خبر

اجرای طرح آنالیز قیمت کالاهای اساسی در اصفهان

مسئول قرارگاه متمرکز یکپارچه نظارت و بازرسی بازار اصفهان از اجرای طرح آنالیز قیمت کالاهای اساسی خبر داد. جواد محمدی فشارکی از اجرای طرح آنالیز قیمت کالاهای اساسی در اصفهان خبر داد و گفت: در این طرح، هزینه‌های واقعی تولید کالا از مرحله تأمین نهاده و انرژی تا دستمزد، استهلاک و سایر هزینه‌های تولید بررسی می‌شود و پس از محاسبه هزینه تمام‌شده، سود مجاز به آن اضافه خواهد شد. مسئول قرارگاه متمرکز یکپارچه نظارت و بازرسی بازار استان اصفهان افزود: این طرح تاکنون در بازار کالاهایی مانند مرغ، گوشت، لوله و اتصالات، سیمان و دیگر کالاهای پرمصرف اجرا شده و هدف آن رسیدن به قیمت منطقی و واقعی کالاها در بازار است. او با اشاره به اجرای این طرح در بازار مرغ ادامه داد: در این فرآیند، هزینه‌های مربوط به مرغداران، کشتارگاه‌ها و سایر حلقه‌های زنجیره تولید به‌صورت دقیق بررسی شد و پس از انجام چند مرحله راستی‌آزمایی، قیمت منطقی این محصول به دست آمد. محمدی فشارکی گفت: همین رویکرد در بازار گوشت قرمز نیز دنبال شد و گروه‌های بازرسی با حضور در کشتارگاه‌ها، بررسی اسناد و مستندات و ارزیابی هزینه‌های دامداران، فرآیند آنالیز قیمت را انجام دادند.

صرفه‌جویی ۲۰ همتی از محل اسقاط خودروهای فرسوده

مدیر ستاد نوسازی ناوگان و اسقاط خودروهای فرسوده گفت: اسقاط ۶۸۰ هزار خودروی فرسوده طی سه سال، علاوه بر صرفه‌جویی نزدیک به ۲ میلیارد لیتر سوخت و بازگشت ۴۴۰ هزار تن مواد اولیه به چرخه تولید، بیش از ۲۰ هزار میلیارد تومان صرفه‌جویی اقتصادی برای کشور به همراه داشته است.

محمدصادق حاتمی در نشست خبری آیین رونمایی آغاز نوسازی موتورسیکلت‌های فرسوده با موتورسیکلت برقی در شهر اصفهان در چارچوب تفاهمنامه ۹۶ هزار دستگاه گفت: فرآیند اسقاط و نوسازی خودرو بر اساس قانون ساماندهی صنعت خودرو (مصوب ۱۴۰۱)، از تکالیف محوری وزارت صنعت، معدن و تجارت و سازمان گسترش و نوسازی صنایع ایران (ایدرو) است و این فرآیند با مشارکت شبکه‌ای متشکل از حدود ۲۲۰ مرکز اسقاط، ۸۰ شرکت خودروساز، ۲۰۰۰ واردکننده، صندوق حمایت از تحقیقات و توسعه صنایع پیشرفته و شبکه بانکی کشور به مرحله اجرا درآمده است. او افزود: در حال حاضر نزدیک به ۷۰۰ هزار دستگاه موتورسیکلت در شهر اصفهان تردد می‌کنند که از این تعداد، حدود ۶۰۰ هزار دستگاه معادل ۸۰ درصد فرسوده هستند و از سوی دیگر، هر موتورسیکلت کاربراتوری فرسوده به‌اندازه هفت دستگاه خودروی انژکتوری آلایندگی تولید می‌کند؛ از این رو، نوسازی ناوگان این کلان‌شهر در اولویت قطعی قرار گرفته و با توجه به زیرساخت‌های فراهم‌شده توسط مدیریت شهری اصفهان و پیشگامی این شهر در پذیرش فناوری‌های پاک، اصفهان به‌عنوان دومین اولویت کشور و رسما به‌عنوان الگوی برقی‌سازی ناوگان انتخاب شد و تجربیات آن در سایر کلان‌شهرها نیز به کار گرفته خواهد شد. مدیر ستاد نوسازی ناوگان و اسقاط خودروهای فرسوده درباره تسهیلات اختصاص‌یافته به راکبان موتورسیکلت‌های کار در اصفهان توضیح داد: در فاز نخست این طرح، جایگزینی ۵۰۰ دستگاه موتورسیکلت برقی هدف‌گذاری شده و با اصلاح آیین‌نامه اجرایی ماده ۱۰ قانون ساماندهی صنعت خودرو، مشوق‌های ویژه‌ای برای ناوگان برقی در نظر گرفته شد؛ بطوری‌که راکبان موتورسیکلت‌های فرسوده مشمول دریافت تا سقف ۱۴۰ میلیون تومان یارانه اسقاط معادل چهار گواهی اسقاط خواهند شد که این رقم دو برابر مشوق‌های موتورسیکلت‌های بنزینی است. او با اشاره به آمادگی زیرساختی اصفهان برای پشتیبانی از این طرح گفت: در حال حاضر ۴۲ ایستگاه شارژ در سطح شهر اصفهان راه‌اندازی شده که ۲۶ ایستگاه آن اختصاصیِ موتورسیکلت با ظرفیت شارژ همزمان ۵۲ دستگاه است که تنها ۸۵ درصد ظرفیت این ایستگاه‌ها مورد استفاده قرار می‌گیرد و ۱۵ درصد ظرفیت مازاد آماده پذیرش ناوگان جدید است که امکان توسعه آن تا چندین هزار دستگاه نیز وجود دارد. مدیر ستاد نوسازی ناوگان و اسقاط خودروهای فرسوده با اشاره به ابعاد تفاهمنامه کشوری نوسازی ۹۶ هزار دستگاه ناوگان عمومی و تجاری خاطرنشان کرد: این تفاهمنامه معطوف به کلان‌شهرهاست و سهم‌بندی آن شامل ۴۰۰۰ دستگاه تاکسی برقی برای تهران، ۲۰۰۰ دستگاه تاکسی برقی برای سایر کلان‌شهرها، ۲۰ هزار دستگاه تاکسی دوگانه‌سوز برای کلان‌شهرها (به‌جز تهران) و ۷۰ هزار دستگاه موتورسیکلت کار در تهران و سایر کلان‌شهرها است. حاتمی گفت: در طول ۲۰ سال گذشته مجموعا دو میلیون و ۶۷۰ هزار دستگاه خودرو اسقاط شده و این در حالی است که تنها در دوره سه‌ساله اخیر، ۶۸۰ هزار دستگاه خودرو اسقاط که معادل ۲۵ درصد کل عملکرد ۲۰ سال گذشته کشور است و این حجم از اسقاط موجب صرفه‌جویی نزدیک به دو میلیارد لیتر سوخت در کشور و بازگشت ۴۴۰ هزار تن مواد اولیه شامل مس، آلومینیوم، فولاد، لاستیک و پلاستیک به چرخه تولید صنایع، به‌ویژه صنایع فولادی اصفهان شد که ارزش اقتصادی این بازیافت و صرفه‌جویی بیش از ۲۰ هزار میلیارد تومان (۲۰ همت) برآورد می‌شود.

حاتمی یادآور شد: با اصلاح آیین‌نامه اجرایی ماده ۱۰ قانون ساماندهی صنعت خودرو که در ۱۲ مردادماه سال جاری ابلاغ شد، سقف ظرفیت اسقاط سالانه کشور از ۲۵۰ هزار دستگاه به ۷۰۰ هزار دستگاه ارتقا یافته و بر اساس مصوبه کمیسیون زیربنایی دولت، اولویت‌بندی نوسازی کلان‌شهرها بر عهده کارگروه ملی آلودگی هوا قرار گرفت که بر مبنای شاخص‌های جمعیت، سهم منابع متحرک در آلایندگی و میزان مصرف سوخت، شهرهای تهران، مشهد و اصفهان در صدر اولویت‌های کشور تعیین شده‌اند.

با یک حمله سایبری گسترده، کدام بخش‌های زندگی مردم متوقف می‌شود؟

چرنوبیل دیجیتال؛ بدون شلیک حتی یک گلوله!

سید مهدی رضوی

برای اغلب مردم، امنیت سایبری زمانی معنا پیدا می‌کند که کارت بانکی کار نکند، درگاه پرداخت از دسترس خارج شود، پیامک احراز هویت نرسد، یک سامانه دولتی باز نشود یا خبر افشای اطلاعات شخصی منتشر شود. در چنین موقعیتی، شهروند با مفاهیمی مانند بدافزار، باج‌افزار، نفوذ یا حمله زنجیره تأمین کاری ندارد؛ مسئله او این است که خدمت مورد نیازش چرا متوقف شده و چه زمانی برمی‌گردد. پشت همین اختلال‌های ظاهراً ساده، اما مسئله‌ای عمیق‌تر قرار دارد. زیرساخت‌های دیجیتال کشور دیگر مجموعه‌ای از سامانه‌های مستقل نیستند. بانک‌ها، خدمات پرداخت، احراز هویت، ارتباطات، خدمات دولتی و پایگاه‌های داده از طریق ارتباطات، واسطه‌ها و زیرساخت‌های مشترک به یکدیگر وابسته شده‌اند. بنابراین آسیب‌پذیری فقط به معنای امکان نفوذ به یک سامانه نیست؛ خطر مهم‌تر آن است که یک اختلال محدود بتواند به بحران گسترده‌تری تبدیل شود. سال‌هاست پیشرفت دیجیتال با تعداد سامانه‌ها، خدمات برخط، مراکز داده و میزان اتصال دستگاه‌ها سنجیده می‌شود. اما وقتی سازمان‌ها مستقل از یکدیگر سامانه می‌سازند و سپس برای اتصال آنها لایه‌های مختلفی ایجاد می‌کنند، پیچیدگی افزایش می‌یابد و تغییر یا خرابی یک جزء می‌تواند آثار پیش‌بینی‌نشده‌ای بر اجزای دیگر داشته باشد. از سوی دیگر، حتی وقوع یک حمله به‌تنهایی تعیین نمی‌کند که یک حادثه به بحران ملی تبدیل شود یا نه. مدت زمان قطعی، توان بازیابی، معماری زیرساخت و کیفیت ارتباط با مردم تعیین می‌کنند که یک رخداد فنی در همان سطح باقی بماند یا به بحران اقتصادی و اجتماعی تبدیل شود. برای واکاوی این مسئله با شاهین سمیع عادل، پژوهشگر حوزه مدیریت و امنیت فناوری اطلاعات، گفت‌وگو کرده‌ایم. او معتقد است تهدید اصلی فقط نفوذ به سامانه‌ها نیست؛ مسئله مهم‌تر، گلوگاه‌هایی است که به دلیل تمرکز یا وابستگی متقابل می‌توانند دامنه یک اختلال را گسترش دهند. از این منظر، چرنوبیل دیجیتال بیش از آنکه نام یک حمله باشد، توصیف وضعیتی است که در آن یک نقطه آسیب‌پذیر می‌تواند آغازگر یک بحران زنجیره‌ای شود.

بسیاری از مردم وقتی عبارت حمله سایبری را می‌شنوند، تصور می‌کنند یک هکر وارد یک سامانه می‌شود و اطلاعاتی را سرقت می‌کند. شما از چرنوبیل دیجیتال صحبت می‌کنید. این تعبیر دقیقاً به چه معناست و چه تفاوتی با یک حمله معمولی دارد؟

اگر بخواهیم موضوع را ساده اما دقیق تعریف کنیم، تفاوت اصلی در دامنه پیامدهاست. یک حمله ممکن است فقط یک سامانه را مختل کند و پس از مدتی نیز برطرف شود. اما در یک سناریوی پرخطر، حمله به نقطه‌ای می‌رسد که تعداد زیادی از خدمات به آن وابسته‌اند و اختلال از یک بخش به بخش‌های دیگر منتقل می‌شود. اینجا مفهوم گلوگاه اهمیت پیدا می‌کند. گلوگاه در فناوری نقطه‌ای است که بخش‌های مختلف به آن وابسته‌اند و اختلال در آن می‌تواند عملکرد بخش‌های دیگر را نیز تحت تأثیر قرار دهد. اگر یک زیرساخت حیاتی بیش از اندازه متمرکز باشد یا چند خدمت مهم از یک جزء مشترک استفاده کنند، همان جزء می‌تواند به نقطه شکست واحد تبدیل شود. فرض کنید بخشی از زیرساخت پرداخت با اختلال جدی مواجه شود. اگر بانک‌ها، خدمات پرداخت و برخی خدمات عمومی مسیرهای جایگزین نداشته باشند، اثر حادثه فقط متوجه یک سامانه نخواهد بود. مردم ممکن است نتوانند خرید کنند، کسب‌وکارها نتوانند پرداخت‌های خود را انجام دهند و بخشی از فعالیت اقتصادی در مدت کوتاهی دچار مشکل شود. بنابراین مسئله فقط قدرت فنی مهاجم نیست؛ باید دید معماری ما تا چه اندازه اجازه می‌دهد یک اختلال گسترش پیدا کند. در یک نظام تاب‌آور، احتمال نفوذ را نمی‌توان به صفر رساند، اما می‌توان کاری کرد که دامنه یک نفوذ محدود بماند، خدمات حیاتی ادامه پیدا کنند و سامانه آسیب‌دیده در کوتاه‌ترین زمان ممکن بازیابی شود. در چنین شرایطی، مدت قطعی و سرعت بازیابی خدمات به اندازه جلوگیری از نفوذ اهمیت پیدا می‌کند. بنابراین وقتی از چرنوبیل دیجیتال حرف می‌زنیم، هشدار درباره یک حمله خاص نیست؛ درباره معماری‌ای است که ممکن است اجازه دهد یک نقطه شکست، پیامدهایی بسیار بزرگ‌تر از خود آن نقطه ایجاد کند.

پس مسئله اصلی فقط امنیت هر سامانه به‌صورت جداگانه نیست. اگر چند سامانه هرکدام به‌طور مستقل امن باشند، اما همه آنها به یک زیرساخت مشترک وابسته باشند، آیا همچنان با یک آسیب‌پذیری جدی مواجهیم؟

دقیقاً. یکی از خطاهای رایج در سیاست‌گذاری امنیت سایبری این است که امنیت را در محدوده هر سازمان بررسی کنیم؛ اینکه بانک چه سامانه‌ای دارد، وزارتخانه چه فایروالی نصب کرده یا بیمارستان چگونه از شبکه خود حفاظت می‌کند. اما در سطح ملی، باید یک لایه بالاتر را دید: شبکه وابستگی‌ها. ممکن است هر سازمان استانداردهای امنیتی خودش را رعایت کرده باشد، اما اگر همه آنها به یک گلوگاه مشترک وابسته باشند، ضعف همان گلوگاه می‌تواند چندین سازمان را همزمان تحت تأثیر قرار دهد. در اینجا امنیت یک سازمان دیگر از امنیت سایر اجزای اکوسیستم جدا نیست. هر سازمان ممکن است سامانه خود را منطقی و مناسب بداند، اما مجموعه تصمیم‌های جداگانه می‌تواند وابستگی‌های پیچیده‌ای ایجاد کند که تغییر یا خرابی یک جزء، بخش‌های دیگری را نیز گرفتار کند. در زیرساخت‌های حیاتی این مسئله اهمیت بیشتری دارد. اگر یک سامانه پشتیبان، شبکه مشترک، مرکز داده، سرویس هویتی یا مسیر ارتباطی به اندازه‌ای مهم باشد که چندین خدمت حیاتی بدون آن نتوانند کار کنند، باید آن را یک نقطه شکست مهم در نظر گرفت. در چنین شرایطی، داشتن تجهیزات امنیتی بیشتر در هر سازمان لزوماً مشکل را حل نمی‌کند. مهم‌تر این است که بدانیم گلوگاه‌های اصلی کجا هستند و اگر یکی از آنها دچار اختلال شد، چه خدماتی تحت تأثیر قرار می‌گیرند. کشوری که نمی‌داند کدام زیرساخت‌ها گلوگاه هستند، ممکن است در زمان بحران تازه متوجه شود که چند خدمت متفاوت، در واقع به یک نقطه مشترک وابسته بوده‌اند.

در سال‌های گذشته، توسعه دولت دیجیتال بیشتر با ایجاد سامانه و متصل کردن دستگاه‌ها دنبال شده است. آیا ممکن است همین مسیر، به جای افزایش تاب‌آوری، آسیب‌پذیری را بیشتر کرده باشد؟ این احتمال جدی است؛ البته مشکل خودِ اتصال سازمان‌ها نیست. برای ارائه بسیاری از خدمات عمومی، ارتباط میان دستگاه‌ها ضروری است. مسئله زمانی آغاز می‌شود که اتصال را با یکپارچگی اشتباه بگیریم. یکپارچگی فقط این نیست که دو سامانه بتوانند داده رد و بدل کنند. فرآیندها، داده‌ها، مسئولیت‌ها و استانداردها نیز باید هماهنگ باشند. اگر هر سازمان ابتدا سامانه خودش را بسازد و بعد صرفاً برای تبادل داده، رابطه‌هایی میان سامانه‌ها ایجاد کند، ممکن است به جای یک معماری منسجم، شبکه‌ای از وابستگی‌های پیچیده شکل بگیرد. همین مسئله در زندگی روزمره مردم نیز دیده می‌شود. شهروند برای دریافت یک خدمت ممکن است مجبور شود چند بار اطلاعاتی را وارد کند که دستگاه‌های دولتی از قبل در اختیار دارند، یا برای یک خدمت ساده از چند سامانه عبور کند. در این حالت، فناوری به جای حذف پیچیدگی، آن را به محیط دیجیتال منتقل کرده است. در طراحی زیرساخت‌های حیاتی باید به اصل حداقل وابستگی لازم توجه کرد. ارتباط باید برقرار باشد، اما به اندازه‌ای که برای ارائه خدمت ضروری است؛ دسترسی‌ها محدود باشند؛ نقاط حساس قابل شناسایی باشند و در صورت بروز حادثه بتوان یک بخش را از بخش دیگر جدا کرد، بدون اینکه کل خدمت از کار بیفتد.

یک دغدغه عمومی این است که وقتی همه‌چیز دیجیتال می‌شود، اگر زیرساخت دچار اختلال شود، خود مردم بیشترین آسیب را می‌بینند. در یک حمله گسترده سایبری، زندگی روزمره مردم از چه مسیرهایی می‌تواند تحت تأثیر قرار گیرد؟

اثر یک حمله گسترده سایبری الزاماً با قطع کامل اینترنت یا خاموش شدن همه سامانه‌ها آغاز نمی‌شود. ممکن است مجموعه‌ای از اختلال‌های ظاهراً کوچک شکل بگیرد که در کنار هم، اثر بزرگی ایجاد کنند. برای مردم، اولین نشانه می‌تواند مشکل در پرداخت، خدمات بانکی، دریافت پیام تأیید، دسترسی به یک سامانه دولتی یا دریافت یک استعلام باشد. اگر این اختلال‌ها همزمان یا پشت سر هم در چند حوزه رخ دهند، اثر آنها بسیار بیشتر از هر اختلال به‌تنهایی خواهد بود. وقتی مردم احساس می‌کنند دسترسی آنها به پول یا خدمات مالی مختل شده است، مسئله از سطح فنی عبور می‌کند و وارد قلمرو اقتصاد رفتاری می‌شود. در آن مرحله، هراس و نااطمینانی می‌تواند به اندازه خود اختلال اهمیت پیدا کند. به همین دلیل، برای هر زیرساخت حیاتی باید یک سؤال ساده مطرح شود: اگر این خدمت برای چند ساعت از دسترس خارج شود، چه اتفاقی برای زندگی مردم می‌افتد؟ اگر پاسخ این باشد که بیمارستان، بانک، تجارت، حمل‌ونقل یا خدمات عمومی دچار اختلال جدی می‌شوند، آن خدمت دیگر یک سامانه عادی نیست؛ یک زیرساخت حیاتی است و باید با سطح بالاتری از تاب‌آوری طراحی شود.

شما بر تاب‌آوری تأکید دارید. برای افکار عمومی، تاب‌آوری دقیقاً یعنی چه؟ آیا منظور این است که هیچ‌گاه سامانه‌ای از کار نیفتد؟

نه. تاب‌آوری دقیقاً از جایی شروع می‌شود که بپذیریم اختلال ممکن است رخ دهد. تاب‌آوری یعنی اگر حادثه‌ای رخ داد، بتوان شدت و دامنه آن را محدود کرد، خدمات ضروری را ادامه داد و سامانه را در کوتاه‌ترین زمان ممکن به وضعیت عادی برگرداند. این تفاوت مهمی با نگاه سنتی به امنیت دارد. در نگاه سنتی، سازمان تلاش می‌کند از نفوذ جلوگیری کند؛ اما در رویکرد تاب‌آوری، در کنار پیشگیری، برای زمانی که دفاع شکست می‌خورد نیز برنامه داریم. در نظام بانکی این تفاوت روشن است. اگر یک بانک پس از حمله بتواند خدمات حیاتی را از مسیر پشتیبان ادامه دهد، اثر حادثه محدودتر خواهد بود؛ اما اگر همه مسیرها به یک زیرساخت وابسته باشند و هیچ جایگزینی وجود نداشته باشد، یک حمله محدود می‌تواند به بحران اقتصادی تبدیل شود. تاب‌آوری چند جزء دارد: معماری توزیع‌شده، پشتیبان واقعی، مسیر جایگزین، بازیابی سریع، تمرین و آمادگی نیروی انسانی. موضوع مهم این است که نسخه پشتیبان روی کاغذ کافی نیست. باید آن را آزمایش کرد. باید سازمان را در شرایطی قرار داد که بخشی از زیرساخت عمداً از دسترس خارج شود و سپس دید آیا واقعاً می‌تواند خدمت را ادامه دهد یا خیر. امنیت واقعی در روز عادی کمتر دیده می‌شود؛ ارزش آن در روز بحران مشخص خواهد شد.

اگر مهاجم نتواند سیستم‌ها را برای مدت طولانی از کار بیندازد اما بتواند به داده‌های مردم یا اطلاعات حساس حاکمیتی دسترسی پیدا کند، آیا این سناریو از نظر شما کم‌خطرتر است؟

لزومی ندارد. گاهی نشت داده از خود اختلال نیز خطرناک‌تر است، زیرا اختلال ممکن است پس از چند ساعت یا چند روز برطرف شود، اما داده‌ای که افشا شده دیگر به حالت محرمانه بازنمی‌گردد. داده امروز یکی از مهم‌ترین دارایی‌های حاکمیتی است. اطلاعات هویتی، مالی، درمانی، مکانی و ارتباطی، اگر کنار هم قرار بگیرند، فقط مجموعه‌ای از اطلاعات پراکنده نیستند؛ تصویری بسیار دقیق از افراد، سازمان‌ها و جامعه ایجاد می‌کنند. از این جهت، موضوع فقط حریم خصوصی نیست. داده می‌تواند بر امنیت، اقتصاد، تصمیم‌سازی و حتی مدیریت بحران اثر بگذارد. در عین حال، پراکندگی مسئولیت نیز یک خطر است. داده میان چند سازمان توزیع شده و هر سازمان بخشی از آن را در اختیار دارد، اما همیشه روشن نیست چه نهادی مسئول نهایی حفاظت، یکپارچگی و دسترسی صحیح به آن است. در چنین شرایطی، حکمرانی داده اهمیت پیدا می‌کند. باید مشخص باشد چه داده‌ای جمع‌آوری می‌شود، چرا جمع‌آوری می‌شود، چه کسی به آن دسترسی دارد، چه مدت نگهداری می‌شود و در صورت رخداد، چه نهادی باید پاسخ‌گو باشد. اگر این قواعد روشن نباشد، فناوری امنیتی به‌تنهایی کافی نیست. نشت داده می‌تواند اعتماد عمومی را نیز کاهش دهد. وقتی مردم احساس کنند اطلاعات شخصی آنها ممکن است در یک حادثه افشا شود، اعتماد آنها به خدمات دیجیتال کاهش پیدا می‌کند؛ و اینجاست که حفاظت از داده فقط یک مسئله فنی نیست؛ بلکه بخشی از اعتماد عمومی به نهادهای دیجیتال کشور است.

در کنار مسئله داده، یک بحث دیگر هم مطرح است: استقلال دیجیتال. بسیاری از مردم تصور می‌کنند وقتی سرورها داخل کشور هستند، پس زیرساخت نیز کاملاً در اختیار کشور است. این برداشت تا چه اندازه درست است؟

این برداشت فقط بخشی از واقعیت را توضیح می‌دهد. محل استقرار مرکز داده مهم است، اما حاکمیت دیجیتال فقط به جغرافیا محدود نمی‌شود. باید کل زنجیره فناوری را دید؛ از سخت‌افزار و سیستم‌عامل گرفته تا نرم‌افزار، مجازی‌سازی، سازوکارهای به‌روزرسانی، خدمات ابری و نیروی انسانی متخصص. ممکن است سرور داخل کشور باشد، اما اگر بخش‌هایی از فناوری آن به زنجیره‌ای وابسته باشد که در شرایط بحران کنترل آن در اختیار ما نیست، هنوز یک وابستگی مهم باقی مانده است. البته این به معنای کنار گذاشتن همه فناوری‌های خارجی نیست. هیچ کشوری در دنیای امروز همه فناوری‌های مورد نیاز خود را به‌طور کامل در داخل تولید نمی‌کند. مسئله اصلی، شناخت و مدیریت وابستگی‌هاست. باید بدانیم کدام وابستگی برای کشور حیاتی است، کدام یک قابل جایگزینی است و برای کدام مورد باید ذخیره، گزینه جایگزین یا توان داخلی ایجاد شود. در سیاست‌گذاری، وابستگی‌ای خطرناک است که هم حیاتی باشد، هم جایگزین نداشته باشد و هم در زمان بحران قابل مدیریت نباشد. بنابراین استقلال دیجیتال را نباید با داخل یا خارج بودن یک سرور اندازه گرفت؛ باید با یک سؤال عملی سنجید: اگر زنجیره خارجی فناوری برای مدتی مختل شد، آیا هنوز می‌توانیم خدمات حیاتی خود را ادامه دهیم؟ اگر پاسخ مثبت باشد، یعنی وابستگی را مدیریت کرده‌ایم. اگر پاسخ منفی باشد، صرفاً قرار گرفتن سرور در داخل کشور مشکل را حل نمی‌کند.

اگر بخواهیم به دنبال راه‌حل باشیم، اولویت با خرید تجهیزات بیشتر است، یا باید ساختار حکمرانی و معماری دیجیتال را تغییر داد؟

خرید تجهیزات لازم است، اما اگر معماری و حکمرانی اصلاح نشود، تجهیزات جدید هم در همان ساختار قبلی قرار می‌گیرند و الزاماً نتیجه متفاوتی ایجاد نمی‌کنند. به نظر من، اصلاح باید از سه سطح آغاز شود. سطح نخست، معماری است. باید گلوگاه‌های مهم کشور شناسایی شوند؛ مشخص شود کدام خدمات به یک نقطه مشترک وابسته‌اند؛ نقاط شکست واحد کاهش پیدا کنند؛ زیرساخت‌های مهم توزیع شوند و برای خدمات حیاتی مسیرهای جایگزین واقعی ایجاد شود. سطح دوم، حکمرانی است. باید نهادی وجود داشته باشد که معماری دیجیتال را در مقیاس ملی ببیند، نه فقط در محدوده یک وزارتخانه یا سازمان. ممکن است هر سازمان برای خودش تصمیم درستی بگیرد، اما در مجموع، حاصل این تصمیم‌ها ساختاری پرریسک ایجاد کند. سطح سوم، آمادگی واقعی است. باید سناریوی حمله و اختلال را پیش از وقوع تمرین کرد. نه صرفاً با تهیه یک گزارش، بلکه با یک آزمون واقعی که مشخص کند اگر بخشی از زیرساخت از دسترس خارج شد، چه کسی تصمیم می‌گیرد، چه کسی خدمت را ادامه می‌دهد، داده از کجا بازیابی می‌شود و چگونه با مردم ارتباط برقرار خواهد شد. در هر بحران، آنچه بیش از همه اهمیت دارد زمان است! اگر سازمانی برای تصمیم‌های اولیه خود ساعت‌ها یا روزها زمان لازم داشته باشد، حتی بهترین تجهیزات امنیتی نیز نمی‌توانند خسارت را به‌طور کامل کاهش دهند.

برخی برای مقابله با تهدیدهای سایبری، قطع یا محدود کردن اینترنت بین‌الملل را راهی برای کاهش آسیب‌پذیری می‌دانند؛ نظر شما چیست؟

قطع اینترنت ممکن است در یک سناریوی بسیار خاص و برای مدت محدود، بخشی از یک اقدام اضطراری باشد، اما نمی‌توان آن را جایگزین امنیت سایبری دانست. این دو مسئله اساساً متفاوت‌اند. امنیت یعنی بتوانیم زیرساخت را حتی در شرایط تهدید، ایمن و قابل استفاده نگه داریم؛ قطع ارتباط در واقع کاهش یا حذف بخشی از قابلیت ارتباطی است. مشکل از جایی آغاز می‌شود که تصور کنیم با قطع ارتباط، تهدید هم از بین می‌رود. بسیاری از آسیب‌پذیری‌های ما در داخل شبکه‌ها، سامانه‌های سازمانی، نرم‌افزارهای مورد استفاده، تجهیزات، مراکز داده و زنجیره تأمین فناوری وجود دارند. بنابراین قطع اینترنت لزوماً این آسیب‌پذیری‌ها را برطرف نمی‌کند. از طرف دیگر، اینترنت فقط مسیر ورود تهدید نیست؛ یکی از ابزارهای دفاع نیز هست. سازمان‌ها برای دریافت به‌روزرسانی‌های امنیتی، تبادل اطلاعات درباره تهدیدهای جدید، دسترسی به منابع فنی، همکاری با شرکت‌ها و مراکز تخصصی و حتی بازیابی برخی خدمات به ارتباطات بین‌المللی نیاز دارند. اگر ارتباط را به شکل گسترده قطع کنیم، ممکن است بخشی از ظرفیت دفاعی خودمان را نیز تضعیف کنیم. پیامد اقتصادی آن هم بسیار جدی است. امروز یک کسب‌وکار کوچک ممکن است فروش، پرداخت، تبلیغات، ارتباط با مشتری، خدمات پس از فروش و تأمین‌کنندگان خود را بر بستر اینترنت انجام دهد. قطع اینترنت فقط شرکت‌های بزرگ فناوری را متضرر نمی‌کند؛ فروشگاهی که از شبکه‌های اجتماعی مشتری می‌گیرد، پزشکی که با سامانه‌های برخط کار می‌کند، پلتفرمی که خدمات ارائه می‌دهد و حتی کسب‌وکاری که برای ارتباط با تأمین‌کننده خود به اینترنت وابسته است، تحت تأثیر قرار می‌گیرد. اما شاید مهم‌تر از هزینه آن، مسئله اعتماد باشد. اگر مردم تجربه کنند که در هر بحران، اولین راه‌حل قطع ارتباط است، به‌تدریج این تصور شکل می‌گیرد که زیرساخت دیجیتال کشور در برابر بحران تاب‌آوری ندارد. در حالی که هدف حکمرانی دیجیتال باید دقیقاً برعکس این باشد.

و پرسش آخر؛ اگر بخواهید یک هشدار روشن به سیاست‌گذاران و یک توضیح روشن به مردم بدهید، آینده را چگونه می‌بینید؟ آیا واقعاً ممکن است کشوری بدون جنگ نظامی، فقط از طریق زیرساخت دیجیتال دچار بحران گسترده شود؟

بله، چنین امکانی وجود دارد، اما نباید آن را یک پیش‌بینی آخرالزمانی دانست. مسئله بیشتر به تصمیم‌هایی مربوط می‌شود که امروز درباره معماری زیرساخت‌های کشور می‌گیریم. کشوری که خدمات حیاتی خود را بیش از اندازه متمرکز می‌کند، وابستگی‌های متقابل را نمی‌شناسد، داده‌های حساس را بدون حکمرانی روشن نگهداری می‌کند و برای زمان بحران مسیر جایگزین ندارد، به‌تدریج آسیب‌پذیر می‌شود؛ حتی اگر در روزهای عادی همه سامانه‌ها به‌ظاهر درست کار کنند. خطر واقعی هم لزوماً یک خاموشی کامل نیست. ممکن است چند اختلال در بانک، ارتباطات، خدمات عمومی یا داده در فاصله‌ای کوتاه رخ دهد. هرکدام به‌تنهایی قابل مدیریت باشند، اما مجموع آنها بر فعالیت اقتصادی و اعتماد عمومی اثر بگذارد. بخشی از خسارت بحران حتی بعد از بازگشت سامانه‌ها باقی می‌ماند.

اگر مردم تجربه کنند که یک خدمت مهم چند بار از دسترس خارج شده یا اطلاعاتشان در معرض خطر بوده، رفتار آنها تغییر می‌کند و بازگرداندن اعتماد دشوارتر از تعمیر یک سامانه خواهد بود. به همین دلیل، باید در نگاه خود به امنیت سایبری تجدیدنظر کنیم. تا امروز بخش زیادی از تمرکز بر این بوده که چگونه جلوی حمله را بگیریم. این کار همچنان مهم است، اما کافی نیست.

باید همزمان بدانیم اگر نفوذ اتفاق افتاد، چگونه دامنه آسیب را محدود کنیم، چگونه خدمات حیاتی را ادامه دهیم و چگونه اعتماد مردم را حفظ کنیم. فناوری به خودی خود امنیت نمی‌آورد. معماری، حکمرانی، آمادگی و مسئولیت‌پذیری است که امنیت را به تاب‌آوری تبدیل می‌کند.

چرنوبیل دیجیتال زمانی شکل می‌گیرد که یک کشور تصور کند صرفاً با بیشتر کردن سامانه‌ها و بیشتر کردن اتصال، قدرتمندتر شده است؛ در حالی که ممکن است همزمان نقاط وابستگی بیشتری ایجاد کرده باشد. قدرت واقعی زیرساخت دیجیتال در روز عادی سنجیده نمی‌شود بلکه زمانی معلوم می‌شود که بخشی از سیستم از کار افتاده، اما خدمات حیاتی همچنان ادامه دارند، مردم سردرگم نمی‌شوند و کشور می‌تواند به وضعیت عادی بازگردد. در آینده برای فلج کردن یک کشور شاید نیازی به شلیک حتی یک گلوله نباشد؛ کافی است یک گلوگاه دیجیتال پیدا شود و ما پیش از آن، بیش از اندازه به آن وابسته شده باشیم.

خبر

جشنواره سیب؛ آغاز مسیر اقتصادسمیرم

فرماندار سمیرم گفت: نخستین جشنواره سیب این شهرستان با هدف تبدیل سیب سمیرم به یک زنجیره ارزش اقتصادی، توسعه بازار، جذب سرمایه‌گذاری، تقویت صنایع تبدیلی و بسته‌بندی و افزایش سهم باغداران از درآمد این محصول برگزار می‌شود.

محمود مسلم‌زاده اظهار کرد: این جشنواره باید فراتر از یک رویداد فرهنگی و برداشت محصول، به بستری برای ایجاد حرکت اقتصادی، اجتماعی و گردشگری در شهرستان تبدیل شود. او با اشاره به جایگاه سمیرم به عنوان یکی از قطب‌های تولید سیب کشور افزود: بخش قابل توجهی از اقتصاد و معیشت مردم شهرستان به سیب وابسته است، اما سهم باغداران از ارزش اقتصادی نهایی محصول متناسب با زحمات و هزینه‌های تولید نیست. مسلم‌زاده مهم‌ترین بخش جشنواره را بخش اقتصادی و تجاری دانست و تأکید کرد: باید از حضور تولیدکنندگان، صادرکنندگان، خریداران، سرمایه‌گذاران و مسئولان برای ایجاد ارتباطاتی استفاده کنیم که پس از پایان جشنواره نیز ادامه داشته باشد. او افزود: هدف ما این است که جشنواره از «صحنه» به «میز مذاکره» و از «میز مذاکره» به «قرارداد و سرمایه‌گذاری» برسد. فرماندار سمیرم با اشاره به افزایش هزینه نهاده‌ها، دستمزد، کود و سم، آبیاری، بسته‌بندی و حمل‌ونقل، محدودیت منابع آبی و خسارت‌های طبیعی بیان کرد: باید نگاه خود را از تولید بیشتر به سمت اقتصادی‌تر کردن تولید و افزایش سهم باغدار از ارزش نهایی محصول تغییر دهیم.

بیانیه کارکنان مجتمع‌های دخانیات

کارکنان مجتمع دخانیات نسبت به فراخوان شناسایی بهره‌بردار و سرمایه‌گذار شرکت دخانیات ایران اعتراض کردند و خواستار شفاف‌سازی شدند.

به گزارش مهر، شرکت دخانیات کشور درحالی بار دیگر مسئله واگذاری مجتمع های تحت پوشش خود را درسراسر ایران مطرح کرده و این واگذاری را در راستای تحقق اهداف اصل۴۴ قانون اساسی و برنامه های کلان دولت و با استناد به مصوبات مجمع عمومی مبنی بر مردمی سازی اقتصاد و ارتقای کارآمدی بنگاه های اقتصادی می داند. کارکنان مجتمع های دخانیات به عنوان یکی از مخالفان جدی این واگذاری به تجربه تلخ واگذاری این شرکت در دهه ۹۰ اشاره می‌کنند که بالغ بر ۱۵سال گذشته در حالی این مسئله مطرح شد که ۵۵ درصد سهام شرکت جای بدهی‌های دولت به صندوق فولاد واگذار شد (در واقع شرکت دخانیات و کارکنان آن قربانی بدهی‌های دولت شدند) و از سال ۹۴ و ۹۵ کارکنان دخانیات در سراسر کشور به صورت داوطلبانه و قانونی سهام دار و سهام بر بخشی از درصد باقیمانده دخانیات شدند،بطوری که هرماه بخشی از حقوق دریافتی آنها کسر می‌شود اما باگذشت بیش از ۱۰ سال هنوز سودی از فروش عرضه وصادرات دخانیات به جیب هیچ یک از آنها نرفته است. محمود ساسانی، عضو شورای اسلامی کار مجتمع های دخانیات در این زمینه گفت: در حالی امروز بار دیگر مسئله واگذاری شرکت‌های دخانیات در کل کشور مطرح شده که سهامداران (کارمندان و کارگران) از آن هیچ گونه اطلاعی ندارند و این عدم آگاهی نگرانی آنها را افزون تر کرده است .او به صدور بیانیه کارکنان مجتمع های دخانیات اشاره کرد و گفت: کشاورزان، کارگران و کارمندان دخانیات امروز به عنوان سهامداران مجتمع دخانیات ، آگهی فراخوان شناسایی،بهره بردار و سرمایه گذار مجتمع دخانیات ایران را بدون اذن سهام‌بران یک تخلف قانونی می دانند و نسبت به این تصمیم ابراز نگرانی کردند . ساسانی که سابقه نزدیک به ۲۰ سال کار در مجتمع دخانیات را دارد در خصوص ابعاد بیشتر این ماجرا اذعان کرد: این فراخوان درحالی است که مسئولان باید پیش از هر گونه تصمیم، تضمین های رسمی و لازم الاجرا در باره حفظ اشتغال، حقوق و مزایا، امنیت شغلی ، سوابق بیمه ای ، سنوات خدمت و سایر حقوق مکتسبه کارکنان را اخذ و سپس اقدام کنند. او ادامه داد: شرکت دخانیات ایران هم اکنون حدود ۵ هزار نیروی کار دارد. احمدکریمی دیگر عضو شورای اسلامی کار مجتمع های دخانیات افزود: هر گاه تصمیمات اقتصادی بدون بررسی همه جانبه، نظارت کافی،احراز دقیق اهلیت، شفافیت کامل و تضمین حقوق ذی نفعان اتخاذ شود، ممکن است اهداف اولیه تحقق نیابد و مجموعه با چالش های مدیریتی، اقتصادی، تولیدی و اجتماعی مواجه شود. از این رو شوراهای اسلامی کار معتقدند که تجربه دهه ۹۰ باید به عنوان یک سرمایه مدیریتی و حقوقی مورد آسیب‌شناسی قرار گیرد و تصمیمات امروز نباید بدون بهره‌گیری از درس آموخته های گذشته اتخاذ شود. او خصوصی سازی مجتمع های دخانیات را صرفا یک تصمیم اداری یا یک جابجایی مدیریتی نمی داند و می گوید: این مسئله بحث بر سر آینده تولید، سرمایه های شرکت، نیروی انسانی، توتونکاران، تنباکو کاران، دارایی‌های ملی و نحوه اداره یکی از قدیمی ترین مجموعه های تولیدی کشور است بر همین اساس شوراهای اسلامی کار شرکت دخانیات لازم می‌دانند با واگذاری راهبری، بهره‌برداری و فعالیت های عملیاتی و تولیدی شرکت دخانیات ایران به اشخاص یا مجموعه های ثالث، بدون ضرورت اثبات شده ، بدون شفافیت کامل، بدون مطالعاتکارشناسی و بدون تضمین های محکم و قابل اجرا صراحتا مخالفت کنند. این عضو شورای اسلامی کار مجتمع‌های دخانیات خاطرنشان کرد: بر اساس قانون کار جمهوری اسلامی ایران، قانون اجرای سیاست های کلی اصل ۴۴ قانون اساسی ، قانون ارتقای سلامت نظام اداری و مقابله با فساد و سایر قوانین مرتبط، هرگونه واگذاری تغییر در شیوه اداره یا بهره برداری از بنگاه های اقتصادی باید با رعایت کامل اصول شفافیت، پاسخگویی ، احراز اهلیت ، حفظ حقوق مکتسبه کارکنان ، استمرار تولید، نظارت موثر وصیانت از منافع عمومی انجام پذیرد.