنعتی از بهترین تجربیات درخصوص نحوه ارزیابی امنیتی و امن‌سازی سامانه‌های کنترل صنعتی در اختیار
۵) ارتقاء توانمندی‌ها و قابلیت‌های متولیان، مدیران و کارکنان زیرساخت‌های صنعتی در بررسی و تحلیل حوادث سایبری و اتخاذ تصمیمات به هنگام و موثّر برای پیشگیری و مقابله با آنها در جهت بازیابی سریع وضعیت مطلوب

ماده ۴: منظور

رئیس دستگاه اجرایی با بکارگیری ظرفیت‌های تخصصی در اختیار (از جمله شرکت‌های مورد تایید) اقدامات عملیاتی سایبری و عملیات مشترک پدافند ترکیبی خود را با رویکرد پیش‌بینانه، پیشگیرانه، پیش‌کنش‌گرانه، واکنش‌گرایانه، و بازیابی و با راهبرد دفاع عمیق، لایه به لایه، شبکه‌ای - جزیره‌ای و مبتنی بر معماری اعتماد صفر و برآورد مستمر و تطبیقی مخاطرات و اعتماد (CARTA) در چهار مرحله ۱- قبل از حمله سایبری، ۲- در آستانه حمله سایبری، ۳- حین حمله سایبری و ۴- پس از حمله سایبری اجرا می‌نماید؛ مجموعه این اقدامات با آرایه‌بندی زیر انجام می‌شود:
۱- ایجاد واحد امنیت سایبری صنعتی تخصصی
۲- رصد و پایش آسیب‌پذیری و تهدیدات آن حوزه
۳- تشکیل تیم‌های تخصصی امنیت و پدافند سایبری صنعتی
۴- هم‌افزایی و هماهنگی با دستگاه‌های مسئول در کشور
۵- ایجاد سازوکار بهره‌گیری از ظرفیت‌ها و توان دانشگاه‌ها، بخش خصوصی و سازمان‌های مردم‌نهاد مورد تایید امنیتی و پدافندی
۶- ایجاد سازوکار بهره‌گیری از ظرفیت‌ها برای عملیات مشترک پدافند سایبری - پدافند شیمیایی؛ و عملیات مشترک پدافند سایبری - پدافند پرتوی جهت کنترل پیامد نشت آلودگی‌های شیمیایی و پرتوی (برابر نظام عملیاتی پدافند شیمیایی و طرح ملی مقابله با تهدیدات پرتوی)

ماده ۷: تدبیر

دستگاه‌های اجرایی موضوع ماده ۵ قانون مدیریت خدمات کشوری، سازمان‌های نیروهای مسلح و بخش خصوصی که دارای زیرساخت‌های صنعتی و سامانه‌های فناوری عملیاتی هستند، مشمول این دستورالعمل قرار می‌گیرند.

ماده ۵: حوزه شمول

روسای دستگاه‌های اجرایی ماموریت‌ها و اهداف زیر را در زیرساخت‌های سایبری صنعتی زیرمجموعه خود طرح‌ریزی، هدایت و راهبری و اجرا می‌نمایند:
۱) شناسایی، دسته‌بندی، اولویت‌بندی شبکه‌ها و سامانه‌های کلیدی، ضروری ولازم زیرساخت‌های صنعتی و فناوری عملیاتی
۲) پایش و رصد مداوم تهدیدات، تشخیص و هشدار عملیاتی آن و به اشتراک‌گذاری اطلاعات تهدید
۳) ارزیابی و آزمون امنیتی و بازرسی مداوم به منظور کشف آسیب‌پذیری‌های زیرساختی صنعتی و فناوری عملیاتی
۴) شناسایی، دسته‌بندی، اولویت دهی و مدیریت و کاهش مخاطرات و پیامدها، اولویت‌بندی و امن‌سازی
۵) تهیه و اجرای برنامه‌های عملیاتی پدافند سایبری زیرساخت‌های صنعتی شامل CERP، CBCP و CDRP،
۶) اجرای برنامه‌های ارتقای آمادگی و رزمایش سایبری در زیرساخت‌های صنعتی و فناوری عملیاتی
۷) بازخوردگیری و روزآمدسازی برنامه‌ها و اقدامات پدافند سایبری در زیرساخت‌های صنعتی و فناوری عملیاتی
۸) انجام عملیات رصد، پایش، تشخیص و هشدار تهدیدات الکترونیک و الکترومغناطیس و آمن‌سازی و مصون‌سازی الکترونیکی در برابر آنها
۹) انجام عملیات مشترک پدافند سایبری با پدافند (شیمیایی - پرتوی) جهت کنترل پیامد نشت آلودگی شیمیایی و پرتوی
۱۰) انجام عملیات رصد، پایش، تشخیص و هشدار تهدیدات ریزپرنده و عملیات مقابله با آنها

ماده ۶: اهداف و ماموریت‌های عمده زیرساخت‌های مشمول این دستورالعمل:

متداول‌ترین حملات سایبری-فیزیکی به سامانه‌های صنعتی شامل موارد زیر است:

۱) حملات نفوذ و جاسوسی و جمع‌آوری اطلاعات و شناسایی زیرساخت

۲) حملات روز صفر (سوء استفاده از آسیب‌پذیری امنیتی که به صورت عمومی منتشر نشده است)

۳) حملات نشت داده و استراق سمع کانال‌های ارتباطی (دسترسی به اطلاعات حساس و محرمانه فرآیندهای صنعتی)

۴) حملات منع خدمات (از کار انداختن سامانه‌ها با جلوگیری از دسترسی به منابع پردازشی و تحت کنترل گرفتن فرآیند سیستم هدف به وسیله مهاجم)

۵) حملات تزریق داده‌های غلط (تزریق کدها و دستورات غلط به سامانه‌های کنترل صنعتی و وادارکردن سامانه به اجرای اقدامات خارج از ماموریت و هدف تعیین شده)

۶) حملات آلوده‌سازی بسته‌های داده (ارسال مجدد بسته‌های داده آلوده شده با دستورات مخرب که پیامد آن اختلال و تخریب می‌باشد)

۷) حملات کانال جانبی (جمع‌آوری غیرقانونی داده‌های سامانه‌های صنعتی از نشت اطلاعات در تجهیزات صنعتی)

ماده ۹: انواع حملات سایبری فیزیکی به سامانه‌های صنعتی

الف) آسیب‌پذیری مربوط به سیاست‌ها و رویه‌ها

ب) آسیب‌پذیری مربوط به چیدمان و آرایه‌بندی سامانه‌ها

پ) آسیب‌پذیری مربوط به سخت‌افزار سامانه‌ها

ت) آسیب‌پذیری مربوط به نرم‌افزار سامانه‌ها (سیستم عامل و سایر برنامه‌ها)

ث) آسیب‌پذیری مربوط به شیوه حفاظت در برابر بدافزارها

ج) آسیب‌پذیری مربوط به آرایه‌بندی شبکه

چ) آسیب‌پذیری مربوط به سخت‌افزار و نرم‌افزار شبکه

ح) آسیب‌پذیری مربوط به حفاظت محیطی شبکه

خ) آسیب‌پذیری مربوط به ارتباطات

د) آسیب‌پذیری مربوط به اتصالات بی‌سیم

ذ) آسیب‌پذیری مربوط به پایش و ثبت وقایع و رخدادهای شبکه

ر) آسیب‌پذیری مربوط به کارکنان

ماده ۱۰: انواع آسیب‌پذیری‌های سامانه‌های کنترل صنعتی

تهدیدات زیر بعنوان تهدید پایه در حوزه زیرساخت‌های صنعتی و فناوری عملیاتی درنظر گرفته شده است:

۱) تهدید سایبری زیرساختی

۲) تهدیدات سایبری ترکیبی

- ✓ تهدید سایبری- شیمیایی
- ✓ تهدید سایبری- هسته‌ای

۳) تهدید از درون

۴) تهدیدات امنیتی و خرابکاری

۵) تهدیدات الکترومغناطیس

۶) تهدیدات الکترونیک

۷) تهدیدات ریزیرنده

ماده ۸: تهدیدات پایه مفروض زیرساخت‌های صنعتی

عملیات پدافند سایبری در زیرساخت‌های صنعتی و فناوری عملیاتی در سه سطح زیرساختی، حوزه‌ای و ملی دسته‌بندی می‌شود.

الف) عملیات پدافند سایبری زیرساختی صنعتی و فناوری عملیاتی

این نوع از عملیات در مقابل تهاجم سایبری علیه یک زیرساخت صنعتی با اهمیت بالای سایبری و یا وابسته به سایبر با نقش و کارکرد صنعتی و فناوری عملیاتی با قدرت تولید مخاطرات محلی انجام می‌شود.

ب) عملیات پدافند سایبری حوزه‌ای

این نوع از عملیات در مقابل تهاجم سایبری گسترده علیه یک زیرساخت صنعتی با اهمیت بالای سایبری و یا وابسته به سایبر با نقش و کارکرد حوزه‌ای با قدرت تولید مخاطرات عمده انجام می‌شود.

ج) عملیات پدافند سایبری ملی

این نوع از عملیات در مقابل تهاجم سایبری علیه مجموعه‌ای از چند زیرساخت صنعتی با اهمیت بالای سایبری و یا وابسته به سایبر با نقش و کارکرد ملی و قدرت تولید مخاطرات فاجعه‌بار انجام می‌شود.

د) عملیات پدافند ترکیبی سایبری - شیمیایی/ سایبری - هسته‌ای

به مجموعه عملیات ترکیبی پدافند سایبری از زیرساخت صنعتی در مقابل تهاجم سایبری و عملیات پدافند شیمیایی/هسته‌ای، به منظور کنترل پیامدهای ناشی از نشت شیمیایی/هسته‌ای بر مردم، محیط و زیرساخت اطلاق می‌شود.

ه) عملیات پدافند ترکیبی سایبری - رسانه و مردم محور

به مجموعه عملیات پدافند ترکیبی سایبری صنعتی با ترکیب رسانه با قابلیت هدایت و بکارگیری مردم و انتقال پیامدهای ناشی از قطع زنجیره تولید محصول و خدمت به مردم با هدف تولید آشوب، نا امنی، خرابکاری و تخریب اطلاق می‌شود.

ماده ۱۱: سطوح عملیات پدافند سایبری

ماده ۱۲: الزامات پدافند سایبری در زیرساخت‌های صنعتی و فناوری عملیاتی

مهم‌ترین الزامات پدافند سایبری در زیرساخت‌های صنعتی و فناوری عملیاتی در موضوعات زیر دسته‌بندی و ارائه شده‌اند و رعایت آنها در زیرساخت‌های ویژه، حیاتی، حساس، مهم و قابل حفاظت صنعتی لازم‌الاجراست:

۱) الزامات سازمانی و مدیریتی

متولیان زیرساخت‌های صنعتی و عملیاتی باید اقدامات زیر را انجام دهند:

الزام۱- تشکیل و سازماندهی ساختار امنیت و پدافند سایبری مورد نیاز در دستگاه برابر الگوی ابلاغی سازمان

الزام۲- سازماندهی تیم‌های عملیاتی ارزیابی امنیتی، اَمن‌سازی، پایش و رصد و شواهد دیجیتال و پاسخگویی به رخدادهای سایبری

الزام۳- ایجاد سازوکار حفظ و نگهداری صحیح و ارجاع بی‌درنگ شواهد و قرائن مربوط به تهدیدات و حملات سایبری به مراجع ملی حوزه امنیت و پدافند سایبری جهت رسیدگی بی‌وقفه و سریع به حوادث سایبری در زیرساخت‌های صنعتی و عملیاتی.

۲) الزامات معماری شبکه و معماری امنیتی شبکه

الزام۱- استفاده از معماری امنیت و پدافند سایبری چندلایه، رویکرد چندین نام‌نمای تجاری (Multi Branding) ارتباطات درهم تنیده، برخوردار از نسخ پشتیبان و نقاط گره موازی، متناسب با رویکرد دفاع در عمق، چارچوب CARTA و رعایت معماری Zero Trust

الزام۲- اتخاذ تمهیدات فنی و عملیاتی و حفاظتی برای اتصال مراکز عملیات امنیت (SOC) به مرکز عملیات پدافند سایبری کشور (CDOC) و عملیاتی کردن آنها

الزام۳- تنظیم روابط، ارتباطات، پروتکل‌ها و شیوه چینش و هم‌بندی تجهیزات شبکه و امنیت و پدافند سایبری با رویکرد ارتقای سطح امنیت و حفاظت از کل و تک تک اجزای شبکه

۳) الزامات ارتباطاتی در شبکه کنترل صنعتی و فناوری عملیاتی

الزام۱- استفاده از شبکه‌های با سیم مبتنی بر پروتکل اَمن در درون مجموعه‌های صنعتی

الزام۲- استفاده از شبکه‌های باسیم مبتنی بر فیبر نوری در بیرون از مجموعه صنعتی و استفاده از ارتباطات مبتنی بر روش TDM در شرایط خاص (عدم امکان استفاده از فیبر نوری)

الزام۳- اَمن‌سازی، چندلایه‌سازی و رمزنگاری ارتباطات با رویکرد استفاده از افزونگی مناسب جهت تاب‌آوری و پایداری ارتباطات در طرح‌های ارتباطی

۴) الزامات سخت افزاری در شبکه کنترل صنعتی و فناوری عملیاتی

الزام۱- تامین تجهیزات سخت افزاری با اولویت تامین از داخل کشور*

الزام۲- اجرای بروز رسانی اَمن و مطمئن اجزای سخت افزاری سامانه‌های صنعتی و فناوری عملیاتی

الزام۳- اجرای ارزیابی‌های نوبه‌ای برای حصول اطمینان از عدم آلودگی سخت افزارها به بدافزارها و ایمپلنت‌های سخت/میان افزاری

الزام۴- رعایت افزونگی سخت افزاری درخصوص تجهیزات سخت افزاری خاص

۵) الزامات نرم افزاری در شبکه کنترل صنعتی و فناوری عملیاتی

الزام۱- تامین محصولات نرم افزاری با اولویت تامین از داخل کشور*

الزام۲- حصول اطمینان از استحکام، اصالت و یکپارچگی ساختار نرم افزار، سیستم عامل و پایگاه داده‌های مورد استفاده در هر لایه

الزام۳- استفاده از سازوکار اَمن و مطمئن بروز رسانی و ارتقای نرم افزار

۶) الزامات پشتیبان گیری و امحای اطلاعات

الزام۱- پشتیبان‌گیری بلادرنگ یا با فاصله زمانی کوتاه از سامانه‌ها و پایگاه داده‌های با اهمیت بالا

الزام۲- ذخیره‌سازی و نگهداری داده‌ها و اطلاعات در چند محل اَمن مناسب

الزام۳- حصول اطمینان از آلوده نبودن اطلاعات پشتیبان و حفظ وضعیت عملیاتی با انجام آزمون عملیاتی- امنیتی؛

۷) الزامات زنجیره تامین

الزام۱- کاهش و مدیریت مخاطرات مرتبط با زنجیره تامین محصولات و خدمات و بهره‌گیری از اقدامات پیشگیرانه مناسب برای به حداقل رساندن این مخاطرات

الزام۲- حصول اطمینان از اَمن بودن زنجیره تامین و انتخاب تامین‌کنندگان و فروشندگان مورد وثوق و شیوه‌ی بارگیری، حمل و تحویل ایمن و مناسب

الزام۳- تامین تجهیزات از منابع تامین داخلی برای با درنظر گرفتن ملاحظات امنیتی

۸) الزامات برون سپاری

الزام۱- حصول اطمینان از صلاحیت‌های امنیتی، پدافندی و کارآمدی شرکت‌ها و مراکز طرف قرارداد برای واگذاری طرح‌های مشاوره، نظارت و اجرا

الزام۲- عقد توافق‌نامه عدم افشای اطلاعات (NDA) در تنظیم و انعقاد قراردادها

الزام۳- پایش مستمر امنیتی از عملکرد شرکت‌ها و مراکز طرف قراردادهای برون سپاری و صدور هشدارهای لازم درصورت بروز هرگونه نقض امنیت

الزام۴- استفاده از ظرفیت‌های داخلی برای انعقاد قراردادهای برون‌سپاری با درنظر گرفتن ملاحظات امنیتی

۹) الزامات تعمیر و نگهداری

الزام۱- طراحی، ایجاد و راه‌اندازی واحد تخصصی تعمیر و نگهداری حوزه سیستم‌های کنترل صنعتی و فناوری عملیاتی برابر استانداردهای معتبر در زیرساخت مربوطه

الزام۲- انجام تعمیرات تارده‌سه در واحد تخصصی مراکز با اهمیت بالا به منظور کنترل نشت داده و استمرار خدمات ضروری و انعقاد قرارداد با مراکز تخصصی مربوطه برای رده‌های بالاتر

الزام۳- قطع هرگونه دسترسی پیمانکاران به حوزه تجهیزات کنترل صنعتی و فناوری عملیاتی از طریق فیزیکی و یا منطقی پس از انجام و اتمام ماموریت

۱۰) الزامات نیروی انسانی و آموزش

الزام۱- استفاده از کارکنان با سطح تحصیلات و دانش مناسب در زیرساخت‌های صنعتی و فناوری عملیاتی

الزام۲- اجرای آموزش‌ها، توانمندسازی، روزآمدسازی مهارتی و هوش تهدیدات بصورت نوبه‌ای و منظم

الزام۳- تدوین و اجرای برنامه عمومی امنیت کارکنان زیرساخت شامل خط مشی، مخاطرات جایگاه شغلی، غربالگری کارکنان، موافقت‌نامه‌های سطوح دسترسی، نقش‌ها و مسئولیت‌های اشخاص ثالث

الزام۴- غربالگری دقیق کارکنان جایگاه‌های کلیدی

۱۱) الزامات پدافند ترکیبی

در زیرساخت‌های صنعتی دارای زنجیره تولید خدمت و محصول، با وابستگی کارکردی بین زیرساخت و مردم، الزامات زیر رعایت شود:

الزام۱- تهیه و اجرا طرح‌های پاسخ اضطراری به تهدیدات ترکیبی و آموزش، تمرین و تکرار آن بصورت نوبه‌ای

الزام۲- تهیه و اجرای طرح‌های پدافند نوین و تمرین و احصای آمادگی به منظور کنترل پیامدهای ناشی از نشست مواد خطرناک در زیرساخت‌های صنعتی دارای فرایندها و محصولات پرخطر مانند محصولات شیمیایی، بیولوژیک، سموم و هسته‌ای

الزام۳- تدوین و اجرای برنامه‌های تضمین تداوم کارکردهای ضروری زنجیره تولید خدمت و محصول در شرایط حملات سایبری و تمرین و حصول اطمینان از آمادگی‌های لازم بطوریکه در شرایط حمله سایبری، هیچ کدام از محصولات کلیدی از کار نیافتد و هیچ یک از خدمات اساسی قطع نگردد.

الزام۴- تعیین سخنگوی مجرب و ماهر و تعیین سیاست‌های رسانه‌ای در وضعیت‌های عملیاتی سایبری، برای هر زیرساخت صنعتی به منظور کنترل و آرامش بخشی فضای افکار عمومی و اطلاع‌رسانی به موقع

الزام۵- تدوین و اجرای برنامه کاهش و مدیریت تهدیدات درون‌زا به منظور خنثی‌سازی هر نوع اقدام دشمن از درون

۱۲) الزامات الکترونیک، الکترومغناطیس و ریزپرنده

الزام۱- ایجاد پوشش حفاظتی برای زیرساخت‌های حاوی تجهیزات الکترونیک و سایبری بخصوص ذخیره‌سازها و پردازشگرها

الزام۲- استفاده از فیلتر EMP و یا EMI در ورودی برق مرکز داده شبکه کنترل صنعتی و فناوری عملیاتی بر اساس طبقه‌بندی مصوب

الزام۳- استفاده از شبکه زمین گسترده (الکترومغناطیس) در مرکز داده شبکه کنترل صنعتی و فناوری عملیاتی

الزام۴- حفاظت الکترومغناطیس در برابر شنود (TEMPEST) جهت جلوگیری از نشت اطلاعات

الزام۵- جانمایی مراکز داده تجهیزات کنترل صنعتی و فناوری عملیاتی در عمق (طبقات منفی) زمین جهت حفاظت از زیرساخت صنعتی

الزام۶- استفاده از تجهیزات منعکس کننده و یا فریب فعّال در اطراف زیرساخت صنعتی جهت جلوگیری از ردیابی و شناسایی دقیق توسط دشمن در طبقات منفی

الزام۷- استفاده از تجهیزات ضد اختلال در تجهیزات مرجع زمانی جهت تداوم همزمانی تجهیزات با ساعت جهانی

الزام۸- اجرای فرایند غربالگری با احتمال بالا در کشف آلودگی صنعتی جهت جلوگیری از ورود تجهیزات آلوده به تروجان‌های سخت افزاری و یا تراشه‌های آلوده به کاشته‌های نامطلوب صنعتی

الزام۹- استفاده مستمر از توان ارزیابی امنیتی مراکز ارزیابی مورد تایید سازمان در جهت کاهش و یا رفع تهدیدات مبتنی بر تراشه‌های الکترونیک و تجهیزات سخت افزاری و میان افزاری آلوده

الزام۱۰- کاهش و یا رفع تهدیدات مبتنی بر ربات‌های پرنده، هوشمند و کنترل پذیر از راه دور که قابلیت فعال سازی کاشته‌های صنعتی بر روی تراشه‌های تجهیزات سخت افزاری و میان افزاری زیرساخت صنعتی را دارند و اقدام برابر الگوی ابلاغی سازمان

ماده۱۳: اقدامات عملیاتی پدافند سایبری در حوزه زیرساخت صنعتی

الف) قبل از تهاجم سایبری

در این مرحله، اقدامات زیر اجرا می شود:

۱- تعریف سیاست ها، روال ها و خط مشی های عملیاتی پدافند سایبری

۲- کاهش آسیب پذیری ها و اَمن سازی زیرساخت صنعتی و فناوری عملیاتی

۳- ارتقای آمادگی برای مواجهه با رخدادها

۴- تهیه و یا بروزرسانی طرح های پاسخ به شرایط اضطرار سایبری (CERP) و استمرار خدمات ضروری (CBCP)

۵- اجرای اقدامات عملیات پیشگیرانه پدافند سایبری شامل اقدامات فوری که شرایط موجود حمله و حادثه را تغییر می دهد.

ب) در آستانه تهاجم سایبری

در این مرحله، با هدف ارتقای آمادگی و برهم زدن تصویر و تمرکز دشمن از زیرساخت صنعتی اقدامات زیر انجام می شود:

۱- تعیین وضعیت عملیاتی و آمادگی پدافند سایبری زیرساخت های صنعتی و فناوری عملیاتی متناسب با شرایط تهدید زیرساخت

۲- تنظیم و اجرای آرایش دفاعی و پدافند سایبری زیرساخت های صنعتی و فناوری عملیاتی

۳- تکمیل اقدامات عملیات پیشگیرانه پدافند سایبری ابلاغی سازمان

۴- تلاش برای کنترل و کاهش پیامدهای احتمالی

۵- ارتقای آمادگی و آماده شدن برای دفاع سایبری در برابر طیف تهدیدات

۶- انجام عملیات پیش کنش گرانه پدافند سایبری به منظور برهم زدن تمرکز دشمن درصورت امکان

۷- اقدامات مرتبط با الزامات عملیاتی در آستانه رخداد سایبری در حوزه زیرساخت صنعتی

ج) در حین تهاجم سایبری

در این مرحله، اقدامات زیر انجام می شود:

۱- کنترل و مدیریت صحنه عملیاتی تهاجم سایبری

۲- خنثی سازی تهاجم و محدودسازی منطقه مورد حمله

۳- انسداد و انحراف مسیرهای تهاجم احتمالی تهدید

۴- کاهش پیامدهای احتمالی و صدمات و خسارات ناشی از تهاجم سایبری

۵- جلوگیری از گسترش دامنه حملات به بخش های دیگر

۶- تعیین منشاء حمله و مشخصات مهاجم

۷- حفظ شواهد و قراین فنی به منظور انجام اقدامات فارنزیک و ردیابی مسیرهای تهاجم

۸- اقدامات مرتبط با الزامات عملیاتی در حین رخداد سایبری در حوزه زیرساخت صنعتی

د) پس از تهاجم سایبری

در این مرحله، اقدامات زیر اجرا می شود:

۱- بازیابی داده ها و اطلاعات از دست رفته

۲- برگرداندن سریع شبکه ها و سامانه ها به وضع عادی

۳- تحلیل حمله و یافتن منشاء و مسیرهای حمله و اهداف دشمن

۴- تجزیه و تحلیل خسارات ناشی از حمله

۵- بررسی و ثبت و مستندسازی تجربیات ناشی از حمله سایبری دشمن

۶- به روزرسانی و بازخوردگیری طرح های عملیاتی CBCP، CDRP، CERP.

۷- اقدامات مرتبط با الزامات عملیاتی پس از رخداد سایبری در حوزه زیرساخت صنعتی

ماده۱۴: نقش ها و وظایف

الف) وزارت ارتباطات و فناوری اطلاعات

۱) تهیه طرح پدافند سایبری در لایه زیرساخت با تعیین ساختار و فرمانده و الزامات فنی لازم با هدف افزایش بازدارندگی، پایداری، بازگشت پذیری و تاب آوری در مقابل انواع تهدیدات سایبری در تراز جنگ سایبری

۲) طراحی و پیاده سازی ملاحظات پدافند غیرعامل در شبکه ملی اطلاعات با هدف افزایش پایداری و تاب آوری شبکه های اختصاصی زیرساخت های صنعتی کشور مبتنی بر این شبکه تحت نظارت سازمان

۳) ایجاد ارتباطات پایدار و اَمن در شبکه ارتباطات اختصاصی زیرساخت های ویژه، حیاتی، حساس، مهم و قابل حفاظت صنعتی کشور جهت امکان ارائه خدمات درتمامی شرایط درچارچوب مقررات و ضوابط پدافند غیرعامل

۴) جلوگیری از سرایت انواع تهدیدات و حملات سایبری از بخش ارتباطات به زیرساخت های صنعتی (زیرساخت های ویژه، حیاتی، حساس، مهم و قابل حفاظت صنعتی کشور که به زیرساخت ارتباطی یا شبکه ملی اطلاعات متصل هستند باید در مقابل انواع تهدیدات و حملات سایبری بطور اخص حملات منع سرویس توزیع شده (DDOS) مصون باشند)

۵) تأمین نیازهای عملکردی و امنیتی مناسب اعم از ناحیه بندی زیرساختی، ایجاد محیط امن با سطح بندی و طبقه بندی همراه با ایجاد قابلیت حیطه بندی (خدماتی، جغرافیایی، زیرساختی) و تاب آوری حداکثری در طراحی، پیاده سازی، استقرار، پشتیبانی و بروزرسانی و ارتقای شبکه ملی اطلاعات

ب) وزارت دفاع و پشتیبانی نیروهای مسلح

۱) ایجاد و سازماندهی واحد عملیاتی پدافند سایبری صنعتی به منظور پشتیبانی عملیاتی و تخصصی تحت هدایت و راهبری و کنترل قرارگاه پدافند سایبری

۲) طراحی و تولید محصولات سخت‌افزاری و نرم‌افزاری امنیتی صنعتی و فناوری عملیاتی کلیدی با راهبری سازمان

۳) تشکیل کارگروه تهیه، تدوین، تنظیم و روزآمدسازی ضوابط، مقررات فنی-پدافندی رایانیکی (سایبری) زیرساخت‌های صنعتی و فناوری عملیاتی در دانشگاه صنعتی مالک اشتر با راهبری و هدایت سازمان

۴) آموزش و تربیت نیروی انسانی متخصص در حوزه پدافند سایبری و سایر رشته-گرایش‌های مرتبط با آن در مقاطع و سطوح مختلف

۵) راهبری، هدایت و مدیریت کاهش تهدیدات درون‌زاد زیرساخت‌های سایبری صنعتی و فناوری عملیاتی وزارت و حصول اطمینان از آسیب‌ناپذیری (حداقل آسیب‌پذیری ممکن) اطلاعاتی و ضد اطلاعاتی

ج) وزارت علوم، تحقیقات و فناوری

۱) برنامه‌ریزی جامع برای آموزش و تربیت نیروی انسانی متخصص در مقاطع کارشناسی، کارشناسی ارشد و دکتری در حوزه پدافند سایبری زیرساخت‌های صنعتی و سایر رشته-گرایش‌های مرتبط بین‌رشته‌ای با همکاری سازمان

۲) ایجاد حداقل یک دانشکده تخصصی در حوزه پدافند سایبری در دانشگاه‌های برتر کشور با هماهنگی سازمان.

۳) پژوهش و تولید و مدیریت دانش تخصصی پدافند سایبری زیرساخت‌های صنعتی و بومی‌سازی آن در نظام آموزشی ذیربط

د) وزارت صمت

۱) حمایت از طراحی و تولید محصولات و خدمات سخت‌افزاری و نرم‌افزاری صنعتی و فناوری عملیاتی کلیدی با راهبری سازمان

۲) اجتناب از ثبت سفارش محصولات غیربومی سخت‌افزاری و نرم‌افزاری صنعتی و فناوری عملیاتی سایبری که مشابه داخلی و مورد تایید سازمان دارد.

هـ) وزارت اطلاعات و سازمان اطلاعات سپاه

۱) راهبری، هدایت و مدیریت کاهش تهدیدات درون‌زاد زیرساخت‌های سایبری صنعتی و فناوری عملیاتی (با هماهنگی حراست‌ها و حفاظت اطلاعات) و حصول اطمینان از آسیب‌ناپذیری (حداقل آسیب‌پذیری ممکن) اطلاعاتی و ضد اطلاعاتی زیرساخت‌های سایبری صنعتی و فناوری عملیاتی

۲) رصد، پایش، تشخیص، برآورد و هشدار تهدیدات و آسیب‌پذیری‌ها و مخاطرات زیرساختی سایبری صنعتی و فناوری عملیاتی و اشتراک اطلاعاتی بین ذی‌نفعان

۳) برآورد دقیق و اشراف اطلاعاتی مناسب بر تهدیدات زیرساخت‌های سایبری و وابسته به فضای سایبر با اهمیت بالای صنعتی و فناوری عملیاتی و پشتیبانی اطلاعاتی از سازمان

و) سازمان پدافند غیرعامل کشور

۱) راهبری و نظارت بر مصون‌سازی و پیاده‌سازی طرح‌های پنج‌گانه در زیرساخت‌های ویژه، حیاتی، حساس، مهم و قابل حفاظت صنعتی سایبری

۲) پایش، رصد، برآورد و تشخیص و هشدار تهدیدات و کشف آسیب‌پذیری‌ها در فضای سایبر زیرساخت‌های صنعتی و فناوری عملیاتی از طریق ایجاد زیرساخت مناسب پایش و رصد در مرکز عملیات قرارگاه پدافند سایبری کشور

۳) هدایت، راهبری و نظارت بر طرح‌ریزی، آموزش، تمرین و اجرای رزمایش‌های منظم نوبه‌ای و آمادگی سایبری در زیرساخت‌های ویژه، حیاتی، حساس، مهم و قابل حفاظت صنعتی سایبری.

۴) ایجاد زیرساخت فرماندهی و کنترل در مرکز عملیات قرارگاه پدافند سایبری کشور و تجهیز و راه‌اندازی مرکز اشتراک‌گذاری اطلاعات برآورد تهدید سایبری سطح ملی (ISAC&ISAS) و برآورد عملیاتی پدافند سایبری سطح ملی

۵) ایجاد و تقویت هماهنگی عملیات پدافند سایبری در سطح ملی، با هماهنگ‌سازی معیارها، پروتکل‌ها و استانداردهای پدافند سایبری

۶) ایجاد هماهنگی در زمینه ذخیره‌سازی، مبادله و به اشتراک‌گذاری اطلاعات دارایی‌ها، قابلیت‌ها، توانایی‌ها، آمادگی‌ها

۷) ایجاد و سازماندهی یگان عملیاتی پشتیبانی پدافند سایبری و واحدهای واکنش و امداد رایانیکی و زیرساخت‌های تشخیصی تخصصی و عملیاتی‌سازی آنها در شرایط تهاجم سایبری

۸) سازماندهی و راهبری مرکز تنظیم، تصویب و ابلاغ ضوابط، مقررات، الزامات و استانداردهای پدافند سایبری صنعتی

۹) تهیه و ابلاغ اسناد موضوعی زیر و مرتبط با این دستورالعمل ظرف مدت ۲ ماه از تاریخ ابلاغ آن:

- ✓ طرح تشکیل و سازماندهی ساختار امنیت و پدافند سایبری موردنیاز در دستگاه‌های اجرایی
- ✓ جزییات معماری امنیت و پدافندسایبری چندلایه، رویکرد چندین نام‌نمای تجاری (Multi Branding) ارتباطات درهم‌تنیده، برخوردار از نسخ‌پشتیبان و نقاط گره موازی، چارچوب CARTA و معماری Zero Trust
- ✓ الگوی راهنمای تهیه اقدامات پیشگیرانه برای کاهش و مدیریت مخاطرات مرتبط با زنجیره تامین محصولات و خدمات
- ✓ راهنمای تهیه برنامه کاهش یا رفع تهدیدات زیرساخت‌های صنعتی سایبری مبتنی بر ربات‌های پرنده، هوشمند و کنترل‌پذیر از راه دور
- ✓ الگوی اقدامات مرتبط با الزامات عملیاتی در آستانه رخداد سایبری/در حین رخداد سایبری/پس از رخداد سایبری در حوزه زیرساخت صنعتی

ز) دستگاه‌های اجرایی دارای زیرساخت‌های صنعتی سایبری

۱) طراحی، استقرار و عملیاتی‌سازی سامانه پدافند سایبری به منظور پایش، رصد، تشخیص، کشف، هشدار و مقابله با تهدیدات و حملات سایبری در مقیاس جنگ سایبری علیه زیرساخت‌های صنعتی زیرمجموعه و سرمایه‌های متصل و مرتبط به آن

۲) ایجاد شبکه‌های اختصاصی و غیراشتراکی برای زیرساخت‌های ویژه، حیاتی، حساس، مهم و قابل حفاظت صنعتی و فناوری عملیاتی تحت نظارت سازمان

۳) استفاده از راهکارهای جزیره‌ای‌سازی شبکه‌های صنعتی و فناوری عملیاتی برای مقابله و کاهش اثرات حملات سایبری و تمرین مستمر آنها

ماده۱۵: دستورات هماهنگی

کلیه دستگاه‌های دارای زیرساخت‌های صنعتی و فناوری عملیاتی موظّف به اجرای موارد زیر هستند:

۱) تهیه، بازنگری، بروزرسانی و پیاده‌سازی طرح‌های عملیاتی پدافند سایبری زیرساخت‌های صنعتی و فناوری عملیاتی اعم از:

- ✓ طرح امن‌سازی و مصون‌سازی زیرساخت سایبری - صنعتی
- ✓ طرح کاهش آسیب‌پذیری‌های زیرساخت سایبری - صنعتی
- ✓ طرح مدیریت وابستگی‌های متقابل زیرساخت سایبری - صنعتی
- ✓ طرح ارزیابی و ارتقاء آمادگی‌های زیرساخت سایبری - صنعتی
- ✓ طرح عملیاتی تداوم کارکردهای اساسی
- ✓ طرح پاسخ اضطراری به حوادث و تهدیدات زیرساخت سایبری - صنعتی
- ✓ طرح بازیابی و برگشت‌پذیری زیرساخت سایبری - صنعتی

۲) اتصال و ارتباط برخط به مرکز اشتراک‌گذاری و تحلیل اطلاعات تهدید (ISAC) سازمان و رعایت ملاحظات پدافند سایبری ابلاغی سازمان

۳) تهیه و تدوین اسناد پدافند سایبری زیرساخت‌های صنعتی و فناوری حوزه‌های زیرمجموعه و بخشی خود (SSP) ظرف مدت یک سال از ابلاغ این دستورالعمل

۴) تدوین و پیاده‌سازی برنامه عملیاتی مدیریت و کاهش تهدیدات درون‌زاد زیرساخت‌های صنعتی و فناوری عملیاتی

۵) اجرای برنامه‌های آموزشی منسجم و رزمایش هدفمند ارتقاء آمادگی و توانمندسازی مدیران و کارشناسان و مدیران متولی زیرساخت‌های صنعتی و فناوری عملیاتی

۶) پیاده‌سازی رویکرد انتقال اقدامات و برنامه‌های پدافند سایبری زیرساخت‌های صنعتی و فناوری عملیاتی از پیوست به ذات طرح‌های توسعه زیرساختی در مراحل مطالعه و طراحی

۷) تهیه و اجرای برنامه‌های مصون‌سازی تخصصی و مدیریت مخاطرات در زیرساخت‌های صنعتی و فناوری عملیاتی با خطرپذیری بالا

۸) تهیه گزارش‌های سالانه شامل برآورد تهدیدات، آسیب‌پذیری‌ها، وابستگی‌های متقابل و مخاطرات و اقدامات انجام شده هر دستگاه در برابر آنها همراه با تجزیه و تحلیل و ارسال به سازمان

ماده۱۶– وفق تبصره۱ قانون تشکیل سازمان، مستنکفین از اجرای الزامات و ضوابط این دستورالعمل در مراکز و دستگاه‌های اجرایی مشمول، علاوه بر جبران خسارات وارد شده، به مجازات موضوع ماده (۵۷۶) کتاب پنجم قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده) مصوب ۱۳۷۵/۳/۰۲ محکوم می‌شوند و چنانچه خسارتی وارد نشده باشد برابر قانون رسیدگی به تخلفات اداری مصوب ۱۳۷۲/۰۹/۰۷ با مستنکف رفتار خواهد شد.

ماده۱۷– سازمان بر حُسن اجرای این دستورالعمل، نظارت نموده و اجرای آن را بصورت سالیانه به کمیته دائمی گزارش کند.

ماده۱۸– این تصویب‌نامه در هجده ماده در تاریخ بیست و هشتم شهریورماه سال یکهزار و چهارصد و دو هجری شمسی در هفتاد و هفتمین جلسه کارگروه (کمیته) دائمی به تصویب رسید. دستورالعمل عملیاتی پدافند سایبری زیرساخت‌های صنعتی کشور مشتمل بر هجده ماده که در تاریخ ۱۴۰۲/۰۶/۲۸ در هفتادوهفتمین جلسه کارگروه (کمیته) دائمی پدافند غیرعامل کشور به تصویب رسید.

دستورالعمل پیش‌گیری و مقابله با حوادث سایبری در وضعیت‌های سایبری مختلف

دستورالعمل پیش‌گیری و مقابله با حوادث سایبری در وضعیت‌های سایبری مختلف، حاوی الگو و اقدام‌های اساسی با هدف مقابله با حملات سایبری احتمالی، حملات سایبری قریب‌الوقوع، حملات سایبری قطعی و حوادث سایبری در دستگاه‌ها می‌باشد.

۱ وضعیت‌های سایبری

وضعیت‌های سایبری ممکن، شامل چهار وضعیت سفید (تحت کنترل) سایبری، زرد سایبری (حمله سایبری احتمالی)، نارنجی سایبری (حمله سایبری قریب‌الوقوع) و قرمز سایبری (حمله سایبری قطعی) می‌باشد.

۲ شاخص‌های تعیین وضعیت سایبری

شاخص‌های تعیین وضعیت سایبری کشور، عبارتند از:

- وجود یا عدم وجود، نوع و سطح بلوغ منشأ تهدید سایبری علیه دارایی‌های سایبری دستگاه
- جدیت منشأ تهدید، شامل وجود یا عدم وجود قصد، انگیزه و اراده تهدید، وجود یا عدم وجود پیشینه‌ای از اقدام‌های عملیاتی و مهیا بودن یا نبودن شرایط محیطی
- وجود یا فقدان طرح یا برنامه مشخص منشأ تهدید سایبری برای انجام حمله علیه دارایی‌های سایبری دستگاه
- احتمال وقوع حمله سایبری توسط منشأ تهدید، شامل چهار وضعیت غیرمحتمل، محتمل، قریب‌الوقوع و قطعی
- مشخصات حمله سایبری احتمالی، شامل ابعاد، سطح و شدت حمله
- احتمال موفقیت حمله احتمالی سایبری (احتمال وقوع حادثه ناشی از حمله سایبری)
- پیامدهای احتمالی حادثه، اعم از پیامد سایبری، فیزیکی، اجتماعی یا ترکیبی

مقادیر شاخص‌های فوق، برای هر یک از وضعیت‌های سایبری، به شرح ذیل است:

الف) وضعیت سفید سایبری (تحت کنترل)

- عدم وجود منشأ تهدید سایبری علیه دارایی‌های سایبری دستگاه **یا**
- فقدان انگیزه و اراده تهدید، عدم وجود سوابق اقدام، مهیا نبودن شرایط محیطی **یا**
- فقدان طرح یا برنامه حمله سایبری به دارایی‌های سایبری دستگاه توسط منشأ تهدید سایبری **یا**
- غیرمحتمل بودن وقوع حمله سایبری علیه دارایی‌های سایبری دستگاه **یا**
- ابعاد، سطح و شدت حمله احتمالی سایبری: فاقد مقدار و فاقد اهمیت **یا**
- احتمال موفقیت حمله احتمالی سایبری (احتمال وقوع حادثه): فاقد مقدار و فاقد اهمیت **یا**
- پیامدهای احتمالی حادثه: فاقد مقدار و فاقد اهمیت

ب) وضعیت زرد سایبری (حمله سایبری احتمالی)

- وجود هکر یا گروه هکری دارای توانایی و آمادگی تهاجمی سایبری و
- برخوردار از انگیزه و اراده تهدید قابل توجه، پیشینه تلاش یا اقدام مخرّب و شرایط محیطی تا حدودی مهیا و
- وجود طرح/برنامه کلی (و عدم وجود سناریوی مشخص) حمله سایبری به دارایی‌های سایبری دستگاه و
- محتمل بودن وقوع حمله سایبری و
- مبهم یا محدود بودن ابعاد، سطح و شدت حمله احتمالی سایبری و
- محتمل بودن موفقیت حمله احتمالی سایبری (محتمل بودن وقوع حادثه) و
- پیامد احتمالی صرفاً سایبری ناشی از وقوع حادثه

ج) وضعیت نارنجی سایبری (حمله سایبری قریب‌الوقوع)

- وجود گروه هکری سازمان‌یافته، مزدوران سایبری کشور متخاصم یا گروه‌های تروریستی و
- برخوردار از انگیزه و اراده تهدید قوی، پیشینه اقدام مخرّب موفق و شرایط محیطی مهیا و
- وجود طرح کلی و برنامه (حداقل یک سناریو برای اجرای حمله در یک حوزه خاص) حمله سایبری و
- قریب‌الوقوع بودن حمله سایبری و
- گستردگی ابعاد، منطقه‌ای یا ملی بودن سطح و شدید بودن حمله احتمالی سایبری و
- زیاد بودن احتمال موفقیت حمله احتمالی سایبری (وقوع حادثه) و
- ترکیبی (سایبری و فیزیکی) بودن پیامدهای احتمالی ناشی از وقوع حادثه

د) وضعیت قرمز سایبری (حمله سایبری قطعی)

- وجود گروه‌های تروریستی یا یگان‌های سایبری نظامی کشور متخاصم و
- برخوردار از انگیزه و اراده تهدید بسیار قوی، پیشینه اقدام فاجعه‌بار و شرایط محیطی بسیار مهیا و
- وجود طرح کلی و برنامه حاوی سناریوهای مختلف برای اجرای حمله سایبری در حوزه‌های مختلف و
- قطعی بودن وقوع حمله سایبری و
- فراگیر بودن ابعاد، ملی بودن سطح و فاجعه‌بار (بسیار شدید) بودن حمله احتمالی سایبری و
- خیلی زیاد بودن احتمال موفقیت حمله احتمالی سایبری و
- ترکیبی (سایبری و فیزیکی و اجتماعی) بودن پیامدهای احتمالی ناشی از وقوع حادثه

۳ مسئول تعیین وضعیت سایبری

- پیشنهاد وضعیت سایبری یک دستگاه، بر عهده بالاترین مقام اجرایی دستگاه و تعیین (تائید) آن بر عهده دستگاه هماهنگ‌کننده می‌باشد
- تعیین وضعیت سایبری با این شیوه، حداکثر برای ۱۰ دستگاه اجرایی، قابل انجام می‌باشد
- پیشنهاد وضعیت سایبری سفید، زرد و نارنجی، برای دستگاه‌های اجرایی از سطح یک وزارت‌خانه یا حوزه تا سطح ملی، بر عهده دستگاه هماهنگ‌کننده و تعیین (تائید) آن بر عهده مرکز ملی فضای مجازی به‌عنوان فرمانده فضای مجازی کشور است
- پیشنهاد وضعیت سایبری قرمز، بر عهده مرکز ملی فضای مجازی و تعیین (تائید) آن بر عهده شورای عالی امنیت ملی است

۴ چارچوب اقدام‌های دستگاه‌ها در طرح پیش‌گیری و مقابله با حوادث سایبری

در طرح پاسخ اضطراری سایبری، اقدام‌ها بر اساس چارچوب و الگوی زیر، انجام می‌گیرند:

الف) ایجاد آمادگی (ارتقاء عادی آمادگی) در مقابل انواع تهدیدها، حملات و حوادث سایبری (در وضعیت سفید سایبری)

ب) آماده‌باش سطح یک (ارتقاء فوری آمادگی) در مقابل حمله سایبری احتمالی (در وضعیت زرد سایبری)

ج) آماده‌باش سطح دو (ارتقاء آنی آمادگی) در مقابل حمله سایبری قریب‌الوقوع (در وضعیت نارنجی سایبری)

د) مقابله با حمله سایبری قطعی یا در حال وقوع (در وضعیت قرمز سایبری)

ه) رسیدگی به حادثه سایبری و بازیابی پیامدهای آن (پس از وقوع حادثه سایبری، در هر وضعیت سایبری)

۵ اقدام‌های دستگاه‌ها در هر وضعیت سایبری

پس از تعیین و ابلاغ تغییر وضعیت سایبری دستگاه و متناسب با وضعیت سایبری جدید، لازم است تیم امنیت سایبری دستگاه، نسبت به انجام اقدام‌های مشخص شده برای آن وضعیت، به شرح ذیل، اقدام نمایند:

الف) اقدام‌های وضعیت سفید سایبری

در وضعیت سفید سایبری، با هدف ایجاد آمادگی (ارتقاء عادی آمادگی) در مقابل انواع تهدیدها، حملات و حوادث سایبری، مجموعه‌ای از اقدام‌ها به شرح ذیل، باید توسط دستگاه انجام گیرند:

۱. تعیین و صدور حکم برای مسئول امنیت سایبری دستگاه

۲. تعیین و صدور احکام اعضاء کمیته امنیت سایبری دستگاه

۳. تشکیل جلسات منظم کمیته امنیت سایبری دستگاه

۴. تدوین، تصویب و ابلاغ خط‌مشی امنیت سایبری دستگاه

۵. شناخت، احصاء ویژگی‌ها، ارزش‌گذاری و طبقه‌بندی دارایی‌های سایبری دستگاه و تدوین سند دارایی‌های سایبری دستگاه

۶ شناسایی و رفع انواع آسیب‌پذیری‌های موجود در دارایی‌های سایبری دستگاه، شامل:

- شناسایی و رفع آسیب‌پذیری‌های شناخته‌شده از طریق پویش امنیتی و وصله‌زنی خودکار آسیب‌پذیری‌ها
- شناسایی و رفع آسیب‌پذیری‌های روز صفر از طریق آزمون نفوذ توسط شرکت‌های دارای مجوز و برگزاری مسابقات باگ‌بانتی از طریق سکوهای دارای مجوز
- شناسایی و رفع آسیب‌پذیری‌های ایجاد شده توسط دشمن در دارایی‌های حیاتی زیرساخت، با استفاده از ظرفیت آزمایشگاه ارزیابی صیانتی وزارت دفاع و پشتیبانی نیروهای مسلح ج.ا.ا

۷ رصد، پایش و شناسایی تهدیدهای سایبری موجود علیه دارایی‌های سایبری دستگاه، شامل:

- شناسایی منشأ تهدیدهای سایبری (هکرها، تیم‌های هکری، سرویس‌های امنیتی و یگان‌های سایبری متخاصم) فعال علیه دارایی‌های سایبری دستگاه بر اساس گزارش‌های برآورد تهدید سایبری مراجع ملی از قبل سازمان پدافند غیرعامل، قرارگاه سایبری و تهدیدات نوین و ...
- شناسایی آلودگی‌های سایبری دارایی‌های سایبری دستگاه، بر اساس اطلاعات دریافتی از دستگاه هماهنگ‌کننده و انجام پویش امنیتی این دارایی‌ها

۸ ارزیابی و تحلیل مخاطرات امنیتی دارایی‌های سایبری دستگاه، شامل:

- سند دارایی‌های سایبری دستگاه
- فهرست تهدیدهای سایبری موجود علیه دارایی‌های سایبری دستگاه
- فهرست آسیب‌پذیری‌های رفع‌نشده، اعم از شناخته‌شده، روز صفر و ایجاد شده
- فهرست مخاطرات امنیتی دارایی‌های سایبری دستگاه
- ارزیابی شدت و احتمال وقوع هر یک از مخاطرات امنیتی دارایی‌های سایبری دستگاه و تخمین میزان خسارات احتمالی ناشی از وقوع آن

۹ تدوین طرح امن‌سازی دارایی‌های سایبری دستگاه، حاوی چهارجنبه ساختاری (معماری سیستمی زیرساخت)، سازمانی (تشکیلات امنیت)، پرسنلی (تیم امنیت) و فناورانه (ابزارها و سامانه‌های امنیتی مورد نیاز)، شامل:

- تعیین نحوه مدیریت انواع مخاطرات موجود علیه دارایی‌های سایبری دستگاه (اجتناب، پذیرش، انتقال و رفع)
- تعیین نحوه رفع (محافظت از دارایی‌های سایبری در مقابل) مخاطرات سایبری غیر قابل اجتناب، غیر قابل پذیرش و غیر قابل انتقال ناشی از دسترسی غیرمجاز، نفوذ و حمله انواع تهدیدهای سایبری با منشأ داخلی یا خارجی

۱۰ اجرای طرح امن‌سازی دارایی‌های سایبری دستگاه، شامل:

- تأمین سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح امن‌سازی دارایی‌های سایبری دستگاه
- استقرار، پیکربندی و آزمون سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح امن‌سازی دارایی‌های سایبری دستگاه
- راهبری سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح امن‌سازی دارایی‌های سایبری دستگاه

۱۱ تدوین طرح تضمین تداوم مأموریت‌های دستگاه در مواجهه با حملات سایبری (BCP)، حاوی چهار جنبه ساختاری (معماری سیستمی زیرساخت)، سازمانی (تشکیلات امنیت)، پرسنلی (تیم امنیت) و فناورانه (ابزارها و سامانه‌های امنیتی مورد نیاز)، شامل:

- تعیین نحوه ایجاد و سنجش میزان آمادگی سایبری دستگاه در مقابل حملات سایبری احتمالی (تمرین یا رزمایش سایبری)
- تعیین نحوه تشخیص و مقابله با حمله سایبری احتمالی (ارتقاء فوری آمادگی در وضعیت زرد سایبری)
- تعیین نحوه تشخیص و مقابله با حمله سایبری قریب‌الوقوع (ارتقاء آنی آمادگی در وضعیت نارنجی سایبری)
- تعیین نحوه مقابله با حمله سایبری قطعی یا در حال وقوع (در وضعیت قرمز سایبری)

۱۲ اجرای طرح تضمین تداوم مأموریت‌های دستگاه، در مواجهه با حملات سایبری و رزمایش‌های سایبری

- تأمین سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح تضمین تداوم مأموریت‌های دستگاه
- استقرار، پیکربندی و آزمون سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح تضمین تداوم مأموریت‌های دستگاه
- راهبری سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح تضمین تداوم مأموریت‌های دستگاه

۱۳ تدوین طرح بازیابی دارایی‌های سایبری از پیامدهای ناشی از حادثه سایبری (DRP) دستگاه، حاوی چهارجنبه ساختاری (معماری سیستمی زیرساخت)، سازمانی (تشکیلات امنیت)، پرسنلی (تیم امنیت) و فناورانه (ابزارها و سامانه‌های امنیتی موردنیاز)، شامل:

- تعیین نحوه تشخیص و صحت‌سنجی حادثه سایبری و گزارش‌دهی آن به دستگاه هماهنگ‌کننده
- تعیین نحوه رسیدگی اولیه به (محدودسازی، قرنطینه و کنترل) حادثه سایبری
- تعیین نحوه رسیدگی تکمیلی به (شناسایی و تحلیل ادله (فارنزیکس)) حادثه سایبری به‌منظور تعیین منشأ، ابعاد و چگونگی وقوع حادثه سایبری و تعیین میزان خسارات ناشی از آن
- تعیین نحوه پاک‌سازی آلودگی‌های ناشی از حادثه سایبری
- تعیین نحوه بازیابی و ترمیم خسارات ناشی از حادثه سایبری
- تعیین نحوه ابقاء (برقراری) خدمات دارایی‌های سایبری دستگاه

۱۴ اجرای طرح بازیابی دارایی‌های سایبری دستگاه در مواجهه با حادثه سایبری و رزمایش‌های سایبری

- تأمین سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح بازیابی دارایی‌های سایبری دستگاه
- استقرار، پیکربندی و آزمون سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح بازیابی دارایی‌های سایبری دستگاه
- راهبری سازوکارهای فناورانه، ساختاری، فرآیندی و انسانی پیش‌بینی شده در طرح بازیابی دارایی‌های سایبری دستگاه

۱۵ اشتراک‌گذاری اطلاعات امنیت سایبری دستگاه با دستگاه هماهنگ‌کننده

- اطلاعات دارایی‌های سایبری دستگاه
- اطلاعات تهدیدهای سایبری دستگاه
- اطلاعات آسیب‌پذیری‌های سایبری رفع‌شده توسط دستگاه
- اطلاعات حملات سایبری انجام شده علیه دارایی‌های سایبری دستگاه
- اطلاعات حوادث سایبری به‌وقوع پیوسته در دستگاه
- اطلاعات خسارات ناشی از حوادث سایبری به‌وقوع پیوسته

ب) اقدام‌های وضعیت زرد سایبری

در وضعیت زرد سایبری، حمله سایبری احتمالی علیه دارایی‌های سایبری دستگاه شناسایی شده است و بر این اساس، با هدف آماده‌باش سطح یک (ارتقاء فوری آمادگی) در مقابل این حمله سایبری احتمالی، مجموعه‌ای از اقدام‌ها مطابق بخش تعیین نحوه تشخیص و مقابله با حمله سایبری احتمالی از طرح تضمین تداوم مأموریت‌های دستگاه در مواجهه با حملات سایبری و حداقل شامل اقدام‌های ذیل، باید توسط دستگاه انجام گیرند:

۱ تعیین و در دسترس بودن نماینده دستگاه از ساعت ۷:۰۰ تا ۲۲:۰۰ جهت همکاری با دستگاه هماهنگ‌کننده

۲ در دسترس قرار دادن آخرین نسخه از اطلاعات دارایی‌های فناوری اطلاعات دستگاه (اطلاعات ساختار، تجهیزات و خدمات شبکه و مسئول مدیریت/پشتیبانی هر یک از آن‌ها)

۳ صدور هشدار سایبری و آگاهی‌رسانی به دستگاه‌های تابعه و پرسنل مرتبط با فضای سایبر دستگاه

۴ اطمینان از قطع کلیه دسترسی‌های از راه دور مدیریتی ایجاد شده برای مدیران و پیمانکاران به تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۵ پشتیبان‌گیری از کلیه اطلاعات تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۶ اطمینان از صحت اطلاعات پشتیبان و نگهداری آن‌ها به صورت آفلاین در محل امن

۷ اطمینان از رفع تمامی آسیب‌پذیری‌های شناخته‌شده در تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۸ اطمینان از صحت تنظیمات مربوط به ثبت لاگ تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۹ اطمینان از ثبت لاگ تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۱۰ اطمینان از کفایت منابع لازم برای ثبت و نگه‌داری لاگ، حداقل برای مدت ۳ ماه و عدم رونویسی آن‌ها

۱۱ حذف حساب‌های کاربری غیرضروری و بلااستفاده در شبکه سازمانی، تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۱۲ الزام کاربران شبکه سازمانی دستگاه به تغییر کلمات عبور و استفاده از کلمات عبور پیچیده، مطابق اصول مندرج در خط مشی امنیتی

۱۳ به‌روز رسانی تمامی نرم‌افزارها و میان‌افزارهای تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه و اطمینان از استقرار آخرین نسخه پایدار آن‌ها

۱۴ به‌روز رسانی تمامی سامانه‌های امنیتی، به‌ویژه ضد بدافزار

۱۵ اطمینان از پوشش تمامی دارایی‌های سایبری دستگاه توسط سامانه‌های امنیتی

۱۶ اطمینان از رصد دوره‌ای (حداکثر ۲۴ ساعته) دارایی‌های سایبری دستگاه و امنیت آن‌ها توسط تیم یا افراد مسئول

۱۷ اطمینان از رعایت خط مشی امنیتی دستگاه توسط مدیران، پیمانکاران و کاربران دستگاه، به‌ویژه افراد مسئول در حوزه امنیت سایبری

۱۸ اطمینان از زون‌بندی مناسب شبکه و تفکیک بخش‌ها و خدمات مختلف شبکه، متناسب با سطح طبقه‌بندی خدمات و افراد دریافت‌کننده خدمات

- اطمینان از رعایت افزونگی برای دارایی‌های کلیدی سایبری دستگاه و راه‌اندازی نسخه افزونه سامانه‌های اطلاعاتی کلیدی دستگاه به‌صورت Active Standby، به‌نحوی که در صورت وقوع حادثه و از دسترس خارج شدن آن سامانه، نسخه افزونه بلافاصله قابلیت جایگزینی داشته باشد
- عدم تغییر سامانه‌های اطلاعاتی موجود یا عملیاتی نمودن خدمت (سامانه اطلاعاتی) جدید، قبل از انجام ارزیابی امنیتی و رفع آسیب‌پذیری‌های احتمالی

۱۹ اطمینان از تغییر پیکربندی سامانه‌های امنیتی، تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه، نسبت به مقادیر پیش‌فرض

۲۰ اطمینان از فعال بودن سازوکار تحلیل حوادث امنیتی در شبکه سازمانی دستگاه

۲۱ اعمال محدودیت در دسترسی افراد مختلف، متناسب با اختیارات و مسئولیت آن‌ها و صرفاً در زمان‌های موردنیاز

۲۲ حصول اطمینان از آمادگی تیم امنیت سایبری دستگاه جهت مواجهه با حمله سایبری احتمالی، از طریق برنامه‌ریزی و برگزاری تمرین سایبری

۲۳ اعلام هرگونه رفتار مشکوک در شبکه، کاربران و سامانه‌ها به دستگاه هماهنگ‌کننده (شماره تلفن .....-۰۲۱ یا آدرس پست الکترونیکی XXXXX@YYY.ir)

۲۴ آمادگی رسیدگی به حوادث احتمالی و همکاری با تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده جهت:

- ✓ هماهنگی حضور تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده در محل دستگاه
- ✓ اعطای فوری کلیه دسترسی‌های کاربری و مدیریتی لازم به این تیم، جهت انجام عملیات رسیدگی به حادثه

ج) اقدام‌های وضعیت نارنجی سایبری

در وضعیت نارنجی سایبری، حمله سایبری قریب‌الوقوع علیه دارایی‌های سایبری دستگاه شناسایی شده است و بر این اساس، با هدف آماده‌باش سطح دو (ارتقاء آنی آمادگی) در مقابل حمله سایبری قریب‌الوقوع، مجموعه‌ای از اقدام‌ها مطابق بخش تعیین نحوه تشخیص و مقابله با حمله سایبری قریب‌الوقوع از طرح تضمین تداوم مأموریت‌های دستگاه در مواجهه با حملات سایبری و حداقل شامل اقدام‌های ذیل، باید توسط دستگاه انجام گیرند:

۱ تعیین و در دسترس بودن نماینده دستگاه به‌صورت شبانه‌روزی (۷*۲۴) جهت همکاری با دستگاه هماهنگ‌کننده

۲ در دسترس قرار دادن آخرین نسخه از اطلاعات دارایی‌های فناوری اطلاعات دستگاه (اطلاعات ساختار، تجهیزات و خدمات شبکه و مسئول مدیریت/پشتیبانی هر یک از آن‌ها)

۳ صدور هشدار سایبری و آگاهی‌رسانی به دستگاه‌های تابعه و پرسنل مرتبط با فضای سایبر دستگاه

۴ اطمینان از قطع کلیه دسترسی‌های از راه دور مدیریتی و کاربری ایجاد شده برای مدیران، پیمانکاران و کاربران به تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه و محدود نمودن دسترسی کاربران به خدماتی که کاربر خارج از کشور ندارند، صرفاً به دسترسی از طریق شبکه IP داخل کشور (ایران اکسس نمودن)

۵ پشتیبان‌گیری از کلیه اطلاعات ضروری تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۶ اطمینان از ثبت لاگ تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۷ اطمینان از کفایت منابع لازم برای ثبت و نگه‌داری لاگ، حداقل برای مدت ۳ ماه و عدم رونویسی آن‌ها

۸ تغییر خودکار کلمات عبور تمامی کاربران شبکه سازمانی دستگاه، مطابق اصول مندرج در خط‌مشی امنیتی

۹ اطمینان از به‌روز بودن تمامی سامانه‌های امنیتی، به‌ویژه ضد بدافزار

۱۰ رصد مداوم دارایی‌های سایبری دستگاه و امنیت آن‌ها توسط تیم یا افراد مسئول

۱۱ اطمینان از رعایت کنترل دسترسی بین زون‌های مختلف شبکه، به ویژه خدمات بیرونی دستگاه از سامانه‌های اطلاعاتی داخلی (اداری)

۱۲ اطمینان از رعایت افزونگی برای سامانه‌های اطلاعاتی ارائه‌دهنده خدمات دستگاه و راه‌اندازی نسخه افزونه این سامانه‌ها به صورت Active Standby، به نحوی که در صورت وقوع حادثه و از دسترس خارج شدن آن سامانه، نسخه افزونه بلافاصله قابلیت جایگزینی داشته باشد

۱۳ عدم تغییر سامانه‌های اطلاعاتی موجود یا عملیاتی نمودن خدمت (سامانه اطلاعاتی) جدید

۱۴ اطمینان از قابل اعتماد بودن پیکربندی سامانه‌های امنیتی، تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۱۵ اعمال شدید محدودیت در دسترسی افراد مختلف، متناسب با اختیارات و مسئولیت آن‌ها و صرفاً در موارد ضروری

۱۶ حصول اطمینان از آمادگی تیم امنیت سایبری دستگاه جهت مواجهه با حمله سایبری احتمالی، از طریق برگزاری جلسه هماهنگی و تنظیم صورتجلسه انجام کلیه مأموریت‌های فوق

۱۷ اعلام هرگونه رفتار مشکوک در شبکه، کاربران و سامانه‌ها به دستگاه هماهنگ‌کننده (شماره تلفن .....-۰۲۱ یا آدرس پست الکترونیکی XXXXX@YYY.ir)

۱۸ آمادگی رسیدگی به حوادث احتمالی و همکاری با تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده جهت:

- هماهنگی حضور تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده در محل دستگاه
- اعطای فوری کلیه دسترسی‌های کاربری و مدیریتی لازم به این تیم، جهت انجام عملیات رسیدگی به حادثه

د) اقدام‌های وضعیت قرمز سایبری

در وضعیت قرمز سایبری، وقوع حمله سایبری قطعی علیه دارایی‌های سایبری دستگاه شناسایی شده است و بر این اساس، با هدف مقابله با حمله سایبری قطعی یا در حال وقوع، مجموعه‌ای از اقدام‌ها مطابق بخش تعیین نحوه تشخیص و مقابله با حمله سایبری قطعی از طرح تضمین تداوم مأموریت‌های دستگاه در مواجهه با حملات سایبری و حداقل شامل اقدام‌های ذیل، باید توسط دستگاه انجام گیرند:

۱ تعیین و حضور فیزیکی نماینده دستگاه به صورت شبانه‌روزی (۲۴*۷) در محل خدمت، جهت انجام مداوم مأموریت‌ها و همکاری با دستگاه هماهنگ‌کننده

۲ در دسترس قرار دادن آخرین نسخه از اطلاعات دارایی‌های فناوری اطلاعات دستگاه (اطلاعات ساختار، تجهیزات و خدمات شبکه و مسئول مدیریت/پشتیبانی هر یک از آن‌ها)

۳ صدور هشدار سایبری و آگاهی‌رسانی به دستگاه‌های تابعه و پرسنل مرتبط با فضای سایبر دستگاه

۴ اطمینان از قطع کلیه دسترسی‌های از راه دور مدیریتی و کاربری ایجاد شده برای مدیران، پیمانکاران و کاربران به تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه و محدود نمودن دسترسی کاربران به خدماتی که کاربر خارج از کشور ندارند، صرفاً به دسترسی از طریق شبکه IP داخل کشور (ایران اکسس نمودن)

۵ پشتیبان‌گیری از کلیه اطلاعات ضروری تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۶ اطمینان از ثبت لاگ تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۷ اطمینان از کفایت منابع لازم برای ثبت و نگه‌داری لاگ، حداقل برای مدت ۳ ماه و عدم رونویسی آن‌ها

۸ تغییر خودکار کلمات عبور تمامی کاربران شبکه سازمانی دستگاه، مطابق اصول مندرج در خط مشی امنیتی

۹ اطمینان از به‌روز بودن تمامی سامانه‌های امنیتی، به‌ویژه ضد بدافزار

۱۰ رصد مداوم دارایی‌های سایبری دستگاه و امنیت آن‌ها توسط تیم یا افراد مسئول، الزاماً به‌صورت محلی

۱۱ اطمینان از رعایت کنترل دسترسی بین زون‌های مختلف شبکه، به ویژه خدمات بیرونی دستگاه از سامانه‌های اطلاعاتی داخلی (اداری)

۱۲ اطمینان از رعایت افزونگی برای سامانه‌های اطلاعاتی ارائه‌دهنده خدمات دستگاه و راه‌اندازی نسخه افزونه این سامانه‌ها به‌صورت Active Standby، به‌نحوی که در صورت وقوع حادثه و از دسترس خارج شدن آن سامانه، نسخه افزونه بلافاصله قابلیت جایگزینی داشته باشد

۱۳ عدم تغییر سامانه‌های اطلاعاتی موجود یا عملیاتی نمودن خدمت (سامانه اطلاعاتی) جدید

۱۴ اطمینان از قابل اعتماد بودن پیکربندی سامانه‌های امنیتی، تجهیزات شبکه، سامانه‌های اطلاعاتی و پایگاه‌های داده دستگاه

۱۵ اعمال شدید محدودیت در دسترسی افراد مختلف، متناسب با اختیارات و مسئولیت آن‌ها و صرفاً در موارد ضروری

۱۶ حصول اطمینان از آمادگی تیم امنیت سایبری دستگاه جهت مواجهه با حمله سایبری احتمالی، از طریق برگزاری جلسات هماهنگی روزانه و تنظیم صورتجلسه انجام کلیه مأموریت‌های فوق

۱۷ اعلام هرگونه رفتار مشکوک در شبکه، کاربران و سامانه‌ها به دستگاه هماهنگ‌کننده (شماره تلفن .....-۰۲۱ یا آدرس پست الکترونیکی XXXXX@YYY.ir)

۱۸ آمادگی رسیدگی به حوادث احتمالی و همکاری با تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده جهت:

۱۹ هماهنگی حضور تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده در محل دستگاه

۲۰ اعطای فوری کلیه دسترسی‌های کاربری و مدیریتی لازم به این تیم، جهت انجام عملیات رسیدگی به حادثه

ه) اقدام‌های پس از وقوع حادثه سایبری

در صورت وقوع حادثه سایبری، با هدف رسیدگی به حادثه و بازیابی خسارات ناشی از آن، مجموعه‌ای از اقدام‌ها مطابق طرح بازیابی دارایی‌های سایبری دستگاه و حداقل شامل اقدام‌های ذیل، باید توسط دستگاه انجام گیرند:

۱ صحت‌سنجی حادثه سایبری

۲ گزارش نمودن حادثه سایبری به دستگاه هماهنگ‌کننده

۳ فراهم نمودن امکان حضور تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده در محل وقوع حادثه

۴ فراهم نمودن امکان دسترسی تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده به اطلاعات و سامانه‌های متأثر از حادثه سایبری

۵ فراهم نمودن امکان رسیدگی اولیه به (کنترل و مهار) حادثه سایبری توسط تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده

۶ فراهم‌نمودن امکان رسیدگی تکمیلی به (شناسایی و تحلیل ادله (فارنزیکس)) حادثه سایبری به‌منظور تعیین منشأ، ابعاد و چگونگی وقوع حادثه سایبری و تعیین میزان خسارات ناشی از آن، توسط تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده

۷ پاک‌سازی آلودگی‌های ناشی از حادثه سایبری با هدایت تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده و مجری‌گری تیم امنیت دستگاه یا توسط ارائه‌دهنده خدمات امنیتی دارای مجوز

۸ بازیابی و ترمیم خسارات ناشی از حادثه سایبری با هدایت تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده و مجری‌گری تیم امنیت دستگاه یا توسط ارائه‌دهنده خدمات امنیتی دارای مجوز

۹ ابقاء (برقراری) خدمات دارایی‌های سایبری دستگاه با هدایت تیم رسیدگی به حادثه دستگاه هماهنگ‌کننده و مجری‌گری تیم امنیت دستگاه یا توسط ارائه‌دهنده خدمات امنیتی دارای مجوز

۱۰ اجرای توصیه‌های تیم رسیدگی به حادثه و ارتقاء وضعیت امنیت سایبری دستگاه