
بسم الله
الرحمن
الرحيم

فهرست

[یادداشت حامی]

امنیت سایبری از مفاهیمی است که به اندازه کافی مورد توجه قرار نگرفته است. امنیت یک زیرساخت است؛ مثل اینترنت، شبکه، حمل‌ونقل، برق، آب، گاز و هر بستر دیگری که بشر آن را برای زیست بهتر خود توسعه داده است. در جهانی که امنیت وجود نداشته باشد، هیچ فعالیت سالم و سازنده‌ای قابل انجام و پیگیری نیست. اکنون که شبکه‌های کامپیوتری گسترش یافته‌اند و جهان دیجیتال به بخشی از زندگی روزمره تبدیل شده، همه ما در جهان سایبر ـ فیزیکی زندگی می‌کنیم. همان‌گونه که امنیت در جهان فیزیکی اهمیت دارد، در جهان سایبری هم مقوله مهمی است که متأسفانه به اندازه کافی جدی گرفته نشده است.

امنیت سایبری (امنیت رایانه‌ای یا امنیت فناوری اطلاعات) یعنی حفاظت از سامانه‌های اطلاعاتی در برابر آسیب به سخت‌افزار، نرم‌افزار و اطلاعات نرم‌افزاری؛ امنیت سایبری مقوله‌هایی مانند محافظت در برابر حمله محروم‌سازی از سرویس (اختلال) و بات‌نت‌ها (گمراهی) را هم در بر می‌گیرد.

متأسفانه در موضوع امنیت سایبری آنچه کمتر به آن توجه می‌شود، رخنه‌پذیری از طریق منابع انسانی است. ممکن است کسب‌وکارها موضوع امنیت را صرفاً موضوعی فنی ببینند و تصور کنند که با خرید تجهیزات پیشرفته می‌توانند امنیت را برقرار کنند، در حالی که بیشتر رخنه‌های امنیتی از طریق منابع انسانی سازمان‌ها صورت می‌گیرد.

با توجه به افزایش وابستگی به سامانه‌های رایانه‌ای و اینترنت در بیشتر جوامع، شبکه‌های

بی‌سیم مانند بلوتوث و وای‌فای و رشد دستگاه‌های هوشمند مانند تلفن هوشمند، تلویزیون و دستگاه‌های کوچک مانند اینترنت اشیا؛ امنیت سایبری اهمیت روبه‌رشدی پیدا کرده است.

تهدیداتی مانند جرائم مجازی، آسیب‌پذیری، شنود، بدافزار، جاسوس‌افزار، باج‌افزار، تروجان، ویروس‌ها، کرم‌رایانه‌ای، روت‌کیت‌ها، کی‌لاگرها، تراش‌دادن داده، اکسپلویت، درب پشتی، بمب منطقی و حمله محروم‌سازی از سرویس، هر روز نقش جدی‌تری در زندگی سایبر ـ فیزیکی پیدا می‌کنند. کوچک‌ترین اختلالی در فعالیت‌های سایبری به آسیب‌های جدی در دنیای فیزیکی منجر می‌شود. نمی‌توان انتظار داشت که بدون در نظر گرفتن روال‌های امنیتی شاهد این باشیم که امنیت سایبری برقرار شود. با در نظر گرفتن این موضوع مهم که امنیت یک مفهوم نسبی است، پیچیدگی این حوزه بیشتر هم می‌شود.

نویسندگان کتاب امنیت سایبری معتقدند که شرکت‌ها دو دسته هستند؛ آنهایی که هک شده‌اند و آنهایی که در آینده هک می‌شوند! با این نگاه طبیعی است که مدیران سازمان‌های امروز باید خودشان را برای پس از هک آماده کنند! نه تنها برای هک نشدن؛ بلکه برای بعد از هک نیز باید آماده باشیم. همه کسب‌وکارهای بزرگ و کوچک امروز جهان در معرض هک‌شدن قرار دارند. انواع آسیب‌پذیری‌ها، سیستم‌های سایبری را تهدید می‌کند و تلاش برای کتمان رخنه‌ها صرفاً به عمیق‌تر شدن شکاف‌ها منجر می‌شود. سیستم‌های نرم‌افزاری و سخت‌افزاری امروز به‌صورت پیوسته باید ارتقا یابند تا هکرها یک قدم عقب‌تر باشند، ولی نکته مهم‌تر و بعضاً فراموش‌شده این است که نه تنها سیستم‌های سخت‌افزاری و نرم‌افزاری؛ بلکه منابع انسانی نیز به‌صورت پیوسته

باید تحت آموزش قرار بگیرند. روش‌های قدیمی، دیگر پاسخگو نیست و ما نمی‌توانیم انتظار داشته باشیم که با روش‌های تاریخ‌مصرف‌گذشته امنیت سایبری را تأمین کنیم.

آموزه‌های این کتاب بسیار ساده و به‌غایت کاربردی است. دیدگان شما را دعوت می‌کنیم به صفحات آتی این کتاب، به این امید که بهره لازم برای غنی‌تر کردن رویکردهای ارتقای امنیت در سازمان شما نیز حاصل آید.

شرکت بهسازان ملت

[یادداشت ناشر]

امروزه موضوع امنیت سایبری به یک مسئله حیاتی برای کسب‌وکارها تبدیل شده، اما هنوز هم هستند کسب‌وکارهایی که تا وقتی با مشکل امنیتی و نشت داده‌های خود مواجه نشده‌اند، اهمیت امنیت سایبری را درک نمی‌کنند. طبق یک نقل قول معروف از کارشناسان امنیتی، نشت داده بالأخره اتفاق می‌افتد و هکرها راهی خواهند یافت تا به سیستم‌های یک شرکت نفوذ کنند. اما نکته بااهمیت میزان خسارتی است که پس از این اتفاق به بار می‌آید. به عبارت دیگر حمله سایبری و نشت داده در دنیای کنونی گریزناپذیر است و فقط با آمادگی قبلی و اتخاذ رویکردهای صحیح امنیتی می‌توان از میزان خسارت آن کاست. البته همچنان یک راه وجود دارد که بتوانیم تا حد زیادی خودمان را از شر حملات سایبری رها کنیم؛ اینکه از کامپیوترها استفاده نکنیم. همان‌طور که در یکی از مقالات کتاب و به نقل از «ویلیس ویر» از پیشگامان حوزه امنیت و حریم خصوصی چنین جمله‌ای آمده است: «تنها کامپیوتری که به‌طور کامل امن است، کامپیوتری است که کسی از آن استفاده نمی‌کند.»

بزرگ‌ترین شرکت‌های فناوری با این مسئله در سطح وسیع مواجه شده‌اند. شرکت یاهو در سال ۲۰۱۶ هدف حمله وسیع سایبری قرار گرفت و اطلاعات سه میلیارد کاربرش به دست هکرها افتاد. شرکت مایکروسافت نیز انگشت اتهام را به سمت هکرهای چینی در خصوص هک‌شدن ایمیل‌های این شرکت نشانه رفته است. همین چند ماه پیش بود که هک حساب افراد مشهور در توییتر و درخواست بیت‌کوین از کاربران سروصدای زیادی به پا کرد. نمونه‌های داخلی فراوانی

را هم می‌توان به‌عنوان نمونه ذکر کرد. از هک اطلاعات شـــرکت رایتل گرفته تا هک وب‌سایت سازمان تأمین اجتماعی و هک سیستم‌های بندر شهید رجایی از جمله مواردی است که صرفاً در سال جاری صورت پذیرفته است. همه این موارد اهمیت بهداشت سایبری را برجسته می‌کنند.

اینکه چه اقداماتی انجام دهید که قربانی یک حمله سایبری بزرگ در شرکت و سازمان خود نشوید یا اگر در معرض چنین واقعه‌ای قرار گرفتید، چه اقداماتی انجام دهید، از جمله مهم‌ترین مسائلی اســـت که باید هر مدیر یا رهبر کسب‌وکاری برای آن آماده باشـــد و تمهیداتی برای آن بیندیشد.

این کتاب به ما از اشتباهات تکراری مدیران پس از وقوع یک حمله سایبری می‌گوید. از اینکه منابع انسانی سازمان و آموزش آنان مهم‌ترین سد جهت جلوگیری از وقوع یک حمله سایبری هستند. کتاب از این صحبت می‌کند که مدیران چطور در حرف از اهمیت سایبری می‌گویند، اما در عمل آن را جدی نمی‌گیرند یا اینکه اصلاح عادات غلط کارکنان در حوزه امنیتی می‌تواند مانع یک فاجعه شود.

کتاب امنیت سایبری بر خلاف تصور کتابی خواندنی و جذاب است که نه‌تنها به ما هشدار می‌دهد که امنیت ســـایبری را جدی بگیریم؛ بلکه راهکار ارائه می‌دهد. امیدواریم انتشار این کتاب بتواند گامی هرچند کوچک در راســـتای بالا بردن حساسیت‌ها نسبت به موضوع امنیت سایبری در کشورمان باشد.

قاسم سرافرازی
انتشارات راه‌پرداخت

مقدمه

اکنون همه مادر گیر این مساله هستیم

الکس بلو[1]

زمانی اینترنت تنها یک ایده محض بود؛ آینده‌ای به‌ظاهر غیر قابل تصور که در آن همه‌چیز و همه‌کس با هم ارتباط پیدا می‌کردند. تصور بر این بود که در چنین دنیایی جریان‌های بدون وقفه از اطلاعات و داده‌ها، پیشرفتی بی‌سابقه را در ارتباطات، سلامت، حمل‌ونقل، اتوماسیون و تجارت رقم بزنند و البته در این دنیا نقشی برای ربات‌ها هم در نظر گرفته می‌شد. دنیای امروز ما چندان دور از این تصورها نبوده و همین فناوری‌ها هستند که نحوه عملکرد شرکت‌ها و دولت‌ها را از اساس تغییر داده‌اند. در میان این رویاهای شیرین، متخصصان امنیت هشدار داده‌اند که این دنیای به‌هم‌پیوسته ما می‌تواند خطرآفرین هم باشد. هکرها، هوش مصنوعی پیشرفته و بازیگران بد در دولت‌ها و ابرشرکت‌ها تهدیدهای قابل توجهی برای زندگی روزمره ما هستند. حتی بهترین آرمانشهر سایبری هم می‌تواند یک دنیای شیطانی زیرزمینی در درون خود داشته باشد.

امروزه در دنیای واقعی، همان فناوری‌های مفید، پیامدهای جدید و متغیری را برای امنیت سایبری افراد، شرکت‌ها و دولت‌ها به وجود آورده‌اند. این پیامدها می‌توانند به‌سادگی ایجاد رمز عبوری جدید و سخت پس از نفوذ اطلاعاتی باشند یا می‌توانند ریسک‌هایی ترسناک باشند؛ مانند اینکه دشمنی خارجی بتواند چراغ‌های خیابان را خاموش کند یا سیستم‌های تصفیه آب را از کار بیندازد یا حتی به زیرساخت‌های نظامی غلبه کند.

هرچند مدیریت این ریسک‌ها از قدیم به عهده کارشناسان و تکنیسین‌ها بوده است، اما دیگر نمی‌توان حوزه امنیت سایبری را به متخصصان فناوری اطلاعات محدود کرد. در عوض همه ما مدیران، چه در سازمان‌های خصوصی و چه در سازمان‌های دولتی، باید به نقش امنیت سایبری در وظایف و مسئولیت‌هایمان پی ببریم و خود را در زمینه تغییرات ریسک‌ها در امنیت سایبری به‌روز نگه داریم. این کتاب به افراد غیرحرفه‌ای کمک می‌کند تا به‌سرعت، درکی عمیق از حوزه امنیت سایبری به دست آورند. این کتاب چند موضوع بسیار مهم را پوشش می‌دهد و مطالعه

1. Alex Blau

آن دو مزیت برای شما دارد؛ اول اینکه با مسائل فعلی و مسائل آتی در حوزه امنیت سایبری آشنا می‌شوید؛ مسائلی که با نقش، سازمان و صنعت شما مطابقت دارند. دوم اینکه متوجه خواهید شد که هم بخشی از مشکلات امنیتی سازمان هستید و هم نقشی کلیدی در شناسایی و مدیریت راه‌حل‌های امنیتی ایفا می‌کنید.

تعداد صنایعی که برای تعیین استراتژی و مدیریت عملیات خود به جمع‌آوری داده و اطلاعات در مورد تمام جوانب کسب‌وکار، به‌ویژه مشتری‌ها وابسته‌اند، هر روز بیشتر می‌شود. هرچند دسترسی به چندین پتابایت داده، بهره‌وری عملیاتی را بهبود می‌بخشد و فرصت‌های جدیدی به وجود می‌آورد، اما این حجم عظیم داده می‌تواند خسارت‌هایی نیز برای شرکت‌ها و افراد به همراه داشته باشد. اکنون حمله‌های سایبری و نفوذ اطلاعاتی رواج یافته و هر ساله پرحجم‌تر و پرهزینه‌تر می‌شوند و با وجود توانایی روزافزون ما در جلوگیری از این حمله‌ها و بالا بردن فناوری امنیت و بهداشت سایبری، این نفوذها کاهش نیافته است. باید انتظارات خود را از توانایی‌هایمان بالا ببریم، این ریسک‌ها را کاهش دهیم و بپذیریم که نفوذهای اطلاعاتی اجتناب‌ناپذیر هستند.

از زمانی که اطلاعات مشتری برای هکرها ارزشمندتر شده و دولت‌ها قوانینی را برای جریمه شرکت‌ها، به علت از دست دادن اطلاعات مشتری یا نفوذ به آن، وضع کرده‌اند، شرکت‌هایی که حضور اینترنتی دارند و اطلاعات مشتریان را جمع‌آوری می‌کنند با ریسک‌های بیشتری مواجه شده‌اند؛ اما این نکته دیگر فقط در مورد بانک‌ها و سازمان‌های خدمات مالی صدق نمی‌کند.

این پارادایم جدید نیازمند یک طرز فکر متفاوت است و این کتاب به رهبران غیرفنی، از جمله مدیران اجرایی، اعضای هیات‌مدیره و سایر مسئولان در تنظیم قوانین؛ از طراحی و بازاریابی گرفته تا منابع انسانی و حسابداری، با هدف سرعت‌بخشیدن به وضعیت فعلی این حوزه کمک می‌کند. کتاب امنیت سایبری اصول مقدماتی را معرفی می‌کند و در عین حال به موضوعاتی چون نحوه مشارکت هیات‌مدیره و مدیران اجرایی در حوزه امنیت سایبری، سرمایه‌گذاری و تصمیم‌گیری در این حوزه، اهمیت تعیین عوامل انسانی در امنیت سایبری و اینکه چرا همه اعضا باید در این رابطه نقشی ایفا کنند، ارتباطات و عکس‌العمل مناسب در پی نقض داده‌ها، دفاع فعال و اصول «هک متقابل»[1]، ارزش رو به فزونی حریم خصوصی در امنیت سایبری، ملاحظات امنیت سایبری برای تجارت بین‌الملل و نیز آینده هوش مصنوعی در امنیت سایبری نگاه ویژه‌ای دارد. این موارد

1. Hacking back

منتخب به درک‌تان در انتخاب مشاور مناسب در مورد مسائل حیاتی، هم‌سطح ماندن با رقبا و همکاران و شناسایی اثرات بالقوه بر تیم، سازمان و صنعتی که در آن فعال هستید، کمک می‌کند. همچنین خواندن این کتاب به شـــما کمک خواهد کرد تا تشخیص دهید سازمان شما در آینده چگونه باید برای همراه‌شدن با جریان‌های امنیت سایبری پیشرفت کند.

این کتاب صرفا بیانگر آغاز راه است. امنیت سایبری هنوز یک حوزه نسبتا جدید است که خود را به‌صورت پویا با تغییرات محیط رگولاتوری نوپا و توسعه فناوری‌های جدید تطبیق خواهد داد. برخی از این تغییرات به‌سود تمامی افراد جامعه خواهد بود. به‌عنوان مثال، در حال حاضر مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR) شـــرکت‌ها را بـــه رعایت اقدامات احتیاطی بیشتر و مراقبت از داده‌های مشتری ترغیب و از مدل‌های کسب‌وکاری که متکی بر فروش چنین داده‌هایی به اشخاص ثالث هستند جلوگیری می‌کند. با این حال، دیگر تغییرات، مانند پیشرفت‌ها در حوزه هوش مصنوعی و محاسبات کوانتومی، تهدیدهای جدید و بالقوه‌ای را به وجود خواهند آورد که می‌توانند اقدامات فعلی ما در حوزه امنیت سایبری را کم‌ارزش کنند و برای کسب‌وکارها و دولت‌ها مشـــکلاتی به وجود بیاورند. درک این ریسک‌ها و فرصت‌های جدید برای موفقیت شرکت‌ها و همچنین به‌طور کلی حفاظت از مردم و جامعه در آینده حیاتی خواهد بود.

حوزه امنیت ســـایبری صرفا متعلق به آینده‌پژوهان فناوری و بومیان دیجیتال نیســـت. همه ما چه بخواهیم و چه نخواهیم به این دنیای جدید وارد شـــده‌ایم. همه ما (جامعه جهانی) باید دست‌به‌دست یکدیگر دهیم تا از رخداد یک فاجعه مرتبط با فناوری جلوگیری کنیم. لازم است این مساله برای همگان روشن شود که تک‌تک افراد جامعه درگیر این مساله هستند و باید برای رفع تهدیدهای این حوزه نقش خود را ایفا کنند.

۱. ناامنی اینترنت

اندی بوچمن

این یک حقیقت تلخ اســت؛ اهمیتی ندارد که ســازمان شــما چه مقدار برای جدیدترین سخت‌افزارها و نرم‌افزارها، آموزش و همچنین منابع انسانی در حوزه امنیت سایبری هزینه کرده یا اینکه سیستم‌های پایه‌ای خود را از ســایر سیستم‌ها جدا کرده باشد. اگر سیستم‌های حیاتی که در راستای ماموریت سازمان‌تان قرار دارند، دیجیتالی و به طریقی به اینترنت متصل باشند (به احتمال زیاد متصل هستند، حتی اگر شــما طور دیگری فکر کنید)، آنها هرگز نمی‌توانند کاملا ایمن شوند.

این مساله حائز اهمیت است، چون در حال حاضر سیستم‌های دیجیتال و متصل به اینترنت به‌صورت مجازی در هر بخشــی از اقتصاد ایــالات متحده نفوذ دارند و در ســال‌های اخیر پیچیدگی فعالیت‌های خرابکارانه و عاملان آنها (اعم از گروه‌های تحت حمایت دولت‌های مرکزی، سازمان‌های جنایی و گروه‌های تروریستی) بسیار زیاد افزایش یافته است.

حملات رخ‌داده در ایالات متحده علیه دولت محلی آتلانتا و علیه یک شبکه داده[1] مشترک بین چهار اپراتور خطــوط لوله گاز، ســرقت داده‌ها از «آکوئیفاکــس» و حملات بدافزاری «واناکرای»[2] و «نات‌پتیا»[3] را ملاحظه کنید. در مورد بسیاری از حوادث شناخته‌شده سال‌های اخیر، شرکت‌های قربانی نشت داده تصور می‌کردند که سیستم دفاع سایبری قدرتمندی دارند.

من عضو یک تیم در آزمایشــگاه ملی آیداهو (INL) هستم که در حال بررسی این موضوع اســت که ســازمان‌های حیاتی برای اقتصاد و امنیت ملی ایالات متحده چگونه می‌توانند به بهترین شکل از خود در برابر حملات ســایبری محافظت کنند. تمرکز ما روی سامانه‌هایی بود که به سیستم‌های کنترل صنعتی (مانند آنهایی که گرما و فشــار را در ابزارهای الکتریکی و پالایشــگاه‌های نفت تنظیم می‌کنند) وابســته‌اند و راهکاری ارائه دادیم کــه با هیچ‌یک از

1. Data network
2. WannaCry
3. NotPetya

راهکارهای سنتی همخوانی نداشت: «کارکردهایی که اگر دچار نقص شوند، کسب‌وکار شما را به خطر می‌اندازند، شناسایی کنید، آنها را تا حد ممکن از اینترنت جدا کنید، وابستگی آنها به فناوری‌های دیجیتال را تا کمترین میزان ممکن کاهش دهید و پایش و کنترل آنها را از طریق دستگاه‌های آنالوگ و افراد مورد اعتماد پشتیبانی کنید.»

اگرچه روش ما هم چنان در مرحله آزمایشی است، اما سازمان‌ها می‌توانند بسیاری از اصول این رویکرد را هم‌اکنون نیز اعمال کنند.

مسلما، این راهبرد (که برای کسب‌وکارهای کاملا مبتنی بر اطلاعات امکان‌پذیر نیست) ممکن است هزینه‌های عملیاتی را افزایش و در بعضی موارد کارایی را کاهش دهد؛ اما تنها راهی است که می‌توانیم اطمینان پیدا کنیم که سیستم‌های حیاتی از طریق ابزارهای دیجیتال مورد حمله قرار نگیرند. در این فصل، من روش‌های این آزمایشگاه برای شناسایی چنین سیستم‌هایی را ارائه خواهم کرد. حملات معمولا از طریق کارکردها یا فرایندهای آسیب‌پذیری رخ می‌دهند که رهبران هرگز فکر نمی‌کردند این‌قدر حیاتی باشند که مختل کردن آنها بتواند به از کار افتادن سازمان‌شان منجر شود. ما در سال‌های اخیر از اصول این روش در شرکت‌ها و ارتش ایالات متحده استفاده کرده‌ایم و یک طرح آزمایشی یک‌ساله بسیار موفقیت‌آمیزی از این رویکرد را در شرکت «Florida Power & Light» که یکی از بزرگ‌ترین شرکت‌های خدمات الکتریکی ایالات متحده است، اجرا کرده‌ایم. هم‌اکنون دومین طرح آزمایشی در یکی از مراکز نظام‌وظیفه ایالات متحده در حال انجام است. همچنین آزمایشگاه ملی آیداهو در جست‌وجوی راهی برای متداول‌کردن این فرایند است. این موضوع احتمالا به معنای مشارکت با شرکت‌های خدمات مهندسی منتخب و اعطای مجوز و آموزش به آنها جهت اعمال این روش خواهد بود.

تهدید موجود

در سال‌های دور، پمپ‌های مکانیکی، کمپرسورها، شیرفلکه‌ها، رله‌ها و عملگرهای مکانیکی در شرکت‌های صنعتی به کار گرفته می‌شدند. آگاهی موقعیتی از گیج‌های آنالوگ[1] و مهندسان ماهر و مورد اعتمادی که از طریق مدار تلفن ثابت با دفتر مرکزی در ارتباط بودند،

1. Analog gauges

حاصل می‌شد. به غیر از دستکاری زنجیره تامین یا همکاری با یکی از کارکنان، تنها راهی که یک خرابکار می‌توانست عملیات یک شرکت را مختل کند، این بود که به کارخانه وارد شود و از سه ستون فیزیکی امنیتی عبور کند؛ گیت‌ها، نگهبانان و سلاح‌ها.

امروزه عملیات در ۱۲ بخش از ۱۶ بخش زیرساختی که وزارت امنیت داخلی ایالات متحده آنها را حیاتی قلمداد کرده است[۱]، به‌صورت نسبی یا کامل به سیستم‌های کنترل و ایمنی دیجیتال وابسته هستند. هرچند فناوری‌های دیجیتال قابلیت و کارایی شگفت‌انگیزی را به ارمغان می‌آورند، اما ثابت شده که بسیار در معرض حملات سایبری قرار دارند. نقاط ضعف سیستم‌های شرکت‌های بزرگ، آژانس‌های دولتی و موسسات دانشگاهی دائما توسط خرابکاران و با استفاده از ابزارهای خودکاری که به‌راحتی در وب تاریک در دسترس هستند، مورد بررسی قرار می‌گیرند؛ بسیاری از این ابزارها رایگان هستند و قیمت نمونه‌های پیشرفته به صدها یا هزاران دلار می‌رسد (گران‌ترین آنها حتی با پشتیبانی فنی همراه است). اغلب آنها می‌توانند توسط تیم‌های امنیت سایبری باتجربه خنثی شوند، اما در حقیقت دفاع در برابر حملات برنامه‌ریزی‌شده و هدفمند که (اگر نگوییم سال‌ها) ماه‌ها طراحی آن طول کشیده، تقریبا غیرممکن است.

اثرات مالی حملات سایبری رو به افزایش است. تنها دو حمله واناکرای و نات‌پتیا در سال ۲۰۱۷، به‌ترتیب خساراتی بالغ بر چهار میلیارد دلار و ۸۰۰ میلیون دلار در بر داشتند. طبق گزارش‌ها در حمله واناکرای که ایالات متحده و بریتانیا، کره شمالی را به دست‌داشتن در آن متهم کردند، از ابزارهای به‌سرقت‌رفته از آژانس امنیت ملی استفاده شده بود. این باج‌افزار برای حمله از یک شکاف در دستگاه‌های مبتنی بر ویندوزی که پچ امنیتی مایکروسافت را نصب نکرده بودند، استفاده کرد و پس از ورود به سیستم، داده‌ها را رمزگذاری کرد؛ این حمله به از کار افتادن صدها هزار کامپیوتر در بیمارستان‌ها، مدارس، کسب‌وکارها و خانه‌ها در ۱۵۰ کشور منجر شد؛ سپس از قربانیان درخواست باج کرد. حمله نات‌پتیا که اعتقاد بر این است روسیه به‌عنوان بخشی از تلاش‌های خود در بی‌ثبات‌سازی اوکراین در آن دست داشته است، از طریق یک به‌روزرسانی در نرم‌افزار یک شرکت حسابداری اوکراینی اجرا شد. نات‌پتیا با حمله

---

۱. بخش‌هایی که به‌دلیل دارایی‌ها، سیستم‌ها و شبکه‌هایشان، خواه به‌صورت فیزیکی یا مجازی، برای ایالات متحده بسیار حیاتی تلقی می‌شوند، به‌طوری که نقص یا نابودی آنها اثرات مهلکی بر امنیت، اقتصاد، بهداشت یا ایمنی عمومی ملی خواهد گذاشت.

به دولت و سیستم‌های کامپیوتری اوکراین آغاز شد و به دیگر بخش‌های جهان گسترش یافت و شرکت‌هایی مانند شرکت کشتیرانی دانمارکی «مرسک»، شرکت دارویی «مرک»، شرکت تولیدکننده شکلات «کدبری» و غول تبلیغاتی «دبلیو پی پی» را آلوده کرد.

آسیب‌پذیری رو به رشد

تحول دیجیتال با رشد اتوماسیون، اینترنت اشیا، پردازش و ذخیره‌سازی ابری، هوش مصنوعی و یادگیری ماشین شتاب بیشتری می‌گیرد. گسترش و وابستگی روزافزون به فناوری‌های پیچیده، متصل به اینترنت و مبتنی بر نرم‌افزارهای دیجیتال در حوزه امنیت سایبری مشکلات جدی به وجود آورده است. در یک مقاله که در سال ۲۰۱۴ توسط مرکز امنیت نوین آمریکا منتشر شد، «ریچارد جی دانزیگ»، وزیر سابق نیروی دریایی و رئیس هیات‌مدیره این مرکز، تناقض‌های مطرح‌شده توسط فناوری‌های دیجیتال را توضیح داده است: «فناوری‌های دیجیتال در عین حال که قدرت بی‌سابقه‌ای را به ارمغان می‌آورند، امنیت کاربران را کمتر می‌کنند. قابلیت‌های ارتباطی آنها همکاری و شبکه‌سازی را امکان‌پذیر می‌کند، اما در عین حال راه را برای نفوذ هموارتر می‌سازد. متمرکزسازی داده، کارایی و مقیاس عملیات را بسیار بهبود بخشیده است، اما این متمرکزسازی به نوبه خود به‌صورت بالقوه حجم داده‌ای را که می‌تواند به‌دنبال یک حمله به سرقت رود یا تخریب شود، افزایش می‌دهد. پیچیدگی‌های سخت‌افزاری و نرم‌افزاری قابلیت‌های زیادی ایجاد می‌کند، اما این پیچیدگی‌ها نقاط آسیب‌پذیری را به وجود می‌آورند و قدرت کشف نفوذها را کاهش می‌دهند... در مجموع سیستم‌های سایبری به ما غذا می‌دهند، اما در عین حال ما را ضعیف کرده و مسموم می‌کنند.»

واقعیت این است که این فناوری‌ها به قدری پیچیده‌اند که حتی وندورهایی که آنها را ایجاد کرده و به‌خوبی می‌شناسند نیز به‌طور کامل نقاط آسیب‌پذیر آنها را درک نمی‌کنند. وندورها معمولا اتوماسیون را به‌عنوان راهی برای از بین بردن ریسک‌های ایجادشده توسط انسان‌های مستعد خطا به فروش می‌رسانند، اما این اقدام صرفا ریسک‌ها را با ریسک‌های جدید جایگزین می‌کند. در حال حاضر سیستم‌های اطلاعاتی چنان پیچیده‌اند که شرکت‌های ایالات متحده به‌طور متوسط باید بیش از ۲۰۰ روز زمان بگذارند تا تشخیص دهند که مورد رخنه سایبری قرار