ماهنامه اداره کل پدافند غیرعامل
شماره ۵۷/ خرداد ماه ۱۴۰۰

ماهنامه دیجیتالی پدافند غیرعامل

مدیرکل پدافند غیرعامل استانداری:

درک درست از اهمیت پدافند زیستی و پایبندی به اصول پدافند غیرعامل در حوزه دامپزشکی، ارتقاء سلامتی و بهداشت جامعه را فراهم می‌آورد

جلسه آموزشی طرح نویسی در منطقه آزاد ارس برگزار شد.

در این شماره می‌خوانید:

مکان‌یابی از منظر پدافند غیرعامل

آسیب‌پذیری

اکثر توزیع‌های Linux، تحت تأثیر آسیب‌پذیری polkit

هک دستگاه‌های VPN Pulse Secure

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

جهت دسترسی به آرشیو نشریه به این لینک مراجعه فرمایید.

تداوم نظم عمومی

مردم به معنای واقعی کلمه یک نظم عمومی را در مواجهه‌ی با این حادثه پذیرفته‌اند که البتّه باید ادامه پیدا کند؛ این نظم عمومی بایستی وجود داشته باشد، باید تصمیم‌های ستاد ملّی [مبارزه با کرونا] -که در این زمینه، مسئول درجه‌ی اوّل است- جدّی گرفته بشود و بر طبق آنها عمل بشود.


بسم الله الرحمن الرحیم

فهرست مطالب:

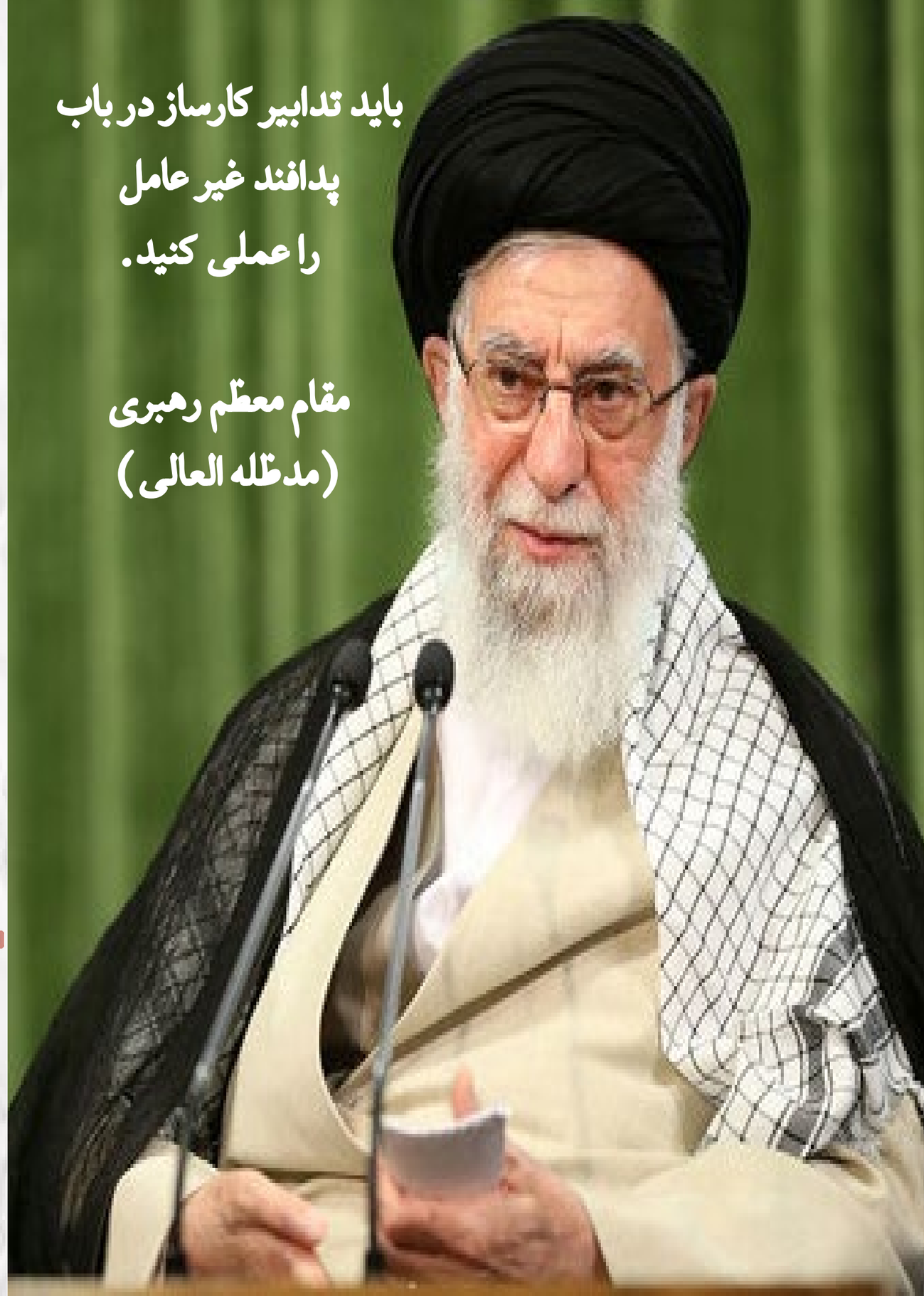
مدیر مسئول:
محمد باقر آقایی

سردبیر:
لیدا رسول اهری

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

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

passivedefense@ostan-as.gov.ir



مدیرکل پدافند غیرعامل استانداری آذربایجان‌شرقی با امیرحسین بهداد مدیرکل دامپزشکی استان دیدار و گفت وگو کرد.

محمد باقر آقایی ضمن تقدیر و تشکر از اقدامات ارزنده مجموعه دامپزشکی استان خاطر نشان کرد، درک درست از اهمیت پدافند زیستی و پایبندی به اصول پدافند غیرعامل در حوزه دامپزشکی، ارتقاء سلامتی و بهداشت جامعه را فراهم می‌آورد.

ایشان علاوه بر تأکید بر روی رصد، پایش و نیز احصاء تهدیدات زیستی، آموزش مقابله با انواع تهدیدات را از مهم‌ترین اقدامات پدافندی عنوان نمودند.

با توجه به مسئولیت اداره کل دامپزشکی در حفظ و حراست از سرمایه دامی و تأمین سلامت و بهداشت جامعه انسانی در تأمین غذای مردم در شرایط عادی، بحرانی و تهاجمی دشمن نقش حیاتی دارد.

به همین دلیل استراتژی پدافند غیرعامل اداره کل دامپزشکی باید استفاده از سیستم‌های مراقبتی از بیماری های دامی و قرنطینه‌های داخلی کشور با برنامه‌های مدونی در دستور کار باشد تا بتوانند به موقع از شیوع اپیدمی‌های منطقه‌ای و بین المللی جلوگیری نموده تا غافگیر نشوند.

ایشان در ادامه به مباحث تخصصی پدافند زیستی در مرزها و گمرکات استان، آزمایشگاه‌ها، کشتارگاه‌ها، مراکز پرورش دام و اصلاح ژنتیک پرداختند. در همین راستا دو طرف بر ضرورت همکاری دو جانبه تأکید کردند.

همچنین امیرحسین بهداد با قدردانی از همکاری اداره کل پدافند غیرعامل به بیان اقدامات پدافندی انجام یافته از جمله ساماندهی میادین دام و کنترل بیماری‌های دامی پرداختند.

جلسه آموزش طرح نویسی در منطقه آزاد ارس

آقای محمودیان کارشناس پدافند غیرعامل استانداری در جلسه آموزش طرح نویسی گفت: با توجه به ساختار و بافت منطقه آزاد ارس، شرایط اقلیمی و آمایش سرزمینی، نوع تهدیدات و نقاط آسیب‌پذیر در این منطقه متفاوت می‌باشد.

هدف از برگزاری این جلسه آشنایی با مخاطرات انسان‌ساخت و شناسایی نقاط آسیب‌پذیر منطقه آزاد ارس و ارائه راهکارهای عملی با هم‌اندیشی اعضای کمیته است.

رستمی دبیر پدافند غیرعامل منطقه آزاد ارس، ضمن تشکر از اداره کل پدافند غیرعامل استانداری در برپایی این جلسه و حمایت مدیرکل در اجرای طرح‌های پدافند غیرعامل در منطقه آزاد ارس، گزارش مبسوطی در خصوص عملکرد پدافند غیرعامل در حوزه کالبدی، امنیتی و شیمیایی ارائه نمودند.

در پایان طبق دستور کار جلسه جهت تهیه شیوه نامه عملیات پدافند شیمیایی و طرح مصون‌سازی زیرساخت‌های شیمیایی، تصمیمات لازم اتخاذ گردید.

مدیرکل پدافند غیرعامل استان آذربایجان شرقی از مطالعات طرح جامع پدافند غیر عامل شیمیایی شرکت کلر پارس خبر داد

با توجه به دغدغه‌ها و تهدیدات شیمیایی و حساسیت موجود در خصوص فعالیت شرکت کلر پارس از منظر تهدیدات زیست محیطی، ضرورت ایجاب می‌نماید تا در این حوزه مطالعات و تحقیقات علمی جامعی صورت پذیرد.

مدیرکل پدافند غیرعامل استان گفت: به منظور ایمن سازی و تداوم کار شرکت کلر پارس در شرایط عادی و در شرایط بحرانی و اضطراری و جلوگیری از هرگونه خسارات احتمالی جانی، مالی و زیست محیطی متصور در استان، به خصوص شهر تبریز و شهرستان‌های همجوار، اداره کل پدافند غیرعامل درصدد است طرح مطالعاتی جامعی در این خصوص انجام گیرد. با عنایت به تفاهم‌نامه ای که بین این اداره کل و دانشگاه تبریز بسته شده است دانشگاه تبریز مجری اجرای طرح مطالعاتی خواهد بود.

در همین راستا در چند روز آینده انشاءالله دیدار سه جانبه‌ای جهت هماهنگی و بررسی‌های اولیه طرح مطالعاتی با محوریت اداره کل پدافند غیرعامل استان، دانشگاه تبریز و شرکت کلر پارس ترتیب داده خواهد شد.

امید است قرارداد طرح مطالعاتی در هفته پدافند شیمیایی منعقد گردد.

مکان‌یابی از منظر پدافند غیرعامل

تهیه و تنظیم: ساسان بداقلو(کارشناس امریه اداره کل پدافند غیرعامل)

منبع:
۱. بداقلو، ساسان، امین نیری، بهناز، علیزاده، نسیم، (۱۳۹۸)، پدافند غیرعامل در شهرهای بندری ایران، چاپ اول، تهران : انتشارات علم و دانش.

مقدمه

برای رسیدن به الگوی دفاعی پایدار، اصولی را برای پدافند غیرعامل طراحی کرده‌اند که این اصول باید به راهبردها و راهکارهای اجرایی تبدیل شود. مفهوم عبارت دفاع غیرنظامی عبارت است از حفاظت از غیرنظامیان در شرایط جنگی؛ و از این رو مشتمل بر بخشی از دفاع ملی است که در پی تمهیدات لازم به‌منظور کسب آمادگی کافی در برابر هرگونه حمله احتمالی به یک کشور ایجاد می‌گردد. طبق این تعریف، دفاع غیرنظامی باید ایمنی جمعیت غیرنظامی کشور و ادامه حیات آنان در زمان جنگ را تضمین نماید. دفاع غیرنظامی به‌صورت سیستماتیک اهداف زیر را دنبال می‌نماید:

• مجموعه تمهیدات دفاع عامل و غیرعامل برای افراد و تأسیسات غیرنظامی، مجموعه فعالیت‌هایی که می‌توان با انجام آن از بروز و استمرار سوانحی که جان و مال مردم را تهدید می‌کند جلوگیری نمود و یا در صورت بروز آثار آن را کاهش داد.

• کاهش خسارات مالی و صدمات جانی وارده بر غیرنظامیان در اثر حوادث طبیعی یا غیرطبیعی

• به حداقل رسانیدن آثار حاصل از حملات نظامی بر جمعیت غیرنظامی

• مقابله فوری با شرایط اضطراری حاصل از حملات نظامی بر جمعیت غیرنظامی

• بازیابی و برقراری تسهیلات و خدمات به آسیب دیدگان

اهداف اصلی پدافند غیرعامل شامل استمرار فعالیت‌های زیربنایی، تأمین نیازهای حیاتی، تداوم خدمات‌رسانی عمومی و تسهیل اداره کشور در شرایط تهدید و بحران تجاوز خارجی و همچنین حفظ بنیه دفاعی به‌رغم حملات خصمانه و مخرب دشمن از طریق اجرای طرح‌های پدافند غیرعامل می‌باشد. در راستای دستیابی به اهداف ذکر شده باید در زمان اجرای پدافند غیرعامل به این اقدامات توجه داشت: مکان‌یابی، اعلام خبر، استحکامات، پراکندگی، پوشش، فریب، استتار، اختفا.

ملاحظات پدافند غیرعامل در مکان‌یابی

یکی از مهم‌ترین اصول پدافند غیرعامل، اصل مکان‌یابی است. مکان‌یابی فرآیندی است که طی آن بهترین مکان برای سایت یا فعالیت مورد نظر بر اساس یک سری شاخص‌ها و اصول انتخاب می‌شود. چون نوع فعالیت و درجه اهمیت مکان می‌تواند بر شاخص‌های مکان‌یابی و لاجرم انتخاب مکان تأثیرگذار باشد. در یک تقسیم‌بندی پدافندی، مراکز را به سه دسته تقسیم می‌کنند:

۱ـ مراکز حیاتی: مراکزی هستند که در صورت انهدام کلی یا قسمتی از آن‌ها موجب بروز بحران، آسیب و صدمات جدی و مخاطره‌آمیز در نظام سیاسی، دفاعی، فرماندهی و کنترل، هدایت امور تولیدی و اقتصادی پشتیبانی، ارتباطی و مواصلاتی، اجتماعی با سطح تأثیرگذاری سراسری در کشور گردد.

۲ـ مراکز حساس: مراکزی هستند که در صورت انهدام کلی یا قسمتی از آن‌ها موجب بروز بحران، آسیب و صدمات جدی و مخاطره‌آمیز در نظام سیاسی، دفاعی، فرماندهی و کنترل، هدایت امور تولیدی و اقتصادی پشتیبانی، ارتباطی و مواصلاتی، اجتماعی با سطح تأثیرگذاری منطقه‌ای در کشور گردد.

۳ـ مراکز مهم: مراکزی هستند که در صورت انهدام کلی یا قسمتی از آن‌ها موجب بروز آسیب و صدمات محدود در نظام سیاسی، دفاعی، فرماندهی و کنترل، هدایت امور تولیدی و اقتصادی پشتیبانی، ارتباطی و مواصلاتی، اجتماعی با سطح تأثیرگذاری محلی در کشور گردد .

این موضوع که چگونه می‌توان از اصل مکان‌یابی برای نیل به سایر اصول پدافند غیرعامل بهره برد همیشه به‌عنوان یک چالش مهم مطرح بوده است. مکان‌یابی مطلوب را می‌توان مهم‌ترین اقدام پدافند غیرعامل در کاهش آسیب‌پذیری مراکز حیاتی و حساس محسوب نمود؛ زیرا اگر در مرحله صفر پروژه طراحی، احداث و تأسیس مراکز حیاتی و حساس عوامل و معیارهای ذیربط دفاعی و امنیتی از قبیل حداکثر استفاده از عوارض طبیعی، آمایش سرزمینی، رعایت پراکندگی، پرهیز از انبوه و حجیم‌سازی، مقاوم‌سازی اولیه رعایت و نظارت گردد از بروز بسیاری از مشکلات پیچیده و هزینه‌بر بعدی جلوگیری به عمل خواهد آمد.

اهمیت بالای مراکز حیاتی، حساس و مهم کشور و حتی مراکز با درجات اهمیت پایین‌تر ایجاب می‌کند تا در مکان‌یابی آن‌ها علاوه بر در نظر گرفتن کلیه شاخص‌های موجود، به شاخص‌های پدافند غیرعامل، یعنی شاخص‌هایی که بتواند آسیب‌پذیری مجموعه را کاهش و استمرار تولید را افزایش دهد، نیز پرداخته شود. تجربیات به دست آمده در این زمینه نشان می‌دهد که در مکان‌یابی از منظر پدافند غیرعامل باید به موارد زیر توجه داشت:

۱ـ ساخت پناهگاه: دو اصل از اصول نه‌گانه پدافند غیرعامل، اصل اختفا و اصل پوشش می‌باشد. بدین معنی که با مخفی کردن مرکز یا فعالیت مورد نظر،

با روش‌های مختلف یا استفاده از پوششی بر روی آن می‌توان به‌نوعی دشمن را فریب داد و از دید مستقیم دشمن دور کرد. در مراکز فعالیت، نیروی انسانی متخصص مشغول کارند که لزوم حفظ آن‌ها در هنگام هرگونه بحران و تهدید از اولویت‌ها می‌باشد. از آنجایی که یکی از اهداف پدافند غیرعامل تداوم حیات و استمرار فعالیت مراکز حیاتی، حساس و مهم در زمان بحران می‌باشد، لذا لازم است برای افزایش امنیت نیروی انسانی ماهر مشغول به فعالیت در این سایت‌ها با مکان‌یابی مطلوب بهترین مکان‌ها جهت ساخت پناهگاه شناسایی و مکان‌یابی شود. چرا که با مکان‌یابی بهینه می‌توان زمان دسترسی به پناهگاه را کاهش داده و علاوه بر این با استفاده از چیدمان مطلوب کاربری‌ها و عوارض طبیعی موجود در سطح زمین، ضریب ایمنی سایت‌های مورد نظر را تا حد زیادی ارتقا داد.

۲ـ عمق سرزمینی: یکی از مباحثی که در پدافند غیرعامل در جانمایی مراکز فعالیت وجود دارد، استقرار آن‌ها در فاصله‌ای دور از مرزهای کشور می‌باشد. هرچند که استاندارد دقیقی در این زمینه وجود ندارد و این فاصله باید بر اساس فاکتورهای زیادی تعیین شود ولی این مسئله باید در مکان‌یابی رعایت شود. پر واضح است که با پیشرفت‌های زیاد تکنولوژیکی به‌ویژه در زمینه علوم نظامی و تسلیحات، اهمیت فاصله از مرزهای کشور کاهش یافته است اما نمی‌توان نسبت به این مسئله بی‌توجه بود چرا که گاهی اوقات حتی فاصله چند کیلومتری می‌تواند بر تصمیم دشمن به حمله یا عدم حمله تأثیر بگذارد.

۳ـ پراکندگی و تفرق: از دیگر موضوعاتی که در مکان‌یابی از منظر پدافند غیرعامل باید به آن توجه نمود، موضوع پراکندگی و تفرق است. با مجتمع و متمرکز کردن کلیه تأسیسات و احداثات مربوط به یک سایت، دشمن با صرف هزینه کمتر، آسیب بیشتری به آن‌ها وارد می‌کند. اما چنانچه کلیه ساختمان‌ها و تأسیسات مربوط به یک سایت به‌صورت پراکنده و جدا از هم ساخته شوند، هم آسیب‌پذیری را کاهش می‌دهد و هم میزان هزینه پرداختی کشور متخاصم برای از بین بردن این تأسیسات را افزایش می‌دهد که این موضوع می‌تواند دشمن را از تصمیم حمله منصرف کند. اصل تفرق نیز در مورد افراد بکار می‌رود. یعنی علاوه بر پراکنده‌سازی و کوچک‌سازی تأسیسات، تا جایی که امکان دارد باید افراد را نیز از هم دور کرد. به همین علت در برنامه‌ها و طرح‌های آمایش سرزمین از تمرکز زدایی علاوه بر مزایای زیادی که دارد به‌عنوان یک اصل برای افزایش ضریب امنیتی و دفاعی کشور نیز یاد می‌کنند.

۴ـ دسترسی: بدون شک دسترسی به شبکه‌های ارتباطی از پارامترهایی است که تاکنون در مکان‌یابی سایت‌ها و مراکز مختلف مورد توجه قرار گرفته است اما در مقوله پدافند غیرعامل باید به دسترسی به‌عنوان یک اصل کلیدی نگاه کرد. دلیل آن هم این است که کالاها و خدمات تولید شده در مراکز حیاتی، حساس و مهم کشور به اندازه‌ای برای کشور مهم هستند که اولاً باید مواد اولیه مورد نیاز برای آن‌ها به محل تولیدشان انتقال یابد، ثانیاً کالای تولیدشده باید از محل تولید به دست مصرف‌کننده برسد. بدین منوال، دسترسی برای انجام این دو مرحله بسیار اساسی است. گاهی اوقات سایت یا مرکز فعالیت به حدی مهم و حیاتی است که نیاز است از چندین نوع دسترسی استفاده شود.

۵ـ انرژی‌های ثانویه: برای تداوم و استمرار تولید صنایع و مراکز مهم نیاز است علاوه بر مرکز اولیه تأمین انرژی، مراکز دیگری نیز به‌عنوان تأمین‌کننده انرژی ثانویه در نظر گرفته شود تا در هنگام بحران، صنایع تولیدکننده کالاهای اساسی برای کشور، استمرار تولید داشته باشند و بتوانند بکار خود ادامه دهند.

۶ـ عدم قرارگیری در مسیر دالان‌های هوایی: مسیر دالان‌های هوایی، مسیرهایی هستند که برای تردد و عبور و مرور هواپیماها استفاده می‌شوند. علت مهم‌بودن این مقوله در مکان‌یابی از منظر پدافند غیرعامل این است که زمانی که یک هواپیمای مسافربری در مسیر دالان‌های هوایی یا غیر آن در حرکت است، چنانچه یک یا حتی چند هواپیمای نظامی و جنگنده در زیر آن حرکت کند رادارها و ردیاب‌ها قادر به نشان دادن هر دوی آن‌ها نیستند. از آنجا که ممکن است دشمن از این روش‌ها برای حمله و غافلگیرکردن به تأسیسات حیاتی کشور استفاده کند، ضروری است تا جایی که امکان دارد مراکز حیاتی، حساس و مهم کشور در مسیر دالان‌های هوایی قرار نگیرند.

مطالعات صورت گرفته

تاکنون تحقیقات متعددی در خصوص برنامه‌ریزی پدافند غیرعامل و ضرورت توجه به پدافند غیرعامل توسط محققین ایرانی و بین‌المللی انجام شده است. ایکرت و همکارش در مقاله‌ای تحت عنوان «طراحی بهینه تحت عدم قطعیت در ساختار پدافند غیرعامل در برابر بهمن‌های برف: از چارچوب بیزضی عمومی به مدل تحلیلی ساده» کوشیده تا با الهام گرفتن از خطرات طبیعی دیگر، به یافتن روش‌های جایگزین بر اساس حداکثر سود اقتصادی از ساختار دفاعی، دست یابند. در این پژوهش، از سه مدل با عنوان‌های مدل مخاطرات و عدم قطعیت‌های مرتبط، مدل هزینه کمی و محاسبه خطر و مدل خطی اثر مانع استفاده گردیده است. همچنین یک مدل فرضی نیز با توجه به توسعه‌های بیشتر ممکن، ارائه گردیده است.

برنافر و همکاران مقاله‌ای تحت عنوان «برنامه ریزی پدافند غیرعامل (مطالعه موردی: شهر لنگرود)» در ماهنامه تخصصی راه و ساختمان به چاپ رساندند که در آن به کاهش خسارات وارد بر شهر، حراست از سرمایه‌های انسانی و مادی شهر و همچنین کنترل کیفی و کمی توسعه شهر توجه شده و نگارندگان به این نتیجه رسیده‌اند که در چهارچوب برنامه‌های شهری این شهر، به موضوع دفاع به‌عنوان یک اصل کلیدی پرداخته نشده و لازم است مفاهیم اصلی پدافند غیرعامل در بافت فعلی شهر و پروژه‌های در دست اجرا و آتی مورد عنایت و بهره برداری قرار گیرند.

ابوالحسنی نیز در تحقیقی با عنوان «پدافند غیرعامل- معماری و طراحی شهری در ایران» به بررسی عوامل تأثیرگذار در آسیب‌پذیری شهری و ارائه راهکارهایی در طراحی شهری و معماری با رویکرد پدافند غیرعامل پرداخته است. در پژوهشی دیگر که نتایج آن منجر به تألیف مقاله‌ای تحت عنوان «ارزیابی ساختار شهر لنگرود جهت برنامه ریزی پدافند غیرعامل» گردید، حسینی امینی و همکاران، با توجه به‌موقعیت استراتژیک این شهر، راهکارهایی جهت افزایش پایداری دفاعی شهر متناسب با نیازهای دفاعی- امنیتی آن و ویژگی‌های جغرافیایی شهر لنگرود ارائه کرده‌اند.

اسماعیلی نیز در پایان نامه کارشناسی ارشد خود تحت عنوان «آمایش شهری با رویکرد پدافند غیرعامل (مطالعه موردی: شهر بیرجند)» به بررسی و شناخت عوامل و عناصر شهری آسیب پذیر شهر بیرجند می‌پردازد و در پایان به این نتیجه می‌رسد که تاکنون در طرح‌های شهری تهیه شده در سطح شهر بیرجند، به مقوله پدافند غیرعامل توجهی نشده است و پراکندگی، استتار، اختفا و پوشش از جمله اصول پدافند غیرعامل است که در تهیه طرح‌های شهری و مکان‌یابی کاربری‌های حساس، مهم و حیاتی این شهر می‌بایست مورد توجه قرار گیرد.

در پژوهشی دیگر پریزادی و همکاران به مطالعه «بررسی و تحلیل تمهیدات پدافند غیرعامل در شهر سقز با رویکردی تحلیلی» پرداخته‌اند. جهت انجام بررسی پرسشنامه‌ای بین کارشناسان ادارات و سازمان‌های دولتی و بخش خصوصی توزیع و گردآوری شد. این پژوهش نشان داد که کارشناسان در مواجه با بحران تا حدی آگاه هستند. در کتابی تحت عنوان «الزامات معمارانه در دفاع غیرعامل پایدار» به قلم نظریان، مطرح شد که طراحی معماری دفاعی با رویکرد دفاع غیرعامل در کشور تاکنون بسیار نادیده گرفته شده است و برای رفع این نقص، وی به ارائه رویه‌های علمی طراحی میان رشته‌ای پرداخته است.

پورمحمدی و همکاران، موضوع برنامه‌ریزی متناسب با پدافند غیرعامل را با تأکید بر ارزیابی و برنامه‌ریزی بهینه کاربری اراضی شهری را در وضع موجود شهر سنندج بر اساس داده‌ها و نقشه‌های گردآوری شده مورد سنجش و تحلیل قرار داده است. نتایج این مطالعه حاکی از آن بود که تجمیع تأسیسات و تجهیزات شهری، کاربری نظامی و مسکونی و کاربری‌های خارج از محدوده که در اضلاع شرقی و جنوب شرقی شهر سنندج واقع شده‌اند، این قسمت از شهر را ناسازگار کرده و آن را تبدیل به یک نقطه بحرانی، پهنه مخاطره‌آمیز، محل تجمیع کاربری‌های حساس و استراتژیک کرده است.

زرقانی و رضوی نژاد در پژوهشی دیگر به بررسی «تحلیل ریسک اهمیت مراکز حیاتی، حساس و مهم کلان شهر مشهد با استفاده از مدل *ANP*» با بهره گیری از رویکرد تحلیلی ضمن بررسی مراکز با اهمیت ویژه در کلانشهر مشهد، ارزش ریسکی هر یک از آن‌ها را به روش *ANP* تبیین کردند تا مشخص شود هر کدام از این دارایی‌ها نسبت به یکدیگر دارای چه درجه‌ای از اهمیت هستند.

برنافر و افرادی، به مطالعه «اولویت‌بندی مراکز حیاتی، حساس و مهم بندر انزلی و ارائه راهکارهای دفاعی از دیدگاه پدافند غیرعامل» پرداختند. نتایج این پژوهش حاکی از آن بود که توسعه و ایجاد فضاهای امن در مراکز مهم، ایجاد مراکز مهم متعدد به‌جای مراکز حساس منفرد، کاهش خطر ناشی از کاربری‌های خطرزا و پراکنش مراکز مهم در سطح شهر انزلی راهبردی مؤثر در حفظ امنیت این شهر می‌باشد.

هوشمندسازی و مانیتورینگ اتاق سرور

منبع: www.danapardaz.net

مقدمه

تداوم بسیاری از کسب و کارها به طور مستقیم به دسترس پذیری سرویس‌های *IT* بستگی داشته و هر گونه اختلال در زیر ساخت‌های شبکه موجب توقف کار سازمان و ایجاد زیان‌های سنگین خواهد شد. در اینجا به موضوع مهم مانیتورینگ اتاق سرورها و مراکز داده پرداخته، بایدها و نبایدها و روش‌های مانیتورینگ در این مراکز مورد بررسی قرار می‌گیرد.

چرا در مانیتورینگ اتاق سرور و دیتاسنتر کنترل دما مهم می‌باشد؟

گرما دشمن شماره یک سرورها و تجهیزات شبکه شما است، دشمنی خطرناک که اگر از آن غفلت کنید برای شما کابوس ایجاد می‌کند. سرورها، سوئیچ‌ها، فایروال ها و سایر دستگاه‌هایی که در اتاق سرور و یا دیتاسنتر قرار دارند به طور قابل توجهی گرما تولید می‌کنند، پردازنده این دستگاه‌ها به طور شبانه‌روزی مشغول کار و تولید گرما است، برای همین مانیتورینگ ۲۴ ساعته دما در این مراکز بسیار مهم بوده و شما باید از یک راهکار مانیتورینگ شرایط محیطی پیشرفته و قابل اعتماد برای این موضوع استفاده کنید.

سرورها و تجهیزات شبکه فقط تا سطح مشخصی از دما، می‌توانند بکار خود ادامه دهند. بالا بودن دما، بخصوص اگر به صورت همیشگی باشد می‌تواند موجب سوختن یک تراشه و یا فرسایش خیلی سریع این دستگاه‌ها شود. تعویض *CPU* یک سرور به طور حتم کار جذابی نیست، از آن بدتر اینکه بخواهید یک سرور را به طور کامل تعویض یا تعمیر کنید، برای همین باید قبل از اینکه کار به آنجا بکشد و بخواهید به تعداد زیادی از مدیران و مشتری‌ها پاسخگو باشید، به فکر یک راهکار نظارت بر شرایط محیطی باشید.

استفاده از یک سیستم مانیتورینگ شرایط محیطی که حسگرهای آن در مکان‌های درستی از اتاق سرور یا دیتاسنتر نصب شده باشند، موجب می‌شود که مدیران دیتاسنتر یا مدیران شبکه همیشه وضعیت دما و رطوبت و سایر پارامترهای محیطی مهم را زیر نظر داشته باشند و بصورت بلادرنگ از تغییرات دما آگاهی پیدا کنند تا در صورت نیاز اقدامات لازم را در سریع‌ترین زمان لازم انجام دهند. در واقع سیستم مانیتورینگ اتاق سرور به مدیر شبکه این اطمینان را می‌دهد که همیشه همه شرایط تحت کنترل بوده و نظارتی دائمی بر این منابع حیات بخش سازمان وجود دارد.

اگر دما در اتاق سرور و دیتاسنتر بالا رود چه اتفاقی می

افتد؟

بالا رفتن دما در اتاق سرور یا مراکز داده، باعث می شود سرورها و دستگاه‌ها برای پایین آوردن دما به فن پردازشگر خود دستور دهند که با سرعت بسیار بالایی کار کند، اما این کار هم فقط تا حد مشخصی می‌تواند مؤثر باشد و پس از مدت کوتاهی دما آن قدر بالا می رود که سرورها به صورت خودکار خاموش می‌شوند. وقتی دمای اطراف *CPU* به حدود ۳۵ درجه سلسیوس برسد و برای چند دقیقه در این دما کار کند، ریسک خرابی آن به طور قابل توجهی افزایش پیدا می‌کند، در چنین شرایطی حتی اگر شما *CPU* را جابجا کنید و مشکل گرما را برطرف کنید، باز هم ممکن است بعد از مدتی با مشکلات دیگری که ناشی از صدمه‌های کوچک ذوب شدگی اجزا کوچک بوردهای سیستم باشد مواجه شوید.

خاموش شدن خودکار، مکانیسم ساده‌ای برای جلوگیری از خرابی تراشه‌ها است که توسط تولیدکنندگان سرور ها پیش‌بینی شده است ولی خاموشی هم یعنی از کار افتادگی و از کار افتادگی هم یعنی از بین رفتن هزینه و اعتبار. سیستم مانیتورینگ اتاق سرور سرمایه‌گذاری مطمئنی است که برای جلوگیری از ضرر و زیان‌های جبران ناپذیر باید انجام دهیم. از نشانه‌های دیگر دمای بالا، خطاهای پر تکرار حافظه (*Memory Errors*) و هنگ کردن عجیب برنامه‌های کاربردی و سیستم عامل می‌باشد بطوریکه استفاده از سیستم را با اختلال روبرو می‌کند.

ارتباط دمای اتاق سرور و هزینه برق

مصرف برق در اتاق سرورها و دیتاسنترها خیلی زیادتر از آن چیزی است که احتمالاً تصورش را می‌کنید. خوب است که بدانید یک دیتاسنتر با اندازه متوسط، حدود ۱۰۰ برابر یک ساختمان بزرگ اداری و تجاری برق مصرف می‌کند، همچنین مصرف برق در یک مرکز داده بزرگ، با مصرف برق یک شهرستان کوچیک برابری می‌کند! شاید باورتان نشود که دیتاسنترها حدود ۳% از کل برق ایالات متحده آمریکا را مصرف می‌کنند و تحقیقات ثابت کرده برخی تغییرات مثل مانیتورینگ صحیح دما به طور قابل توجهی موجب کاهش انرژی می‌شود. یکی از مهم‌ترین دلایل هوشمندسازی اتاق سرور هم مدیریت هزینه‌ها و بهینه‌سازی مصرف برق در دیتاسنترها است. در دیتاسنترها بیشترین انرژی صرف جلوگیری از گرم

دیتاسنتر زیرآبی شرکت مایکروسافت

به همین خاطر شرکت‌های غول‌پیکر فناوری مثل گوگل، آمازون و مایکروسافت سرمایه‌گذاری خیلی زیادی برای حرکت به سمت انرژی‌های سبز کرده‌اند، مثلاً مایکروسافت پروژه خلاقانه و البته جسورانه‌ای برای دیتاسنترهای زیرآبی دارد و فازهای اولیه آزمایش آن را در سواحل اسکاتلند با موفقیت پشت سر گذاشته است. یکی از تلاش‌های مهم دیگری که برای کاهش هزینه انرژی در مراکز داده و هوشمندسازی اتاق سرور توسط تولیدکنندگان بزرگ سرور در جریان است و هدف آن تغییر طراحی پردازشگرها برای عملکرد بهینه در دمای بالاتر است. مطالعاتی که توسط *Intel* و *Microsoft* انجام شده نشان می‌دهد که بیشتر سرورها می‌توانند در دماهایی بالاتر از محیط بکار خود ادامه دهند و این موجب کاهش ترس از خرابی سرورها شده است. همچنین شرکت *Dell* به تازگی اعلام کرده که سرورهای خود را برای کار کردن تا دمای ۴۵ درجه سانتیگراد ضمانت می‌کند.

میزان دمای مناسب اتاق سرور چقدر است؟

دمای مناسب اتاق سرور ۱۸ الی ۲۷ درجه سلسیوس است. البته نباید این موضوع را نادیده گرفت که میزان دما در مکان‌های مختلف محیط دیتاسنتر یا اتاق سرور با هم متفاوت است و قرار دادن حسگرهای دما در نقاط مناسب بسیار اهمیت دارد. در واقع مانیتورینگ اتاق سرور باید به صورت اصولی و مهندسی شده انجام شود.

میزان رطوبت مناسب اتاق سرور چقدر است؟

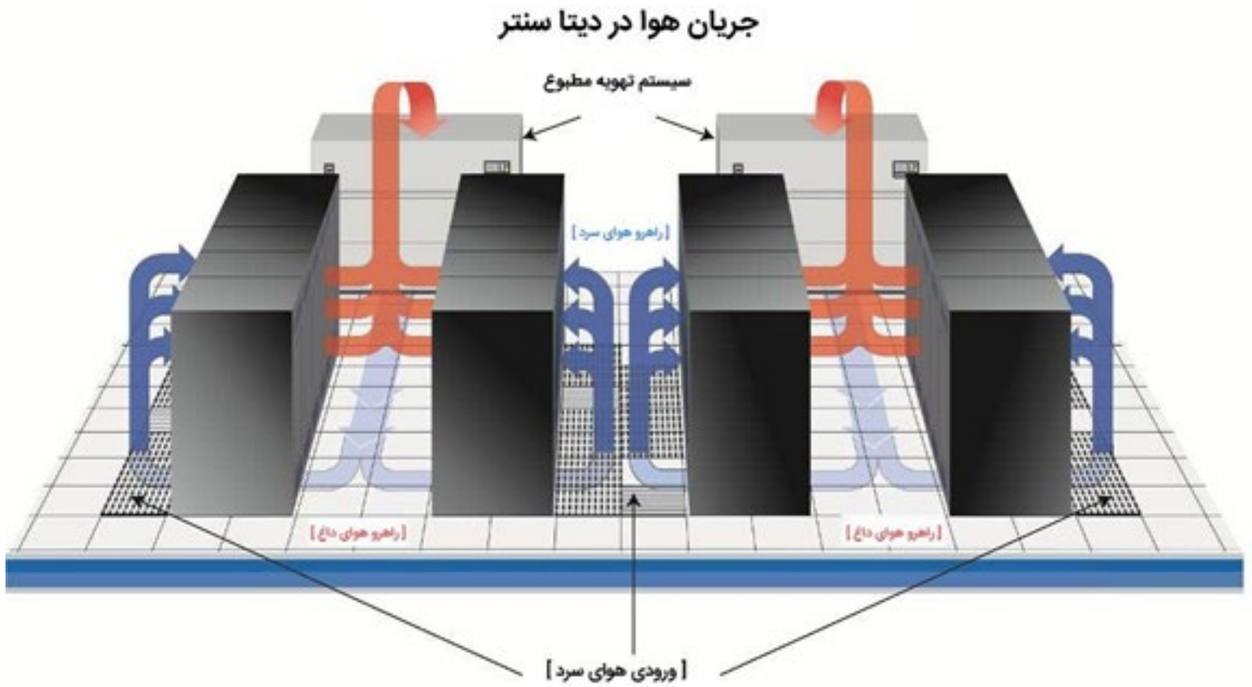
رطوبت، میزان بخار موجود در هوا است که به دو صورت رطوبت مطلق و رطوبت نسبی اندازه‌گیری می‌شود. در خصوص مانیتورینگ شرایط محیطی اتاق سرور ما باید رطوبت نسبی را اندازه گیری کنیم.

اول بیایید تعریف رطوبت نسبی را یک‌بار با هم مرور کنیم؛ «رطوبت نسبی یعنی میزان ذرات آب معلق در هوا (با دمای مشخص) نسبت به حداکثر ذرات آبی که هوا در همان دما می‌تواند داشته باشد، به زبان ساده‌تر نسبت رطوبت هوا نسبت به رطوبت اشباع.» در اتاق سرورها و مراکز داده نگهداری رطوبت نسبی بین ۴۵٪ تا ۵۵٪ برای کارکرد بهینه و قابل اعتماد سرورها و تجهیزات شبکه پیشنهاد می‌شود.

اهمیت طراحی جریان هوا در اتاق سرور

طراحی اتاق سرور و چیدمان رک‌ها و تجهیزات، نقش مهمی در رابطه با کنترل دما و رطوبت دارد. اینکه اتاق سرور از ابتدا برای این منظور ساخته شده باشد و یا بر اساس نیاز، یکی از اتاق‌های موجود را به عنوان اتاق سرور در نظر گرفته باشید در اصل ماجرا تغییری ایجاد نمی‌کند و شما باید حتماً به طراحی صحیح جریان هوا (*Airflow*) توجه کنید.

در طراحی اتاق سرور باید حتماً توجه داشته باشید که راهروهای هوای سرد و گرم از هم جدا باشد. مراقب باشید که هوای گرم خروجی از یک دستگاه به یک ورودی هوای یک دستگاه دیگر وارد نشود. مانیتورینگ جریان هوا همچنین شما را از خرابی دستگاه‌های تهویه باخبر می‌کند.



در چیدمان رک‌ها و طراحی راهروها توجه کنید که همیشه رک‌ها روبروی هم باشند و هیچ وقت قسمت جلویی یک رک رو به پشت رک دیگری نباشد تا هوای سرد و گرم در یک راهرو قرار نگیرند.

چه تعداد سنسور دما و در چه نقاطی از اتاق سرور نیاز داریم؟

یکی از اشتباهاتی که معمولاً در مانیتورینگ دمای اتاق سرور رخ می‌دهد این است که دما را فقط در سطح اتاق اندازه گیری می‌کنند. انجمن گرمایش، سرمایش و تهویه مطبوع امریکا (*ASHRAE*)، پیشنهاد می‌کند که برای هر رک از ٦ سنسور دما استفاده کنید و این سنسورها را به قسمت پایین، وسط و بالای رک در جلو و پشت رک نصب کنید.

البته موسسه گارتنر (*Gartner*)، اظهار می‌کند که استفاده از ۳ سنسور دما برای هر رک کفایت می‌کند:

۱) اولین سنسور در قسمت پایین جلوی رک نصب شود برای اندازه گیری دمای هوای سرد ورودی به رک.

۲) سنسور دوم در قسمت بالای جلوی رک نصب شود برای اینکه بدانیم آیا هوای سرد به قسمت‌های فوقانی رک هم می‌رسد یا خیر.

۳) سنسور سوم هم باید به قسمت بالای پشت رک نصب شود که داغ ترین نقطه است.

در مانیتورینگ اتاق سرور علاوه بر دما و رطوبت چه پارامترهای دیگری را باید در نظر بگیریم؟

دما و رطوبت تنها شاخص‌هایی نیستند که باید زیر نظر داشته باشید، برای داشتن یک اتاق سرور ایمن با راندمان بالا شما باید پارامترهای دیگری را هم در سیستم کنترل و مانیتورینگ اتاق سرور زیر نظر بگیرید.

نَشت آب

به طور معمول نَشت آب تهدیدی است که کمتر مورد توجه قرار می‌گیرد، غافل از اینکه صدمات سنگینی می تواند به جا بگذارد. با وجود اینکه بیشتر اتاق سرورها و مراکز داده از کف‌های کاذب استفاده می‌کنند و آب هم همیشه به دنبال پایین‌ترین نقاط است، این تهدید خیلی بیشتر هم شده است. وجود آب در اتاق سرور یا مرکز داده به سادگی قابل تشخیص نیست. برای مثال ممکن است دستگاه تهویه دچار اشکال شده و نشت آب از آن وارد کف کاذب شده باشد و شما آن را نبینید، تا زمانی که دیگر دیر شده باشد. بنابراین بکارگیری سنسورهای نشت آب از اهمیت بسیار بالایی برخوردار است.

در اتاق سرورها و دیتاسنترها، نشت آب معمولاً از سه منبع می‌تواند اتفاق بیافتد:

- دستگاه‌های تهویه و کولرها: این دستگاه‌ها بیشترین احتمال نشت آب را دارند و خرابی و فرسودگی آن‌ها می تواند موجب ایجاد سیلاب در اتاق سرور شود! شما باید حتماً زیر هر یک از این دستگاه‌ها یک سنسور نشت آب قرار دهید.
- سقف و کف اتاق: ممکن است به دلیل بارندگی و یا ترکیدگی لوله‌ها، نشت آب اتفاق بیافتد، به همین دلیل بایستی در محیط اطراف اتاق و در پایین‌ترین نقاط چند سنسور نشت آب نصب کنید.
- پنجره‌ها: اگر اتاق سرور شما پنجره داشته باشد، در مواقعی که باران می‌بارد و پنجره به درستی عایق نشده باشد ممکن است آب به داخل نشت کند، پس باید زیر هر یک از پنجره‌ها حتما یک سنسور نشت آب نصب کنید.

ادامه دارد ...

آسیب‌پذیری

اکثر توزیع‌های Linux تحت تأثیر آسیب‌پذیری polkit

محققان از شناسایی ضعفی در *polkit* خبر داده‌اند که سوءاستفاده از آن، مهاجم با دسترسی محدود را قادر به دستیابی به سطح دسترسی *root* می‌کند.

سرویس اصالت‌سنجی *polkit* به‌صورت پیش‌فرض بر روی بسیاری از توزیع‌های اخیر *Linux* نصب شده است. باگ مذکور با شناسه *CVE*-۲۰۲۱-۳۵۶۰ در دسته آسیب‌پذیری‌های *Local Privilege Escalation* قرار می‌گیرد.

وصله این آسیب‌پذیری در دسترس قرار گرفته است. گفته می‌شود تمامی نسخ *polkit* که در ۷ سال اخیر (از نسخه ۰,۱۱۳) منتشر شده‌اند به *CVE*-۲۰۲۱-۳۵۶۰ آسیب‌پذیر هستند.

اگرچه بسیاری از توزیع‌های *Linux* اخیراً فاقد نسخ آسیب‌پذیر *polkit* بوده‌اند اما درهرصورت هر توزیع که در آن نسخه ۰,۱۱۳ یا نسخ بعد از آن لحاظ شده است، آسیب‌پذیر تلقی می‌شود. متأسفانه سوءاستفاده از آسیب‌پذیری مذکور بسیار آسان بوده و با اجرای چند فرمان و بکارگیری ابزارهای معمول و شناخته شده‌ای همچون *kill*، *bash* و *dbus-send* می‌توان از آن استفاده کرد.

باتوجه به سهولت در سوءاستفاده از این آسیب‌پذیری و انتشار عمومی جزئیات آن، به‌روزرسانی نسخ مورداستفاده Linux به نسخ وصله‌زده، دراسرع‌وقت توصیه می‌شود.

چند ماه قبل نیز مهاجمان یک آسیب‌پذیری ۱۵ ساله را در *iSCSI* هسته *Linux* شناسایی کردند که تمامی توزیع‌ها را متأثر می‌کرد. هرچند ماژول آسیب‌پذیر مذکور به‌صورت پیش‌فرض فعال نیست اما فراخوانی آن توسط مهاجم در برخی سناریوها قابل تصور است. سوءاستفاده از این آسیب‌پذیری نیز مهاجم را قادر به دستیابی به سطح دسترسی *root* می‌کند.

هک دستگاه‌های VPN Pulse Secure

محققان امنیت سایبری در تیم امنیتی *FireEye's Mandiant* اخیراً نسخه جدیدی از بدافزار را شناسایی کرده‌اند که دستگاه‌های *VPN Pulse Secure* را هدف قرار می‌دهد.

این دستگاه‌ها و راه‌حل‌های ارائه شده توسط شبکه خصوصی مجازی *Pulse Secure (VPN)* توسط چندین سازمان به طور گسترده استفاده می‌شود تا شبکه‌ها و سیستم‌های *IT* داخلی خود را از حملات سایبری ایمن نگه دارند. تیم امنیتی *FireEye's Mandiant* تأیید کرد که حملات سایبری که با بهره‌برداری از آسیب‌پذیری‌ها علیه چندین سازمان در ایالات متحده و اروپا انجام می‌شد، توسط هکرهای *APT* چینی اجرا شده بود. آسیب‌پذیری‌هایی که توسط هکرها مورد سوءاستفاده قرار می‌گیرد در زیر ذکر شده است:

- *CVE*-۲۰۲۱-۲۲۸۹۳ (اصلی)، *CVE*-۲۰۱۹-۱۱۵۱۰ (متصل به حملات)
- *CVE*-۲۰۲۰-۸۲۶۰، *CVE*-۲۰۲۰-۸۲۴۳ (متصل به حملات)

در میان این نقص‌های امنیتی، *CVE*-۲۰۲۱-۲۲۸۹۳ اصلی‌ترین مورد است و هکرها به شدت از این نقص امنیتی سوءاستفاده می‌کنند. تحلیلگران امنیتی این آسیب‌پذیری را بحرانی تشخیص داده و نمره شدت *CVSS* را ۱۰ اختصاص داده‌اند.

این آسیب‌پذیری *Pulse Connect Secure* را تشدید می‌کند و به هر مهاجم غیرمجاز اجازه می‌دهد تا کد دلخواه را بر روی سیستم آسیب‌دیده از راه دور اجرا کند. کارشناسان فارنزیک *Madiant* برخی از توصیه‌ها را برای اصلاح یک دستگاه آسیب‌دیده *Pulse Secure* پیشنهاد کرده‌اند که در زیر ذکر شده است:

- تمام رمزهای عبور را *Reset* کنید.
- ابزار *Pulse Integrity Checker* را اجرا کنید.
- در صورت تشخیص اینکه دستگاه *Pulse Secure* قبلاً به خطر افتاده است، باید احتیاط لازم را کرد.
- به جدیدترین نسخه نرم‌افزار ارتقا دهید.
- برای نظارت بر فعالیت‌های غیرمعمول، لاگ‌های مربوط را مرور کنید.
- به‌جای رابط وب، کاربران باید به کنسول دستگاه ارتقا یابند تا اطمینان حاصل شود که هیچ منطق مخربی در یک دستگاه سالم جایگزین نمی‌شود.
- ورود ایمن را فعال کنید.

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

به‌روزرسانی‌هایی به منظور وصله آسیب‌پذیری‌های موجود در محصولات *SAP* منتشر شد؛ ۲ مورد از این آسیب‌پذیری‌ها، دارای شدت بحرانی و سایر موارد دارای شدت بالا و متوسط هستند. مهمترین آسیب‌پذیری وصله شده، آسیب‌پذیری *CVE*-۲۰۲۱-۲۷۶۰۲ است که دارای شدت ۹,۹ از ۱۰ است و بهره‌برداری موفقیت‌آمیز از این آسیب‌پذیری منجر به اجرای کد از راه دور شده و به مهاجم امکان می‌دهد محرمانگی، صحت و دسترس پذیری برنامه را به خطر بیاندازد. توصیه می‌شود هرچه سریع‌تر وصله‌های امنیتی منتشر شده در سیستم‌های آسیب‌پذیر اعمال گردد. همچنین تنظیم مجوزهای دسترسی و محدود کردن دسترسی کاربران جهت کاهش مخاطرات این آسیب‌پذیری ضروری است.

شرکت مایکروسافت، در مجموعه اصلاحیه‌های امنیتی در مجموع ۵۰ آسیب‌پذیری Windows و دیگر محصولات مختلف این شرکت را ترمیم می‌کنند. درجه اهمیت ۵ مورد از این آسیب‌پذیری‌ها «حیاتی» و ۴۵ مورد «مهم» اعلام شده است. از میان ۵۰ آسیب‌پذیری اعلام شده مایکروسافت، ۷ آسیب‌پذیری ترمیم شده از نوع روز- صفر هستند که از حداقل ۶ مورد آن‌ها، از مدتی قبل مهاجمان سوءاستفاده کرده‌اند؛ لذا اعمال فوری به‌روزرسانی‌ها و وصله‌های امنیتی مربوط اکیداً توصیه می‌شود.

گروه *PuzzleMaker*، در جریان حملاتی کاملاً هدفمند، ابتدا از یک ضعف امنیتی روز- صفر در *Chrome* در زنجیره *Exploit* بهره گرفته و در ادامه با ترکیب دو آسیب‌پذیری مذکور سطح دسترسی خود را در *Windows* ارتقا داده است. در نهایت نیز مهاجمان با ایجاد یک *Remote Shell* بر روی آن، امکان آپلود و دانلود فایل‌ها و اجرای فرمان‌ها را برای خود فراهم می‌کرده‌اند.

شرکت *Adobe* به‌روزرسانی‌هایی را به منظور وصله آسیب‌پذیری در محصولات خود منتشر کرده است. آسیب‌پذیری *Path Traversal* (*CVE*-۲۰۲۱-۲۸۵۸۸) با شدت بالای ۸,۸ از ۱۰ در *Adobe RoboHelp Server* وجود دارد که بهره‌برداری موفقیت‌آمیز از آن به مهاجم امکان اجرای کد از راه دور را خواهد داد. این آسیب‌پذیری نسخه‌های ۲۰۱۹,۰,۹ به قبل از *Adobe RoboHelp Server* را تحت تأثیر خود قرار می‌دهد. هیچ‌گونه روشی جهت کاهش مخاطرات این آسیب‌پذیری منتشر نشده است؛ بنابراین به‌روزرسانی این محصول به نسخه ۲۰۲۰,۰,۱ توصیه می‌گردد. آسیب‌پذیری *CVE*-۲۰۲۱-۲۸۵۸۲ با شدت ۸,۸ از ۱۰ محصولات ۲۰۲۰ *Adobe Photoshop* نسخه ۲۱,۲,۸ به قبل و ۲۰۲۱ *Adobe Photoshop* نسخه ۲۲,۴,۱ به قبل را تحت تأثیر خود قرار داده و بهره‌برداری موفقیت‌آمیز از آن به مهاجم امکان اجرای کد از راه دور را خواهد داد. اعمال وصله‌های منتشر شده این آسیب‌پذیری را رفع می‌کند.

شرکت سیسکو اخیراً به منظور وصله آسیب‌پذیری‌های موجود در محصولات خود به‌روزرسانی‌هایی را منتشر نموده است؛ محصولات *Cisco ASR ۵۰۰۰ Series Software*، *Cisco Webex Network Recording Player*، *Cisco Webex Player*، Cisco SD-WAN Software دارای آسیب‌پذیری با شدت بالا می‌باشند. با توجه به اینکه هیچ‌گونه روش موقتی جهت کاهش مخاطرات آسیب‌پذیری‌های مذکور منتشر نشده است. توصیه می‌شود در اسرع وقت نسبت به به‌روزرسانی سیستم‌های آسیب‌پذیر اقدام شود. یک مورد از محصولات سیسکو دارای آسیب‌پذیری با شدت بالا ۸,۱ از ۱۰ و سایر موارد دارای شدت ۷,۸ هستند. بهره‌برداری موفقیت‌آمیز از این آسیب‌پذیری‌ها منجر به اجرای کد از راه دور بر روی دستگاه‌های آسیب‌پذیر، ارتقای سطح دسترسی و بی‌اثر کردن ساز و کارهای احراز هویت خواهد شد.

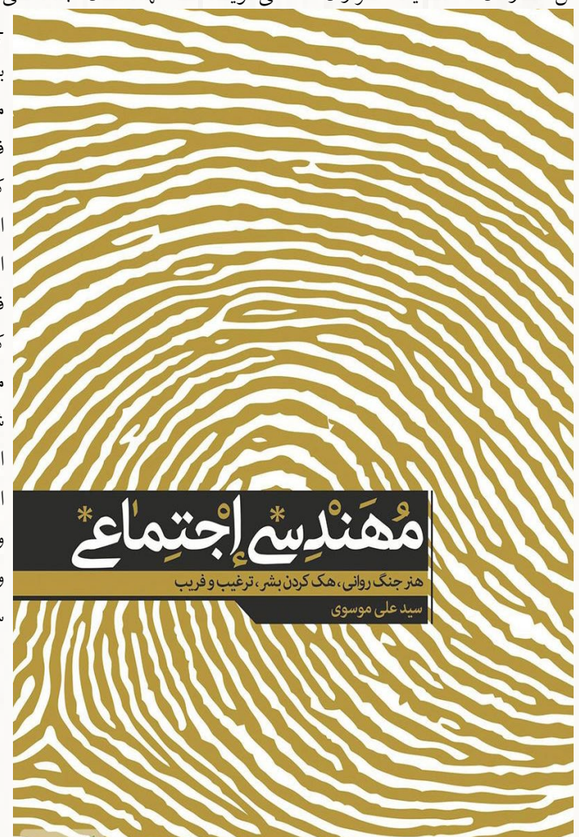
شرکت *VMware* به‌روزرسانی‌هایی را به منظور وصله دو آسیب‌پذیری *CVE*-۲۰۲۱-۲۱۹۸۵ و *CVE*-۲۰۲۱-۲۱۹۸۶ در محصولات خود منتشر کرده است. توصیه می‌شود هرچه سریع‌تر نسبت به به‌روزرسانی محصولات آسیب‌پذیر اقدام شود.

وجود چندین آسیب‌پذیری در سرویس‌دهنده *Oracle* که به مهاجم احراز هویت‌نشده این امکان را می‌دهد تا با دسترسی به شبکه قربانی از این آسیب‌پذیری‌ها سوءاستفاده نماید. بهره‌برداری موفق از این آسیب‌پذیری ها به مهاجم این امکان را می‌دهد تا کنترل سرویس دهنده *WebLogic* را در دست گرفته و به اطلاعات موجود در سرویس‌دهنده دسترسی کامل داشته باشد. دسترسی مهاجم به شبکه قربانی می‌تواند از طریق سه پروتکل ارتباطی *IIOP*، *http*، *T۳* صورت پذیرد.

معرفی کتاب
حوزه پدافند مردم محور

کتاب مهندسی اجتماعی: هنر جنگ روانی، هک کردن بشر، ترغیب و فریب نوشتهٔ سیدعلی موسوی، به بررسی ابعاد و زوایای مختلف مهندسی اجتماعی در تمامی عرصه‌ها به ویژه علوم نظامی می‌پردازد و راهکارهایی را برای جلوگیری از سوءاستفاده سود جویان ارائه می‌کند. مهندسان اجتماعی معمولاً از روش دنباله‌روی در سازمان‌های کوچک یا کمپانی‌های بزرگی که از کارمندانشان کارت ورود می‌خواهند، استفاده می‌کنند. در هر حال، مهاجمین معمولاً در کمپانی‌های کوچک و متوسط است که می‌توانند با افراد حراست گرم بگیرند و به‌نوعی راه خودشان را به درون سازمان بیابند.

مشخصاً حملات مهندسان اجتماعی پراکنده بوده و به عنوان یک تهدید بزرگ برای سازمان‌های مختلف محسوب می‌شود. مهندسان اجتماعی می‌توانند با دسترسی به اطلاعات حساس سازمان‌ها، سالیانه هزاران یا حتی میلیون‌ها دلار ضرر را به آن‌ها وارد کنند. امروزه اکثر مهاجمین از تاکتیک‌های گوناگون شبکه‌های اجتماعی استفاده می‌کنند تا بتوانند به اطلاعات شخصی و حرفه‌ای اهدافشان دست پیدا کنند. معمولاً کارمندان جدید هستند که بیشتر تحت آسیب مهندسان اجتماعی قرار می‌گیرند و پس از آن پیمانکاران، کارکنان منابع انسانی، دستیاران اجرایی، پرسنل *IT* و رهبران کسب و کار در رده‌های بعدی جای می‌گیرند. متأسفانه تعدادی از سازمان‌ها از طرح‌های بازدارنده و آگاهی‌بخش لازم در زمینهٔ مقابله با مهندسی اجتماعی بهره نمی‌برند. همچنین سازمان‌هایی هستند که سیاست‌های امنیتی یا آموزش تاکتیک‌های بازدارنده در برابر مهندسی اجتماعی را ندارند.



این کتاب اطلاعات ارزشمندی را در زمینهٔ مهندسی اجتماعی ارائه می‌کند. در فصل اول، شما دربارهٔ ماهیت مهندسی اجتماعی و خواسته‌های مهندسان در کنار تاکتیک‌های گوناگون مورد استفاده توسط آن‌ها خواهید آموخت.

فصل دوم از این کتاب اطلاعات مرتبط در زمینهٔ تاکتیک‌های روان‌شناسی را ارائه می‌کند که معمولاً مهاجمین از آن‌ها برای اجرای طرح‌های مهندسی اجتماعی خود بهره می‌گیرند. در فصل سوم با ابزارهای مورد استفادهٔ این مهندسان آشنا می‌شوید. فصل چهارم به شما می‌گوید که مهندسان اجتماعی برای شروع کار خود از چه دیالوگ‌هایی برای برقراری ارتباط استفاده می‌کنند.

فصل پنجم به مقایسه کلاهبرداری‌های مهندسان اجتماعی در گذشته و امروز می‌پردازد و در فصل ششم می‌آموزید که چگونه تا حدودی مانع از کار این مهندسان شوید.

این کتاب برای تمامی افراد به‌خصوص مدیران و رئیسان سازمان‌ها و کارکنان آنان بسیار سومند و مفید است.

طرح‌های کسر خدمت سربازی

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

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

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

سایت های مرتبط با پدافند غیرعامل

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

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

استانداری آذربایجان شرقی – پدافند غیرعامل
http://www.ostan-as.gov.ir/Page/۴۲/

پلیس فتا
http://www.cyberpolice.ir

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