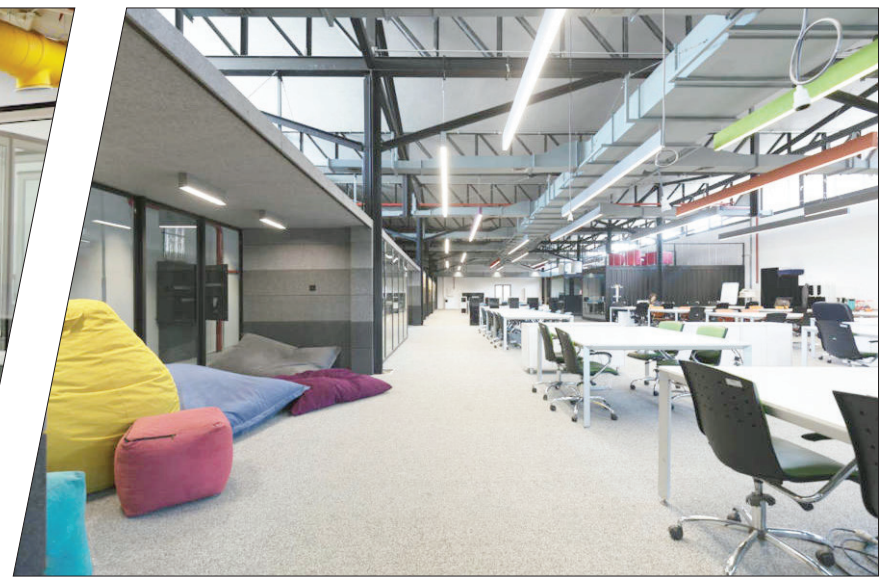

دارند را ناممکن می‌سازد.

از سوی‌دیگر، باتوجه به بین‌المللی بودن بازار رمزارز و لزوم اتصال به اینترنت جهانی برای اقداماتی مثل بازارگردانی، سرویس‌دهی به کاربران و مدیریت کیف‌پول‌ها، محدودیت‌های اینترنت بحران حمله سایبری را عمیق‌تر کرد. یکی از پیامدهای مستقیم نارسایی‌های زیرساختی در زمان وقوع حمله سایبری به نوبیتکس، اختلال عملکرد یا از کار افتادن سامانه‌های پایش است که خط اول دفاعی در برابر فعالیت‌های غیرمجاز محسوب می‌شوند.

در حالت عادی صرافی‌های رمزارز از این سامانه‌ها برای نظارت بر تراز و جریان دارایی‌ها، به‌ویژه در کیف‌پول‌های گرم بهره می‌برند و حتی برخی نیز تراکنش‌های مشکوک را در شبکه‌های اجتماعی گزارش می‌کنند. ۲۸ خردادماه که هکرها به نوبیتکس حمله کردند، به‌دلیل همین اختلالات زیرساختی، پیام‌های هشدار با تأخیر معناداری به نوبیتکس رسید و همین موضوع پنجره زمانی بهره‌برداری مهاجمان را گسترش داد و به آن‌ها فرصت داد تا حجم بیشتری از دارایی‌ها را از کیف‌پول‌های گرم نوبیتکس تخلیه کنند. درواقع تأخیر در هشدار، مستقیماً به افزایش مقیاس خسارت مالی نوبیتکس منجر شد.

از وجهی دیگر، ما می‌دانیم که حکمرانی دیجیتال کارآمد، متکی و متعهد به برنامه‌ریزی دقیق، ترسیم نقشه راه و تدوین پروتکل‌های ازپیش‌تعریف‌شده برای مدیریت بحران‌های امنیتی است. در چنین چارچوبی، واکنش به حوادثی مانند حمله سایبری، دسترسی از راه دور، امن و لایه‌بندی شده است؛ نه حضور فیزیکی. حادثه نوبیتکس دقیقاً ضعف در این حوزه را نیز نمایان ساخت. نیاز تیم فنی به حضور فیزیکی در دیتاسنترهای تهران برای قطع دسترسی مهاجم، یک گلوگاه بحرانی بود. این درحالی‌است که در آن شرایط جنگی نیروهای کلیدی نوبیتکس در دسترس نبودند و همین وابستگی فیزیکی نیز منجر به کُند کردن واکنش‌ها شد.

انتقال دارایی ناتمام ماند

تحلیل جامع بحران سایبری نوبیتکس نشان می‌دهد که تأثیرات مخرب محدودیت‌های اینترنتی، فراتر از اختلال در فرآیند واکنش به حادثه بوده و ابعاد پیشگیرانه و استراتژیک گسترده‌تری را نیز در برمی‌گیرد. گفته می‌شود از چندروز قبل از حمله هکرها، مدیران نوبیتکس هم‌زمان که تقاضای کاربران برای برداشت‌های رمزارزی افزایش می‌یافت، موجودی کیف‌پول‌های گرم خود را افزایش می‌دادند.

این تصمیمی استراتژیک بود و هدف آن، تضمین تداوم بی‌وقفه خدمات و پاسخگویی به نیاز کاربران بود. بااین‌حال شب قبل از حادثه، زمانی که تیم‌های فنی در حال اجرای پروتکل امنیتی استاندارد، یعنی انتقال وجوه مازاد از کیف‌پول‌های گرم به کیف‌پول‌های سرد بودند، با اختلال گسترده در اینترنت بین‌الملل مواجه شدند و فرآیند تخلیه امن وجوه ناتمام ماند.

نکته اینکه در صرافی‌های رمزارز، بخش اعظم دارایی‌های کاربران در کیف‌پول‌های سرد و آفلاین نگهداری می‌شود که مصون از حمله و آسیب است. بااین‌حال حفظ درصدی از دارایی‌ها به‌عنوان سرمایه در گردش در کیف‌پول‌های گرم برای پردازش تراکنش‌های روزمره اجتناب‌ناپذیر است. در موضوع نوبیتکس به‌نظر می‌رسد قطعی اینترنت، باعث شد تا در لحظه حمله، حجمی بیش از حد معمول دارایی‌ها، در این کیف‌پول‌های آنلاین باقی بماند.

خلأ سیاست‌گذاری معقول

شهاب حسینی، کارشناس ارتباطات و فعال فضای مجازی معتقد است، جنگ ۱۲ روزه میان ایران و اسرائیل فراتر از جغرافیای نظامی، به بطن اقتصاد دیجیتال ایران ضربه زده است. او می‌گوید، اتفاق‌هایی مانند حمله سایبری به بزرگ‌ترین بازار رمزارزی کشور، فقط سطح ماجراست و اگر دقیق‌تر شویم به خلأیی بزرگ در سیاست‌گذاری معقول و حکمرانی اصولی فضای مجازی می‌رسیم.

او می‌گوید: «در شرایطی که دنیا امنیت سایبری را زیرساخت رشد دیجیتال می‌داند، در ایران اینترنت با هر بحران سیاسی یا امنیتی، به ابزاری برای انسداد تبدیل می‌شود. تجربه ثابت کرده که قطع ارتباطات به هیچ‌وجه مانع تهدیدات نمی‌شود، اما همواره ابزار مقابله را از دست شهروندان، کسب‌وکارها و حتی نهادهای خودی خارج می‌کند.»

به باور حسینی، اختلال و قطعی اینترنت، ارتباط مستقیمی با بحرانی‌تر شدن حمله سایبری به نوبیتکس داشته است. او چنین توضیح می‌دهد: «به‌رغم اینکه نوبیتکس با تکیه به منابع داخلی خود خسارت‌ها را جبران کرد و اجازه نداد به کاربران آسیبی وارد شود، براساس داده‌های موجود، زمان طلایی جلوگیری از گسترش این حمله مصادف بود با اختلالات گسترده اینترنت در کشور و قطعی یا اختلال شدید اینترنت که مانع از واکنش سریع تیم‌های امنیتی شد. مدیران این صرافی، هنوز تمام ابعاد و چالش‌های رخ‌داده در این مدت را شرح نداده‌اند، اما مشخص است که شرایطی بحرانی بر شرکت حاکم بوده است.»

حسینی به گزارش‌های کسب‌وکارها و نهادهای صنفی درباره افت شدید درآمد یا توقف خدمات بیش از ۸۰ کسب‌وکارهای آنلاین و زیان‌های ۱۰۰ درصدی برخی پلفترم‌ها اشاره می‌کند و توضیح می‌دهد که باوجود همه این آسیب‌ها، شرایط اینترنت هنوز به پیش از دوره بحران نرسیده است: «بیش از یک‌ماه از جنگ می‌گذرد، اما اینترنت ایران هنوز به حالت پایدار بازنگشته است. فعال‌سازی سیاست‌هایی نظیر اینترنت طبقاتی، عدم بازگشت پروتکل‌هایی مانند IPv۶، UDP، QUIC و اختلالات مداوم در سرویس‌های کلود، بخشی از موانع بازیابی وضعیت طبیعی اینترنت کشور است. اقشار مختلف اعم از کاربران عادی تا گیمرها، فریلنسرها، فین‌تک‌ها و فعالان بازار دیجیتال، همگی‌شان با مشکلات فنی گسترده دست‌وپنجه نرم می‌کنند.»

این فعال دسترسی به اینترنت آزاد هشدار می‌دهد، با چنین رویه‌ای آینده اقتصاد دیجیتال کشور روشن نیست: «اقتصاد دیجیتال ایران قرار بود موتور محرک رشد ایران در دهه آینده باشد اما در حال حاضر همه‌چیز در ابهام فرو رفته است. در شرایطی که جهان بر محور هوش مصنوعی، بلاک‌چین و فناوری‌های نو در حال پیش‌روی است، ایران با تصمیماتی که بعضاً غیرکارشناسی و گاه سیاسی هستند، عملاً خود را از مدار توسعه کنار گذاشته است.»

او خاطرنشان می‌کند: «هیچ سرمایه‌گذاری خارجی یا حتی داخلی‌ای حاضر نیست به چنین بستر پرریسکی ورود کند؛ مگر آنکه بودجه دولتی یا رانتی داشته باشد که زیان برایش مفهومی نداشته باشد. این یعنی، فضای استارتاپی و نوآورانه ایران، که به‌طور سنتی متکی بر سرمایه‌های جسورانه و بخش خصوصی بوده، به‌تدریج در حال انجماد است.»

حسینی تاکید دارد که نباید اجازه داد ماجراهای هک نوبیتکس، فقط به‌عنوان یک اتفاق «پوشش داده شود» و از حافظه عمومی پاک شود. بلکه باید درس‌های مهمی از آن گرفت؛ مهم‌ترین‌اش اینکه قطع اینترنت، نه یک راه‌حل، بلکه بخشی از بحران است. سیاست‌گذاران باید بدانند که در دنیای امروز، اینترنت نه یک ابزار لوکس، که یک زیرساخت حیاتی ملی است.

تشدید بی‌اعتمادی عمومی

وحید فرید، کارشناس فناوری نیز معتقد است که وضعیت فعلی اینترنت و شرایطی که کاربران و کسب‌وکارهای آنلاین با آن روبه‌رو هستند، موجب بی‌اعتمادی کاربران و کسب‌وکارها به سیاست‌های دولت در حوزه فناوری اطلاعات شده و این بی‌اعتمادی به سادگی قابل بازگشت نیست. او با مقایسه قطعی‌های اینترنت دوران جنگ با حوادث آبان‌ماه ۹۸، بر این باور است که در جریان جنگ، سیاست‌گذاران و تصمیم‌گیران سطح متفاوتی از محدودیت‌های اینترنتی را اعمال کردند که سابقه نداشت.

فرید می‌گوید: «ما در طول دوران جنگ، هشت یا ۹ روز قطع کامل اینترنت را تجربه کردیم. گزارش‌های جهانی هم این موضوع را تأیید می‌کنند؛ در برخی روزها ترافیک اینترنت به حدود سه درصد کاهش یافته بود، یعنی ۹۷ درصد اینترنت کشور عملاً غیرفعال بود. آن سه درصد باقی‌مانده هم مربوط به اینترنت طبقاتی و دسترسی‌های خاص برخی نهادها و اقشار بود. جالب آنکه شدت قطعی اینترنت در این دوره، حتی از آبان‌ماه ۹۸ هم بیشتر بود. در آن‌زمان اینترنت کاربران قطع بود، اما دیتاسنترهای بزرگ به اینترنت دسترسی داشتند اما در جریان جنگ اخیر، حتی دیتاسنترها نیز به‌صورت کامل قطع شدند و کاربران و کسب‌وکارها دچار مشکل و ضرر و زیان شدند.»

فرید بر این باور است که نباید در تحلیل پیامدهای قطعی و اختلال اینترنت، دچار خطای‌دید استراتژیک شد. او می‌گوید: «زمانی که یک کسب‌وکار اینترنت ندارد و زیرساخت‌اش دچار اختلال یا هک شده، اگر بخواهد دوباره خدماتش را راه‌اندازی کند، نیازمند دسترسی به راهکارها و ابزارهای فنی است که لزوماً داخلی نیستند؛ بسیاری از نرم‌افزارها وابسته به پکیج‌های خارجی‌اند ازجمله سیستم‌عامل‌ها، زبان‌های برنامه‌نویسی، اکستنشن‌ها و ماژول‌های متعدد. بدون دسترسی به اینترنت، راه‌اندازی مجدد زیرساخت‌ها به‌سادگی ممکن نیست. درباره نوبیتکس اگر اینترنت قطع نبود و خارج کردن دارایی‌های کاربران از کیف‌پول‌ها انجام شده بود، طبیعتاً موجودی کمتری باقی می‌ماند و خسارت کمتری وارد می‌شد.»

فرید تشدید بی‌اعتمادی عمومی به سیاست‌گذاران در پی تداوم قطعی و اختلال‌های اینترنت و طرح بحث‌هایی مانند اینترنت طبقاتی را به‌عنوان واقعیت‌های ناخوشایند در شیوه فعلی حکمرانی فضای‌مجازی کشور بیان می‌کند. او می‌گوید: «اینترنت طبقاتی که برخی نهادها مانند سازمان نظام صنفی دنبال می‌کنند، نگرشی تقلیل‌گرایانه و خطرناک است. این رویکرد، این حقیقت کلیدی را نادیده می‌گیرد که اقتصاد دیجیتال تنها شامل پلتفرم‌های بزرگ نیست. آسیب واقعی و گسترده به‌صورت زیان انباشته و خاموش، به هزاران فروشنده آنلاین و کسب‌وکار خُرد وارد می‌شود.»

نگرانی درباره آینده

نوبیتکس یک مطالعه موردی است که نشان می‌دهد چطور ریسک‌های ساختاری و تحمیلی ناشی از خطاهای فاحش در تنظیم‌گری و نظارت حوزه‌ای کلیدی مانند اینترنت در کشور ما، به یک بحران تمام‌عیار تبدیل می‌شود.

خسارت‌های هنگفت و ضرر و زیان‌های کسب‌وکارهای آنلاین از جنگ ۱۲ روزه به این‌سو و حتی طرح موضوعاتی مانند اینترنت طبقاتی کسب‌وکارها، همگی جلوه‌های ناخوشایند سیاست‌ها و راهبردهای محدودیت‌نگرانه‌ای مانند فیلترینگ، اختلال و ناپایداری اینترنت است که کاربران و کسب‌وکارها را در بحران فرو می‌برد و معادله تاب‌آوری‌شان را پیچیده‌تر و دشوارتر می‌کند و این نگران‌کننده است.

زیان ۱۵ هزار میلیارد تومانی در یک‌ماه و کاهش هولناک ۳۰ درصدی اشتغال در بخش اقتصاد دیجیتال، تنها ارقامی روی کاغذ نیستند. اینها روایت فروپاشی آرزوها، بیکاری متخصصان و فلج‌شدن اقتصادی است که مثل همه کشورهای دیگر باید و می‌توانست پیشران توسعه می‌بود. آن ۱۲روز و بعد از آن، بیش از یک بحران گذرا، آیینه‌ای تمام‌نما از چالش‌های عمیقی است که کسب‌وکارهای آنلاین ایران هرروز با آن دست‌وپنجه نرم می‌کنند؛ تلاش برای بقا در زمینی که زیر پایشان هر لحظه خالی شود.

حمله سایبری به نوبیتکس، روشن است که قطعی و اختلال در اینترنت، توانایی واکنش سریع تیم‌های فنی و امنیت نوبیتکس را در لحظات طلایی پس از حمله، به‌شدت کاهش داده و عملاً کسب‌وکارها را در برابر مهاجم فلج می‌کند. نوبیتکس در شرایطی تحت حمله قرار گرفت که دسترسی به اینترنت بین‌الملل محدود شده بود، شبکه بانکی اختلال داشت و سرویس‌هایی مثل ارسال پیامک و پیام‌رسان‌ها هم دچار مشکل شده بودند. از طرفی نیز بسیاری از نیروهای متخصص آن مثل دیگر شهروندان، از شهر خارج شده بودند

انتشار دوره آموزشی کلاد در آروان آکادمی

فاز سوم و آخر از مسیر آموزشی آروان آکادمی، شامل دوره‌های «Professional cloud Architect» و «Expert DevOps Engineer» منتشر شدند؛ این مسیر آموزشی به‌طورکلی ۱۸۰ ساعت آموزش و ۵۴۰ ساعت تمرین‌های مرتبط با متخصصان این حوزه را شامل می‌شود. این دو دوره‌ی اخیر علاوه‌بر استادان دوره‌های پیشین با همراهی آرش حاتمی، محمدرضا داورزنی، محمود احمدی و محمدعرفان شمس - که همگی از متخصصان حوزه‌ی ابر هستند - ارائه شده است.

باشگاه فارغ‌التحصیلان آروان آکادمی هزارتایی شد!

مسیر آموزشی آروان آکادمی از دو رشته‌ی اصلی «Cloud Architect» و «DevOps Engineer» تشکیل شده بود که درمجموع ۷۲۰ ساعت محتوای آموزشی و تمرینی را تشکیل دادند که در مدت‌زمان یک‌سال به ۴۷۱۲۰ ساعت تماشای ویدئوها رسیده است. در این‌مدت، ۱۲۶۰۰ دانش‌پذیر در آروان آکادمی ثبت‌نام کردند که نزدیک هزار نفر از آنان موفق به دریافت گواهی پایان دوره شدند.

مسیرهای آموزشی آکادمی کامل شدند

سال گذشته و بهار امسال، دوره‌های پیشین در قالب فاز یک و فاز دو منتشر شدند که شامل دوره‌های «Associate Cloud Architect» و «Foundational Cloud Practitioner» در مسیر آموزشی معماری ابری و دوره‌های «Professional DevOps Engineer» و «Associate DevOps Engineer» در دوره‌ی دواپس هستند. دوره‌ی آخر دواپس، دوره‌ی «Expert DevOps Engineer» از ۱۸ ساعت محتوای آموزشی و ۵۴ ساعت تمرین تشکیل شده است و در دیگر دوره‌ی معماری ابری به‌نام «Professional Cloud Architect»، ۱۶ ساعت آموزش و ۴۸ ساعت محتوای تمرینی وجود دارد.

این تازه شروع ماجراست!

با انتشار دو دوره‌ی نهایی، مسیر آموزشی تعریف‌شده در آروان آکادمی تکمیل شد و برای پربارشدن مسیرهای آموزشی، به‌زودی دوره‌های کوتاه‌مدت متنوعی در موضوعات مختلف مرتبط به کلاد در صفحه‌ی آروان آکادمی در دسترس قرار خواهند گرفت. سپیده رحمانی؛ مسئول بخش آموزش آروان کلاد درباره‌ی انگیزه‌ی ادامه‌داشتن آموزش‌های آروان آکادمی می‌گوید: «در این سال‌ها این نکته بسیار بدیهی بوده که وضعیت مهاجرت سرمایه‌ی انسانی متخصص از ایران در وضعیت خطرناکی است؛ وضعیتی که ممکن است منبع متخصصان کشور را با خلأ مواجه کند. در پی راستی‌آزمایی این ادعا نیستم اما مشاهدات ما به‌عنوان کسانی که سال‌هاست در اکوسیستم نوآوری و فناوری کشور فعالیت می‌کنیم، این ادعا را تایید می‌کند. به این معنا باید بگویم که توان ما به‌عنوان یک استارتاپ در ایران، درون آروان آکادمی نمایان‌گر شد. ما با فراهم آوردن آموزش‌های فناورانه به‌شکل تخصصی، دسترس‌پذیر، با استانداردهای جهانی و رایگان تلاش می‌کنیم تا آموزش‌های دانش ابری را به‌دست کسانی که در پی محتوای تخصصی هستند - فارغ از محدودیت‌های جغرافیایی، زمانی و مالی - برسانیم. به همین دلیل این دوره‌ها را عملی و مناسب بازار کار ایران و جهان طراحی کردیم تا دانش‌پذیران پس از دریافت آموزش بتوانند تجربه‌ی شغلی‌شان را شروع کنند. با این توضیح و دغدغه‌ها، باید بگویم که شاید پایانی برای گستره‌ی فعالیت‌های آروان آکادمی نتوانیم تصور کنیم». رحمانی در ادامه می‌گوید پس از این فاز، در دوره‌های کوتاه‌مدت، سرفصل‌های گسترده‌تری از آموزش در حوزه‌ی فناوری را به دوره‌های آروان آکادمی اضافه خواهیم کرد که به‌زودی و در ماه‌های آتی جزئیات آن را اطلاع خواهیم داد.» اگر از مخاطبان آروان آکادمی هستید و پیشنهادی برای دوره‌های کوتاه‌مدت با موضوع‌های مرتبط با کلاد دارید، می‌توانید از راه ایمیل pr@arvancloud.ir با موضوع آروان آکادمی، پیشنهادهای‌تان را به‌دست ما برسانید.

چرا آروان آکادمی؟

آروان آکادمی در مسیر مسئولیت اجتماعی آروان به‌دنبال «توانمندسازی آموزشی» است. آروان آکادمی از ابتدای سال ۱۴۰۳ به‌وجود آمده است تا با فراهم آوردن محتوای باکیفیت و به‌روز حوزه‌ی ابری به‌شکل آنلاین و رایگان، دسترسی به محتوای تخصصی حوزه‌ی کلاد را فارغ از محدودیت‌های جغرافیایی برای همه‌ی علاقه‌مندان آن فراهم آورد. آروان آکادمی تلاش کرده است آموزش‌های خود را منطبق بر مسیر شغلی، طراحی و در اختیار دانش‌پذیران قرار دهد تا علاقه‌مندان به حوزه‌ی ابری بتوانند در بهینه‌ترین حالت ممکن، آموزش‌ها را در مسیر حرفه‌ای‌شان دنبال کنند. برای ثبت‌نام در آروان آکادمی و بهره‌مندی از محتوای این دوره‌ها به‌شکل رایگان، می‌توانید به صفحه‌ی آروان آکادمی مراجعه کنید.