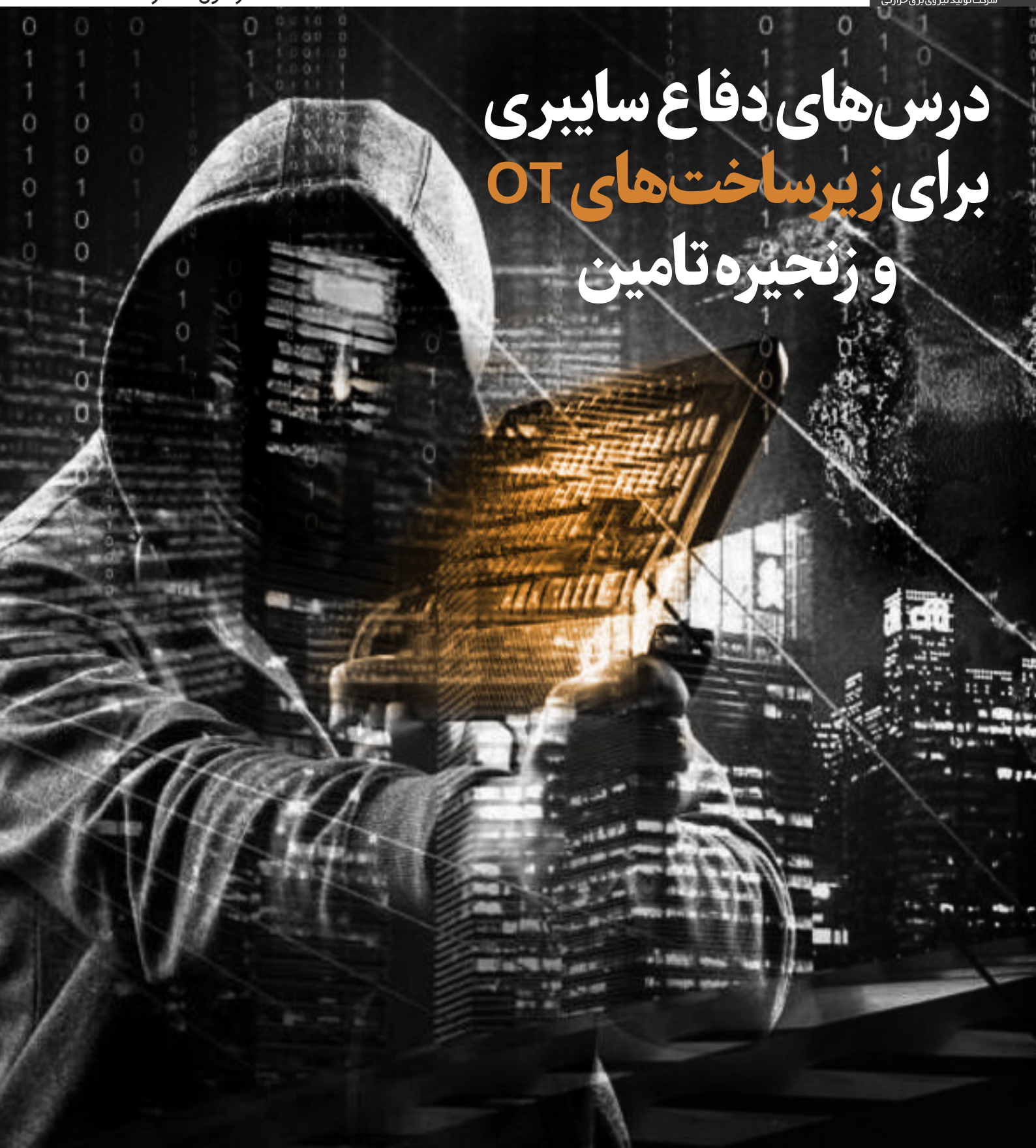
شرکت مادر تخصصی تولید نیروی برق حرارتی
پژوهشگاه نیرو
برسام
برنامه سازمانی آگاهی رسانی امنیت سایبری
شرکت تولید نیروی برق حرارتی

دیده‌بان امنیت سایبری

- هفت دلیل مهم آگاهی‌رسانی امنیت سایبری
- روان‌شناسی سایبری، کلید امن‌سازی عنصر انسانی در سازمان‌ها

شماره اول ▪ مرداد ماه ۱۴۰۱



درس‌های دفاع سایبری برای زیرساخت‌های OT و زنجیره تامین

دیده‌بان امنیت سایبری

شماره اول ـ مردادماه ۱۴۰۱

فهرست

آگاهی‌رسانی امنیت سایبری به این هفت دلیل مهم است:

به طور متوسط هر رخنه اطلاعاتی برای شرکت‌های بریتانیایی ۲٫۹ میلیون پوند هزینه در بر داشته است.
در سال ۲۰۱۹، خطای انسانی عامل ۹۰ درصد این رخنه‌های اطلاعاتی بود.

این دلایل به تنهایی برای متقاعد کردن افراد در خصوص اهمیت آگاهی‌رسانی امنیت سایبری کافی است.

بر اساس گزارش اخیر سازمان مهارت‌های دیجیتالی، فرهنگی، رسانه‌ای و ورزشی در خصوص مهارت‌های امنیت سایبری در سال گذشته تنها ۱ کسب‌وکار از ۹ کسب‌وکار (۱۱٪) به کارکنان غیرسایبری خود آموزش‌ها و مطالب آگاهی‌رسانی امنیت سایبری ارائه کرده است.
در بعضی سازمان‌ها آموزش معمولا به‌صورت اجباری است، اما در ۳ مورد از ۱۰ مورد (۳۰٪) بخش خصوصی، این‌گونه نیست. به نظر می‌رسد که هنوز افراد بسیاری در مورد مزایای آگاهی‌رسانی امنیت سایبری متقاعد نشده‌اند.
سوال اینجاست که چرا آموزش دانش امنیت سایبری تا این حد مهم است؟ در اینجا به ذکر هفت دلیل می‌پردازیم.

۱. جلوگیری از رخنه ها و حملات

برای آگاهی‌رسانی امنیتی لازم نیست با اهداف بزرگ شروع کنیم. شروع کار با بدیهی‌ترین آگاهی‌رسانی‌های امنیت سایبری نیز به جلوگیری از نقض حریم داده‌ها کمک می‌کند. اینکه بگوییم با چه تعداد جلسه آموزشی می‌توانیم از رخنه‌های اطلاعاتی جلوگیری کنیم دشوار است. در یک شرایط و فضای ایده‌آل، ما می‌توانیم یک آزمایش کنترل‌شده را برای مقایسه کسانی که آموزش دیده‌اند و کسانی که آموزش ندیده‌اند به اجرا بگذاریم.

ممکن است برای بسیاری از سازمان‌ها این یک گام بسیار بلند باشد. اما بدان معنا نیست که ما نمی‌توانیم نرخ بازگشت سرمایه (ROI) در این خصوص را شاهد باشیم. به سادگی می‌توانیم تعداد حوادث قبل و بعد از اقدامات آموزشی و آگاهی‌رسانی در حوزه امنیت سایبری را با هم مقایسه کنیم. معیارهای به‌دست‌آمده را می‌توان برای جمع‌آوری شاخص نرخ بازگشت سرمایه استفاده کرد.

رخنه‌های اطلاعاتی می‌تواند میلیون‌ها دلار هزینه در پی داشته باشد در حالی که آموزش نسبتاً ارزان است. محاسبه نرخ بازگشت سرمایه‌ای که برای آموزش اختصاص داده می‌شود چندان مشکل نیست.

۲. فرهنگ‌سازی در خصوص امنیت سایبری

فرهنگ‌سازی در زمینه امنیت مدت‌هاست که برای مدیران ارشد امنیت اطلاعات (CISOs) مانند هدفی دست‌نیافتنی دیده می‌شود. به این ترتیب دستیابی به چنین فرهنگی به‌طور آشکارا بسیار دشوار است.
با کمک آگاهی‌رسانی امنیت سایبری، خیلی از افراد مسیر درست حرکت را پیدا می‌کنند. فرهنگ‌سازی در زمینه امنیت به معنای تعریف و تزریق ارزش‌های امنیتی در تار و پود کسب‌وکار است. آموزش‌هایی که آگاهی از موقعیت و شرایط (دلیل در معرض خطر بودن) را با خود به همراه دارد و علاوه بر آن مزایایی برای کار و زندگی شخصی ارائه می‌دهد.
پلتفرم‌های آموزشی پیشرفته می‌توانند به توسعه فرهنگ امنیت کمک کنند و کارکنان را در خط مقدم دفاع قرار دهند.

۳. تقویت سیستم دفاع فناورانه

سیستم‌های دفاعی فناورانه، سلاح ارزشمندی در جلوگیری از رخنه‌ها هستند؛ اما دفاع فناورانه نیازمند ورود افراد به این حوزه است. فایروال‌ها باید توسط افراد تنظیم شوند؛ هشدارهای امنیتی باید تایید شوند و نرم‌افزارها باید به‌روز شود.
امروزه تعداد کمی از کسب‌وکارها به کار کردن بدون داشتن سیستم دفاع فناورانه فکر می‌کنند. با این حال، بدون آموزش و آگاهی‌رسانی لازم، نمی‌توان از پتانسیل دفاع‌های فناورانه بهره کافی برد.
امروزه مهاجمان به‌ندرت خود را برای حمله به مشاغل، آن هم فقط از طریق ابزارهای فناورانه، به زحمت می‌اندازند. مهاجمان امروزی

معمولاً افراد را هـــدف قرار می‌دهند و این آســـان‌ترین راه برای ورود به شبکه‌های محافظت‌شده است.

۴. به مشتریان خود اطمینان دهید

مصرف‌کنندگان بیـــش از پیش از تهدیدات ســـایبری آگاه هســـتند. آنها به عنوان مشـــتری، خواهان احســـاس امنیت و حفاظت هستند. کســـب‌وکاری که برای بهبود امنیت ســـایبری، اقداماتی صورت دهد، بهتر می‌تواند اعتماد کاربران را جلب کند. یک کســـب‌وکار قابل اعتماد، کسب‌وکاری است که مشتریان به آن وفادار بمانند.

این مطلب فقط یک فرضیه نیست. یک نظرســـنجی که اخیرا توسط Arcserve انجام شد نشان داد که ۷۰٪ از مخاطبان سازمانی معتقدند که مشـــاغل به اندازه کافـــی برای تضمیـــن امنیت ســـایبری اقدامی نمی‌کنند. تقریباً دو ســـوم مخاطبان از تجارت با کسب‌وکارهایی که در سال گذشته حمله سایبری را تجربه کرده، اجتناب می‌کنند.

واضح اســـت که مشـــتریان به اعتبارنامه های امنیتی توجه می‌کنند.

این تهدید با همکاری دولت و قانون‌گذاران در سطح ملی و بین‌المللی، یک رویکرد مشـــارکتی در پیش گرفته‌ایم.» همـــکاری cybersafe و مرجع ناظر امور مالی در زمینه تاب آوری سایبری.

پیروی از قانون در کنار دانش امنیتی خوشایندتر است. کسانی که چنین آموزش‌هایی را در ســـازمان خود ارائه می‌دهند امنیت بیشتری را تجربه خواهند کرد که البته در بسیاری از صنایع، بخشی از الزامات قانونی است.

۶. مسئولیت اجتماعی یک کسب‌وکار

همان‌طور که WannaCry و NotPetya در ســـال ۲۰۱۷ نشان دادند، حملات سایبری می‌توانند با سرعت بالایی گســـترش پیدا کنند. هرچه شبکه‌های بیشتری آلوده شوند، سایر شـــبکه‌ها بیشتر در معرض خطر قرار می‌گیرند. ضعف یک شـــبکه می‌تواند تهدید کلی و فزاینده‌ای برای سایر شبکه‌ها باشد.

فقـــدان آموزش‌های دانـــش امنیـــت ســـایبری در یک ســـازمان، ســـازمان‌های دیگر را نیز در معرض آســـیب قرار می‌دهد. درست مثل

زمانی که آگاهی‌رسانی امنیت ســـایبری را برای کسب‌وکار خود در نظر می‌گیرید، مشتریان، شما را مســـئولیت‌پذیرتر قلمداد خواهند کرد. این یک گام مثبت است.

۵. قانون‌مداری

به طور واضح باید گفت پیـــروی از قانون به تنهایـــی دلیلی برای ارائه طرح‌های آگاهی‌رسانی امنیت سایبری نیســـت. کسانی که آموزش را صرفاً برای رعایت مقررات انجام می‌دهند خطر کم‌کاری و ســـرهم‌بندی کردن امور را دارند.

با این حال، قانون‌گذاران بیش از پیش خواهان اجرای آگاهی‌رســـانی امنیت سایبری در صنایع هستند. «شرکت‌ها در هر اندازه و وسعتی و از هیئت‌مدیره گرفته تا تک‌تک کارمندان؛ باید «فرهنگ امنیتی» را توسعه دهند. امنیت سایبری یک مسئولیت همگانی است و ما برای مقابله با اینکه درِخانه خود را بـــاز بگذارید در حالی که کلیدهای خانه همســـایه داخل منزل شماست.

آگاهی‌رسانی امنیت سایبری فقط به نفع شما نیست. منفعت این کار به مشـــتریان، تامین‌کنندگان و هر فرد دیگری که با شـــبکه شما مرتبط است، می‌رسد.

۷. بهبود رفاه کارکنان

تحقیقات به‌خوبی نشان داده اســـت که آگاهی‌رسانی امنیت سایبری فقط افراد را در محل کار ایمن نگه نمی‌دارد بلکه آنها را در زندگی شخصی خود نیز ایمن می‌کند. در بیشـــتر موارد، این مزیـــت خاص موردتوجه کسی قرار نگرفته‌است. بنابراین اگر آگاهی‌رسانی امنیت سایبری دارای کارایی لازم باشـــد هم کارفرما و هم کارمنـــدان از آن نفع می‌برند و این باعث بهبود کلی عملکرد می‌شود.

درس‌های دفاع سایبری برای زیرساخت‌های OT و زنجیره تامین

دنیای سایبری در سال ۲۰۲۲ بسیار شلوغ و پرتنش بود. در حالی که در سال ۲۰۲۱ نشانه‌هایی مبنی بر افزایش فعالیت تهدیدکنندگان و هدف گرفتن محیط‌های OT با باج‌افزار وجود داشت، جنگ در اوکراین، بسیاری از کسب‌وکارها را بر آن داشت تا با سخت‌گیری بیشتری انعطاف‌پذیری فناوری‌های عملیاتی (OT) و زیرساخت‌های زنجیره تأمین خود را بررسی کنند.

آژانس امنیت زیرساخت سایبری (CISA) اندکی پس از آغاز تهاجم به اوکراین گزارش داد که روسیه زیرساخت‌های حیاتی اوکراین را هدف قرار داده است تا این کشور را قبل از تهاجم در هفته‌های منتهی به حمله روسیه در ۲۴ فوریه فلج کند. چرا این مسئله مهم است؟ موفقیت یا شکست این تلاش‌ها تا حد بسیار زیادی به جمع‌آوری اطلاعات در خصوص هدف، برقراری ارتباط سالم و زیر سلطه گرفتن سازمان‌های مختلف و بهره‌گیری از یک پی‌لود برای دستیابی به هدف نهایی حمله بستگی دارد. این نوع رفتار عاملین تهدید به درگیری‌های نظامی محدود نمی‌شود و غالبا به گروه‌های تبهکار تهدیدکننده که در کار خود موفق هستند نیز نسبت داده می‌شود. حمله انکار سرویس ممکن است به عنوان روشی برای ایجاد اختلال، منحرف کردن مسیر و جلب توجه به سمتی دیگر استفاده شود در حالی که حمله دیگری علیه هدف اصلی انجام می‌شود.

روسیه در حملات سایبری علیه OT و زیرساخت‌های حیاتی پیشتاز است.

آنچه تاکنون شاهد آن بوده‌ایم شامل تلاش‌هایی برای پاک کردن سیستم‌ها به کمک باج‌افزار، کمپین‌های اطلاعات دروغ و حملات انکار سرویس توزیع‌شده (DDOS) علیه زیرساخت‌های دولت اوکراین است که بر توانایی آن در ارائه اطلاعات به افراد در داخل و خارج از اوکراین تأثیر گذاشته است.

CISA اول مارس در یک هشدار خاطرنشان کرد:

- در ۱۵ ژانویه، مرکز جاسوسی تهدید مایکروسافت (MSTIC) فاش کرد که بدافزاری تحت عنوان ویسپرگیت (WhisperGate) برای هدف قرار دادن سازمان‌ها در اوکراین استفاده می‌شود. بنابر اظهار مایکروسافت، ویسپرگیت مخرب است و به گونه‌ای طراحی شده که دستگاه‌های هدف گرفته شده دیگر قابل راه‌اندازی و اجرا نیستند. این سیستم‌ها بر چندین سازمان دولتی، غیرانتفاعی و فناوری اطلاعات تأثیر گذاشت که همگی در اوکراین مستقر هستند.
- در ۲۳ فوریه، چندین محقق امنیت سایبری فاش کردند که بدافزاری تحت عنوان هرمتیک وایپر (HermeticWiper) علیه سازمان‌ها در اوکراین به کار گرفته می‌شود. طبق گفته سنتینلبز، این بدافزار ابزارهای مجهز به ویندوز را هدف قرار می‌دهد و رکورد اصلی بوت را دستکاری می‌کند که منجر به اختلال و خرابی در بوت بعدی می‌شود.

فناوری عملیاتی و زنجیره تامین در خط حمله احتمالی هستند

من به مطالعه گذشته علاقه زیادی دارم و به همین دلیل است که همیشه فکر می‌کنم نشان دادن ریشه‌های OT در ۲۰ سال گذشته و درک اینکه چقدر امروز مرز بین محیط‌های داده شرکتی و OT محو شده، مفید است.

در حال حاضر برخی از مردم هنوز به OT به‌عنوان یک حوزه تخصصی در امنیت سایبری نگاه می‌کنند که باید پرسنل متخصصی به آن اختصاص داده شود اما واقعیت این است که OT تغییر کرده است. فناوری عملیاتی، دیگر فقط در داخل تاسیسات هسته‌ای یا نیروگاه‌های مرتبط با تامین انرژی و آب یافت نمی‌شود. OT از زیرساخت‌های فیزیکی و حیاتی و شبکه‌ها فراتر رفته و به فناوری عملیاتی روزمره شرکت گسترش یافته است.

OT تبدیل به یک الگوی رفتاری برای خرده فروشی و میزبانی شده است. به یک الگوی رفتاری برای بسیاری از صنایع تبدیل شده است زیرا کسب‌وکارهای دیجیتال و 5G را برای افزایش درآمد و توانایی خود در دستیابی به مشتریان به جلو می‌راند. OT اکنون نقش فزاینده‌ای در زنجیره تامین و نیروی کار دیجیتال ما ایفا می‌کند که این نقش شامل توانمندسازی کارمندان و پیمانکاران برای موفقیت در انجام مأموریت‌هایشان است. در مورد نیروهای کار مختلط، همه این ویژگی‌های مختلف به OT گره می‌خورند.

در تحقیقات مرتبط با تهدید می‌بینیم که مهاجمان از این واقعیت که OT برنامه‌های دفاع سایبری کسب‌وکارها را به روش‌های جدید، اما با برخی تاکتیک‌ها و تکنیک‌های سنتی به پیش می‌برد، بهره‌برداری می‌کنند.

جالب اینجاست که عوامل تهدید لزوماً برای محیط OT در حال تعریف حملات جدید یا به‌روزرسانی حملات قدیمی نیستند. در عوض، آنها بسیاری از تهدیدها و تاکتیک‌هایی را که هر روز استفاده می‌شوند به کار می‌برند؛ به این دلیل که مهاجم هنوز باید به نوع پوشش دفاعی سازمان نگاه کند، سپس نحوه به‌کارگیری و انتقال بدافزار، شناسایی اهداف، دسترسی فرمان و کنترل، استخراج داده‌ها و رد گم کردن را بیابد. در واقع هیچ چیز جدیدی در این بین وجود ندارد و از همان راهکارهای موثر قبلی برای هدف گرفتن فناوری عملیاتی استفاده می‌شود.

تهدید OT بسیار واقعی است. ما شاهد حجم باورنکردنی تحقیقات درباره تهدیدها و پشتکار بسیار زیاد مهاجمان، سازمان ها و دولت‌های تبهکار برای بهره‌برداری از محیط OT هستیم.

تفاهم با شرکای زنجیره تامین سازمان و سیستم‌های مورد نیاز برای بهره‌برداری موثر از زنجیره تامین

اجازه بدهید از دو منظر متفاوت در مورد زنجیره تامین صحبت کنیم. اولین منظر این است که یک سازمان باید فروشندگانی را که برای همکاری انتخاب می‌کند تا حد امکان حفظ، کنترل و بررسی کند تا اطمینان حاصل شود که آنها از خطرپذیری‌های قابل قبول در شرکت شما فراتر نمی‌روند.

منظر دوم چگونگی تضمین تداوم زنجیره تامین و نقش امنیت در انعطاف‌پذیری سیستم عملیاتی است. بهترین راه برای انجام این کار استفاده از چارچوب امنیت سایبری NIST است. NIST زنجیره تامین را به چندین حوزه تقسیم می‌کند: شناخت، محافظت، کشف، واکنش و بازیابی. NIST همچنین به زعم من امکان بازنگری سریع این موضوع دارد که چگونه یک سازمانه سطح حمله کلی را که دربرگیرنده زنجیره تامین است، می‌شناسد؟

این دانش به معادله OT گره خورده است زیرا بسیاری از اصول امنیتی با بررسی زیرساخت‌های شرکتی متولد شده‌اند. آیا محیط پیرامونی امن است؟ آیا ما زیرساخت‌های اساسی را در اختیار داریم تا به پذیرش آنها پایبند باشیم؟

هنگامی که پاسخ این سوال را دادید به عنوان یک کسب‌وکار انعطاف‌پذیری بیشتری دارید که فراتر از اثبات پذیرش است. در مرحله بعد، باید مشخص کنید که چه چیزی را در اولویت قرار دهید. این اولویت‌بندی شامل شناخت سطح حمله و نحوه حفظ دارایی‌های حیاتی است.

این دانش شامل دسترسی فیزیکی نیز می‌شود. به عنوان مثال، درک فرایند انتقال کامیون‌ها از یک ساختمان به ساختمان بعدی یا کشتی‌هایی که از یک بندر به بندر دیگر می‌روند، می‌تواند پایبندی و انعطاف‌پذیری سایبری را تضمین کند.

هم‌اکنون، در حالی که ما با تهدیدات سایبری ایجاد شده به‌واسطه جنگ اوکراین و روسیه روبرو هستیم، مهم است که متوجه شویم این اقدامات در ابعاد وسیعی در جهان گسترش یافته و سازمان‌ها برای ایمن ماندن باید همه جنبه‌های تجارت خود، ازجمله فناوری عملیاتی و زنجیره تامین را در نظر بگیرند.

تقویت افراد، فرایندها و فناوری‌های دفاع سایبری برای پاسخگویی به تهدیدات OT و زنجیره تامین

اگرچه کشورهای خارج از اوکراین درگیر مواجه فیزیکی یا رویارویی مستقیم با روسیه نیستند، اما بسیاری از کشورها با اوکراین همسو شده‌اند و از تحریم‌های سنگین علیه روسیه حمایت می‌کنند. ایالات متحده، کانادا، بریتانیا، آلمان و سایر کشورهای ناتو و همچنین کشورهایی مانند استرالیا، همگی تحریم‌های مالی شدیدی علیه روسیه صورت داده‌اند. این‌گونه اقدامات مستلزم آن است که نهادهای شرکتی این کشورها نسبت به اقدامات تلافی جویانه در عرصه دیجیتال هوشیاری بیشتری داشته باشند.

چنین حمله تلافی‌جویانه‌ای نباید از سوی یک دولت-ملت درگیر در مناقشه باشد. نگرانی من بیشتر در مورد ناسیونالیست‌های داخل روسیه یا وابسته به روسیه است که امکان دارد در حمایت از روسیه در برابر تحریم‌ها، به دنبال کمک یا واکنش و حمله سایبری باشند. علاوه بر این، من نگران فرصت‌طلبان مالی هستم که کاملاً با انگیزه منافع مالی به دنبال سوءاستفاده از این مسئله هستند. این نوع اقدام تلافی‌جویانه می‌تواند علیه زیرساخت‌های شرکت‌ها یا کشورهایی صورت گیرد که در مورد افکار و دیدگاه‌های خود در مورد اقدام روسیه در اوکراین بسیار باز و شفاف عمل کرده‌اند.

اگر کسب‌وکار شما هنوز وضعیت انعطاف‌پذیری برای خود در نظر نگرفته است، ممکن است زمان آن فرا رسیده‌باشد که کارشناسان امنیتی شرکت به آموزش فعالانه و راهنمایی همکاران و هیئت‌مدیره بپردازند تا درمورد معنای تهدیدات OT و زنجیره تأمین برای کسب‌وکار شفاف‌سازی شود. آیا شرکت، به برنامه دفاع سایبری برای مقابله با این تهدیدها مجهز شده است و آیا اطمینان دارید که کسب‌وکار متوجه خطرات و توانایی دفاع سایبری و انعطاف‌پذیری در برابر این خطرات است؟

همه ما در این روند نقشی داریم و اگر قبلاً به آن فکر نکرده‌ایم، زمان خوبی است که این بحث‌ها را با تیم‌های امنیتی و کسب‌وکار پیش ببریم.

کوین میتنیک در سال ۲۰۰۲ گفت که ضعیف‌ترین حلقه در زنجیر امنیت اطلاعات، عنصر انسانی است و از آن پس ما این حرف به کرات شنیده‌ایم. به‌صورت کلی محیط فعلی ما در بهترین حالت محیطی ناامن است. با یادگیری برخی درس‌ها و آموزش‌های روان‌شناسی سایبری، عامل انسانی می‌تواند از ضعیف‌ترین حلقه زنجیر به قدرتمندترین بخش آن تبدیل شود.

روان‌شناسی سایبری
کلید امن‌سازی عنصر انسانی در سازمان‌ها

روان‌شناسی سایبری دقیقاً چیست؟

روان‌شناسی سایبری به‌عنوان یک نظام به بررسی تعامل میان ذهن و رفتار انسان در قالب فرم‌های مختلف فناوری ارتباطات و اطلاعات می‌پردازد. این فرم‌ها نه فقط شامل ایمیل، اینترنت یا رسانه‌های اجتماعی می‌شوند که واقعیت مجازی، بازی‌ها و دستگاه‌های هوشمند را نیز در بر می‌گیرند.

در عمل، نهایت همه این داستان‌ها درک این موضوع است که انسان‌ها فناوری را چگونه درک می‌کنند. با یک مثال پیش برویم. همکار شما موهایش را با مدلی تازه کوتاه کرده‌است. تعریف‌کردن از او نشانه ادب شماست. شما می‌توانید این موضوع را در اداره بر زبان بیاورید، می‌توانید به او پیامک بزنید، می‌توانید در صفحه فیس‌بوکش در این باره بنویسید یا حتی یادداشتی بنویسید و به شیشه ماشین‌اش بچسبانید.

اگر فقط داده‌ها را در نظر بگیریم در همه این حالت‌ها شما محتوای واحدی را منتقل کرده‌اید، اما درک اشارات و دلالت‌های ضمنی رسانه‌ای که برای انتقال این پیام انتخاب کرده‌اید و انتخاب بهترین گزینه ممکن در واقع عصاره و چکیده روان‌شناسی سایبری است.

اگر بخواهیم با اصطلاحات عملکردی برای حرفه‌ای‌های امنیت صحبت‌کنیم باید انطباق با سیاست‌های امنیتی را مدنظر بگیرید. فرض کنیم شما تغییری را در سیاست امنیتی سازمان‌تان اعمال کرده‌اید. بهترین راه اطلاع‌رسانی در این زمینه چیست؟ در بیشتر موارد این کار از طریق ایمیل صورت‌می‌گیرد، اما آیا این واقعاً بهترین شیوه است؟ به‌طور مشابه اگر تصمیم داشته‌باشید که افراد واقعاً رفتارشان را عوض‌کنند، ارسال یک ایمیل به همه کارکنان روش مناسبی برای اعمال تغییر است؟ اولین درس روان‌شناسی سایبری این است که «بستر انتقال پیام خود نیز حاوی پیام است.»

درس دوم هم درست به همین اندازه مهم است. اگر دوباره به مثال چسباندن یادداشت به شیشه ماشین برگردیم، انتخاب بستر انتقال پیام کاملاً به این بستگی دارد که مخاطب شما کیست و توجه به همین نکته برای شما کافی است. روان‌شناسی به تنوع وسیع رفتارهای آدمی توجه دارد و درنتیجه روان‌شناسی سایبری توجه به همین موضوع در حوزه فناوری اطلاعات است.

برای داشتن امنیت رو به پیشرفت و مناسب، نیازمند درک و پذیرش از سوی همه اعضای سازمان از مدیرعامل گرفته تا پیمانکاران موقت هستیم. به این ترتیب روان‌شناسی سایبری یعنی از مرز کاربر نهایی هم فراتر برویم تا به این ترتیب بتوانیم درک کنیم که افراد در دنیای واقعی به‌واسطه جنسیت، سن، شخصیت، تجربه‌های قبلی، فرهنگ و البته میزان حقوق با هم متفاوت هستند.

می‌دانیم که آنچه در اینترنت اتفاق می‌افتد به‌نوعی متفاوت با دنیای واقعی است، اما در عین حال آنچه در اینترنت روی می‌دهد خود زندگی واقعی است. شاید چند مفهوم کلاسیک موضوع را آشکارتر کند.

اول اینکه اینترنت طراحی شده تا ارتباطات را ساده کند به این ترتیب ما کاملاً در آن غرق می‌شویم. این همان چیزی است که از آن با نام حضور از راه دور یا Telepresence یاد می‌کنند. یک کارمند معمولی شما به احتمال زیاد نمی‌داند که چه حجمی از محاسبات پیچیده باید صورت‌بگیرد تا او بتواند از طریق تلفن هوشمند و شبکه‌های وای‌فای عمومی به ایمیل کاری خود دسترسی پیدا کند. از دید مهندسان انجام چنین کاری بسیار ساده و راحت است، اما از دید مدیر امنیت اطلاعات شرکت، فرایندی بسیار دشوار خواهدبود.

با توجه به اینکه کارمندان از همه اتفاقاتی که در پس‌زمینه رخ می‌دهد غافل هستند، نمی‌دانند که چنین کاری تا چه حد خطرناک خواهدبود. آگاهی درباره امنیت سایبری مستلزم شکستن این تصور «حضور از راه دور» است.

دوم اینکه در هرجای اینترنت که بگردید، چیزی در حدود ۹۰ درصد افرادی که به یک فروم سر می‌زنند، فقط مطالب را می‌خوانند و در حد قابل ذکری در مباحث مشارکت نمی‌کنند. این کار را پاورچین رفتن یا Lurking می‌نامند. درنتیجه وقتی کارمندی وارد یک سیستم کامپیوتری سازمانی می‌شود تا زمانی که کسی با او تعاملی انجام

نداده‌اســت خود را نامرئی تصور می‌کند. این زمانی است که تهدیدات داخلی ظاهر می‌شــوند، چرا که این کارمندان هیچ‌گاه فکر نمی‌کنند که ممکن است کسی در حال تماشای فعالیت‌های‌شان باشد، اما برای یک مدیر امنیت اطلاعات ســؤال اصلی این است که شبکه داخلی شرکتش تا چه حد قابل رویت است. امنیت سایبری مستلزم مدیریت چیزهایی است که ما نامرئی فرض می‌کنیم.

ســوم اینکه در فلســفه ســنتی اینترنت همه با هم برابر هســتند و هیچ کنترل مرکــزی وجود نــدارد. این موضــوع را کاهــش مقام یا Minimization of status می‌نامیــم. تقریباً غیرممکن اســت که بتوانیم افرادی را که در اینترنت هســتند به اجبار به کاری وادار کنیم. در ساده‌ترین حالت، آنها فقط برای سرگرمی هم که شده مقاومت می‌کنند. نتیجه نهایی این حرف این اســت کــه تلاش برای پیاده‌ســازی نظم و قانون در حوزه فناوری اطلاعات کاری دشــوار اســت. امنیت سایبری مســتلزم کنترل چیزهایی اســت که از اســاس برای مقاومت در برابر حاکمیت طراحی شده‌اند.

مزیت‌های روان‌شناســی سایبری در محیط کســب‌وکارهای امروزی چیست و چرا به آن احتیاج داریم؟

برای این مشــکلات راه‌حلی وجود دارد. یک فرآینــد مدیریت امنیت اطلاعات مبتنی بر روان‌شناسی سایبری، توقعات زیادی در زمینه کنترل عنصر انســانی ســازمان دارد. این توقعات چه هســتند؟ ما بیشتر به تسخیر قلب‌ها و همدلی نیاز داریم تا به ترس.

ترغیب احساسی: ما به تسخیر قلب‌ها و ذهن‌های بیشتر و ترس کمتر و همدلی نیاز داریم. این کار مســتلزم آموزش معمول، متنوع و دائمی است. افراد برخلاف ماشین‌ها به‌ندرت براساس اطلاعات منطقی تغییر رفتار می‌دهند. آنها به روابط عمومی و اندیشه‌زایی احتیاج دارند. گروه امنیت سایبری باید با منابع انسانی سازمان و کارکنان تیم‌های عملیاتی دوست شوند.

رهبری توزیع‌شــده: به تیم‌ها اجــازه دهید که سیاســت‌های خاص خودشــان را توســعه دهند. اینکه شــما نمی‌توانید یک کنترل متمرکز داشته‌باشــید به ایــن معنی نیســت کــه نمی‌توانید هیــچ کنترلی داشته‌باشــید. تصمیم‌گیــری در زمینه امنیت اطلاعــات را به رده‌های پایین‌تــر و بیرونی‌تر محــول کنید تــا ماژول‌های مقاوم مجــزا از هم داشته‌باشند.

شهروند شبکه شــدن: مدیران امنیت اطلاعات می‌خواهند تمام شبکه داخلی ســازمان را ببینند، اما در عمل این کار غیرممکن اســت، پس از اعضای شــبکه برای این کار کمک بگیرید. افراد علاوه‌بر اینکه باید درگیر امنیت سایبری شده‌باشــند، باید مکانیزم‌های مشخص گزارش‌دهی را هم در اختیار داشته‌باشند.

چالش‌های احتمالــی همه‌گیر شــدن این موضوع میان شــرکت‌ها چیســت؟ آیا هیچ صنعتی وجود دارد که به روان‌شناســی ســایبری نیازمندتر باشد یا راحت‌تر با آن تطبیق پیدا کند؟

درحال‌حاضر از دید روان‌شناســی مشــکل اصلی در حلقه‌های امنیت سایبری، شــور و هیجان کاذب زیاد است که بیشــتر هم مبتنی‌بر ترس است درنتیجه کاربران راه چاره را در بی‌طرفی و سکوت می‌بینند: زمانی که باید درگیر امنیت سایبری باشــند و به آزادی درباره آن صحبت کنند، ترجیح می‌دهند حرفی نزنند و وانمود کنند که اصلاً اهمیتی ندارد.

به ناگزیــر همه‌گیر شــدن سیاســت‌های امنیت ســایبری مبتنی‌بر روان‌شناسی ســایبری، چالش‌هایی را با خود به همراه خواهدداشت. مدل رفع تکلیفی آگاهی‌دهی (کلاس آموزشــی نصــف روز، یک روز از سال برای کل کارکنان) در لیست بســیاری از مدیران باعث تیک‌خوردن گزینه امنیت ســایبری می‌شــود. همان‌طور که می‌دانید چنین مدلی، تأثیــر چندانی بر فرهنگ محیط کار نخواهدداشــت. مهم نیســت آن کلاس نصف روز چقدر خوب برگزار شود به محض این که یکی از کارکنان رده‌بالای شــرکت در حال تخلف از سیاست‌های امنیتی دیده‌شود، همه اثرات آن کلاس از بین خواهدرفت. تقلید نکته اصلی است! یک نفر این کار را انجام می‌دهد، بقیه می‌بیننــد و انجام می‌دهند و به‌تدریج به یک روند معمول تبدیل می‌شود.

پیاده‌سازی هر شــیوه‌ای به جز این کلاس‌های نصف روز به‌طور ضمنی مبین این است که مشــکل بزرگ‌تری در کار است. هرچند روان‌شناسی سایبری به ما می‌آموزد که در چنین شــرایطی حتماً مشکلات سازمانی بزرگ‌تری وجود دارد.

قانون کانوی (Conway law) قانونی عجیب از دنیای طراحی نرم‌افزار باقی‌مانده از دهه ۶۰ اســت که می‌گوید: «هر سازمانی که سیستمی را طراحی می‌کند، ناگزیر درنهایت سیستمی می‌ســازد که شبیه سیستم ارتباطات داخلی خودش اســت.» به همین ترتیب درنهایت شما هم به یک سیاست امنیت اطلاعاتی خواهیدرســید که نشان‌دهنده ساختار ارتباطی سازمان شما خواهدبود.

درنتیجه اگر سیســتم ارتباطات ســازمان شما مشــکل داشته‌باشد، سیاست امنیت اطلاعات شــما آن را منعکس کرده و بنابراین به‌درستی کار نمی‌کند. مهم اســت که به رده‌های بالای شــرکت تاکید کنید که اگر سیاست امنیت اطلاعات‌شان ضعیف است، این موضوع نشان‌دهنده ضعف ساختار سازمان شماست.

نفع مســتقیم پیاده‌ســازی یک سیاســت امنیت اطلاعــات مبتنی بر روان‌شناســی ســایبری چیســت و این منفعت چگونــه در میان بخش‌های مختلف سازمان تقسیم می‌شود؟

در گزارش Europol IOCTA هم از «عنصر انســانی» امنیت اطلاعات نام برده شــده اســت. آن‌جا از این عنصر به عنوان محیطی برای جرائم سایبری یاد شده اســت که مدام تهاجمی‌تر می‌شــود. تنها راه پیش رو در چنیــن محیطی همکاری و همراهی بیشــتر به‌صــورت افقی میان بخش‌های مختلف کســب‌وکار و بــه صورت عمودی میــان رده‌های مختلف یک سازمان است.

کسب‌وکارهایی که بتوانند هدف‌های سازمانی‌شان را با سیاست‌های امنیت اطلاعات هم‌راســتا کنند برای گذر از دهه آینده شانس بیشتری خواهند داشــت. این صنایع شامل کســب‌وکارهای مبتنی‌بر فناوری، مخابرات، ســازمان‌های مالی و اعتباری و رســانه‌ها خواهدبود. البته همان‌طور که پیش‌تر توضیح دادیم، هر ســازمانی که به تفکر صحیح و درست بپردازد، ارزش تدوین یک سیاســت امنیت اطلاعات سایبری را درک خواه کرد.

در فراینــد کار روزمره، امنیت به چه معنی اســت؟ ســازمان‌هایی که بتوانند اهمیت امنیت اطلاعات را در میان کارکنان‌شــان نهادینه کنند، شــرکت‌هایی که برای آموزش امنیت سایبری و آگاهی رسانی قدم‌های جدی برداشــته‌اند در آینده پیش رو برتری چشم‌گیری خواهند داشت، چراکه جرایم سایبری به وضوح سودآور و پول‌ساز هستند.

کارگروه فرهنگ‌سازی و آگاهی‌رسانی امنیت سایبری
شرکت مادرتخصصی تولید نیروی برق حرارتی (برسام)

تلفن دبیرخانه کارگروه برسام : ۵۸۳۷۶۶۴۲
پست الکترونیکی کارگروه برسام : Barsam[at]tpph.ir