در دنیای مجازی شبکه‌های رایانه‌ای که به زندگی امروزین جهانیان را رنگ و بوی دیگرگونی داده است، همه شکل اتفاق و ماجرایی رخ می‌دهد. در این بین تبهکاران هم ردپایی از خود به جا می‌گذارند و دست‌اندکاران امر همیشه مناقشه برانگیز «قانون» می‌کوشندتا مانع خلاف‌کاری و فسادهای روی خط شوند. از این پس صفحهٔ «لبهٔ تاریکی» در مجلهٔ شبکه، محملی است برای مرور اخبار و گزارش‌های رویایی خیر و شر در این وادی.

هکرهای کرایه‌ای!

بهروز نوعی‌پور

اشاره

به عنوان مسؤول یک شبکه کامپیوتری، چگونه می‌خواهید امنیت شبکه خود را بالا ببرید؟ گزینه‌های متعددی پیش روی شماست. بهترین آن‌ها این است که دانش خود و پرسنل شبکه را در زمینهٔ مسائل امنیتی بالا ببرید و از تجهیزات نرم‌افزاری قوی استفاده کنید. اما راه‌های دیگری هم هست. این روزها خیلی از شبکه‌ها به فکر استخدام هکرها افتاده‌اند! این افراد استخدام می‌شوند تا نقاط ضعف و رخنه‌های شبکه و سایت شما را کشف کنند و رهنمودهای لازم را برای برطرف کردن آن‌ها در اختیارتان قرار دهند. این مقاله خلاصه‌ای از چندین مقاله و خبر در این زمینه است که توسط نویسنده گردآوری و تنظیم شده و ابعاد مسألهٔ «هکربودن» را به عنوان یک شغل بررسی می‌کند.

نمادی از همایش «کلاه مشکی» ها که محل گرد آمدن جمع زیادی از هکرهای حرفه‌ای بود.

کرایه کردن و استخدام هکرها به تدریج به یک کار متداول تبدیل می‌شود. در کشورهای در حال توسعه‌ای مثل عربستان و چین که دولت محدودیت‌های شدیدی را بر استفاده مردم از سایت‌های اینترنتی وارد می‌کند، جوانان بسیاری هستند که کارشان هک کردن موانع و عبور کردن از فیلترها و دیواره‌های آتش است. این جوانان توسط صاحبان کافی‌نت‌ها و دیگر مراکز سرویس‌دهی اینترنت به صورت ساعتی کرایه می‌شوند تا امکان دسترسی برای کاربرانی را که که حاضرند برای مشاهدهٔ سایت‌های دلخواه خود پول بیشتری بپردازند، فراهم کنند. حتی بعضی از اشخاص متمول (مثلاً در عربستان) این هکرها را در منزل کرایه می‌کنند تا برای چند ساعت امکان دسترسی آن‌ها به سایت‌های دلخواه آنها را فراهم کنند. در کشورهای صنعتی، هکرها به گونهٔ دیگری کرایه می‌شوند. در این کشورها شرکت‌ها و سازمان‌های مختلفی که در محل خود، سایت یا شبکه کامپیوتری ویژه‌ای دارند، از بیم رخنه‌های امنیتی موجود در شبکه خود و برای اجتناب از حوادث احتمالی در آینده، هکرهای کار کشته را به طور موقت (یا دائم) استخدام می‌کنند تا با میل و تقاضای کارفرما، شبکهٔ آن‌ها هک شود و از این طریق نقاط ضعف و نفوذپذیری سیستم‌های‌شان پیدا شود. گاهی اوقات همین کارفرما به هکری که کرایه کرده است پول بیشتری می‌دهد تا خودش نقطه ضعفی را که یافته است، مسدود کند یا از هکرها می‌خواهد به کارشناسان سازمان مشاوره و راهنمایی‌های لازم برای برطرف کردن نقاط آسیب‌پذیر را بدهند. به این ترتیب به نظر می‌رسد «هکری» به یک شغل پول‌ساز تبدیل شده که در شرایط خلاء قانونی یا در کنار قانون به حیات خود ادامه می‌دهد.

طنز قضیه در آن است که گاهی اوقات همین دولت‌ها نیز هکرها را برای یافتن نقاط نفوذپذیر فیلترها و دیواره‌های آتش خود استخدام می‌کنند و مبالغی کلان به آن‌ها برای مسدود کردن این گذرگاه‌ها می‌پردازند. حتی در کشوری مثل آمریکا که موانع فرهنگی اندکی برای دسترسی مردم به سایت‌های اینترنتی وجود دارد، سازمان‌هایی مثل اف‌بی‌آی (پلیس آمریکا) هکرهای سابقه‌دار و حرفه‌ای را به طور مخفیانه برای کشف روش‌های عملیاتی سایر هکرها، خلاف‌کاران و دزدان شبکه‌ای و نیز نفوذ به

تشکیلات سازمان‌های تبهکاری، تروریستی و غیره اجیر می‌کنند.

مزدورهای عصر شبکه در سرتاسر جهان همه روزه مشغول کارند، گاهی اوقات با قصد جاسوسی علمی، اقتصادی یا سیاسی، گاهی اوقات به قصد خرابکاری و ضربه‌زدن و گاهی به قصد یافتن نقاط ضعف سیستم‌ها و شبکه‌های کامپیوتری. در این میان آن چه بیش از هر علت دیگری موجب رواج پدیدهٔ «هکرهای کرایه‌ای» شده است و حیات و بقای این قشر از جامعه را تداوم بخشیده است، همانا مزایای استفاده کردن از تجربیات هکرها برای مقابله با تهدیدات سایر هکرهای متخاصم است. منطق این راهبرد یک مَثَل قدیمی است که می‌گوید: «دشمنِ دشمن شما دوست شماست.» اگرچه بدیهی است که چند جفت چشم تیزبین و متخصص برای وارسی و اندازه‌گیری وضعیت امنیتی شبکه شما بسیار سودمند به نظر می‌رسند، اما این سوال مطرح است که آیا می‌توان به کسانی که در حمله و نفوذ به سایر شبکه‌ها شناخته شده هستند، در سازمان خود اعتماد کرد؟ چه دلیلی وجود دارد که هکری که تا دیروز دشمن بالقوه شبکه شما به شمار می‌رفت، امروزپس از دریافت مبلغی پول معتمد شما باشد؟ این اعتماد تا کجا و کی دوام خواهد آورد؟

پرسش‌های دیگری نیز مطرح‌اند: از کجا معلوم که هکر استخدام شده، صادقانه تمام رخنه‌های امنیتی را که کشف کرده است، به شما اطلاع دهد؟ شاید بخواهد برخی از آن‌ها را برای هنگام دریافت دستمزد و چانه‌زنی محفوظ نگه دارد. شاید برخی از آن‌ها را هرگز به شما اطلاع ندهد تا راه را برای کسب درآمد دوباره در آینده برای خود یا دوستانش باز بگذارد. آیا ممکن است هکر استخدامی شبکه شما در اصل مزدور کسان دیگری باشد و با ماسک اعتماد برانگیزی نزد شما آمده باشد تا رخنه‌های امنیتی شبکه شما را برطرف کند؟ حتی ممکن است شبکهٔ شما با وجود انواع حصارهای امنیتی و دیواره‌های آتش، به سختی از بیرون شرکت یا سازمان قابل نفوذ باشد، اما پس از کرایه کردن هکری که به قصد یافتن رخنه‌ها آمده است، در داخل سازمان شما و بدون این‌که کسی متوجه شود نقاط آسیب‌پذیر جدیدی را که تا قبل از آن وجود نداشته است، خود پدید آورد تا نهایتاً بتواند بر سر آن‌ها با کارفرما یا افراد دیگر معامله کند.

عجیب است که با وجود این همه پرسش نگران‌کننده، روز به روز به تعداد سازمان‌ها و

ریچارد کلارک، مشاور رییس جمهور آمریکا در زمینه امنیت رایانه‌ای ، در همایش «کلاه مشکی‌ها» سخنرانی کرد.

شرکت‌هایی که در اروپا، ژاپن و آمریکا هکرهای حرفه‌ای را کرایه می‌کنند، افزوده می‌شود. شاید در جامعهٔ زیرزمینی هکرها مرام و مسلکی وجود دارد که براساس یک توافق نانوشته و ثبت نشده، هکرهای حرفه‌ای از سوءاستفاده بیش از حد از پرسش‌های فوق اجتناب می‌کنند تا بازار این نوع نیمه مشروع از کاسبی‌شان هم‌چنان داغ بماند!

بعضی از روان‌شناسان عصر شبکه این‌طور استدلال می‌کنند که نفوذگری شبکه‌ای لزوماً به یک شخصیت بد و ضداجتماعی نیاز ندارد و پدیدهٔ فیزیولوژیکی «باکتری‌های مفید» را به عنوان نمونهٔ مشابهی در حوزهٔ متفاوت «بهداشت» یادآوری می‌کنند.

گروه دیگری از کارشناسان مسائل اجتماعی حتی از این هم فراتر می‌روند و تحلیل پیچیده‌تری ارائه می‌کنند. آنان معتقدند رشد پدیدهٔ «هکرهای کرایه‌ای» یک نوع واکنش اجتماعی از سوی صاحبان سایت‌ها و شبکه‌ها به حضور این قشر از جامعهٔ فراصنعتی است و اضافه می‌کند همان‌طور که هکرهای حرفه‌ای از مهندسی اجتماعی برای فریب دادن قربانیان خود استفاده می‌کنند، شرکت‌ها و سازمان‌های باهوش با نزدیک کردن خود به جامعهٔ هکرها و اجتناب از غریبه نگه‌داشتن هکرها نسبت به سازمان مطبوع خود، نوعی مصونیت اجتماعی در برابر تهدیدات آنان پدید می‌آورند. این رهیافت در حقیقت سطح پیچیده‌تری از مهندسی اجتماعی است که از طریق آن صاحبان و رؤسای سازمان‌ها و شرکت‌ها می‌کوشند نوعی همزیستی مسالمت‌آمیز میان مجموعهٔ خود و جامعهٔ هکرها به وجود آورند تا حضور دائمی هکرها در سازمان و شرکت گونه‌ای از پادتن و واکسن اجتماعی را در سرتاسر سازمان منتشر کند. شاید از این طریق پرسنل شرکت را نسبت به خطرات احتمالی هوشیار و گوش به زنگ و آماده برای رویارویی با حوادث نگه دارند.

فرضیه‌هایی مانند این موجب پدید آمدن دانش جدیدی به نام Cybersecurity شده است. اصل اول این دانش می‌گوید: «هکرها را غیرخودی نکن و میان خودت و هکرها مرز نکش! در حقیقت با آن‌ها دوستی کن. برای آن‌ها خرج کن! آن‌ها را مجرم، تروریست و عقده‌ای نخوان!»

چندی پیش خبرگزاری آسوشیتدپرس ماجرای جالبی را گزارش کرد. ریچارد کلارک مشاور جرج بوش در زمینهٔ امنیت کامپیوتری تصمیم می‌گیرد در یکی از همایش‌های بزرگ هکرهای آمریکا به نام «کلاه مشکی» شرکت کند. روز دهم مرداد وی به سالن همایش «کلاه مشکی» در لاس وگاس مراجعه می‌کند و مشاهده می‌کند که جمعیت زیادی از کارشناسان امنیت و هکرها مشغول رایزنی با یکدیگر در زمینهٔ مشکلات امنیتی هستند. کلارک طی سخنرانی‌ای که در جمع هکرها ایراد می‌کند بر این واقعیت صحه می‌گذارد که بسیاری از رخنه‌های امنیتی که در نرم‌افزارهای مهم و متداول وجود دارند توسط خود سازندگان‌شان شناخته نشده‌اند، در حالی که بسیاری از کاربران مستقل این نقاط آسیب‌پذیر را کشف کرده‌اند. کلارک در سخنرانی خود کارشناسان و هکرهای حاضر در سالن را تشویق می‌کند که نرم‌افزارها و سیستم‌های کامپیوتری را هرچه زودتر هک کنند و در زمینهٔ ارائه دستاوردهای خود به دولت و شرکت‌های کامپیوتری همکاری کنند. وی تأکید می‌کند که «بعضی از ما افراد حاضر در این سالن به لزوم پیدا کردن هرچه سریع‌تر نقاط آسیب‌پذیری رسیده‌ایم.»

سخنان کلارک به آخرین یافته‌های یک مؤسسهٔ پژوهشی دولتی دربارهٔ امنیت کامپیوتری اشاره داشت که طی آن گزارش شده بود این مؤسسه هزاران رخنهٔ امنیتی گوناگون را در بافت نرم‌افزارهای شرکت‌های سان مایکروسیستمز، مایکروسافت، اوراکل و AOL و دیگر شرکت‌های کامپیوتری پیدا کرده است که به نحوه فاجعه باری امنیت کسب و کار الکترونیکی را تهدید می‌کنند.

کلارک از هکرها خواست پس از یافتن رخنه‌ها بلافاصله به شرکت‌های سازنده مراجعه کنند و بر سر ارائه یافته‌های خود به آن‌ها به توافق برسند و معامله کنند و در صورت عدم کسب نتایج دلخواه به دولت مراجعه کنند و طرح‌های خود را ارائه کنند.

سخنان کلارک بازتاب‌های مختلفی را به دنبال داشت. بعضی شرکت‌های کامپیوتری از همکاری بیشتر هکرها و سازندگان نرم‌افزار

استقبال کردند و بعضی دیگر هشدار دادند که چنین پیشنهاداتی ممکن است موجب رواج اخاذی هکرها از سازندگان نرم‌افزار شود. بعضی از تحلیل‌گران اظهار داشتند که ممکن است این راهبرد موجب پدید آمدن بازار سیاهی شود که در آن هکرها، دلالان و کارشناسان امنیتی، پرسنل شرکت‌ها و مأموران دولت به خرید و فروش موردی باگ‌ها و رخنه‌های امنیتی می‌پردازند.

خالی از لطف نیست که بدانید کنفرانس «کلاه مشکی» از سوی مؤسسات و شرکت هایی مثل Princewaterhouse Coopers و مایکروسافت و چندتای دیگر حمایت و پشتیبانی می‌شود و هر سال طی یک همایش دو روزه راه‌های نفوذ به سیستم‌ها و اخلال در آن‌ها را بررسی می‌کند.

همهٔ این بحث‌ها و مشاجرات منجر به ابهامات و پرسش‌های دیگری شده‌اند که خود به خود بر پیچیدگی حقوقی موضوع افزوده‌اند. یک مسألهٔ مهم این است که موضع دولت در این زمینه باید چگونه باشد؟ آیا دولت باید هکرها را تشویق کند؟ آیا دولت باید با پدیدهٔ «هکرهای کرایه‌ای» مقابله کند؟ کارشناسان اقتصادی مسألهٔ سود و زیان را در این تصمیم‌گیری دخیل می‌دانند. آن‌ها معتقدند در کشورهایی با اقتصاد تولیدی مثل آمریکا سود دولت بیشتر در این است که هکرها را تشویق به همکاری با شرکت‌ها کند، اما در کشورهایی که عمدتاً مصرف‌کنندهٔ محصولات کامپیوتری هستند شاید وضعیت متفاوت باشد. اگرچه به طور طبیعی تعداد مصرف‌کنندگان هر محصولی از تعداد تولیدکنندگان آن بیشتر است و می‌توان پیش‌بینی کرد که هکرها از بابت معامله و چانه‌زنی با بازار مصرف‌کنندگان به سود بیشتری دست خواهند یافت.

از سوی دیگر تکلیف ابعاد حقوقی مسأله هنوز روشن نیست. در واقع دولت نمی‌تواند از یک سو هکر بودن را جرم بداند و از سوی دیگر از توانایی‌های این افراد برای کشف نقاط ضعف سیستم‌ها بهره‌کشی کند.

این تناقض حقوقی در انواع قدیمی‌تر نفوذگری و تجاوز به منافع دیگران وجود نداشته است. پلیس هر کشوری ممکن است برای مقابله با جرائم مشهود از تجربیات دزدان و تبهکاران سابق استفاده کند، اما گسترهٔ این فعالیت محدود است، چرا که تجاوز دیگران به منافع شخصی حادثه‌ای است که بخش ناچیزی از زندگی هر انسان معمولی را تشکیل می‌دهد در حالی که به دلیل گسترش بی‌سابقهٔ کامپیوترها و شبکه‌های ارتباطی، بسیاری از مردم، شبانه‌روز در معرض تهدید دائمی هکرها و نفوذگران شبکه‌ای هستند و اگر بنا باشد دولت و مردم از توانایی‌های هکرهای حرفه‌ای برای کشف نقاط آسیب‌پذیر سیستم‌های خود استفاده کنند، ابعاد این پدیده بسیار گسترده خواهد بود. آیا در این صورت مسألهٔ «تجاوز شبکه‌ای» از نظر حقوقی، ارزشی و اخلاقی مفهومی دوگانه نخواهد بود؟