مهندسین مشاور
موج برتر اندیشه

Consulting Engineers
Moj bartar andishe

افزایش تاب‌آوری و پایداری سامانه‌های پایش تصویری و الکترونیکی تحت شبکه

با هدف پیشگیری از بحران در جنگ‌های نظامی و سایبری

تهیه شده در واحد فنی و مهندسی شرکت مهندسین مشاور موج برتر اندیشه

تیرماه ۱۴۰۴

باسمہ تعالیٰ

شناسنامه سند		
طبقه بندی سند		عمومی
موضوع		افزایش تاب‌آوری و پایداری سامانه‌های پایش تصویری و الکترونیکی تحت شبکه
شماره سند		M0137D0404
گیرنده سند (بهره برداران)		سازمان های خصوصی و دولتی
تولید کننده سند	نام سازمان	شرکت مهندسین مشاور موج برتر اندیشه
	نام واحد سازمانی یا پروژه	فنی و مهندسی
	نام، نام خانوادگی و سمت سازمانی تهیه کنندگان	الهام رمضان نژاد – مدیر تحقیق و توسعه (R&D) محمد یوسفی نیا – مدیر فنی و مهندسی
	نام، نام خانوادگی و سمت سازمانی تاییدکنندگان	سید علی جوادپور – مدیرعامل
شماره نسخه (ویرایش فعلی)		1/1
تاریخ تهیه و تنظیم		۱۴۰۴/۰۴/۰۷
تعداد صفحات نسخه		۳۷ ص
تذکرات حقوقی		تمامی حقوق مالکیت فکری و معنوی این سند متعلق به شرکت مهندسین مشاور موج برتر اندیشه بوده و در راستای مسئولیت اجتماعی و توسعه امنیت درکشور، هرگونه بهره برداری جزیی یا کلی از سند و انتشار کاغذی یا الکترونیکی تمام یا بخش هایی از آن با ذکر منبع مجاز می باشد.
اطلاعات تماس تهیه کننده سند		
آدرس		تهران، یوسف آباد، تقاطع اسدآبادی–فتحی شقاقی، مجتمع تجاری هنر
تلفن / دورنگار		۰۲۱-۸۲۸۰۱۳۶۶-۷ ۰۲۱-۸۲۸۰۹۵۸۸
پایگاه اینترنتی		www.mojbartar.com
پست الکترونیکی		info@mojbartar.com

فهرست

مقدمه

با توسعه روزافزون فناوری‌های ارتباطی و گسترش کاربرد سیستم‌های پایش تصویری و الکترونیکی در مناطق حیاتی، زیرساختی و شهری، مقوله امنیت فیزیکی و سایبری این سیستم‌ها به یکی از اصلی‌ترین دغدغه‌های مدیران، تصمیم‌سازان و کارشناسان امنیت اطلاعات تبدیل شده است. سیستم‌های پایش تصویری و الکترونیکی به دلیل ماهیت عملکردی خود، به‌عنوان یکی از مهمترین بخش‌های کلیدی در امنیت پیرامونی شناخته می‌شوند و هرگونه تهدید یا حمله سایبری به آن می‌تواند منجر به ایجاد اختلال در عملیات سازمان، نفوذ به مراکز حساس و کاهش شدید سطح امنیت محیطی گردد.

این سند با هدف ارتقاء سطح امنیت سایبری سیستم‌های نظارتی و الکترونیکی تدوین گردیده است و تلاش می‌کند با ارائه دستورالعمل‌ها، چک‌لیست‌ها و راهکارهای ساختاری، مدیریتی و فنی، زمینه‌ساز طراحی، پیاده‌سازی، بهره‌برداری و پایداری ایمن این سامانه‌ها در برابر انواع تهدیدات سایبری، خرابکارانه و بحران‌های طبیعی و جنگی باشد.

مطالب این سند در شش فصل اصلی ساماندهی شده است. در فصل نخست، اصول و الزامات تقویت امنیت سایبری سیستم‌های پایش تصویری و الکترونیکی تبیین می‌شود. فصل دوم به اقدامات ساختاری و مدیریتی برای استقرار و نگهداری امن سامانه‌ها اختصاص یافته است. در فصل سوم، رویکرد سیستم یکپارچه پایش و واکنش امنیتی برای زیرساخت‌های نظارتی تصویری ارائه شده است. فصل چهارم به ارائه راهکارهای پدافند غیرعامل در حفاظت فیزیکی از زیرساخت‌های نظارتی می‌پردازد و در فصل پنجم، راهکارهای مقابله با حملات سایبری در سیستم‌های نظارتی عنوان می‌گردد. نهایتاً، فصل ششم به بررسی راهکارهای جامع پایداری سیستم در شرایط بحران و جنگ اختصاص دارد.

همچنین جهت اجرایی ساختن راه حل ها، در پایان، مجموعه‌ای از چک‌لیست‌های کاربردی برای پایش و ارزیابی امنیت سایبری این سامانه‌ها ارائه شده است.

امید است به‌کارگیری این راهکارها در طراحی، پیاده‌سازی، بهره‌برداری و مدیریت سیستم‌های پایش تصویری و الکترونیکی، موجب ارتقاء تاب‌آوری سایبری زیرساخت‌ها و افزایش اطمینان مدیران و ذینفعان در راستای صیانت از دارایی‌های حیاتی کشور گردد.

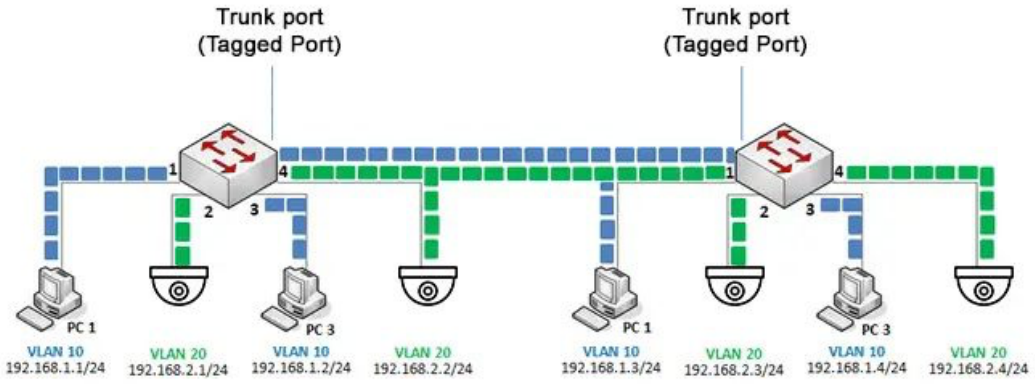
فصل اول

الزامات امنیت سایبری سیستم‌های پایش تصویری (CCTV) و الکترونیکی

اقدامات امنیتی در سطح شبکه و سخت افزار

✓ جداسازی شبکه(Network Segmentation)

یکی از اولین و حیاتی‌ترین اقدامات، جداسازی شبکه سیستم‌های نظارتی از سایر بخش‌های سازمان است. این جداسازی باید هم از نظر فیزیکی و هم منطقی انجام شود. برای جداسازی فیزیکی، بهتر است از سوئیچ‌ها و روترهای مستقل برای شبکه دوربین‌ها استفاده شود. از آنجاییکه جداسازی شبکه دوربین و سایر ارتباطات باید حتما مجزا باشد ولی در سازمان های کوچک و غیر زیرساختی که این امکان وجود ندارد، ایجاد VLAN های اختصاصی راه‌حل مناسبی است.



شکل ۱-۱ : نمونه ای از نحوه ایجاد VLAN در ارتباطات سازمان

به عنوان مثال می‌توان تمام دوربین‌ها را در VLAN 20 و سایر ارتباطات سازمان را در VLAN 10 قرار داد. سپس با تنظیم قوانین فایروال، فقط ارتباطات ضروری بین این VLAN ها را مجاز کنید. این کار مانع از آن می‌شود که نفوذ در بخش شبکه سازمان، به سیستم‌های نظارتی هم سرایت کند. علاوه بر این، بهتر است تمام ارتباطات بین اجزای سیستم با پروتکل‌های امن مانند HTTPS (HyperText Transfer Protocol Secure) یا SFTP (SSH File Transfer Protocol) انجام شود، نه نسخه‌های ناامنی مثل HTTP (Hypertext Transfer Protocol) یا FTP (File Transfer Protocol) که داده‌ها را به صورت متن ساده منتقل می‌کنند.

✓ استفاده از فایروال و سیستم‌های تشخیص/جلوگیری از نفوذ (IDS/IPS)

فایروال‌های معمولی بر اساس آدرس IP و پورت فیلتر می‌کنند، اما فایروال‌های لایه 7 که همان فایروال‌های برنامه کاربردی (Application aware Firewalls) هستند می‌توانند محتوای ترافیک شبکه را هم تحلیل کنند. این ویژگی برای

سیستم‌های نظارتی حیاتی است چون می‌تواند پروتکل‌های مخصوص مانند RTSP (Real Time Streaming Protocol) یا ONVIF (Open Network Video Interface Forum) را بررسی کند. برای مثال، می‌توان تنظیم کرد که فقط دستگاه‌های خاصی اجازه استفاده از پروتکل RTSP را داشته باشند. درکنار فایروال، سیستم‌های تشخیص وجلوگیری از نفوذ IDS (Intrusion Detection System) و IPS (Intrusion Prevention System) لایه امنیتی دیگری اضافه می‌کنند. این سیستم‌ها می‌توانند الگوهای حملات رایج مانند اسکن پورت‌ها یا تلاش برای ورود به NVR را تشخیص دهند. همچنین یک IPS پیشرفته حتی می‌تواند چنین ترافیکی را در لحظه مسدود کند.

برای پیاده‌سازی مؤثر، بهتر است این ابزارهای امنیتی را مستقیماً در نقاط ورودی شبکه نظارتی نصب کنید و قوانین آن را به طور منظم به‌روزرسانی کنید.

✓ سخت‌سازی تجهیزات (Device Hardening)

بسیاری از دستگاه‌های بکارگرفته شده در سیستم های نظارتی به صورت پیش‌فرض سرویس‌ها و تنظیمات ناامنی دارند که باید غیرفعال شوند. اولین قدم، غیرفعال کردن تمام سرویس‌های غیرضروری است .مثلاً اگر SSH (Secure Shell) یا Telne (TELecommunication NETwork)را برای مدیریت سیستم یا تجهیزات استفاده نمی‌کنید، این سرویس‌ها را کاملاً خاموش کنید. پروتکل SNMP هم اگر نیاز نیست باید غیرفعال شود، چون نسخه‌های قدیمی آن آسیب‌پذیری‌های شناخته‌شده‌ای دارند. مورد بعدی، تغییر تمام گذرواژه‌های پیش‌فرض است. بسیاری از حملات موفق فقط به این دلیل رخ می‌دهند که مدیر سیستم گذرواژه پیش‌فرض دستگاه را تغییر نداده است. بهتر است از گذرواژه‌های پیچیده استفاده کنید و هر چند ماه یکبار آن‌ها را تغییر دهید.

✓ غیرفعال‌سازی پورت‌های فیزیکی بلااستفاده

امنیت سایبری فقط به نرم‌افزار محدود نمی‌شود، بلکه پورت‌های فیزیکی بلااستفاده می‌توانند راه نفوذ مهاجمان باشند. تمام پورت‌هایUSB و Ethernet اضافی که استفاده نمی‌شوند، باید غیرفعال شود. این کار از اتصال دستگاه‌های غیرمجاز به سیستم جلوگیری می‌کند. اما غیرفعال‌سازی نرم‌افزاری به تنهایی کافی نیست و پیاده‌سازی کنترل‌های فیزیکی مانند نصب درپوش‌های قفل شونده برای پورت‌هایUSB ، استفاده از کیت‌های مسدودکننده پورت‌های شبکه و اعمال مهر و پلمپ فیزیکی بر روی درگاه‌ها، لایه دیگری از حفاظت را ایجاد می‌کند.

امنیت نرم‌افزار و Firmware تجهیزات

✓ به‌روزرسانی منظم Firmware و سیستم‌عامل

پایه اساسی هر سیستم نظارتی مدرن، Firmware دستگاه‌ها و سیستم‌عامل سرورهاست و تجربه نشان داده که بسیاری از حملات موفق، ناشی از استفاده‌ی نسخه‌های قدیمی و دارای آسیب‌پذیری‌های شناخته شده است. برای حفظ امنیت سیستم‌های نظارتی، باید یک فرآیند منظم و ساختاریافته برای به‌روزرسانی‌ها تعریف کرد. این فرآیند با رصد مستمر اطلاعیه‌های امنیتی تولیدکنندگان آغاز می‌شود.

هر به‌روزرسانی جدید باید با دقت مورد بررسی قرار گیرد تا تأثیر آن بر عملکرد کلی سیستم ارزیابی شود و همچنین باید توجه شود تا پیش از نصب هر وصله امنیتی در محیط عملیاتی، آن را در یک محیط آزمایشی مشابه تست کنیم تا از عدم ایجاد اختلال در عملکرد سیستم اطمینان حاصل نماییم.

نکته کلیدی که نباید فراموش شود، مستندسازی دقیق تمام تغییرات اعمال شده است. این مستندات باید شامل نسخه‌های نصب شده، تاریخچه تغییرات و نتایج تست‌های انجام شده باشد. چنین رویکردی نه تنها امنیت سیستم را تضمین می‌کند بلکه در صورت بروز هرگونه مشکل نیز امکان ردیابی و عیب‌یابی را فراهم می‌آورد.

به خاطر داشته باشید که در دنیای امنیت سایبری، به‌روزرسانی‌های منظم همانند واکسیناسیون دوره‌ای برای سیستم‌های نظارتی عمل می‌کنند و اولین خط دفاعی در برابر تهدیدات روزافزون سایبری محسوب می‌شوند.

✓ کنترل نسخه و ارزیابی امنیتی نرم‌افزارهای مانیتورینگ

در دنیای پیچیده امروز که تهدیدات امنیتی هر روز شکل جدیدی به خود می‌گیرد، نرم‌افزارهای مدیریت تصاویر به عنوان هسته اصلی سیستم‌های نظارتی، نیازمند توجه ویژه‌ای هستند. این نرم‌افزارها که رابط اصلی کاربران با سیستم بوده، اگر به درستی انتخاب و نگهداری نشوند، مستعد تبدیل شدن به نقطه ضعف کل سیستم می‌باشند.

تشبیه آن را می توان اینگونه تصور کرد "ساختمانی با بهترین سیستم‌های امنیتی، اما با قفل‌های ضعیف روی درهای ورودی" این دقیقاً همان اتفاقی است که وقتی نرم‌افزارهای مدیریت تصاویر بدون در نظر گرفتن ملاحظات امنیتی انتخاب می‌شوند، رخ می‌دهد. بهترین راه این است که از همان ابتدا نرم‌افزارهایی انتخاب شوند که امنیت در ذات آنها جریان دارد، نرم‌افزارهایی که با فلسفه "امنیت از ابتدا "طراحی شده‌اند، نه اینکه ویژگی‌های امنیتی به عنوان وصله‌ای بر روی آنها اضافه شده باشد

در عمل، حفظ امنیت این نرم‌افزارها نیازمند یک برنامه منظم و سیستماتیک است. هر ماه باید یک بررسی کامل انجام داد و پس از هر به‌روزرسانی، سیستم را مجدداً ارزیابی کرد، به طور مداوم فعالیت‌های غیرعادی را زیر نظر گرفت و هر از چندگاهی دسترسی کاربران را بازبینی کرد. نتایج این بررسی‌ها باید به دقت تحلیل شود تا مشکلات واقعی از هشدارهای کاذب تشخیص داده شوند.

✓ استفاده از سیستم‌عامل‌های مقاوم و ایمن

سیستم‌عامل مناسب می‌تواند مانند نگهبانی خستگی‌ناپذیر توسط کنترل دسترسی و نظارت مداوم از داده‌های حساس محافظت کند. سیستم‌عامل‌های معمولی که روی کامپیوترهای شخصی نصب می‌شوند، برای محیط‌های حساس نظارتی مانند دوربین‌های تحت شبکه پیشرفته یا مراکز کنترل امنیتی به اندازه کافی ایمن نیستند. اینجاست که باید به سراغ سیستم‌عامل‌های ویژه‌ای برویم که از ابتدا برای مقابله با تهدیدات طراحی شده‌اند.

برای سیستم‌هایی که بر پایه لینوکس کار می‌کنند، نسخه‌های مقاوم‌سازی شده مانند Linux Hardened گزینه مناسبی هستند. این سیستم‌عامل‌ها با ابزارهای پیشرفته‌ای مثل SELinux مجهز شده‌اند که مانند یک نگهبان سختگیر، دقیقاً مشخص می‌کند هر برنامه یا کاربر چه کارهایی می‌تواند انجام دهد. حتی اگر هکری بتواند به سیستم نفوذ کند، این محدودیت‌های شدید مانع از انجام اقدامات مخرب توسط او می‌شود.

اگر محیط شما بر پایه ویندوز کار می‌کند، نسخه‌های امن سازی شده مانند Windows IoT Secure وجود دارد که برای دستگاه‌های حساس طراحی شده‌اند. این سیستم‌عامل‌ها ویژگی‌های جالبی دارند؛ مثلاً فقط نرم‌افزارهای تأیید شده را اجرا می‌کند یا هنگام روشن شدن سیستم، از بارگذاری برنامه‌های غیرمجاز جلوگیری می‌کند.

اما نصب این سیستم‌عامل‌های امن کافی نیست. باید آنها را به درستی تنظیم و پیکربندی کرد. مثلاً در لینوکس، بسیاری از قابلیت‌های غیرضروری که ممکن است روزنه‌ای برای نفوذ باشد، باید خاموش شوند. یا سیاست‌های محدودکننده باید با دقت تنظیم شوند تا هم امنیت حفظ شود و هم سیستم به خوبی کار کند.

پس از نصب و راه اندازی اولیه، کار تمام نمی‌شود. این سیستم‌عامل‌ها مانند یک خودروی لوکس نیاز به سرویس و نگهداری منظم دارند. به‌روزرسانی‌های امنیتی باید بلافاصله نصب شوند، فعالیت‌های سیستم باید زیر نظر باشد و تنظیمات باید هر چند وقت یکبار بررسی و به‌روزرسانی شوند.

این سطح از توجه و دقت ممکن است در ابتدا هزینه‌بر به نظر برسد، اما در مقایسه با خسارت‌های ناشی از نفوذ هکرها یا افشای تصاویر محرمانه، سرمایه‌گذاری هوشمندانه‌ای است. در جهانی که پیچیدگی تهدیدات امنیتی به‌صورت روزافزون در حال افزایش است، به‌کارگیری سیستم‌عامل‌های امن و مقاوم نه یک گزینه اختیاری، بلکه ضرورتی اجتناب‌ناپذیر محسوب می‌شود.

احراز هویت و دسترسی

سامانه های نظارت تصویری نیازمند رویکردی چندبعدی برای تضمین امنیت هستند. روزهایی که یک رمز عبور ساده می‌توانست از دسترسی غیرمجاز جلوگیری کند گذشته است و امروزه ما با چالش‌های امنیتی پیچیده‌تری روبرو هستیم که نیازمند راهکارهای هوشمندانه‌تری می‌باشند.

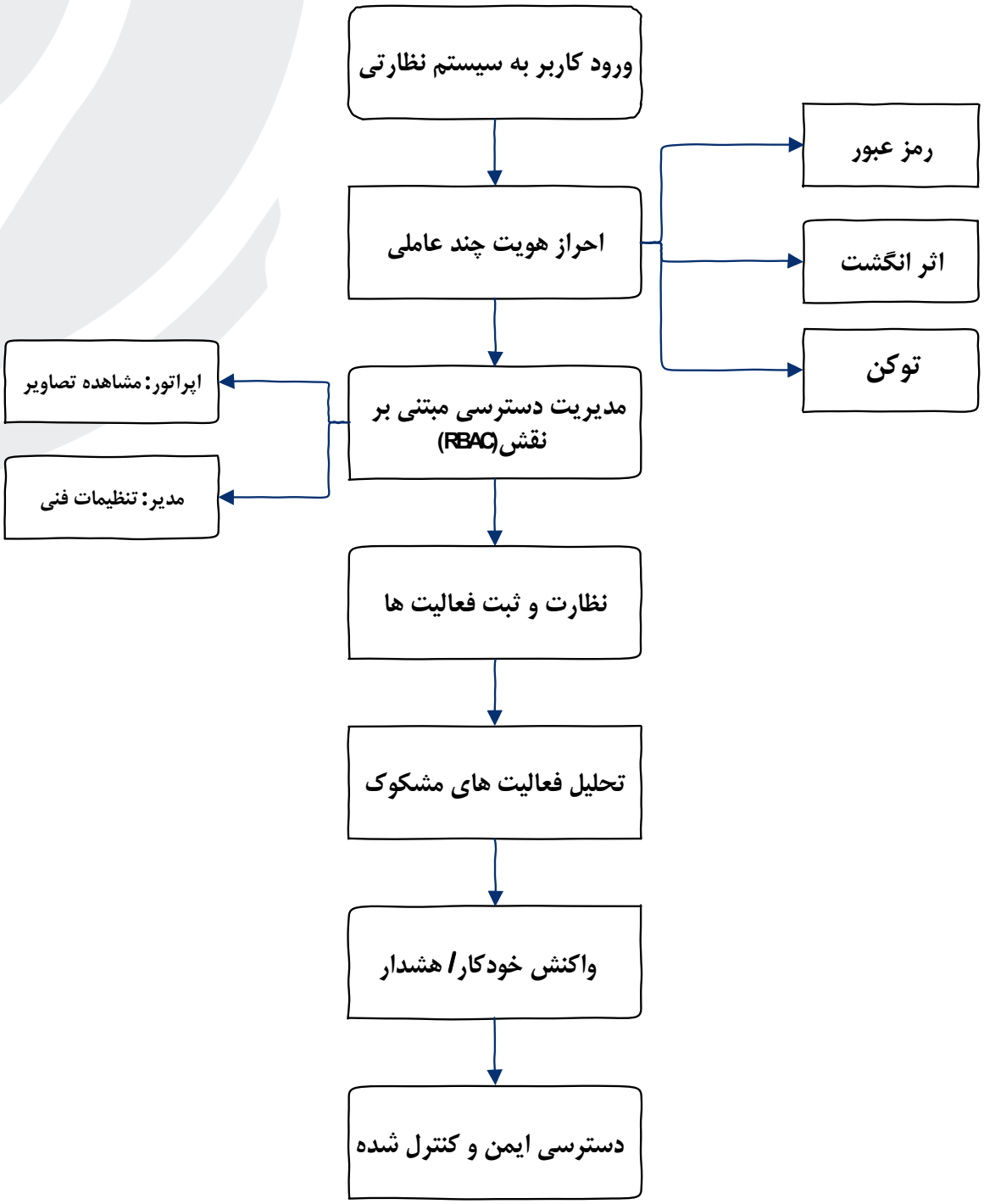
احراز هویت چندعاملی یا MFA (Multi-Factor Authentication) اولین خط دفاعی قدرتمند در این سیستم‌ها محسوب می‌شود. این سیستم به جای تکیه بر یک روش ساده احراز هویت، از ترکیب چندین لایه امنیتی استفاده می‌کند. تصور کنید برای ورود به سیستم نظارتی ساختمان خود، هم باید رمز عبور شخصی خود را وارد کنید و هم کدی که به تلفن همراهتان ارسال شده است را تأیید نمایید و هم اثر انگشت خود را اسکن کنید. این سه لایه امنیتی در کنار هم، احتمال نفوذ غیرمجاز را به حداقل می‌رساند. در محیط‌های حساس‌تر مانند مراکز نظامی یا تأسیسات حیاتی، حتی از توکن‌های سخت‌افزاری کوچکی استفاده می‌شود که مانند کلیدهای فیزیکی عمل می‌کنند و در برابر پیچیده‌ترین حملات سایبری مقاوم هستند.

اما امنیت فقط به مرحله ورود به سیستم محدود نمی‌شود. پس از احراز هویت موفق، سیستم باید دقیقاً مشخص کند که هر کاربر به چه بخش‌هایی می‌تواند دسترسی داشته باشد. اینجاست که سیستم مدیریت دسترسی مبتنی بر نقش یا RBAC (Role-Based Access Control) وارد عمل می‌شود. در این سیستم، دسترسی‌ها بر اساس وظایف و مسئولیت‌های هر شخص تعریف می‌شود. برای مثال، یک نگهبان ساختمان ممکن است فقط بتواند تصاویر زنده دوربین‌های مشخصی را مشاهده کند در حالی که مدیر فنی سیستم به تمام تنظیمات و آرشیو تصاویر دسترسی دارد. این تفکیک دقیق دسترسی‌ها نه تنها امنیت سیستم را افزایش می‌دهد بلکه در صورت بروز هرگونه مشکل امنیتی، ردیابی و شناسایی منشأ آن را بسیار ساده‌تر می‌کند.

در پس‌زمینه این سیستم مکانیزم‌های پیشرفته ثبت و تحلیل فعالیت‌ها به طور مداوم در حال نظارت هستند. این سیستم‌های هوشمند مانند نگهبانانی همیشه بیدار تمام فعالیت‌های کاربران را ثبت و تحلیل می‌کنند. آنها می‌توانند الگوهای غیرعادی مانند تلاش برای دسترسی به بخش‌های ممنوعه یا فعالیت در ساعات غیرمعمول را شناسایی کنند و در زمانی که چنین فعالیت‌های مشکوکی تشخیص داده شود، سیستم می‌تواند به صورت خودکار واکنش نشان دهد، از مسدود کردن موقت دسترسی گرفته تا ارسال هشدار فوری به تیم امنیتی. برای اینکه این سیستم‌های پیچیده به خوبی عمل کنند نیازمند برنامه‌ریزی دقیق و اجرای صحیح است. تمام کاربران باید از روش MFA برای ورود به سیستم استفاده کنند. ماتریس دسترسی‌ها باید به طور دوره‌ای بازبینی و به‌روزرسانی شود. سیستم‌های ثبت وقایع باید همیشه فعال و تحت نظارت باشند و مهم‌تر از همه، وقتی سیستم هشداری می‌دهد باید بلافاصله و به صورت مناسب به آن پاسخ داده شود.

این رویکرد جامع به سازمان‌ها کمک می‌کند تا سیستم‌های نظارتی خود را در برابر تهدیدات روزافزون ایمن نگه داشته در حالی که همچنان برای کاربران مجاز، قابل دسترس و کاربرپسند باقی بماند. در عصری که امنیت سایبری به یکی از بزرگ‌ترین چالش‌های سازمان‌ها تبدیل شده است، پیاده‌سازی چنین سیستم‌های امنیتی پیشرفته‌ای نه یک انتخاب، بلکه یک ضرورت

اجتناب‌ناپذیر است. این سرمایه‌گذاری در امنیت، می‌تواند در بلندمدت از هزینه‌های گزاف ناشی از نقض امنیت و دسترسی غیرمجاز جلوگیری کند.



شکل ۲-۱ : نمای شماتیک از اعمال سیاست‌های احراز هویت و دسترسی

فصل دوم

اقدامات ساختاری و مدیریتی

سیاست‌های امنیتی هوشمند

امروزه سیستم‌های نظارت تصویری به مهم ترین رکن اساسی امنیت سازمان‌ها تبدیل شده است. این سیستم‌های پیچیده که متاسفانه به اشتباه به شبکه‌های سازمانی متصل هستند در معرض طیف گسترده‌ای از تهدیدات سایبری و فیزیکی قرار دارند. برای حفاظت مؤثر از این دارایی‌های حیاتی، نیازمند رویکردی جامع و هوشمند در سیاست‌گذاری و مستندسازی هستیم.

سیاست امنیت سایبری برای سیستم‌های تصویری نباید صرفاً یک سند فرمالیته باشد، بلکه باید به عنوان یک راهنمای پویا و کاربردی طراحی شود که همگام با تحولات تهدیدات به‌روزرسانی گردد. این سیاست باید با دقت تمام جنبه‌های فنی و سازمانی را پوشش دهد و از تعریف دقیق دارایی‌ها و نقش‌ها گرفته تا پروتکل‌های پاسخ به حوادث و دستورالعمل‌های بازیابی را بیان کند. به عنوان مثال، باید مشخص کند که در صورت حمله سایبری همزمان با یک واقعه امنیتی مهم، چه اقداماتی باید به ترتیب اولویت انجام شود یا اگر مرکز کنترل به هر دلیلی از کار افتاد، چه راهکارهای جایگزینی وجود دارد.

مستندسازی دقیق و نظام‌مند، ستون فقرات مدیریت امنیتی مؤثر محسوب می‌شود. هر تغییر در تنظیمات سیستم، هر به‌روزرسانی نرم‌افزاری و هر تعدیل در سطح دسترسی کاربران باید با جزئیات کامل ثبت شود. یک سیستم مستندسازی ایده‌آل، اطلاعات را به صورت متمرکز و یکپارچه نگهداری می‌کند و دسترسی به آن را به شکل کنترل‌شده مدیریت می‌نماید. همچنین امکان ردیابی تغییرات و بازیابی سریع اطلاعات را نیز فراهم می‌آورد. این مستندات باید با استانداردهای صنعتی مطابقت داشته تا در مواقع ضروری به راحتی قابل استفاده باشند.

برای اجرای مؤثر این سیاست‌ها، نیازمند پیاده‌سازی فرآیندهای منظمی هستیم. بازنگری دوره‌ای سیاست‌ها با توجه به تهدیدات جدید، انجام تمرینات عملی برای تست سناریوهای بحران و به‌روزرسانی منظم مستندات در هنگام تغییرات سیستم، از جمله این فرآیندهاست. فناوری‌های پیشرفته‌ای مانند سیستم‌های مدیریت اطلاعات امنیتی SIEM (Security Information and Event Management) و ابزارهای اتوماسیون مستندسازی می‌توانند نقش مهمی در پشتیبانی از این فرآیندها ایفا کنند.

در نهایت، موفقیت این چارچوب امنیتی مستلزم مشارکت تمام ذینفعان سازمانی و تعهد مدیریت ارشد به اجرای مستمر آن است. با پیاده‌سازی این رویکرد جامع سازمان‌ها می‌توانند اطمینان حاصل کنند که سیستم‌های نظارت تصویری و الکترونیکی آنها نه تنها در برابر تهدیدات فعلی مقاوم هستند بلکه برای چالش‌های امنیتی آینده نیز آمادگی لازم را دارند. این فرآیند مستمر بهبود و به‌روزرسانی، کلید حفظ امنیت در محیطی است که تهدیدات به سرعت در حال تحول و پیچیده‌تر شدن هستند

✓ مدیریت چرخه حیات امنیتی

حفظ امنیت سیستم‌های نظارتی نیازمند نظم و انضباط مدیریتی است. این شامل بازبینی دوره‌ای سیاست‌ها، ارزیابی مستمر ریسک‌ها و به‌روزرسانی مستندات متناسب با تغییرات سیستم می‌شود. یک رویکرد پیشگیرانه موفق، تست منظم بازیابی از بکاپ‌ها را نیز در برنامه خود جای می‌دهد تا از کارایی آنها در شرایط بحرانی اطمینان حاصل شود.

✓ یکپارچه‌سازی با ساختار سازمانی

سیاست‌های امنیتی نباید در انزوا عمل کنند، بلکه باید به طور کامل با ساختار مدیریتی و عملیاتی سازمان ادغام شوند. این بدان معناست که تمام سطوح سازمان، از مدیریت ارشد گرفته تا اپراتورهای سیستم، از مسئولیت‌ها و پروتکل‌های امنیتی آگاه بوده و به آنها متعهد بمانند. آموزش مستمر پرسنل و برگزاری دوره‌های آگاهی بخشی امنیتی، تضمین می‌کند که این سیاست‌ها در عمل نیز رعایت شوند.

✓ نظارت و بهبود مستمر

حلقه تکمیل‌کننده‌ی این فرآیند، استقرار مکانیزم‌های نظارتی هوشمند است که عملکرد سیستم را در برابر معیارهای تعیین شده ارزیابی می‌کند. این نظارت باید منجر به شناسایی نقاط ضعف و بهبود مستمر سیاست‌ها شود. استفاده از چارچوب‌های استانداردی مانند ISO 27001 می‌تواند به ساختاردهی این فرآیند کمک شایانی نماید.

توانمندسازی تخصصی نیروی انسانی در مواجهه با تهدیدات سایبری سیستم‌های نظارتی

امنیت سایبری سیستم‌های پایش تصویری به عنوان یکی از حساس‌ترین بخش‌های زیرساخت امنیتی سازمان‌ها، نیازمند رویکردی همه‌جانبه است که در آن آموزش تخصصی پرسنل از ارکان اساسی محسوب می‌شود. در این چارچوب، برنامه‌ریزی آموزشی باید به گونه‌ای طراحی شود که اپراتورها و کارشناسان فنی را به سطحی از تخصص برساند که بتوانند نه تنها وظایف روزمره خود را انجام دهند بلکه به عنوان خط مقدم دفاع سایبری عمل کنند.

برای دستیابی به این هدف، ابتدا لازم است دوره‌های تشخیص تهدیدات سایبری به صورت کاملاً تخصصی و متناسب با ویژگی‌های سیستم طراحی شود. این آموزش‌ها باید شامل شناسایی نشانه‌های نفوذ به سیستم باشد که می‌تواند شامل مواردی مانند تغییرات غیرمنتظره در تنظیمات دوربین‌ها، اختلال در جریان ویدئویی، افزایش غیرعادی بار پردازشی سرورهای ضبط یا تلاش‌های مکرر برای دسترسی به بخش‌های حساس سیستم و... باشد. در این آموزش‌ها باید به اپراتور آموخته شود که چگونه این نشانه‌ها را از مشکلات معمول فنی تشخیص داده و چه اقدامات اولیه‌ای را باید انجام دهد.

در سطح پیشرفته‌تر، آموزش تشخیص دستکاری‌های تصویری از اهمیت ویژه‌ای برخوردار است. این آموزش‌ها باید شامل روش‌های شناسایی دستکاری‌های هوشمندانه مانند جعل عمیق (deepfake) در تصاویر نظارتی، دستکاری فراداده‌های ویدئویی یا حملات فریب‌آمیز به الگوریتم‌های تحلیل تصویر باشد. کارشناسان باید با تکنیک‌های پیشرفته تشخیص اصالت تصاویر و روش‌های تأیید یکپارچگی جریان‌های ویدئویی آشنا شوند.

تمرینات عملی شبیه‌سازی حملات سایبری (Red Team/Blue Team) باید به صورت دوره‌ای و با سناریوهای متنوع برگزار شود. این تمرینات نباید محدود به حملات معمول باشد بلکه باید شامل سناریوهای پیچیده‌ای مانند حملات زنجیره‌ای به سیستم‌های نظارتی، بهره‌برداری از آسیب‌پذیری‌های روز صفر یا حملات پیشرفته مستمر APT (Advanced Persistent Threat) باشد. در این تمرینات، تیم Red Team باید با تکنیک‌های واقعی حمله به سیستم‌های نظارتی آشنا باشد، در حالی که تیم Blue Team باید روش‌های تشخیص، مقابله و بازیابی را تمرین کند.

پس از هر تمرین، جلسات تحلیل دقیق با حضور تمامی ذینفعان باید برگزار شود که در آن تمام مراحل حمله، پاسخ‌های دفاعی، نقاط قوت و ضعف سیستم به دقت بررسی شود. این جلسات باید منجر به به‌روزرسانی مستندات امنیتی، اصلاح سیاست‌ها و بهبود فرآیندها شود. نتایج این تحلیل‌ها باید به صورت بازخوردهای عملی به برنامه‌های آموزشی بازگردانده شده تا چرخه بهبود مستمر کامل شود.

برای تضمین اثربخشی برنامه‌های آموزشی لازم است برای سیستم، ارزیابی دقیقی طراحی شود که شامل آزمون‌های عملی، شبیه‌سازی‌های غافلگیرانه و سنجش توانایی واقعی پرسنل در شرایط شبیه‌سازی شده بحران است. نتایج این ارزیابی‌ها باید به صورت فردی و سازمانی تحلیل شود و مبنای برنامه‌ریزی آموزشی بعدی قرار گیرد.

این برنامه جامع آموزشی باید به صورت مستمر و باتوجه به تحولات تهدیدات سایبری و تغییرات تکنولوژیکی به‌روزرسانی شود. ارتباط تنگاتنگ با مراکز تحقیقاتی امنیت سایبری، شرکت در کنفرانس‌های تخصصی و پایش مستمر تهدیدات جدید در صنعت نظارت تصویری، از ملزومات حفظ اثربخشی این برنامه‌هاست. در نهایت، این آموزش‌ها باید منجر به ایجاد فرهنگ امنیتی قوی در سازمان شود که در آن تمام پرسنل نسبت به تهدیدات سایبری هوشیار بوده و مسئولیت حفاظت از سیستم را به صورت جمعی بر عهده بگیرند.

برنامه‌ریزی جامع تداوم خدمات و بازیابی سیستم‌های نظارتی تصویری

✓ سیستم پشتیبان‌گیری سلسله مراتبی برای داده‌های تصویری

پیاده‌سازی یک استراتژی پشتیبان‌گیری چندلایه برای داده‌های ویدئویی نیازمند توجه به چندین فاکتور حیاتی است. در لایه اول، داده‌های خام با استفاده از آرایه‌های ذخیره‌سازی RAID-6 یا RAID-10 با قابلیت تحمل خطای بالا ذخیره می‌شوند. این لایه باید از فناوری‌هایی مانند Self-Healing Storage استفاده کند که قادر به تشخیص و ترمیم خودکار خرابی‌های سکتوری است. لایه دوم شامل پشتیبان‌گیری افزایشی (Incremental Backup) هر ۶ ساعت و پشتیبان‌گیری کامل روزانه روی سیستم‌های ذخیره‌سازی مجزا با قابلیت Snapshot است. برای داده‌های حیاتی، لایه سوم شامل پشتیبان‌گیری آفلاین روی رسانه‌های WORM (Write Once Read Many) با ظرفیت بالا و مقاوم در برابر دستکاری است که در مکانی امن خارج از سایت با کنترل دسترسی بیومتریک نگهداری می‌شوند. تمامی پشتیبان‌ها باید با الگوریتم‌های رمزنگاری ایمن محافظت شده و از ماژول امنیتی سخت‌افزاری HSM (Hardware Security Module) برای مدیریت کلیدهای رمزنگاری و انجام عملیات امنیتی استفاده شود.

✓ معماری Failover پیشرفته برای سیستم‌های نظارتی

پیاده‌سازی سیستم‌های Failover در محیط‌های نظارتی نیازمند طراحی خاصی است که با ماهیت Real-Time این سیستم‌ها سازگار باشد. در سطح سرورهای مدیریت ویدئو VMS(Video Management System)، باید از خوشه‌های فعال–فعال(Active-Active) با توزیع بار هوشمند استفاده شود که از پروتکل‌هایی مانندVRRP (Virtual Router Redundancy Protocol) یا HSRP (Hot Standby Router Protocol) برای مدیریت انتقال سشن‌ها بهره می‌برند. برای دوربین‌های IP ، پیاده‌سازی مکانیزمMulticast Failover امکان انتقال بدون وقفه جریان‌های ویدئویی به سرورهای جایگزین را فراهم می‌کند. در سطح ذخیره‌سازی، استفاده از فناوری‌هایی مانند Storage Replication Adapter (SRA)در محیط‌های مجازی‌سازی، امکان همگام‌سازی بلادرنگ بین مراکز داده اصلی و ثانویه را ایجاد می‌کند. برای سناریوهای بحرانی، باید از سیستم‌های نظارتی موقت مبتنی بر فناوری‌های Edge Recordingاستفاده کرد که در آن دوربین‌ها قادر به ضبط محلی روی کارت حافظه تا زمان بازیابی سیستم مرکزی هستند.

فصل سوم

سیستم یکپارچه پایش و واکنش امنیتی در زیرساخت‌های نظارت تصویری

طبقه بندی سند : عمومی
افزایش تاب‌آوری و پایداری سامانه‌های پایش تصویری و الکترونیکی تحت شبکه
بهره برداران : سازمان های خصوصی و دولتی
ویرایش – شماره سند : 1/1 – M0137D0404
تدوین : شرکت مهندسین مشاور موج برتر اندیشه

تشخیص تا پاسخگویی خودکار

پیاده‌سازی یک معماری جامع برای نظارت و پاسخگویی امنیتی در سیستم‌های تصویری نیازمند رویکردی چندلایه و فنی است که تمامی جنبه‌های تشخیص تهدید، تحلیل رفتار و پاسخ به حوادث را پوشش دهد. در این چارچوب، سیستم‌های نظارتی باید به شکلی طراحی شوند که قابلیت یکپارچه‌سازی کامل با مراکز عملیات امنیت(SPR (Security Operations Center را داشته باشند، به طوری که تمامی رویدادهای امنیتی به صورت لحظه‌ای قابل رصد و تحلیل باشند.

در طراحی یک سیستم نظارتی ایمن و هوشمند، باید به دنبال ایجاد چارچوبی یکپارچه بود که از لبه شبکه تا مرکز داده را تحت پوشش امنیتی قرار دهد. این سیستم با بهره‌گیری از آخرین فناوری‌ها، قادر خواهد بود تهدیدات را شناسایی، تحلیل و پاسخ دهد.

در سطح تجهیزات نظارتی مانند دوربین‌های IP و سرورهای ضبط، عامل‌های سبک‌وزنی نصب می‌شوند که به صورت هوشمندانه داده‌های لاگ را جمع‌آوری و پردازش می‌کنند. این عامل‌های پیشرفته با استفاده از پروتکل‌های امنی مانند MQTTSکه با رمزنگاری AES-256 محافظت می‌شوند، ارتباطی ایمن با مرکز عملیات امنیت برقرار می‌کنند. یکی از ویژگی‌های کلیدی این سیستم، توانایی پردازش داده‌ها در محل است که به طور چشمگیری حجم اطلاعات انتقالی را کاهش می‌دهد.

مرکز تحلیل این سیستم بر پایه یک پلتفرم SIEM پیشرفته بنا شده که از قابلیت‌های تحلیل رفتار کاربر و نهاد بهره می‌برد. با استفاده از الگوریتم‌های یادگیری عمیق مانند LSTM و CNN که به طور خاص برای محیط‌های نظارتی آموزش دیده‌اند، سیستم قادر است کوچکترین ناهنجاری‌ها را با دقت بسیار بالا تشخیص دهد. این شامل تغییرات غیرمجاز در تنظیمات، الگوهای دسترسی غیرعادی و انحرافات در ترافیک شبکه می‌شود.

مکانیزم هشداردهی این سیستم به صورت هوشمندانه و مبتنی بر سطح خطر طراحی شده است. برای تهدیدات حیاتی مانند تلاش برای تغییرfirmwar سیستم به صورت خودکار در کمتر از ۵۰۰ میلی‌ثانیه واکنش نشان داده و دستگاه مورد نظر را قرنطینه می‌کند. در مورد تهدیدات با سطح خطر متوسط، سیستم با افزایش میزان لاگ‌گیری و ارسال هشدار به اپراتورها، شرایط را تحت کنترل می‌گیرد.

قابلیت پاسخگویی خودکار SOAR (Security Orchestration, Automation and Response) یکی از ویژگی‌های ممتاز این سیستم است که امکان یکپارچه‌سازی با سایر سیستم‌های امنیتی مانند کنترل دسترسی شبکه را فراهم می‌آورد. این قابلیت به سیستم اجازه می‌دهد در صورت شناسایی تهدید بلافاصله اقدامات متقابل مناسب مانند جداسازی دستگاه‌های آلوده یا بازگردانی تنظیمات امن را انجام دهد.

برای افزایش دقت در تشخیص تهدیدات، از فناوری‌های پیشرفته تحلیل محتوای ویدئویی استفاده شده است. این فناوری‌ها قادرند کوچکترین تغییرات در فریم‌های ویدئویی و فراداده‌های مربوطه را شناسایی کنند که می‌تواند نشانه‌ای از دستکاری تصاویر باشد.

در نهایت، تمام این قابلیت‌ها در قالب یک داشبورد مدیریتی یکپارچه ارائه می‌شود که به اپراتورها این امکان را می‌دهد تا به صورت لحظه‌ای از وضعیت امنیتی تمامی تجهیزات مطلع شوند و در شرایط بحرانی تصمیم‌گیری سریع و آگاهانه داشته باشند. این داشبورد با بهره‌گیری از تکنیک‌های پیشرفته تجسم داده، ارتباط بین رویدادهای مختلف را به وضوح نمایش می‌دهد.

این راهکار جامع نه تنها امنیت سیستم‌های نظارتی را به سطح جدیدی ارتقا می‌دهد، بلکه با کاهش بار عملیاتی تیم‌های امنیتی امکان مدیریت کارآمدتر منابع را فراهم می‌آورد. پیاده‌سازی چنین سیستمی نیازمند توجه به جزئیات فنی و در نظر گرفتن نیازهای خاص هر محیط نظارتی است.

سیستم یکپارچه تحلیل هوشمند تصاویر امنیتی با رویکرد تشخیص تهدیدات پیشرفته

سیستم‌های نظارتی مدرن با بهره‌گیری از فناوری‌های پیشرفته هوش مصنوعی و یادگیری ماشین، تحولی چشمگیر در حوزه امنیت و نظارت ایجاد کرده‌اند. این سیستم‌ها بر اساس یک معماری چندلایه طراحی شده‌اند که ترکیبی از الگوریتم‌های یادگیری عمیق، پردازش تصویر پیشرفته و سیستم‌های تصمیم‌گیری بلادرنگ را در خود جای داده است.

در هسته مرکزی این سیستم‌ها، لایه پردازش تصویر با استفاده از شبکه‌ها و معماری‌های مبتنی بر Transformer عمل می‌کند. این فناوری‌ها امکان استخراج ویژگی‌های پیچیده از جریان‌های ویدئویی را با دقت فریم به فریم فراهم می‌آورند. مدل‌های پیشرفته تشخیص اشیاء در این سیستم‌ها به کار گرفته شده است که قادرند با دقت در شرایط نوری مختلف چندین شیء را همزمان شناسایی و ردیابی کنند.

برای تشخیص رفتارهای مشکوک، از معماری‌های ترکیبی استفاده می‌شود که توانایی تحلیل الگوهای حرکتی در بازه‌های زمانی متوالی را دارند. این سیستم‌ها پس از آموزش بر روی مجموعه داده‌های گسترده از سناریوهای امنیتی، می‌توانند فعالیت‌های غیرعادی مانند حرکت‌های نامتعارف، توقف‌های طولانی در مناطق حساس یا رفتارهای تهاجمی را با نرخ خطای کمتر از ۲٪ تشخیص دهند.

سیستم‌های تشخیص دستکاری دوربین‌ها با تحلیل تغییرات ناگهانی در پارامترهای تصویر مانند تغییرات رنگ، شار نوری و الگوهای حرکت زمینه، قادر به شناسایی دستکاری سخت‌افزاری و نرم‌افزاری مختلف مانند (پوشاندن لنز دوربین- تغییر جهت دوربین- ضربه زدن یا تخریب فیزیکی- قطع کابل‌های ارتباطی- تغییر مکان دوربین- تابش نور شدید به سنسور- استفاده از لیزر برای اختلال در تصویربرداری- تغییر دمای محیط- کاهش عمدی کیفیت تصویر- دسترسی غیرمجاز به تنظیمات دوربین و...) هستند. همچنین، سیستم‌های تشخیص ورود غیرمجاز با ترکیب تکنیک‌های تشخیص چهره پیشرفته و تحلیل رفتاری، حتی در شرایط چالش برانگیز مانند تغییرات نور یا پوشش صورت نیز عملکرد قابل اطمینانی دارند.

مکانیزم هشدار فوری این سیستم‌ها بر اساس معماری رویداد محور طراحی شده که امکان پردازش و واکنش در کمترین زمان را فراهم می‌کند. این سیستم‌ها از طریق API های استاندارد ONVIF و پروتکل‌های امنیتی با پلتفرم‌های مدیریت ویدئویی یکپارچه شده و امکان فعال‌سازی خودکار اقدامات متقابل را ایجاد می‌کنند.

برای حفظ امنیت سایبری، این سیستم‌ها از رمزنگاری سرتاسری AES-256 ، احراز هویت چندعاملی و سیستم‌های تشخیص نفوذ مبتنی بر رفتار استفاده می‌کنند و به‌روزرسانی‌های امنیتی به صورت ماهانه انجام می‌شود. پیاده‌سازی موفق این سیستم‌ها نیازمند سخت‌افزارهای قدرتمندی شامل پردازنده‌های گرافیکی با توان پردازشی بالا، حافظه‌های پرسرعت و سیستم‌های

ذخیره‌سازی All-Flash است. در محیط‌های بزرگ، معماری Edge-to-Cloud با توزیع هوشمند پردازش بین دستگاه‌های لبه و مراکز ابری، بهترین راهکار محسوب می‌شود.

فصل چهارم

راهکارهای پدافند غیرعامل
در حفاظت فیزیکی زیرساخت‌های نظارتی

حفاظت فیزیکی زیرساخت‌ها

برای تأمین امنیت فیزیکی زیرساخت‌های نظارتی، مجموعه‌ای از اقدامات هماهنگ و فنی ضروری است. ابتدا باید تمام تجهیزات حیاتی شامل سرورها، دستگاه‌های DVR/NVR و سوئیچ‌های شبکه در رک‌های استاندارد با قفل‌های الکترونیکی پیشرفته نصب شوند. این قفل‌ها باید مجهز به سیستم‌های احراز هویت چندعاملی شامل کارت‌های هوشمند، کدهای PIN و تشخیص بیومتریک باشند و به یک سیستم مدیریت دسترسی مرکزی متصل شوند تا تمامی ترددها با دقت ثبت گردد.

دوربین‌های نظارتی خارجی نیازمند دارا بودن و یا استفاده از محفظه‌های ضد خرابکاری با استاندارد IK10 هستند که از مواد مستحکم ساخته شده و به سنسورهای حساس به دستکاری مجهز باشند. این سنسورها باید قادر به تشخیص هرگونه ضربه، تغییر موقعیت یا باز شدن غیرمجاز بوده و بلافاصله به سیستم مرکزی هشدار ارسال نمایند. برای تأمین برق پایدار، استفاده از UPS های صنعتی و پنل های خورشیدی با قابلیت پشتیبان‌گیری حداقل ۸ ساعت و ژنراتورهای اضطراری با سیستم راه‌انداز خودکار ضروری است. این سیستم‌های برق باید مجهز به محافظهای ولتاژ چندمرحله‌ای باشند تا از آسیب‌های ناشی از نوسانات برق جلوگیری کنند.

نظارت محیطی مؤثر مستلزم نصب دوربین‌های با کیفیت بالا با قابلیت دید در شب و لنزهای قابل تنظیم است که به سیستم تحلیل تصویر هوشمند متصل باشند. همچنین، شبکه‌ای از سنسورهای دقیق برای پایش دما، رطوبت، نشت آب و لرزش باید در محل استقرار تجهیزات نصب شود. سیستم اطفاء حریق گاز پایدار نیز باید برای محافظت از تجهیزات در برابر آتش‌سوزی طراحی گردد.

کنترل دسترسی فیزیکی باید با استفاده از سیستم‌های پیشرفته شامل احراز هویت چندعاملی و ثبت دقیق ترددها انجام شود. کابل‌کشی شبکه باید از نوع شیلددار با استاندارد بالا انتخاب شده و به سیستم ارتینگ مناسب متصل گردد. برای تجهیزات بسیار حساس، استفاده از محفظه‌های فارادی جهت محافظت در برابر حملات الکترومغناطیسی توصیه می‌شود.

ذخیره‌سازی امن تصاویر نیازمند رمزنگاری پیشرفته داده‌ها با الگوریتم‌های قوی و پیاده‌سازی سیستم پشتیبان‌گیری چندلایه است. نگهداری تصاویر باید برای مدت حداقل ۹۰ روز تضمین شود. اجرای موفق این راهکارها مستلزم بازرسی‌های دوره‌ای، تست منظم سیستم‌ها، به‌روزرسانی مستندات و آموزش مستمر پرسنل است. تمامی این اقدامات باید مطابق با استانداردهای بین‌المللی مربوطه طراحی و اجرا شوند تا بالاترین سطح امنیت فیزیکی برای سیستم‌های نظارتی تأمین گردد.

فصل پنجم

راهکارهای مقابله با حملات سایبری در سیستم‌های نظارتی

✓ حملات Man-in-the-Middle

برای مقابله با این نوع حملات، پیاده‌سازی رمزنگاری پیشرفته در تمامی کانال‌های ارتباطی ضروری است. پروتکل HTTPS باید با نسخه TLS 1.3 یا بالاتر برای ارتباطات وب و احراز هویت دوطرفه پیاده‌سازی شود. برای جریان‌های ویدئویی، پروتکل RTSPباید با لایه امنیتی SRTP همراه شود و از مکانیزم‌های احراز هویت قوی مانند DTLS-SRTP استفاده گردد. همچنین، پیاده‌سازی سیستم مدیریت کلید مرکزی (KMS) برای توزیع و به‌روزرسانی دوره‌ای کلیدهای رمزنگاری توصیه می‌شود.

✓ حملات Denial of Service

مقابله با این حملات نیازمند استراتژی چندلایه است. در سطح شبکه، استفاده از فایروال‌های نسل جدید (NGFW) با قابلیت تشخیص و مسدودسازی الگوهای ترافیک غیرعادی ضروری است. پیاده‌سازی مکانیزم‌های Rate Limiting برای محدود کردن درخواست‌های ورودی به هر دوربین یا سرور ضبط باید انجام شود. استفاده از سرویس‌های mitigation DDoS مبتنی بر ابر نیز برای جذب و فیلتر کردن ترافیک حمله قبل از رسیدن به زیرساخت اصلی توصیه می‌شود. تنظیم timeout های مناسب برای اتصالات و محدود کردن تعداد اتصالات همزمان نیز از دیگر اقدامات مؤثر است.

✓ دستکاری Firmware

برای جلوگیری از این نوع حملات، استفاده از تجهیزاتی که از امضای دیجیتالی firmware پشتیبانی می‌کنند، الزامی است. سیستم باید قابلیت بررسی یکپارچگی firmware در هر بار راه‌اندازی (Secure Boot) و به صورت دوره‌ای در حین کار را داشته باشد. پیاده‌سازی مکانیزم‌های Remote Attestation برای تأیید سلامت firmware دستگاه‌ها از راه دور و استفاده از Trusted Platform Module (TPM) برای ذخیره‌سازی امن کلیدها و اطلاعات حساس نیز توصیه می‌شود. تمامی به‌روزرسانی‌های firmware باید از طریق کانال‌های امن و با احراز هویت قوی انجام پذیرد.

✓ حملات Credential Stuffing

مقابله با این حملات نیازمند استراتژی چندبعدی است. پیاده‌سازی احراز هویت چندعاملی (MFA) برای تمامی حساب‌های مدیریتی اجباری است. سیستم باید سیاست‌های قوی برای رمزهای عبور شامل طول حداقل ۱۲ کاراکتر، ترکیب حروف، اعداد و نمادها، و تغییر دوره‌ای هر ۹۰ روز را اعمال کند. پیاده‌سازی مکانیزم‌های تشخیص ناهنجاری که بتواند الگوهای ورود ناموفق و تلاش‌های غیرعادی را شناسایی کند، ضروری است. استفاده از لیست سیاه برای آدرس‌های IP مشکوک و پیاده‌سازی سیستم‌های CAPTCHA پس از چندین تلاش ناموفق نیز توصیه می‌شود. برای حساب‌های حساس، استفاده از احراز هویت مبتنی بر ریسک (Risk-Based Authentication) که فاکتورهایی مانند موقعیت جغرافیایی، دستگاه و زمان دسترسی را در نظر می‌گیرد می‌تواند مؤثر باشد.

فصل ششم

راهکارهای جامع پایداری سیستم‌های حیاتی در شرایط بحران و جنگ

✓ ارتباطات پایدار و مقاوم

برای تضمین تداوم ارتباطات در شرایط بحرانی، باید یک ساختار چندلایه و خودترمیم طراحی شود. در لایه اول، شبکه‌های رادیویی زمینی با دستگاه‌های چندبانده (VHF/UHF/HF) که از تکنیک‌های پرش فرکانسی با استفاده از رمزنگاری AES-256 امکان ارتباط امن را فراهم می‌کنند. این سیستم‌ها باید قابلیت کار در محیط‌های دارای اختلال الکترونیکی را داشته باشند. در لایه دوم، شبکه‌های مش (Mesh) با معماری خودترمیم شونده، ارتباطات را حتی در صورت آسیب‌دیدگی بخشی از گره‌ها حفظ می‌کنند. لایه سوم شامل ارتباطات ماهواره‌ای با ترمینال‌های VSAT قابل حمل است که مستقل از زیرساخت‌های زمینی عمل می‌کنند. برای نقاط حساس، ارتباطات نقطه به نقطه با فناوری لیزر می‌تواند یک مسیر ارتباطی پرسرعت و غیرقابل رهگیری ایجاد کند. واحدهای ارتباطی سیار در خودروهای مجهز به آنتن‌های مخفی‌شونده نیز امکان جابه‌جایی و استقرار سریع در نقاط مختلف را فراهم می‌کنند.

✓ تامین انرژی پایدار و مطمئن

سیستم‌های حیاتی نیازمند منابع تغذیه کاملاً افزونه با قابلیت کار مداوم هستند. در این ساختار، UPSهای صنعتی از نوع دوسویه (Double Conversion)با قابلیت پشتیبانی حداقل ۸ ساعت به عنوان اولین لایه محافظتی عمل می‌کنند. این دستگاه‌ها باید مجهز به سیستم‌های خنک‌کننده مستقل باشند. لایه بعدی شامل ژنراتورهای دیزلی با پیکربندی ریداندنت (N+1) و مخازن سوخت ۷۲ ساعته است که به سیستم راه‌انداز خودکار مجهز هستند. برای افزایش انعطاف‌پذیری، ترکیب منابع انرژی مختلف مانند پنل‌های خورشیدی با باتری‌های لیتیومی، توربین‌های بادی کوچک و سیستم مدیریت هوشمند انرژی توصیه می‌شود. توزیع جغرافیایی مراکز تأمین برق در چندین موقعیت جداگانه با فاصله مناسب، از قطعی کامل سیستم جلوگیری می‌کند.

✓ زیرساخت سخت‌افزاری مقاوم

معماری سخت‌افزاری باید بر پایه افزونگی کامل طراحی شود که در آن تمام تجهیزات حیاتی به صورت دوبل و مستقل کار می‌کنند. این معماری شامل مسیرهای شبکه کاملاً مجزا از نظر فیزیکی است. استقرار مراکز داده در تاسیسات زیرزمینی با محفظه‌های ضد انفجار و سیستم‌های خنک‌کننده مستقل، مقاومت سیستم را در برابر حملات فیزیکی افزایش می‌دهد. پراکندگی جغرافیایی مراکز داده با حداقل فاصله مناسب از یکدیگر، از آسیب همزمان تمامی ظرفیت‌ها جلوگیری می‌کند. استفاده از تجهیزات نظامی‌شده که استانداردهای سخت‌گیرانه محیطی را رعایت می‌کنند، در محیط‌های خشن ضروری است.

✓ مدیریت بحران و بازیابی

برنامه‌ریزی جامع برای شرایط بحران شامل تدوین سناریوهای مختلف، ایجاد نقشه‌های عملیاتی دقیق و تعیین زنجیره فرماندهی جایگزین است. تمرینات منظم شبیه‌سازی شرایط بحران مانند قطعی ارتباطات یا تخلیه مراکز، آمادگی تیم‌ها را افزایش می‌دهد. از نظر لجستیکی، ایجاد انبارهای پراکنده از قطعات یدکی حیاتی، تهیه کیت‌های تعمیرات سریع و انعقاد قراردادهای تأمین اضطراری با تأمین‌کنندگان متعدد، امکان بازیابی سریع را فراهم می‌کند. سیستم‌های فرماندهی سیار با قابلیت استقرار سریع و واحدهای پشتیبانی فنی متحرک انعطاف‌پذیری عملیاتی را تضمین می‌کنند.

✓ مقابله با تهدیدات خاص

برای محافظت در برابر پالس الکترومغناطیس(EMP) ، نصب محافظ‌های جریان گذرا (TVSS) و پیاده‌سازی سیستم‌های زمین‌کردن پیشرفته ضروری است. در برابر جنگ الکترونیک، سیستم‌های جنگ الکترونیک (ECM) و ضد جنگ الکترونیک (ECCM)همراه با گیرنده‌های طیف گسترده و آنتن‌های تطبیقی هوشمند کارایی ارتباطات رادیویی را حفظ می‌کنند .تکنیک‌های استتار و پنهان‌سازی مانند پوشش‌های جاذب امواج راداری، سیستم‌های کنترل انتشار حرارتی و معماری استتارشونده، احتمال شناسایی و هدفگیری تجهیزات را کاهش می‌دهند.

آموزش مستمر پرسنل در دوره‌های تخصصی شرایط بحران و برگزاری تمرینات میدانی منظم و ارزیابی دوره‌ای توانمندی‌ها، عامل انسانی این سیستم‌های پیچیده را آماده نگه می‌دارد. این راهکارها باید به صورت یکپارچه و با در نظر گرفتن شرایط خاص هر سازمان پیاده‌سازی شوند تا حداکثر سطح آمادگی در برابر تهدیدات مختلف ایجاد شود.

پیوست

چک لیست های عملیاتی

طبقه بندی سند : **عمومی**

افزایش تاب‌آوری و پایداری سامانه‌های پایش تصویری و الکترونیکی تحت شبکه	بهره برداران : سازمان های خصوصی و دولتی
ویرایش – شماره سند : M0137D0404 – 1/1	تدوین : شرکت مهندسین مشاور موج برتر اندیشه

امنیت شبکه و زیرساخت				
اقدام امنیتی	مسئول اجرا	تاریخ اجرا	وضعیت	توضیحات
ایجاد VLAN اختصاصی				
تفکیک فیزیکی سرورها				
تفکیک فیزیکی سوئیچ‌های نظارتی				
تنظیم ACL بین VLAN ها				
نصب فایروال NGFW				
مسدودسازی پروتکل‌های ناامن (Telnet/FTP/HTTP)				
مستندسازی کامل معماری شبکه				
امنیت سخت‌افزار و نرم‌افزار				
اقدام امنیتی	**مسئول اجرا**	**تاریخ اجرا**	**وضعیت**	**توضیحات**
تغییر گذرواژه‌های پیش‌فرض				
غیرفعال‌سازی سرویس‌های غیرضروری				
به‌روزرسانی firmware				
فعال‌سازی Secure Boot				
نصب آخرین وصله‌های امنیتی				
فعال‌سازی لاگ‌گیری جامع				
ثبت اطلاعات سخت‌افزاری در CMDB				
مدیریت دسترسی و رمزنگاری				
اقدام امنیتی	**مسئول اجرا**	**تاریخ اجرا**	**وضعیت**	**توضیحات**
پیاده‌سازی MFA				
استقرار RBAC				
فعال‌سازی TLS 1.3				
پیاده‌سازی SRTP				
رمزنگاری بکاپ‌های ویدئویی				
مانیتورینگ و پاسخگویی				
اقدام امنیتی	**مسئول اجرا**	**تاریخ اجرا**	**وضعیت**	**توضیحات**
راه‌اندازی سیستم ثبت وقایع				
یکپارچه‌سازی با SIEM				
تدوین برنامه پاسخ به حوادث				
امنیت فیزیکی				

طبقه بندی سند : عمومی
افزایش تاب‌آوری و پایداری سامانه‌های پایش تصویری و الکترونیکی تحت شبکه
بهره برداران : سازمان های خصوصی و دولتی
ویرایش – شماره سند : 1/1 – M0137D0404
تدوین : شرکت مهندسین مشاور موج برتر اندیشه

اقدام امنیتی	مسئول اجرا	تاریخ اجرا	وضعیت	توضیحات
نصب رک‌های قفل‌دار				
استفاده از محفظه‌های ضد خرابکاری				
تأمینUPS				
شبیه‌سازی حملات				
آموزش و آگاهی				
اقدام امنیتی	**مسئول اجرا**	**تاریخ اجرا**	**وضعیت**	**توضیحات**
ارزیابی دانش امنیتی کارکنان				
برگزاری دوره آموزشی				
آموزش آگاهی امنیتی پرسنل				
آموزش اپراتورهای سیستم نظارتی				

ارتباطات پایدار				
اقدام امنیتی	مسئول اجرا	تاریخ اجرا	وضعیت	توضیحات
پیاده‌سازی شبکه رادیویی چندبانده (VHF/UHF/HF)با رمزنگاریAES-256				
فعال‌سازی قابلیت پرش فرکانسی (FHSS) در دستگاه‌های ارتباطی				
استقرار شبکه مش (Mesh) خودترمیم‌شونده				
راه‌اندازی سیستم ارتباطات ماهواره‌ای قابل حمل				
تجهیز واحدهای سیار به سیستم‌های ارتباطی مخفی‌شونده				
ایجاد مسیرهای ارتباطی لیزری نقطه به نقطه برای نقاط حساس				
نصب آنتن‌های تطبیقی هوشمند برای مقابله با جنگ الکترونیک				
تامین انرژی				
اقدام امنیتی	**مسئول اجرا**	**تاریخ اجرا**	**وضعیت**	**توضیحات**
نصب UPS صنعتی دوسویه با ۸ ساعت پشتیبانی				
راه‌اندازی ژنراتورهای دیزلی ریداندنت				
تامین مخازن سوخت ۷۲ ساعته				
استقرار سیستم مدیریت هوشمند انرژی				
نصب پنل‌های خورشیدی با باتری‌های لیتیومی				
راه‌اندازی توربین‌های بادی کوچک مقیاس				
ایجاد توزیع جغرافیایی مراکز تامین برق				
زیرساخت سخت‌افزاری				
اقدام امنیتی	**مسئول اجرا**	**تاریخ اجرا**	**وضعیت**	**توضیحات**
پیاده‌سازی معماری ریداندنت کامل				
ایجاد مسیرهای شبکه کاملاً مستقل فیزیکی				
استقرار مراکز داده زیرزمینی				
راه‌اندازی سیستم‌های خنک‌کننده مستقل				
پراکندگی جغرافیایی مراکز داده				
استفاده از تجهیزات نظامی‌شده استاندارد				
مدیریت بحران				
اقدام امنیتی	**مسئول اجرا**	**تاریخ اجرا**	**وضعیت**	**توضیحات**
تدوین سناریوهای مختلف بحران				
ایجاد نقشه‌های عملیاتی دقیق				

تعیین زنجیره فرماندهی جایگزین				
راه‌اندازی سیستم فرماندهی سیار				
ایجاد انبارهای پراکنده قطعات یدکی				
تهیه کیت‌های تعمیرات سریع				
مقابله با تهدیدات خاص				
اقدام امنیتی	**مسئول اجرا**	**تاریخ اجرا**	**وضعیت**	**توضیحات**
راه‌اندازی سیستم‌های محافظ جریان گذرا				
پیاده‌سازی زمین‌کردن پیشرفته				
نصب گیرنده‌های طیف گسترده				
استفاده از پوشش‌های جاذب امواج راداری				
راه‌اندازی سیستم کنترل انتشار حرارتی				

شرکت مهندسین مشاور موج برتر اندیشه

افزایش تاب‌آوری و پایداری سامانه‌های پایش تصویری و الکترونیکی تحت شبکه

تیر ماه ۱۴۰۴