سال نهم شماره چهل و نهم اردیبهشت ۱۴۰۲
دوماهنامه اقتصاد و مدیریت فناوری اطلاعات بیست‌هزار تومان

آیا «پاداش در ازای کشف باگ‌ها» باید قانونی شود؟

# دیدبان فناوری

یادگیری ماشینی برای امنیت نه جرایم سایبری

ISSN : ۲۴۲۳-۵۲۷X

# روان‌شناسی سایبری

## کلید امن‌سازی عنصر انسانی در سازمان‌ها

بسم الله الرحمن الرحیم


دیده‌بان فناوری

دوماهنامه اقتصاد و مدیریت فناوری اطلاعات

صاحب‌امتیاز: موسسه دیده‌بان ایما تدبیر
مدیرمسئول: علیرضا صالحی
زیرنظر شورای نویسندگان
گرافیک و صفحه‌آرایی: هلدینگ رسانه‌ای دیده‌بان
آدرس: سهروردی شمالی، کوچه حاج حسنی، پلاک ۵۵، واحد یک، تلفن: ۸۸۷۴۹۴۱۲
چاپ: کهن


## در این شماره می‌خوانید:

# blockchain
# هک کردن بلاک‌چین

کنستانتینو کاراگیانیس، مدیر تکنولوژی و مشاور امنیت شرکت آمریکایی BT در کنفرانس RSA2017 بیان کرده‌است که اینترنت تکامل‌یافته بدون امنیت در ذهن ما وجود دارد و اکنون بهای آن را می‌پردازیم. اکنون با استفاده از تکنولوژی Blockchain، ما فرصت فراهم‌کردن امنیت درست را از طریق یک رویکرد تعمدی و تعاملی داریم. Blockchain (زنجیره بلوک) فناوری است که از طریق آن هر دو طرف کاربری داده‌هایی را با یکدیگر مبادله می‌کنند که در یک بلوک فشرده می‌شود، بلوکی که کاراگیانیس از آن به‌عنوان «مبادله‌ای که کاملاً محاسباتی» یاد می‌کند. این بلوک با آمیزه‌ای شناسایی می‌شود که از نظر منطقی به بلوک‌های قبل از خود در زنجیره ارجاع داده‌می‌شود. در صورت شناسایی یک بلوک جدید، آن بلوک به بقیه زنجیره اضافه می‌شود، اما اگر یک بلوک تغییریافته اضافه شود، ترکیب تغییر کرده و همه چیزها برگشت می‌خورد. این مدل برای ایجاد تبادل شفاف و اعتماد ساخته شده‌است.

کاراگیانیس یادآور شد که این زنجیره به‌طور نمایی هر چهار سال قوی‌تر شده، بنابراین سبب افزایش حجم مبادلات قبلی می‌شود. مشهورترین روش زنجیره بلوکی تا به امروز، دیجیتالی شدن پول نقد و آمدن بیت‌کوین است که سبب افزایش حجم مبادلات می‌شود، چرا که ایجاد آن دشوار است.

تاکنون زنجیره بلوک مفهوم خود را وامدار دیگر اپلیکیشن‌هایی نظیر مدیریت دارایی‌های دیجیتال نظیر موسیقی یا روش‌های احراز هویت بوده است.

اما از دیگر سو، حملات مؤثر و هک روی زنجیره بلوک به‌عنوان یکی از محبوبیت‌های بیت‌کوین افزایش یافته است. مثال‌های کاراگانیس نشان می‌دهد که حملات نه علیه مفهوم بلکه در اجرا بوده‌است.

سایت کیف پول بیت‌کوین به نام پایگاه سکه‌ای امن‌ترین سایت برای خرید بیت‌کوین است، اما فقط برای حملات علیه سیستم‌های معکوس و زنجیره بلوکی.

اگر یک مسئله خاص کاربری نظیر تماس‌های از دست رفته یا گذرواژه‌های در معرض خطر وجود داشته‌باشد، این مشکل کاربر است.

هیچ FTIC از سرمایه‌گذاری پشتیبان نمی‌گیرد. کاراگانیس بیان کرده‌است که تلفن‌های هوشمند اندرویدی به سبب آپدیت‌های امنیتی ضعیف خود (به جز دستگاه‌های جدید)، آسیب‌پذیرترین دستگاه‌ها هستند.

اگرچه بزرگ‌ترین نگرانی این است که اگر زنجیره بلوکی بر اساس خانه‌های پوشالی دیجیتالی (از لحاظ امنیت) ساخته شده‌است به سبب استفاده از کلیدهای رمزنگاری عمومی در معرض مبادلات دیگر و آسیب‌پذیری در مقابل کدهای اصلاح خطا با محاسبات کوانتوم قرار می‌گیرد.

**حملات مؤثر و هک روی زنجیره بلوک به‌عنوان یکی از حوزه‌های محبوب افزایش یافته است**

## چه پیشنهادی دارید؟

تا زمانی‌که ممکن باشد، سازمان‌ها باید هرگونه کاربرد زنجیره بلوک را به‌منظور توسعه و یا به‌کارگیری آن، بدون امن‌سازی فراموش‌کنند و حتی‌الامکان از سایر فناوری‌ها بهره بگیرند. این امر باید شامل تایید این مورد باشد که آیا اپلیکیشن‌ها پروتکل و زنجیره بلوک را پوشش می‌دهند یا درصدد انجام چیزی جدید و تجربی هستند که درصد ریسک را افزایش می‌دهد.

او همچنین پیشنهاد می‌کند که امنیت اپلیکیشن را امتحان کنند تا تعهدات اخلاقی را برای عاری بودن از نواقص و انتخاب فروشندگانی که دارای تجربه حقیقی هستند به مورد اجرا بگذارند. کاراگانیس گسترش اجتماع زنجیره بلوک برای مشارکت‌های امنیتی برای آینده این تکنولوژی را پیشنهاد می‌نماید. به نحوی که همه بازیگران اصلی و از جمله امن‌سازان این قبیل فرآیندها در آن مشارکت داشته باشند.

# خودپردازها همچنان نقطه آسیب‌پذیری امنیت بانکی هستند

**علی‌رغم تحولات امنیتی مانند EMV، دستگاه‌های خودپرداز درمقابل حملات کلاهبردارانه نرم‌افزاری و فیزیکی آسیب‌پذیرند. از آنجا که مصرف‌کنندگان به‌طورکلی مسئولیتی در قبال سرقت از عابربانک ندارند، عرضه‌کنندگان کارت و اپراتورهای خودپرداز، متحمل ضرر و زیان فراوان می‌شوند. معیارهای مقابله شامل توسعه سیستم ضداسکیمینگ، فناوری، به‌روز کردن تنظیمات امنیتی OS و محدودکردن خودپردازها به‌گونه‌ای می‌شود که به‌وسیله هکرها قابل‌کنترل نباشند. باب میرا، تحلیلگر ارشد گروه بانکی امریکایی Celent، می‌گوید: «خودپرداز در طول زمان یک منبع سودآور برای کلاهبرداران بوده‌است به‌ویژه از طریق دستگاه‌های اسکیمینگ که اطلاعات کارت را برای ایجاد کارت‌های جعلی ذخیره‌می‌کنند تا بتوانند از آنها پول بگیرند و یا در خرید خرد از آن استفاده کنند.» به‌طورکلی احتمال می‌رود که خودپردازهای غیربانکی بیشتر مورد هدف باشند، چرا که در حول آنها تدابیر امنیتی کمتری لحاظ شده‌است اگرچه خودپردازهایی که بانک‌ها آنها را در تصاحب خود دارند به‌طور منظم از اسکیمینگ ضربه خورده‌اند.**

مترجم:
مسلم مسلمی‌زاده

توسعه‌دهندگان اینترنت اگر به EMV نپیوندند بابت زیان مالی توسط شرکت پشتیبان به خاطر کلاهبرداری‌های احتمالی از آنها مجبور به پرداخت غرامت خواهندبود

## EMV

مستر کارد و ویزا به‌عنوان بخشی از مهاجرت صنعت کارت‌های خودپرداز آمریکا به چیپ کارت‌های EMV، اکتبر ۲۰۱۶ و نوامبر ۲۰۱۷ را به‌عنوان آخرین مهلت این کار به اپراتورهای خودپرداز ابلاغ کردند. بعد از این مهلت قانونی، اگر یک کارت EMV به شکل کلاهبردارانه در خودپردازی که EMV را پشتیبانی نمی‌کند مورد سوءاستفاده قرار بگیرد، متقاضی مسئول جبران آن ضرر و زیان خواهدبود.

## دادخواست برای موارد غیر EMV

توسعه‌دهندگان اینترنت اگر به EMV نپیوندند بابت زیان مالی توسط شرکت پشتیبان به خاطر کلاهبرداری‌های احتمالی از آنها مجبور به پرداخت غرامت خواهندبود و یا ممکن است قراردادشان با شرکت را از دست بدهند.

Meara می‌گوید: «از نظر تئوریک نقل‌مکان به EMV کلاهبرداری را کم خواهدکرد، اما برای توسعه‌دهندگان مدت‌زمانی طول خواهد کشید تا به این سیستم نقل‌مکان کنند. در این فاصله، قوانین انتقال مسئولیت برای توسعه‌دهندگان یک مشوق الزام‌آور خواهدبود تا این تغییر را آغاز کنند. تصدیق اعتبار کاربر شامل خدمات بدون کارت و یا کیف پول‌های مبتنی‌بر تلفن همراه هوشمند، می‌تواند راه‌حل درازمدت بهتری باشد، اما برای آینده کمی کند خواهدبود.»

از ژانویه ۲۰۱۶ حدود ۵۱ درصد از ۱۲۰ توسعه‌دهنده خودپرداز شرکت‌کننده در پیمایش آمادگی برای حضور در خودپردازِ EMV که توسط اتحادیه صنعت خودپرداز (ATMIA) برگزار شده‌بود، قبلاً نیمی از دستگاه‌هایشان را به EMV ارتقا داده‌بودند. اگرچه این پیمایش به این نتیجه رسید که ۴۴ درصد خودپردازهای دارای قابلیت EMV تراکنش‌های EMV را نمی‌پذیرفتند، عمدتاً به‌خاطر اینکه کارکرد آنها به‌وسیله اپراتور خاموش شده‌بود.

هنگامی که کانادا در سال ۲۰۱۲ به EMV پیوست، بسیاری از خودپردازها به‌وسیله پشتیبان‌هایشان قطع اتصال شدند، چرا که به EMV نپیوسته بودند. بن نیئف، تحلیلگر ارشد گروه آمریکایی Aite ، می‌گوید که برخی از خودپردازها در آمریکا نیز به‌دلیل مشابهی اتصالشان قطع خواهدشد. طبق نظر این کارشناس «توسعه‌دهندگان اینترنت آمریکایی درآمد زیادی از جریمه بر روی خروج از سیستم کسب می‌کنند (۳ تا ۴.۵ دلار به‌ازای هر خروج)، بنابراین مشوق‌هایی برای خروج از EMV به‌وجود می‌آید.»

## اسکیمینگ

در آوریل ۲۰۱۶ شرکت Fico، شرکت آمریکایی نرم‌افزار تحلیل تقلب، شاهد بیشترین نرخ خطر کشف رمز خودپرداز به‌وسیله خدمات هشدار کارت خود بوده‌است. شمار خودپردازهایی که در سال ۲۰۱۵ تحت خطر کشف رمز (compromise) به‌وسیله دستگاه‌های اسکیمینگ بوده‌اند نسبت به سال ۲۰۱۴ به‌میزان ۵۴۶ درصد رشد داشته‌اند.

مطابق آمار FICO، اعمال خلاف قانون در خودپردازهای غیربانکی مانند کشف رمز خودپرداز در بالاترین نرخ خود بوده‌است که در آن نرخ کشف رمز ۱۰ برابر بوده‌است. در سال ۲۰۱۵ خودپردازهای غیربانکی ۶۰ درصد کل کشف رمزها را به خود اختصاص دادند در حالی که ۳۹ درصد از این نرخ را در سال ۲۰۱۴ داشتند.

نایف می‌گوید: «مجرمان می‌دانند که EMV ها در آینده به آمریکا می‌رسند و می‌خواهند در زمان مناسب آن را اسکیم کنند. شما می‌توانید داده‌های mag-stripe کارت‌های EMV را اسکیم کنید، اما کاری بسیار دشوار است، اگرچه از نظر فنی اسکیم‌کردن کارت داده‌ها از چیپ‌های EMV امکان‌پذیر است. مجرمان از چیپ‌های EMV در مقیاسی اقتصادی نمی‌توانند برای اسکیم استفاده کنند. طبق نظر اد اوبرایان، مدیر گروه‌های مشاوره خدمات کانال‌های بانکی شرکت آمریکایی مرکاتور، عرضه‌کنندگان آمریکایی کارت‌ها دچار ضرر و زیان‌های فراوانی از جانب خطر اسکیم‌شدن کارت‌هایشان می‌شوند.

نایف می‌گوید: «مشتریان از بابت تقلب کارت جریمه نمی‌شوند، به جز موارد بسیار نادری که اثبات آنها بسیار دشوار است مثلاً اگر رمز خود را روی برگه یادداشت بنویسند و آن را بر روی کارت بچسبانند و بر روی میزشان نصب کنند.»

لاچلان گان، مدیر اجرایی تیم امنیتی خودپرداز اروپایی، می‌گوید: «سارقان همواره از اسکیمرهای کارت‌های مغناطیسی برای خواندن اطلاعات کارت‌های مغناطیسی اروپایی EMV در مدل اروپایی EMV استفاده کرده‌اند و از کارت‌های کپی‌شده مشابه برای غیر EMV در خودپردازهای ایالات متحده استفاده کرده‌اند. برای اینکه اجازه داده‌شود تا دارندگان کارت از کارت‌شان در اروپا استفاده کنند، کارت‌های اروپایی هنوز کارت‌های مغناطیسی هستند. در سال ۲۰۱۶، EAST عنوان کرد که زیان ناشی از اسکیمینگ از جانب کارت‌های اروپایی که اطلاعات آنها خارج از اروپا ربوده شده‌است از سال ۲۰۰۸ تا کنون بی‌سابقه بوده‌است.

تی جی هوران، نایب رئیس FICO در مسائل مرتبط با کلاهبرداری، می‌گوید: «برای مقابله با اسکیمینگ، FICO امنیت فیزیکی بیشتر در اطراف خودپردازها را پیشنهاد می‌کند، به‌ویژه در اطراف خودپردازهایی که درون یک ساختمان قرار ندارند.» ما طرفدار استفاده از ابزارهای ضداسکیمینگ هستیم که می‌توانند به کشف و ممانعت از نصب ابزارهای خارجی به خودپرداز منتج شوند. این ابزارها در اشکال مختلف وجود دارند، اما بهترین ابزارهای ضداسکیمینگ، آنهایی هستند که به دستگاه این قابلیت را می‌دهند که در صورت بروز اختلال، خاموش شوند و یا اینکه هشداری را تولید کنند.

نایف می‌گوید: «توسعه‌دهندگان خودپرداز در فناوری‌های ضداسکیمینگ مانند جیتر سرمایه‌گذاری کرده‌اند که از یک حرکت نامنظم افقی در هنگام قرار دادن کارت در خودپرداز بهره‌می‌برد تا اطلاعات مغناطیسی کارت را ناخوانا کند که تحت اسکیمینگ قرار نگیرد یا در فناوری جمینگ سرمایه‌گذاری کرده‌اند که فرکانس‌های غیرمنظمی ایجاد می‌کند تا دستگاه‌های اسکیمینگ را مختل کند. بسیاری از تولیدکنندگان فناوری‌های ضد اسکیمینگ را بر دستگاه‌هایشان اعمال می‌کنند که اگر یک ابزار نتوانست مچ کلاهبردار را بگیرد ابزار دیگر این کار را انجام دهد.

داگلاس راسل، سرپرست مدیریت ریسک شرکت انگلیسی DFR، می‌گوید: « به نظر می‌رسد که اسکیم‌کردن خودپرداز در کشورهایی که کارت‌های کاملاً چیپ‌شده EMV را اجرا کرده‌اند و تدابیر امنیتی مانند جمینگ فعال و دستگاه‌های کشف اسکیمر را توسعه‌داده‌اند، کند شده‌باشد؛ اما هنوز به‌عنوان پرنفوذترین نوع کلاهبرداری از خودپرداز در سراسر جهان است. بنگاه‌های پیشروی کلاهبرداری آموخته‌اند که بر بسیاری از راه‌حل‌های ضداسکیمینگ با نازک‌کردن اسکیمرهایشان غلبه کنند (اصطلاحاً دستگاه‌های اسکیمینگ اینزرت) به‌طوری‌که بتوانند در داخل کارت‌خوان ATM واقعی قرار داده‌شوند و زیر بار جمینگ فعال و بسیاری از تکنولوژی‌های عیب‌یاب نروند که درحال‌حاضر توسعه یافته‌اند.

استراق سمع که شامل اتصال یک دستگاه ضبط‌کننده صدا در محدوده کارت‌خوان خودپرداز مادر می‌شود به‌عنوان یک روش رایج برای کشف رمز داده‌های کارت در خودپردازهایی می‌شود که راه‌حل‌های ضداسکیمینگ در آنها به کار گرفته شده‌است.»

**مطابق آمار FICO، اعمال خلاف قانون در خودپردازهای غیربانکی مانند کشف رمز خودپرداز در بالاترین نرخ خودبوده‌است که در آن نرخ کشف رمز ۱۰ برابربوده‌است**

## تحقیق آزمایشگاه کسپرسکی

جان گوئرو، محقق ارشد امنیت در آزمایشگاه کسپرسکی می‌گوید: «در برخی موارد، حمله‌کنندگان از بدافزارهایی مانند «اسکیمر» استفاده‌می‌کنند تا خودپردازها را تبدیل به اسکیمرهای کارت بکنند و بتوانند تقلب‌های بیشتری با کارت انجام دهند. در بیشتر موارد، مهاجمان به‌دنبال گرفتن پول از خودپردازها هستند، سیاست‌های پیشگیری از این سرقت شامل جایگزین‌کردن قفل‌های پیش‌فرض و به‌روز کردن نرم‌افزار استفاده‌شده برای اجرای خودپرداز می‌شود. حذف سربارهای غیرضروری مانند نرم‌افزار مدیریت از راه دور که به حمله‌کنندگان امکان دسترسی از راه دور را می‌دهد و همچنین به‌کارگیری راه‌حل‌های مناسب ضدبدافزاری نیز راهکار دیگری است.»

آن‌گونه که کسپرسکی اعلام کرده‌است در دوره ۲۰۱۵-۲۰۱۴، بانک‌ها در کل جهان، تحت‌تأثیر ۱۰۰ مورد حمله بدافزار خودپردازی Carbanak قرار گرفتند که این حمله بدافزاری برای هر بانک بین ۲.۵ تا ۱۰ میلیون دلار هزینه داشت.

گوئرو می‌گوید: «در ارتباط با مورد Carbanak به خودپردازها آموزش داده شده‌بود که تا پول را قبل از زمان معین‌شده بپردازند و همچنین به محتوای خودپرداز حمله کنند و با یک حامل پول که در اطراف کشیک می‌دهد هماهنگ باشند تا در زمان مقتضی بدون علامت دادن سربرسد.»

کمپانی فروش NCR می‌گوید: برای مقابله با بدافزارها، برنامه‌های خودپرداز باید در یک حساب «لاک داون» با حداقل امکانات اجرا شوند. همچنین توسعه‌دهندگان خودپرداز باید نرم‌افزارهای مؤثر فایروال و ضدبدافزار را به‌کار بگیرند.

در هرصورت، امنیت خودپرداز چیزی فراتر از بهترین رویه را دربرمی‌گیرد. توسعه‌دهندگان خودپرداز و دریافت‌کنندگان آن باید با استانداردهای «مجمع استانداردهای امنیتی صنعت پرداخت با کارت» مانند PCI DSS کنار بیایند. بهای تخطی از PCI DSS شامل جریمه نقدی به اضافه مسئولیت زیان‌های ناشی از کلاهبرداری‌هایی می‌شود که به تضییع حقوق دیگران می‌انجامد.

## دسترسی از راه دور به خودپرداز

جان گان مشاور، رئیس شرکت امنیت داده VASCO در زمینه ارتباطات مشترک، می‌گوید: «دو راه وجود دارد که تلفن‌های همراه می‌توانند به کاهش سرقت از ATM کمک کنند» یکی از این راه‌ها به‌وسیله کارت‌های بانکی امکان‌پذیر می‌شود و دیگری بدون کارت صورت می‌پذیرد. در مورد اول، بانکی می‌تواند یک گذرواژه یک‌بار مصرف را به شماره موبایل ثبت‌شده مشتری از طریق روش‌های امن انتشار بفرستد تا زمانی که از کارت استفاده‌می‌کنند به خودپرداز وصل‌شوند. بانک می‌تواند این کار را تنها در شرایط وجود ریسک‌های بالاتر و نه برای یکی از موقعیت‌های مکانی متداول خودپردازها انجام دهد همچنین می‌تواند این کار را در ارتباط با میزان برداشت خاص و یا زمان‌های خاصی از روز انجام دهد.»

طبق نظر نایف، بانک‌ها همچنین می‌توانند این اجازه را به مشتریان بدهند که تراکنش‌های خودپرداز بدون کارت را با استفاده از گوشی هوشمند انجام دهند تا آسیب‌پذیری کارت‌ها را در خودپرداز کاهش دهد.

گان می‌گوید: «در یک برداشت خودپرداز از راه دور، مشتری تمام جزییات تراکنش را به اپلیکیشن موبایل بانک خود وارد می‌کند سپس بانک یک کد QR بر روی صفحه خودپرداز ارائه‌می‌کند که به‌وسیله گوشی هوشمند خوانده‌می‌شود. اگر دستگاه و کاربر هم‌خوانی داشته‌باشند، تراکنش اتفاق‌می‌افتد و پول مهیا می‌شود. سرقت اطلاعات کارت‌های مغناطیسی برای هکرها بسیار آسان است، اما سرقت اطلاعات گوشی هوشمند اگر گوشی به‌خوبی مورد استفاده قرار بگیرد بسیار دشوار خواهدبود.»

درحالی‌که بانک‌های ایالت متحده دسترسی به خودپرداز موبایل مبتنی‌بر QR را آغاز کرده‌اند، دیگر امکانات بدون کارت خودپرداز، رمزهای یک‌بار مصرفی هستند که به‌وسیله پیامک فرستاده‌می‌شوند، روشی که به‌وسیله بانک‌های بریتانیایی و کیف‌پول‌های موبایل مبتنی‌بر NFC استفاده‌می‌شود. NFC خوان‌های وصل‌شده به خودپردازها می‌توانند خدمات بدون کارت را ممکن سازند. اگرچه بانک مرکزی آمریکا در ماه می ۲۰۱۶ اعلام‌کرد که مشتریانش قادر خواهندبود تا از کیف پول‌های دیجیتال مانند اندروید پی برای برداشت بدون کارت از خودپرداز استفاده‌کنند، نایف بر این باور است که بیشتر بانک‌ها، تصمیم خواهندداشت تا به کاربران این اجازه را بدهند که از کیف پول‌های موبایلی مبتنی‌بر NFC برای برداشت‌های بدون کارت استفاده‌کنند.

نایف می‌گوید: «به‌طور بالقوه، اپل پی، اندروید پی و غیره می‌توانند برای استخراج پول از خودپردازها استفاده‌شوند، اما عرضه‌کنندگان می‌خواهند کنترل‌شان را بر تراکنش‌های خودپرداز حفظ کنند. عرضه‌کنندگان (انتشاردهندگان) به نظر من به این کیف پول‌های موبایلی ثالث (واسط) اجازه استخراج پول را از خودپرداز نخواهند داد.»

جوزف والنت، تحلیلگر ارشد خدمات مشاوره تکنولوژی‌های نوظهور شرکت مرکاتور، می‌گوید: «دریافت پول مبتنی‌بر «توکنیزیشن (جایگزینی دیتای حساس با غیرحساس)» شماره کارت‌ها و نمونه‌سازی کارت‌های هاست (HCE) یک راهکار مقابله‌ای برای مجرمانی است که تلاش می‌کنند اطلاعات کارت‌ها را در خودپردازها به‌دست آورند. حتی اگر یک رمز را به دست بیاورند، نمی‌توانند کار خاصی با آن انجام‌دهند.»

در توکنیزیشن عمل جایگذاری اعداد کارت تراکنش خودپرداز و پوز با اعداد یک‌بار مصرف صورت می‌گیرد که شماره کارت واقعی در نرم‌افزار HCE مبتنی‌بر کلود ذخیره می‌شود و این نرم‌افزار به‌وسیله یک عرضه‌کننده و یا شخص ثالث مانند مسترکارت و ویزا اجرا می‌شود.

نایف می‌گوید: «خودپرداز مبتنی‌بر NFC کاملاً سریع به انگلستان مهاجرت خواهدکرد چرا که در آنجا از اقبال عمومی بیشتری نسبت به ایالات متحده آمریکا برخوردار است.» ابرایان از شرکت مرکانتور، می‌گوید: «به‌واسطه عامل گیتینگ برای پول گرفتن از خودپردازهای مبتنی‌بر NFC نیاز است که تلفن‌های همراه هوشمند با NFC سازگار باشند. اکثر بانک‌ها به‌دنبال ابعاد مختلف استناد به شخص (برای انجام تراکنش) هستند در عین حالی که برخی مردم تلفن هوشمند ندارند و یا با کدهای QR نمی‌توانند به‌راحتی کار کنند.» او می‌گوید: «کدهای QR و رمزهای یک‌بار مصرف نمایانگر راه‌حل موقتی و آسان‌تر برای بانک‌ها هستند. آنها می‌توانند راه‌حل‌های مبتنی‌بر QR را اکنون اجرا کنند و زمانی که NFC بر روی گوشی‌های هوشمند بسیار فراگیر شود به خودپردازهای مبتنی‌بر NFC کوچ کنند».

## بیومتریکس

راسل، مدیریت ریسک شرکت DFR، می‌گوید: «خودپردازهایی که بیومتریک را پشتیبانی می‌کنند، سرانجام تحت‌تأثیر نیاز به امنیت بیشتر به‌عنوان ابزاری برای بهبود دربرگیری مالی، کوچک‌تر می‌شوند.»

ژاپن در خیلی از خودپردازهایش اسکنرهای تشخیص اثرانگشت و شناسایی اثر کف دست را فعال کرده‌است. در جای دیگر، پذیرش داوطلبانه بیومتریک از سوی مشتری به‌وسیله تعداد دستگاه‌های الکترونیکی مخصوص مشتری به‌ویژه به‌وسیله گوشی‌های هوشمند که قابلیت‌های بیومتریک را به اشتراک می‌گذارد مورد معاینه قرار گرفته‌است، اما سیستم‌های بیومتریک به‌طور ذاتی امن نیستند و حملات می‌توانند در خودپردازهای بیومتریک که خطر کشف رمز در آنها وجود دارد با موفقیت صورت پذیرد، علاوه‌بر اینکه دستورهای بیومتریک دیگر نیز می‌تواند صورت‌بگیرد.

## بدافزار

بدافزارها باعث تهدیدات عمده برای خودپردازها می‌شوند. نایف می‌گوید: «چالشی که با بدافزارها وجود دارد این است که بسیاری از خودپردازها حتی در ایالات متحده نسخه‌های قدیمی ویندوز را اجرا می‌کنند که دیگر به‌وسیله مایکروسافت پشتیبانی نمی‌شوند و با آخرین به‌روزرسانی‌های امنیتی هماهنگ نیستند.»

از آوریل ۲۰۱۴، هر خودپردازی که برنامه‌هایش به جای ویندوز ۷ به‌وسیله سیستم‌عامل XP اجرا می‌شود، بسته‌های امنیتی مایکروسافت را دیگر دریافت نخواهدکرد که این کار باعث می‌شود تا در برابر بدافزارها و مداخلات شبکه آسیب‌پذیر شوند و الزامات استاندارد امنیتی صنعت داده‌ها (PCI DSS) در ارتباط با تنظیمات امنیتی مرتبط با رفع آسیب‌پذیری‌ها در زمینه کارت‌های پرداخت را نقض کنند. نایف می‌گوید: «PCI DSS از خودپردازها خواسته‌است که ویندوز ۷ یا ۱۰ پچ شده را استفاده‌کنند.»

نایف می‌گوید: «اما زمان می‌برد که سیستم یک بانک به‌روز شود. برای یک بانک بزرگ با ده‌ها هزار خودپرداز، پروژه بزرگی خواهدبود که تمام این سیستم‌ها به‌روزرسانی شوند به‌ویژه اگر بانک برای شعب مختلف، خودپردازهای متفاوت داشته‌باشد. اکثر حملاتی که من مشاهده‌کرده‌ام، نیازمند درجه‌ای از دسترسی فیزیکی هستند. تقریباً برای سارقان آسان است که یک فلش یو اس بی را به خودپرداز بزنند، اما سؤال اینجاست که آیا آنها می‌توانند این حمله‌های فیزیکی را به نتیجه برسانند؟ آن‌هم در شرایطی که نیاز باشد نیم‌ساعت وقت صرف‌شود که هر خودپردازی با بدافزار ویروسی شود و سپس شما مجبور شوید میول‌های (mules) پول را بپردازید تا پول به شما بپردازد؟ و بدانید چه زمانی دیگر ارزش آن را ندارد و اگر نتوانید به میزان لازم حمله‌ها را اندازه‌گیری کنید، متوقف شوید ؟»

نایف می‌گوید:«آسیب‌پذیری در نرم‌افزارهای شبکه وجود دارد و به مجرمان این اجازه را می‌دهد که از راه دور وارد شبکه‌های خودپرداز شوند. این حملات به مراتب پیچیده‌ترند و به مهارت بیشتری نیاز دارند.»

او می‌گوید: «هکرها نیاز دارند که از دروازه‌های تکنولوژیک فراوان عبور کنند تا بتوانند از راه دور وارد شبکه‌های خودپرداز شوند. این بدان معنا نیست که این اتفاق نمی‌تواند رخ بدهد، اما برخی مجرمان برایشان آسان‌تر است که تا از دستگاه‌های فیزیکی عبور کنند و به آن میزان پولی ؛

# بازتعریف امنیت در اینترنت سرویس‌ها

## (Internet of Services)

**درحالی‌که شرکت‌ها در حال کسب درآمد از اینترنت اشیا هستند، مدافعان امنیت و حریم شخصی با چالش‌هایی روبرو خواهندشد. دنی برادبری (Danny Bradbury) مشکلی در حال شکل‌گیری را بررسی می‌کند.**

مترجم: احمد شریف‌پور

**وینس وارینگتون:** «مهم این است که شما چگونه اشیا را به هم مرتبط کرده و سرویس‌های ارزش افزوده را روی آن سوار کنید.»

طیف وسیعی از ابزارها، از تلفن‌های هوشمند گرفته تا سیستم‌های اتوماسیون خانگی، نورهای هوشمند، پوشیدنی‌های مرتبط با سلامت و سنسورهای توکار خودروها، پلتفرمی باورنکردنی را ایجاد کرده‌اند که ما از آن به‌عنوان اینترنت اشیا (IoT) یاد می‌کنیم، اما این کهکشان عظیم ابزارهای متصل به هم، تنها قدم نخست در مسیر سفری طولانی است. قدم بعدی احتمالا ساخت سرویس‌هایی است که بر روی این بستر کار کنند. این لایه جدید که ما می‌توانیم آن را (IoS) بنامیم چالش‌های امنیتی خاص خودش را به همراه دارد.

وینس وارینگتون (Vince Warrington)، مدیر یک شرکت مشاوره امنیتی به نام «هوش محافظ» (Protective Intelligence) در بریتانیا است. او می‌پرسد: «چرا ممکن است یک تختخواب متصل به اینترنت داشته‌باشید؟» و می‌افزاید که اینترنت‌سرویس‌ها می‌تواند برای اتصال همه‌چیز به هم، کاربردهایی نیز خلق کند. به گفته او «مهم این است که شما چگونه اشیا را به هم گره زده و سرویس‌های ارزش افزوده را روی آن سوار کنید.» او به‌عنوان مثال می‌گوید یک تختخواب متصل به اینترنت ممکن است حرکت را حس کند و نورهای هوشمند می‌توانند گزارش دهند که چه زمانی روشن یا خاموش شده‌اند. یک سرویس آنلاین می‌تواند این داده‌ها را تحلیل کرده و تغییر وضعیت یا تغییر الگوی خواب یک فرد سالخورده را به خویشاوندانش گزارش دهد یا خودروهای متصل به هم می‌توانند با پارکومترها مرتبط شده و به‌صورت خودکار در حین نزدیک‌شدن به مقصد، مناسب‌ترین جای پارک را رزرو کنند. تلفن‌های هوشمند که آنها هم یکی از اجزای IoT هستند، پیش از این هم از اطلاعات موقعیت مکانی برای رزرو خودروهای اوبر استفاده‌می‌کرده‌اند که خود مثال دیگری از چنین سرویس‌هایی است.

**به گفته راب فان کرانبرگ، قدرت در دستان کسی خواهدبود که بتواند همه این شبکه‌ها و داده‌هایشان را به‌صورت یکپارچه و یک‌جا به هم متصل کند**

### تفکر دوباره درباره مدل محاسباتی

اندی مال‌هالند (Andy Mulholland)، نایب‌رئیس شرکت مشاوره فناوری Constellation Research که پیش‌تر هم مدیر ارشد فناوری شرکت Capgemini Group بوده‌است، می‌گوید که IoS می‌تواند از داده‌هایی که ابزارهای مختلف IoT جمع‌آوری می‌کنند استفاده کرده و نیازهای ما را به شیوه‌هایی غالبا مبهم، برآورده کند. او می‌گوید: «به جای داشتن چیزهایی براساس فرایندهای ثابت با خروجی‌های از پیش تعیین‌شده، ما چیزهایی بر اساس تعامل و احتمالات داریم و از آنها خروجی‌هایی خردمندانه دریافت می‌کنیم.»

چیزی که گفتیم در عمل به چه معناست؟ چنین چیزی ما را از دنیای ساده تعامل‌های دوسویه (مثلا یک خرید آنلاین ساده) که در آن کامپیوتر و اپراتور برای رسیدن به یک نتیجه قابل پیش‌بینی همکاری می‌کنند، فراتر خواهدبرد. به این ترتیب چنین تراکنش‌هایی بسیار کل‌نگر و پیچیده خواهندبود. به‌عنوان مثال


اوبر آرایه‌ای از نقاط داده (داده‌هایی از تلفن هوشمند مشتری مانند موقعیت مکانی به همراه امتیازات راننده و مسافر در سیستم را به کار می‌گیرد که از درون یک الگوریتم پیچیده عبور می‌کنند.

اسب تک‌شاخ IoS ، یعنی اوبر را در نظر بگیرید که شرکت‌های تاکسی‌رانی سنتی را در سرتاسر دنیای غرب تهدید می‌کند. تاکسی نشان‌دهنده مدل پیش از IoS است. مدلی که در آن مشتریان از طریق تلفن یا یک وب‌سایت درخواست تاکسی می‌دهند و توزیع‌کننده، نزدیک‌ترین ماشین را برای آنها ارسال می‌کند. این یک تراکنش ساده است که بر اساس یک روند کاملا تعریف‌شده صورت می‌پذیرد و احتمالا تنها دو نقطه داده ثابت دارد: مشتری و راننده تاکسی.

اما اوبر کلا به شکلی متفاوت کار می‌کند. با استفاده از آرایه‌ای از نقاط داده (داده‌هایی از تلفن هوشمند مشتری مانند موقعیت مکانی به همراه امتیازات راننده و مسافر در سیستم اوبر) که از درون یک الگوریتم پیچیده عبور می‌کنند اوبر به یک نتیجه مبهم می‌رسد. مال‌هالند می‌گوید: «بستگی به این دارد که کجا هستید، چه می‌خواهید، تاکسی که بهترین همخوانی را با نیازهای شما دارد کجا قرار گرفته‌است. البته داده‌های دیگری هم هستند؛ مثلا اینکه هوا چطور است یا میزان تقاضا برای تاکسی در آن لحظه چگونه است. آیا رویداد خاصی در جریان است؟ با در نظر گرفتن همه اینها یک خروجی به دست می‌آید که پیش‌بینی نشده است.»

این مکانیسم افسانه‌ای ممکن است به‌سادگی مشکل کاربر را حل کند یا بابت یک سواری ساده از آنها صدها دلار پول بگیرد. پیش‌بینی این که کدام حالت رخ می‌دهد مشکل است، چرا که برخلاف تراکنش‌های الکترونیکی معمول با نتایج قابل پیش‌بینی، این الگوریتم اختصاصی گنگ و مبهم همه‌کاره است و تمام آن مجموعه داده‌های پیچیده IoT خدمتکارانش هستند.

یکی از تاثیرات این نقاط داده اضافی و فرایندهای الگوریتمی این است که کل فرایند بسیار پیچیده‌تر شده و درنتیجه مدیریت آن بسیار دشوارتر می‌شود. مال‌هالند می‌گوید: «شیوه کار مدل‌های داده (که خود اساسی‌ترین چیزی است که مردم درک و دستکاری می‌کنند) نیز بسیار متفاوت خواهدبود»

خود مدل‌های داده هم در دنیای جدید IoS نسبت به دنیای قبلی بسیار متفاوت خواهندبود. این امر باعث دوری آنها از پایگاه‌داده‌های رابطه‌ای (Relational Database) سنتی با آن جداول و روابط قدیمی و ریشه‌دار و روی آوردن به پایگاه‌داده‌های گرافی و سایر نمونه‌های NoSQL خواهدشد که از اساس طراحی‌شده‌اند تا حجم عظیمی از داده‌ها را از منابع متعدد گردآوری و ذخیره کرده و روابط میان آنها را مستند کنند.

مال‌هالند می‌گوید: «این داده‌ها براساس زمینه و شرایط رویداد خلق می‌شوند». برای تأمین اطلاعات این ساختارهای داده جدید، دستگاه‌های متصل به IoT ازجمله تلفن‌های هوشمند به‌صورت مداوم با اطلاعات مرتبط با زمینه، موقعیت و محیط اطراف تحریک شده و داده‌هایی را ارسال می‌کنند. این داده‌ها طیف وسیعی از اطلاعات را (از موقعیت شما گرفته تا جابه‌جایی شما در داخل خانه) شامل می‌شوند. تمام اینها ردپایی را از حرکت و اقدامات افراد فراهم می‌کنند که مال‌هالند آن را «اگزوز دیجیتال» می‌نامد.

## یک اگزوز سمی

این خروجی یا اگزوز می‌تواند خلوت و حریم شخصی افراد را آلوده‌کند. سودها جامته (Sudha Jamthe) ، نویسنده کتاب «اینترنت اشیا و ازهم‌گسیختگی» است و در برنامه تحصیلات دنباله‌دار استنفورد هم مدل‌های تجاری IoT را تدریس‌می‌کند. او هشدار می‌دهد داده‌هایی که درباره افراد جامعه و از طریق تعامل روزانه آنها با IoS تولید می‌شود می‌تواند به حریم شخصی آسیب برساند، چرا که هیچ‌کس بر روی اینکه از این داده‌ها چگونه استفاده‌می‌شود تمرکز نکرده‌است. زمانی که سازنده ترموستات هوشمند خانه‌اش بخواهد با سازنده ساعت هوشمندش کار کند تا ورود و خروج هریک از افراد خانه را ببیند از دید او خط قرمزها شکسته‌شده‌اند.

او می‌گوید: «آنها می‌گویند که از این داده‌ها به هیچ منظور دیگری استفاده نمی‌کنند و تنها می‌خواهند بدانند که من چه زمانی از خانه خارج می‌شوم یا به آن وارد می‌شوم تا بتوانند تنظیمات دما را تغییر دهند، اما این از آن دست اطلاعاتی نیست که من بخواهم با کسی به اشتراک بگذارم.»

راب کرانبرگ (Rob Keranenberg) ، رئیس «جامعه ابرمتصل اینترنت اشیا» (IoT Hyper-Connected Socity) در «مجمع تحقیقات اروپایی اینترنت اشیا» (The European Research Cluster on Internet of things) است. به عقیده او شبکه‌های IoT و سرویس‌هایی که روی آنها سوار می‌شوند هنوز بسیار از هم منفصل و تکه‌تکه هستند. خود این امر می‌تواند مشکلات امنیتی به‌وجود آورد، چرا که سازندگان و توزیع‌کنندگان مختلف IoS از لحاظ امنیت و حریم شخصی در سطوح متفاوتی قرار دارند.

او می‌گوید: «همه محصولات آنها هم‌اکنون هم یک پل ارتباطی از یک شبکه به شبکه دیگری هستند. قدرت در دستان کسی خواهدبود که بتواند همه

یکی از تاثیرات این نقاط داده اضافی و فرایندهای الگوریتمی این است که کل فرایند بسیار پیچیده‌تر شده و درنتیجه مدیریت آن بسیار دشوارتر می‌شود

این شبکه‌ها و داده‌هایشان را به‌صورت یکپارچه و یک‌جا به هم متصل کند. داستان درباره دسترسی به مجموعه‌های عظیمی از داده‌هاست که می‌توانید آنها را در قالب خدمات و سرویس‌های جدید با هم ترکیب کنید.»

ما همین حالا هم شاهد نمونه‌های ترسناکی از نقض حریم خصوصی هستیم و این درست زمانی اتفاق می‌افتد که شرکت‌های IoS داده‌های کافی برای خودشان جمع کرده‌اند. اوبر اخیرا باعث بروز حساسیت‌هایی شده‌است، چرا که برنامه‌هایی برای ردگیری موقعیت کاربران (حتی زمانی که از اپ اوبر استفاده‌نمی‌کنند) دارد و با نمایش پیشنهادهای ویژه در فهرست مخاطبان تلفن‌های کاربران، برایشان مزاحمت فراوانی ایجاد کرده‌است. این شرکت، محل اقامت شبانه مسافرانش را با جمع‌آوری اطلاعات سفر آنها ردگیری کرد و آنها را در قالب یک پست وبلاگی منتشر ساخت! عوامل اجرایی این شرکت مسافرت‌های خبرنگاران را نیز ردگیری کردند و آن را به‌عنوان ابزار فخرفروشی و حربه تبلیغاتی به‌کار گرفتند. اگر تنها یک شرکت با چنین خودنمایی، حریم خصوصی افراد را نقض می‌کند هکرها با چنین داده‌هایی چکار خواهندکرد؟

## برخی راه‌حل‌ها

البته راه‌حل‌هایی هم برای این مشکلات امنیتی و حریم خصوصی تهدیدکننده IoS وجود دارد. این راه‌حل‌ها هم سیاسی و هم فناورانه هستند. سیاستمداران محلی می‌توانند قوانین مربوط به «استفاده از داده» خودشان را اعمال کنند، درست به همان شکلی که در آیین‌نامه محافظت از داده‌های عمومی اروپا General Data Protection Regulation)) GDPR دیده‌می‌شود. این آیین‌نامه از ماه می سال ۲۰۱۸ اجرایی خواهدشد. به‌عنوان نمونه‌ای اختصاصی‌تر درباره دستگاه‌های متصل که سازنده IoS هستند، می‌توانیم به ابلاغیه کمیسیون اروپا درباره استانداردهای ICT اشاره کنیم که از اعضای این اتحادیه می‌خواهد استانداردهایی را برای حمایت از ارتباطات امن و قابل‌اعتماد میان اشیا، دستگاه‌های دیجیتال و افراد، توسعه دهند و اعمال کنند.

جامته می‌گوید: «به نظر می‌رسد اتحادیه اروپا سیاست‌های بهتری وضع کرده‌است که به ما می‌گوید از داده‌ها چگونه استفاده خواهدشد. در آمریکا قضیه اصلا به این شفافیت نیست. اینجا شرکت‌های سازنده اصلا نمی‌خواهند در این مورد صحبت کنند و به این ترتیب کاربران را عصبی کرده و می‌ترسانند.»

با دانستن این نکته که بیشتر افراد از سرویس‌های مبتنی‌بر IoT تحت مالکیت شرکت‌های آمریکایی استفاده‌می‌کنند ، راب فان کراننبرگ توصیه می‌کند که ما برای شیوه و امکان استفاده از داده‌هایمان در IoT و سرویس‌های وابسته به آن، سیاست‌های شخصی وضع کنیم. او روی محصولی به نام Dowse Privacy Hub کار می‌کند که یک پروژه سخت‌افزاری منبع‌باز است و افراد را قادر می‌سازد داده‌هایی را که از شبکه‌های شخصی و خصوصی‌شان ارسال می‌شود، کنترل کنند. به این پروژه به دید یک روتر مخصوص حریم شخصی نگاه کنید. او می‌گوید: «ما می‌خواهیم این کار را انجام دهیم، چرا که فکر می‌کنیم اوضاع دارد از کنترل خارج می‌شود.»

## کوه دیگری از مشکلات

اما مشکلات امنیتی IoS تنها در لایه مربوط به IoT باقی نمی‌مانند. مشکلات امنیتی در سایر لایه‌ها نیز می‌تواند کل سرویس را آسیب‌پذیر کند. سانجای خاتری (Sanjay Khatri)، مدیر بازاریابی سرویس‌های IoT در شرکت جاسپر (Jasper)، است که در مارس ۲۰۱۶ توسط سیسکو خریداری شد. او توضیح‌می‌دهد که این لایه‌ها شامل سخت‌افزار دستگاه‌هایی که داده‌ها را جمع‌آوری می‌کنند و شبکه‌هایی که امکان ارسال این داده‌ها را فراهم می‌کنند نیز می‌شود. جاسپر یک پلتفرم برای اکوسیستم IoT است که به شرکت‌های IoS کمک می‌کند دستگاه‌هایشان را مدیریت کرده و با استفاده از سرویس‌های ارزش افزوده از طریق آنها به پول برسند.

سازندگان ابزارها و دستگاه‌ها ممکن است مرتکب اشتباهات اساسی شوند، مثلا از کدهای امضا نشده استفاده‌کنند یا دستگاه‌ها را آن‌قدر کم‌مصرف بسازند که قادر به پشتیبانی از رمزنگاری نباشند. رابط‌های کاربری با تنظیمات اشتباه می‌توانند به از دست رفتن کنترل در ابر منجر شود.

خاتری می‌گوید: «شما به راه‌هایی برای کاهش خطرات بزرگ مقیاس دستگاه‌های متصل نیاز دارید» و می‌افزاید که جاسپر سرویس‌هایی نظیر اعتبارسنجی دستگاه‌ها و تشخیص رفتار غیرنرمال در گروه‌های بزرگ این ابزارهای متصل را عرضه می‌کند. شرکایی که در اکوسیستم جاسپر حضور دارند اداره اموری نظیر رمزنگاری داده‌ها و امن‌سازی لایه انتقال داده‌ها را برعهده می‌گیرند.

خاتری توضیح می‌دهد شرکایی که برای ارتباط با جاسپر به جای شبکه‌های وای‌فای عمومی از اتصالات موبایل مبتنی‌بر سیم‌کارت روی دستگاه‌های‌شان استفاده‌می‌کنند به‌صورت طبیعی لایه

انتقال داده‌های IoT را که همه سرویس‌ها روی آن قرار دارند، تقویت می‌کنند.

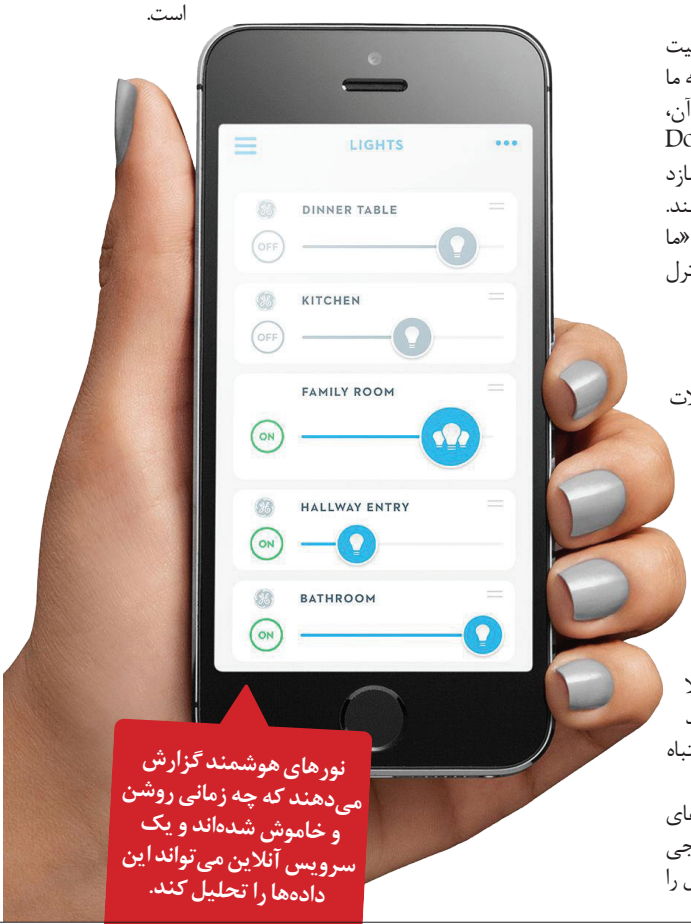
## مشکلات فرهنگی

متخصصان هشدار می‌دهند گرچه ممکن است سرویس‌هایی وجود داشته‌باشند که به افزایش امنیت و حریم خصوصی در IoS کمک‌کنند، اما درنهایت چیزی که ما به آن احتیاج داریم یک تحول فرهنگی است. خبره‌های سنتی امنیت IT غالبا با فرایندهایی خطی سروکار دارند که به‌خوبی درک شده و بر ورودی‌های کاملا مشخصی استوار است. مال هالند معتقد است که IoS پر تنوع با آن پیوندهای ضعیفش و با مجموعه داده‌های پیچیده و الگوریتم‌های غیرقطعی که روی آنها اجرا می‌شود، بسیار فراتر از مشکلاتی هستند که این متخصصان عادت به حل‌کردن آن داشته‌اند. او می‌گوید: «اگر فکر می‌کنید با یک پیشامد شروع می‌شود و بعد به‌صورتی غیرمنتظره به یک خروجی مبدل می‌شود، فقط روبرو شدن با آن را تصور کنید»

در مورد کسانی که مجبورند در محیط سازمانی با IoS تعامل داشته‌باشند هم همین قضیه صادق است. آنها هم ممکن است به برنامه‌نویسی یک SCADA به‌صورت توکار عادت داشته‌باشند که تنها با ابزارهای مخصوصی آن‌هم در یک شبکه بسته ارتباط برقرار می‌کند.

خاتری می‌گوید: «ناگهان همه آنها مجبور می‌شوند که همه‌چیز را برای برقراری ارتباط باز کنند.» و این فقط شامل کارکنان شرکت نمی‌شود بلکه شرکای طرف سوم را نیز دربرمی‌گیرد. او می‌افزاید: «این کار از زیر دست بسیاری از آنها می‌گذرد و من فکر نمی‌کنم که حتی روش‌های استاندارد IT هم واقعا به درون برخی از این حوزه‌ها سرک کشیده‌باشد.»

چالش‌های امنیتی و حریم خصوصی پیش روی شرکت‌های IoS و کاربران‌شان بسیار گسترده و بغرنج هستند. شرکت‌ها تازه در حال فهمیدن این موضوع هستند که مدل‌های تجاری IoS چگونه کار خواهندکرد و فناوری را برای حمایت از آن است.




نورهای هوشمند گزارش می‌دهند که چه زمانی روشن و خاموش شده‌اند و یک سرویس آنلاین می‌تواند این داده‌ها را تحلیل کند.

# روان‌شناسی سایبری

## کلید امن‌سازی عنصر انسانی در سازمان‌ها

مترجم:
احمد شریف پور



سیاران مک‌ماهون (Ciaran McMahon) مفهوم روان‌شناسی سایبری را بررسی می‌کند تا ببینیم چه معنایی دارد و چگونه می‌تواند به شیوه کارآمدی در کسب‌وکار مورد استفاده قرار بگیرد.

کوین میتنیک در سال ۲۰۰۲ گفت که ضعیف‌ترین حلقه در زنجیره امنیت اطلاعات عنصر انسانی است و از آن پس ما این حرف را به کرات شنیده‌ایم. آمارهای موجود در زمینه رفتار، سیاست‌ها و هوشیاری مردم نسبت به جرایم سایبری، تکان‌دهنده است. براساس مطالعات کنترل سلامتی داده‌ای که Databarrack در سال ۲۰۱۵ و در میان حرفه‌ای‌های حوزه IT انگلستان انجام شده‌است، ۲۴ درصد مطالعه‌شوندگان اظهار کرده‌اند که در سازمان‌شان اشتباهات انسانی یکی از عوامل از دست رفتن داده‌ها در سال پیش از آن بوده‌است. در همین حال گزارش Protiviti از امنیت IT و حریم خصوصی در سال ۲۰۱۵ نشان می‌دهد که ۳۳ درصد شرکت‌های فعال در آمریکای شمالی هیچ سیاستی برای امنیت اطلاعات ندارند.

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 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 مشابهی 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 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 بواسطه 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 کم‌کم 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. در نتیجه وقتی کارمندی وارد یک سیستم کامپیوتری سازمانی می‌شود تا زمانی که کسی با او تعاملی انجام نداده‌است خود را نامرئی تصور می‌کند. این زمانی است که تهدیدات داخلی ظاهر می‌شوند،

روان‌شناسی به تنوع وسیع رفتارهای آدمی توجه دارد و درنتیجه روان‌شناسی سایبری توجه به همین موضوع در حوزه فناوری اطلاعات است

چرا که این کارمندان هیچ‌گاه فکر نمی‌کنند که ممکن است کسی در حال تماشای فعالیت‌های‌شان باشد، اما برای یک مدیر امنیت اطلاعات سؤال اصلی این است که شبکه داخلی شرکتش تا چه حد قابل رویت است. امنیت سایبری مستلزم مدیریت چیزهایی است که ما نامرئی فرض می‌کنیم.

سوم اینکه در فلسفه سنتی اینترنت همه با هم برابر هستند و هیچ کنترل مرکزی وجود ندارد. این موضوع را «کاهش مقام» یا Minimization of status می‌نامیم. تقریباً غیرممکن است که بتوانیم افرادی را که در اینترنت هستند به اجبار به کاری وادار کنیم. در ساده‌ترین حالت، آنها فقط برای سرگرمی خالص هم که شده مقاومت می‌کنند.

یک نمونه بارز این رفتار این است که هیچ کمپین تبلیغاتی و روابط عمومی که بر مبنای هشتگ‌ها طراحی شده‌باشد، بدون سرقت شدن (به این معنی که هشتگ موردنظر دقیقاً برخلاف ایده‌های کمپین مورد استفاده قرار بگیرند) پیش نرفته‌است. نتیجه نهایی این حرف این است که تلاش برای پیاده‌سازی نظم و قانون در حوزه فناوری اطلاعات کاری دشوار است. امنیت سایبری مستلزم کنترل چیزهایی است که از اساس برای مقاومت در برابر حاکمیت طراحی شده‌اند.

## مزیت‌های روان‌شناسی سایبری در محیط کسب‌وکارهای امروزی چیست و چرا به آن احتیاج داریم؟

برای این مشکلات راه‌حلی وجود دارد. یک فرآیند مدیریت امنیت اطلاعات مبتنی بر روان‌شناسی سایبری، توقعات زیادی در زمینه کنترل عنصر انسانی سازمان دارد. این توقعات چه هستند؟ این توقعات حداقل به مصالحه در سه مورد احتیاج دارد: ترغیب احساسی: ما به تسخیر قلب‌ها و ذهن‌های بیشتر و ترس کمتر و همدلی نیاز داریم. این کار مستلزم آموزش معمول، متنوع و دائمی است. افراد برخلاف ماشین‌ها به‌ندرت براساس اطلاعات منطقی تغییر رفتار می‌دهند. آنها به روابط عمومی و پروپاگاندا احتیاج دارند. گروه امنیت سایبری باید با منابع انسانی سازمان و کارکنان تیم‌های عملیاتی دوست شوند.

رهبری توزیع‌شده: به تیم‌ها اجازه دهید که سیاست‌های خاص خودشان را توسعه دهند. اینکه شما نمی‌توانید یک کنترل متمرکز داشته‌باشید به این معنی نیست که نمی‌توانید هیچ کنترلی داشته‌باشید. تصمیم‌گیری در زمینه امنیت اطلاعات را به رده‌های پایین‌تر و بیرونی‌تر محول کنید تا ماژول‌های مقاوم مجزا از هم داشته‌باشید.

شهروند شبکه شدن: مدیران امنیت اطلاعات می‌خواهند تمام شبکه داخلی سازمان را ببینند، اما در عمل این کار غیرممکن است، پس از اعضای شبکه برای این کار کمک بگیرید. افراد علاوه‌بر اینکه باید درگیر امنیت سایبری شده‌باشند، باید مکانیزم‌های سرراست گزارش‌دهی را هم در اختیار داشته‌باشند.

## چالش‌های احتمالی همه‌گیر شدن این موضوع میان شرکت‌ها چیست؟ آیا هیچ صنعتی وجود دارد که به روان‌شناسی سایبری نیازمندتر باشد یا راحت‌تر با آن تطبیق پیدا کند؟

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

به ناگزیر همه‌گیر شدن سیاست‌های امنیت سایبری مبتنی‌بر روان‌شناسی سایبری، چالش‌هایی را با خود به همراه خواهدداشت. مدل رفع تکلیفی آگاهی‌دهی (کلاس آموزشی نصف روز، یک روز از سال برای کل کارکنان) در لیست بسیاری از مدیران باعث تیک‌خوردن گزینه امنیت سایبری می‌شود. همان‌طور که می‌دانید چنین مدلی، تأثیر چندانی بر فرهنگ محیط کار نخواهدداشت. مهم نیست آن کلاس نصف روز چقدر خوب برگزار شود به محض این که یکی از کارکنان رده‌بالای شرکت 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 می‌بینند و انجام می‌دهند و به‌تدریج به یک روند معمول تبدیل می‌شود.

**اگر سیستم ارتباطات سازمان شما مشکل داشته‌باشد، سیاست امنیت اطلاعات شما آن را منعکس کرده و بنابراین به‌درستی کار نمی‌کند**

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

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

درنتیجه اگر سیستم ارتباطات سازمان شما مشکل داشته‌باشد، سیاست امنیت اطلاعات شما آن را منعکس کرده و بنابراین به‌درستی کار نمی‌کند.

مهم است که به رده‌های بالای شرکت تاکید کنید که اگر سیاست امنیت اطلاعات‌شان ضعیف است، این موضوع نشان‌دهنده ضعف ساختار سازمان شماست.

## نفع مستقیم پیاده‌سازی یک سیاست امنیت اطلاعات مبتنی بر روان‌شناسی سایبری چیست و این منفعت چگونه در میان بخش‌های مختلف سازمان تقسیم می‌شود؟

در گزارش Europol IOCTA پارسال هم از «عنصر انسانی» امنیت اطلاعات نام برده شده است. آن‌جا از این عنصر به عنوان محیطی برای جرائم سایبری یاد شده است که مدام تهاجمی‌تر می‌شود. تنها راه پیش رو در چنین محیطی همکاری و همراهی بیشتر بصورت افقی میان بخش‌های مختلف کسب‌وکار و به صورت عمودی میان رده‌های مختلف یک سازمان است.

کسب‌وکارهایی که بتوانند هدف‌های سازمانی‌شان را با سیاست‌های امنیت اطلاعات هم‌راستا کنند برای گذر از دهه آینده شانس بیشتری خواهند داشت. صنایعی که چنین کاری با موفقیت بالاتری اتفاق خواهدافتاد قاعدتاً شامل کسب‌وکارهای مبتنی‌بر فناوری، مخابرات، سازمان‌های مالی و اعتباری و رسانه‌ها خواهدبود. البته همان‌طور که پیش‌تر توضیح دادم، هر سازمانی که به تفکر صحیح و درست بپردازد، ارزش تدوین یک سیاست امنیت اطلاعات سایبری را درک خواه کرد.

به لطف تعداد زیاد نشت‌های اطلاعاتی گسترده، عبارت «ما امنیت را بسیار جدی گرفته‌ایم» به یکی از بی‌معنی‌ترین کلیشه‌های سال ۲۰۱۵ تبدیل شد. کار دیگر به این شکل پیش نخواهدرفت. به‌زودی عموم مردم و نمایندگان‌شان خواهان یکپارچگی و امنیت اطلاعات بیشتر و بهتر خواهند شد.

در فرآیند کار روزمره، امنیت به چه معنی است؟ سازمان‌هایی که بتوانند اهمیت امنیت اطلاعات را در میان کارکنان‌شان نهادینه کنند، شرکت‌هایی که برای آموزش امنیت سایبری قدم‌های جدی برداشته‌اند در آینده پیش رو برتری چشم‌گیری خواهند داشت، چرا که جرایم سایبری وضوح سودآور و پول‌ساز هستند.

یک تجربه رو در رو بسیار بهتر از این است که امیدوار باشیم یک گروه پیام ما را دریافت کرده‌اند.

# آیا برنامه
# «پاداش در ازای کشف باگ‌ها»
# باید قانونی شود؟

**با وجود هکرهای بلک‌هت که قادر هستند گوگل و اپل را آسیب‌پذیر کنند، «دوی ویندر» به‌دنبال کشف این موضوع است که آیا مدل پاداش در ازای کشف باگ‌ها (باگ بانتی) اساساً در مقابل باگ‌ها آسیب‌پذیر شده‌است؟**

**اپل اخیراً به زمره شرکت‌هایی پیوسته‌است که برنامه پاداش به یافتن آسیب‌ها را دنبال‌می‌کنند که این برنامه با اسم طرح باگ بانتی بهتر شناخته‌می‌شود. این پروژه که در ابتدا برای ده‌ها محقق شناخته‌شده نزد اپل محدود شده‌بود به‌ازای یافتن هر اشکال امنیتی اساسی رقمی برابر با ۲۰۰ هزار دلار پرداخت می‌کند. این رقم تا زمانی که شما پی می‌برید که یک شرکت خصوصی کوچک به نام Exodus Intelligence به‌ازای هر اشکال یافت‌شده امنیتی ناشناخته در iOS مبلغ ۵۰۰ هزار دلار پیشنهاد می‌دهد، زیاد به نظر می‌رسد. درحالی‌که Exodus می‌گوید مشتریانش که حق اشتراکی معادل حداقل ۲۰۰ هزار دلار به‌ازای هر سال برای دسترسی به intel به‌منظور کشف این آسیب‌پذیری می‌پردازند، بیشتر در فاز تدافعی‌اند تا تهاجمی. صنعت امنیت نیاز دارد که بداند که آیا این برنامه‌های باگ بانتی یک مفهوم نقض‌شده‌اند که نیاز به قانون‌گذاری دارد یا خیر.**

## پول کجاست؟

اپل، تنها شرکتی نیست که به شکارچیان باگ‌ها و کاشفان آسیب‌پذیری‌ها پول می‌پردازد، اگرچه که حداکثر پرداختش بالاترین پولی است که در صنعت برای یافتن باگ‌ها پرداخت‌می‌شود. هرچند روزهایی که محققان، یاهو را به تمسخر می‌گرفتند سپری شده‌است، اما هنوز سؤال این است که باونتی‌ها چه هستند؟ و چگونه بین شرکت‌های بزرگ و شرکت‌های کوچک تمایز قائل می‌شوند؟

وزارت جنگ آمریکا یک برنامه آزمایشی را به نام «پنتاگون را هک کنید» از طریق HackerOne آغاز کرد و ۷۰ هزار دلار برای باونتی‌ها به ۵۸ محقق برای ۱۳۴ مشکل امنیتی پرداخت کرد و اولین مشکل امنیتی ظرف ۱۵ دقیقه یافت‌شد. فیس‌بوک یک برنامه باونتی را در سال ۲۰۱۱ آغاز کرد و ۴.۳ میلیون دلار را به ۸۰۰ باونتی در ۱۲۷ کشور پرداخت کرد که یک‌میلیون دلار از این مبلغ تنها در سال ۲۰۱۵ پرداخت شد. حداکثر پولی که مایکروسافت برای کشف اشکالات امنیتی می‌پردازد ۱۰۰ هزار دلار است درحالی‌که Uber تنها ۱۰ هزار دلار پرداخت‌می‌کند. یک سایت دارای محتوای غیراخلاقی پرمخاطب با پرداخت مبلغ ۲۵ هزار دلار حداکثر در وسط لیست قرار می‌گیرد و خود HackerOne ۱۰ هزار دلار برای باگ‌های حاد یافت‌شده پرداخت‌می‌کند.

آن‌گونه که «کن مونرو» به‌عنوان یکی از شرکای پیامد اخلاقی هک Pen Test Partners اعلام کرده‌است «جزییات برنامه‌های کشف باگ بدون معطلی بر روی سایت‌هایی مانند HackerOne و BugCrowd در دسترس گذاشته‌می‌شوند و گوگل از زمان شروع برنامه کشف باگش در سال ۲۰۱۰ بیش از ۶ میلیون دلار به محققان امنیتی پرداخته‌است. به جای خرسندی از جوایز پیشین و تکیه برآنها، گوگل اخیراً جوایز مرتبط با Chromebook را دوبرابر کرده‌است و مبلغ را از ۵۰ هزار دلار به ۱۰۰ هزار دلار رسانده‌است.

نکته این است که شرکت‌های پیشنهاددهنده جوایز کشف باگ به‌طورکلی این جایزه را برمبنای اندازه کسب‌وکارشان انجام‌می‌دهند، بنابراین شرکت‌های کوچک‌تر سقف پرداخت پایین‌تری خواهند داشت.

متاسفانه کارگزاران و واسطه‌ها که خدمات خود را به بالاترین قیمت در مناقصه‌ها انجام‌می‌دهند، دستمزدی بالاتر از آن چیزی می‌خواهند که حتی شرکت‌های بزرگ قادر به پرداخت آن هستند به‌ویژه اگر آن باگ از یک سیستم آسیب‌پذیری بالا (CVSS) برخوردار باشد.

(CVSS) استانداردی است که به رتبه‌بندی شدت آسیب‌پذیری امنیتی دست‌می‌زند و فرمولی را به‌وجود آورده‌است که در آن معیارهایی چون بازده نهایی و اثر تخریبی باگ در آن مؤثرند. نیل کوک، معمار ارشد امنیت Open-Xchange، می‌گوید: «باگ‌هایی که رتبه بالایی در CVSS داشته‌باشند و بر شمار بالایی از دستگاه‌ها تأثیر بگذارند و یا موارد استفاده مشخص برای حاکمیت‌های ملی داشته‌باشند معمولاً از ۱۰۰ هزار دلار شروع می‌شوند و می‌توانند با ارقامی چندین‌برابر نرخ پایه به فروش برسند». اگرچه این انواع آسیب‌پذیری‌ها بسیار کمیاب هستند. کوک می‌افزاید: «افرادی که تنها بر روی قسمت تاریک مسئله کارمی‌کنند ممکن است وقت بسیاری را برای یافتن یک باگ صرف‌کنند و این زحمت و مشکلی است که مردم آن را نمی‌بینند».

کوک می‌گوید: «ما یافته‌های بسیار کمی داشته‌ایم که به‌وسیله محققان به‌دست آمده‌اند که به یک اشکال اساسی منتج شده‌اند و در خطوط تولید ما وجود داشته‌اند. اگر بی‌توجه به این آسیب‌پذیری‌ها باشیم به‌طور بالقوه می‌تواند یک APT داشته‌باشد که اگر مورد بررسی مجدد قرار نگیرند، پیامدهای ناخواسته بد خواهند داشت. ROI از بودجه مورد نیاز برای اجرای این برنامه بسیار بالاتر رفت، بنابراین مشخص است که به‌صرفه نباشد.»

همچنین گاوین میلارد، مدیر فنی EMEA ، می‌گوید: «با انگیزه دادن به محققان و توسعه‌دهندگان از طریق برنامه‌های کشف باگ، مسائل بیشتری می‌توانند کشف شوند و با آنها برخورد صورت بگیرد که میزان حمله را پایین بیاورند». همه بر این باور نیستند که برنامه کشف باگ تأثیر مثبتی بر افشاسازی آسیب‌پذیری فعال دارد.

آمیچای شولمان، مدیر ارشد فناوری شرکت امپروا، می‌گوید: «این رویه باعث‌می‌شود که پایین‌ترین قیمت ممکن از دسترس خارج‌شود و باعث می‌شود که فروش با رقم بالاتر این آسیب‌پذیری‌ها به دیگر افراد و گروه‌هایی که قیمت‌های بالاتری می‌پردازند شکل قانونی به خودش بگیرد.»

توماس ریچاردز، مشاور ارشد Cigital درحالی‌که معتقد است مفهوم هنوز وجود دارد بر این باور است که دلالان امنیت باگ (zero-day brokers) قبل از برنامه‌های فعلی در برنامه‌هایی که قبلاً به‌وسیله شرکت‌ها ارائه می‌شدند وجود داشته‌اند و بر همین مبنا «نبردی طولانی برای رقابت در مقابل بازار واسطه‌های امنیت باگ دارند».

البته اینکه آیا واسطه‌ها در نفس خود یک موضوع منفی هستند بستگی به تعریف یک واسطه در مرحله اول دارد. فقط به این خاطر که یک نفر به‌عنوان واسطه بین شرکت کامپیوتری و محققان امنیت قرار می‌گیرد، قرار گرفتن در یک طرف معامله، وجهه یک نفر را بد نمی‌کند. در واقع می‌تواند برعکس باشد و به دو طرف معامله اطمینان می‌دهد که دو طرف معامله به حق خود می‌رسند و یک سؤال دیگر را پیش می‌کشد که آیا صنعت کشف باگ نیاز به یک سازمان‌دهنده رسمی دارد یا خیر.

## مسائل قانون‌گذاری

نیل کوک به شرکت‌هایی مثل HackerOne به‌عنوان مجرایی بین محققان و شرکت‌ها می‌نگرد که خود شکل یک نوع مقررات داوطلبانه دارد تا اینکه اجباری باشد. «به‌عنوان بخشی از قوانین طرح، شرکت‌ها به انتشار مسائل امنیتی مورد درخواست‌شان از طریق فرایند مسئولیت افشاسازی می‌پردازند که خود سیستمی شفاف و باز است». شرکت‌های مجزا نرخ‌های کشف باگ را تعریف و تعیین می‌کنند و به تعریف و تحدید HackerOne نمی‌پردازند و محققان قبل از اینکه قرارداد ببندند از قوانین آگاهی کامل دارند.

آنچه شما احتیاج دارید احتمالاً این است که روش افشاسازی اطلاعات در یک کشور تغییر دهید. در ایالات متحده که افشاسازی بر داده‌های مشتریان تاثیرگذار است در ۴۷ ایالت از ۵۰ ایالت تغییر روش افشای اطلاعات اجباری است و انگیزه زیادی برای پنهان‌سازی اطلاعات وجود ندارد. مونرئو بر این باور است که «فعالیت‌های افشاگرانه خود تغذیه‌کننده برنامه‌های کشف باگ است و این خود دلیلی بر این قضیه است که چرا بسیاری شرکت‌های آمریکایی این فعالیت‌ها را انجام می‌دهند.»

«با پرورش یک فرهنگ آزادتر در بریتانیا که شاید روزی نسخه پسابرگزیت آن نیز در سال ۲۰۱۸ تدوین شود، شاهد خواهیم‌بود که برنامه‌های ضد باگ مقبولیت بیشتری به‌عنوان یک پیامد خواهد داشت و اینکه خواهیم دید که آیا احکام بیشتری نیز درباره آن صادر خواهدشد.»

**همه بر این باور نیستند که برنامه کشف باگ تأثیر مثبتی بر افشاسازی آسیب‌پذیری فعال دارد**

# چگونگی تحقق استانداردهای استراتژی ملی امنیت سایبری بریتانیا

نویسنده: وندی ام. گراسمن
مترجم: مسلم مسلمی‌زاده

**استراتژی امنیت سایبری بریتانیا از نوامبر سال ۲۰۱۶ معرفی شد و مورد استقبال قرار گرفته‌است، اما باید ببینیم آیا می‌تواند با معیارهای فراوانی هماهنگ شود که تهدیدات امنیتی را موجب می‌شود.**

دولت مثل همه یک تیتر را می‌خواند: رخنه در TalkTalk، تلاش برای سرقت ۹۸۱ میلیون دلاری از سیستم سوییفت بانک بنگلادش و رخنه در شبکه برق اوکراین، آسیب‌پذیری‌های موجود در قلب سیستم را نشان داد. به‌علاوه، حملات اخیر Mirai botnet که دوربین‌های مداربسته، روترها، مانیتورهای کوچک و دیگر دستگاه‌هایی را که به‌وسیله حمله‌کنندگان قابل تهدید هستند تحت کنترل درآورد مشخص ساخت که حتی کاربران تحصیلکرده‌ای که دستگاه‌هایشان را از نمایندگی‌های معتبر تهیه‌می‌کنند، همیشه قادر به حفاظت از خود نیستند.

استراتژی امنیت سایبری اعلام‌شده به‌وسیله فیلیپ هاموند، صدراعظم بریتانیا در آغاز نوامبر، بیانگر برخی از این مسائل است. بخشی از آن که مشخص‌ترین‌شان توافق هزینه ۱،۹ میلیارد پوند در طی پنج‌سال آینده برای بهبود امنیت سایبری کشور بود به‌طورکلی مورد استقبال قرار گرفته‌است. موضوع مهم‌تر این است که جزییات استراتژی اجرا خواهدشد و به‌ویژه موفقیت آن اندازه‌گیری خواهدشد.

## ریشه‌های استراتژی

پیتر سامر، یک استاد مدعو در دانشگاه مونت فورت و یک استاد پاره‌وقت Digital Forensics در دانشگاه بیرمنگام، می‌گوید که مقدمات استراتژی جدید در سال ۲۰۱۱-۲۰۱۰ به‌وسیله دفتر بیمه و امنیت سایبری (OSCIA) پایه‌ریزی شد. OSCIA در دفتر کابینه بنا شد و خودش از اعقاب پشتیبان مرکزی بیمه اطلاعات (CSIA) بود.

NCSC تازه ایجاد شده‌است و شامل شماری از اجزای قبلی دولت می‌شود: زیرساخت ملی، CPNI (یک محصول مشترک از MI۵، GCHQ، باقی‌مانده OSCIA و بخش حفاظتی GCHQ بود. کیاران مارتین، مدیر جدید NCSC و عضو قبلی هیئت رئیسه GCHQ بوده‌است.

به‌عنوان یکی از نتایج آن اجرای قبلی، «سامر» بر این باور است که NCSC برای به‌دست‌آوردن اعتماد تلاش خواهد کرد: «بدون شک مهارت‌های فراوانی وجود دارد اما این واقعیت هست که GCHQ یک آژانس امنیتی است که باید تا حدی مخفیانه عمل کند». طبق نظر او «هیچ‌یک از فعالیت‌های این بدنه به یک استراتژی تمام و کمال نمی‌انجامد». به یک دلیل، بسیاری از بخش‌های زیرساختی خطیر ملی انگلستان، خارج از کنترل دولت قرار دارند، چرا که مالکیت آنها در دست شرکت‌های خصوصی است که بسیاری از آنها در خارج کشور وجود دارند. حتی بسیاری از فرایندهای دولتی به این چنین شرکت‌هایی برون‌سپاری شده‌است. طبق نظر سامر «درنتیجه، این استراتژی به جای آنکه الزام‌آور باشد بسیار اقناع‌کننده است.»

## اندازه‌گیری هدف

مشکل بزرگ‌ترِ «برین شورتن» رئیس انجمن امنیت خیریه، نبودن راهی برای اندازه‌گیری موفقیت است. سؤال او این است: «شما بهتر را چگونه تعریف می‌کنید»؟ «اگر ما یک حمله امنیتی معروف نداشته‌باشیم به این دلیل است که حمله‌ای صورت نگرفته‌است و آیا به این خاطر نیست که دولت وارد عمل شده‌است و بریتانیا را یک محیط دشوار برای حمله سایبری تبدیل کرده‌است؟ ما دقیقاً نمی‌دانیم. بر روی گزارش‌هایی که دولت و پلیس امنیتی می‌تواند از موفقیت آنها منتشر کند محدودیت‌هایی نهاده شده‌است.»

در عوض او می‌گوید که به‌دنبال هدفی است تا بتواند اندازه‌گیری کند. در مورد کاهش شمار حملات DDoS یا هک‌های موفق و افزایش آگاهی در بین جمعیت هنوز مشکلاتی وجود دارد. اگر شمار حملات DDoS کاهش پیدا کند، آیا کاری که ما می‌کنیم صحت دارد و یا اینکه حمله‌کنندگان به تکنیک‌های جدید دست یافته‌اند؟ به‌علاوه آیا ما داریم تمام حملات DDoS را با هدف بریتانیا می‌شماریم یا فقط آنهایی که در اینجا آغاز می‌شوند؟ بنابراین وقتی استراتژی می‌گوید «چشم‌انداز ما برای ۲۰۲۱ این است که بریتانیا، امن و در مقابل تهدیدات سایبری مقاوم و در دنیای دیجیتال موفق و باصلابت باشد (بخش ۱،۴)»، این جملات چه معنایی خواهد داشت؟ ما چگونه آن را اندازه بگیریم؟

**چشم‌انداز ما برای ۲۰۲۱ این است که بریتانیا، امن و در مقابل تهدیدات سایبری مقاوم و در دنیای دیجیتال موفق و باصلابت باشد**

## یک استراتژی بدون استراتژی

مارتین تامس، یک مهندس نرم‌افزار و مشاور مستقل، می‌گوید: «بزرگ‌ترین مشکل با NCSS این است که یک استراتژی نیست. هیچ چشم‌اندازی از این موضوع وجود ندارد که یک نرم‌افزار باید چه مشخصاتی داشته‌باشد که ما بتوانیم بدانیم که سیستم‌های مبتنی‌بر نرم‌افزار به اندازه کافی امن هستند. بدون یک هدف موثق و فنی، NCSS قادر نخواهدبود تا نقشه یک مسیر مطمئن را برای یک آینده امن سایبری طراحی کند».

تامس بر این باور است که نبود یک هدف نهایی در استراتژی به این معناست که استراتژی برخی امکانات واقعی را نادیده می‌گیرد. از یک سو، معرفی یک قانون الزام‌آور برای امنیت و امنیت در نرم‌افزار باعث بیداری صنعت خواهدشد. از سوی دیگر هزینه جایگزینی بی‌شمار اجزای نرم‌افزار و کتابخانه‌های مستعمل با نمونه‌هایی که به‌خوبی مهندسی شده‌اند به نفع هزینه شکست‌های مداوم سیستم‌های کامپیوتری امروزی مقایسه خواهدشد. چنین فعالیتی در زمینه مهندسی نیاز به همکاری بین‌المللی برای ارائه زبان‌های مختلف، ابزارهای حمایتی و اجزای هسته‌ای خواهد داشت، اما می‌تواند ما را به سمت سیستم‌های در حال توسعه با کیفیت‌های خیلی بهتر نسبت به امروز سوق دهد. در مهندسی سنتی، فروریختن یک پل باعث می‌شود که دلیل آن ریزش مورد مطالعه قرار بگیرد و اصول جدیدی برای عدم تکرار آن تجربه در نظر گرفته‌می‌شود.

## خارج از دسترس

راس اندرسون، مهندس امنیت دانشگاه کمبریج، یک‌سری طرح‌های استراتژی خاص را مطالعه می‌کند. وی در نقد تونی بلیر، نخست وزیر سابق انگلیس که کلاس‌های کامپیوتر مدارس را با کلاس‌های امنیت سایبری جایگزین کرد، می‌گوید: «بسیار خنده‌دار است که بگوییم آنها در مدارس امنیت سایبری را درس خواهند داد درحالی که قادر به تدریس برنامه‌نویسی کامپیوتری هم نیستند.»

او نیز مانند «شورتنف» به نقد استراتژی از بعد استانداردهای شکست‌خوردن برنامه‌ها می‌پردازد. در مورد اخیرِ Tesco که ۲۰ هزار مشتری روی هم رفته ۲،۵ میلیون پوند به سارقان سایبری باختند، اولین جایی بود که «مرجع استانداردهای مالی»، یک بانک را مجبور کرد که به شکل فوری به جبران خسارت یک مشتری بپردازد. او می‌گوید: «اگر آن استراتژی جدید بود و در تمامی موارد اجرا می‌شد، عالی به نظر می‌آمد.»

چنین نوعی از رویکرد البته ذکر نشده‌است. اندرسون هم بر این باور است که چنین مداخلاتی از سوی فعالان هک که اهداف را انتخاب می‌کنند، گزارش نشده‌است و دیده نشده‌است که نارضایتی خود را آشکار سازند. به‌علاوه «درباره خلافکاران سازمان‌دهی‌شده ترولا، اخبار جعلی یا دیگر مواردی که ما دیده‌ایم چیزی وجود ندارد» و چیزی که اندرسون در طول یک دهه از آن دفاع می‌کند وجود ندارد.

او می‌گوید: «ما باید مشخص کنیم که می‌خواهیم چه چیزهای بدی را متوقف سازیم. امنیت اطلاعات موضوعی مرتبط با قدرت است. در روزگار قدیم، این امر به‌وسیله مردان شمشیرزن، قفل‌ها، قلعه‌ها و برج‌ها محقق می‌شد.

**همه ما موافقیم که حفاظت از اطلاعات حیاتی سازمان امری بدیهی است. نشت‌های اطلاعاتی که زیان‌های زیادی به بار می‌آورند به ما یادآوری می‌کنند که نگرانی ما کاملاً به‌جاست. از دست رفتن اطلاعات سازمان می‌تواند به کاهش سهم سازمان از بازار و کاهش قیمت سهام منجر شود.**

اما چیزی که به نظر می‌رسد بر سر آن توافق نداریم این است که در هر کسب‌وکاری چه کسی مسئولیت حفاظت از اطلاعات را برعهده دارد. سعی کنید در سازمان خودتان همین سؤال را مطرح کنید و ببینید چه جواب‌هایی دریافت‌می‌کنید. آیا مدیر اطلاعات شرکت تنها وظیفه خود را روشن نگه‌داشتن سیستم‌ها و اطمینان از کارکردشان می‌داند؟ اگر در سازمان‌تان مدیر امنیت اطلاعات دارید، آیا همیشه در تضاد منافع با مدیر اطلاعات شرکت قرار دارد که می‌خواهد بودجه‌ها را تراز نگه دارد؟ آیا گروه منابع انسانی سازمان می‌پذیرد که آگاهی از اصول امنیت از وظایف گروهی است که راهنماهای کاری منابع انسانی را می‌نویسند؟ آیا می‌توانید کسی را پیدا کنید که قبول کند مسئولیت امنیت سایبری به عهده اوست؟ پاسخ شما هم احتمالاً خیر است و مشکل همین‌جاست. گرچه غالباً پیشنهاد می‌شود که مسئولیت اشتراکی برای امنیت راه‌حل این مشکل است، اما این تنها باعث می‌شود که کل وظیفه مربوط به این کار دست‌به‌دست شود و در آخر هم هیچ‌کس مسئولیت آن را نپذیرد.

خب، پس واقعاً چه کسی مسئول امنیت اطلاعات است و برای اینکه کارش را به‌خوبی انجام‌دهد به چه پشتیبانی‌هایی نیاز دارد؟

## امنیت به یک قهرمان نیاز دارد

عموماً زمانی که یک شرکت مورد نفوذ قرار می‌گیرد و دچار نشت اطلاعاتی می‌شود، همه انگشت‌ها به سمت بخش IT نشانه می‌روند. شاید منطقی به نظر برسد، هرچه نباشد به سختی می‌توان این مشکل را به تیم تولید نسبت داد! شاید هم نه، اگر مسئولیت امنیت به عهده تیم IT است، پس باید بودجه امنیت هم از بودجه فناوری سازمان پرداخت شود. نکته منفی اینجاست که در این صورت هم احتمال زیادی وجود دارد که بودجه امنیت در میان سایر نیازها و الزامات حیف‌ومیل شود و این کاملاً ناعادلانه است که بخواهیم مسئولیت و سرزنش‌های ناشی از مشکلات را برعهده بخشی بگذاریم که در اولویت‌بندی بودجه دچار مشکل و تداخل است.

سازمان‌ها برای کنترل بهتر امنیت اطلاعات نیاز به قهرمانی دارند که خارج از بخش IT باشد. شاید یک مدیر امنیت اطلاعات یا Chief Information Security Officer (CISO) با نقشی کاملاً مجزا و بودجه‌ای که خودش بتواند مدیریت‌کند. تحقیقی که به‌تازگی انجام شده‌است، نشان می‌دهد که ۵۴ درصد سؤال‌شوندگان یک «مدیر امنیت اطلاعات» دارند که مسئولیت برنامه‌های امنیتی آنها را برعهده دارد و ۴۹ درصد هم یک «مدیر امنیت» (Chief Security Officer(CSO دارند. چیزی که مشخص نشده این است که نقش مدیر امنیت اطلاعات در داخل سازمان‌های بررسی شده چیست و اینکه این عملکرد تا چه حد خودکار شده‌است.

به این ترتیب آیا امنیت باید یک بخش و عملکرد مجزا برای خودش باشد؟ تیمی کوچک که توسط یک مدیر امنیت اطلاعات هدایت می‌شود و در چارت سازمانی با نقطه‌چین به سایر قهرمان‌های امنیت در تیم‌های عملکردی دیگر متصل می‌شود؟ اما اگر سازمان به اندازه‌ای کوچک باشد که نتواند یک مدیر امنیت اطلاعات تمام‌وقت را استخدام کند، ممکن است برون‌سپاری این عملکرد منطقی به نظر برسد. در این صورت هزینه‌کردن برای یک متخصص طرف سوم برای کمک به برنامه‌ریزی و مدیریت استراتژی سیستم امنیتی به شرکت کمک می‌کند یک سرمایه‌گذاری امنیتی مشخص و آشکار انجام‌دهد.

## ضعف افراد یا فناوری؟

بودجه امنیت اطلاعات غالباً در بخش IT لحاظ می‌شود و خطر این است که این بودجه‌ها به احتمال زیاد صرف خرید چیزهای دیگری مثلاً افزایش سطح امنیتی شبکه شود که قرار است به حل مشکل کمک‌کنند، اما مشکل این است که بسیاری از درزهای اطلاعاتی کنونی به‌واسطه مشکلات فناورانه اتفاق نیفتاده‌اند، بلکه به‌سادگی ممکن است نتیجه بی‌توجهی به هشدارهایی باشد که فناوری نشان می‌داده‌است. حال چه مشکل در سیستم اعلام هشدار باشد و چه در نبود منابع کافی برای پایش دایمی سیستم‌ها و تحلیل هشدارها.

ریشه بسیاری از نشت‌های اطلاعاتی در سازمان خود شما وجود دارد و ممکن است عمدی باشد، گرچه در بیشتر موارد تصادفی است. هزینه کاهش این نشت‌ها در حال افزایش است و همین باعث شد کسب‌وکارها تمرکز بیشتری بر روی امنیت IT داشته‌باشند، اما یک استراتژی که شما را مجبور به خرید ابزارهای بیشتر برای کاهش ریسک کند خود بخشی از مشکل است و این بسیار متفاوت از استراتژی است که بر آموزش و آگاهی تمرکز کرده‌است.

هزینه‌کردن بودجه‌ای زیاد برای راه‌اندازی برنامه‌های آموزشی و افزایش آگاهی کارکنان می‌تواند تفاوت چشمگیری در سازمان ایجادکند و به‌صورت بالقوه یکی از مهم‌ترین چیزهایی است که یک سازمان می‌تواند با آن به مقابله مشکلات امنیتی برود. در تحقیقی که اخیراً صورت پذیرفته‌است، ۴۶ درصد سؤال‌شوندگان نیروی کار را به‌عنوان یکی از اصلی‌ترین ضعف‌های امنیتی سازمان معرفی کرده‌اند. درک اینکه افراد و نه فقط فناوری، راه‌حل این مشکل است خود گامی در جهت صحیح به‌نظر می‌رسد.

## زمان تفکر دوباره در مورد آموزش امنیت سایبری فرا رسیده‌است

اما باید در مورد برنامه‌های آموزشی و آگاهی‌بخشی از نو فکر کرد تا بتوان کارایی آنها را افزایش داد. تحقیق دیگری که اخیراً انجام شده‌است نشان داد که ۵۳ درصد سازمان‌ها برنامه‌های آگاهی‌بخشی برای کارکنان را در دستور کار خود دارند، اما چند درصد این برنامه‌ها مؤثر هستند؟ سؤال دیگر این که در کشورهایی که دورکاری به‌سرعت در حال فراگیر شدن است، آیا تقویت الزامات امنیتی دشوارتر است؟ آموزش ویدئویی و برگزاری کارگاه‌ها ممکن است زمانی‌که کارکنان از میزشان دور هستند مفید باشد، اما به‌محض این که به پشت میزشان برگردند و بین انتخاب یک گذرواژه ساده و چیزی که ممکن است هفته بعد یادشان برود، مردد شوند همه تأثیر خود را از دست خواهنددداد. یک ویدئوی بازآموزی سالانه ۹۰ دقیقه‌ای احتمالاً مؤثرترین روش برای یادآوری اهمیت حفاظت از اطلاعات نخواهدبود. شاید مؤثرتر این باشد که متخصصانی را به‌کار بگیرید که افراد یا کل یک دپارتمان را مورد حملات فیشینگ (Phishing) قرار دهند. تاکتیک‌های شوکه‌کننده به‌سرعت به کارکنان نشان خواهدداد که جرایم سایبری چگونه به‌سرعت و بدون هیچ هشداری به وقوع خواهند پیوست و این به یقین روشی مؤثرتر از نمایش یک ویدئوی دیگر خواهدبود.

## آیا هیئت‌مدیره مسئول است؟

یک سازمان وظیفه مواظبت از کارمندان، مشتریان، تأمین‌کنندگان و سهامدارانش را برعهده دارد و اعضای هیئت‌مدیره روزبه‌روز بیشتر متوجه‌می‌شوند که جرایم سایبری مشکلی است که به اقدامات عملی نیاز دارد. از بسیاری جهات هیئت‌مدیره باید به همان اندازه که مسئولیت بهره‌وری مالی سازمان را می‌پذیرد مسئولیت پیاده‌سازی اقدامات عملی در زمینه امنیت سایبری را نیز بپذیرد. مشکل این است که بسیاری از هیئت‌های ریاست شرکت‌ها درست متوجه این موضوع نیستند و هماهنگ ماندن با دنیای دائماً در حال تغییر امنیت اطلاعات کار دشواری است. مهم است که هیئت‌مدیره متوجه مسئولیت خود در زمینه اولویت‌بخشیدن به امنیت سایبری باشد و اطمینان حاصل کند که در درون سازمان روال‌های درست در حال اجرا هستند و بودجه کافی در اختیار دارند. این موضوع می‌تواند شامل درک ریسک امنیتی سازمان، تعیین حدود انتظارات از مدیران، موافقت با ایجاد سمت شغلی مدیر امنیت اطلاعات، تصمیم‌گیری در مورد اینکه آیا

**ریشه بسیاری از نشت‌های اطلاعاتی در سازمان خود شما وجود دارد و ممکن است عمدی باشد، گرچه در بیشتر موارد تصادفی است**

خود هیئت‌مدیره به متخصص امنیتی اختصاصی نیاز دارد یا نه، ارزیابی بودجه و همین‌طور روال‌ها و عملکردهای امنیت سایبری که درحال‌حاضر در شرکت اجرا می‌شوند و درنهایت اجباری‌کردن استفاده از متخصصان امنیت خارج از شرکت شود. در وضعیتی که ۳۴ درصد شرکت‌های جهان نسبت به هزینه‌های بازاریابی، هزینه کمتری را صرف امنیت اطلاعات می‌کنند، الزامی است که بودجه به‌درستی تقسیم و توزیع شود تا بتوان درباره امنیت اطمینان حاصل کرد.

## آیا درک کافی از میزان ریسک دارید؟

شاید اولین گام در تعیین اینکه مسئولیت امنیت اطلاعات باید برعهده چه کسی باشد، این است که به‌صورت کامل درک‌کنیم که تمام بخش‌های کسب‌وکار ما تا چه اندازه در معرضِ ریسک و خطر قرار دارند. خدمات ارزیابی ریسک (که معمولاً توسط شرکت‌های طرف سوم ارائه‌می‌شود) بخش‌های مختلف ازجمله پذیرش ریسک، برخورد با ریسک، فناوری، امنیت کلود، بخش‌های عملیاتی و ریسک طرف سوم را برای دیدن آسیب‌پذیری‌ها و راه‌های نفوذ بررسی می‌کند. آزمون‌های نفوذ هدف‌گذاری‌شده، برداشتی صحیح از تهدیدات امنیتی برای شما به‌وجود خواهدآورد و استفاده از این شواهد برای اطلاع‌رسانی به تصمیم‌گیرندگان می‌تواند راهی مفید برای درک میزان قرار گرفتن شما در معرض ریسک باشد. نتیجه نهایی می‌تواند یک نقشه راه مفصل و پرجزییات باشد که به شما در مدیریت امنیت کمک‌کند، نیروهای کار شما را آموزش‌دهد و یک برنامه کاری عمیق برای شما فراهم‌کند که شامل موارد تجاری هم باشد و به شما نشان‌دهد که مسئولیت در کجای سازمان باید قرار بگیرد.

## نکته اصلی پاسخ به‌موقع به پیشامدها است

پس از آنکه سازمان تصمیم گرفت که چه کسی مسئول امنیت است، ایجاد یک برنامه واکنش به پیشامدها بسیار مهم است ولی غالباً نادیده انگاشته‌می‌شود. مطالعه‌ای جدید نشان داده‌است که ۷۷ درصد شرکت‌ها، ظرفیت تعامل با پیشامدهای تأثیرگذار و خطرناک را ندارند و غالباً زمانی به سراغ خدمات پشتیبانی می‌روند که حادثه رخ داده‌است. یک برنامه قدرتمند واکنش به پیشامدها، جلوی روی دادن نشت‌های اطلاعاتی را نمی‌گیرد، اما واکنش به‌موقع به نشت اطلاعات می‌تواند به معنای تفاوت میان یک تعامل آرام و بی‌سروصدا با یک مشکل داخلی باشد یا سروکله زدن با تیترهای اول روزنامه‌ها و البته برای اطلاع‌رسانی مؤثر در مورد نشت‌های اطلاعاتی و واکنش به آنها دلایل اقتصادی قابل‌قبولی وجود دارد. کاهش قیمت سهام و نگرانی‌های مشتریان در زمینه قابلیت اطمینان شرکت پس از بروز یک حادثه مربوط به نشت اطلاعات را می‌توان با یک واکنش شفاف و سریع و برقراری ارتباطات به‌موقع با مشتریان به‌خوبی کاهش داد.

## مسئولیت‌پذیری در برابر پاسخگویی

یک حادثه امنیتی می‌تواند تبعات طولانی‌مدتی روی شرکت داشته‌باشد و اکنون امنیت به‌عنوان یک مشکل مربوط به هیئت‌مدیره دیده‌می‌شود. درنهایت مدیرعامل باید پاسخگوی نشت‌های بزرگ اطلاعاتی باشد، اما به توصیه‌های سطح بالا و پرمحتوا از سوی یک متخصص احتیاج دارد


**واکنش به‌موقع به نشت اطلاعات می‌تواند به معنای تفاوت میان یک تعامل آرام و بی‌سروصدا با یک مشکل داخلی باشد**