نشریه تخصصی

سا پنا

نشریه‌ای برای مدیران،
متخصصان و تصمیم‌سازان
حوزه امنیت، فناوری اطلاعات
و زیرساخت

فناوری اطلاعات | امنیت | زیرساخت | نظارت تصویری

شماره ۶
تیرماه ۱۴۰۵

حکمرانی امنیت

تصمیم‌سازی
هوشمند

حکمرانی امنیت؛
از تجهیزات تا تصمیم‌سازی

امنیت زمانی ارزش‌آفرین می‌شود که از سطح فناوری به سطح حکمرانی ارتقا یابد.

در این شماره می خوانید

حکمرانی امنیت چیست و چرا مدیران باید آن را بشناسند؟

امنیت اطلاعات از اتاق هیئت‌مدیره آغاز می‌شود نه از خرید تجهیزات

چرا برخی سازمان‌ها با وجود تجهیزات پیشرفته همچنان ناامن هستند؟

حکمرانی امنیت؛ از تجهیزات تا تصمیم‌سازی

امنیت زمانی ارزش‌آفرین می‌شود که از سطح فناوری به سطح حکمرانی ارتقا یابد

به قلم اسماعیل اکبری

مدیرعامل شرکت شبکه گستر ساینا

در سال‌های گذشته، صنعت امنیت شاهد تحولات چشمگیری بوده است. سازمان‌ها میلیاردها تومان برای خرید دوربین‌های مداربسته، سامانه‌های کنترل تردد، تجهیزات شبکه، مراکز داده و راهکارهای امنیت سایبری سرمایه‌گذاری کرده‌اند. با این حال، تجربه بسیاری از حوادث و بحران‌ها نشان داده است که وجود تجهیزات به‌تنهایی تضمین‌کننده امنیت نیست.

آنچه امروز میان سازمان‌های تاب‌آور و سازمان‌های آسیب‌پذیر تفاوت ایجاد می‌کند، نه صرفاً کیفیت تجهیزات، بلکه کیفیت تصمیم‌گیری است.

در ادبیات نوین مدیریت، مفهوم «حکمرانی امنیت» به عنوان یکی از ارکان اصلی پایداری سازمانی مطرح شده است. حکمرانی امنیت به معنای ایجاد ساختاری است که در آن سیاست‌ها، فرآیندها، مسئولیت‌ها و ابزارهای امنیتی در راستای اهداف کلان سازمان همسو شوند. در چنین رویکردی، امنیت دیگر یک پروژه یا یک واحد سازمانی نیست؛ بلکه بخشی از نظام تصمیم‌سازی و مدیریت ریسک سازمان محسوب می‌شود.

بسیاری از سازمان‌ها دارای تجهیزات پیشرفته هستند اما فاقد نقشه راه امنیتی‌اند. در مقابل، سازمان‌هایی که امنیت را در سطح راهبردی مدیریت می‌کنند، قادرند تهدیدات را پیش از وقوع شناسایی کرده، منابع خود را بهینه تخصیص دهند و در شرایط بحران تصمیم‌های مؤثرتری اتخاذ کنند.

امروزه مرز میان امنیت فیزیکی و امنیت سایبری نیز به سرعت در حال از بین رفتن است. یک دوربین مداربسته، یک سامانه کنترل دسترسی یا حتی یک سنسور هوشمند، بخشی از یک اکوسیستم متصل به شبکه هستند. به همین دلیل، مدیریت جزیره‌ای سامانه‌ها دیگر پاسخگوی نیازهای سازمان‌های مدرن نیست و ضرورت نگاه یکپارچه بیش از هر زمان دیگری احساس می‌شود.

حکمرانی امنیت، مدیران را از سطح خرید تجهیزات به سطح مدیریت ریسک، تاب‌آوری و آینده‌نگری ارتقا می‌دهد. این رویکرد کمک می‌کند تا سرمایه‌گذاری‌های امنیتی نه به عنوان یک هزینه اجتناب‌ناپذیر، بلکه به عنوان ابزاری برای حفظ سرمایه‌های سازمان، تداوم کسب‌وکار و ایجاد مزیت رقابتی دیده شوند.

در این شماره از نشریه ساینا تلاش کرده‌ایم ابعاد مختلف حکمرانی امنیت را بررسی کنیم؛ از نقش سیاست‌گذاری و مدیریت ریسک گرفته تا همگرایی امنیت فیزیکی و سایبری، استانداردهای نوین و الزامات سازمان‌های آینده‌نگر.

باور داریم آینده متعلق به سازمان‌هایی است که امنیت را نه در تجهیزات، بلکه در کیفیت تصمیم‌های خود جست‌وجو می‌کنند.

ناشر :
شرکت شبکه گستر ساینا
www.SainaSoft.com

سردبیر :
اسماعیل اکبری
Akbari@SainaSoft.com

وب سایت :
www.SainaMag.ir

تلفن :
۰۲۶ ۳۲۶۲۰۰۰۰

مجوز های اخذ شده توسط شبکه گستر ساینا

سازمان نظام صنفی رایانه‌ای کشور
انجمن انفورماتیک ایران
سازمان برنامه و بودجه کشور
وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران
وزارت نفت
سازمان آموزش فنی و حرفه‌ای کشور
جمهوری اسلامی ایران
وزارت صنعت، معدن و تجارت
سازمان تنظیم مقررات و ارتباطات رادیویی

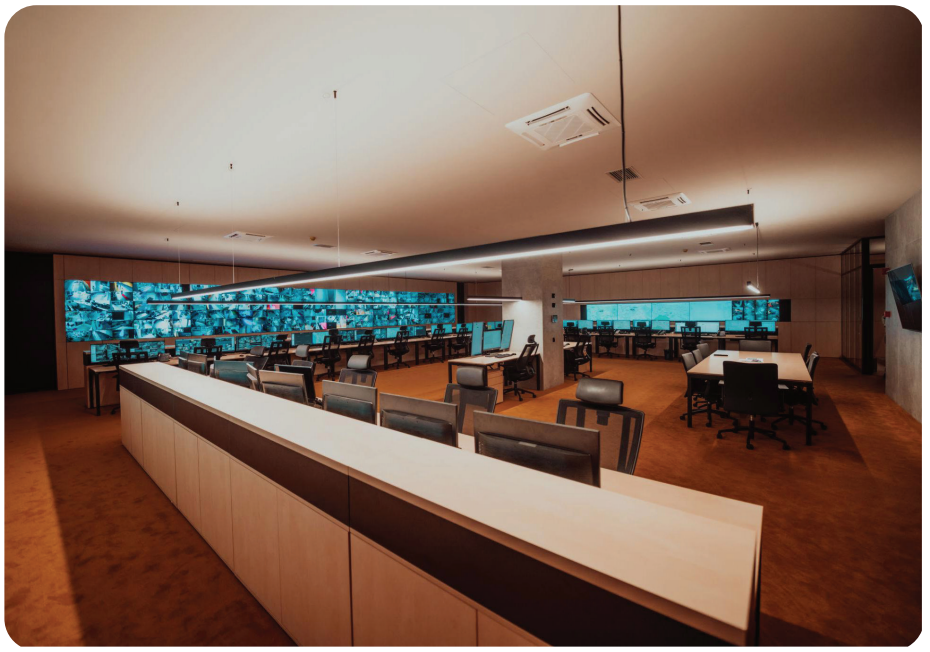
ساینا

ساینا روایت نگاهی مهندسی و سیستماتیک به فناوری اطلاعات، امنیت، زیرساخت و ایمنی در پروژه‌های صنعتی و سازمانی است؛ نگاهی که بر این باور است فناوری زمانی ارزش‌آفرین خواهد بود که به‌صورت یکپارچه طراحی شود، بر تحلیل مهندسی استوار باشد و در خدمت ایمنی، پایداری و تصمیم‌سازی آگاهانه قرار گیرد. شرکت شبکه‌گستر ساینا، به‌عنوان طراح، مشاور و ناظر پروژه‌های فناوری، نظارت تصویری و زیرساخت، تلاش کرده است با گردهم‌آوردن مجموعه‌ای از شرکت‌های تخصصی و هم‌سو، تصویری واقع‌بینانه از الزامات فنی، امنیتی و اجرایی پروژه‌های حیاتی ارائه دهد؛ تصویری که در آن امنیت و پایداری، حاصل طراحی صحیح، تصمیم‌سازی آگاهانه و نظارت حرفه‌ای است، نه محصول انتخاب‌های مقطعی و واکنشی.

این ویژه‌نامه نیز با همین رویکرد منتشر شده است؛ دعوتی به بازنگری در شیوه مواجهه با فناوری و پروژه‌های حساس. رویکردی که به‌جای راهکارهای جزیره‌ای، بر معماری یکپارچه، استانداردمحور و آینده‌نگر تأکید دارد و فناوری را نه هدفی مستقل، بلکه ابزاری برای ارتقای کیفیت تصمیم‌گیری، کاهش ریسک و تضمین موفقیت پروژه‌ها می‌داند.

چرا برخی سازمان‌ها با وجود تجهیزات پیشرفته همچنان ناامن هستند؟

بررسی فاصله میان خرید تجهیزات و ایجاد امنیت واقعی



در سال‌های اخیر بسیاری از سازمان‌ها سرمایه‌گذاری قابل توجهی در حوزه امنیت فیزیکی و الکترونیکی انجام داده‌اند. خرید دوربین‌های مداربسته پیشرفته، سامانه‌های کنترل تردد، تجهیزات ذخیره‌سازی، سیستم‌های تشخیص نفوذ و فناوری‌های مبتنی بر هوش مصنوعی به بخشی از برنامه‌های توسعه زیرساخت امنیتی تبدیل شده است. با این حال، بررسی رخدادهای امنیتی نشان می‌دهد که وجود تجهیزات پیشرفته الزاماً به معنای امنیت بیشتر نیست.

این موضوع یک پرسش مهم را مطرح می‌کند: چرا برخی سازمان‌ها با وجود برخورداری از بهترین تجهیزات، همچنان در معرض تهدیدات امنیتی قرار دارند؟

امنیت؛ حاصل یک اکوسیستم است

یکی از اشتباهات رایج در سازمان‌ها، نگاه تجهیزمحور به امنیت است. در این رویکرد تصور می‌شود که با خرید گران‌ترین تجهیزات، امنیت تأمین خواهد شد؛ در حالی که تجهیزات تنها یکی از اجزای زنجیره امنیت هستند.

امنیت واقعی زمانی شکل می‌گیرد که فناوری، فرآیندها، نیروی انسانی و مدیریت ریسک در کنار یکدیگر قرار گیرند. ضعف در هر یک از این بخش‌ها می‌تواند کل ساختار امنیتی را با چالش مواجه کند.

دوربین‌های زیاد، نظارت کم

در بسیاری از پروژه‌ها تعداد زیادی دوربین نصب می‌شود اما فرآیند مؤثری برای پایش تصاویر وجود ندارد. گاهی اپراتورها آموزش کافی ندیده‌اند، گاهی حجم تصاویر فراتر از توان نظارت انسانی است و در برخی موارد نیز سازوکار مشخصی برای واکنش به هشدارها تعریف نشده است.

در چنین شرایطی سازمان حجم زیادی داده تولید می‌کند، بدون آنکه بتواند از آن برای پیشگیری یا مدیریت حوادث استفاده کند. ثبت تصاویر با مدیریت امنیت تفاوت دارد.

حلقه گمشده؛ فرآیندهای امنیتی

حتی پیشرفته‌ترین تجهیزات نیز بدون فرآیندهای مشخص اثربخشی محدودی دارند.

برای مثال:

* در صورت مشاهده یک رخداد مشکوک چه اقدامی باید انجام شود؟
* مسئول تصمیم‌گیری چه کسی است؟
* چه مدت زمانی برای واکنش تعریف شده است؟
* اطلاعات چگونه مستندسازی و آرشیو می‌شوند؟

اگر پاسخ روشنی برای این پرسش‌ها وجود نداشته باشد، تجهیزات صرفاً نقش ثبت‌کننده رویدادها را ایفا خواهند کرد.

عامل انسانی؛ مهم‌ترین نقطه قوت و ضعف

بخش قابل توجهی از رخدادهای امنیتی ناشی از خطاهای انسانی است. استفاده از رمزهای عبور ضعیف، بی‌توجهی به هشدارها یا رعایت نکردن دستورالعمل‌های امنیتی می‌تواند اثربخشی پیشرفته‌ترین سامانه‌ها را کاهش دهد.

به همین دلیل سازمان‌های موفق، همزمان با توسعه زیرساخت‌های فنی، بر آموزش مستمر کارکنان نیز سرمایه‌گذاری می‌کنند. فرهنگ امنیتی قوی، مکمل فناوری است.

نگهداری؛ بخش فراموش‌شده امنیت

بسیاری از سازمان‌ها برای خرید تجهیزات بودجه مناسبی اختصاص می‌دهند اما برنامه مشخصی برای نگهداری و پشتیبانی ندارند. در نتیجه بخشی از دوربین‌ها از مدار خارج می‌شوند، تجهیزات ذخیره‌سازی دچار مشکل می‌شوند یا نرم‌افزارها بدون به‌روزرسانی باقی می‌مانند.

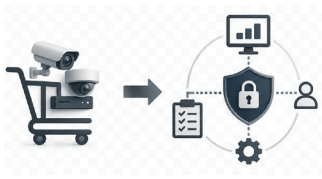
در چنین شرایطی سازمان تصور می‌کند تحت پوشش امنیتی قرار دارد، در حالی که بخشی از زیرساخت عملاً کارایی خود را از دست داده است. امنیت یک پروژه نیست؛ یک فرآیند دائمی است.

نبود نگاه مبتنی بر ریسک

تمام دارایی‌ها و نقاط یک سازمان ارزش یکسانی ندارند. با این حال در بسیاری از پروژه‌ها تجهیزات بدون ارزیابی ریسک و صرفاً بر اساس الگوهای عمومی نصب می‌شوند.

طراحی امنیتی حرفه‌ای باید بر پایه شناسایی تهدیدات، تحلیل آسیب‌پذیری‌ها و تعیین اولویت‌های حفاظتی انجام شود؛ در غیر این صورت منابع در نقاط کم‌اهمیت هزینه شده و بخش‌های حیاتی همچنان در معرض خطر باقی می‌مانند.

از خرید تجهیزات تا معماری امنیت



تجربه نشان داده است که موفق‌ترین سازمان‌ها امنیت را نه به‌عنوان یک محصول، بلکه به‌عنوان یک معماری یکپارچه مدیریت می‌کنند. در این رویکرد تجهیزات، نرم‌افزارها، نیروی انسانی، فرآیندها و مدیریت ریسک به‌صورت هماهنگ عمل می‌کنند.

امروزه دیگر نمی‌توان امنیت را صرفاً با تعداد دوربین‌ها یا قیمت تجهیزات سنجید. فاصله قابل توجهی میان «خرید تجهیزات» و «ایجاد امنیت واقعی» وجود دارد؛ فاصله‌ای که تنها با ترکیب فناوری، فرآیندهای استاندارد، نیروی انسانی آموزش‌دیده، نگهداری مستمر و مدیریت هوشمند ریسک پر می‌شود.

در دنیایی که تهدیدات هر روز پیچیده‌تر می‌شوند، مزیت سازمان‌ها تنها در داشتن تجهیزات پیشرفته نیست؛ بلکه در توانایی تبدیل این تجهیزات به یک سامانه امنیتی یکپارچه و کارآمد نهفته است. به همین دلیل، موفق‌ترین پروژه‌های امنیتی نه با خرید یک فناوری جدید، بلکه با طراحی صحیح، مدیریت مؤثر و نگاه بلندمدت به مقوله امنیت آغاز می‌شوند.

HPE

سرور و تجهیزات شبکه

Professional Server & Network Solutions

- Reliable Performance
- Scalable Solutions
- Secure Infrastructure
- Intelligent Management

Power Your Business with HPE

02632620000

www.SainaSoft.com

پایش رویدادها

مجمع عمومی عادی سالیانه اتحادیه سراسری شرکت‌های فنی و مهندسی حفاظت الکترونیک و شبکه‌های ایمنی در اوایل تیرماه ۱۴۰۵ برگزار می‌شود.

به گزارش روابط عمومی اتحادیه سراسری شرکت‌های فنی و مهندسی حفاظت الکترونیک و شبکه‌های ایمنی، مجمع عمومی عادی سالیانه این اتحادیه با حضور اعضای محترم، مدیران شرکت‌های عضو، فعالان صنعت و نمایندگان بخش‌های مرتبط در اوایل تیرماه سال ۱۴۰۵ برگزار خواهد شد.

این مجمع در چارچوب مفاد اساسنامه اتحادیه و با هدف بررسی عملکرد سال گذشته، ارائه گزارش فعالیت‌های هیئت‌مدیره و بازرس، بررسی و تصویب صورت‌های مالی، تشریح برنامه‌ها و راهبردهای پیش‌رو و همچنین بررسی مهم‌ترین موضوعات و چالش‌های صنعت حفاظت الکترونیک و شبکه‌های ایمنی برگزار می‌شود.

بر اساس اعلام اتحادیه، در این نشست گزارشی از اقدامات انجام‌شده در حوزه‌های مختلف از جمله توسعه تعاملات صنفی، پیگیری مطالبات اعضا، حمایت از کسب‌وکارهای فعال در صنعت، برگزاری دوره‌های آموزشی و توانمندسازی نیروی انسانی، توسعه همکاری‌های بین‌بخشی و برنامه‌های اجرایی سال آینده ارائه خواهد شد.

همچنین اعضای اتحادیه فرصت خواهند داشت دیدگاه‌ها، پیشنهادها و مطالبات خود را در خصوص مسائل صنفی، چالش‌های موجود و راهکارهای توسعه فعالیت‌های اتحادیه مطرح کرده و در فرآیند تصمیم‌سازی و تصمیم‌گیری‌های آتی مشارکت کنند.

اتحادیه سراسری شرکت‌های فنی و مهندسی حفاظت الکترونیک و شبکه‌های ایمنی از تمامی اعضای محترم دعوت کرده است با برنامه‌ریزی مناسب، در این مجمع حضور فعال داشته باشند. زمان دقیق برگزاری، محل تشکیل جلسه، دستور کار و سایر اطلاعات تکمیلی متعاقباً از طریق پایگاه اطلاع‌رسانی رسمی اتحادیه و کانال‌های ارتباطی آن اعلام خواهد شد.

حضور و مشارکت اعضا در مجمع عمومی سالیانه، زمینه‌ساز تقویت همگرایی صنفی، ارتقای جایگاه صنعت حفاظت الکترونیک و شبکه‌های ایمنی و تحقق اهداف و برنامه‌های اتحادیه در سال پیش‌رو خواهد بود.

آزمون احراز صلاحیت مشاوران فناوری اطلاعات به‌صورت سراسری و الکترونیکی در روز پنجشنبه ۸ مردادماه ۱۴۰۵ برگزار خواهد شد.

بر اساس اعلام مراجع برگزارکننده، این آزمون با هدف ارزیابی توانمندی‌های تخصصی و احراز صلاحیت حرفه‌ای مشاوران حوزه فناوری اطلاعات در سطح کشور برگزار می‌شود و متقاضیان می‌توانند در بازه زمانی تعیین‌شده نسبت به ثبت‌نام اقدام کنند.

فرآیند ثبت‌نام از روز چهارشنبه ۱۳ خردادماه ۱۴۰۵ آغاز شده و تا روز چهارشنبه ۲۴ تیرماه ۱۴۰۵ ادامه خواهد داشت. بر اساس ضوابط اعلام‌شده، هر داوطلب مجاز است حداکثر در دو رشته تخصصی ثبت‌نام کند.

هزینه ثبت‌نام برای شرکت در یک رشته ۱۲ میلیون ریال و برای دو رشته ۱۸ میلیون ریال تعیین شده است.

رشته‌های پیش‌بینی‌شده برای این دوره از آزمون شامل نرم‌افزار، زیرساخت و شبکه، مشاوره مدیریت و تحول دیجیتال، هوش مصنوعی و تحلیل داده و پایش و نظارت تصویری است.

برگزارکنندگان این آزمون با تأکید بر اهمیت توسعه نظام حرفه‌ای مشاوره در حوزه فناوری اطلاعات، از تمامی واجدان شرایط دعوت کرده‌اند تا در مهلت مقرر نسبت به ثبت‌نام و تکمیل فرآیند پذیرش اقدام کنند.

این آزمون در شرایطی برگزار می‌شود که نیاز روزافزون سازمان‌ها و کسب‌وکارها به خدمات تخصصی مشاوره فناوری اطلاعات، ضرورت ارزیابی و تأیید صلاحیت حرفه‌ای فعالان این حوزه را بیش از پیش نمایان ساخته است و برگزاری چنین آزمون‌هایی می‌تواند نقش مؤثری در ارتقای کیفیت خدمات مشاوره‌ای و توسعه استانداردهای حرفه‌ای صنعت فناوری اطلاعات کشور ایفا کند.

کمیسیون پایش تصویری نصر؛ نقطه عطفی در آینده صنعت امنیت و نظارت تصویری ایران

به قلم : اسماعیل اکبری

عضو کمیسیون پایش تصویری نصر

از بازار تجهیزات تا اکوسیستم هوشمند امنیت

صنعت پایش تصویری در ایران طی دو دهه گذشته مسیر تحولِ قابل توجهی را پشت سر گذاشته است. سامانه‌هایی که روزی صرفاً برای ثبت و بازبینی تصاویر مورد استفاده قرار می‌گرفتند، امروز به بخشی از زیرساخت‌های حیاتی کشور در حوزه امنیت، مدیریت بحران، حفاظت از دارایی‌ها و حتی تصمیم‌سازی مدیریتی تبدیل شده‌اند.

به‌عنوان یکی از اعضای کمیسیون پایش تصویری سازمان نظام صنفی رایانه‌ای کشور، معتقدم تشکیل این کمیسیون را باید یکی از مهم‌ترین اتفاقات تخصصی سال‌های اخیر در حوزه امنیت و نظارت تصویری دانست. اتفاقی که می‌تواند زمینه‌ساز ارتقای استانداردها، توسعه دانش فنی و شکل‌گیری نگاه حرفه‌ای‌تر به این صنعت در کشور باشد.

ضرورت ایجاد یک مرجع تخصصی

یکی از چالش‌های همیشگی صنعت پایش تصویری در ایران، نبود یک مرجع تخصصی برای هم‌افزایی فعالان این حوزه بوده است. طی سال‌های گذشته شرکت‌های متعددی در زمینه طراحی، اجرا، تأمین تجهیزات و ارائه خدمات فعالیت کرده‌اند، اما نبود استانداردهای یکپارچه و چارچوب‌های مشخص باعث شده کیفیت پروژه‌ها در بخش‌های مختلف کشور تفاوت قابل توجهی داشته باشد.

در بسیاری از پروژه‌ها، نگاه غالب بر انتخاب تجهیزات و کاهش هزینه‌های اولیه متمرکز بوده و موضوعاتی همچون امنیت سایبری، قابلیت توسعه، کیفیت ذخیره‌سازی اطلاعات، نگهداری بلندمدت و بهره‌گیری از فناوری‌های نوین کمتر مورد توجه قرار گرفته است. از نگاه من، یکی از مهم‌ترین مأموریت‌های کمیسیون پایش تصویری ایجاد بستری برای تبادل تجربه، تدوین الزامات تخصصی و ارتقای سطح دانش فنی فعالان این صنعت است؛ موضوعی که می‌تواند به افزایش کیفیت پروژه‌ها و کاهش چالش‌های اجرایی در آینده منجر شود.

صنعتی که دیگر فقط دوربین نیست

واقعیت این است که صنعت پایش تصویری امروز دیگر صنعت «دوربین» نیست؛ بلکه صنعت «داده» است.

هر دوربین به یک حسگر تولید اطلاعات تبدیل شده و روزانه حجم عظیمی از داده‌های تصویری در سازمان‌ها، صنایع، فرودگاه‌ها، بانک‌ها، مراکز درمانی و زیرساخت‌های حیاتی کشور تولید می‌شود. ارزش واقعی این داده‌ها زمانی مشخص می‌شود که بتوان آن‌ها را پردازش، تحلیل و به اطلاعات کاربردی تبدیل کرد.

فناوری‌هایی نظیر تحلیل هوشمند تصاویر، تشخیص چهره، تشخیص پلاک خودرو، شناسایی رفتارهای مشکوک، تحلیل ازدحام جمعیت و مدیریت هوشمند رخدادها امروز به بخش جدایی‌ناپذیر سامانه‌های نظارتی تبدیل شده‌اند.

این تحول موجب شده است متخصصان حوزه پایش تصویری علاوه بر دانش تجهیزات و شبکه، با مفاهیمی مانند هوش مصنوعی، امنیت اطلاعات، ذخیره‌سازی داده، مراکز داده و رایانش ابری نیز آشنا باشند. آینده این صنعت در گرو تلفیق این فناوری‌ها با یکدیگر خواهد بود.

نقش کمیسیون در استانداردسازی و توسعه بازار

یکی از مهم‌ترین نیازهای صنعت پایش تصویری کشور، حرکت به سمت استانداردسازی فنی و اجرایی است. در بسیاری از کشورهای توسعه‌یافته، استانداردهای مشخصی برای طراحی، نصب، بهره‌برداری و نگهداری سامانه‌های نظارتی وجود دارد که موجب افزایش کیفیت پروژه‌ها و کاهش هزینه‌های بلندمدت می‌شود.

کمیسیون پایش تصویری نصر می‌تواند با بهره‌گیری از ظرفیت شرکت‌های تخصصی، دانشگاه‌ها، مراکز پژوهشی و نهادهای مرتبط، زمینه تدوین چنین استانداردهایی را فراهم کند. این موضوع به‌ویژه در پروژه‌های حساس و زیرساختی که کوچک‌ترین ضعف می‌تواند پیامدهای امنیتی قابل توجهی ایجاد کند، اهمیت ویژه‌ای دارد.

از سوی دیگر، این کمیسیون می‌تواند نقش مؤثری در ایجاد ارتباط سازنده میان بخش خصوصی، دستگاه‌های اجرایی و نهادهای تصمیم‌گیر ایفا کند و زمینه توسعه بازارهای تخصصی و رقابت حرفه‌ای‌تر را فراهم آورد.

فرصت‌های جدید برای شرکت‌های تخصصی

تشکیل کمیسیون پایش تصویری تنها یک اقدام صنفی نیست؛ بلکه فرصتی ارزشمند برای شرکت‌های حرفه‌ای فعال در این حوزه محسوب می‌شود.

شرکت‌هایی که توان ارائه راهکارهای جامع شامل مشاوره، طراحی، اجرا، پشتیبانی، امنیت سایبری و تحلیل هوشمند داده‌های تصویری را دارند، می‌توانند نقش مهمی در شکل‌دهی آینده این صنعت ایفا کنند. امروز دیگر موفقیت در بازار صرفاً به فروش تجهیزات وابسته نیست؛ بلکه توانایی ارائه راهکارهای یکپارچه و پایدار، مزیت رقابتی اصلی شرکت‌ها محسوب می‌شود.

آینده‌ای مبتنی بر هوش مصنوعی و امنیت یکپارچه

مسیر آینده صنعت پایش تصویری به‌وضوح مشخص است. سامانه‌های نظارتی در حال حرکت به سمت هوشمندسازی کامل هستند و بخش قابل توجهی از فرآیندهای امنیتی در سال‌های آینده توسط الگوریتم‌های تحلیل تصویر و سامانه‌های مبتنی بر هوش مصنوعی انجام خواهد شد.

در این مسیر، سازمان‌هایی موفق خواهند بود که بتوانند میان پایش تصویری، امنیت سایبری، هوش مصنوعی، مراکز داده و مدیریت ریسک ارتباطی یکپارچه ایجاد کنند. کمیسیون پایش تصویری نصر نیز می‌تواند نقش مهمی در آماده‌سازی صنعت کشور برای ورود به این نسل جدید از فناوری‌ها داشته باشد.

تشکیل این کمیسیون را باید آغاز فصلی تازه در صنعت امنیت و نظارت تصویری ایران دانست؛ فصلی که در آن استانداردسازی، نوآوری، آموزش و همکاری حرفه‌ای جایگزین رویکردهای پراکنده گذشته خواهد شد. آینده این صنعت متعلق به سازمان‌ها و شرکت‌هایی است که امنیت را نه یک محصول، بلکه یک راهبرد پایدار برای حفاظت از سرمایه‌ها، زیرساخت‌ها و دارایی‌های ملی می‌دانند.

حکمرانی امنیت چیست و چرا مدیران باید آن را بشناسند؟

مفاهیم، چارچوب‌ها و نقش مدیریت ارشد در امنیت سازمان

در بسیاری از سازمان‌ها، امنیت همچنان یک موضوع فنی تلقی می‌شود و مسئولیت آن به واحد فناوری اطلاعات یا حراست سپرده می‌شود. اما تجربه سازمان‌های پیشرو نشان می‌دهد امنیت تنها یک مسئله فنی نیست؛ بلکه موضوعی راهبردی است که باید در سطح مدیریت ارشد مورد توجه قرار گیرد.

به همین دلیل مفهوم «حکمرانی امنیت» در سال‌های اخیر به یکی از ارکان مهم مدیریت سازمانی تبدیل شده است. این رویکرد به سازمان‌ها کمک می‌کند امنیت را نه صرفاً به‌عنوان مجموعه‌ای از تجهیزات و فناوری‌ها، بلکه به‌عنوان بخشی از نظام تصمیم‌گیری و مدیریت ریسک در نظر بگیرند.

حکمرانی امنیت؛ فراتر از مدیریت امنیت

مدیریت امنیت بر اجرای اقدامات روزمره، کنترل تهدیدات و پاسخ به حوادث تمرکز دارد، اما حکمرانی امنیت در سطح بالاتری قرار گرفته و سیاست‌ها، مسئولیت‌ها، اهداف و سازوکارهای نظارت را تعیین می‌کند. به بیان ساده، مدیریت امنیت مشخص می‌کند «چگونه امنیت را اجرا کنیم» و حکمرانی امنیت پاسخ می‌دهد «چرا و با چه اولویتی امنیت را مدیریت کنیم».

چرا مدیران باید درگیر امنیت باشند؟

امروزه رخدادهای امنیتی می‌توانند به توقف عملیات، خسارت مالی، آسیب به اعتبار سازمان و از دست رفتن اعتماد ذی‌نفعان منجر شوند. به همین دلیل تصمیمات مرتبط با بودجه، مدیریت ریسک و سرمایه‌گذاری‌های امنیتی باید در سطح مدیریت ارشد مورد توجه قرار گیرد.

امنیت پایدار زمانی شکل می‌گیرد که مدیران ارشد آن را بخشی از راهبرد سازمان بدانند، نه صرفاً مسئولیتی برای واحدهای تخصصی.

ارکان اصلی حکمرانی امنیت

حکمرانی امنیت بر چند اصل کلیدی استوار است:

تعیین سیاست‌ها و راهبردها: ایجاد چارچوبی روشن برای تصمیم‌گیری‌های امنیتی.

مدیریت ریسک: شناسایی و اولویت‌بندی تهدیدات و تمرکز منابع بر مخاطرات اصلی.

تعیین مسئولیت‌ها: مشخص شدن نقش‌ها و پاسخگویی افراد در حوزه امنیت.

پایش و ارزیابی مستمر: سنجش مداوم عملکرد امنیتی و اصلاح نقاط ضعف.

چارچوب‌های شناخته‌شده

سازمان‌ها برای استقرار حکمرانی امنیت از چارچوب‌هایی مانند ISO ۲۷۰۰۱، ISO ۲۷۰۱۴، COBIT و NIST Cybersecurity Framework استفاده می‌کنند. هدف این چارچوب‌ها صرفاً دریافت گواهینامه نیست، بلکه ایجاد ساختاری نظام‌مند برای تصمیم‌گیری و کنترل امنیت است.

اشتباه رایج؛ تمرکز بر تجهیزات

بسیاری از سازمان‌ها سرمایه‌گذاری قابل توجهی در خرید تجهیزات امنیتی انجام می‌دهند، اما به سیاست‌گذاری، مدیریت ریسک و نظارت مدیریتی توجه کافی ندارند. در نتیجه با وجود تجهیزات پیشرفته، همچنان در برابر تهدیدات آسیب‌پذیر باقی می‌مانند.

امنیت بدون حکمرانی، مجموعه‌ای از ابزارهاست که فاقد هماهنگی و جهت‌گیری مشخص است.

نقش مدیریت ارشد

مسئولیت نهایی امنیت در سازمان بر عهده مدیریت ارشد است. مدیرعامل و اعضای هیئت‌مدیره در تعیین اولویت‌ها، تخصیص منابع، شکل‌گیری فرهنگ امنیتی و حمایت از برنامه‌های امنیت نقش محوری دارند.

سازمان‌های موفق امنیت را یک هزینه نمی‌دانند، بلکه آن را سرمایه‌گذاری برای حفظ دارایی‌ها، تداوم کسب‌وکار و افزایش اعتماد ذی‌نفعان تلقی می‌کنند. در چنین رویکردی، حکمرانی امنیت پلی میان اهداف کسب‌وکار و الزامات امنیتی است و به مدیران کمک می‌کند تصمیم‌هایی آگاهانه‌تر و مبتنی بر مدیریت ریسک اتخاذ کنند.

در دنیای امروز، سازمان‌هایی موفق‌تر خواهند بود که امنیت را از سطح تجهیزات و عملیات فراتر برده و آن را به بخشی از نظام حکمرانی و مدیریت خود تبدیل کنند.

دیدگاه
گفت‌وگوی تخصصی سایبنا
مصاحبه | تحلیل | تجربه

گفت‌وگو درباره حکمرانی فناوری اطلاعات، امنیت سایبری، تحول دیجیتال و تاب‌آوری سازمانی

امنیت اطلاعات از اتاق هیئت‌مدیره آغاز می‌شود، نه از خرید تجهیزات

مصاحبه با مهندس رسول‌زاده

مدیر فناوری اطلاعات و فعال حوزه تحول دیجیتال و امنیت اطلاعات

۱. لطفاً خودتان و حوزه مسئولیت خود در سازمان را معرفی کنید

بیش از ۱۵ سال در حوزه فناوری اطلاعات، به‌ویژه در صنایع تولیدی و داروسازی فعالیت داشته‌ام و در سال‌های اخیر در جایگاه مدیریت فناوری اطلاعات مشغول بوده‌ام. حوزه مسئولیت من از مدیریت زیرساخت، شبکه، مراکز داده و امنیت اطلاعات آغاز می‌شود و تا تحول دیجیتال، مدیریت دانش، سامانه‌های سازمانی و بهبود فرایندها ادامه پیدا می‌کند. به اعتقاد من وظیفه مدیر IT صرفاً نگهداری تجهیزات نیست؛ بلکه باید فناوری را در خدمت اهداف کسب‌وکار قرار دهد.

۲. مهم‌ترین چالش فناوری اطلاعات در سازمان‌های امروزی چیست؟

مهم‌ترین چالش امروز، سرعت بالای تغییرات فناوری است. سازمان‌ها در حالی که هنوز با مسائل سنتی درگیر هستند، باید خود را با موضوعاتی مانند هوش مصنوعی، امنیت سایبری و تحول دیجیتال نیز هماهنگ کنند. از نگاه من، مشکل اصلی بسیاری از سازمان‌ها کمبود تجهیزات نیست؛ بلکه نبود فرایندهای استاندارد، مستندسازی و مدیریت دانش است. وابستگی بیش از حد به افراد، یکی از ریسک‌های جدی سازمان‌ها محسوب می‌شود.

۳. حکمرانی فناوری اطلاعات چه ارتباطی با امنیت اطلاعات دارد؟

امنیت بدون حکمرانی فناوری اطلاعات معنا پیدا نمی‌کند. امنیت صرفاً خرید فایروال یا آنتی‌ویروس نیست؛ بلکه از سیاست‌گذاری، مدیریت ریسک، تعیین مسئولیت‌ها و نظارت بر اجرای کنترل‌ها آغاز می‌شود. حکمرانی فناوری اطلاعات چارچوبی فراهم می‌کند که امنیت در آن به‌صورت نظام‌مند مدیریت شود.

۴. مهم‌ترین تهدیدات سایبری امروز سازمان‌ها چیست؟

در گذشته باج‌افزارها در صدر تهدیدات قرار داشتند، اما امروز حملات مهندسی اجتماعی، فیشینگ، نشت اطلاعات و سوءاستفاده از دسترسی‌های داخلی سهم قابل توجهی از رخدادهای امنیتی را تشکیل می‌دهند. واقعیت این است که مهاجمان بیش از تجهیزات، انسان‌ها را هدف قرار می‌دهند.

۵. چگونه می‌توان میان فناوری اطلاعات، حراست و مدیریت ارشد هماهنگی مؤثر ایجاد کرد؟

نخستین گام، ایجاد زبان و اهداف مشترک میان این واحدهاست. فناوری اطلاعات، حراست و مدیریت ارشد هر کدام از زاویه متفاوتی به موضوع امنیت نگاه می‌کنند. تجربه نشان داده است که تشکیل کمیته‌های مشترک، تعریف مسئولیت‌های شفاف و استفاده از ابزارهای تحلیلی و نظارتی نوین می‌تواند این فاصله را کاهش دهد. امنیت زمانی موفق خواهد بود که همه ذی‌نفعان در آن مشارکت داشته باشند.

۶. مهاجرت به خدمات ابری می‌تواند امنیت را افزایش دهد یا ریسک ایجاد می‌کند؟

هر دو حالت ممکن است. خدمات ابری در بسیاری موارد سطح امنیت و پایداری را افزایش می‌دهند، اما مهاجرت بدون بررسی دقیق می‌تواند ریسک‌هایی مانند وابستگی به ارائه‌دهنده، چالش‌های حاکمیت داده و هزینه‌های پنهان ایجاد کند. مهاجرت به ابر باید یک تصمیم راهبردی و مبتنی بر ارزیابی دقیق ریسک باشد.

۷. نقش هوش مصنوعی در آینده امنیت اطلاعات چیست؟

هوش مصنوعی هم فرصت است و هم تهدید. از یک سو در تحلیل رخدادها، تشخیص تهدیدات و خودکارسازی عملیات امنیتی بسیار مؤثر است و از سوی دیگر مهاجمان نیز از همین فناوری بهره می‌برند. در آینده، توانایی سازمان‌ها در استفاده هوشمندانه از داده‌ها و ابزارهای مبتنی بر هوش مصنوعی نقش تعیین‌کننده‌ای در امنیت خواهد داشت.

۸. سازمان‌ها چگونه می‌توانند آمادگی خود را در برابر حملات سایبری افزایش دهند؟

اولین گام، شناسایی دارایی‌ها و ارزیابی ریسک‌هاست. پس از آن باید سیاست‌های امنیتی، پشتیبان‌گیری، مانیتورینگ، تست نفوذ، آموزش کارکنان و برنامه واکنش به حادثه به‌صورت مستمر اجرا شود. امنیت یک پروژه مقطعی نیست؛ بلکه یک فرایند دائمی است.

۹. آینده مدیریت فناوری اطلاعات را در پنج سال آینده چگونه می‌بینید؟

به نظر من نقش مدیر IT از مدیریت زیرساخت به سمت مدیریت ارزش در حال حرکت است. موضوعاتی مانند هوش مصنوعی، تحلیل داده، امنیت سایبری و تحول دیجیتال سهم بیشتری از تصمیمات سازمانی خواهند داشت. همچنین توجه به ریسک‌های پدافند غیرعامل، کیفیت تجهیزات و استفاده از نرم‌افزارهای قابل اعتماد اهمیت بیشتری پیدا خواهد کرد.

۱۰. سه توصیه شما به مدیران سازمان‌ها چیست؟

نخست اینکه فناوری اطلاعات را یک سرمایه‌گذاری راهبردی بدانند، نه یک هزینه. دوم اینکه به همان اندازه که برای تجهیزات هزینه می‌کنند، روی آموزش و فرهنگ سازمانی نیز سرمایه‌گذاری کنند. و سوم اینکه پیش از خرید فناوری‌های جدید، فرایندهای خود را اصلاح و مستندسازی کنند؛ زیرا فناوری خوب روی فرایند ضعیف، تنها مشکلات را سریع‌تر منتقل می‌کند.

آکادمی ساینا
باهوش تر و سریع تر و بهتر

آکادمی ساینا؛ سرمایه‌گذاری بر دانش، نه فقط فناوری

در دنیای امروز، سرعت تغییرات فناوری به اندازه‌ای بالاست که دانش دیروز، لزوماً پاسخگوی نیازهای فردا نیست. سازمان‌هایی که تنها بر تجهیزات، نرم‌افزارها و زیرساخت‌ها تمرکز می‌کنند، دیر یا زود با چالش کمبود نیروی متخصص و فاصله دانشی مواجه خواهند شد. به همین دلیل شرکت شبکه گستر ساینا، در کنار توسعه خدمات و راهکارهای فناوری اطلاعات و ارتباطات، ایجاد و توسعه «آکادمی ساینا» را به عنوان یکی از ارکان راهبردی خود در دستور کار قرار داده است.
آکادمی ساینا با هدف توسعه دانش تخصصی، انتقال تجربیات عملی و تربیت نیروهای توانمند در حوزه فناوری اطلاعات، ارتباطات، زیرساخت شبکه، امنیت اطلاعات، مراکز داده، نظارت تصویری و فناوری‌های نوین شکل گرفته است. این آکادمی تلاش می‌کند پلی میان دانش دانشگاهی و نیازهای واقعی بازار کار ایجاد کند؛ پلی که بسیاری از متخصصان جوان برای ورود موفق به صنعت به آن نیاز دارند.

چرا آکادمی ساینا؟

تجربه سال‌ها فعالیت در پروژه‌های مختلف نشان داده است که موفقیت یک پروژه صرفاً به تجهیزات و فناوری وابسته نیست؛ بلکه دانش و مهارت نیروی انسانی نقش تعیین‌کننده‌ای در کیفیت اجرا و بهره‌برداری از راهکارها دارد. از سوی دیگر، تغییرات سریع فناوری باعث شده است که آموزش مستمر به یک ضرورت تبدیل شود، نه یک انتخاب.
آکادمی ساینا با همین نگاه شکل گرفته تا بستری برای یادگیری مستمر، به‌روزرسانی دانش تخصصی و توسعه مهارت‌های کاربردی فراهم کند.

محورهای آموزشی آکادمی ساینا

برنامه‌های آموزشی آکادمی ساینا بر اساس نیازهای واقعی صنعت طراحی می‌شوند و مهم‌ترین محورهای آن عبارت‌اند از:

* زیرساخت و شبکه‌های کامپیوتری
* امنیت اطلاعات و امنیت سایبری
* سیستم‌های نظارت تصویری و حفاظت الکترونیک
* مراکز داده و زیرساخت‌های سازمانی
* رایانش ابری و مجازی‌سازی
* هوش مصنوعی و کاربردهای آن در کسب‌وکار
* مدیریت فناوری اطلاعات و تحول دیجیتال
* مهارت‌های فروش و مشاوره تخصصی در حوزه فناوری

آموزش مبتنی بر تجربه

یکی از ویژگی‌های اصلی آکادمی ساینا، تمرکز بر آموزش کاربردی و مبتنی بر تجربه است. در این رویکرد، شرکت‌کنندگان علاوه بر مفاهیم نظری، با سناریوهای واقعی پروژه‌ها، چالش‌های اجرایی و راهکارهای عملی مواجه می‌شوند. این موضوع باعث می‌شود دانش کسب‌شده قابلیت استفاده مستقیم در محیط کار را داشته باشد.

توسعه سرمایه انسانی

ساینا معتقد است ارزشمندترین دارایی هر سازمان، نیروی انسانی آن است. آکادمی ساینا بستری برای رشد کارکنان، کارشناسان جوان و علاقه‌مندان به حوزه فناوری فراهم می‌کند تا بتوانند مسیر حرفه‌ای خود را با سرعت و کیفیت بیشتری طی کنند.
سرمایه‌گذاری بر آموزش، در واقع سرمایه‌گذاری بر آینده سازمان است؛ آینده‌ای که در آن دانش، خلاقیت و نوآوری مهم‌ترین مزیت رقابتی خواهند بود.

چشم‌انداز آینده

آکادمی ساینا در مسیر تبدیل شدن به یکی از مراجع تخصصی آموزش فناوری اطلاعات و ارتباطات در کشور حرکت می‌کند. توسعه دوره‌های تخصصی، برگزاری کارگاه‌های عملی، همکاری با دانشگاه‌ها و مراکز علمی، ایجاد مسیرهای مهارت‌آموزی و ارائه گواهینامه‌های تخصصی از جمله برنامه‌های پیش‌بینی‌شده برای آینده این مجموعه است.
ما باور داریم که توسعه فناوری بدون توسعه دانش امکان‌پذیر نیست. آکادمی ساینا با همین باور شکل گرفته است تا در کنار ارائه راهکارهای فناورانه، به توسعه دانش و توانمندسازی سرمایه انسانی نیز کمک کند.

آینده را کسانی می‌سازند که یادگیری را متوقف نمی‌کنند؛ و آکادمی ساینا، خانه یادگیری مستمر است.

مدیریت ریسک؛ زبان مشترک مدیران و متخصصان امنیت

چرا برخی مدیران به هشدارهای امنیتی توجه نمی‌کنند؟

تصور کنید مدیر یک سازمان هستید. در جلسه بودجه، مدیر مالی از کاهش هزینه‌ها می‌گوید، مدیر فروش از افزایش درآمد صحبت می‌کند و مدیر فناوری اطلاعات درخواست بودجه برای ارتقای سامانه‌های امنیتی دارد.

سؤال اینجاست: اگر تاکنون حادثه‌ای رخ نداده، چرا باید برای امنیت هزینه کرد؟

این دقیقاً همان نقطه‌ای است که بسیاری از سازمان‌ها در آن دچار اشتباه می‌شوند. امنیت زمانی ارزش خود را نشان می‌دهد که حادثه‌ای رخ ندهد؛ اما مدیران معمولاً با نتایج ملموس و قابل اندازه‌گیری تصمیم می‌گیرند، نه با تهدیدهای احتمالی. اینجاست که مفهوم «مدیریت ریسک» به زبان مشترک مدیران و متخصصان امنیت تبدیل می‌شود.

امنیت؛ از نگاه فنی تا نگاه مدیریتی

کارشناسان امنیت معمولاً درباره آسیب‌پذیری‌ها، تهدیدها، حملات سایبری، نفوذ فیزیکی یا نقاط ضعف زیرساخت صحبت می‌کنند. اما مدیران ارشد به موضوعات دیگری فکر می‌کنند: توقف کسب‌وکار ، کاهش درآمد ،آسیب به اعتبار سازمان ،مسئولیت‌های قانونی ،نارضایتی مشتریان

در واقع مدیران کمتر نگران یک آسیب‌پذیری فنی هستند؛ آنها نگران پیامدهای تجاری آن هستند. به همین دلیل امنیت زمانی در سازمان جدی گرفته می‌شود که از زبان تهدیدها به زبان ریسک ترجمه شود.

ریسک دقیقاً چیست؟

ریسک حاصل ترکیب دو عامل است:

احتمال وقوع یک رویداد × میزان اثرگذاری آن

ممکن است یک تهدید احتمال وقوع کمی داشته باشد اما در صورت وقوع خسارت بسیار بزرگی ایجاد کند. برعکس، برخی تهدیدها مرتب اتفاق می‌افتند اما تأثیر محدودی دارند. مدیریت ریسک تلاش می‌کند این دو عامل را به صورت منطقی و قابل اندازه‌گیری تحلیل کند تا تصمیم‌گیری بر اساس واقعیت انجام شود، نه احساسات.

اولین گام؛ شناسایی ریسک‌ها

بسیاری از سازمان‌ها تصور می‌کنند فقط حملات سایبری تهدید محسوب می‌شوند؛ در حالی که ریسک‌های امنیتی دامنه بسیار گسترده‌تری دارند: سرقت اطلاعات ،نفوذ غیرمجاز به ساختمان ،خرابی تجهیزات حیاتی ،قطع برق ،خطای انسانی ،دسترسی غیرمجاز کارکنان ،تخریب عمدی یا سهوی دارایی‌ها ،نشت اطلاعات محرمانه

نکته مهم این است که هر سازمان فهرست ریسک‌های خاص خود را دارد و نسخه واحدی برای همه وجود ندارد.

ارزیابی ریسک؛ مهم‌ترین مرحله

یکی از اشتباهات رایج سازمان‌ها این است که همه تهدیدها را با یک درجه اهمیت می‌بینند.

در عمل چنین چیزی ممکن نیست.

اگر منابع محدود باشند، کدام ریسک باید ابتدا کنترل شود؟

اینجاست که ارزیابی ریسک اهمیت پیدا می‌کند.

در این مرحله برای هر ریسک مشخص می‌شود:

احتمال وقوع چقدر است؟

خسارت احتمالی چقدر خواهد بود؟

چه دارایی‌هایی در معرض خطر هستند؟

سازمان تا چه میزان تحمل این ریسک را دارد؟

نتیجه این فرآیند معمولاً به شکل اولویت‌بندی ریسک‌ها ارائه می‌شود.

کنترل ریسک؛ حذف یا مدیریت؟

برخلاف تصور رایج، هدف مدیریت ریسک حذف کامل خطرات نیست.

در دنیای واقعی حذف کامل ریسک تقریباً غیرممکن و از نظر اقتصادی غیرمنطقی است.سازمان‌ها معمولاً یکی از چهار راهکار زیر را انتخاب می‌کنند:

۱. کاهش ریسک

استفاده از دوربین‌های نظارتی، کنترل تردد، سامانه‌های هشدار و راهکارهای امنیت سایبری.

۲. انتقال ریسک

استفاده از بیمه یا برون‌سپاری برخی خدمات.

۳. اجتناب از ریسک

توقف فعالیت‌هایی که ریسک غیرقابل قبول دارند.

۴. پذیرش ریسک

زمانی که هزینه کنترل از خسارت احتمالی بیشتر باشد.

نقش فناوری در مدیریت ریسک

فناوری‌های امنیتی زمانی ارزشمند هستند که بتوانند سطح ریسک را کاهش دهند.

یک دوربین مداربسته صرفاً یک تجهیز نیست؛ ابزاری برای کاهش احتمال وقوع سرقت، افزایش قابلیت کشف حادثه و کاهش خسارت است.

یک سامانه کنترل تردد صرفاً یک گیت یا کارت‌خوان نیست؛ ابزاری برای کنترل دسترسی و مدیریت ریسک‌های انسانی است.

به همین دلیل سازمان‌های پیشرو هنگام خرید تجهیزات امنیتی به مشخصات فنی صرف نگاه نمی‌کنند؛ بلکه به این سؤال پاسخ می‌دهند: «این راهکار چه ریسکی را کاهش می‌دهد؟»

چالش بزرگ مدیران

امروزه تهدیدها سریع‌تر از گذشته تغییر می‌کنند. تحول دیجیتال، هوش مصنوعی، دورکاری و اتصال گسترده سامانه‌ها باعث شده مرزهای سنتی امنیت از بین برود. در چنین شرایطی بزرگ‌ترین خطر برای سازمان‌ها نبود تجهیزات امنیتی نیست؛ بلکه نداشتن نگاه مبتنی بر ریسک است. سازمانی که ریسک‌های خود را نمی‌شناسد، حتی با پیشرفته‌ترین تجهیزات نیز آسیب‌پذیر خواهد بود.

مدیریت ریسک پلی میان دغدغه‌های کسب‌وکار و الزامات امنیتی است. این رویکرد به مدیران کمک می‌کند منابع خود را هوشمندانه تخصیص دهند و به متخصصان امنیت امکان می‌دهد ارزش اقدامات خود را به زبان قابل فهم برای تصمیم‌گیران سازمان بیان کنند.

امنیت زمانی به یک سرمایه‌گذاری مؤثر تبدیل می‌شود که به جای تمرکز بر تجهیزات و فناوری‌ها، بر مدیریت ریسک‌های واقعی سازمان متمرکز شود.

شاید مهم‌ترین سؤال هر مدیر امروز این باشد:

اگر فردا یک حادثه امنیتی رخ دهد، آیا سازمان ما از قبل ریسک آن را شناخته و برای آن برنامه‌ریزی کرده است؟

RAMON®
NETWORK PASSIVE EQUIPMENT

تجهیزات پسیو رامون

ساخت ایران

ثبت سفارش : ۰۲۶۳۲۶۲۰۰۰۰

www.SainaSoft.com

یک سناریوی خوش‌بینانه

به قلم : سروش ذوالمجدی
مشاور ارشد شرکت مشاوره مدیریت ژانوس

هر کس که ادعا کند می‌داند به کدام سمت می‌رویم و دقیقاً قرار است چه اتفاقی بیفتد، به راستی دروغ می‌گوید. تنها تفاوت سازمان‌هایی (و البته مدیرانی) که در شرایط عدم قطعیت و متغیر بازار (شرایطی که ما در بالاترین سطح آن زندگی می‌کنیم) موفق عمل می‌کنند، تنها سازمان‌هایی هستند که آمادگی مواجهه با سناریوهای متفاوت را در خود ایجاد کرده اند و یا در بدبینانه‌ترین حالت، به آن سناریوها اندیشیده‌اند.

در روزی که این مطلب نگاشته می‌شود(۲۶ خردادماه ۱۴۰۵)، اخباری مهم از توافق میان ایران و آمریکا به گوش می‌رسد و این توافق با توجه به این موضوع است که ایران و آمریکا در طی چهار دهه در کش و قوس تنش، مذاکره، جنگ و ناآرامی بوده‌اند. از سویی دیگر ایران پس از جنگ اخیر به ناگزیر وارد فاز بازسازی خواهد شد(چه در شرایط صلح و چه در شرایط جنگ). اما توجه به این نکته لازم است که دوران سازندگی در شرایطی که منابع مالی مکفی در اختیار کشور باشد و تاجران و تولیدکنندگان با دشواری‌های ناشی از تحریم مواجه نباشد بسیار متفاوت انجام خواهد شد.

مکنزی(McKinsey & Company) به عنوان یکی از بزرگترین شرکت‌های مشاوره‌ای دنیا در سال ۲۰۱۶ گزارشی در خصوص ایران پس از برجام و فرصت‌های سرمایه‌گذاری در آن منتشر کرده است(Trillion Growth 1$ Iran: The ,2016 ,McKinsey Global Institute Opportunity?)، گزارشی که بخش‌هایی از آن در برهه‌های زیادی به ما (به‌عنوان یک شرکت مشاوره مدیریت)، در مواجهه با مسائل و احساس نیاز به استناد به تحقیقاتی جامع کمک کرده است. به همین دلیل تلاش می‌کنم در ادامه توضیحات مختصری از یکی از سناریوهای پیش رویمان(سناریوی خوش‌بینانه) به شما ارائه کنم.

جهش

بازخوانی فرصت‌های ۱ تریلیون دلاری در دوران صلح

اگر سناریوی خوش‌بینانه محقق شود و سایه سنگین تحریم‌ها و تنش‌های چهاردهه گذشته از سر اقتصاد ایران کنار رود، ما با یک بازسازی عادی روبرو نخواهیم بود؛ بلکه با یک تحول ساختاری سرعت‌یافته مواجه می‌شویم که منابع مالی آزاد شده و جریان سرمایه بین‌المللی، سوخت موتورهای آن خواهند بود. گزارش سال ۲۰۱۶ مکنزی، دقیقاً مختصات این سناریو را ترسیم می‌کند: پتانسیل افزودن ۱ تریلیون دلار به تولید ناخالص داخلی (GDP) و خلق ۹ میلیون شغل جدید در این دوران.

مکنزی در این سناریو، پیشران‌های حرکت ایران را به چهار موتور اصلی تقسیم می‌کند که در شرایط صلح و دسترسی به منابع، می‌توانند جهشی بی‌سابقه را تجربه کنند.

سرمایه‌گذاری تجمعی ۳.۵ تریلیون دلاری و مدرن‌سازی زیرساخت‌ها

در این سناریو، بزرگ‌ترین نیاز و در عین حال ملموس‌ترین فرصت، در بخش زیرساخت و ساخت‌وساز نهفته است. مکنزی نیاز به سرمایه‌گذاری بیش از ۱.۵ تریلیون دلاری را در این بخش پیش‌بینی می‌کند. با رفع محدودیت‌های مالی، پروژه‌های ملی از توسعه بنادر استراتژیک (مانند چابهار و بندرعباس) گرفته تا نوسازی خطوط ریلی و شبکه‌های انرژی کشور، دیگر با بودجه‌های قطره‌چکانی و محدود اداره نخواهند شد. این حجم از ساخت‌وساز، خود به تنهایی محرک صدها صنعت بالادستی و پایین‌دستی خواهد بود.

جهش صنایع رقابت‌پذیر و بازار تشنه خودرو[با کیفیت]

ایران بزرگ‌ترین بازار خودرو در منطقه است. مکنزی در سناریوی رشد خود، ظرفیت این بازار را تولید ۳.۲ میلیون دستگاه خودرو در سال و تبدیل شدن ایران به هاب صادراتی منطقه (عراق، سوریه و آسیای مرکزی) می‌داند. در شرایط صلح، ورود غول‌های خودروسازی جهان و انتقال فناوری، بهره‌وری پایین این صنعت را متحول خواهد کرد و زنجیره تأمین داخلی را به استانداردهای جهانی متصل می‌سازد. در کنار تحلیل مکنزی در این خصوص باید این نکته را در نظر داشته باشیم که صنعت خودرو ایران با وجود ناکارآمدی در تولید محصولات به‌روز و با کیفیت، توانسته است شبکه‌ای قدرتمند لوجستیکی و پشتیبانی ایجاد کند که ایجاد آن در هر کشوری به چند دهه فعالیت و میلیاردها دلار سرمایه نیاز خواهد داشت. به همین دلیل جذابیت این صنعت در طرف مقابل نیز به وضوح قابل مشاهده است.

زنجیره ارزش فراتر از خام‌فروشی در بخش انرژی

دسترسی به خوراک گاز کم‌هزینه، قیمت تمام‌شده تولیدات پتروشیمی ایران را به یک‌پنجم بازار جهانی می‌رساند(هر چند که این محصولات به قیمت دلاری و متناسب با قیمت‌های جهانی به فروش می‌رسند). در سناریوی خوش‌بینانه، با جذب فناوری‌های پیشرفته بین‌المللی، سهم ارزش افزوده ناخالص (GVA) پتروشیمی می‌تواند از ۷ میلیارد دلار به ۴۰ میلیارد دلار جهش کند. این یعنی عبور کامل از خام‌فروشی نفت و گاز و تبدیل شدن به قدرت اول پتروشیمی منطقه.

اقتصاد دانش‌بنیان و سرمایه انسانی نخبگان

نقطه عطف گزارش مکنزی، تأکید بر سرمایه انسانی ایران است؛ کشوری که یک‌سوم فارغ‌التحصیلان آن در رشته‌های مهندسی (هم‌تراز با آمریکا) تحصیل کرده‌اند. در سناریوی باز شدن مرزهای اقتصادی، بخش فناوری اطلاعات و ارتباطات (ICT) ظرفیت ۴ برابر شدن و رسیدن به ارزش ۳۱ میلیارد دلار را داراست. تهران در این سناریو می‌تواند به هاب برون‌سپاری خدمات دیجیتال و فناوری اطلاعات در منطقه تبدیل شود.

آمادگی برای موج بزرگ

همان‌طور که در مقدمه اشاره شد، هیچ‌کس آینده را پیش‌بینی نمی‌کند و ما نیز این قانون مستثنی نیستیم.. با این وجود این سناریو، یکی از ۵ سناریوی پیش‌بینی شده‌ی گروه مطالعات استراتژیک شرکت مشاوره مدیریت ژانوس در اوج دوران تنش و جنگ بوده است. ورق خوردن تاریخ به سمت این سناریوی خوش‌بینانه، به معنای ورود به مسابقه‌ای است که برندگان آن، سازمان‌های آماده هستند. شرکت‌هایی که از هم‌اکنون استانداردهای مدیریتی خود را ارتقا داده، زنجیره تأمین خود را بازتعریف کرده و مدل‌های کسب‌وکارشان را برای مقیاس‌پذیری در یک بازار بزرگ و رقابتی آماده ساخته‌اند، موج‌سواران این تحول تریلیون دلاری خواهند بود. سازمان‌هایی که می‌دانند هرچند این اتفاقات به یک شبه اتفاق نخواهند افتاد، تنها برای کسانی قابل بهره‌برداری خواهند بود که در خط اول مسابقه منتظر شلیک شروع مسابقه باشد.

تداوم توسعه صنعت افتا؛ افزایش شرکت‌های فعال در حوزه امنیت سایبری

بررسی‌های انجام‌شده نشان می‌دهد که با وجود شرایط ویژه ماه‌های اخیر، روند توسعه صنعت امنیت سایبری کشور متوقف نشده و شرکت‌های جدیدی به جمع فعالان حوزه افتا افزوده شده‌اند.
بر اساس اعلام مرکز مدیریت راهبردی افتای ریاست جمهوری، فرآیند صدور مجوزها و ارائه خدمات به شرکت‌های متقاضی فعالیت در حوزه امنیت اطلاعات و ارتباطات (افتا) در طول این مدت با سرعت و دقت لازم ادامه داشته است. نتیجه این روند، ورود ده‌ها شرکت جدید به اکوسیستم امنیت سایبری کشور و گسترش ظرفیت ارائه خدمات و تولید محصولات بومی بوده است.
در حال حاضر بیش از یک‌هزار و ۶۰۰ شرکت دارای مجوز افتا در کشور فعالیت می‌کنند و بخش قابل توجهی از نیازمندی‌های حوزه امنیت سایبری توسط شرکت‌های داخلی تأمین می‌شود. همچنین صدها شرکت دانش‌بنیان و خصوصی در زمینه تولید محصولات امنیتی، خدمات تخصصی و راهکارهای دفاع سایبری مشغول فعالیت هستند.

دیگر نکات قابل توجه، ازسرگیری برگزاری آزمون‌های تخصصی افتا و ادامه فرآیند ارزیابی و صدور مجوزهاست که نقش مهمی در حفظ استانداردهای فنی و ارتقای کیفیت خدمات این صنعت ایفا می‌کند. کارشناسان معتقدند افزایش تعداد شرکت‌های فعال در حوزه افتا، علاوه بر تقویت توانمندی‌های بومی، می‌تواند به توسعه بازار خدمات امنیت اطلاعات، افزایش رقابت تخصصی و ارتقای تاب‌آوری سایبری سازمان‌ها و کسب‌وکارهای کشور منجر شود.

واکنش بازارهای جهانی به اخبار توافق ایران و آمریکا

انتشار اخبار مربوط به توافق میان ایران و آمریکا، واکنش قابل توجهی در بازارهای مالی جهان به همراه داشت. در نخستین ساعات پس از انتشار این خبر، قیمت بیت‌کوین با رشد بیش از ۲ درصدی از مرز ۶۵ هزار دلار عبور کرد و ارزش کل بازار رمزارزها نیز افزایش یافت.
تحلیلگران معتقدند کاهش تنش‌های ژئوپلیتیکی و چشم‌انداز ثبات بیشتر در منطقه، از مهم‌ترین عوامل افزایش تمایل سرمایه‌گذاران به دارایی‌های پرریسک از جمله ارزهای دیجیتال بوده است. در این میان برخی رمزارزها عملکردی فراتر از میانگین بازار ثبت کردند و رشد قابل توجهی را تجربه نمودند.
همزمان، بازار انرژی مسیر متفاوتی را در پیش گرفت. قیمت نفت خام در واکنش به احتمال کاهش ریسک‌های منطقه‌ای و بهبود شرایط عرضه، با افت محسوسی مواجه شد و بهای نفت برنت و نفت WTI کاهش یافت.

کارشناسان با وجود واکنش مثبت اولیه بازارها، معتقدند جزئیات توافق و همچنین تصمیمات آتی بانک‌های مرکزی جهان می‌تواند در روزهای آینده بر روند بازارهای مالی و انرژی تأثیرگذار باشد. از این رو، سرمایه‌گذاران همچنان با دقت تحولات سیاسی و اقتصادی را دنبال می‌کنند.

توپ هوشمند جام جهانی؛ فناوری در خدمت داوری دقیق‌تر

جام جهانی ۲۰۲۶ تنها ویترین مهارت بازیکنان نیست؛ بلکه یکی از پیشرفته‌ترین فناوری‌های ورزشی جهان نیز در آن به نمایش گذاشته شده است. توپ رسمی این رقابت‌ها با نام «تریوندا» به حسگرهای هوشمندی مجهز شده که قادرند در هر ثانیه صدها داده حرکتی را ثبت و ارسال کنند. این توپ با بهره‌گیری از یک تراشه داخلی، اطلاعات موقعیت و حرکت خود را به‌صورت لحظه‌ای در اختیار سامانه‌های تحلیل مسابقه قرار می‌دهد. داده‌های جمع‌آوری‌شده با دوربین‌های ردیاب مستقر در ورزشگاه ترکیب شده و به سیستم کمک‌داور ویدیویی (VAR) منتقل می‌شود.

هدف اصلی این فناوری، افزایش دقت تصمیمات داوری در صحنه‌های حساس مانند آفساید، عبور توپ از خط دروازه و تشخیص لحظه دقیق برخورد توپ با بازیکنان است. به این ترتیب، نقش خطای انسانی در تصمیم‌گیری‌های حساس مسابقات به حداقل می‌رسد.
در کنار فناوری هوشمند، طراحی جدید توپ نیز مورد توجه قرار گرفته است. کاهش تعداد پنل‌ها و بهبود ویژگی‌های آیرودینامیکی باعث شده رفتار توپ در شرایط مختلف آب‌وهوایی پایدارتر و قابل پیش‌بینی‌تر باشد.
ورود چنین فناوری‌هایی نشان می‌دهد آینده ورزش حرفه‌ای بیش از هر زمان دیگری به داده، هوش مصنوعی و سامانه‌های هوشمند وابسته خواهد بود؛ جایی که تصمیمات کلیدی نه‌تنها بر پایه مشاهده انسانی، بلکه با تکیه بر تحلیل لحظه‌ای داده‌ها اتخاذ می‌شوند.

فناوری زمانی
ارزش‌آفرین است که به
تصمیم‌سازی آگاهانه
منجر شود.

امنیت، فقط در تجهیزات خلاصه نمی‌شود؛
در حکمرانی، در پکپارچگی، در تحلیل
و در تصمیم‌های درست شکل می‌گیرد.

ساینا؛ همراه مطمئن سازمان‌های آینده‌نگر

شبکه گستر ساینا
شرکت فناوری اطلاعات و ارتباطات

مشاور | طراح | ناظر | مجری

پروژه‌های فناوری اطلاعات، امنیت، نظارت تصویری و زیرساخت

چشم‌انداز ما:
ایجاد زیرساخت‌های امن، هوشمند و پایدار

تیمی از
متخصصان مجرب
و گواهی‌دار

۳۱
استان تحت پوشش
خدمات و پشتیبانی

۵۰۰+
پروژه اجرا شده در
سراسر کشور

۲۰+
سال تجربه
موفق

امنیت، پایداری کسب‌وکار شماست.
تصمیم درست، آینده‌ای مطمئن.

02632620000

www.SainaSoft.com