جمهوری اسلامی ایران
وزارت کشور
استانداری آذربایجان شرقی

سال ۱۳۹۸
سال رونق تولید

سازمان پدافند غیرعامل کشور

ماهنامه اداره کل پدافند غیر عامل

شماره ۳۲، اردیبهشت ماه ۱۳۹۸

رهبر معظم انقلاب:

نیروی انتظامی با ناامن کننده فضای مجازی برخورد جدی کند

رئیس سازمان پدافند غیرعامل کشور:

مطالعه طرح پدافند غیرعامل کلانشهر تبریز باید در اولویت برنامه‌های سال ۱۳۹۸ شهرداری باشد

سرپرست اداره کل پدافند غیرعامل استانداری آذربایجان شرقی منصوب شد

در این شماره می‌خوانید:


امروز اهمیت پدافند غیر عامل
قاعدتاً برای مسئولین بایستی
شناخته شده باشد اهتمام شما
کار را پیش می‌برد.
مقام معظم رهبری، فرماندهی کل قوا
حضرت امام خامنه‌ای

جمهوری اسلامی ایران
وزارت کشور
استانداری آذربایجان شرقی

سازمان پدافند غیرعامل کشور

ماهنامه اداره کل پدافند غیر عامل – شماره ۳۲

مدیر مسئول:

محمد باقر آقایی

سردبیر:

لیدا رسول اهری

نشانی:

تبریز، میدان شهدا، استانداری آذربایجان شرقی، اداره کل پدافند غیرعامل

تلفن: ۳۵۲۹۱۳۱۸-۰۴۱

دورنگار: ۳۵۲۹۱۳۵۹-۰۴۱

فهرست مطالب:

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

passivedefense@ostan-as.gov.ir

نیروی انتظامی با ناامن کننده فضای مجازی برخورد جدی کند

حضرت آیت‌الله خامنه‌ای فرمانده معظم کل قوا در دیدار فرماندهان و مدیران نیروی انتظامی، با تأکید بر لزوم استمرار حرکت این نیرو به سمت نیروی انتظامیِ مطلوب جمهوری اسلامی، نقش آن را در تحقق شعار سال یعنی «رونق تولید» و همچنین تأمین امنیت فضای مجازی مهم برشمردند.

رهبر انقلاب اسلامی به تأمین امنیت فضای مجازی اشاره کردند و گفتند: فضای مجازی امروز در زندگی مردم گسترش زیادی پیدا کرده است و در عین منافع و امکانات، خطرات بزرگی نیز دارد. ایشان ناامن شدن فضای مجازی را موجب ضرر و زیان به مردم دانستند و بر وظیفه نیروی انتظامی در تأمین امنیت فضای مجازی تأکید کردند.

حضرت آیت‌الله خامنه‌ای، «جلوگیری از خرید و فروش سلاح» را یکی دیگر از وظایف مهم نیروی انتظامی برشمردند و افزودند: در برخی کشورها مانند آمریکا، خرید و فروش سلاح به علت منافع مافیای کمپانی‌های اسلحه‌سازی آزاد است و برای مردم آن مشکل‌ساز است، اما در کشور ما که چنین مشکلی وجود ندارد و خرید و فروش سلاح ممنوع است، باید جلوی آن گرفته شود. رهبر انقلاب اسلامی با تأکید بر جلوگیری از خرید و فروش سلاح در فضای مجازی، گفتند: قاتل دیروز روحانیِ همدانی در صفحه اینستاگرام با چهار نوع اسلحه تصاویری از خود منتشر کرده است که مقابله با این‌گونه موارد وظیفه نیروی انتظامی است.

سرپرست اداره کل پدافند غیرعامل استانداری آذربایجان شرقی منصوب شد

استاندار آذربایجان شرقی در حکمی، محمدباقر آقایی را به سمت سرپرست اداره کل پدافند غیرعامل استانداری منصوب کرد. در حکم صادر شده از سوی دکتر پورمحمدی آمده است: نظر به تخصص و تجارب، به موجب این حکم جناب‌عالی را به سمت سرپرست اداره کل پدافند غیرعامل استانداری منصوب می‌کنم.

امید است با توکل به خداوند متعال و در راستای تحقق اهداف و آرمان های نظام مقدس جمهوری اسلامی و دولت تدبیر و امید، در حوزه پدافند غیرعامل منشاء خیر و تحول باشید.

محمدباقر آقایی دارای مدرک کارشناسی علوم سیاسی و پیش از این معاون مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی بوده است. مسئول اجرایی قرارگاه پدافند زیستی استان، مسئول رزمایش پدافند غیرعامل استان، رئیس گروه تهدیدات تخصصی پدافند غیرعامل و کارشناس دفتر سیاسی، انتخابات و تقسیمات کشوری استانداری از جمله عناوین کاری و به شمار می‌رود.

رئیس سازمان پدافند غیرعامل کشور: لزوم پیگیری نگاه بومی در فضای سایبری/ زیرساخت‌های فضای مجازی باید ملی باشد.

رئیس سازمان پدافند غیرعامل کشور با اشاره به گسترش فضای سایبری در همه حوزه‌ها و ابعاد زندگی بشر، گفت: نباید در استفاده از این فضا صرفاً از ارزش‌ها و اصول القایی صاحبان فناوری تبعیت کرد بلکه لازم است نگاه ایرانی و اسلامی را در فضای سایبر ملی کشور دنبال کنیم.

سردار جلالی در دومین کنفرانس ملی پدافند سایبری در دانشگاه آزاد اسلامی واحد مراغه، در خصوص فناوری‌های پیشرو از جمله IOT، گفت: این فناوری اجسام بی‌جان را هوشمند کرده و به عبارتی به آن‌ها جان می‌دهد؛ اما در کنار آن همه تهدیدهای فضای سایبری را به دنیای فیزیکی انتقال می‌دهد.

وی در خصوص محصولات خارجی مورد استفاده در زیرساخت‌ها و سازمان‌ها نیز گفت: بررسی‌های کارشناسان ما در آزمایشگاه روی یک مدل از دوربین‌های حفاظتی نشان داد که در میان‌افزار آن، قطعه کدی تعبیه شده بود که از تصاویر گرفته‌شده یک نسخه به آدرس IP خاص ارسال می‌کرد که این خود یک مشکل امنیتی ایجاد می‌کند؛ در واقع ابزاری که برای امنیت استفاده می‌شود به ابزار ضد امنیتی تبدیل می‌شود.

جلالی با اشاره به اینکه هدف از بازدارندگی، ایجاد ترس از قدرت و منصرف کردن دشمن از حمله است، افزود: بازدارندگی شامل سه مرحله پایداری و آسیب ناپذیری، قدرت پاسخ و پشیمان کنندگی دارد؛ بنابراین باید در حوزه پدافند، آسیب‌ناپذیر باشیم و با داشتن حداکثر تاب‌آوری در برابر تهدیدات، آسیب‌پذیری‌هایمان را به صفر نزدیک کنیم.

پدافند غیرعامل در حوزه‌های فناورانه، صد درصد علمی و دانش‌پایه و نیازمند کار دانشگاهی است؛ بنابراین دانشگاه‌های سراسر کشور از جمله دانشگاه آزاد اسلامی اگر بتوانند به سؤالات ما در حوزه‌های مختلف پدافند غیرعامل جواب بدهند به طور کامل از آن‌ها حمایت خواهیم کرد.

جلالی درباره نقش مهم شبکه‌های اجتماعی در جامعه گفت: شبکه‌های اجتماعی یکی از نیازهای واجب و ضرورت اجتماعی امروز بشر بوده و انسان

پیشرفته بدون آن‌ها زندگی‌اش مختل می‌شود؛ اما شبکه اجتماعی که پایگاهش دست دشمن باشد، در حقیقت سلاحی است علیه ما. زیرساخت این شبکه‌ها باید ملی و بومی بوده و مدیریتشان دست خودمان باشد که بتوانیم آن را اداره کنیم و درصورتی‌که به ما حمله شد بتوانیم پاسخ دهیم و این موضوعی کاملاً اساسی است.

رئیس سازمان پدافند غیرعامل کشور با اشاره به ضرورت توسعه زیرساخت‌های سایبری در کشور اظهار داشت: یکی از راه‌های مقابله با تهدیدات سایبری توسط دشمن و خنثی‌سازی آن‌ها، توسعه زیرساخت‌های سایبری بر اساس فناوری‌های بومی در کشور است. یکی از مهم‌ترین برنامه‌های سازمان پدافند غیرعامل در کشور بومی‌سازی زیرساخت‌های سایبری بوده و در این راستا اقدامات مهمی درحال انجام است.

وی دانشگاه‌ها را پایگاه اصلی راهبردشناسی در زمینهٔ حوزه‌های سایبری دانست و تصریح کرد: پدافند سایبری با فناوری‌های نو درآمیخته و این فناوری‌ها ترکیبی از تهدیدها و فرصت‌ها به وجود آورده‌اند. رویکرد ما باید استفاده از فرصت‌ها در برابر دفع تهدیدات باشد؛ بنابراین برای هر حوزه فناورانه، راهبرد لازم است که چگونه از تهدید آن اجتناب و از فرصت‌هایش استفاده کنیم. نقش دانشگاه‌ها در این زمینه با هدایت پایان‌نامه‌ها به سمت تهدید شناسی حوزه سایبری، قابل توجه و چشمگیر می‌تواند باشد.

رئیس سازمان پدافند غیرعامل کشور با نماینده ولی‌فقیه و امام جمعه شهر تبریز دیدار کردند

در این دیدار سردار جلالی حوزه‌های "دستور کار ۲۰۳۰ برای توسعه پایدار" موسوم به سند ۲۰۳۰ را مورد بررسی قرار داده و به این مسئله اشاره نمودند که بیشتر حوزه‌ها از ۱۴ حوزه موجود در سند، از منظر پدافند غیرعامل تهدید محسوب می‌شوند.

ایشان با بیان این‌که سازمان پدافند غیرعامل مستندات مربوطه تمامی موارد را بررسی نموده است، اعلام داشتند آماده تحلیل تهدیدات با مدارک کافی می‌باشند.

رئیس سازمان پدافند غیرعامل در ادامه اظهار داشتند: مهم‌ترین تهدید در سال جاری شبکه‌های اجتماعی هستند.

ایشان با اشاره به اهمیت فضای مجازی و بیان این‌که شبکه‌های اجتماعی زیرساخت حیاتی

محسوب می‌شوند، خواستار همکاری حوزه‌های علمیه و دانشگاه‌ها در جهت تهیه و تدوین مبانی شبکه‌های مجازی منطبق با فرهنگ ایران اسلامی شدند.

آیت‌الله آل هاشم نماینده ولی‌فقیه در استان آذربایجان شرقی و امام جمعه شهر تبریز نیز ضمن قدردانی از تلاش‌های سردار جلالی و سازمان در جهت اجرا پیاده نمودن اهداف پدافند غیرعامل در کشور، آمادگی حوزه‌های علمیه در خصوص همکاری در مطالعات مسائل شرعی فضای مجازی را اعلام نمودند و بررسی مباحث فقهی در حوزه پدافند غیرعامل و یاری رسانی در جهت آگاه‌سازی جوانانی که سواد رسانه‌ای کافی و آگاهی از تهدیدات فضای مجازی ندارند را از وظایف حوزه‌ها برشمردند.

دیدار رئیس سازمان پدافند غیرعامل کشور با استاندار آذربایجان شرقی

سردار جلالی رئیس سازمان پدافند غیرعامل کشور طی دیداری با دکتر پورمحمدی استاندار آذربایجان شرقی، به بحث و گفتگو در خصوص مسائل مختلف در حوزه پدافند غیرعامل پرداختند. سردار جلالی با اشاره به جاری شدن سیل و اتفاقات اخیر در چند استان، بر اهمیت نحوه مدیریت آب‌های سطحی شهر تأکید نمودند. ایشان همچنین پیگیری طرح جامع استان را مورد تأکید قرار داده و خواستار اجرای اقدامات لازم در این زمینه شدند.

رئیس سازمان پدافند غیرعامل کشور با بیان این‌که مشکل احتمالی پیش روی دیگر در سال جاری در زمینه برق خواهد بود، خواستار مجهز شدن تمام دستگاه‌های اجرایی استان به خصوص بیمارستان‌ها به ژنراتورهای برق اضطراری شدند.

ایشان با تقدیر از عملکرد مناسب اداره کل پدافند غیرعامل استان در سال گذشته در برگزاری رزمایش زیستی، اجرای مانور و رزمایش‌های بیشتر در سال جدید را ضروری دانستند.

سردار جلالی در انتها به مسئله حضور فعال نماینده سازمان پدافند غیرعامل در شورای عالی شهرسازی اشاره کرده و ایجاد رویه‌ای مناسب جهت جلوگیری از گسترش ساخت‌وساز در محدوده گسل‌ها را از اوامر مهم و لازم‌الاجرا برشمردند.

در این جلسه استاندار آذربایجان شرقی از اتمام ساخت ۳۵ کیلومتر از خط انتقال آب رودخانه ارس خبر داده و تکمیل این خط انتقال را گامی مهم در جهت عملی نمودن اهداف پدافند غیرعامل

دانستند. دکتر پورمحمدی بیان داشتند: انتقال آب ارس – زرینه‌رود دغدغه تأمین آب شرب سالم شهروندان را رفع خواهد کرد.

ایشان در ادامه نسبت به احداث شهرک جدید شهریار بر روی گسل و تهدیدات احتمالی ناشی از آن هشدار دادند. دکتر پورمحمدی در انتها به موضوع تهدیدات متصور بر مهران‌رود و تهدیدات نیروگاه هسته‌ای متسامور با قدمت ۵۰ سال، واقع در ارمنستان را که از معدود نیروگاه‌های هسته‌ای جهان بدون ساختار مهار اولیه می‌باشد، پرداختند.

سردار جلالی در جلسه مدیریت شهری کلانشهر تبریز؛

مطالعه طرح پدافند غیرعامل کلانشهر تبریز باید در اولویت برنامه‌های سال ۱۳۹۸ شهرداری باشد

جلسه مدیریت شهری کلانشهر تبریز با حضور سردار جلالی رئیس سازمان پدافند غیرعامل کشور و معاونین مربوطه، مدیرکل پدافند غیر عامل استان، مدیرکل مسکن و شهرسازی استان برگزار شد.

سردار جلالی رئیس سازمان پدافند غیر عامل کشور در این جلسه با اشاره به اینکه راه حل مشکلات استان بیشتر در تصمیم گیری داخل استان می‌باشد بر ضرورت تدوین طرح‌های مرتبط با مأموریت‌های پدافند غیرعامل تأکید کرده و خواستار تسریع در اجرای مطالعات پدافند غیر عامل کلانشهر تبریز با مشارکت سازمان شدند.

همچنین ایشان با اشاره به حضور نماینده سازمان پدافند غیرعامل در جلسات شورای عالی شهرسازی و معماری، یادآوری نمودند شهرداران محترم بایستی مشکلات و نیازمندی‌های شهرها را با ارائه مستندات لازم به معاونت امور شهری سازمان ارسال نمایند تا در تصویب طرح‌های مرتبط با مدیریت شهرها مانند طرح جامع شهرها مورد بررسی قرار گرفته و اعمال شود.

مهندس شهین باهر شهردار کلانشهر تبریز در جلسه بررسی تهدیدات، نظامات فنی و اجرایی و مطالعه پدافند غیرعامل کلانشهر تبریز با اشاره به خسارات سیل در استان‌های مختلف کشور بر ضرورت اجرای اقدامات پیشگیرانه قبل از وقوع حوادث، تأکید کردند. همچنین ایشان افزودند شهر تبریز به علت قرارگیری در مجاورت گسل تبریز و عبور مهران‌رود از وسط شهر در معرض تهدیدات طبیعی و غیر طبیعی می‌باشد.

دکتر شکور اکبر نژاد رئیس شورای اسلامی کلانشهر تبریز نیز در این جلسه با اشاره به لزوم شناسایی صحیح تهدیدات و نیازهای آینده کشور، بر مدیریت علمی و عقلانی، استفاده از تجربیات بشری و ایجاد روابط و همکاری‌های بین‌المللی به‌ویژه با کشورهای همسایه برای مواجهه با بحران‌ها تأکید کردند.

در پایان جلسه اعضای محترم شورای اسلامی کلانشهر تبریز با ارائه پیشنهادات و نظرات خود در خصوص تهدیدات شهر تبریز خواستار تشریح برنامه‌های سازمان برای موارد مطروحه شدند.

آموزش امنیت سایبری مدیران

مقدمه:

در دنیای فیزیکی رابطه‌ای مستقیم بین رشد علم و فناوری و تأمین امنیت وجود دارد هر چه علم و فناوری پیشرفته‌تر می‌شود امنیت بهتر تأمین می‌شود؛ اما در دنیای نوین به دلیل ابداع روش‌های دسترسی پنهان در بازار دیجیتال این مسئله بالعکس است. مدیران از حساس‌ترین لایه‌های درگیر در استفاده از ابزارهای دیجیتال، رایانه‌ای و ارتباطی هستند و منابع هر سازمان با گرایش مدیر مربوطه در این زمینه‌ها مصرف می‌گردد. مدیریت در هر سیستم اصلی‌ترین عامل به کارگیری منابع سازمانی است. راهبرد اصلی سازمان توسط مدیران طراحی و اجرا می‌گردد، هرگونه شکست در این لایه شکست اهداف سازمان را به ارمغان می‌آورد.

۱- پروتکل‌های امنیتی و اصول ایمن‌سازی توسط مدیران و سازمان

برای برقراری یک محیط ایمن عوامل جامعیت، محرمانگی، شناسایی و اعتبارسنجی، دسترس‌پذیری و انکارناپذیری باید برقرار باشد و این شرایط در صورتی می‌تواند امنیت را ایجاد نماید که در محیط بومی شکل گرفته باشد. برای رسیدن به یک طرح مناسب و کارا باید در سه مورد زیر تصمیم‌گیری شود:

ارائه سرویس در برابر امن سازی: سرویس‌هایی که در شبکه ارائه می‌شوند باید آنقدر ارزشمند و مهم باشند که صرف زمان و انرژی برای امن سازی آن‌ها بیهوده نباشد. یعنی این‌که با صرفه و صلاح سازگاری داشته باشند.

سادگی استفاده در برابر امنیت: هر چه سیستم امن‌تر باشد استفاده از آن مشکل‌تر می‌شود زیرا امنیت محدودیت ایجاد می‌کند؛ بنابراین باید بین قابلیت استفاده و میزان امنیت، تعادل ایجاد کرد.

هزینهٔ برقراری امنیت در برابر خطر از دست دادن: طراحی و پیاده‌سازی امنیت نیازمند صرف هزینه‌هایی در بخش‌های نیروی انسانی، نرم‌افزار و سخت‌افزار خواهد بود. در صورتی‌که احتمال از دست دادن یا دچار مشکل شدن یک منبع بسیار پایین باشد و آن منبع از درجهٔ اهمیت بالایی نیز برخوردار نباشد صرف هزینه زیاد برای امن سازی آن بهینه نخواهد بود.

۱-۱- فرآیند امن سازی

امنیت یک فرآیند است که باید به چرخهٔ حیات سازمان تزریق شود. امنیت نه تنها بر روی اطلاعات یا تجهیزات بلکه بر تمام ارکان سازمان باید حاکم باشد. موضوعات موجود در مقولهٔ مدیریت امنِ فناوری اطلاعات و ارتباطات نوعاً شامل موارد زیر می‌باشد:

سیاست امنیتی، تحلیل مخاطرات، انتخاب حفاظ، طرح دقیق امنیتی سیستمی، پیاده‌سازی حفاظها در هر سیستم، طرح پشتیبانی و تداوم فعالیت، ارزیابی و نظارت، تحمل‌پذیری خطا، مدیریت تغییرات، طرح مواجهه با حوادث غیرمترقبه، اطلاع‌رسانی و آموزش امنیتی.

۱-۲- برنامه‌ریزی امنیتی

برای پیاده‌سازی امنیت در یک سازمان، دو نوع برنامه‌ریزی نیاز است. برنامه‌ریزی کلان‌تر برای خط‌مشی‌ها و برنامه‌ریزی جزئی‌تر برای سیاست‌های امنیتی.

۱-۲-۱- برنامه‌ریزی استراتژیک امنیت

هدف از برنامه‌ریزی استراتژیک برای امنیت فراهم آوردن اطلاعات لازم جهت مدیریت و تصمیم‌گیری در مورد سرمایه‌گذاری‌های امنیتی است. استراتژی‌های امنیتی رسیدن به اهداف حرفه را با شناسایی و آدرس‌دهی نیازمندی‌های امنیتی در عملکرد آن سازمان، فراهم آوردن زیرساخت‌ها، افراد و فرآیندهایی که آن نیازمندی‌ها را فراهم می‌کند ممکن می‌سازد. استراتژی‌ها با استفاده از اهداف حرفه و اهداف امنیتی و میزان قابلیت فعلی برای تأمین این اهداف طراحی می‌شوند و باید به طور دوره‌ای بازبینی و اصلاح شوند.

۱-۲-۲- برنامه‌ریزی سیاست‌های امنیتی

پس از تعیین خط‌مشی‌های یک سازمان، سیاست‌های آن برنامه‌ریزی‌شده، استانداردها و سپس روال‌ها و راهنماهای امنیتی مربوطه برای پیاده‌سازی آن سیاست‌ها در یک محیط واقعی توسعه داده شده و نهایتاً در اختیار کاربران و مدیران قرار می‌گیرند.

سیاست‌های امنیتی که خوب تدوین شده‌اند دارای ویژگی‌های زیر هستند:

- توسط مدیران سیستم قابل پیاده‌سازی و اجرا هستند.
- رویه‌های تدوین شده ساده، قابل اجرا و مورد پذیرش هستند.
- توسط ابزارهای تأمین‌کننده امنیت موجود، قابل اعمال هستند.
- به طور مشخص مسئولیت‌ها و وظایف کاربران، کادر فنی و مدیران را تعیین می‌کنند.

سیاست امنیتی باید در حوزه‌های بسیاری از سازمان مانند سیاست دسترسی، سیاست تشخیص هویت، سیاست حسابداری، سیاست گزارش تخلفات، سیاست حریم خصوصی افراد، سیاست نگهداری شبکه، سیاست دسترس‌پذیری، سیاست‌های آگاهی‌رسانی تعیین شود.

پس از تعیین سیاست‌ها، رویه‌های امنیتی باید برای کاربران نهایی، مدیران شبکه و مدیران امنیتی و سایر افراد درگیر نوشته شود. همچنین رویه‌های امنیتی باید چگونگی برخورد با حوادث مختلفی که رخ می‌دهند را مشخص کنند. این رویه‌ها باید به کاربران و مدیران شبکه آموزش داده شوند. پس از آن دیواره‌های آتش، ضدویروس‌ها، سیستم‌های تشخیص تهاجم بومی شده و ... برای امن سازی سازمان به کار گرفته می‌شوند و رویه‌های امنیتی پیاده‌سازی می‌شوند. سیاست‌های امنیتی، تکنولوژی و متدولوژی استفاده از سیستم‌های امن، گام‌های جزئی برای دنبال کردن وظایف امنیتی مربوطه را مشخص می‌کند. در این راستا پس از شناخت وضعیت معماری موجود و تهیه معماری امنیتی مطلوب باید برنامه‌ای برای حرکت از سمت معماری موجود به سمت معماری مطلوب طراحی، اجرا و کنترل شود. سیاست‌های امنیتی باید در دسته‌های مدیریت امنیت، امنیت اطلاعات، امنیت پرسنل، امنیت شبکه و سیستم شامل سیاست‌های توسعه نرم‌افزار، سیاست‌های شبکه و مدیریت سیستم و برنامه‌ریزی تداوم عملکرد سازمان، ارائه شوند.

۱-۲-۳- استراتژی‌های طراحی سیاست‌ها

در سازمان باید تشکیلاتی برای تأمین امنیت شبکه از نقطه نظر ساختار، شرح وظایف و جایگاه آن در چارت سازمانی و برنامه‌های تأمین نیروی انسانی طراحی شود. این تشکیلات در سه سطح سیاست‌گذاری، مدیریت اجرایی و سطح فنی به طراحی، نظارت و اجرای طرح‌ها و برنامه‌های امنیتی می‌پردازند.

برنامه‌ریزی‌ها باید به دو صورت کوتاه مدت و بلندمدت یا (میان مدت) با توجه به اهداف امنیت سازمان طراحی شوند.

برای این که سیاست‌های امنیتی به خوبی پیاده‌سازی شوند تمام افرادی که وظیفهٔ نگهداری و محافظت

سیستم را به عهده دارند باید در پیاده‌سازی آن‌ها همکاری کنند. برای برنامه‌ریزی و دادن طرح‌ها و رویه‌های امنیتی ابتدا باید سرمایه‌ها و ریسک‌ها را شناسایی و درجه‌بندی نمود. پس از طراحی برنامه امنیت سازمان، طراحی برنامه آگاهی‌رسانی، تربیت نیروی انسانی و آموزش امنیت در سازمان و همچنین طرح پشتیبانی حوادث امنیتی سازمان را نیز باید طراحی نمود. در هر سازمان پس از تهیه سیاست‌ها و استانداردها و روال‌های امنیتی، معماری موجود سازمان بررسی شده، رخنه‌ها و خطرات آن مشخص می‌شوند. سپس با توجه به اهداف و سیاست‌ها، نیازمندی‌های امنیتی شناسایی و اولویت‌بندی می‌گردند. پس از انتخاب هدف‌ها و سیاست‌های امنیتی باید به تهیه روال‌ها و دستورالعمل‌های اجرایی جهت عملیاتی کردن آن سیاست‌ها پرداخت.

۱-۳- سیاست‌های مدیریتی:

سیاست‌های مدیریتی در سه بخش شامل مدیریت نظارت بر سیستم، کنترل‌های امنیتی و مدیریت تهدیدهای حقوقی و حیثیت بررسی می‌شود. در بخش اول مدیران سیستم مسئولیت توسعه استراتژی‌های تجاری را بر عهده دارند. تصمیم اولیه از دید مدیریتی این است که آیا نیازی به ارائه سرویس‌ها و افزودن این سرویس‌ها به سرویس‌های سنتی وجود دارد یا خیر؟ به طور خاص سیستم نظارت بایستی از ترکیب واضح و بدون ابهام طرح‌های ارائه شده برای سرویس‌های جدید با اهداف موجود در سیاست‌های مورد نظر اطمینان حاصل کند. همچنین تحلیل ریسک بر روی فعالیت‌ها و سرویس‌های جدید پیشنهادی، نظارت بر پردازش‌های انجام شده بر روی ریسک‌های تعیین شده، ارزیابی نتایج فعالیت سیستم الکترونیکی و غیره از مواردی است که باید اجرا شوند. به طور مشخص توجه به اصول زیر ضروری است:

اصل اول نظارت کامل بر فعالیت‌ها و سیاست‌ها: مدیران سیستم باید نظارت مدیریتی لازم مرتبط با فعالیت‌ها، شامل سیاست‌ها و کنترل‌های مورد نیاز برای مدیریت این ریسک‌ها را به انجام رسانند.

- توجه به عوامل ریسک متفاوتی که با بومی‌سازی، صحت، امنیت، قابلیت دسترسی و محصولات الکترونیکی ارتباط پیدا می‌کنند.

- اطمینان از این که سعی و تلاش لازم برای تحلیل تهدیدات، قبل از هر نوع فعالیت مهم صورت می‌گیرد.

اصل دوم فرآیند کنترل امنیت: مدیران بایستی مفاهیم کلیدی مربوط به فرآیند کنترل امنیتی را بکار گیرند که این عناصر کلیدی شامل موارد زیر است:

در نظر گرفتن فرد یا افرادی از کارمندان برای نظارت بر به کارگیری صحیح سیاست‌های امنیتی؛ استفاده از کنترل‌های فیزیکی کافی برای جلوگیری از دسترسی فیزیکی غیرمجاز به محیط‌های رایانه‌ای؛ اعمال کنترل‌های کافی و اجرای فرآیندهای نظارتی برای جلوگیری از دسترسی‌های داخلی و خارجی غیرمجاز به کاربردها و پایگاه‌های داده. انجام آزمایش‌ها و بازبینی منظم کنترل‌ها و اقدامات امنیتی شامل نصب نسخه‌های جدیدتر نرم‌افزارها و یا بسته‌های تکمیلی آن‌ها.

اصل سوم فرآیند جامع نظارت: مدیران بایستی یک فرآیند جامع و در حال پیشرفت برای نظارت و مدیریت ارتباطات موجود بین سازمان و عوامل خارجی و نیز شرکت‌های بخش سوم وابسته تدوین نمایند.

کنترل‌های امنیتی:

مدیران مسئولیت انجام فرآیند کنترل‌های امنیتی را بر عهده دارند.

اصل چهارم احراز هویت: سازمان بایستی اقدامات مناسب برای احراز هویت، شناسایی و بررسی مجوزهای مشتریان را انجام دهد.

اصل پنجم عدم امکان‌پذیری انکار هویت: سازمان‌ها بایستی روش‌های احراز هویت تراکنش که از عدم انکار پشتیبانی می کند را مورد استفاده قرار دهند.

اصل ششم تفکیک صحیح وظایف: ساختارها بایستی از انجام اقدامات مناسب در رابطه با تفکیک صحیح وظایف در سیستم‌های پایگاه‌های داده و کاربردها اطمینان حاصل نمایند.

اصل هفتم اطمینان از کنترل مجوزهای دسترسی: سیستم‌ها بایستی از کنترل مجوزهای دسترسی و انجام دسترسی‌های مجاز به سیستم‌های الکترونیکی، پایگاه های داده و کاربردها اطمینان کامل حاصل نمایند.

اصل هشتم اطمینان از صحت تراکنش‌ها: سازمان‌ها بایستی از انجام اقدامات مناسب برای حفظ صحت داده‌ها، رکوردها و اطلاعات مربوط به تراکنش‌های اطلاعاتی، اطمینان کافی حاصل نمایند.

اصل نهم ره‌گیری تراکنش‌ها: در سیستم‌های اطلاعاتی، بایستی از انجام عملیات ردگیری تمامی تراکنش‌های انجام شده اطمینان حاصل شود.

اصل دهم حفظ محرمانگی اطلاعات: میزان محرمانگی اطلاعات بر حسب میزان حساسیت آن‌ها تعیین می‌شود. هر نوع سوء استفاده و یا افشای غیرمجاز اطلاعات، باعث می‌شود که ریسک حقوقی و ریسک حیثیت به وجود آید.

مدیریت ریسک‌های حقوقی و حیثیت: سازمان‌ها مسئولیت دارند تا به نحو مناسب از افشای اطلاعات کاربران جلوگیری کرده و اقدامات لازم برای حفاظت از داده‌های آنان را انجام دهند. اصول زیر به بررسی سیاست‌ها و ملزومات لازم برای ریسک‌های حقوقی و حیثیت می‌پردازد.

اصل یازدهم بومی‌سازی امنیت: با عناصر وارداتی امکان تأمین امنیت برای سازمان وجود نخواهد داشت.

اصل دوازدهم اقدامات امنیتی سازمان: اقدامات امنیتی باید از سوی سازمان‌ها برای به وجود آوردن محرمانگی لازم برای کاربران انجام شود.

اصل سیزدهم رویدادهای غیرمنتظره: سیستم باید طرح‌های مدیریتی لازم برای کاهش مسائل حاصل از رویدادهای غیرمنتظره شامل حملات داخلی و خارجی را فراهم کند.

اصل چهاردهم روحیه سلطه گری نظام سلطه: نظام سلطه همیشه به دنبال اشرافیت بر اطلاعات و ارتباطات دیگران می‌باشد و در این راه سرمایه‌گذاری‌های فراوانی انجام می‌دهد. یکی از این سرمایه‌گذاری‌ها در طرح اشلون می‌باشد که در آن کشورهای سلطه‌گر سه مثلث شوم اشلون و سیستم‌های هوشمند و نظام‌های سلطه‌گر را به هم پیوند داده و با طراحی سیستم‌های مورد نیاز کشورهای در حال توسعه و قرار دادن سیستم‌های مدیریت راهبردی پنهان بر روی آن و فروش به دیگر کشورها، در زمان‌های حساس و مورد نیاز کنترل سیستم‌های اطلاعاتی و ارتباطی آن کشورها را به دست می‌گیرند.

ادامه دارد ....

منبع: خلاصه‌ای از کتاب

۱- آموزش امنیت سایبری مدیران – ناصر نامخواه – بهار ۱۳۹۰

تهیه و تنظیم: لیدا رسول اهری- کارشناس آموزش و پژوهش اداره پدافند غیر عامل

مطالعه امکان سنجی بکارگیری پدافند غیرعامل در بخش حمل و نقل زمینی

مقدمه:

کاملاً واضح است که دفاع در برابر تهدیدات ناشی از جنگ‌های فوق مدرن در قرن حاضر، نیازمند ساز و کارهای نوین عصر خود است. بدون این ساز و کارها نمی‌توان چارچوب مطمئنی برای تحکیم مبانی دفاعی کشور متصور بود. دفاع همواره از دو منظر عامل و غیرعامل، مورد توجه کارشناسان و طراحان جنگ بوده است. دفاع همیشه به معنی قرار گرفتن در موضع دفاعی در یک رویایی مستقیم با دشمن نیست (هرچند ممکن است چنین شرایطی هم اجتناب ناپذیر باشد)، بلکه می‌توان به راحتی با بهره‌گیری از شیوه‌های نوین علمی در چارچوب اقدامات پدافند غیرعامل، مانع شناسایی، ردیابی و یا هدف‌گیری توسط دشمن شد. این اقدام اساساً بسیار منطقی، کم‌هزینه و پایدارتر خواهد بود. حمل و نقل یکی از اجزای مهم اقتصاد ملی محسوب می‌گردد و به دلیل داشتن نقش زیربنایی، تأثیر فراوانی بر فرآیند رشد اقتصادی کشور دارد. این بخش در برگیرنده فعالیت‌هایی است که به شکلی گسترده در تمامی زمینه‌های تولید، توزیع و مصرف کالا و خدمات، جریان داشته و در مجموعه فعالیت‌های اقتصادی نقش غیرقابل انکاری بر عهده دارند. با عنایت به اهمیت فوق‌العاده این صنعت، لزوم سرمایه‌گذاری برای توسعه و نگهداری زیربناها، ناوگان و تجهیزات موجود از طریق ارتقای کیفیت فنی و دانش مدیریت سیستم‌های حمل و نقل، ضروری است. بطور کلی از این صنعت می‌توان به عنوان یک سلاح راهبردی برای توسعه روابط سیاسی استفاده نمود و درهای اقتصاد و توسعه پایدار و ایجاد انگیزه برای سرمایه‌گذاری خارجی و دادن تضمین پایدار در مناسبات اقتصادی و توسعه ملی کشور را گشود. از این رو نگهداری و بقای سیستم جهت ارائه خدمت در زمان‌های اضطراری

مانند جنگ و وقوع بحران‌های طبیعی بسیار با اهمیت است با توجه به احتمال وقوع حمله، سیستم حمل و نقل با توجه به گستره وسیع آن در معرض خسارات و آسیب‌های زیادی قرار می‌گیرد.

فلسفه وجودی پدافند غیر عامل در حوزه حمل و نقل:

به دنبال معرفی فلسفه وجودی پدافند غیر عامل در حوزه حمل و نقل نیاز به بیان مأموریت که شامل تهیه و اجرای مجموعه‌ای از اصول و مقدمات و تدابیری است که بدون استفاده از سلاح، موجب تداوم و استمرار فعالیت‌های حمل و نقلی کشور در شرایط تهدید می‌باشد. این مهم از طریق کاهش آسیب‌پذیری زیرساخت‌های حیاتی، حساس و مهم حمل و نقل با در نظر گرفتن و برآورد تهدیدات و همچنین سیاست‌گذاری و هدایت راهبردی و تدوین و تصویب ضوابط و دستورالعمل‌های پدافند غیرعامل و نظارت بر حسن اجرای آن امکان‌پذیر می‌گردد. جهت کاهش آسیب‌پذیری زیرساخت‌ها بخصوص در حوزه حمل و نقل باید موارد زیر رعایت گردد:

۱-حداکثر بهره‌برداری در حوزه حمل و نقل به صورت ایمن.

۲- پیش‌بینی تهدیدات، تأمین دفاع غیرعامل حوزه حمل و نقل و کاهش آسیب‌پذیری زیرساخت‌های حیاتی، حساس و مهم در مقابل تهدیدات.

۳- کاهش آسیب‌پذیری زیرساخت‌های حساس و حیاتی در حوزه حمل و نقل به منظور استمرار فعالیت مورد نیاز در شرایط جنگ.

۴- تضمین چرخه تأمین و لجستیک سیستم‌های حیاتی و حساس حمل و نقل کشور

اصول و سیاست‌های حاکم بر پدافند غیرعامل:

از اصول و سیاست‌های حاکم بر پدافند غیرعامل در حوزه حمل و نقل می‌توان به استفاده حداکثر از زیرساخت‌های حمل و نقل، حداکثر استفاده از تکنولوژی های مناسب بومی، کنترل نظارت و ارزیابی مستمر اقدامات پدافند غیرعامل در حوزه حمل و نقل کشور، نهادینه‌سازی فعالیت‌های پدافند غیرعامل در حوزه حمل و نقل کشور، تأکید بر اولویت‌بندی در تخصیص منابع به پروژه‌های پدافند غیرعامل با توجه به محدودیت منابع و استفاده از توان نیروهای مسلح کشور در شرایط تهدید در حوزه حمل و نقل اشاره کرد.

دفاع غیرعامل در حوزه حمل‌ونقل:

جهت تدوین سند راهبردی دفاع غیرعامل در حوزه حمل‌ونقل، نیاز به جهت‌گیری برای اجرای الزامات پدافند غیرعامل در این حوزه است که شامل چشم‌انداز، مأموریت، اصول و سیاست‌های کلی، اهداف و راهبردها است. برای داشتن چشم‌انداز پدافند غیرعامل در حوزه حمل و نقل زمینی (ریلی و جاده‌ای)، باید تصویری از سیستم، پس از موفقیت در پیاده‌سازی استراتژی‌ها و برنامه‌های اجرایی در پایان افق برنامه‌ریزی را در نظر بگیریم. جهت دست‌یابی به اهداف پدافند غیرعامل در حوزه حمل و نقل، موارد زیر بایستی تأمین گردد:

۱- برخورداری از سیستم یکپارچه و هماهنگ و کارآمد پدافند غیر عامل در حوزه حمل و نقل بین شهری کشور.

۲- توانمندی در تأمین حداکثر ایمنی و پایداری و به حداقل رساندن آسیب‌پذیری زیرساخت‌های حمل و نقل در برابر تهدیدات دشمن.

۳- توانمندی در تولید دانش فنی و برخوردار از پشتوانه تحقیقاتی و پژوهشی مورد نیاز در زمینه پدافند غیرعامل در حوزه حمل و نقل.

۴ - دارا بودن باور عمومی در مسئولین و کارکنان حمل و نقل نسبت به رعایت اصول پدافند غیرعامل.

۵- بکارگیری حداکثری ظرفیت تحقیقاتی، پشتیبانی و عملیاتی پدافند غیرعامل کشور در حوزه حمل و نقل.

اهداف استراتژیک پدافند غیرعامل در حوزه حمل و نقل:

مهم‌ترین و اساسی‌ترین هدف استراتژیک پدافند غیرعامل در حوزه حمل و نقل، کاهش آسیب‌پذیری و افزایش ماندگاری زیرساخت‌های حمل و نقل است که برای دستیابی به این هدف می‌توان هدف اساسی را به اهداف کوچک‌تر تعریف و در اهداف اصلی و فرعی هدف اساسی مد نظر قرار گیرد. لذا در پیاده‌سازی راهبردهای پدافند غیرعامل در حمل و نقل انتظار می‌رود اهداف اصلی و فرعی حاصل شود تا با حصول این اهداف، هدف اساسی تأمین گردد. لذا جهت دست‌یابی به اهداف استراتژیک پدافند غیرعامل بایستی به موارد زیر توجه گردد:

-افزایش قابلیت بقا، استمرار عملیات و فعالیت حمل و نقل کشور در شرایط تهدید و جنگ

- فرهنگ‌سازی در حوزه دفاع غیرعامل در حمل و نقل کشور

- اجرای کامل دستورالعمل‌ها و آئین‌نامه‌های دفاع غیرعامل مورد نیاز در طراحی و ساخت سیستم‌های حمل و نقل

- دستیابی به دانش حفاظت از زیرساخت‌های اساسی حمل و نقل کشور

انتظار می‌رود با بکارگیری برنامه‌های اجرایی و راهکارهای عملی، بتوانیم به نهادینه‌سازی پدافند غیرعامل در ساختار حمل و نقل زمینی و اهداف خرد و کلان مورد نظر دست یافت.

منابع:

۱- پدافند غیرعامل و مدیریت بحران- محمدصادق فتوحی- محل انتشار (اولین کنفرانس پدافند غیرعامل و سازه‌های مقاوم) - ۱۳۸۹

۲- مقدمه‌ای بر اصول و مبانی اساسی پدافند غیرعامل- ترجمه جمشید عباسپور- ناشر (قرارگاه خاتم‌الانبیا) - ۱۳۸۴

تهیه و تنظیم : احد ماهری- رئیس گروه طرح و اجرا اداره کل پدافند غیر عامل، رضا خوش روا- کارشناس امریه پدافند غیر عامل

تروریسم شیمیایی

سابقه تاریخی استفاده از مواد شیمیایی برای از بین بردن انسان‌ها به زمانی برمی‌گردد که افراد با آغشته کردن آب و غذای پادشاهان به انواع سموم آن‌ها را از پای در می‌آوردند که این کار تأثیری بر سلامت اجتماع نداشت، اما امروزه فناوری، امکان تولید موادی را به ما داده است که بکارگیری آن‌ها می‌تواند آثار مخربی بر روی اجتماع داشته باشد.

هدف آدمی از ساخت سلاح‌های کشتارجمعی در ابتدا تخریب و به هم ریختگی مقر دشمن بود اما اکنون به سلاح‌هایی روی می‌آورد که بدون ایجاد تخریب بتواند باعث مرگ و میر یا ناتوانی افراد شود. جنگ جهانی اول سرآغازی برای استفاده از سلاح‌های شیمیایی بود و استفاده از این جنگ‌افزارها در جنگ جهانی دوم به صورت لگاریتمی افزایش یافت و مواد بسیار کشنده‌ای تولید شد. تحقیقات نشان داده است که هم اکنون پنجاه هزار گونه از مواد شیمیایی موسوم به ترکیبات ارگانو فسفره وجود دارد که یک شیمیدان به راحتی می‌تواند آن‌ها را تولید کند؛ چرا که فرمول شیمیایی و مراحل ساخت آن در متون علمی و اینترنت وجود دارد. در سال‌های اخیر گروه‌های سیاسی برای نشان دادن توان خود استفاده از این گونه مواد را سرلوحه کار قرار داده‌اند که متأسفانه در دو دهه اخیر با توجه به راه‌های بسیار ساده پخش این مواد در بین مردم در مناطق شلوغ، استفاده ازاین‌گونه سلاح‌ها وقایع دلخراشی را سبب شده است. مواد و عوامل شیمیایی از سه منظر زنگ هشدار را برای مسئولان امنیتی و اجرایی جامعه و به ویژه مسئولین اورژانس و نیروی انتظامی و ... به عنوان یکی از سازمان‌های مسئول تأمین امنیت عمومی و اجتماعی و سلامتی به صدا در می‌آورد:

۱- استفاده گروه‌های تروریستی از عوامل شیمیایی برای انجام خرابکاری و ایجاد ناامنی (مانند فاجعه گاز سارین در ژاپن).

۲- پخش و توزیع ناخواسته مواد شیمیایی به علت حوادث غیرمترقبه و ایجاد ضایعات و تلفات برای مردم (مانند فاجعه کارخانه بوپال هند و فاجعه قطار نیشابور).

۳- استفاده از مواد شیمیایی توسط پلیس برای کنترل اغتشاشات (مانند گروگان‌گیری چچن).

با توجه به این موارد، نیروی انتظامی و اورژانس به عنوان یک نیروی حاضر در کلیه نواحی و مناطق کشور برای تأمین امنیت و سلامت، در راستای انجام این وظیفه هم با تسلط بر روش‌های تشخیص حملات تروریستی شیمیایی و شناسایی عوامل شیمیایی، باید در سطوح مختلف تجهیز شوند و آموزش‌های لازم را ببینند و با برنامه‌ریزی لازم، ضمن هماهنگی با مبادی ذیربط در مراحل مختلف قبل، حین یا بعد از حمله آن‌چنان آماده وارد عمل شوند که ضمن امیدبخشی به شهروندان و ایجاد آرامش خاطر بین آن‌ها، اقدامی سریع و مؤثر در مقابله با این حملات به عمل آورند.

روش‌های انتشار عوامل شیمیایی:

۱- مایعات: برای انتشار مایعات سیستم‌هایی طراحی می‌شوند که بتوانند حداکثر پوشش هدف را برای دستیابی به چگالی آلودگی مورد نظر فراهم کنند، برای دستیابی به بهترین پوشش، جنگ افزار باید روی هدف عمل کند.

سه روش مختلف برای عمل جنگ افزار عبارتند از:

الف) گلوله انفجاری ب) تانک افشاننده ج) شکست آیرودینامیک مقادیر حجیم

۲) گازها: گازها دو دسته هستند. دسته اول مایعات با فشار بخار بالا که در دمای معمولی گاز می‌باشند. این عوامل وقتی در محیط قرار می‌گیرند خود به خود تبخیر می‌شوند.

دسته دوم مایعات با فشار بخار متوسط هستند که وقتی منتشر می‌شوند، عمدتاً بخار می‌شوند. این مواد در شرایط دمای معمولی هوا، مایع باقی می‌مانند. نقطه جوش این ترکیبات بسیار بالاتر از دمای جوش آب است. این گازها روش‌های انفجاری شدید از قبیل سیستم‌های توپخانه، سیستم‌های چندتایی پرتاب راکت، بمب‌ها و موشک‌های دارای کلاهک‌های متعدد منتشر می‌شوند.

۳) آیروسل ها: آیروسل ها به عنوان ذرات کوچک مایع یا جامد معلق در یک محیط گازی تعریف می‌شوند. رفتار آیروسل نزدیک به رفتار گاز یا بخار است. اندازه آیروسل ها به‌گونه‌ای است که با جنگ‌افزارهای انتشار مایع قابل انتشار نیستند.

استفاده از عوامل شیمیایی برای تهدید عمومی:

استفاده ابزاری از این عوامل توسط بعضی از گروه‌های سیاسی در برخی نقاط جهان دیده شده است که با مراجعه به تاریخچه استفاده از این مواد می‌توان نتایج دردناک آن را نیز مطالعه کرد. موارد زیر چند نمونه معروف از این کاربردهاست.

نمونه‌هایی که ما را بر آن می‌دارد که همیشه خطرات ناشی از این نوع تروریسم شوم را جدی بگیریم و همیشه در فکر چاره‌ای برای مقابله با آن باشیم.

اهمیت آموزش نیروهای انتظامی و اورژانسی و آتش‌نشانی و ... در زمینه به کارگیری مواد شیمیایی.

در کنترل برخی از اجتماعات غیرقانونی و یا اغتشاشات پلیس مجبور به استفاده از مواد شیمیایی است، این مواد شیمیایی با ایجاد ضعف و ناتوانی در عملکرد تجمع کنندگان، به نیروهای انتظامی اجازه می‌دهد تا بر محیط غلبه پیدا کند و برنامه‌های کنترل و ایجاد امنیت خود را پیاده سازد. به همین منظور باید نیروی انتظامی و اورژانس، آموزش‌های لازم در بکارگیری نوع مواد شیمیایی را دیده باشد تا ناخواسته به جای کنترل تجمعات خود بحران سازی نکند، نمونه زیر نمونه‌ای از اشتباه پلیس است که به دلیل عدم اطلاع کافی از یک ماده شیمیایی به‌جای آنکه تأمین امنیت کند، برعکس امنیت عمومی را تهدید کرده است.

برای مقابله با گروگان‌گیری ۲۳ اکتبر ۲۰۰۲ در تئاتر شهر مسکو که توسط گروگان گیرهای چچنی انجام شده بود، از اسپری کردن ماده مخدری به نام فنتانیل از طریق تهویه سالن تئاتر بهره‌برداری شد، استفاده از این دارو که نقض پیمان ۱۹۹۷ است، باعث مرگ و میر ۱۱۵ نفر از ۷۵۰ نفر گروگان شد، هر چند دانشمندان روسی به استفاده از ماده دیگری اشاره نکردند اما پزشکان آلمانی با معاینه دو نفر از گروگان‌های آلمانی، وجود مادهٔ هالوتان را نیز تأیید کردند، هالوتان معمولاً در پزشکی به همراه فنتانیل استفاده می‌شود.

پس از این اشتباه، پزشکان روسی دریافتند که با استفاده از نالوکسان که یک آنتاگونیست مواد مخدر است می‌توان اثر مسمومیت را از بین برد.

از دهه ۱۹۷۰ پنتاگون فنتانیل و خانوادهٔ آن را به عنوان مواد احتمالی کنترل اغتشاشات معرفی کرد و اعلام شد که به نظر ایالات‌متحده، تسلیحات شیمیایی حداقل تا ۱۹۹۴ توسط مخدرها از رده خارج خواهند شد.

چه باید کرد:

۱) توجیه اهمیت موضوع در شوراهای تأمین و تشکیل کارگروه‌های لازم.

۲) آموزش گروه‌های پلیس برای انجام اقدامات تأمینی مناسب.

۳) ارائه آموزش‌های لازم به مردم از طرق مختلف.
۴) تجهیز آزمایشگاه‌های شیمی جنایی در شهرستان‌ها و مناطق برای بررسی اولیه عوامل شیمیایی.
۵) تجهیز آزمایشگاه‌های شیمی جنایی در مراکز استان‌ها و نیز آزمایشگاه مرکزی برای بررسی عوامل شیمیایی.
۶) شناسایی امکانات موجود در مراکز تحقیقاتی و پژوهشی و نیز دانشگاه‌ها و انعقاد تفاهم‌نامه‌های همکاری برای استفاده از تجهیزات موجود برای شناسایی سریع عوامل شیمیایی.

نتیجه‌گیری

در پایان ضمن تأکید بر این موضوع که حمله شیمیایی تروریست‌ها به اماکن مسکونی به عنوان یک موضوع بسیار جدی، به آسانی می‌تواند امنیت و آرامش عمومی را بر هم بزند، یادآور می‌شود که: ساخت بسیاری از عوامل شیمیایی در بعد صنعتی ساده است، مانند روش ساخت گاز سارین در مقیاس صنعتی.
برنامه‌ریزی کافی و تعلیم منظم، کلید آمادگی برای حملات تروریستی است. مأموران بهداشت باید از علائم و گزارش‌های ناشی از شیوع بیماری‌های حاصل از مواد شیمیایی آگاه باشند. مشاهدات بالینی و اپیدمیولوژیک، که در زیر می‌آیند ممکن است نشان از حملات تروریستی باشند:
الف) افزایش غیر معمول تعداد افراد بیمار خصوصاً با علائم بیماری‌های تنفسی، عصبی، پوستی یا گوارشی.
ب) تجمیع علائم و یا شیوع بیماری‌های وابسته به سنین خاص، (مثل عوارض سلاح‌های شیمیایی در کودکان)
ج) تأثیر هم‌زمان بر انسان، جانوران و گیاهان.
۶) علائم غیرمعمول بیماری‌ها و جمع شدن این عوامل باید سریعاً گزارش شود. کارکنان اورژانس باید به مراکز کنترل پزشکی و به تیم‌های اعزامی اطلاع‌رسانی کنند. وزارت بهداشت و مرکز کنترل سموم نیز باید به این موضوع توجه داشته باشند. بنابراین برای حفظ امنیت عمومی لازم است پلیس با هماهنگی سایر دستگاه‌های برقرارکننده امنیت اقدامات تأمینی لازم را به عمل آورد.

منابع:

۱- ساخت اجتماعی امنیت (درآمدی بر جامعه‌شناسی امنیت)، اصغر افتخاری، فصلنامه دانش انتظامی، سال سوم

تهیه و تنظیم: شمسعلی محمودیان – کارشناس پدافند غیرعامل

کشف حفره امنیتی خطرناک در لپ‌تاپ‌های Dell

این آسیب‌پذیری در برنامه SupportAssist شناسایی شده که برای اسکن سیستم، عیب‌یابی، رفع مشکل و دانلود و نصب خودکار درایورها کاربرد دارد. حفره امنیتی توسط یک محقق امنیتی ۱۷ ساله به نام «بیل دمیرکاپی» پیدا شده و به هکرها اجازه می‌دهد تحت شرایط خاصی از طریق اجرای کد از راه دور به سیستم قربانی دسترسی پیدا کنند.

در این نوع حمله هکر با اتصال به شبکه محلی کاربر وی را به یک صفحه مخرب هدایت کرده و از طریق اجرای کدهای جاوا اسکریپت عملکرد برنامه SupportAssist را تغییر می‌دهد. این برنامه به خاطر سطح دسترسی ادمین بخش عمده‌ای از تنظیمات را در اختیار هکر قرار خواهد داد.

مهاجم می‌تواند با تغییر تنظیمات SupportAssist نرم‌افزار را وادار سازد به‌جای دانلود فایل از سرورهای اصلی، فایل‌های مخرب را از محل مورد نظر هکر دانلود کرده و روی سیستم هدف نصب کند. برای در امان ماندن از این خطر مطمئن شوید که برنامه SupportAssist نسخه ۳,۲,۰,۹۰ یا بالاتر باشد.

روش جدید انتشار بدافزار TrickBot

آزمایشگاه FortiGuard به تازگی ایمیلی را بررسی کرده که با شیوه‌ای جدید در حال انتشار بدافزار TrickBot است.

TrickBot نوعی بدافزار بارگذاری‌کننده است که می‌تواند سایر مؤلفه‌های مخرب را دانلود و آن‌ها را اجرا کند. ایمیل‌های مخرب تحت موضوعاتی مانند تراکنش‌های مالی و فاکتورهای خرید ارسال می‌شوند. کاربر قربانی وادار می‌شود تا برای دانلود فایل تراکنش مالی، روی یک لینک مخرب کلیک کند که این لینک یک فایل Zip مخرب، حاوی بدافزار، دانلود می‌کند. آدرسی که فایل Zip از آن دانلود می‌شود یک دامنه عادی است که به نظر می‌رسد مورد نفوذ مهاجمین قرار گرفته باشد.

در صورتی که قربانی فایل VBS را اجرا کند، یک فایل exe در رایانه وی بارگذاری و سپس به a.exe تغییر نام داده می‌شود. این فایل یک نمونه بدافزار TrickBot است که در بخش Task Scheduler سیستم قربانی نصب می‌شود. بدافزار سپس در پوشه %AppData% به gpuDriver تغییر نام می‌دهد: در ادامه بدافزار اطلاعات سیستم را برای سرور فرمان و کنترل (C&C) ارسال می‌کند تا مؤلفه‌های مخرب دیگر را انتقال دهد.

مرکز ماهر هشدار داد؛

شناسایی ۳۰۰ نمونه بدافزار اندرویدی/ فریب کاربر با تلگرام‌های جعلی

مرکز ماهر در اطلاعیه‌ای از شناسایی بدافزارهای RTR خبر داد و هویت توسعه دهنده این بدافزارها را فاش کرد. بدافزارهای RTR دسته‌ای از بدافزارها هستند که توسط توسعه‌دهنده متخلفی با نام مستعار RTR منتشر شده‌اند. بر اساس بررسی‌های انجام شده از سوی مرکز ماهر، تاکنون بیش از ۳۰۰ نمونه از بدافزارهای RTR شناسایی شده است. برخی از این بدافزارها در فروشگاه‌های اندرویدی کافه بازار، مایکت، گوگل پلی و ایران اپس منتشر شده‌اند و برخی دیگر از طریق تبلیغات تلگرامی و دانلود خودکار توسط دیگر برنامه‌ها روی دستگاه قربانیان قرار گرفته‌اند.

به‌طور کلی بدافزارهای RTR را می‌توان در ۵ شاخه مختلف دسته‌بندی کرد:

۱. بدافزارهای مخفی شونده که از نام‌های مستهجن برای جذب مخاطب استفاده می‌کنند.

۲. نسخه‌های جعلی و غیررسمی تلگرام که از آن‌ها برای فروش عضو، ارسال تبلیغات در گروه‌ها و ... استفاده می‌کنند.

۳. برنامه‌های کاربردی که اغلب با استفاده از سرویس‌های ارسال هشدار، عملیات مخرب مختلفی روی دستگاه قربانی انجام می‌دهند.

٤. بدافزارهای ارزش‌افزوده که برای چندین شرکت مختلف ارزش‌افزوده، بدافزارهای واسطی را منتشر کرده و از این طریق به عضوگیری برای این سرویس‌ها پرداخته‌اند.

۵. برنامه‌هایی همنام با برنامه‌های محبوب و معروف خارجی مانند برخی پیام‌رسان‌ها.

بازی رایانه‌ای ضد دیابت هم تولید شد.

به تازگی یک بازی رایانه‌ای ضد دیابت تولید شده که به مغز افراد می‌آموزد تا کمتر شکر مصرف کنند و بدین شکل سلامتی خود را حفظ کنند. محققان برای اولین بار بازی رایانه‌ای را طراحی کرده‌اند که بخش‌هایی از مغز را هدف قرار می‌دهد که به پالس های تحریک کننده نیاز به شکر را منتشر می‌کنند. با از کار افتادن این بخش‌های مغز و عدم انتشار پالس توسط آن‌ها مغز از شکر احساس بی‌نیازی می‌کند.

پژوهشگران امیدوارند در آینده با طراحی بازی‌های مشابه بتوانند مغز را به‌گونه‌ای دستکاری کنند که بتواند از برخی عادات ناپسند دیگر مانند لذت بردن از کشیدن سیگار یا پرخوری نیز دست بردارد. بازی یاد شده با موفقیت بر روی ۱۰۹ داوطلب که همگی اضافه وزن داشته و علاقه زیادی به خوردن انواع شیرینی و شکر داشتند آزمایش شده و نتیجه آن امیدبخش بوده است.

این بازی که در دانشگاه درکسل آمریکا طراحی شده فعلاً در مرحله آزمایشی است و البته واکنش زنان به آن در مجموع بهتر از مردان بوده است. در فرایند بازی مذکور ابتدا مواد شیرین مورد علاقه هر فرد شناسایی می‌شود و سپس فرایند بازی به گونه‌ای پیش می‌رود که کاربر مجبور شود در برابر وسوسه خوردن این شیرینی‌ها مقاومت کند تا به موفقیت برسد. روند بازی و دشواری آن نیز در هر مرحله بیشتر می‌شود.

واتس‌اپ به جاسوس‌افزار رژیم صهیونیستی آلوده شد

شکافی در اپلیکیشن پیام‌رسان واتس‌اپ به هکرها اجازه داده یک نرم‌افزار جاسوسی تجاری متعلق به رژیم صهیونیستی را روی موبایل تعدادی از کاربران نصب کنند. واتس‌اپ اعلام کرده در اوایل ماه می متوجه شده هکرها می‌توانند با نصب یک نرم‌افزار نظارتی روی آیفون و دستگاه‌های اندروید از کاربران جاسوسی کنند. این نرم‌افزار جاسوسی با یک تماس در واتس‌اپ روی موبایل فرد موردنظر نصب می‌شود.

شرکت NSO متعلق به رژیم صهیونیستی این نرم‌افزار جاسوسی را توسعه داده است. یکی از دلالان تجهیزات جاسوسی به فایننشال تایمز گفته حتی اگر کاربر به تماس واتس‌اپی پاسخ ندهد، بازهم نرم‌افزار مذکور روی دستگاه او نصب می‌شود. همچنین شماره تلفن مربوط به این تماس از فهرست تماس‌های کاربر خودبه‌خود حذف می‌شود.

روز یکشنبه هفته جاری پس از آنکه موبایل یکی از وکلای حقوق بشر هدف این نرم‌افزار واقع شد، مهندسان واتس‌اپ به‌سرعت شکاف امنیتی موجود در پیام‌رسان را برطرف کردند. در بیانیه این شرکت آمده است: این حمله تمام نشانه‌های مربوط به فعالیت‌های شرکتی را دارد که با دولت‌ها و سازمان‌های جاسوسی همکاری می‌کند. این نرم‌افزارها موبایل کاربر را کنترل می‌کنند.

همچنین به گفته یک منبع آگاه واتس‌اپ این اختلال را هفته گذشته به وزارت دادگستری ایالات‌متحده آمریکا گزارش کرده است. به‌هرحال مهم‌ترین و شناخته‌شده‌ترین محصول جاسوسی شرکت NSO متعلق به رژیم صهیونیستی Pegasus نام دارد و می‌تواند به‌طور خودکار میکروفون و دوربین موبایل فرد مورد نظر را روشن کند، ایمیل‌های او را بررسی کند و اطلاعات مربوط به موقعیت مکانی وی را جمع‌آوری کند. بسیاری از دولت‌ها از این نرم‌افزار جاسوسی استفاده می‌کنند.

بانک مرکزی پیرو بخشنامه‌ای در خصوص جایگزینی رمزهای پویا به جای رمزهای ایستا در پرداخت‌های بانکی تأکید کرده که بانک‌ها می‌توانند با قبول مسئولیت هرگونه سوءاستفاده از مسائل امنیتی و جبران خسارات احتمالی وارد شده به مشتریان، برای تراکنش‌های زیر پانصد هزار تومان در روز از همان رمزهای ایستای سابق استفاده کنند. همچنین اعلام‌شده که تأمین امنیت مشتریان نظام بانکی از اول خردادماه تماماً بر عهده بانک‌ها بوده و مرجع قضایی در این مورد بسیار جدی عمل خواهد کرد. بانک مرکزی همچنین ذکر کرده که رمز دوم یک‌بارمصرف هیچ‌گونه هزینه‌ای برای مشتریان بانک نباید به همراه داشته باشد. در این بخشنامه آمده که بانک‌ها در صورت راهکار جایگزین دیگری می‌توانند آن را با بانک مرکزی در میان بگذارند. بانک مرکزی تأکید کرده که رمز دوم یک‌بارمصرف نباید محدود به گوشی‌های هوشمند شود.

به منظور پشتیبانی حداکثری از مشتریان ضرورت دارد امکانات ارائه رمز محدود به استفاده از برنامه‌های کاربردی گوشی‌های هوشمند نشده و ارائه آن از طریق سایر ابزارها نظیر پیامک، پیام‌رسان‌های داخلی مجاز و نظایر آن برای مشتریان بانک‌ها نیز حسب تشخیص بانک فعال شود .گفتنی است به جز بخشنامه بانک مرکزی که اخیراً منتشر شده، «عبدالناصر همتی» رئیس‌کل بانک مرکزی نیز در طی یادداشتی در سایت بانک مرکزی اعلام کرده که این موضوع طرح تأمین امنیت حساب‌ها بوده و نبایستی به کسب‌وکارهای نوپا لطمه‌ای وارد کند. بیشتر بانک‌ها ازجمله بانک ملی، سامان، ملت، سینا، تجارت و چندین بانک دیگر مدتی است که اپلیکیشن‌های مختص ایجاد رمز یک‌بارمصرف خود را ایجاد کرده‌اند.

توضیحات مهم بانک مرکزی در مورد رمزهای یک‌بارمصرف بانکی

مهم‌ترین به‌روزرسانی های ماه جاری شرکت‌های تولید کننده سخت افزار و نرم افزار

سیسکو وصله‌های امنیتی جهت رفع ده‌ها آسیب‌پذیری در محصولات خود منتشر کرده است. در میان نقص‌هایی که سیسکو برطرف ساخته است، آسیب‌پذیری بحرانی در سوئیچ‌های Nexus 9000 وجود دارد که با شناسه‌ی CVE- CVE- 2019- 1804 ردیابی می‌شود و رتبه‌ی CVSS 9.8 را دریافت کرده است.

آسیب‌پذیری بحرانی دیگر در محصول Elastic Services Controller (ESC) سیسکو وصله شده است و از طریق آن یک مهاجم احراز هویت نشده با دسترسی راه دور می‌تواند از این آسیب‌پذیری سوء استفاده کند و فرایند احراز هویت روی REST API را دور بزند و با دسترسی سطح مدیر، اقدامات دلخواه را انجام دهد. نمره CVSS این آسیب‌پذیری ۱۰ محاسبه شده که به دلیل امکان بهره‌برداری روی شبکه و عدم نیاز به دسترسی خاص مهاجم یا تعامل قربانی است.
تمامی نسخه‌های اصلی ESC شامل ٤،١، ٤،٢، ٤،٣ یا ٤،٤ نسبت به این نقص آسیب‌پذیر هستند. به منظور رفع این باگ، وصله‌های امنیتی برای هر یک از نسخه‌ها منتشر شده است.

سیسکو همچنین وصله‌هایی برای بیش از ۲۰ آسیب‌پذیری با شدت بالا که نرم‌افزار Web Security Appliance (WSA)، Umbrella Dashboard، Adaptive Security Appliance (ASA) و Firepower Threat Defense (FTD)، مسیریاب‌های RV320 و RV325، IP Phone سری‌های ۷۸۰۰ و ۸۸۰۰، نرم‌افزار Application Policy Infrastructure Controller (APIC) و سوئیچ‌های Nexus 9000 را تحت‌تأثیر قرار می‌دهد، منتشر ساخته است.

سوءاستفاده از این آسیب‌پذیری‌ها به مهاجمان اجازه‌ی افزایش امتیاز، ایجاد انکار سرویس در دستگاه‌های متأثر، سرقت نشست‌ها، دسترسی به یک داشبورد، دور زدن احراز هویت گواهینامه، استقرار یک نشست VPN یا کشف کلیدهای خصوصی یک دستگاه متأثر می‌دهد.

اوراکل به‌روزرسانی امنیتی را برای رفع آسیب‌پذیری روز صفرم روی سرور Oracle WebLogic که شناسهٔ CVE-2019-2725 به آن اختصاص داده شده است، منتشر کرد. مهاجم می‌تواند از طریق این آسیب‌پذیری، از راه دور دستورات را بدون ارسال مجوز و با ارسال یک درخواست HTTP ویژهٔ ساخته‌شده، مورد سوءاستفاده قرار دهد.

سرورهای WebLogic همواره موردعلاقه‌ی هکرها بوده‌اند. به این علت که سرورهای WebLogic معمولاً به مقادیر زیادی از منابع دسترسی دارند. علاوه بر این، به دلیل اینکه سرورهای WebLogic اغلب در شبکه‌های سازمانی یا برای اجرای اینترانت‌ها یا دیگر برنامه‌های سازمانی دولتی مستقر می‌شوند، هرگونه مشکلی از یک سرور WebLogic به راحتی می‌تواند به یک فاجعه تبدیل شود و اطلاعات حساس تجارتی را در اختیار هکرها قرار دهد.

NVIDIA یک به روزرسانی امنیتی برای رفع سه آسیب‌پذیری با درجه حساسیت بالا در درایورهای GPU خود منتشر کرده است که منجر به اجرای کد، ایجاد وضعیت انکار سرویس، افزایش دسترسی یا افشای اطلاعات روی سیستم‌های ویندوز آسیب‌پذیر می‌شوند.

به گزارش پایگاه اینترنتی BleepingComputer، با اینکه برای سوء استفاده از این آسیب‌پذیری‌ها مهاجم نیاز به دسترسی محلی دارد، اما می‌توان با بهره‌برداری از ابزارهای مخرب دارای دسترسی راه دور از نقص‌های یک رایانه دارای نسخه درایور GPU آسیب‌پذیر، سوء استفاده کرد.

شرکت NVIDIA نسخه‌های جدید درایور گرافیکی سیستم‌عامل ویندوز را منتشر کرده است که آسیب‌پذیری‌های ذکر شده در آن‌ها رفع شده‌اند.

گوگل نسخه ۷٤ مرورگر کروم را برای سیستم‌عامل‌های ویندوز، مک و لینوکس منتشر کرده است که در آن ۳۹ آسیب‌پذیری امنیتی برطرف شده است. در ۳۹ آسیب‌پذیری رفع شده در نسخه ۷٤،۰,۳۷۲۹,۱۰۸ تنها ۵ مورد دارای درجه حساسیت بالا هستند.

دروپال یک به‌روزرسانی امنیتی برای رفع آسیب‌پذیری موجود در هسته‌ی دروپال منتشر کرد. این آسیب‌پذیری با شناسهٔ "CVE-2019-11831" مشخص شده است و دارای درجه‌ی «متوسط» است. یک مهاجم می‌تواند از راه دور از این آسیب‌پذیری برای کنترل وب‌سایت آسیب‌دیده استفاده کند.

به‌روزرسانی امنیتی دروپال، وابستگی‌های شخص ثالث را که در هستهٔ دروپال موجودند یا مورد نیاز آن هستند، رفع می‌کند.
به کاربران و مدیران توصیه می‌شود به‌روزرسانی‌های لازم را برای رفع این آسیب‌پذیری انجام دهند:

- کاربرانی که از دروپال ۸,۷ استفاده می‌کنند، آن‌را به ۸,۷,۱ به‌روزرسانی کنند.
- کاربرانی که از دروپال ۸,٦ یا قبل از آن استفاده می‌کنند، آن‌را به ۸,٦,۱٦ به‌روزرسانی کنند.
- کاربرانی که از دروپال ۷ استفاده می‌کنند، آن‌را به ۷,٦۷ به‌روزرسانی کنند.

نسخه‌های دروپال ۸ قبل از ۸,٦x. به پایان عمر خود رسیده‌اند و پوشش‌های امنیتی را دریافت نمی‌کنند.

باتوجه به اهمیت آسیب‌پذیری‌های ذکرشده، به‌روزرسانی این محصولات برای رفع نقایص موجود امری ضروری است و به کاربران توصیه می‌شود تا هرچه سریع‌تر وصله‌های منتشرشده را اعمال کنند.

معرفی کتاب

جنگ سایبری؛ عملیات اطلاعاتی در جهان متصل

کتاب «جنگ سایبری؛ عملیات اطلاعاتی در جهان متصل»، نوشته مایک چپل **Mike Chapple** و دیوید سیدل **David Seidl**، متخصصان برجسته حوزه امنیت سایبری با اتکا به نگاهی واقع‌بینانه و تجربی، به تشریح و توضیح مسائلی در خصوص جنگ سایبری می‌پردازد. این نوشتار، مخاطب را در یک میدان جنگ سایبری فرضی، قرار می‌دهد. خوانندگان اثر یادشده، تاریخ جنگ‌های سایبری، فناوری‌های مورد استفاده ازسوی گروه‌های هکری در عملیات تهاجمی و تدافعی و شکل‌گیری دکترین نظامی مبتنی بر جنگ سایبری را در این کتاب می‌آموزند.

انتشار این کتاب، به اول سپتامبر ۲۰۱۴ باز می‌گردد. با وجود گذشت زمانی ۵ ساله از چاپ و پخش آن به صورت عمومی، چیزی از ارزش محتوای آن، برای مشتاقان این حوزه، نکاسته است.

از نکات برجسته این کتاب می‌توان به موارد زیر اشاره کرد:

- مطالعه موردی حملات سایبری مشهور تاریخ و تشریح کامل شرایط و اتفاقات
- کاربرد برخی اطلاعات طبقه بندی شده نشت یافته از نهادهای اطلاعاتی مانند داده‌های ادوارد اسنودن، از سازمان امنیت ملی ایالات متحده
- برخی فعالیت‌های تمرینی به منظور آماده‌سازی-دانشجویان این حوزه، برای تبدیل‌شدن به کارشناس امنیت سایبری

طرح‌های کسر خدمت سربازی

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

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

سایت های مرتبط با پدافند غیرعامل	
وب سایت پایداری ملی	http://www.paydarymelli.ir
مرکز مطالعات پدافند غیرعامل	http://www.pdrc.ir
استانداری آذربایجان شرقی – پدافند غیرعامل	http://ostan-as.gov.ir/?PageID=42
پلیس فتا	http://www.cyberpolice.ir/
مرکز مطالعات فنی و مهندسی پایداری ملی	http://mafpa.ir/
سایت دومین کنفرانس ملی پدافند سایبری	hamayesh.iau-maragheh.ac.ir/cp2018

جهت دسترسی به آرشیو نشریه به این لینک مراجعه فرمایید.