بررسی نقش شرکت امنیت سایبری سایبرآرک در راهبرد امنیتی جدید اسرائیل

از پتاح تیکوا تا صحنه جهانی

مهسا جعفری‌فر

با گسترش تهدیدات دیجیتال، قابلیت‌های سایبری به‌تدریج به یکی از ارکان اصلی امنیت ملی اسرائیل تبدیل شده‌اند؛ به‌گونه‌ای که در سند امنیت ۲۰۳۰ اسرائیل به‌عنوان یکی از محورهای کلیدی برنامه‌ریزی راهبردی رژیم تا ۵ سال آینده معرفی شده‌اند. در این چهارچوب، شرکت‌ها و استارتاپ‌های فناوری نه‌تنها اقتصاد و امنیت داخلی رژیم را تقویت می‌کنند، بلکه با عرضه فناوری‌های پیشرفته به متحدان بین‌المللی، به افزایش نفوذ سیاسی و قدرت نرم اسرائیل نیز کمک می‌کنند. سایبرآرک نمونه‌ای شاخص از این شرکت‌هاست؛ که در اسرائیل متولد شده و حالا به عنوان یکی از رهبران جهانی امنیت سایبری شناخته می‌شود.

تولد و شکل‌گیری سایبرآرک

داستان شرکت نرم‌افزاری سایبرآرک از سال ۱۹۹۹ در اسرائیل آغاز می‌شود. این شرکت توسط اودی موکادی و آلون کوهن، کهنه‌سربازان یگان ۸۲۰۰ و واحد رایانه‌ای ارتش اسرائیل (Mamram) در پتاح تیکوا تأسیس شد. سایبرآرک به نسل اول بازیگران امنیت سایبری اسرائیل تعلق دارد و در دوره‌ای تأسیس شده که مفهوم «سایبر» هنوز به عنوان یک حوزه مستقل، مهم و راهبردی در سیاست‌ها و بازارهای جهانی تثبیت نشده بود. ایده اولیه شکل‌گیری این شرکت بر پایه مشاهده یک ضعف حیاتی در امنیت سازمان‌ها شکل گرفت. مؤسسان سایبرآرک متوجه شدند که حساب‌های کاربری ممتاز و با دسترسی بالا (مانند مدیران سیستم، سرور یا نرم‌افزارهای حیاتی) محافظت نمی‌شوند و هدف اصلی حملات مهاجمان سایبری هستند و در صورت نفوذ، می‌توانند کل شبکه را در معرض خطر قرار دهند. این ایده نقطه شروع سفر سایبرآرک در مسیر پر پیچ و خم امنیت سایبری بود.

پیشگام هویت دیجیتال

سایبرآرک از همان ابتدا تمرکز خود را بر محافظت از حساب‌های پرخطر گذاشت و در سال ۲۰۰۵ اولین محصول امنیتی خود را عرضه کرد که بر پایه فناوری «Digital Vault» یا همان «گنجینه دیجیتال» طراحی شده بود تا از اطلاعات و حساب‌های حساس شرکت‌ها محافظت کند. این فناوری رمز عبورها و کلیدهای دسترسی مهم را در یک مخزن مرکزی امن حفظ می‌کرد به گونه‌ای که فقط افراد مجاز بتوانند وارد شوند و همه فعالیت‌ها ثبت می‌شد. اهمیت محافظت از حساب‌های حساس، به‌ویژه برای نهادهای دولتی، زیرساخت‌های حیاتی و صنایع حساس، باعث شد محصولات این شرکت از همان ابتدا مورد توجه سازمان‌های بزرگ قرار گیرد. سایبرآرک خیلی زود توانسته بود به اهمیت «امنیت هویت» پی ببرد و همین موضوع به کلید موفقیتش تبدیل شد. با گذر زمان و افزایش موج تهدیدات سایبری، ایمن‌سازی هویت‌های حساس مورد توجه بازار امنیت سایبری قرار گرفت؛ بازاری با عنوان «مدیریت دسترسی ممتاز» که سایبرآرک از مدت‌ها قبل جایگاهش را در آن تثبیت کرده بود.

بودجه اولیه سایبرآرک از طریق سرمایه‌گذاران خطرپذیر تأمین شد (گروهی از سرمایه‌گذاران که روی شرکت‌های کوچک با پتانسیل رشد بالا سرمایه‌گذاری می‌کنند). تا سال ۲۰۱۴ درآمد سالانه سایبرآرک به حدود ۶۶ میلیون دلار رسید؛ رقمی که برای یک شرکت امنیت سایبری تخصصی، نشان‌دهنده وجود مشتریان بزرگ سازمانی و جایگاه تثبیت‌شده در بازار جهانی بود.

ورود سایبرآرک به بورس آمریکا

در سال ۲۰۱۴ سایبرآرک درخواست عرضه اولیه سهام خود را به کمیسیون بورس و اوراق بهادار آمریکا ارائه کرد. ورود به بورس نزدک در سال ۲۰۱۴ نقطه عطف مهم در مسیر رشد این شرکت بود. سایبرآرک پس از ورود به بورس در عرضه اولیه‌اش حدود ۸۸ میلیون دلار سرمایه جذب کرد و مسیر رشد خود را هم‌زمان با گسترش تهدیدات دیجیتال جهانی ادامه داد و محصولاتش در طیفی گسترده از سازمان‌های دولتی، بانک‌ها، شرکت‌های انرژی، صنایع دفاعی و زیرساخت‌های حیاتی در سراسر جهان مورد استفاده قرار گرفت.

اسرائیل باید رهبر جهانی فناوری امنیت سایبری باشد

در سال ۲۰۱۸، نتانیاهو اعلام کرد که اسرائیل خود را یکی از پنج قدرت جهان در حوزه سایبری می‌داند. این جاه‌طلبی در سند امنیت ۲۰۳۰ اسرائیل منعکس شد، در این سند حوزه سایبری هم سطح با قدرت نظامی و اطلاعاتی قرار گرفت؛ نکته‌ای که نشان‌دهنده تغییری مهم در محاسبات امنیتی رژیم بود. تأکید صریح نخست‌وزیر بر دستیابی به قابلیت‌های سایبری در سطح قدرت‌های بزرگ و اعلام عمومی نتانیاهو نشان داد در رویکرد جدید اسرائیل حوزه سایبری به یک حوزه استراتژیک برای بازدارندگی دشمنان و نمایش قدرت تبدیل شده و شرکت‌های فناوری فراتر از کارکرد تجاری به عنوان بازوهای امنیت ملی رژیم در نظر گرفته شدند. در این چهارچوب، توانایی رشد، برندسازی و برتری بر رقبا اهمیت ویژه‌ای پیدا می‌کند. سایبرآرک باید به عنوان یکی از رهبران جهانی عرصه امنیت هویت قابلیت‌های خود را ارتقا می‌داد تا کماکان بازیگر اصلی این عرصه باقی بماند.

حضور در سیلیکون‌ولی سایبری اسرائیل

در سال ۲۰۲۱ سایبرآرک مرکز تحقیق و توسعه خود را در بترسیع راه‌اندازی کرد. در سند امنیت سایبری ۲۰۳۰، بترسیع به عنوان یکی از هسته‌های عملیاتی این چشم‌انداز برجسته شده است. این شهر، میزبان پارک فناوری گاو-یام است که به «سیلیکون‌ولی سایبری اسرائیل» معروف است و قرار است بستری فراهم کند تا شرکت‌های پیشرو مانند سایبرآرک، در کنار فعالیت‌های تحقیق و توسعه، امکان دسترسی مستقیم و همکاری با دانشگاه بن‌گوریون و استعدادهای فارغ‌التحصیل یگان ۸۲۰۰ را داشته باشند. طبق داده‌های سازمان نوآوری اسرائیل، استارتاپ‌های امنیت سایبری که توسط فارغ‌التحصیلان یگان ۸۲۰۰ هدایت می‌شوند، موفق‌تر در جذب سرمایه بین‌المللی هستند و سریع‌تر جایگاه خود را در بازار جهانی پیدا می‌کنند.

یگان ۸۲۰۰ یکی از ستون‌های اصلی قدرت سایبری اسرائیل به شمار می‌رود؛ این واحد نیروهای متخصص در حوزه‌های اطلاعاتی و سایبری را آموزش می‌دهد و هم‌زمان به عنوان یک مرکز نوآوری و استعدادیابی برای صنعت فناوری عمل می‌کند. فارغ‌التحصیلان این یگان نه‌تنها در ساختارهای نظامی و اطلاعاتی اسرائیل فعالند، بلکه بسیاری از آن‌ها بنیان‌گذار یا مدیر شرکت‌های بزرگ امنیت سایبری در سطح جهانی شده‌اند.

هدف این است که این تعاملات در کنار نوآوری و تربیت نیروی متخصص، زمینه اثرگذاری بر هنجارها و استانداردهای بین‌المللی فضای سایبری را فراهم کرده و نفوذ جهانی اسرائیل را در این حوزه تثبیت کنند. میان سایبرآرک و یگان ۸۲۰۰ ارتباطی درهم‌تنیده و استراتژیک برقرار است؛ علاوه بر اینکه اودی موکادی، بنیانگذار شرکت، کهنه‌سرباز همین یگان است؛ بخش قابل توجهی از مدیران و کارکنان سایبرآرک نیز از فارغ‌التحصیلان همین واحد هستند؛ به‌طوری که در جریان جنگ، تعدادی از آن‌ها به خدمت ذخیره فراخوانده شدند.

سایبرآرک هویت انسان و ماشین را امن می‌کند

سال گذشته، سایبرآرک با پرداخت ۱٫۵۴ میلیارد دلار، شرکت آمریکایی ونافی (Venafi) را خرید؛ این شرکت در مدیریت هویت‌های دیجیتال غیرانسانی (ماشینی) تخصص دارد. این خرید بازار سایبرآرک را حدود ۱۰ میلیارد دلار بزرگ‌تر کرد و به آن امکان داد امنیت تمامی هویت‌ها، چه انسان‌ها و چه سیستم‌ها و برنامه‌ها، را به صورت یکپارچه و ساده در شبکه‌ها و زیرساخت‌های ابری فراهم کند. همچنین این راهکار برای شرکت‌های کوچک و بزرگ قابل استفاده است و امنیت داخلی و خارجی سازمان‌ها را تضمین می‌کند. مدیرعامل سایبرآرک گفت: «این خرید نقطه عطفی برای ما بود. حالا می‌توانیم هر هویتی (چه انسان و چه ماشین) را امن کنیم و به شرکت‌ها کمک کنیم در برابر حملات پیچیده محافظت شوند.»

امنیت هویت AI؛ میدان جدید نبرد سایبرآرک

اوایل امسال، این شرکت از توسعه مرکز هوش مصنوعی خود در اسرائیل خبر داد و جذب ده‌ها متخصص جدید را آغاز کرد. مدتی بعد محصول جدیدی برای امنیت هویت و دسترسی عامل‌های هوش مصنوعی معرفی کرد. عامل‌های هوش مصنوعی برنامه‌ها یا ربات‌هایی هستند که به صورت خودکار کارهایی را انجام می‌دهند و گاهی برای انجام وظایفشان به دسترسی‌های ویژه به سیستم‌ها نیاز دارند. این دسترسی‌ها اگر کنترل نشوند، می‌توانند زمینه سوءاستفاده یا حملات سایبری را فراهم کنند. محصول جدید سایبرآرک با اعمال کنترل‌های مناسب دسترسی، اطمینان می‌دهد که عامل‌های AI فقط به منابعی دسترسی دارند که نیاز دارند و هیچ دسترسی اضافه‌ای ندارند. این راهکار باعث کاهش ریسک‌های امنیتی، جلوگیری از دسترسی‌های غیرمجاز و امکان گسترش امن پروژه‌های هوش مصنوعی در سازمان‌ها می‌شود.

پرتنز زگو، یکی از مدیران ارشد سایبرآرک، در این باره گفت: «قابلیت‌های هوش مصنوعی که ما در حال توسعه آن‌ها هستیم، همان چیزی است که ما را متمایز می‌کند. یک مرکز امنیت سایبری سنتی ممکن است روزانه ۱۰۰ رخداد را مدیریت کند؛ اما با هوش مصنوعی می‌توان ۵ هزار مورد را پردازش کرد. این است معنای واقعی عملیات امن.» این پیشرفت فناورانه سایبرآرک زمینه‌ساز یکی از بزرگ‌ترین پیشنهادات ادغام در دنیای امنیت سایبری شد.

شرکت امنیت سایبری پالوآلتو در معامله‌ای ۲۵ میلیارد دلاری، سایبرآرک را می‌خرد

شاید در نگاه اول این تیتر فقط یک خبر اقتصادی معمول به نظر برسد؛ از جنس ادغام‌های بزرگ شرکتی و جابه‌جایی سهام در بازار فناوری؛ اما در واقع این خبر، از یکی از مهم‌ترین جابه‌جایی‌های قدرت در صنعت امنیت سایبری پرده برداشت. تحلیلگران این اتفاق را زلزله‌ای در دنیای سایبری توصیف کرده و پیش‌بینی کردند که نتیجه این معامله، نیرویی فراتر از مجموع بخش‌های آن ایجاد کند و برای سال‌ها رهبری بی‌چون‌وچرای این صنعت را تثبیت کند.

شرکت پالوآلتو نتورکس که توسط نیر زوک، کهنه‌سرباز یگان ۸۲۰۰ و کارآفرین آمریکایی-اسرائیلی، تأسیس شده در زمینه امنیت شبکه و کامپیوتر تخصص دارد و از شرکت‌ها در برابر نفوذهای خارجی محافظت می‌کند. محصولات این شرکت به‌طور گسترده در نهادهای دولتی، شرکت‌های بزرگ و زیرساخت‌های حساس در سراسر جهان استفاده می‌شوند. تا پیش از این، تمرکز پالوآلتو بیشتر بر محافظت از شبکه‌ها و مقابله با حملات بیرونی بود. خرید سایبرآرک، این خلأ راهبردی را پر کرد و پازل امنیتی پالوآلتو را با افزودن لایه کنترل هویت، تکمیل کرد. خبر خرید ۲۵ میلیارد دلاری شرکت اسرائیلی سایبرآرک توسط پالوآلتو، توجه تحلیل‌گران، رسانه‌های فناوری و بازارهای مالی را به طور گسترده به خود جلب کرد. پالوآلتو تاکنون چنین معامله بزرگی را تجربه نکرده بود. بزرگ‌ترین خریدهای پیشین این شرکت معمولاً در محدوده چند میلیارد دلار بودند؛ اما خرید سایبرآرک با اختلاف، گران‌ترین و جسورانه‌ترین ادغام تاریخ این غول امنیتی محسوب می‌شد. سؤال این بود: چه چیزی پالوآلتو را به سمت انجام این خرید جسورانه سوق داد؟

کارکنان سایبرآرک و مقامات بزرگ دهمین سالگرد ورود به بازار سهام عمومی را در سال ۲۰۲۴ جشن می‌گیرند

به‌روزرسانی راهبرد ملی امنیت سایبری

در فوریه ۲۰۲۵، اسرائیل راهبرد ملی امنیت سایبری خود را به‌روزرسانی کرد و اعلام کرد که نسخه جدید باتوجه به درس‌های آموخته شده از عملیات «شمشیرهای آهنین» و سایر حوادث سایبری بزرگ در جهان تدوین شده است. در این سند تأکید شده باتوجه به اینکه اسرائیل مانند چین یا آمریکا توان زیادی برای تأثیرگذاری جهانی ندارد، شرکت‌های اسرائیلی باید از طریق ائتلاف‌سازی و مشارکت‌های استراتژیک با شرکت‌های بزرگ بین‌المللی، قدرت نرم و اثرگذاری خود را در عرصه جهانی افزایش دهند. علاوه بر این، امنیت هویت نیز در راهبرد جدید امنیت سایبری جایگاهی ویژه دارد؛ حوزه‌ای که محور اصلی تمرکز سایبرآرک است. در این چهارچوب، آنچه پالوآلتو به سایبرآرک ارائه می‌دهد، تنها یک ارزش‌گذاری سخاوتمندانه سهام نیست، بلکه این ادغام سایبرآرک را در موقعیت جدیدی قرار می‌دهد که بتواند برای شکل‌دهی به آینده رهبری جهانی امنیت سایبری در راستای اهداف اسرائیل نقش خود را ایفا کند.

۱۷ اکتبر؛ آزمون سخت امنیت دیجیتال اسرائیل

۷ اکتبر ۲۰۲۳ و جنگی که پس از آن آغاز شد، تنها معادلات نظامی اسرائیل را به چالش نکشید؛ بلکه به طور بی‌سابقه‌ای نقاط ضعف سایبری و اطلاعاتی رژیم را نیز آشکار کرد. در طول دو سال اخیر شدت حملات سایبری علیه اسرائیل سه برابر شده است. فشار بی‌وقفه بر زیرساخت‌های دیجیتال، نشان داد که برتری سایبری اسرائیل، برخلاف تصور رایج، مطلق و بدون خلأ نیست. این روند در درگیری مستقیم و غیرمستقیم با ایران وارد مرحله‌ای تازه شد؛ بوسی کارادی، رئیس اداره ملی سایبری اسرائیل (INCD)، در اولین سخنرانی عمومی خود از زمان تصدی این سمت گفت که ایران در طول جنگ ۱۲ روزه ۱۲۰۰ عملیات هک مهندسی اجتماعی علیه اسرائیل انجام داده و دوربین‌های پارکینگ و سایر جاده‌ها را هک کرد تا حرکات افراد مهم اسرائیلی را زیر نظر بگیرد و پازل امنیتی پالوآلتو را با افزودن لایه کنترل هویت، تکمیل کرد. خبر خرید ۲۵ میلیارد دلاری شرکت اسرائیلی سایبرآرک توسط پالوآلتو، توجه تحلیل‌گران، رسانه‌های فناوری و بازارهای مالی را به طور گسترده به خود جلب کرد. پالوآلتو تاکنون چنین معامله بزرگی را تجربه نکرده بود. بزرگ‌ترین خریدهای پیشین این شرکت معمولاً در محدوده چند میلیارد دلار بودند؛ اما خرید سایبرآرک با اختلاف، گران‌ترین و جسورانه‌ترین ادغام

سیاست
هفته‌نامه تحلیلی روزنامه فرهیختگان
شماره چهل و سوم | هفته اول دی ماه ۱۴۰۴
FARHIKHTEGANONLINE

جنگ ۱۲ روزه با ایران، به طور محسوسی شدت گرفته است. از این زاویه، خرید سایبرآرک توسط پالوآلتو نتورکس را می‌توان نه فقط یک معامله تجاری بزرگ، بلکه واکنشی به واقعیت‌های جدید امنیتی پس از ۷ اکتبر و در چهارچوب راهبرد امنیت سایبری جدید اسرائیل دانست. اظهارات اودی موکادی در مصاحبه با یدیعوت آحارونوت در نوامبر ۲۰۲۴ که تنها چند ماه پیش از اعلام ادغام مطرح شده، نشان می‌دهد سایبرآرک تا آن زمان برنامه‌ای برای ادغام نداشته و این معامله بیش از آن‌که قابل پیش‌بینی باشد، به تغییری ناگهانی در معادلات شباهت دارد. «شما گفته بودید که بسیاری از شرکت‌های کوچک‌تر امنیت سایبری در نهایت توسط بازیگران بزرگ‌تر خریداری می‌شوند. آیا نگران نبودید که سایبرآرک هم یکی از آن‌ها باشد؟

«سؤال فوق‌العاده‌ای است. ما ۲۵ سالگی تأسیس شرکت و ۱۰ سال حضورمان به‌عنوان یک شرکت بورسی را صرفاً برای تفریح جشن نگرفتیم. هدف ما از ابتدا این بوده که یک شرکت پایدار بسازیم؛ شرکتی که خریدار باشد، نه خریداری‌شده و بتواند به رشد خود ادامه دهد. درعین‌حال، قصد نداریم یک فروشگاه همه‌چیزفروش باشیم. تمرکز ما تخصصی است و می‌خواهیم در حوزه امنیت هویتی پیشرو بمانیم.»

ادغام یا نفوذ؟

خرید و ادغام شرکت سایبرآرک مسیری برای گسترش نفوذ نیروی انسانی آموزش‌دیده در واحد ۸۲۰۰ در صنعت فناوری جهانی است؛ مسیری که این نیروها را از اسرائیل به موقعیت‌های اثرگذار در شرکت‌های بزرگ بین‌المللی منتقل می‌کند. پاول بیگار، رئیس سازمان پژوهشی «Tech for Palestine»، می‌گوید: «این خریدها راهی هستند برای انتقال نیروهای واحد ۸۲۰۰ از اسرائیل و قرار دادن آن‌ها در موقعیت‌های اثرگذار در صنعت فناوری آمریکا. این شرکت‌ها داده‌های مشتریانِ مشتریان خود را مدیریت می‌کنند. اگر شما یک بانک باشید و از پالوآلتو نتورکس استفاده کنید، اطلاعات مربوط به همه مشتریان شما و تراکنش‌هایشان از سرورهایی عبور می‌کند که تحت کنترل جاسوس‌ها یا جاسوس‌های سابق هستند.» حضور فارغ‌التحصیلان واحد ۸۲۰۰ در صنعت فناوری جهانی قابل توجه است. تا اواسط سال ۲۰۲۵ بیش از ۱۴۰۰ کهنه‌سرباز اطلاعاتی اسرائیل در شرکت‌های فناوری آمریکا مشغول به کار بوده‌اند که حدود ۹۰۰ نفر از آن‌ها سابقه خدمت در واحد ۸۲۰۰ داشته‌اند.

امنیت سایبری در خدمت اقتصاد اسرائیل

چشم‌انداز امنیتی ۲۰۳۰ اسرائیل، اقتصاد را به‌عنوان یکی از ستون‌های اصلی امنیت ملی تعریف می‌کند و تأکید دارد که نوآوری و فناوری نقش مرکزی در امنیت اقتصادی دارند. در این چهارچوب، امنیت سایبری به‌عنوان یک فرصت تجاری عظیم و یک محرک مهم برای اقتصاد اسرائیل است.

ارزش سهام سایبرآرک در سه سال گذشته مسیر صعودی چشمگیری را طی کرده و تقریباً سه برابر شده است. در طول این مدت قیمت سهام این شرکت از حدود ۱۵۰ دلار به بیش از ۴۰۰ دلار رسید و ارزش بازار آن را به بیش از ۲۰ میلیارد دلار رساند. این موفقیت مالی، سایبرآرک را به دومین شرکت ارزشمند اسرائیلی در بورس وال استریت تبدیل کرد. با اعلام ادغام سایبرآرک و پالوآلتو، ارزش این شرکت به حدود ۲۵ میلیارد دلار افزایش یافت. این معامله به تنهایی حدود ۲ میلیارد دلار درآمد مالیاتی برای اسرائیل به همراه خواهد داشت. این ارقام در شرایطی اهمیت بیشتری پیدا می‌کنند که طبق آمارها، در سال ۲۰۲۳ حدود ۲۰ درصد از تولید ناخالص داخلی اسرائیل و ۵۳ درصد از صادرات رژیم به بخش فناوری اختصاص داشته است.

حرکت سایبری به سوی افق ۲۰۳۰

ادغام سایبرآرک با پالوآلتو نتورکس، بیش از آن‌که یک معامله اقتصادی بزرگ باشد، نماد رویکرد امنیتی جدید اسرائیل در دهه پیش رو است که در آن، فضای سایبری به طور راهبردی به عنوان بعدی جدید از منازعه به رسمیت شناخته شده است. در این چهارچوب، اسرائیل می‌کوشد با قرار دادن خود در لایه‌های حیاتی امنیت سایبری جهانی، از قدرتی بهره ببرد که نه متکی به حضور نظامی مستقیم است و نه اجماع‌های سیاسی، بلکه بر وابستگی ساختاری دیگران به فناوری‌های امنیتی صهیونیست‌ها بنا شده است. این مدل اسرائیل را به بازیگری حیاتی و «غیرقابل حذف» در زیرساخت دیجیتال جهان تبدیل می‌کند و ابزاری مهم برای جبران عمق راهبردی محدود اسرائیل است.