رویکرد و حاکمیت امنیت – Security Governance

بیانه رسمی امنیت اطلاعات

در چارگون، امنیت اطلاعات یک قابلیت جانبی نیست، بلکه سنگ بنای اعتماد در عصر اقتصاد دیجیتال بوده و بخشی جدایی‌ناپذیر از چرخه طراحی، توسعه، استقرار و پشتیبانی محصولات نرم‌افزاری ماست. ما متعهد به حفظ محرمانگی، تمامیت و دسترس‌پذیری اطلاعات مشتریان هستیم و امنیت را در تمام تصمیمات فنی و سازمانی لحاظ می‌کنیم. با توجه به اینکه محصولات ما در بستر سازمان‌های بزرگ کشور و به‌صورت On-Premise مستقر می‌شوند، مسئولیت‌پذیری در قبال کاهش ریسک‌های امنیتی برای ما یک اصل بنیادین است.

پیام و رویکرد فرزاد رحمانی (مدیرعامل چارگون) درباره تعهد به امنیت

حملات سایبری گسترده اخیر نشان داد که امنیت، فقط یک دغدغه فنی نیست؛ بلکه مؤلفه‌ای بنیادین برای بقا و پیشرفت در دنیای دیجیتال است. فرزاد رحمانی، مدیرعامل چارگون، در گفت‌وگویی مفصل، از مسئولیت‌پذیری سازمان‌ها، تجربه باگ‌بانتی، تفکر

امنیت‌محور در توسعه محصول و لزوم شکل‌گیری یک اکوسیستم امنیتی سخن می‌گوید.

در عصری که مرزهای امنیت نه فقط در خاک، بلکه در فضای داده و زیرساخت‌های دیجیتال تعریف می‌شود، امنیت سایبری دیگر فقط دغدغه مدیران فناوری یا متخصصان امنیت اطلاعات نیست؛ بلکه یک مسئله عمومی، ملی و حتی اجتماعی است. فرزاد رحمانی، مدیرعامل شرکت چارگون، که یکی از باسابقه‌ترین فعالان حوزه نرم‌افزارهای سازمانی در کشور است، در این گفت‌وگو نگاهی ساختاری، فرهنگی و فنی به امنیت اطلاعات دارد و تأکید می‌کند: «امنیت نباید در لحظه آخر به محصول دوخته شود؛ بلکه باید از لحظه تولدش در تار و پود آن تنیده باشد.»

امنیت؛ جنگی خاموش، اما واقعی

رحمانی با اشاره به حملات سایبری اخیر که باعث اختلال جدی در خدمات بانکی و رمزارزی کشور شد می‌گوید: «ما در یکی از پرمخاطره‌ترین برهه‌های تاریخ فناوری کشور زندگی می‌کنیم. این یک جنگ واقعی است؛ فقط صدای گلوله ندارد. جنگی که زیرساخت‌های بانکی، صرافی‌های دیجیتال، و حتی زندگی روزمره مردم را هدف قرار می‌دهد.»

او با صراحت ادامه می‌دهد: «دیگر کسی نمی‌تواند بگوید امنیت سایبری یک موضوع دور از ذهن یا انتزاعی است. مردم در هفته‌های اخیر و با حملات سایبری به دو بانک و یکی از بزرگ‌ترین صرافی‌های دیجیتال کشور با پوست و استخوان‌شان فهمیدند که آسیب به زیرساخت‌های دیجیتال و اطلاعات یعنی مختل شدن زندگی روزمره‌شان. اینکه بانک کار نمی‌کند، صرافی قطع شده، یا داده‌هایشان در خطر است. این یعنی امنیت

اطلاعات، امنیت دارایی‌ها و امنیت روانی جامعه.»

امنیت، جزئی از DNA محصول

فرزاد رحمانی با اشاره به مسیر 27 ساله تولید و توسعه راهکارهای سازمانی و اهمیت موضوع امنیت در این روند، تأکید می‌کند که در چارگون، امنیت نه‌تنها شعار نیست، بلکه در همه سطوح طراحی، توسعه، تست و ارائه خدمات جاری است: «ما از همان زمانی که به یک محصول فکر می‌کنیم، امنیت در ذهن ما اولویت دارد. اگر این کار را نکنیم، حتی بهترین محصول هم بدون امنیت، ارزشی برای ارائه ندارد. امنیت چیزی نیست که مثل یک پَچ در آخرین لحظه اعمال شود، بلکه باید از ابتدا طراحی و پیاده‌سازی شود.»

او ادامه می‌دهد: «برای ما، امنیت فقط گرفتن گواهی نیست. تفکر امنیت‌محور باید در فرهنگ سازمانی نهادینه شود. هر کس در تیم ما می‌داند محصولی که می‌سازد، باید بتواند در برابر تهدیدات واقعی دوام بیاورد.»

گواهی امنیت؛ برچسب نیست، سند مسئولیت است

مدیرعامل چارگون با رد نگاه تزئینی به گواهی‌نامه‌های امنیتی می‌گوید: «ما گواهی افتا هم برای محصول و هم برای خدمات‌مان داریم، همچنین تأییدیه امنیتی از سازمان پدافند غیرعامل. اما برای ما، گواهی پایان راه نیست. اینها فقط مهر تأییدی بر بینش و فرآیندی‌ست که در سازمان ما جاری است. از دید ما، گواهی یک لوگو نیست؛ یک سند تعهد است.»

او در ادامه با اشاره به گواهی‌ها و مجوزهای امنیتی توضیح می‌دهد: «بحث گواهی امنیتی برای برخی صرفاً یک مدرک یا لوگوی اعتماد است، اما معتقدم این موضوع، نتیجه یک فرآیند پیچیده و مسئولانه است. همان‌طور که شما از یک دارو انتظار دارید گواهی تأییدیه سلامت داشته باشد تا با اطمینان خاطر از آن استفاده کنید، کاربران هم باید مطمئن باشند که نرم‌افزارها از منظر امنیت مورد ارزیابی قرار گرفته‌اند. اما مهم‌تر از خود گواهی، مسیری‌ست که به آن ختم می‌شود. یعنی تعهد به استاندارد، آمادگی پاسخگویی، و شفافیت در مواجهه با تهدیدات.»

چالش ساختاری و راهکار پیشرو

رحمانی به چالش‌های موجود در ساختارهای امنیت سایبری کشور هم اشاره دارد: «ما در کشور با مشکلات ساختاری زیادی در این زمینه مواجه هستیم؛ از طولانی بودن فرآیندهای اخذ گواهی گرفته تا پراکندگی و تعدد نهادهای ناظر. اما راه‌حل، کنار گذاشتن گواهی نیست. اتفاقاً باید این مسیر را حرفه‌ای‌تر و چابک‌تر کنیم. نقد داریم، ولی اصل موضوع را انکار نمی‌کنیم. استاندارد، اگرچه ممکن است سخت‌گیرانه باشد، اما لازمه توسعه پایدار است.»

او تأکید می‌کند: «ما سال‌ها قبل از اینکه گرفتن گواهی الزامی شود، به‌طور داوطلبانه این مسیر را طی کردیم. چون می‌دانستیم مشتریان ما نیاز به اطمینان دارند. و این اعتماد، با ادعا به‌دست نمی‌آید؛ باید سند داشته باشد.»

باگ‌بانتی؛ نگاه آینده‌نگر به امنیت

یکی از اقدامات پیشرو چارگون، پیاده‌سازی برنامه باگ‌بانتی (Bug Bounty) است؛ چیزی که در ایران کمتر سابقه دارد. رحمانی در این خصوص توضیح می‌دهد: «ما تصمیم گرفتیم محصولمان را در معرض ارزیابی عمومی متخصصان امنیت قرار دهیم. با همکاری دو شرکت ناظر (باگ‌دشت و راورو)، محصول را منتشر کردیم تا هر متخصص امنیتی که توانایی کشف آسیب‌پذیری دارد، بررسی و گزارش کند.»

او با اشاره به فرهنگ‌سازی این حرکت می‌گوید: «امنیت همیشه با ترس و نگرانی دیده شده. انگار موضوعی است که فقط باید درِ گوشی درباره‌اش صحبت کرد. اما توصیه من این است که با شفافیت با آن روبه‌رو شویم. امنیت با ترس حاصل نمی‌شود، با دانایی و مشارکت حاصل می‌شود.»

چشم‌انداز چارگون؛ امنیت به‌مثابه مسئولیت مستمر

رحمانی تأکید می‌کند که چارگون فقط به تست یا گواهی‌نامه اکتفا نمی‌کند، بلکه این نگاه را در طول عمر محصول ادامه می‌دهد: «ما متعهدیم که باگ‌بانتی را ادامه دهیم، ارزیابی‌های امنیتی را به‌طور دوره‌ای انجام دهیم، گواهی‌ها را به‌روز کنیم و با مشاوران امنیتی در تعامل دائم باشیم. در کنار این، تیم امنیتی اختصاصی داریم که روی امنیت در لایه‌های مختلف تمرکز دارد.»

مدیرعامل چارگون به نقش کل اکوسیستم دیجیتال در امنیت اشاره می‌کند: «هیچ شرکت یا فردی به‌تنهایی نمی‌تواند امنیت را تضمین کند. امنیت محصولِ تعامل است؛ تعامل بین توسعه‌دهنده، ناظر، رگولاتور، کارفرما، کاربر و حتی رسانه. تا وقتی فقط یک حلقه فعال باشد و بقیه بی‌تفاوت، پیشرفتی حاصل نمی‌شود. ما نیاز به یک فرهنگ امنیتی

فراگیر داریم. این فرهنگ باید از مدیران ارشد شروع شود؛ چون وقتی مدیر یک سازمان امنیت را جدی بگیرد، این اهمیت به لایه‌های پایین‌تر منتقل می‌شود.»

او نتیجه‌گیری می‌کند: «اگر امنیت را سرمایه‌گذاری ببینیم، نه هزینه، آن‌وقت مسیر متفاوتی می‌رویم. چون نرم‌افزار فقط یک محصول نیست، یک مسئولیت است. هرچه تعامل بین توسعه‌دهنده، ناظر، مصرف‌کننده و رسانه بیشتر باشد، امنیت واقعی‌تری شکل می‌گیرد.» رحمانی در پایان تأکید می‌کند: «در آینده‌ای نزدیک، سازمان‌هایی که امنیت را نادیده بگیرند، نه فقط آسیب‌پذیر، بلکه بی‌اعتبار خواهند شد. مردم امروز آگاه‌اند، رسانه‌ها مطالبه‌گرند، و سرمایه‌گذاران به ریسک امنیتی حساس‌اند. امنیت، شرط بقا در آینده‌ای‌ست که اقتصاد دیجیتال در آن حرف اول را می‌زند. و اعتماد، بزرگ‌ترین سرمایه برند است. این اعتماد، بدون امنیت دوام نمی‌آورد.»

چارچوب‌های مرجع امنیتی

رویکرد امنیتی چارگون مبتنی بر استانداردها و چارچوب‌های شناخته‌شده، الزامات و دستورالعمل‌های نهادهای ملی مانند مرکز مدیریت راهبردی افتا و از لحاظ بین‌المللی مانند OWASP است. این، الزامات و دستورالعمل‌ها همواره در طراحی کنترل‌های امنیتی ما لحاظ می‌شوند. این ترکیب باعث می‌شود محصولات ما هم از منظر فنی و هم از منظر انطباق مقرراتی قابل اتکا باشند.

ساختار سازمانی امنیت

چارگون دارای ساختار مشخص حاکمیت امنیت اطلاعات است که شامل مدیر امنیت

اطلاعات، فرآیندهای رسمی مدیریت ریسک، مدیریت رخداد و کنترل‌های داخلی می‌شود. تصمیمات امنیتی در قالب کمیته‌های تخصصی با حضور مدیرعامل و مدیران ارشد بررسی شده و مدل «سه خط دفاعی» در مدیریت کنترل‌ها رعایت می‌شود؛ به این معنا که توسعه، نظارت و ممیزی داخلی از یکدیگر تفکیک شده‌اند تا تضاد منافع کاهش و اثربخشی کنترل‌ها افزایش یابد. در این سه خط دفاعی، اصول کلیدی استقلال و بی‌طرفی، تفکیک وظایف، هماهنگی و ارتباطات و گزارش‌دهی چندسطحی می‌باشند. همچنین از مزایای به‌کارگیری این مدل شفافیت در مسئولیت‌ها، بهبود مدیریت ریسک، افزایش اعتماد ذینفعان، انطباق با قوانین و مقررات و بهبود فرآیند تصمیم‌گیری را می‌توان نام برد.