
بسم الله الرحمن الرحيم

عنوان

پدافند غیر عامل در کلام رهبر انقلاب اسلامی

ارائه دهنده

سعید نصیری

بخش اول

مبانی پدافند رایانیکی

تعریف پدافند و انواع آن

پدافند یکی از مفاهیم کلیدی در حوزه دفاعی و امنیتی است. به مجموعه‌ای از اقدامات برای مقابله با تهدیدات و حفاظت از افراد، تأسیسات و منابع ملی اشاره دارد. در کشورهایی مانند ایران، که با تهدیدات مختلف منطقه‌ای و جهانی روبرو است، پدافند اهمیت ویژه‌ای دارد. به‌طور کلی، پدافند به دو نوع اصلی پدافند عامل و پدافند غیرعامل تقسیم می‌شود.

پدافند عامل

- پدافند عامل شامل مجموعه ای از اقدامات و تدابیر است که به طور مستقیم برای دفع و مقابله با حملات نظامی و تهدیدات دشمن صورت میگیرد .اقدامات دفاعی فعال که به کمک نیروی انسانی و تجهیزات نظامی برای مقابله مستقیم با تهدیدات انجام می گیرد مانند استفاده از سیستم موشکی

پدافند غیر عامل

- پدافند غیر عامل به مجموعه اقداماتی که بدون استفاده از نیروی نظامی ،به کاهش آسیب ها و تلفات در مواجهه با تهدیدات و حملات کمک می کند .این پدافند به صورت پیشگیرانه و برنامه ریزی شده به حفاظت از تاسیسات حیاتی ،افراد و زیر ساخت های کشور در مقال تهدیدات می پردازد و نقش مهمی در کاهش تلفات انسانی و اقتصادی در زمان بحران دارد .

پدافند غیر عامل و جایگاه آن در فضای سایبری

در دنیای مدرن ،فضای سایبری به عنوان عرصه پنجم نبرد (پس از زمین ،دریا ،هوا و فضا)شناخته شده است .بنابراین پدافند غیر عامل با حفظ همان فلسفه اصلی به این عرصه منتقل می شود .جایگاه پدافند غیر عامل در حوزه سایبری ایران ،فراتر از یک مجموعه اقدامات فنی است .این مفهوم یک راهبرد کلان ملی و یک فلسفه دفاعی است که هدف نهایی آن ،تبدیل کردن فضای سایبری کشور به یک محیط تاب آور و غیر قابل انکار است .موفقیت در این مسیر تنها از طریق عزم ملی ،سرمایه گذاری بلند مدت ،آموزش نیروی انسانی ،هماهنگی بین نهاد ها و فرهنگ سازی عمومی امکان پذیر خواهد یود . در جهان امروز ،امنیت سایبری معادل امنیت ملی است و پدافند غیر عامل سایبری ،ستون فقرات این امنیت به شمار می رود .

تفاوت پدافند رایانیکی با امنیت اطلاعات

امنیت سایبری رویکرد گسترده یک سازمان برای محافظت از داده‌ها، شبکه‌ها و دستگاه‌های خود در برابر تهدیدات الکترونیکی یا دیجیتالی است. این خطرات می‌تواند شامل مواردی از جمله دسترسی غیرمجاز یک طرف مخرب به شبکه، دستگاه یا محتوا یا نصب بدافزار در دستگاه یا شبکه باشد.برای جلوگیری از این تهدیدها ،کنترل های امینت سایبری ،از جمله دسترسی به شبکه و Wi-Fi ،تنظیمات سخت افزار و نرم افزار و فایروال ها باید وجود داشته باشد .

امنیت اطلاعات تا حدی زیر چتر امنیت سایبری قرار می گیرد و به طور خاص بر حفاظت از محتوا و داده ها تمرکز دارد. اطلاعات می تواند اشکال مختلفی داشته باشد؛ از محتوای دیجیتال (صرفاً) مانند ویدیوها و صفحات گسترده گرفته تا فرمت های فیزیکی مانند فایل های کاغذی یا اسناد چاپی. تهدیدات امنیت اطلاعات عبارتند از: سرقت داده های فیزیکی، حذف محتوا، به خطر افتادن یکپارچگی محتوا، و دسترسی غیرمجاز به داده ها و محتوا. عناصر کنترل اطلاعات دیجیتالی می توانند شامل رمزگذاری و محافظت از رمز عبور و یا حفاظت فیزیکی، مانند استفاده از قفل برای انبارهای بایگانی باشد.

از آنجایی که اطلاعات شرکت‌ها می‌توانند در برابر حملات دیجیتالی و فیزیکی آسیب‌پذیر باشند، برای شرکت‌ها مهم است که علاوه بر کنترل‌های امنیت سایبری خود، کنترل‌های امنیتی اطلاعاتی قوی داشته باشند. این دو در کنار یکدیگر برای محافظت از سازمان ها در برابر تهدیدات مختلف ضروری هستند. آموزش همچنین یک جنبه ضروری از سیاست‌های سایبری و امنیت اطلاعات است و باید به عنوان فرصتی برای توضیح سیاست‌ها روش‌ها به کارکنان استفاده شود. با آموزش کارمندان برای تشخیص خطرات امنیتی و ارائه دانش به آنها در مورد اینکه اگر فکر می کنند مورد حمله قرار گرفته اند چه کاری انجام دهند، شبکه، دستگاه ها و محتوای شرکت محافظت می شود.

اهمیت پدافند سایبری در خدمات شهری و زیر ساخت های حیاتی

پدافند غیرعامل یا همان دفاع بدون اسلحه یکی از بخش‌های مهم و نوین الگوی دفاع در جمهوری اسلامی است که وظیفه صیانت از مردم و حفاظت از زیرساخت‌های حیاتی در برابر تهدیدات را برعهده دارد و در سال ۱۳۸۲ با توجه به ضرورت چنین سازمانی در کنار پدافند عامل کشور بر اساس فرمان رهبر معظم انقلاب به عنوان عالی‌ترین مقام در جمهوری اسلامی ایران تشکیل شد.

این سازمان از طریق سیاست گذاری، برنامه ریزی و راهبری و هدایت و سازماندهی و نظارت، موضوع مصون سازی زیرساختهای کشور و صیانت از مردم را از طریق فرهنگ سازی و آموزش عمومی و تخصصی، آمادگی و ارتقاء مقاومت ملی، پایش تهدیدات، طبقه بندی و سطح بندی مراکز و حوزه ها، کاهش آسیب پذیری‌ها، نهادینه سازی اصول، الزامات و ملاحظات فنی مهندسی پدافند غیرعامل در ذات طرح و پروژه های ملی، استانی کشور، تسهیل مدیریت بحران و تداوم کارکردهای ضروری کشور، راهبری می کند.

سازمان پدافند غیرعامل اگرچه زیر مجموعه ستاد کل نیروهای مسلح جمهوری اسلامی ایران تعریف می شود ولی حوزه عملکرد آن فراگیر و همه دستگاه های اجرایی، نهادها و سازمان های عمومی و غیردولتی و همچنین زیرساخت های کشور را در برمی‌گیرد. از همین رو، برای تعامل بهتر با دستگاه های اجرایی، متناسب با ویژگی‌های دستگاه‌ها، معاونت‌های متناظری در سازمان پدافند غیرعامل کشور پیش بینی شده است.

همچنین این سازمان برای پاسخگویی به انواع تهدیدات احتمالی، قرارگاه های تخصصی را با موضوعات خاص تشکیل داده است که بر بررسی دائمی تهدیدات انسان ساخت و ایجاد آمادگی لازم برای مقابله با آنها تمرکز دارند.

نمونه تهدیدات واقعی علیه سازمان های خدماتی

حملات به زیرساخت حیاتی انرژی – نمونه خارجی
مطالعه موردی: حمله به شبکه برق اوکراین (۲۰۱۵)
این حمله یکی از اولین نمونه های موفق حمله سایبری به زیرساخت حیاتی بود. مهاجمان با استفاده از بدافزار BlackEnergyو بهره گیری از آسیب پذیری های نرم افزاری، به سیستم کنترل صنعتی SCADAشبکه برق اوکراین نفوذ کردند. آنها نه تنها به صورت دیجیتالی، بلکه با از کار انداختن سیستم های تلفن و تزریق کدهای مخرب در firmwareسوئیچ های برق، باعث قطعی گسترده برق شدند. این حادثه به خوبی نشان داد که چگونه یک حمله سایبری میتواند اثرات فیزیکی ملموس و گسترده داشته باشد

حملات به بخش سلامت – نمونه خارجی
مطالعه موردی: بیمارستان های جمهوری چک (۲۰۲۰)
در این حمله، مهاجمان با استفاده از یک باجافزار پیشرفته، سیستم های اطلاعاتی چندین بیمارستان بزرگ را هدف قرار دادند. آنها با رمزنگاری پرونده های پزشکی و سیستم های نوبتدهی، نه تنها دسترسی پرسنل به داده های حیاتی را مسدود کردند، بلکه امکان برنامه ریزی برای جراحی های اورژانسی را نیز از بین بردند. این حمله منجر به به تعویق افتادن درمان های ضروری و ایجاد هرج و مرج در مدیریت بیمارستان شد و وابستگی مراکز درمانی به سیستم های دیجیتال را به خوبی نشان داد

حملات به زیرساخت های خدماتی ایران – نمونه داخلی
مورد: اختلال در خدمات خودپردازهای بانکی (۱۴۰۰)
در این حادثه، مهاجمان با سوء استفاده از یک آسیب پذیری در سامانه مرکزی بانک ها، توانستند باعث ایجاد اختلال در خدمات خودپردازها شوند. اگرچه اطلاعات محرمانه مشتریان به خطر نیفتاد، اما اختلال ایجاد شده در خدمات روزمره بانکی، اثرات روانی و اجتماعی قابل توجهی داشت و اعتماد عمومی به سیستم بانکی را کاهش داد. این رویداد بر لزوم وجود سامانه های پشتیبان و طرحهای تداوم کسبوکار در بخش خدمات مالی تأکید کرد

بخش دوم

شناسایی تهدیدات سایبری در محیط شهرداری

انواع تهدیدات سایبری و راهکارهای دفاعی

تهدیدات سایبری فعالیت‌های آسیب‌رسانی هستند که با هدف تخریب، سرقت یا مختل کردن کامل زندگی دیجیتال افراد صورت می‌گیرد. ویروس‌های کامپیوتری، نقض داده و حملات DDoSتنها چند نمونه از تهدیدات سایبری شناخته شده هستند. باتوجه‌به اینکه امروزه وابستگی نفرات و کسب‌وکارها به استفاده از فناوری‌های وابسته به اینترنت بسیار بیشتر از گذشته شده است، تهدیدات سایبری فراگیرتر شده و در عین حال ما شاهد خطرات سایبری پیشرفته‌تری نیز هستیم.

بدافزارها: یکی از رایج‌ترین انواع تهدیدات سایبری، بدافزارها هستند. بدافزارها نرم‌افزارهای مخربی هستند که توسط یک مجرم سایبری یا هکر جهت مختل کردن یا آسیب‌رسانی به یک رایانه یا شبکه ایجاد می‌شوند. بدافزارها عموماً در قالب‌های مختلفی برای دانلود قرار می‌گیرند و بعد از کلیک افراد روی لینک آنها و اقدام برای دانلود، سیستم فرد را آلوده می‌کنند. در حال حاضر انواع مختلفی از بدافزارها وجود دارند که عبارت‌اند از:

ویروس : برنامه‌ای است که به یک فایل تمیز متصل شده و با تکرار خود به‌سرعت در سراسر سیستم پخش شده و فایل‌های مختلف را با کدهای مخرب آلوده می‌کند.

تروجان :نوع دیگری بدافزار است که به شکلی فریبنده و به‌عنوان یک نرم‌افزار قانونی و مناسب وارد یک سیستم شده و سپس اقدام به تخریب فایل‌های موجود یا سرقت اطلاعات می‌کند.

جاسوس افزار :این نوع از بدافزار بدون اجازه کاربر روی سیستم او نصب شده و کارهایی که کاربر انجام می‌دهد را ضبط کرده و برای مجرمان سایبری ارسال می‌کند.

باج افزار :باج افزارها نیز یک نوع بدافزار هستند که پس از ورود به یک سیستم یا برنامه، فایل‌ها و داده‌های کاربر را رمزنگاری و قفل می‌کند و مجرمان سایبری با تهدید به پاک کردن اطلاعات کاربر او را مجبور به پرداخت هزینه می‌کنند.

آگهی افزار :این نوع بدافزار در قالب تبلیغات فریبنده نمایش داده می‌شود و افراد را ترغیب به کلیک روی آگهی‌های تبلیغاتی مخرب می‌کنند.

فیشینگ :در تهدیدات سایبری فیشینگ عموماً به شکلی کاملاً هدفمند و حرفه‌ای و در قالب یک سایت یا ایمیل قانونی، افراد را وادار به افشای اطلاعات شخصی خودشان مثل اطلاعات بانکی، رمزعبور یا سایر اطلاعات شخصی کرده و سپس ازین اطلاعات جهت سرقت پول یا سواستفاده‌های دیگر استفاده می‌کنند.

آسیب پذیری های رایج در سامانه های شهرداری

گسترش روزافزون استفاده از سامانه های الکترونیک در شهرداری ها و حرکت به سوی خدمات شهری هوشمند، ضرورت توجه جدی به امنیت سایبری را بیش ازپیش برجسته کرده است. با توجه به اینکه شهرداری ها به عنوان یکی از مهم ترین نهادهای خدمات رسان مستقیم به شهروندان، حجم بالایی از داده های حساس شامل اطلاعات هویتی، مالی، مالکیتی و مکانی شهروندان را مدیریت و پردازش می کنند، هرگونه ضعف در امنیت اطلاعات می تواند پیامدهای گسترده ای از جمله اختلال در خدمات عمومی، خسارات مالی، نقض حریم خصوصی و کاهش اعتماد عمومی را به دنبال داشته باشد. مهم ترین چالش ها در امنیت سایبری شهرداری ها، ترکیبی از مشکلات فنی و سازمانی است. از لحاظ فنی، استفاده از سامانه های قدیمی، وابستگی به پیمانکاران بیرونی برای نگهداری سیستم ها، ضعف در رمزنگاری داده ها و فقدان مکانیسم های احراز هویت چندمرحله ای از مهم ترین نقاط ضعف شناسایی شده اند. از جنبه سازمانی و مدیریتی، نبود سیاست های یکپارچه امنیت اطلاعات، کمبود تیم های اختصاصی امنیت سایبری، فرهنگ سازمانی کم توجه به امنیت و ناهماهنگی میان واحدهای فناوری اطلاعات و سایر بخش ها، از چالش های اساسی محسوب می شوند.

تحلیل چند سناریوی واقعی از حملات سایبری به سازمان ها

حمله به سامانه‌های یک شهرداری بزرگ

روش حمله:

- نفوذ از طریق آسیب‌پذیری در سامانه پرداخت عوارض
- استفاده از تکنیک حرکت جانبی در شبکه
- نصب باج‌افزار روی سرورهای حیاتی

مدارک و شواهد:

- لاگ‌های سرور نشان از فعالیت غیرعادی در ساعات غیرکاری
- افزایش غیرمعمول ترافیک شبکه در بخش‌های حساس
- درخواست‌های متعدد به دامنه‌های خارجی مشکوک

تأثیرات فوری:

- تعطیلی سامانه صدور پروانه ساختمان
- اختلال در خدمات پرداخت الکترونیک
- عدم دسترسی به اطلاعات شهروندان
- توقف سامانه‌های نوبت‌دهی

خسارات بلندمدت:

- افشای اطلاعات شخصی شهروندان
- کاهش اعتماد عمومی به خدمات الکترونیک
- هزینه‌های سنگین بازیابی اطلاعات
- از دست رفتن داده‌های تاریخی

حمله به استانداری

روش حمله:

- تهدید داخلی توسط کارمند ناراضی
- سوء استفاده از دسترسی قانونی
- انتقال اطلاعات viaحافظه‌های قابل حمل

مدارک و شواهد:

- گزارش‌های سیستم کنترل دسترسی
- لاگ‌های چاپ و دانلود غیرمعمول
- فعالیت در ساعات غیراداری

تأثیرات فوری:

- سرقت اسناد محرمانه استانی
- افشای اطلاعات طرح‌های توسعه
- لو رفتن اطلاعات جلسات محرمانه

خسارات بلندمدت:

- آسیب به امنیت ملی
- افشای اطلاعات استراتژیک
- ایجاد بی‌اعتمادی در سیستم اداری

حمله به وزارتخانه

روش حمله:

- حمله فیشینگ هدفمند
- نصب در پشتی روی سیستم‌ها
- سرقت مدارک هویتی

مدارک و شواهد:

- ایمیل‌های جعلی با ظاهر رسمی
- اتصالات مشکوک به سرورهای خارجی
- تغییر غیرمجاز در تنظیمات سیستم

تأثیرات فوری:

- سرقت اطلاعات هویتی کارکنان
- دسترسی غیرمجاز به سامانه‌های داخلی
- ایجاد اختلال در ارتباطات اداری

خسارات بلندمدت:

- جعل هویت کارکنان
- سوء استفاده از اطلاعات شخصی
- آسیب به اعتبار سازمانی

بخش سوم

اقدامات دفاعی و راهکار های پیشگیرانه

اصول طراحی امن شبکه و سرور ها در محیط سازمانی

طراحی امنیت شبکه فرآیندی است که هدف آن ایجاد یک زیرساخت امن برای حفاظت از داده‌ها، سیستم‌ها و منابع شبکه در برابر تهدیدات مختلف است. این فرآیند شامل مراحل مختلفی می‌شود که از شناسایی تهدیدات و آسیب‌پذیری‌ها تا پیاده‌سازی و نظارت بر سیاست‌های امنیتی را در بر می‌گیرد.

۱. **تحلیل تهدیدات و آسیب‌پذیری‌ها:** تحلیل تهدیدات و آسیب‌پذیری‌ها یکی از اولین و حیاتی‌ترین مراحل در طراحی امنیت شبکه است. این مرحله به شناسایی و ارزیابی عواملی می‌پردازد که می‌توانند به سیستم‌ها، داده‌ها و منابع شبکه آسیب برسانند. بدون این تحلیل، هرگونه تدابیر امنیتی که پیاده‌سازی شود، ممکن است ناکافی یا نامناسب باشد.

۲. **استفاده از مدل‌های امنیتی:** یکی از مهم‌ترین مراحل در طراحی امنیت شبکه، استفاده از مدل‌های امنیتی است که به‌عنوان چارچوب‌هایی استاندارد برای حفاظت از داده‌ها، سیستم‌ها و منابع شبکه مورد استفاده قرار می‌گیرند. این مدل‌ها راهکارهایی برای پیشگیری از حملات، مدیریت دسترسی‌ها و اطمینان از محرمانگی، یکپارچگی و دسترس‌پذیری اطلاعات ارائه می‌دهند.

۳. **استفاده از فایروال‌ها و سیستم‌های تشخیص و پیشگیری از نفوذ:** فایروال‌ها و سیستم‌های تشخیص و پیشگیری از نفوذ IDS/IPS از اساسی‌ترین ابزارهای امنیت شبکه هستند که به محافظت از زیرساخت‌های شبکه در برابر تهدیدات سایبری کمک می‌کنند. این ابزارها وظایف متفاوتی دارند، اما با همکاری یکدیگر، لایه‌های امنیتی قوی‌تری را ایجاد می‌کنند.

٤. **رمزگذاری داده‌ها :** Data Encryption یکی از مهم‌ترین اصول امنیت شبکه است که با تبدیل اطلاعات به فرم غیرقابل خواندن، از دسترسی غیرمجاز به داده‌ها جلوگیری می‌کند. حتی اگر مهاجمان به اطلاعات دسترسی پیدا کنند، بدون کلید رمزگشایی قادر به خواندن یا استفاده از آن‌ها نخواهند بود.

۵. **کنترل دسترسی و احراز هویت:کنترل دسترسی** و **احراز هویت** دو اصل اساسی در امنیت شبکه هستند که به جلوگیری از دسترسی غیرمجاز به اطلاعات و منابع حساس کمک می‌کنند. این فرآیندها اطمینان می‌دهند که فقط کاربران یا دستگاه‌های مجاز قادر به ورود به سیستم یا استفاده از منابع خاص هستند.

٦. **نظارت و تحلیل ترافیک شبکه:نظارت و تحلیل ترافیک شبکه** فرآیندی است که در آن داده‌ها و فعالیت‌های شبکه به‌طور مداوم بررسی می‌شوند تا رفتارهای مشکوک شناسایی شده و از حملات سایبری یا مشکلات فنی جلوگیری شود. این فرآیند نقش مهمی در حفظ امنیت، بهینه‌سازی عملکرد، و شناسایی تهدیدات در مراحل اولیه ایفا می‌کند.

۷. **بازیابی از بحران و پشتیبان‌گیری:بازیابی از بحران** Disaster Recovery و **پشتیبان‌گیری** Backupدو عنصر کلیدی در برنامه‌ریزی امنیت شبکه هستند که به سازمان‌ها کمک می‌کنند تا در مواجهه با حوادث غیرمنتظره، مانند حملات سایبری، خرابی سخت‌افزار یا بلایای طبیعی، داده‌ها و عملیات حیاتی خود را حفظ و بازگردانی کنند. این فرآیندها تضمین می‌کنند که کسب‌وکار بتواند با حداقل اختلال به کار خود ادامه دهد.

۸. **آموزش و آگاهی‌رسانی کارکنان:آموزش و آگاهی‌رسانی امنیتی** به فرآیند ارتقاء دانش و مهارت‌های کارکنان در زمینه امنیت اطلاعات اشاره دارد. این بخش حیاتی از استراتژی امنیت شبکه، تضمین می‌کند که کارمندان نه‌تنها تهدیدات امنیتی را شناسایی کنند، بلکه از بهترین شیوه‌ها برای جلوگیری از حملات سایبری پیروی کنند.

۹. **آزمایش امنیت شبکه Network Security Testing** :**آزمایش امنیت شبکه** فرآیندی است که طی آن، زیرساخت‌ها، پروتکل‌ها و دستگاه‌های موجود در شبکه از نظر امنیتی ارزیابی می‌شوند. هدف از این آزمایش شناسایی نقاط ضعف و آسیب‌پذیری‌هایی است که ممکن است توسط مهاجمان مورد سوءاستفاده قرار گیرند.

۱۰. **نتیجه‌گیری:**طراحی امنیت شبکه یک فرآیند پیچیده و چند مرحله‌ای است که به ترکیب تکنولوژی‌ها و سیاست‌های مختلف نیاز دارد. با توجه به تهدیدات مختلف و پیشرفت فناوری‌های حمله، ضروری است که مدیران شبکه همواره به‌روزرسانی‌های امنیتی را پیاده‌سازی کرده و شبکه‌های خود را از تهدیدات مختلف محافظت کنند. امنیت شبکه تنها با همکاری تمام بخش‌ها و کارکنان سازمان قابل دست‌یابی است.

سیاست های امنیتی و کنترل دسترسی در سامانه های شهرداری

سیاست‌های امنیتی در شهرداری‌ها باید بر اساس چارچوب‌های قانونی محکم و مشخصی استوار باشد. این مبانی شامل:

- **قانون جرائم رایانه‌ای:** این قانون به عنوان سنگ بنای مقابله با تهدیدات سایبری، حدود قانونی فعالیت‌های سایبری، جرائم مختلف در این حوزه و مجازات متخلفان را به طور شفاف تعیین می‌کند. هر سیاست امنیتی در شهرداری باید با مفاد این قانون همخوانی کامل داشته باشد.
- **قانون حفاظت از داده‌های شخصی:** با توجه حجم انبوه اطلاعات شهروندان در اختیار شهرداری، این قانون چگونگی جمع‌آوری، ذخیره‌سازی، پردازش و انتقال اطلاعات شخصی را تنظیم می‌کند. سیاست‌های شهرداری باید تضمین کننده حریم خصوصی شهروندان و جلوگیری از سوء استفاده از این داده‌ها باشد.
- **مصوبات شورای عالی فضای مجازی:** این شورا تعیین‌کننده خط‌مشی‌های کلان کشور در حوزه فضای مجازی است. سیاست‌های امنیتی شهرداری باید در راستای این مصوبات و در چارچوب سند راهبردی کشور در این حوزه تدوین شود.
- **دستورالعمل‌های سازمان پدافند غیرعامل:** به عنوان نهاد متولی حفاظت از زیرساخت‌های حیاتی کشور، این سازمان الزامات امنیتی خاصی را برای سیستم‌های حساس تعیین می‌کند. شهرداری‌ها به عنوان دارنده بخشی از این زیرساخت‌ها ملزم به رعایت این دستورالعمل‌ها هستند

چارچوب حاکمیتی و مدیریتی:

برای اجرای اثربخش و یکپارچه سیاست‌های امنیتی، استقرار یک ساختار حاکمیتی منسجم و شفاف در شهرداری ضروری است. این ساختار شامل:

•**شورای عالی امنیت سایبری شهرداری:** این شورا در بالاترین سطح مدیریتی شهرداری و با حضور مدیران ارشد (مانند شهردار، معاونان و مدیر کل فناوری اطلاعات) تشکیل می‌شود. وظیفه اصلی آن تصویب سیاست‌های کلان امنیتی، تعیین خط‌مشی‌ها، تصویب بودجه و نظارت عالی بر اجرای سیاست‌ها است.

•**کمیته راهبردی امنیت اطلاعات:** این کمیته زیرمجموعه شورای عالی و متشکل از مدیران میانی و کارشناسان ارشد است. وظایف آن شامل نظارت مستمر بر اجرای سیاست‌های مصوب، بررسی حوادث امنیتی، تخصیص منابع و ارائه گزارش به شورای عالی می‌باشد.

•**تیم عملیات امنیت SOC:** این تیم در سطح عملیاتی مسئول پیاده‌سازی، پایش و نگهداری روزانه کنترل‌های امنیتی است. فعالیت‌های این تیم شامل نظارت بر شبکه و سیستم‌ها، تحلیل تهدیدات، پاسخ به حوادث امنیتی و به روزرسانی مکانیزم‌های دفاعی است.

اصول بنیادین سیاست‌گذاری امنیتی:

تمامی سیاست‌های جزئی و کنترل‌های امنیتی در شهرداری باید بر اساس اصول کلان و بنیادین زیر تدوین شوند:

•**اصل محرمانگی:** اطمینان از اینکه اطلاعات فقط در دسترس افراد مجاز قرار می‌گیرد. این اصل به ویژه برای داده‌های شخصی شهروندان و اطلاعات محرمانه طرح‌های شهری حیاتی است.

•**اصل صحت و تمامیت:** تضمین می‌کند که اطلاعات درست، کامل و بدون تغییر غیرمجاز باقی می‌مانند. هرگونه تغییر در اطلاعات (مانند تغییر کاربری یک ملک) باید به دقت ثبت و کنترل شود.

•**اصل دسترسی‌پذیری:** اطمینان از اینکه سیستم‌ها و اطلاعات هنگامی که افراد مجاز به آن نیاز دارند، در دسترس باشند. این اصل خدمات‌رسانی به شهروندان را تضمین می‌کند.

•**اصل پاسخگویی:** تمامی فعالیت‌های کاربران در سیستم‌ها باید به طور یکتا به فرد عامل قابل انتساب باشد و امکان ردگیری و حسابرسی را فراهم کند. این اصل از بروز تخلف و سوء استفاده جلوگیری می‌کند.

•**اصل دفاع در عمق:** به جای تکیه بر یک لایه دفاعی، چندین لایه امنیتی پشت سر هم مستقر می‌شوند تا در صورت شکست یک لایه، لایه بعدی از دارایی‌ها محافظت کند.

•**اصل کمترین امتیاز:** هر کاربر (شهروند، کارمند، پیمانکار) فقط به حداقل دسترسی لازم برای انجام وظایف قانونی خود دسترسی داشته باشد. این اصل احتمال سوء استفاده و خسارت را به حداقل می‌رساند.

مدیریت رمز عبور ،احراز هویت چند مرحله ای و به روز رسانی نرم افزار ها

مدیریت رمز عبور

۱-۱ سیاست‌های ایجاد رمز عبور قوی:

- **حداقل طول رمز عبور:** ۱۲ کاراکتر برای حساب‌های معمولی و ۱۵ کاراکتر برای حساب‌های مدیریتی
- **پیچیدگی ترکیبی:** استفاده اجباری از حروف بزرگ و کوچک، اعداد و کاراکترهای ویژه
- **ممنوعیت استفاده از اطلاعات شخصی:** نام، نام خانوادگی، تاریخ تولد، کد ملی و واژه‌های قابل حدس
- **تغییر دوره‌ای رمز عبور:** هر ۹۰ روز برای کاربران عادی و هر ۶۰ روز برای کاربران دارای دسترسی ویژه

۲-۱ ابزارهای مدیریت رمز عبور:

- **استفاده از نرم‌افزارهای مدیریت رمز عبور سازمانی:**
  - ذخیره‌سازی امن رمزهای عبور
  - تولید خودکار رمزهای عبور پیچیده
  - به‌اشتراک‌گذاری امن رمزهای عبور بین پرسنل مجاز

احراز هویت چندمرحله‌ای MFA

۱-۲ الزامات پیاده‌سازی MFA:

- **کاربران مشمول:**
  - کلیه مدیران سیستم و شبکه
  - پرسنل دارای دسترسی به اطلاعات محرامنه
  - کاربران دارای دسترسی از راه دور
  - کلیه حساب‌های سرویس

۲-۲ روش‌های پیاده‌سازی:

- **اپلیکیشن‌های Authenticator:**
  - Google Authenticator
  - Microsoft Authenticator
- **توکن‌های سخت‌افزاری:**
  - YubiKey
  - RSA Tokens

به‌روزرسانی نرم‌افزارها

۱-۳ چرخه مدیریت وصله‌های امنیتی:

- **شناسایی وصله‌ها:**
  - پایش مستمر منابع رسمی
  - عضویت در خبرنامه‌های امنیتی
  - استفاده از سیستم‌های مدیریت آسیب‌پذیری

۲-۳ اولویت‌بندی نصب وصله‌ها:

- **درجه اضطراری Critical:**
  - وصله‌های مربوط به آسیب‌پذیری‌های فعال
  - نصب حداکثر ظرف ۲۴ ساعت
- **درجه بالا High:**
  - آسیب‌پذیری‌های با خطر بالا
  - نصب حداکثر ظرف ۷۲ ساعت
- **درجه متوسط Medium:**
  - نصب در اولین پنجره تعمیرات
- **درجه پایین Low:**
  - نصب در به‌روزرسانی دوره‌ای

۳-۳ فرآیند تست و استقرار:

- **محیط آزمایشگاهی:**
  - شبیه‌سازی محیط عملیاتی
  - تست سازگاری با نرم‌افزارهای موجود

مانیتورینگ و پاسخ به رویداد های امنیتی

مانیتورینگ امنیت شبکه NSM (Network Security Monitoring)بخش حیاتی از هر استراتژی امنیتی سایبری جامع است. این شامل نظارت و تجزیه و تحلیل مداوم ترافیک شبکه برای شناسایی و پاسخگویی به تهدیدات و حوادث امنیتی احتمالی می‌شود. هدف NSM شناسایی فعالیت‌های مشکوک یا خبیث در محیط شبکه است، از جمله دسترسی غیرمجاز، نفوذ داده، عفونت مالور، و سایر اشکال تهدیدات سایبری.برای تعریف "پاسخ حادثه" ابتدا باید بدانید که چه حادثه امنیتی را تشکیل می دهد. گزارش Verizonیک حادثه را **"یک رویداد امنیتی است که یکپارچگی، محرمانگی یا در دسترس بودن دارایی اطلاعات را به خطر می اندازد"** تعریف می کند. یک حادثه می تواند شامل حمله باشد، یعنی تلاش عمدی برای دستیابی غیرمجاز در جهت آسیب یا نابودی شبکه. یا یک حادثه می تواند یک تصادف ساده باشد، مانند کارمندی که لپ تاپ شرکت را در ناخواسته گم می کند. یک حادثه ممکن است باعث نقض امنیت داده ها یا سرقت اطلاعات شرکت شود.پاسخ به رخدادهای امنیتی یک رویکرد رسمی و سازمان یافته برای مقابله با انواع حوادث امنیتی است. این معمولاً شامل یک برنامه پاسخ حوادث IPRاست، که مراحلی را که یک شرکت باید پس از وقوع یک حادثه دنبال کند، تعیین می کند. این برنامه ها باید شامل روند واکنش حادثه برای انواع متداول از جمله حوادث ذکر شده در زیر باشد.

روند پاسخ به رخدادهای امنیتی :موسسه SANSشش مرحله از چرخه پاسخ به حادثه را مشخص کرده است:

آماده سازی: در این مرحله سازمانها سیاست ها، برنامه پاسخ به حملات امنیتی، ارتباطات، اسناد و مدارک، تیم ها، ابزارهای کنترل دسترسی و آموزش را تنظیم می کنند.

شناسایی: این مرحله شامل شناسایی فعالیت غیرمعمول و تعیین اینکه آیا حادثه امنیتی صورت گرفته است یا خیر را مشخص میکنند.

مهار: پس از تشخیص اینکه حادثه ای رخ داده است، قدم بعدی شما باید برای جلوگیری از هرگونه صدمه احتمالی باشد.

پاکسازی: در مرحله بعد، شما باید هر کد مخرب را حذف کرده و هرگونه آسیب وارده به سیستم ها و شبکه های خود را تعمیر کنید. و کلیه آثار به جا مانده از حمله را پاکسازی کنید.

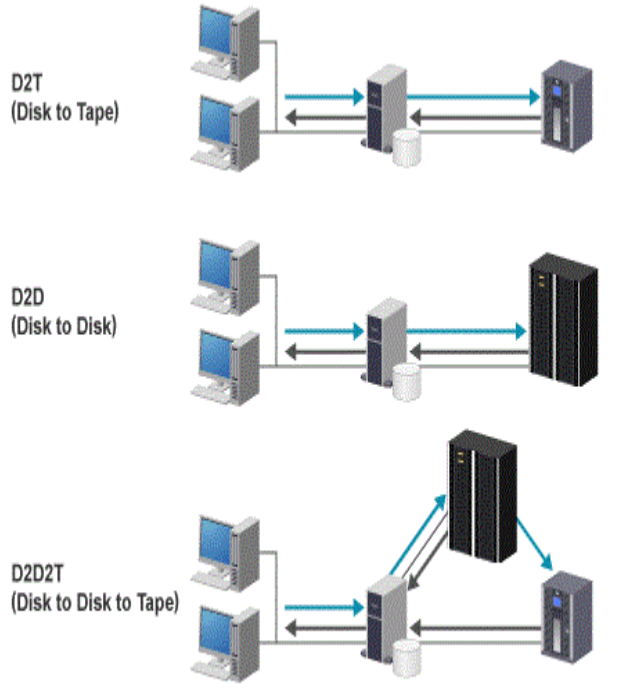
بهبود: پس از رفع مشکل، سازمان ها باید سیستم های آسیب دیده را به آرامی و با دقت به اینترنت برگردانند، و اقدامات لازم را برای اطمینان از این که این حادثه بلافاصله مجدداً رخ نخواهد داد را انجام دهند.

بکار گیری آموخته ها: بعد از اینکه سیستم ها دوباره به طور عادی کار می کنند، تیم باید حادثه را مستند کند و به دنبال راه هایی برای امنیت بیشتر سیستم ها در برابر حملات مشابه باشد.

پشتیبان گیری و بازیابی داده ها

پشتیبان گیری و بازیابی اطلاعات از مهم ترین راهکارهای مورد نیاز هر سازمانی است که توسط مرکز داده شرکت پیشگامان فناوری اطلاعات هامون ارائه می شود. به طور کلی به فرآیند ایجاد و ذخیره سازی یک نسخه کپی از اطلاعات، که در مواقع لزوم بتواند از سازمان در مقابل از دست رفتن اطلاعات محافظت کند، فرآیند پشتیبان گیری و بازیابی اطلاعات گفته می شود. گاهی به این نوع بازیابی اطلاعات، بازیابی عملیاتی Operational Recoveryنیز اطلاق می شود. بازگردانی اطلاعات می تواند در محل اصلی اطلاعات یا محلی جایگزین اتفاق بیفتند تا از آسیب و از دست رفتن اطلاعات جلوگیری کند. هدف اصلی از نسخه های پشتیبان، ایجاد و نگه داری یک نسخه از اطلاعات اصلی سازمان و بازگردانی آنها در زمانی است که اطلاعات اصلی سازمان از بین رفته باشد. از دست رفتن اطلاعات سازمان ممکن است دلایل متعددی از جمله مشکلات نرم افزاری و سخت افزاری، خرابی دیتا، خطاها و خرابکاری های انسانی مانند ویروس ها و باج افزارها و یا پاک شدن تصادفی دیتا داشته باشد. در چنین مواقعی که اتفاقات پیش بینی نشده باعث از بین رفتن دیتای شما می شود، نسخه های پشتیبان این امکان را برای شما فراهم خواهند کارد تا به زمان قبل از این اتفاق بازگردید و سرویس های شما به کار خود ادامه دهند.

نگهداری دیتاها بر روی مدیاها و دستگاه های مختلف برای اطمینان از قابل بازگشت بودن دیتاهای حیاتی سازمان شما بسیار اهمیت دارند. این مدیاها و دستگاه های مختلف می توانند دستگاه های ساده ای مانند External Driveیا USB stickها و یا دستگاه های پیشرفته ذخیره سازی اطلاعات مانند Disk storage، Cloud Storage Containerیا Tape driveها باشند. این دستگاه های جایگزین می توانند در همان محلی که نسخه اصلی اطلاعات شما وجود دارد و یا در محلی به غیر از محل نگهداری اطلاعات اصلی شما باشد.



نقش کارکنان در زمینه دفاع سایبری

کارکنان تنها "عامل انسانی" در سیستم امنیتی نیستند، بلکه **اولین خط دفاع** در برابر تهدیدات سایبری محسوب می‌شوند. هر کارمند، صرف نظر از سمت سازمانی، یک **"نگهبان داده"** است و مسئول حفاظت از اطلاعاتی است که با آن کار می‌کند. علاوه بر این، کارکنان نقش **"سفیران امنیتی"** را ایفا می‌کنند و می‌توانند آموخته‌های خود را به خانواده و جامعه انتقال دهند.

مسئولیت‌های اصلی هر کارمند

- **رعایت سیاست‌های امنیتی سازمان:** پیروی از دستورالعمل‌های امنیتی، نه به عنوان یک اجبار، بلکه به عنوان یک فرهنگ سازمانی
- **گزارش فوری رویدادهای امنیتی مشکوک:** اطلاع‌رسانی سریع در مورد هرگونه فعالیت غیرعادی به تیم امنیتی
- **محافظت از تجهیزات و اطلاعات سازمان:** مراقبت فیزیکی و دیجیتالی از دارایی‌های سازمان
- **مشارکت فعال در دوره‌های آموزشی:** حضور مستمر در برنامه‌های آموزشی و به روزرسانی دانش امنیتی

- کارکنان نه تنها "ضعیف‌ترین حلقه" بلکه "مهم‌ترین دارایی" در زنجیره دفاع سایبری هستند. با سرمایه‌گذاری مستمر بر آموزش و فرهنگ‌سازی می‌توان این دارایی ارزشمند را به قوی‌ترین خط دفاعی تبدیل کرد. موفقیت در این مسیر نیازمند تعهد مدیریت ارشد، برنامه‌ریزی بلندمدت و مشارکت فعال کلیه کارکنان است.

بخش چهارم

الزامات پدافند غیرعامل کشور در حوزه

ICT

الزامات پدافند غیر عامل در حوزه ICT

استقرار مراکز داده امن و مقاوم

در حوزه پدافند غیرعامل، مراکز داده باید به گونه‌ای طراحی شوند که حتی در شرایط تهدید و بحران نیز به کار خود ادامه دهند. این امر مستلزم:

•**مخفی‌سازی و استتار مراکز داده:**
مراکز داده حیاتی باید در مکان‌های غیرقابل پیش‌بینی و دور از نقاط حساس استقرار یابند. برای مثال، یک مرکز داده می‌تواند در دل کوه یا در زیر زمین با عمق مناسب ساخته شود. استفاده از طراحی‌های معماری استتار شده، مانند پنهان‌سازی مرکز داده در پوشش یک ساختمان تجاری یا مسکونی، نیز از جمله این اقدامات است.

•**مقاوم‌سازی در برابر تهدیدات فیزیکی:**
مراکز داده باید در برابر انواع تهدیدات فیزیکی از جمله انفجار، زلزله، سیل و حملات مسلحانه مقاوم باشند. این شامل استفاده از دیوارهای ضخیم، درب‌های ضد انفجار، سیستم‌های امنیتی پیشرفته و کنترل دسترسی چندلایه بیومتریک می‌شود

الزامات امنیت شبکه و ارتباطات

۲-۱ معماری شبکه دفاعی

شبکه‌های ارتباطی باید به گونه‌ای طراحی شوند که در برابر اختلال و نفوذ مقاوم باشند:

•**تفکیک و سگمنت‌بندی پیشرفته:**
شبکه باید به بخش‌های کاملاً مستقل تقسیم شود تا در صورت نفوذ به یک بخش، سایر بخش‌ها در امان بمانند. الگوی "شبکه‌های حبابی" به این معناست که هر بخش به صورت مجزا عمل کرده و اتصالات بین آن‌ها به دقت کنترل می‌شود.

•**راه‌های ارتباطی جایگزین:**
برای جلوگیری از قطعی ارتباطات، باید از چندین مسیر ارتباطی مختلف (فیبر نوری، رادیویی، ماهواره‌ای) استفاده شود. داشتن شبکه ماهواره‌ای اختصاصی می‌تواند در شرایط بحرانی بسیار مفید باشد

الزامات امنیت سامانه‌ها و داده‌ها

۳-۱ محافظت از داده‌ها و سامانه‌ها

حفاظت از داده‌ها و سامانه‌ها در برابر از بین رفتن یا دسترسی غیرمجاز:

•**سیستم‌های پشتیبان‌گیری و بازیابی:**
پشتیبان‌گیری مستمر و خودکار از داده‌ها و سامانه‌های حیاتی ضروری است. مراکز بازیابی فاجعه باید به گونه‌ای طراحی شوند که بتوانند در کمترین زمان ممکن سرویس‌ها را بازیابی کنند.

•**مکانیزم‌های تحمل خطا:**
استفاده از سیستم‌های افزونه و خوشه‌بندی سرویس‌های حیاتی باعث می‌شود که در صورت از کار افتادن یک بخش، بخش دیگر بتواند بار آن را تحمل کند.

۳-۲ امنیت نرم‌افزارها و سکوها

نرم‌افزارها و سکوهای مورد استفاده باید از امنیت بالایی برخوردار باشند:

•**توسعه نرم‌افزارهای امن:**
رعایت اصول توسعه امن نرم‌افزار (Secure SDLC)در تمام مراحل طراحی، توسعه و استقرار نرم‌افزارها ضروری است. انجام آزمون امنیتی مستمر و ممیزی دوره‌ای کدها نیز از دیگر الزامات است.

•**استفاده از سکوهای بومی:**توسعه و استفاده از سیستم‌عامل‌ها و سکوهای نرم‌افزاری بومی می‌تواند وابستگی به فناوری‌های خارجی را کاهش داده و امنیت را افزایش دهد

الزامات مدیریت و عملیات

۴-۱ سیستم‌های پایش و نظارت

نظارت مستمر بر شبکه و سامانه‌ها برای شناسایی و پاسخ به تهدیدات:

- **پایش همه‌جانبه و مستمر:**
مانیتورینگ ۲۴ ساعته شبکه و سامانه‌ها با استفاده از سیستم‌های کشف نفوذ پیشرفته و تحلیل رفتارهای غیرعادی ضروری است.
- **مرکز فرماندهی امنیت سایبری:**
ایجاد یک مرکز فرماندهی امنیت سایبری SOC پیشرفته که بتواند به صورت بلادرنگ وضعیت امنیتی را نمایش داده و امکان تصمیم‌گیری سریع را فراهم کند.

۴-۲ برنامه پاسخ و بازیابی

داشتن برنامه‌های از پیش تعریف شده برای پاسخ به حوادث و بازیابی سرویس‌ها:

- **طرح‌های واکنش به حوادث:**
تدوین برنامه پاسخ به حوادث سایبری برای انواع سناریوهای ممکن و تمرین دوره‌ای این سناریوها با تیم‌های واکنش سریع.
- **سیستم‌های بازیابی خودکار:**
طراحی مکانیزم‌های سوئیچ خودکار و بازیابی خودکار سرویس‌ها برای تضمین تداوم خدمات

الزامات منابع انسانی و آموزشی

۵-۱ تربیت نیروهای متخصص

بدون نیروی انسانی متخصص، حتی بهترین سیستم‌ها نیز نمی‌توانند به خوبی عمل کنند:

- **برنامه‌های آموزشی تخصصی:**
برگزاری دوره‌های پیشرفته امنیت سایبری و آموزش‌های عملی در محیط‌های شبیه‌سازی شده برای تربیت نیروهای متخصص.
- **تیم‌های متخصص پاسخ به حوادث:**
تشکیل تیم‌های واکنش سریع و آموزش تخصصی مقابله با تهدیدات پیشرفته به آن‌ها.

۵-۲ فرهنگ‌سازی امنیتی

ایجاد فرهنگ امنیت سایبری در بین کلیه کاربران:

- **آموزش همگانی:**
اجرای برنامه‌های آگاهی‌بخشی به کلیه کاربران در مورد خطرات سایبری و روش‌های مقابله با آن‌ها.
- **فرهنگ گزارش‌دهی:**
تشویق کاربران به گزارش‌دهی رویدادهای امنیتی بدون ترس از پیامدهای منفی

الزامات پژوهش و توسعه

۶-۱ پژوهش در زمینه تهدیدات سایبری

برای مقابله مؤثر با تهدیدات، آن‌ها را به خوبی شناخت:

- **بررسی و تحلیل تهدیدات:**
انجام پژوهش‌های مستمر در مورد تهدیدات سایبری نوظهور و تحلیل روش‌های مقابله دشمن.

۶-۲ توسعه فناوری‌های دفاعی

توسعه فناوری‌های بومی برای افزایش توان دفاعی:

- **توسعه سامانه‌های دفاع سایبری:**
سرمایه‌گذاری در پژوهش و توسعه فناوری‌های دفاع سایبری و ایجاد آزمایشگاه‌های شبیه‌سازی تهدیدات

مستند سازی ،طبقه بندی اطلاعات و حفاظت فیزیکی مراکز داده

الزامات مستندسازی فرآیندها

- **مستندسازی خط‌مشی‌های امنیتی:**
  - تدوین سند خط‌مشی امنیت اطلاعات ISP
  - مستندسازی استانداردهای فنی امنیتی
  - ثبت رویه‌های عملیاتی امن SOP
- **مستندسازی معماری و پیکربندی:**
  - نقشه‌های دقیق معماری شبکه و سامانه‌ها
  - مستندات پیکربندی تجهیزات زیرساخت
  - نمودارهای جریان داده و ارتباطات

۲-۱ مدیریت مستندات امنیتی

- **کنترل نسخ و به‌روزرسانی:**
  - سیستم کنترل نسخه برای مستندات
  - برنامه زمان‌بندی به‌روزرسانی مستندات
  - مدیریت تاییدیه‌های تغییرات
- **امنیت مستندات:**
  - طبقه‌بندی سطح دسترسی مستندات
  - رمزنگاری مستندات محرمانه
  - سیستم

سطوح طبقه‌بندی اطلاعات

- **داده‌های عمومی:**
  - اطلاعات قابل انتشار برای عموم
  - حداقل سطح کنترل دسترسی
  - مثال: فرم‌های عمومی، اطلاعیه‌ها
- **داده‌های داخلی:**
  - اطلاعات اختصاصی سازمان
  - دسترسی محدود به پرسنل مجاز
  - مثال: دستورالعمل‌های داخلی
- **داده‌های محرمانه:**
  - اطلاعات حساس سازمانی
  - دسترسی مبتنی بر نیاز به دانستن
  - مثال: اطلاعات مالی، طرح‌های تجاری
- **داده‌های فوق‌محرمانه:**
  - اطلاعات حیاتی و بسیار حساس
  - شدیدترین کنترل‌های دسترسی
  - مثال: اطلاعات زیرساخت حیاتی

۲-۲ برچسب‌گذاری و مدیریت داده‌ها

- **سیستم برچسب‌گذاری:**
  - برچسب‌های واضح و استاندارد
  - نشانگرهای سطح طبقه‌بندی
  - تاریخ انقضای طبقه‌بندی

حفاظت فیزیکی مراکز داده

۳-۱ کنترل دسترسی فیزیکی

- **لایه‌های کنترل دسترسی:**
  - محیط پیرامونی (حصار، گیت)
  - محیط ساختمان (ورودی‌ها، پارکینگ)
  - محیط عملیاتی (اتاق سرور)
- **سیستم‌های کنترل تردد:**
  - کارت‌های هوشمند چندعاملی
  - سیستم‌های بیومتریک
  - ثبت کامل ترددها

۳-۲ نظارت و مانیتورینگ فیزیکی

- **سیستم‌های نظارت تصویری:**
  - دوربین‌های با کیفیت بالا
  - پایش ۲۴ ساعته
  - ذخیره‌سازی ویدیوها
- **سیستم‌های اعلام سرقت:**
  - سنسورهای حرکتی
  - سیستم‌های تشخیص نفوذ
  - اتصال به مراکز نظارتی

تداوم خدمات حیاتی شهری در شرایط بحران

در عصر حاضر، بحران‌های سایبری به عنوان تهدیدی جدی برای خدمات حیاتی شهری محسوب می‌شوند. پدافند غیرعامل سایبری با رویکردی پیشگیرانه و انعطاف‌پذیر، زمینه تداوم ارائه این خدمات را حتی در شرایط بحران فراهم می‌سازد

تداوم خدمات حیاتی شهری در برابر حملات سایبری نیازمند رویکردی سیستماتیک و چندلایه است. پیاده‌سازی راهبردهای پدافند غیرعامل سایبری همراه با برنامه‌ریزی دقیق و تمرین مستمر، می‌تواند تاب‌آوری شهری را در برابر بحران‌های سایبری افزایش دهد. این امر علاوه بر حفاظت از جان و مال شهروندان، امنیت ملی را نیز تقویت می‌نماید.

آشنایی با طرح های ملی نظیر جامع پدافند سایبری

طرح جامع پدافند سایبری ملی National Comprehensive Cyber Defense Planبه عنوان یک سند راهبردی کلان، چارچوب یکپارچه‌ای برای مواجهه نظام‌مند با تهدیدات سایبری در سطح ملی ارائه می‌دهد. این طرح بر اساس اصول پدافند غیرعامل و با درنظرگیری الزامات امنیت سایبری جمهوری اسلامی ایران تدوین شده است.

۱. مبانی نظری و حقوقی

- استناد به اصل هشتم قانون اساسی در زمینه مقابله با تهدیدات
- پیروی از سند چشم‌انداز ۱۴۰۴
- انطباق با مصوبات شورای عالی فضای مجازی
- تبعیت از قوانین جرائم رایانه‌ای و حفاظت از داده‌ها

۲. اهداف کلان

- ایجاد امنیت سایبری پایدار در سطح ملی
- تضمین تداوم خدمات حیاتی کشور
- ارتقای تاب‌آوری سایبری
- توسعه توانمندی‌های بومی در حوزه امنیت سایبری

سپاس از توجه شما