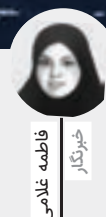


زنجیره امنیت دیجیتال

کارشناسان، راهکار برون رفت از بحران امنیت سایبری را در اصلاح نگرش مدیران، حمایت از نخبگان، آموزش عملی کارکنان و نوسازی زیرساخت های فنی می دانند



گزارش
روز

جنگ همیشه قرار نیست بوی باروت و صدای انفجار بدهد؛ گاهی در سکوت کامل یک اتاق سرور، میان سطرهای بی پایان کد و پشت صفحه نمایش هایی که بی وقفه روشن اند، یک زلزله خاموش رخ می دهد. روزی که بمب بنزین ها از کار می افتند، سامانه های دانشگاهی و بانکی دچار اختلال می شوند. برخی خبرگزاری ها و سرویس های اینترنتی از دسترس خارج می شوند یا شبکه توزیع برق در اوج نیاز با مشکل روبه رو می شود. تازه روشن می شود که امنیت سایبری فقط یک مسئله فنی نیست، بلکه نبض تپنده زندگی روزمره است. اما مسئله فقط وقوع حمله نیست؛ آنچه این تهدید را پیچیده تر و نگران کننده تر می کند، آسیب پذیری هایی است که از درون شکل می گیرد. حفاظت از این نبض دیجیتال، امروز به معادله ای چندوجهی و دشوار بدل شده است؛ معادله ای که در آن، کمبود نیروی متخصص، نگاه هزینه ای به امنیت، بودجه های ناکافی و تداوم استفاده از سامانه های قدیمی و نایمن، هرکدام سهمی جدی در تضعیف لایه های دفاعی دارند.

ریشه های چندگانه یک بحران مستمر

دکتر سید امین حسینی سنو، استاد تمام گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد، در گفت وگو با خبرنگار ما، معتقد است هرچند تهدیدهای بیرونی، جدی است، پاشنه آشیل اصلی را باید در ترک های ساختاری لایه های مدیریتی و فنی کشور جست و جو کرد؛ چالشی که نشان می دهد فاصله میان استانداردهای پدافند غیرعامل و اقدامات عملی، همچنان نگران کننده است. بررسی ریشه ای حملات اخیر به زیرساخت ها، نشان می دهد که با یک پدیده تک عاملی روبه رو نیستیم. حسینی سنو در بخش نخست تحلیل خود، عوامل محرک این بحران را به پنج شاخه متمایز تقسیم می کند که نخستین آن ها، انگیزه های فرامرزی است. موقعیت راهبردی کشور همواره سبب شده است سامانه های حیاتی ما سیل حملات سازمان یافته و مستمر دولت های متخاصم همچون رژیم صهیونیستی و ایالات متحده آمریکا باشند؛ هجمه هایی که هدف اول و آخرشان، فلج کردن خدمات عمومی و ایجاد نارضایتی های مدنی است. یکی از نکاتی که در تحلیل این استاد دانشگاه خودنمایی می کند، پیوند میان مهاجرت و امنیت است. درحالی که تقابل با بازیزگران دولتی متخاصم نظیر رژیم صهیونیستی و آمریکا، هوشیاری صد درصدی می طلبد، واقعیت تلخ مهاجرت نخبگان، دست ساختارهای امنیتی ما را تا حدی خالی کرده است. به باور او، وقتی متخصصان ترازاول به دلیل نبود مشوق ها یا شرایط نامساعد، به جای ماندن، رفتن را برمیگزینند، در عمل «مغز متفکر» دفاع سایبری کشور تضعیف می شود. در چنین شرایطی، حتی اگر بهترین تجهیزات دنیا را هم در اختیار داشته باشیم، بدون کارشناس خبره ای که بتواند بحران را پیش بینی و مدیریت کند، دژهای دیجیتال ما فرومی ریزند.

بار مدیریت داخلی؛ سنگین تر از تحریم ها

این استاد دانشگاه در ادامه، انگشت اتهام را به سمت نگاه سنتی مدیران می گیرد، برای بسیاری از مدیران ارشد، امنیت سایبری هنوز هم یک «هزینه اضافه» و «سربار» است نه یک «سرمایه گذاری حیاتی». نتیجه این رویکرد، تخصیص بودجه های قطره چکانی و بی توجهی به نوسازی زیرساخت هاست. حسینی سنو معتقد است تحریم های بین المللی اگرچه دسترسی به فناوری های نوین و لایسنس های معتبر را دشوار و هزینه بر کرده، اما «انفعال مدیریتی»، باری سنگین تر از تحریم بر دوش امنیت کشور گذاشته است. استفاده از سامانه های قدیمی و وصله پینه شده، دقیقاً همان فرش قرمز است که برای هرکها پهن کرده ایم.

دیوار انسانی؛ ضعیف تر از سپر دفاعی

شاید تکان دهنده ترین بخش در صحبت های حسینی این باشد

که «۹۵ درصد حملات سایبری از طریق «خطای انسانی» به ثمر می رسد، این یعنی پیچیده ترین سپر دفاعی هم حریف یک کارمند نا آگاه که روی یک لینک آلوده کلیک می کند یا رمز عبور ساده ای را برمیگزیند، نمی شوند.» از نگاه او، در این لایه، یاد و چالش اساسی روبه رو هستیم؛ یکی آموزش های فرمالیته؛ به عبارتی دوره هایی که فقط برای پر کردن رزومه ها و رفع تکلیف برگزار می شوند، اما در عمل، هیچ مهارتی به کاربر اضافه نمی کنند. چالش دیگر، فقدان فرهنگ امنیتی است؛ امنیت سایبری هنوز به عنوان یک «فرهنگ همگانی» در سازمان ها نهادینه نشده است. تا زمانی که هر کارمند خود را یک مرزبان سایبری نداند، نفوذ به زیرساخت ها به سادگی یک کلیک، باقی خواهد ماند. در همین لایه فقدان فرهنگ امنیتی، ضعف دانش تخصصی مدیران ارشد نیز خودنمایی می کند. به عقیده حسینی سنو، تا زمانی که لایه مدیریتی درک درستی از پیامدهای فاجعه بار نشست اطلاعات نداشته باشد، پشتیبانی از تیم های فنی در حد شعار باقی می ماند.

جای خالی واکنش سریع

در لایه فنی و زیرساختی اما اوضاع به مراتب پیچیده تر است. استاد تمام گروه مهندسی کامپیوتر دانشگاه فردوسی مشهد تأکید می کند: استفاده گسترده از سامانه های فرسوده و به روز نشده، عملاً کار را برای مهاجمان آسان کرده است. ازسوی دیگر، ضعف در سیستم های دسترسی و اجرانشدن سازوکارهای ساده ای چون احراز هویت دو مرحله ای، به هرکها اجازه می دهد با هک کردن یک حساب کاربری ساده، به کل شبکه نفوذ کنند. همچنین نبود یک طرح مدون برای واکنش نشان دادن به حادثه، باعث می شود که سازمان ها در ساعات اولیه پس از وقوع حمله، دچار انفعال و سردرگمی شدید شوند و نتوانند خدمات خود را به سرعت احیا کنند.

نسخه درمان، از تغییر نگاه تا تغییر ساختار

عبور از این وضعیت بحرانی و ارتقای امنیت زیرساخت ها، نیازمند یک نقشه راه عملی و چندوجهی است. استاد دانشگاه فردوسی مشهد برای برون رفت از این چالش ها، چهار محور اساسی را پیشنهاد می دهد که نخستین گام، اصلاح سیاست گذاری کلان و تغییر فوری نگرش مدیران به موضوع امنیت است؛ «باید با برگزاری کارگاه های توجیهی، مدیران را متوجه این واقعیت کرد که امنیت هزینه بر نیست، بلکه ضامن بقای کل سازمان است. درکنار آن، تخصیص بودجه های مستقل و نظارت دقیق بر نحوه هزینه کردن آن ها، اهمیتی مضاعف دارد. دومین اقدام فوری، طراحی بسته های حمایتی و انگیزشی برای متخصصان داخلی به منظور کاهش نرخ مهاجرت نخبگان و همچنین بازنگری در شیوه آموزش کارکنان با رویکردی کاملاً عملی و سناریو محور است.» در بعد فنی نیز، او بر لزوم پیاده سازی سپر دفاعی نسل جدید با توانایی تحلیل عمیق رفتار شبکه، تأکید می کند. الزام سازمان ها

به استفاده از احراز هویت چند عاملی، به روزرسانی مستمر و بدون تأخیر نرم افزارها، پشتیبان گیری مداوم و نگهداری داده های پشتیبان در بستری خارج از شبکه اصلی، برای مقابله با یاج افزارها و در نهایت انجام تست های نفوذ دوره ای، از دیگر الزاماتی است که باید انجام شود. حسینی سنو در پایان یادآوری می کند: امنیت در فضای تبادل اطلاعات، یک پروژه تمام شدنی نیست، بلکه یک «فرایند همیشگی» است. اگر امروز برای ترمیم دیوارهای انسانی و فنی خود هزینه نکنیم، فردا باید هزینه های گزاف تری را بابت قطعی خدمات و از دست رفتن امنیت ملی بپردازیم.

چالش های بومی سازی در زیرساخت های امنیتی

یکی از مباحث چالش برانگیز در سیاست گذاری های کلان فناوری کشور، بومی سازی ابزارها و سامانه های امنیتی است. دکتر بهره پور، مدیرکل فناوری اطلاعات دانشگاه آزاد اسلامی مشهد، معتقد است که استفاده از محصولات داخلی، در صورت برخورداری از استانداردهای فنی و کیفیت مناسب، می تواند گامی ارزشمند برای تقویت استقلال فناوری کشور باشد. با این حال، وی تأکید می کند که این امر تنها زمانی به یک مزیت راهبردی و واقعی تبدیل می شود که محصولات بومی در شاخص هایی نظیر کیفیت، پایداری عملیاتی، توان رقابت با نمونه های استاندارد را داشته باشند. به گفته این تحلیلگر، فرایند جایگزینی سامانه ها نباید براساس تصمیم های دستوری یا صرفاً تمرکز بر محل تولید محصول، انجام بگیرد. بهره پور تأکید می کند: تجهیزات و نرم افزارهای امنیتی، باید برپایه ارزیابی های دقیق فنی و منطقی بر نیازهای واقعی و عملیاتی هر سازمان انتخاب شود. اگر ابزاری بدون ممیزی های همه جانبه و بررسی های کافری جایگزین ابزار دیگری شود، نه تنها برخی قابلیت های حفاظتی حیاتی از دست می رود، بلکه ریسک های جدید و ناشناخته ای به سازمان تحمیل می شود، از این رو اصالت کارایی و پایداری محصول، همواره باید بر شعارهای بومی سازی ترجیح داده شود.

امنیت سایبری؛ معماری سه بعدی ابزار، فرایند و انسان

نگاه سنتی به امنیت سایبری، آن را به خرید تجهیزات گران قیمت یا نصب نرم افزارهای پیشرفته خلاصه می کند؛ دیدگاهی که به عقیده بسیاری از کارشناسان، خود بزرگ ترین روزه نفوذ است. بهره پور با نقد این رویکرد سخت افزار محور، یادآوری می کند: امنیت، محصول خرید تجهیزات نیست، بلکه یک زنجیره به هم پیوسته از سه رکن حیاتی یعنی «نیروی انسانی»، «فرایند های استاندارد» و «فناوری مناسب» است که باید به شکل هم زمان و متوازن تقویت شوند. وی با بیان اینکه تجهیزات بدون اجرای درست و نظارت مستمر کارایی نخواهند داشت، می افزاید: آموزش مداوم کارکنان، تدوین دستورالعمل های عملیاتی و نظارت دوره ای بر اجرای

آن ها، نقش کلیدی در کاهش آسیب پذیری ها ایفا می کند. بهره پور، بر این باور است که امنیت نباید به عنوان یک وصله اضطراری و پس از وقوع بحران به سامانه ها الحاق شود، بلکه باید از همان نخستین مراحل طراحی و توسعه خدمات دیجیتال، در تاروپود معماری سیستم ها جای گیرد تا پایداری درازمدت خدمات تضمین شود.

سپر بحران؛ از پیشگیری تا مدیریت حوادث ناگهزیر

در دنیای امروز هیچ حصار دیجیتالی، نفوذناپذیر نیست و احتمال وقوع حادثه همواره وجود دارد. مدیرکل فناوری اطلاعات دانشگاه آزاد اسلامی مشهد، با تأکید بر این واقعیت بیان می کند: هیچ سازمانی در دنیا، نمی تواند مدعی مصونیت کامل در برابر حملات سایبری باشد، از همین رو آنچه عیار پایداری یک زیرساخت را مشخص می کند، میزان آمادگی سازمان برای شناسایی به موقع تهدیدها، مهار سریع خسارات و بازگرداندن خدمات به حالت عادی در کوتاه ترین زمان ممکن است. به گفته وی، سازمان های حیاتی به ویژه بانک ها و دانشگاه ها، باید درکنار به کار بردن رویکردهای پیشگیرانه، برنامه های عملیاتی مشخصی برای سناریوهای مختلف بحران تدوین کنند. اجرای مانورهای دوره ای، شبیه سازی حملات و تعیین دقیق حدود وظایف و مسئولیت ها در زمان بحران، تاحد زیادی می تواند از آشننگی های پس از حمله جلوگیری کند و اثرات تخریبی نفوذها را به حداقل ممکن برساند.

زنجیره تأمین؛ بازتعریف مرزهای مسئولیت و پیمانکاری

یکی از نقاط کور در مدیریت امنیت فناوری اطلاعات، وابستگی فراینده سازمان ها به پیمانکاران متعدد است. بهره پور، زنجیره تأمین فناوری را از حساس ترین نقاط امنیت زیرساختی می داند و می افزاید: گستردگی پروژه ها از تولید نرم افزار تا مدیریت مراکز داده و شبکه، نیازمند شفافیت کامل در تقسیم مسئولیت هاست. به اعتقاد وی، اگر بانک ها و سازمان های بزرگ، دید کامل، مستقل و بدون واسطه ای به سامانه ها، سطوح دسترسی، تغییرات کدهای برنامه نویسی و وضعیت امنیتی خود نداشته باشند، پنهان پیمانکاری با ریسک های بزرگی مواجه خواهند شد. وی تصریح می کند: تقسیم وظایف نباید به معنای سلب مسئولیت نظارتی سازمان باشد؛ چراکه اگر هر بخش تنها قطعه کوچکی از پازل را ببیند و هیچ ناظر مستقلی بر کل زنجیره اشراف نداشته باشد، حفره های امنیتی تا زمان وقوع فاجعه، مخفی خواهند ماند. بهره پور در نهایت تأکید می کند که امنیت سایبری، یک پروژه باتاریخ انقضای مشخص نیست، بلکه فرایندی پویا و مستمر است که با گسترش خدمات دیجیتال، نیاز به بازنگری دائم دارد.