ماهنامه اداره کل پدافند غیر عامل
شماره ۳۷/ مهر ماه ۱۳۹۸

ماهنامه دیجیتالی پدافند غیرعامل

معاون سیاسی، امنیتی و اجتماعی استانداری آذربایجان شرقی:
خواستار رصد و شناسایی مستمر آسیب‌ها و تهدیدات حوزه‌های مختلف استانداری و رفع موانع موجود در این زمینه شد

مدیرکل پدافند غیر عامل:
آموزش، اطلاع‌رسانی و فرهنگ‌سازی را اولویت اول پدافند غیرعامل دانست

در این شماره می‌خوانید:

کشف آسیب‌پذیری روز صفر جدید در نسخه‌های قدیمی جوملا

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

آسیب‌پذیری بحرانی اجرای کد از راه دور در مسیریاب‌های D-LINK

استراق سمع

آمازون و گوگل از کاربران توسط بلندگوهای صوتی


بسم الله الرحمن الرحیم

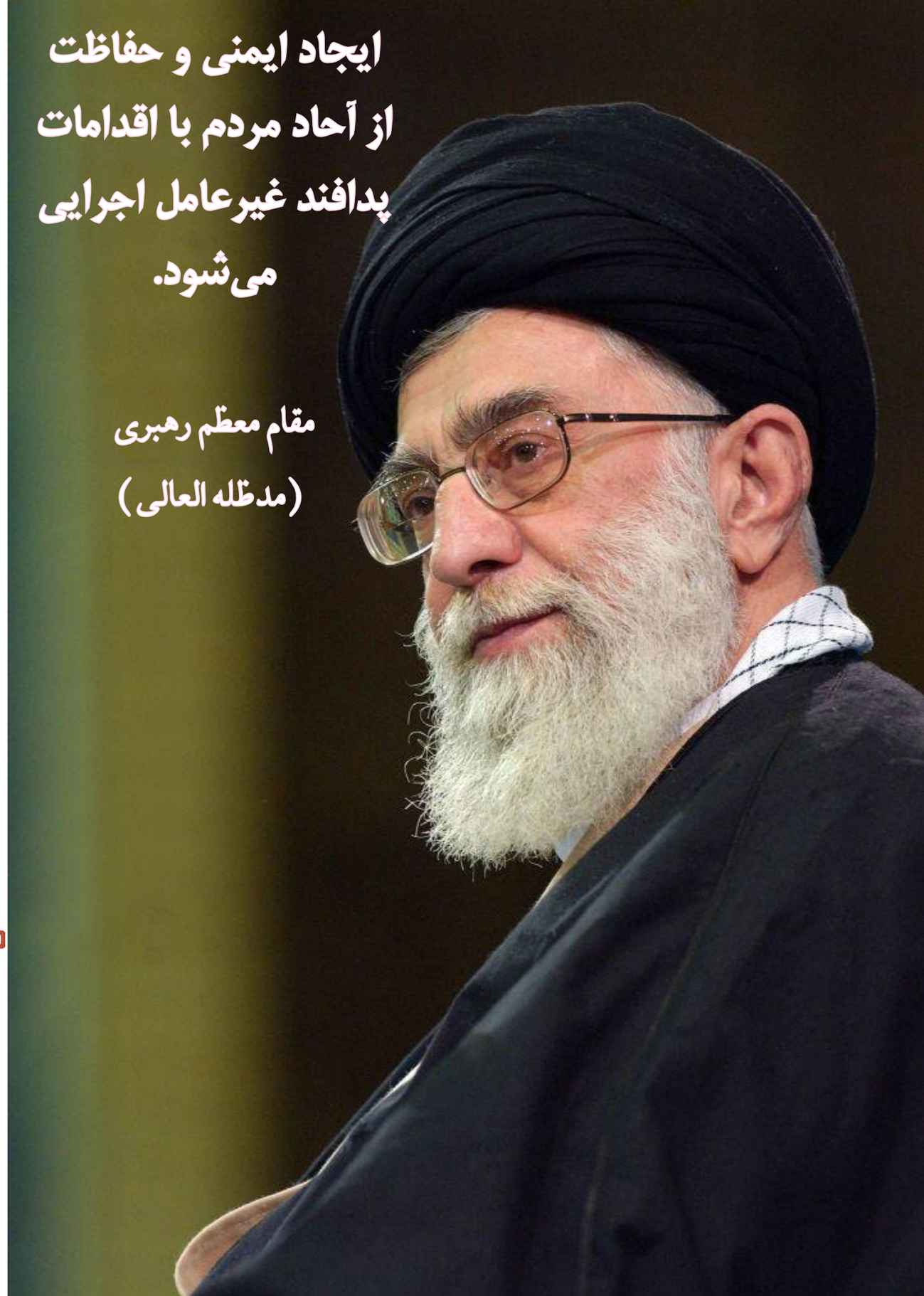
مدیر مسئول:
محمد باقر آقایی

سردبیر:
لیدا رسول اهری

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

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



دومین دوره آموزش عمومی، تخصصی و تربیت مربی پدافند غیرعامل

محمدباقر آقایی در دومین دوره آموزش عمومی، تخصصی و تربیت مربی ویژه مدیران، معاونان و کارشناسان سازمان‌ها و دستگاه‌های اجرایی آذربایجان شرقی، آموزش، اطلاع‌رسانی و فرهنگ‌سازی را اولویت اول پدافند غیرعامل دانست و افزود: هدف از برگزاری این دوره‌های آموزشی نیز نیل به این اهداف است.

وی با بیان اینکه پدافند غیرعامل مکمل پدافند عامل است، اظهار داشت: رزمندگان اسلام در دوران هشت سال دفاع مقدس با توکل به خداوند، رهبری امام خمینی(ره) و حضور مردم با کمترین امکانات در برابر تهدیدات و حملات دشمن بعثی تحت حمایت استکبار جهانی، شرکت کرده و شجاعانه ایستادگی کردند.

آقایی به نامگذاری ۸ تا ۱۴ آبان ماه تحت عنوان هفته پدافند غیرعامل اشاره کرد و افزود: حضور مربیان آموزش دیده در این دوره‌ها جهت آموزش دانش‌آموزان در محورهای آموزشی، فرهنگ‌سازی و گفتمان‌شناسی در خصوص پدافند غیرعامل به عنوان یک ضرورت اجتناب‌ناپذیر و نقطه شروعی برای انتقال این مفاهیم به خانواده‌ها و آحاد مردم جامعه می‌باشد.

این دوره آموزشی در راستای نیازها، ضرورت‌ها و سیاست‌های نظام مقدس جمهوری اسلامی در حوزه پدافند غیرعامل و با هدف آموزش و ارتقای سطح دانش و مهارت مدیران دستگاه‌های اجرایی در بخش‌های عمومی، تخصصی و تربیت مربی برگزار می‌شود.

اساتید دانشکده مهندسی و پدافند غیرعامل دانشگاه جامع امام حسین (ع) در این دوره آموزشی مباحث مربوط به اصول و مبانی پدافند غیرعامل و مباحث تخصصی در حوزه‌های پدافند سایبری، زیستی، شیمیایی و پرتویی، کالبدی، مکان‌یابی، مردم محور و فرهنگی، اقتصادی، سناریونویسی و مدیریت بحران را ارائه می‌کنند.

دومین جلسه کمیته پدافند غیرعامل استانداری

معاون سیاسی، امنیتی و اجتماعی استانداری آذربایجان شرقی در دومین جلسه کمیته پدافند غیرعامل استانداری، خواستار رصد و شناسایی مستمر آسیب‌ها و تهدیدات حوزه‌های مختلف استانداری و رفع موانع موجود در این زمینه شد.

علیار راستگو در این جلسه با اشاره به انتخابات پیش رو، لزوم آماده‌سازی زیرساخت‌های سایبری لازم و توجه جدی به امنیت سایبری استانداری بخصوص سیستم انتخابات را مورد تأکید قرار داد.

محمدباقر آقایی، مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی نیز ضمن ارائه گزارشی از اقدامات انجام یافته در راستای پدافند غیرعامل در استانداری، بر لزوم همکاری و همراهی کلیه واحدهای استانداری در پیشبرد و به ثمر رسیدن طرح‌های در حال اجرا در حوزه‌های سایبری، زیستی و کالبدی تأکید کرد.

اعضای این کمیته پس از این جلسه از روند پیشرفت اجرای طرح تجهیز و استانداردسازی مرکز داده جدید استانداری بازدید کردند.

برپایی غرفه اداره کل پدافند غیرعامل در نمایشگاه «سلامت روان» در دانشگاه تبریز

پنجمین نمایشگاه سلامت روان تحت عنوان «تلنگر» با محوریت آشنایی و پیشگیری از آسیب‌های اجتماعی برای پنجمین سال متوالی در دانشگاه تبریز گشایش یافت.

اداره کل پدافند غیرعامل با برپایی غرفه در نمایشگاه سلامت روان در دانشگاه تبریز به تبیین مفاهیم پدافند غیرعامل در بین دانشجویان این دانشگاه پرداخت.

این نمایشگاه به منظور آشنایی دانشجویان با آسیب‌های اجتماعی و با محوریت بررسی راهکارهای پیشگیری از این آسیب‌ها برگزار شد.

این نمایشگاه از ۱۳ الی ۱۷ مهر ماه در ۱۶ غرفه در قالب بروشور، کتاب، پوستر، عکس، سی دی، نمایش فیلم، تالار گفتگو، تست پزشکی و ... برای بازدید علاقمندان دایر شد که بازدیدکنندگان در این نمایشگاه ضمن آشنایی با برخی آسیب‌های اجتماعی، آگاهی‌های لازم در مورد پدافند غیرعامل را کسب کردند.

برنامه ریزی پدافند و الزامات محیط شناسی در منطقهٔ شهری

تهیه و تنظیم: اداره کل پدافند غیر عامل
منبع: خلاصه کتاب پدافند غیرعامل (استراتژی‌های توسعه و امنیت منطقه شهری) نوشته دکتر محمدرضا پورمحمدی و کیومرث ملکی

۱- مقدمه:

با توجه به نقش و اهمیت منطقهٔ شهری و به ویژه شهرها به عنوان مکان و کانون تمرکز جمعیت، سرمایه، ساخت و ساز و ... در هر کشور و هر منطقه‌ای، شهرها نقش اصلی را در حیات سیاسی، اقتصادی، اجتماعی، فرهنگی آن‌ها ایفا می‌کنند. بنابراین توجه ویژه به حمایت و حفظ شهرها در مقابل این بحران‌ها از ضروریات اصلی برنامه ریزی در سطوح مختلف مدیریتی هر کشوری است. در این میان آنچه نقش اصلی را در تحقق این هدف مهم بر عهده دارد برنامه‌ریزی درست و اصولی در سطح شهر و منطقهٔ شهری با توجه به سنجش خطرپذیری و مسئلهٔ حفاظت از پدیده‌ها و تأسیسات و تجهیزات شهری و دفاع از شهروندان در مقابل حمله در زمان جنگ، زلزله و ... در منطقهٔ شهری است.

۲- پدافند غیرعامل و آمایش

آمایش و مباحث دفاعی:

آمایش سرزمین را مهندسی ترتیبات بهره‌وری بهینه از ظرفیت‌های اجتماعی و طبیعی تعبیر کرده‌اند. ساماندهی نظامی اسکان جمعیت و سطح بندی مراکز شهری و نواحی روستایی بر اساس توضیح فعالیت‌ها و امکانات در پهنهٔ سرزمین، صرفاً در فرایند برنامه ریزی آمایش سرزمین قابل حصول است. آمایش سرزمین نقش عمده ای در تعیین نوع استفاده از منابع طبیعی سرزمین در آینده داشته و فرایندی کلی نگر است که همهٔ جنبه‌های یک سرزمین را در نظر گرفته و پلی ارتباطی بین جنبه‌های اقتصادی، اجتماعی، سنتی و فرهنگی است که تأثیر بسیار زیادی روی منابع محیط زیستی، گونه‌ها و اکوسیستم ها، آب و هوا، سلامتی انسان و در پایان روی کیفیت و وضعیت محیط زیست دارد. آمایش دفاعی، سازماندهی مناسب اماکن و فعالیت‌های نظامی به منظور بهره برداری صحیح و منطقی از توان‌ها و استعدادها در جهت میل به اهداف دفاعی است. برای رسیدن به این اهداف مطالعه پارامترهای ذیل ضروری است: ۱. مطالعهٔ پناهگاه‌های طبیعی، ۲. مکان یابی دفاعی و آسیب پذیری، ۳. مکان یابی موقت ودائمی و نظامی و پشتیبانی، ٤. مکان یابی امکانات و تأسیسات اقتصادی و زیربنایی، ۵. مکان یابی طبیعی، جغرافیایی و فیزیکی زمین

۳- پدافند غیرعامل و برنامه‌ریزی شهری:

پدافند غیرعامل در جامعه شهری عبارت از کاهش آسیب پذیری و افزایش امنیت و ایجاد قابلیت انعطاف پذیری در وضعیت‌های مختلف و عکس العمل‌های بموقع به منظور نجات جان انسان، مردم ساکن و اماکن موجود و به مفهوم حفاظت مؤثر از جان ساکنان یک شهر در جهت مقابله با جنگ و ... است. دستیابی به اهداف پدافند غیرعامل در حوزه‌های شهری نیازمند تعیین شاخص‌هایی در این حوزه است تا بر این اساس بتوان زمینه را برای برنامه‌ریزی و اجرایی کردن آن‌ها فراهم آورد. برخی از این اهداف کلان پدافند غیرعامل در حوزه شهری به شرح زیر است:

- کاهش آسیب‌پذیری زیرساخت‌های اساسی در برابر مخاطرات و تسهیل مدیریت بحران در زیرساخت‌ها در برابر بحران‌ها و پایدارسازی زیرساخت‌های سایبری و حفاظت از مردم در برابر تهدید.
- تضمین تداوم چرخه خدمات ضروری مردم و آسیب ناپذیری حوزه ادارهٔ مردم.
- تأمین نیازمندی‌های اساسی مردم و میسرسازی جابجایی جمعیت شهرها به حومه و برعکس.

٤- پدافند غیرعامل و مدیریت بحران‌ها:

سطح‌بندی میزان بحران و برنامه‌های مدیریتی صحیح می‌تواند راهکار و روش بسیار مناسبی برای مدیریت جامع بحران و پدافند غیرعامل موفق باشد. تدوین، آزمایش و اجرای راهبردهای پدافند غیرعامل برای مقابله با بحران‌های طبیعی و انسانی در جهت کاهش آثار مخرب و منفی آن‌ها و همچنین تقلیل خسارات و تلفات ناشی از حملات هوایی، زمینی و دریایی به هنگام وقوع جنگ‌های نظامی، موضوع بسیار مهمی است که اهمیت اجرایی آن همهٔ زیرساخت‌ها و مراکز حساس و حیاتی نظامی و غیرنظامی، سیاسی ارتباطی و مواصلاتی را شامل می‌شود. بطور کلی در دیدگاه پدافند غیرعامل از کلیهٔ تدابیر، مبانی غیرنظامی و راهبردهای مختلف برای کاهش بحران‌ها استفاده می‌شود. چهار مرحلهٔ اصلی مدیریت بحران بدین قرار است: ۱. آمادگی در برابر خطر و انجام اقدامات پیشگیرانه، ۲. مقابله و واکنش به هنگام وقوع، ۳. بازسازی خسارت‌ها، ٤. کاهش اثر حادثه.

فرایند دستیابی به اصول پدافند غیرعامل در منطقهٔ شهری

بطورکلی فرایند دستیابی به اصول پدافند غیرعامل در منطقهٔ شهری را می‌توان در موارد زیر خلاصه کرد: شناسایی بحران‌های احتمالی در منطقهٔ شهری و تهیه طرح‌ها و برنامه‌های پیشگیری جهت کاهش

خسارت‌های احتمالی یا محدود کردن این خسارت‌ها در منطقهٔ شهری.

• بالا بردن قابلیت بقا، تداوم عملیات و فعالیت‌های حیاتی و امدادی به مراکز مهم در شرایط وقوع بحران.

• احیاء، مرمت و بازسازی مجدد و سیاست‌گذاری و تدوین برنامه برای مدیریت منطقه.

اهداف امداد رسانی فوری پس از بحران:

• حصول اطمینان از ادامهٔ حیات اکثریت تعداد آسیب دیدگان و قراردادن آن‌ها در بهترین وضعیت جسمی.

• اعتماد به نفس و انجام خدمات فوری و اساسی برای کلیهٔ مردم با در نظر گرفتن افرادی که نیاز بیشتری دارند، کسانی که بیشتر آسیب دیده‌اند و در مضیقه‌اند.

• تعمیر یا جایگزین کردن ساختمان‌های ویران شده و اصلاح فعالیت‌های اقتصادی قابل دوام.

شناسایی بحران‌ها و تهدیدات احتمالی:

بطور کلی، شاید بتوان بحران‌ها را به چهار دسته تقسیم کرد:

۱. بحران‌های طبیعی مانند خشکسالی و سونامی و ...

۲. بحران‌های انسان‌ساز مانند انفجار کارخانهٔ اتمی چرنوبیل در سال ۱۹۸٦

۳. بحران‌های امنیتی مانند وقوع جنگ، حمایت‌های برون مرزی برای ایجاد و گسترش شورش‌های مدنی

٤. بحران‌های تأثیرگذار و تأثیرپذیر مانند سوانح هوایی، رکود اقتصادی و قحطی و انفجارها و ...

مقایسهٔ بحران ناشی از تهاجم و بحران‌های ناشی از حوادث طبیعی:

ویژگی‌های مشخصی در بحران‌های ناشی از تهاجم وجود دارند که آن‌ها را از بحران‌های ناشی از حوادث طبیعی متمایز می‌کند. سه مورد از آن به شرح زیر است:

• ماهیت تهدیدات در حوادث طبیعی ثابت است فقط اندازه و شدت آن‌ها تغییر پیدا می‌کند ولی در تهاجم، ماهیت تهدیدات سیال است و علاوه بر اندازه و شدت، سمت و سوی آن و اساساً ماهیت آن به شدت متغیر است.

• اطلاعات نسبت به ماهیت تهدیدات طبیعی کمتر سیال است، یعنی در سیر زمان روش‌های مقابله تغییرات چندانی نیافته‌اند. ولی در تهاجم‌ها به سبب سیال بودن ماهیت تهدیدات، روش‌های مقابله دارای حالت سیال مضاعف است.

• در حوادث طبیعی، امکان پیش بینی‌های مختلف وجود دارد مانند زلزله با توجه به دوره‌های بازگشت یا سیل و خشکسالی و انواع طوفان‌ها، ولی در تهاجم، پیش بینی‌ها بشدت تحت تأثیر عوامل خارجی قرار دارد.

شاخص‌های آسیب پذیری و تخریب در منطقه شهری:

امروزه با پیچیده شدن مسائل شهری، افزایش فزاینده جمعیت، تنوع و کثرت نیازها و احتیاجات، نمی‌توان شهرها را به حال خود رها کرد تا خودشان از طریق برایند عوامل مؤثر شکل گیرند وبه حیاتشان ادامه دهند. از این رو، طرح‌های شهرسازی

و برنامه ریزی شهری، بنیادی‌ترین ابزار شکل دهی به شهرها بر اساس نظم و برنامه‌ای از پیش اندیشیده شده محسوب می شوند. با توجه به این مهم، عوامل آسیب پذیری در منطقهٔ شهری را می‌توان به دو دستهٔ عمده تقسیم کرد:

الف) آسیب پذیری ناشی از عوامل و عوارض طبیعی: زلزله، آتشفشان، طوفان و ...

ب) آسیب پذیری ناشی از عوامل انسان ساخت

۵- پدافند غیرعامل و کاربری اراضی شهری

تعیین ارتباط و رابط مابین پدافند غیرعامل و کاربری اراضی شهری در مدل‌بندی، برنامه ریزی و طرح‌های توسعه شهری بر مبنای اصول پدافند غیرعامل از اهمیت بسیار زیادی برخوردار است که به این صورت می‌باشد:

ویژگی‌ها و ماهیت زمین و کاربری:

کاربری زمین به معنای بکارگیری زمین برای اهدافی خاص توسط انسان تعبیر شده است.

مهم‌ترین ویژگی‌های زمین را به شرح زیر می‌توان بر شمرد: ۱. زمین به عنوان کالای محدود و تجدید ناپذیر، ۲. زمین به عنوان نیاز مبرم و حیاتی بشر، ۳. زمین به عنوان بستر فضای زندگی

چند مورد از معیارهای بهینهٔ مکان یابی کاربری‌ها عبارت است از:

• سازگاری: منظور از مؤلفهٔ سازگاری، قرارگیری کاربری‌های سازگار در کنار یکدیگر و برعکس جداسازی کاربری‌های ناسازگار از یکدیگر است.

• دسترسی: دسترسی به عنوان معیاری دربارهٔ اینکه رسیدن به یک مکان چقدر آسان است، استفاده می‌شود.

• مطلوبیت: منظور از مطلوبیت حفظ عوامل طبیعی، چشم اندازها، فضاهای باز و ... است.

• کارایی: یکی از عوامل اصلی تعیین کنندهٔ مکان کاربری ها در شهر الگوی قیمت زمین شهری است.

پراکنش کاربری اراضی و دفاع شهری:

فهم و درک ماهیت کاربری اراضی شهری اولین قدم در راه گسترش هنر و دانش برنامه‌ریزی کاربری اراضی شهری و مدیریت توسعه است. از این رو برنامه ریزان شهری باید وظیفهٔ خود را به عنوان مدیران مسئول تغییر کاربری زمین به انجام برسانند و این فرصت را فراهم آورند تا همکاری در میان گروه‌هایی با تأملات متنوع و رقیب برای ساختن جامعه بهتر بوجود آید.

آنچه امروزه به عنوان یکی از روش‌های اساسی و اصول برنامه‌ریزی شهری می‌تواند برای کاستن از آثار بلایا مطرح باشد، نگاه امنیتی نسبت به برنامه‌ریزی کاربری اراضی و همچنین نوع مخاطرهٔ مورد تهدید برای کاهش آثار ناشی از وقوع بحران در سطح منطقهٔ شهری است. اصولاً در گزینش جایگاه و مکان استقرار کاربری‌های شهری، موارد زیر باید در نظر گرفته شود:

۱. بررسی عوامل طبیعی در پدافند غیرعامل، ۲. بررسی ملاحظات پدافندی با توجه به موقعیت جغرافیایی ناحیه، ۳. هماهنگی ملاحظات پدافندی و طرح توسعه شهر، ٤. کمک رسانی به موقع هنگام وقوع رویدادهای ناگوار، ۵. توسعهٔ آینده، ایمنی حریم و دسترسی آسان.

منطقهٔ شهری و فاکتورهای مؤثر در مکان یابی

چند مورد از این فاکتورهای مؤثر عبارتند از: ۱.تملک اراضی، ۲. عوارض طبیعی و شرایط محیطی، ۳. تأثیر حوادث و سوانح طبیعی بر انتخاب محل، ٤. امکانات و منابع انرژی، ۵. دسترسی‌ها و راه‌های ارتباطی، ٦. تأمین فضای لازم و پیش بینی توسعه

آب و امنیت

تهیه و تنظیم: میر رسول حسینی اقدم- کارشناس امریه پدافند غیر عامل

منبع: ۱- بخشی مریم، ۱۳۹۳، آب و امنیت، همایش ملی آب، انسان و زمین، اصفهان، شرکت توسعه سازان گردشگری اصفهان
۲- سایت www.waterse.ir

مقدمه:

ایمنی و امنیت از ابتدائی‌ترین اصول جهت دستیابی به استانداردهای مطلوب برای آسایش و رفاه مردم است، به همین دلیل تهدید آن همیشه یکی از اهداف اصلی تروریست‌هاست. انجام یک حمله تروریستی همیشه برای بیش از یک هدف ساده مثل آسیب رساندن، طراحی و اجرا می‌شود.

ایجاد امنیت از جمله وظایف هر دولت است که برای برقراری آن باید همه عوامل اجرایی خود را بکار گیرد. این امنیت ممکن است توسط تروریست‌ها در بخش های مختلف اقتصادی، اجتماعی، سیاسی و نظامی هدف قرار گیرد تا امنیت جامعه را مختل و با ایجاد بی ثباتی و ناامنی به اهداف شوم خود دست یابند. دفاع از مردم در مقابل تهدیدات یکی از ضروری‌ترین نیازها در مرحله اولیه طراحی شهرها به ویژه در طراحی مراکز حساس و استراتژیک مثل سیستم‌های آبرسانی است تا بیشترین و پایدارترین امنیت با کمترین زحمت و مشکلات برای مردم جهت دفاع در مقابل تهدیدات فراهم شود، از طرف دیگر دشمن برای آسیب رساندن به آن‌ها متقبل بیشترین زحمت می‌شود. همیشه برنامه‌ریزی و پیش آگاهی، زمینه‌ساز کسب آمادگی و تجهیزشدن و دفاع متناسب در برابر حوادث احتمالی پیش‌رو است.

در یک تهدید ناهمگون که فناوری جنگی طرفین از تعادل منطقی برخوردار نباشد، عوامل دیگری در کاهش این نابرابری مؤثر است که پرداختن به آن از ضروریات جنگ‌هاست. مسئله شناخت ویژگی‌های صحنه جنگ و عملیات در بهره‌گیری از مؤلفه‌ها و شاخصه‌های مؤثر در قابلیت‌های تاکتیکی، تا حدودی در کاهش توازن در جنگ مؤثر است. یکی از این ویژگی‌ها، شبکهٔ آب‌های منطقهٔ عملیاتی است. شبکهٔ آب از عوامل طبیعی است که در طول تاریخ دارای نقش‌های گوناگونی بوده است. تا قبل از جنگ جهانی دوم شبکهٔ آب نقش بازدارنده داشته اما با پیشرفت فناوری- گرچه امروزه رودخانه‌ها اهمیت سابق خود را ندارند- ولی در مقیاس‌های تاکتیکی و عملیاتی می‌توانند نقش بسیار مهمی داشته باشند. در طول تاریخ رودخانه‌های عمیق و عریض یا رودهایی با سواحل پرشیب، سدهای مؤثری علیه نظامیان زره پوش، پیاده نظام و تانک‌ها بوده‌اند. وجود شهرها، تأسیسات صنعتی، شبکه‌های ارتباطی و سایر امکانات موجب شده که کانال‌ها، آبراهه‌ها، آبگرفتگی‌ها و رودخانه‌ها از خطوط سوق الجیشی مهمی محسوب شوند.

موضوع اصلی:

آب آشامیدنی جزء سرمایه‌ها و زیرساخت‌های کلیدی هر کشوری است که در مقابل حملات تروریستی آسیب پذیر است. دسترسی به آب آشامیدنی سالم، یکی از نیازهای حیاتی جوامع است. بخشی از مدیریت آبرسانی، تأمین امنیت آبرسانی و شبکه توزیع آب است که همچون دستگاه گردش خون در بدن، امکان ادامه فعالیت و حیات را درجامعه میسر می‌سازد.

با توجه به اهمیت تأسیسات آبرسانی، گاهی درعملیات خرابکاری توسط دشمن، این تأسیسات به عنوان مراکز استراتژیک مورد هدف قرار می‌گیرند که ممکن است منجر به آسیب جدی به جامعه و بعضاً ایجاد بحران‌های امنیتی شوند.

دشمن اگر از طریق حملات فیزیکی قادر به آسیب رساندن نباشد، ممکن است با عملیات تخریبی یا آلوده‌سازی، هر بخش از تأسیسات آبی را مورد حمله قرار دهد. جبران خسارات وارده یا جایگزین کردن آن‌ها بسیار سخت و زمان‌بر خواهد بود و علاوه بر آن حوادث ثانویه‌ای را ایجاد خواهد نمود.

در استراتژی‌های انهدامی معرفی شده توسط سرهنگ جان واردن برای ارتش آمریکا بعد از جنگ ویتنام، ۵ حلقه برای نابودی طرف مخاصمه معرفی شده که مهمترین وظیفه در طرح ریزی یک جنگ، شناسایی مراکز ثقل کشور برای تهاجم است که اگر دقیق شناسایی و مورد هدف قرارگیرد کشور مورد تهاجم در اولین روزهای جنگ طعم شکست را خواهد کشید.

در این حلقه‌ها شبکه‌های آبرسانی و مخازن آب در دومین حلقه استراتژیک تعریف شده‌اند. به اینکه با قطع آبرسانی به مردم در واقع سیستم گردش خون مردم قطع می‌شود. این استراتژی‌ها درحمله به کوزوو و عراق مورد استفاده قرارگرفته‌اند.

بسیاری از مردم نمی‌دانند که آب هدف مناسبی برای تروریست‌ها است. اثرات ویژه و مهیج یک هواپیمای آتش گرفته سقوط کرده یا یک بحران گروگان گیری ضعیف است ولی این موارد نقش اثرات یک حمله روی سیستم‌های تأمین آب را در مناطقی افزایش می‌دهند که با سایر حملات تروریستی هم زمان و هماهنگ رخ دهند. از جمله حملات روی سیستم‌های تأمین آب می‌توان تخریب خطوط لوله‌های انتقال آب یا آلودگی گسترده سیستم‌های بهره برداری و از رده خارج کردن آن‌ها را نام

برد. البته یک اقدام تروریستی روی سیستم‌های تأمین آب معمولاً از طریق آلوده کردن شبکه توزیع آب با این هدف که سبب مرگ و میر تعداد زیادی از مردم شوند اتفاق می‌افتد که این مسئله نیازمند یک تروریست حرفه‌ای و متخصص نیست.

با تأسف امروزه در سطح جهان، عملیات خشونت آمیز به وسیله رسانه‌های تصویری مانند سینما و تلویزیون به طور آشکاری با نمایش فیلم‌های مختلف از حوادث خشونت آمیز، به مردم آموزش داده می‌شود.

یک حمله تروریستی یا بیوتروریستی روی تأسیسات آبرسانی، ممکن است صدها نفر را کشته و صدها نفر دیگر را به همان روش تحت تأثیر قرار داده و بیمار کند که در نتیجه منجر به بروز شرایط بحرانی می‌شود. برای مردم تصور تلفات انسانی یک حادثه تروریستی بر تأسیسات آبرسانی قابل قبول و باورکردنی نیست.

دور شدن از خطری که به وسیله آب آشامیدنی مطرح می‌شود کار ساده ای نیست. هر کسی آب را می‌نوشد و یا محصولات محتوی آب را مصرف می‌کند، احتمال آلودگی و بیمار شدنش وجود دارد. اگر تلفات انسانی دریک حادثه تروریستی مرتبط با آب، در هر کجا اتفاق بیافتد، اثرات روانی ملی آن ویرانگر خواهد بود.

تعداد کمی از مردم خواهند توانست بعد از چنین حادثه ای عاقلانه و به دور از احساس و توجه به خطر، فکر کرده و عمل کنند. اثرات روانی این حادثه می‌تواند بیشتر منتشر شده و در مدت طولانی‌تری باقی بماند. در چنین حملاتی امنیت جامعه خدشه دار شده و اعتماد مردم نسبت به مسئولین صنعت آب کم می‌شود به نحوی که جبران آن ممکن است ماه ها زمان ببرد.

اگر حادثهٔ تروریستی در خصوص آلودگی آب مصرفی درکلان شهرها اتفاق بیافتد، آثار و عوارض آن به سادگی قابل کنترل نخواهد بود و مطمئناً به یک بحران امنیتی اجتماعی تبدیل خواهد شد. دشمن با حربه تبلیغات مسموم خود اثرات روحی و روانی حمله تروریستی را تشدید و کنترل آن را برای مسئولین هزینه‌بر، گران و مشکل خواهد نمود.

وقتی تروریست‌ها اقدام به حمله تروریستی می‌کنند هدف آن‌ها علاوه بر ایجاد ناامنی و رعب و وحشت، این است که حمله آن‌ها مخفی و در حاشیه نماند و به خوبی اطلاع رسانی و مطرح گردد. آن‌ها معتقدند ارزش یک حمله باید استعداد انتشار در سطوح بین المللی را داشته و نسبتاً ارزان باشد و با کمک یک تکنولوژی ساده اتفاق افتاده و همزمان چندین هدف را تأمین کند.

چند مورد از نتایج بررسی استفاده از آب در امر آفند و پدافند در برخی از جنگ‌ها و نیز عملیات ۸ سال دفاع مقدس رزمندگان اسلام عبارت است از:

- در حال حاضر آب از نگاه سیاستمداران و نظامیان در دو مقوله ((اهداف)) و ((ابزار)) مورد بررسی قرار می‌گیرد. از منظر دسته اول، آب به عنوان یک ابزار سیاسی جهت نیل به اهداف مورد نظر خود و تأمین بخشی از منافع ملی هر کشور مطرح می‌شود که البته این امکان وجود دارد که با نرسیدن به توافقات بین طرفین، سرانجام به جنگ منجر شود.
- در مواردی آب به عنوان هدف نظامی مورد استفاده قرار می‌گیرد که از جمله آن‌ها می‌توان به بمباران ذخایر و منابع آب اشاره کرد. البته در این گونه موارد ممکن است که آب به عنوان هدف و ابزار به صورت همزمان مورد استفاده قرار گیرد.
- در مواردی ممکن است آب به عنوان یک هدف تروریستی مورد بهره برداری قرار گیرد مثل: ایجاد اختلال در سیستم توزیع آب، انفجار در شبکه‌ها، مخازن و ذخایر آب یا مسموم ساختن آن‌ها.

فعالیت‌های تهدید آمیز در سیستم‌های آبرسانی

خطوط شبکه آبرسانی، مخازن ایستگاه‌های پمپاژ و شیرآلات و دستگاه‌های اندازه‌گیری شرایط مناسبی را برای تروریست‌ها فراهم می‌نمایند، چون در دسترس بوده و معمولاً از حفاظت کافی هم برخوردار نیستند. در چنین شرایطی حتی ممکن است تخریب فیزیکی با پرتاب یک بمب یا استفاده از ماشین و کامیون بمب‌گذاری شده آسانتر از طراحی و اجرای یک حمله بیولوژیک و آلوده نمودن آب باشد.

حملات فیزیکی، شیمیائی، بیولوژیکی و سایبری از جمله روش‌هایی هستند که ممکن است به شرح زیر توسط تروریست‌ها علیه سیستم‌های آبرسانی انجام شود.

الف. تخریب فیزیکی سیستم ها: این اقدام منجر به قطع آبرسانی به علت خرابی تأسیسات و تجهیزاتی مثل پمپ ها، کلریناتورها، رایانه‌ها و ساختمان‌ها شود. در صورت انتشارگاز کلر، سلامتی کارکنان و ساکنین مجاور تصفیه خانه تحت تأثیر قرار می‌گیرد.

ب. آلودگی عمدی شیمیائی که می‌تواند کیفیت آب را در مخازن و شبکهٔ توزیع تحت تأثیر قرار دهد.

ج. حملات سایبری که بهره برداری از تصفیه خانه آب و تاسیسات مربوطه را مختل می‌نماید.

د. حملات بیوتروریستی: تصفیه خانه‌های آب و شبکه توزیع به عنوان اهداف بیوتروریستی شناخته می‌شوند. اگر چه پخش عوامل جنگ بیولوژیک از طریق آئروسل ها کارایی بیشتری دارند اما اثر انتشار عوامل بیماری‌زای قابل انتقال از طریق آب کمتر نیست و این آلودگی عمدی ممکن است در منبع تأمین آب، محل تصفیه خانه و یا درشبکهٔ توزیع آب اتفاق بیافتد.

در زمانیکه ورود مقادیر خیلی کمی از عوامل شیمیایی یا بیولوژیک به آب سلامتی میلیون‌ها نفر را تهدید می کند، مردم حق دارند نگران شوند. آن‌ها باید از سالم بودن آب مصرفی خود و اینکه در هیچ شرایطی این اتفاق نمی‌افتد، اطمینان یابند.

گرچه امکان تهیه مقادیر مورد نیاز مواد آلوده برای آلودگی شبکه آب یک شهر بزرگ خیلی مشکل است ولی اگر دشمن با حملات فیزیکی نتواند آسیب برساند، از عملیات خرابکاری برای آلوده کردن آب استفاده می کند. معمولاً بخش‌هایی آسیب‌پذیرترند که به خوبی حفاظت نمی‌شوند.

نتیجه گیری:

با توجه به این‌که، سیستم‌های تأمین آب از جمله نقاط آسیب پذیر در مقابل ورود عوامل خارجی هستند تشخیص این مطلب که منابع آب ما نسبت به یک حمله تروریستی آسیب پذیر است یا نه، کار ساده‌ای نیست.

در شرایط استراتژیک، تصرف و اشغال و آلوده نمودن آب‌ها نقش مؤثری در فعالیت و حفظ سلامت و روحیه مردم دارد. در نتیجه همیشه آب هدف ایده‌آلی برای یک حمله تروریستی است و بکارگیری بالاترین سطح حفاظتی برای سیستم‌های تأمین آب ضروری است.

درحقیقت حملات عمدی روی سیستم‌های تأمین آب کار ساده و حدسی و اتفاقی نیست، در گذشته اتفاق افتاده و هنوز هم ادامه دارد. لازم است که با ارائه آموزش‌های لازم به مردم، به ویژه نیروهای مورد اعتماد محلی که بومی هر منطقه هستند، به منافع ملی و منطقه‌ای و محلی خود علاقمند هستند، هرگونه تهدید مرتبط با سیستم‌های آبرسانی را به موقع شناسایی، کشف و گزارش کرد.

برآورد ضعیف از دشمن و یا ضعیف تلقی کردن دشمن یک تله و بسیارخطرناک است، چون منتهی به ایجاد شرایط امنیتی خاص می‌شود. این خطاها معمولاً حاصل اشتباهات قابل پیشگیری بوده و می‌توان از این طریق از حملات احتمالی پیشگیری نمود.

کشف آسیب‌پذیری روز صفر جدید در نسخه‌های قدیمی جوملا

به تازگی جزئیات مربوط به یک آسیب‌پذیری در نسخه‌های قدیمی سیستم مدیریت محتوای (CMS) جوملا، یک نرم‌افزار مبتنی بر وب برای ایجاد و مدیریت وب سایت‌ها، منتشر شده است. نقص کشف شده یک تزریق شیء در PHP است که می‌تواند منجر به اجرای کد از راه دور تحت سناریوهای مشخص شود. به عنوان مثال، می‌تواند از طریق فرم ورود به جوملا مورد سوء استفاده قرار گیرد و به مهاجمین اجازه دهد کدی را در سرور سایت اجرا کنند.

این نقص مشابه CVE-۲۰۱۵-۸۵۶۲، یک تزریق شیء در PHP است که منجر به اجرای کد از راه دور می‌شود.

تفاوت بین آسیب‌پذیری جدید و CVE-۲۰۱۵-۸۵۶۲ در تعداد نسخه‌های تحت تأثیر آن‌ها است. آسیب‌پذیری جدید تنها نسخه‌های X.۳ را تحت تأثیر قرار می‌دهد اما آسیب‌پذیری CVE-۲۰۱۵-۸۵۶۲ تمام نسخه‌های در دسترس در زمان خود را تحت تأثیر قرار می‌دهد.

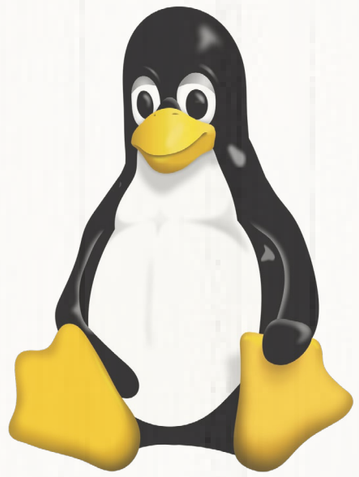
با این حال، با وجود شامل شدن بر سایت‌های کمتری، آسیب‌پذیری جدید تأثیر گسترده‌تری دارد. این آسیب‌پذیری کاملاً از محیط سرور مستقل است. در صورتی که آسیب‌پذیری قدیمی تنها روی سرورهایی کار می‌کند که دارای نسخه‌های PHP قبل از ۵.۴.۴۵، ۵.۵.۲۹ یا ۵.۶.۱۳ هستند.

خوشبختانه توسعه‌دهندگان جوملا مشکل مربوط به آسیب‌پذیری جدید را رفع کرده‌اند. به‌روزرسانی به هر نسخه جوملا با نسخه ۳.۴.۷ یا بالاتر این آسیب‌پذیری‌ها را رفع می‌کند. آخرین جوملا نسخه ۳.۹.۱۲ است.

کشف آسیب پذیری در فرمان Sudo لینوکس

به تازگی یک آسیب‌پذیری در فرمان sudo لینوکس کشف شده است که به کاربران غیرمجاز اجازه می‌دهد تا دستورات را با سطح دسترسی root اجرا کنند. این آسیب‌پذیری تنها در پیکربندی‌های غیر استاندارد لینوکس کار می‌کند و اکثر سرورهای لینوکس تحت تأثیر قرار نگرفته‌اند.

هنگام اجرای دستورات بر روی سیستم عامل لینوکس، کاربران غیرمجاز تا زمانی که دسترسی کافی داشته باشند یا گذرواژه کاربر root را بدانند، می‌توانند از دستور sudo برای اجرای دستورات به عنوان کاربر root استفاده کنند. همچنین فرمان sudo می‌تواند به گونه‌ای پیکربندی شود تا با اضافه کردن دستورالعمل‌های ویژه به فایل پیکربندی /etc/sudoers، کاربر دستورات را به عنوان کاربر دیگر اجرا کند.



با اینکه این آسیب‌پذیری دارای حساسیت بالایی است، اما تنها در حالتی عمل می‌کند که در فایل پیکربندی sudoers به یک کاربر اجازه دسترسی به یک دستور فراهم شده باشد.

با به‌روزرسانی به نسخه ۱.۸.۲۸ sudo یا بالاتر این آسیب‌پذیری رفع می‌شود.

آسیب‌پذیری بحرانی اجرای کد از راه دور در مسیریاب‌های D-LINK

پژوهشگران امنیتی وجود یک آسیب‌پذیری بحرانی اجرای کد از راه دور را در طیف وسیعی از مسیریاب‌های D-Link تأیید کرده‌اند.

آسیب‌پذیری تزریق دستور احرازهویت نشده، firmware های محصولات DIR-۶۵۵، DIR-۶۵۲ ، DHP-۱۵۶۵ شرکت D-Link را تحت تأثیر قرار می‌دهد.

این آسیب‌پذیری با ارسال یک ورودی دلخواه به رابط درگاه PingTest توسط مهاجم مورد بهره‌برداری قرار می‌گیرد که منجر به تزریق دستور و تحت کنترل درآوردن کل سیستم می‌شود. برای این باگ نمره CVSS ۱۰ صادر شده است. به منظور سوءاستفاده از نقص امنیتی، مهاجمان می‌توانند از راه دور به سیستم ورود کنند که اعتبارسنجی آن ضعیف انجام شده است.

احرازهویت ضعیف باعث می‌شود تا کد بدون توجه به سطح دسترسی کاربر اجرا شود. کد مخرب می‌تواند برای ارسال یک درخواست HTTP POST به PingTest، دریافت اطلاعات احرازهویت یا نصب درپشتی ارسال شود.

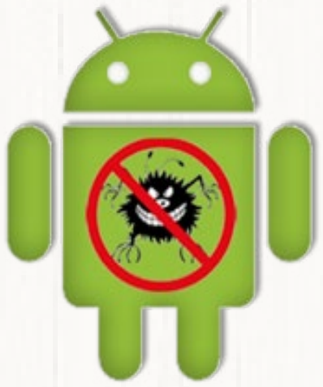
پژوهشگران امنیتی یافته‌های خود را در تاریخ ۲۲ سپتامبر برای D-Link ارسال کردند. این شرکت وجود آسیب‌پذیری را تأیید اما اعلام کرده است از آنجا که عمر پشتیبانی از این محصولات به پایان رسیده است، وصله‌ای برای رفع آن منتشر نخواهد شد. بنابراین کاربرانی که از این مسیریاب‌ها استفاده می‌کنند، برای رفع خطر سوءاستفاده از آسیب‌پذیری‌های آن‌ها، باید محصولات از رده خارج شده خود را جایگزین کنند.

انتقال بدافزار از طریق MSSQL توسط WhiteShadow

پژوهشگران امنیتی یک دانلودکننده بدافزار را ثبت کرده‌اند که از دستورهای Microsoft SQL برای انتقال payload های مخرب استفاده می‌کند.

بدافزار دانلودکننده جدید WhiteShadow نام دارد که برای انتقال انواع بدافزارها به سیستم‌های آسیب‌پذیر استفاده می‌شود. با توجه به استفاده این بدافزار در عملیات‌های توزیع تروجان‌های با دسترسی راه دور مانند AZORult ، Agent Tesla، Crimson RAT و از جمله ثبت‌کننده‌های صفحه کلید(keylogger)، به‌نظر می‌رسد که WhiteShadow یک سرویس انتقال بدافزار است.

توزیع WhiteShadow از طریق ایمیل‌های فیشینگ انجام شده که در پیوست ایمیل‌ها و درون فایل‌های مخرب Word و Excel جاسازی شده است و توسط کدهای ماکرو Visual Basic به سیستم‌های آلوده منتقل می‌شود. در صورتی که قربانی کدهای ماکرو را فعال کند، بدافزار با فراخوانی و اجرای دستورهای SQL دریافتی از سرورهای Microsoft SQL تحت کنترل عوامل تهدید، شروع به کار می‌کند. برای برقراری ارتباط با پایگاه‌داده بصورت دسترسی از راه دور و اجرای دستورها، WhiteShadow از SQLOLEDB استفاده می‌کند. بدافزار هدف به صورت رشته‌های رمز شده ASCII، در پایگاه‌داده ذخیره شده است. زمانی که دستور بارگیری بدافزار توسط WhiteShadow فراخوانی شود، payload مخرب به عنوان یک فایل فشرده PKZip منتقل می‌شود. نصب payload مخرب در سیستم قربانی براساس پیکربندی‌های ذخیره شده در فایل پیوست درون ایمیل انجام می‌شود.



یکی از بدافزارهایی که توسط WhiteShadow منتقل می‌شود Crimson است. باز نکردن ایمیل‌های مشکوک که از منابع نامعتبر دریافت می‌شوند و نظارت بر ترافیک خروجی پورت TCP ۱۴۳۳ یا مسدودسازی آن از راهکارهای جلوگیری از نفوذ این بدافزار است.

استراق سمع

آمازون و گوگل از کاربران توسط بلندگوهای صوتی

در حال حاضر امنیت اطلاعات و حفظ حریم شخصی افراد در حوزه استفاده از بلندگوهای هوشمند اهمیت زیادی یافته است.

چندی قبل فاش شد کارمندان گوگل و اپل کلیپ‌های صوتی ضبط شده از محاورات کاربران در بلندگوهای هوشمند این شرکت‌ها را گوش می‌داده‌اند.

گروهی از محققان متوجه شده‌اند هکرها با کمک اپلیکیشن‌های قابل نصب در پلتفرم‌های «گوگل هوم» و «الکسا»، می‌توانند از کاربران استراق سمع کنند.

محققان شرکت امنیتی Security Research Labs اپلیکیشن هایی به نام Skills برای الکسا و Actions برای گوگل هوم ابداع کرده‌اند. این اپلیکیشن‌ها با سوءاستفاده از شکاف‌های امنیتی توانستند دستگاه‌ها را هک کنند.

این در حالی است که شرکت مذکور چند اپلیکیشن دیگر برای پلتفرم‌ها ابداع کرده که به نظر قانونی می رسند اما دارای کدهای مخرب هستند.

این اپلیکیشن‌ها توانستند اطلاعات شخصی مانند پسوردها را جمع آوری و از کاربران استراق سمع کنند. برای این منظور اپلیکیشن پیام اختلالی منتشر می‌کرد که به نظر می‌رسید فعال نیست اما در واقع همچنان به فعالیت خود ادامه می‌داد و مکالمه کاربران را ثبت می‌کرد.

گروهی از کارشناسان نیز وجود این اپلیکیشن‌ها را تأیید کردند. درحقیقت اپلیکیشن‌ها زمانی حذف شدند که محققان شکاف‌های امنیتی مذکور را به گوگل و آمازون هشدار دادند. در حال حاضر امنیت اطلاعات و حفظ حریم شخصی افراد در حوزه استفاده از بلندگوهای هوشمند اهمیت زیادی یافته است.

«الکسا»، می‌توانند از کاربران استراق سمع کنند.

کشف آسیب‌پذیری روز صفر جدید در سیستم‌عامل اندروید

گوگل به تازگی یک آسیب‌پذیری روز صفر در اندروید کشف کرده که در حال حاضر در حال سوءاستفاده توسط مهاجمین است. این آسیب پذیری در کد کرنل سیستم عامل اندروید وجود دارد و می‌تواند برای دسترسی روت مهاجم در دستگاه مورد استفاده قرار گیرد.

این آسیب پذیری در دسامبر سال ۲۰۱۷ در نسخه‌های کرنل ۳,۱۸ ، ٤.١٤ ، ٤.٤ و ٤.٩ در اندروید رفع شد، اما مشخص شد که نسخه‌های جدیدتر نیز آسیب‌پذیر هستند.

پژوهشگران گوگل می‌گویند که این آسیب‌پذیری گوشی‌های اندرویدی زیر که نسخه اندروید x.۸ و بعد از آن را اجرا می‌کنند، را تحت تأثیر قرار می‌دهد پژوهشگران گوگل همچنین گفته‌اند که بهره‌برداری از این آسیب‌پذیری بدون شخصی‌سازی خاصی در هر دستگاه قابل انجام است، به این معنی که سوءاستفاده از آن باید روی طیف گسترده‌ای از گوشی‌ها کار کند.

خوشبختانه این آسیب‌پذیری روز صفر اندروید به اندازه سایر آسیب‌پذیری‌های روزهای صفر خطرناک نیست.

این نقص روز صفر یک آسیب‌پذیری اجرای کد از راه دور نیست که بتواند بدون تعامل کاربر مورد سوء استفاده قرار گیرد. با این حال این باگ با درجه حساسیت بالا رده‌بندی می‌شود و نیاز به نصب یک برنامه مخرب برای بهره‌برداری بالقوه دارد.

آسیب‌پذیری با شناسه CVE-۲۰۱۹-۲۲۱۵ ردیابی می‌شود و کد اثبات مفهومی (PoC) و جزئیات اضافی آن منتشر و وصله مربوط به آن برای کرنل مشترک اندروید منتشر شده است.

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

یک آسیب‌پذیری در دیوارهای آتش Cyberoam شرکت Sophos وجود دارد که می‌تواند توسط یک مهاجم، امکان دسترسی به شبکه داخلی یک شرکت را بدون ارائه گذر واژه فراهم می‌کند.

این آسیب‌پذیری با ارسال یک درخواست مخرب به کنسول‌های وب مدیر یا SSL VPN، می‌تواند به‌طور بالقوه مورد سوءاستفاده قرار گیرد و مهاجم از راه دور را قادر می‌سازد تا دستورات دلخواه را اجرا کند. در واقع، این نقص یک آسیب‌پذیری مهم برای تزریق پوسته است که می‌تواند به یک مهاجم از راه دور اجازه دهد مجوزهای root را روی تجهیزات آسیب‌پذیر دریافت کرده و با ارسال دستورات مخرب از طریق اینترنت مورد سوء استفاده قرار دهد.

دیوارهای آتش Cyberoam در شرکت‌های بزرگ مورد استفاده قرار می‌گیرند. این دیوارها بازرسی بسته‌های عمیق را برای شبکه، برنامه و امنیت مبتنی بر هویت کاربر را ارائه می‌دهند. دیوار آتش Cyberoam سازمان‌ها را از حملات DDoS ، DoS و IP Spoofing محافظت می‌کند.

شرکت **Adobe** برای رفع آسیب‌پذیری‌هایی که منجر به دسترسی غیرمجاز مهاجم، اجرای دستور در رایانه‌های آسیب‌پذیر یا افزایش دسترسی می‌شوند، چندین وصله امنیتی برای محصولات خود منتشر کرده است.

از مهم‌ترین این آسیب‌پذیری‌ها ٤٥ مورد آسیب‌پذیری بحرانی در Adobe Acrobat و Reader هستند.

دسته اول آسیب‌پذیری‌ها مربوط به Adobe Experience Manager هستند که شامل ۱۲ نقص می‌شوند. این آسیب‌پذیری‌ها منجر به افشای اطلاعات، افزایش سطح دسترسی و اجرای کد از راه دور می‌شوند.

دسته دوم آسیب‌پذیری‌ها برای Adobe Acrobat و Reader منتشر شده‌اند که ٦٨ نقص امنیتی را شامل می‌شوند که در بین آن‌ها ٤٥ مورد دارای درجه اهمیت بحرانی هستند و به مهاجم اجازه اجرای کد را می‌دهند.

دسته‌های آسیب‌پذیری دیگر در Adobe Experience Manager Forms و Adobe Download Manager کشف شده‌اند که با به‌روزرسانی به آخرین نسخه آن‌ها برطرف می‌شوند.

مهم‌ترین آسیب‌پذیری رفع شده در سری جدید به‌روزرسانی‌های **سیسکو** مربوط به محصول Cisco Aironet Access Points و درجه حساسیت بحرانی است. این آسیب‌پذیری به مهاجم احرازهویت نشده با دسترسی راه دور اجازه می‌دهد تا سطح دسترسی خود را در دستگاه هدف افزایش دهد و به اطلاعات حساس دسترسی یابد.

دو آسیب‌پذیری دیگر در دستگاه‌های Cisco Aironet Access Points نیز در به‌روزرسانی‌های اخیر سیسکو رفع شده‌اند. این دو آسیب‌پذیری دارای درجه حساسیت بالا هستند و منجر به ایجاد وضعیت DoS در دستگاه‌های آسیب‌پذیر می‌شوند.

در آسیب‌پذیری‌های جدید کشف شده توسط سیسکو، سه نقص دیگر با درجه حساسیت بالا نیز وجود دارد.

شرکت **مایکروسافت** یک به‌روزرسانی امنیتی خارج از برنامه اضطراری منتشر کرده است که دو آسیب‌پذیری بحرانی را در محصولات خود رفع می‌کند.

نقص‌های برطرف شده یک آسیب‌پذیری روز صفر در مرورگر Internet Explorer و یک باگ در Microsoft Defender هستند. از دو نقص برطرف شده، آسیب‌پذیری روز صفر Internet Explorer مهم‌ترین آن‌ها است، به این دلیل که مهاجمین سایبری هم اکنون در حال بهره‌برداری از آن هستند. آسیب‌پذیری Internet Explorer یک نقص اجرای کد از راه دور است.

آسیب‌پذیری دوم که در به‌روزرسانی‌های منتشر شده رفع شده، یک نقص انکار سرویس (DoS) در Microsoft Defender است.

از مهم‌ترین آسیب‌پذیری‌های دیگر رفع شده دو نقص احرازهویت NTLM هستند. از آسیب‌پذیری‌های قابل توجه دیگر در به‌روزرسانی‌های این ماه دو باگ اجرای کد از راه دور در موتور VBScript و یک مورد در پروتکل دسترسی از راه دور به دسکتاپ هستند.

معرفی کتاب
حوزه پدافند سایبری

«ماهیت نبرد سایبری؛ بر اساس سند راهبردی پدافند سایبری کشور» درباره مباحث و مبانی کلی مرتبط با سایبر است که می‌تواند شناخت بهتر و همه جانبه‌تری به دست اندرکاران، فرماندهان، مدیران و دانش‌جویان این حوزه بدهد و در این زمینه فرهنگ ساز باشد.

برای محافظت از فضای سایبری و مقابله با دشمنان سایبری، تربیت نیروهای توانمند کاری ضروری است و هدف این کتاب هم کمکی برای رسیدن به این مقصود است.

کتاب با مقدمه‌ای از سیر تحول جنگ‌ها وارد مبحث تعاریف و اصطلاحات تخصصی شده است. از مستندات قانونی حوزه پدافند سخن گفته است سپس تاریخچه‌ای از تهدیدات سایبری را بررسی کرده است. در ادامه به مبحث اصلی که همان فضای سایبری است پرداخته و ماهیت، تفاوت‌های فضای سایبری و واقعی، ویژگی‌های فضای سایبری و اینترنت را توضیح داده است. بعد از این مباحث در فصل ششم به گسترش جنگ سایبری و انواع حملات سایبری پرداخته و در فصل هفتم بدافزارهای رایانه‌ای را بررسی کرده است.

در فصل هشتم راهکارهای مختلف دفاع در نبردهای سایبری توضیح داده شده و فصل نهم پدافند غیرعامل در حوزه جنگ سایبری را بررسی کرده و اهمیت آن را توضیح داده است. در انتهای کتاب هم بخشی با نام مبانی دفاع سایبری وجود دارد.

به طور کلی این اثر، اطلاعات نسبتاً جامعی از فضای سایبری و هر آنچه مربوط به آن می‌شود در اختیار خواننده قرار می‌دهد.

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