... پس از چند ثانیه تلفن من به صدا درآمد و شماره مرکز اطلاعات تلفن را نشان داد. وقتی که به تلفن پاسخ دادم، کوین پشت خط بود.

ساعتی با کوین میتنیک

اسطوره نفوذگری

ترجمه: مهرداد مناف‌فر

اشاره

کمتر کسی است که با داشتن نیم نگاهی به مباحث امنیت شبکه‌ها، نام Kevin Mitnick را نشنیده باشد. بسیاری وی را اسطوره نفوذگری نامیده‌اند و خیلی‌ها لقب عقاب را شایسته وی می‌دانند. کوین را به جرأت می‌توان بزرگترین نفوذگر و حال حاضر دنیا دانست. وی پس از گذشت دو سال از صدور حکم بازداشت، سرانجام در سال ۱۹۹۵، به جرم نفوذ به شبکه‌های کامپیوتری شرکت‌های بزرگ و دسترسی غیرمجاز به سورس بسیاری از سیستم‌های عامل، توسط پلیس فدرال آمریکا (FBI) دستگیر و روانه زندان شد. کوین پس از گذراندن ۸ ماه زندانِ انفرادی و ۴ سال زندان عمومی، بدون قبول هیچ‌گونه بازنگری در حکم صادره، سرانجام در اوایل سال ۲۰۰۰ میلادی پس از رسیدن به توافقاتی با مقامات دولتی، تحت قید و شرط‌های بسیار سنگین آزاد شد و در نهایت در ژانویه سال ۲۰۰۳ میلادی آزادی بی‌قید و شرط خود را به دست آورد.

کوین پس از به دست آوردن آزادی کامل خود چندین کتاب را نیز به چاپ رسانده است که از آن جمله می‌توان به کتاب (Art of Deception) (هنر فریبکاری) اشاره کرد که به طور تخصصی بر روی مهندسی اجتماعی و نقش افراد در حفظ امنیت شبکه‌های کامپیوتری بحث کرده و شیوه‌های مختلف کسب اطلاعات از طریق مهندسی اجتماعی را مورد بررسی قرار داده است. در حال حاضر وی مشغول نگارش کتاب دیگری با نام The Art of Intrusion می‌باشد.

کوین میتنیک خود از لحاظ شخصیتی فردی بسیار باهوش و دوست‌داشتنی است که یکی از عوامل موفقیت برنامه‌های آموزشی وی در سراسر دنیا نیز همین امر است. در تاریخ سی‌ام مارس سال ۲۰۰۴ میلادی طی کنفرانسی با نام کنفرانس جهانی Infosec، فرصتی پیش آمد تا مصاحبه‌ای با وی داشته باشیم که در ذیل بخش‌هایی از این گفتگو را می‌خوانید.

● این روزها مشغول چه کاری هستید؟

○ اخیراً کنفرانس‌های متعددی در گوشه و کنار دنیا با هدف آموزش کارکنان سازمان‌های مختلف و افزایش آگاهی آنان در مقابله با حملات مهندسی اجتماعی داشتم. همچنین دوره‌های متعددی در زمینه برپایی شبکه‌های بی‌سیم امن برگزار کرده‌ام. در حال حاضر نیز مشغول نوشتن کتاب جدیدی می‌باشم. شرکتی هم با نام Defensive Thinking تأسیس کرده‌ام که در آن آزمون‌های امنیتی برای شبکه‌های مختلف انجام می‌دهیم. همچنین در چند مورد با سمت مشاور امنیتی در حوزه جرایم سایبر با مسؤولان همکاری دارم. یکی از این موارد مربوط به یکی از پرسنل یکی از شرکت‌های بزرگ کامپیوتری می‌باشد که به طور غیرقانونی سورس چند برنامه محرمانه را بر روی سیستم خود منتقل کرده که قاضی دادگاه پس از تشکیل پرونده به طور رسمی از من جهت ارایه نظر تخصصی دعوت به عمل آورده است. در مورد مشابه دیگری به عنوان یک متخصص امنیتی جهت برآورد میزان خسارات وارده ناشی از ارتکاب جرم رایانه‌ای دعوت به همکاری شده‌ام.

● نظر شما در رابطه با کمک گرفتن از نفوذگران در برقراری امنیت شبکه‌های مختلف دولتی و خصوصی چیست؟

○ سال پیش جهت شرکت در یک جلسه پرسش و پاسخ دعوت شدم. در طی این جلسه که شباهت زیادی به یک بازجویی و منازعه کامل داشت از من سؤال شد که آیا از یک نفوذگر با سابقه برای برقراری امنیت شبکه خصوصی خودم استفاده می‌کنم یا نه؟ در این‌جا بود که از جانب گروهی با این طرز فکر مورد مخاطب قرار گرفتم که اگر فردی در طول عمر خود مرتکب جرمی شود، تا ابد گرایش به سمت بزهکاری داشته و دیگر نمی‌توان به وی اعتماد کرد. در انتهای جلسه هیچ‌یک از طرفین از طرز فکر خود

در این شماره:

۱۷۶/ ساعتی با کوین میتنیک

۱۷۸/ نیمرخ - باب بمر

۱۷۹/ لبه تاریکی - چشم‌انداز مبارزه با هرزه‌نگاری اینترنتی در ایران

۱۸۱/ نوستالژی - پایان یک فصل

تحت عنوان "عصرشبکه" جدی تر و مشخص تر از مؤلفه های فضا ی سایبر حرف خواهیم زد.

دست نکشیدند و جلسه بدون هیچ نتیجه‌ای به پایان رسید. به نظر من مطرح نمودن چنین مسایلی هیچ سودی در بر نخواهد داشت.

فرض کنید نفوذگری وارد شبکه بانک یک شهر شده و میلیون‌ها دلار به سرقت برده است. آیا شما از وی برای برقراری امنیت شبکه بانکی خود استفاده می‌کنید؟ به احتمال قوی جواب شما منفی خواهد بود؛ چون که در زمینه مورد نظر شما، وی مجرم شناخته می‌شود و غالباً بهره گرفتن از چنین فردی ریسک بزرگی به حساب می‌آید. حال فرض کنید بخواهیم از همین فرد در حفظ امنیت اطلاعات مربوط به دانش‌آموزان اداره آموزش پرورش شهر دیگری استفاده نماییم. سؤال این است که آیا حتی در صورت دسترسی وی به اطلاعات مذکور، آیا آن اطلاعات به درد وی خواهند خورد؟ تحت چنین شرایطی با توجه به قابلیت‌ها و استعدادهای وی، استفاده از او ارزش این ریسک را خواهد داشت.

در واقع در همه حال این ریسک وجود خواهد داشت. سابقه کیفری نفوذگران در یک طرف و مهارت‌ها و دانش بالای آنان در طرف دیگر دو امر کاملاً متضاد به شمار می‌رود. در چنین شرایطی تصمیم‌گیری بر عهده شخص کارفرما بوده و حرف آخر را وی خواهد زد. خوشبختانه درباره خود من این امر جنبه مثبتی داشته است. مقامات دولتی جهت ارایه یکسری مشاوره و ارزیابی زیرساخت‌های اطلاعاتی و امنیتی شبکه‌های داخلی خود از من دعوت به عمل آورده است. بنابراین آن‌ها به نحوی با سبک سنگین کردن شرایط، تصمیم به بهره گرفتن از دانش من نموده است.

● محرک اصلی و انگیزه شما در انتخاب این مسیر چه بوده است؟

○ غالباً این سؤال را در قالب علت علاقه من به سورس برنامه‌ها و سیستم‌های عامل می‌پرسند. باید بگویم که دوست داشتم بهترین نفوذگر دنیا باشم. از ضربه زدن به مکانیزم امنیتی سیستم‌ها لذت می‌بردم. برای من عبور از تمهیدات امنیتی موجود بر روی شبکه‌ها، همانند نبردی دوست‌داشتنی بود. دوست داشتم به آن سوی درهای قفل شده سرک بکشم. نه به خاطر به سرقت بردن آن‌چه که در آن سو وجود داشت بلکه فقط و فقط برای ارضای حس کنجکاوی خودم. می‌خواستم در این نبرد پیروز باشم. برای رسیدن به هدف خود تصمیم گرفتم که نفوذ از طریق دستکاری در مکانیزم قفل را تجربه نمایم. هر چه‌قدر شکستن این قفل سخت‌تر می‌شد، نبرد لذت‌بخش‌تر می‌نمود.

بنابراین تصمیم گرفتم تا سورس برنامه خود قفل را به دست آوردم تا از معماری داخلی آن اطلاعاتی کسب نمایم و خطاهای صورت گرفته در روند طراحی آن را استخراج کنم. این کاری بود که من با سورس برنامه سیستم‌های عامل انجام دادم و به خاطر آن محکوم شدم. به هر نوع سیستم‌عاملی که می‌خواستم نفوذ کنم ابتدا سورس آن را از روی شبکه شرکت سازنده آن به دست آوردم و آن را بر روی هارددیسک کامپیوترهای دانشگاه کپی می‌کردم چون که کامپیوتر خودم با ظرفیت ۲۰۰ مگابایت هارد، گنجایش آن حجم از داده را نداشت. سپس به بررسی خط به خط برنامه پرداخته و تمامی حفره‌های موجود را بررسی می‌کردم و روش‌هایی را که برنامه‌نویس جهت رفع آن به کار برده بود مطالعه می‌کردم. چون که غالباً این موارد به وضوح در متن برنامه توضیح داده می‌شوند. پس از آن سعی در نوشتن کدهایی برای سوءاستفاده از این حفره‌ها می‌کردم.

● در مورد گذشته و حال چطور؟

○ در گذشته تصمیمات کودکانه بسیاری گرفته‌ام. اما در حال حاضر سعی در جبران گذشته دارم. سعی می‌کنم از این توانایی‌های خود در جهت کمک به دیگران استفاده نمایم و تا حدی نیز در این امر موفق بوده‌ام. البته مطمئن هستم که نیمی از مردم هنوز از من متنفر بوده و نیمی دیگر مرا دوست دارند. در واقع مردم بسته به برداشت خود از شخصیت و سیمای نشان داده شده از کوین میتنیک در رسانه‌ها، نسبت به من اظهار نظر کرده و جبهه‌گیری می‌کنند. همیشه نظرم این بوده که آن‌چه که در گذشته انجام داده‌ام غیرقانونی بوده و باید مجازات می‌شدم ولی نحوه صدور حکم و مجازات در نظر گرفته شده با نوع جرم اصلاً تطابق نداشته است.

● منظور از عدم تطابقی که ذکر کردید چیست؟ و در کل به نظر شما کدامیک صحیح می‌باشند، قوانین دهه هفتاد یا قوانین حال حاضر؟

○ به نظر من یکسان فرض کردن نفوذگری با عملیات تروریستی در فضای سایبر نوعی اغراق به حساب می‌آید. به طور مثال به تازگی قانون جدیدی به تصویب رسیده است که هر گونه آسیب‌رسانی جانی منجر به جراحت و یا مرگ که از طریق شبکه‌های کامپیوتری صورت پذیرد، دارای چنان مجازاتی سنگین می‌باشد که امکان هیچ‌گونه تجدید نظر در رأی صادره وجود نداشته و به هیچ‌وجه ضمانت و یا قید و شرطی برای تخفیف مجازات وجود نخواهد داشت. در حالی که اگر فردی با استفاده از مثلاً موتور سیکلت و یا یک چکش به شخص دیگری آسیب رساند حکم صادره به مراتب سبک‌تر از حالت اول خواهد بود. حال سؤال این‌جاست که چرا باید چنین شرایطی حاکم باشد؟ مگر رایانه هم همانند همان چکش نوعی وسیله به شمار نمی‌آید؟

همیشه باید مجرمین را برحسب نوع آسیبی که به اجتماع وارد می‌کنند محاکمه نمود، نه برحسب نوع ابزار مورد استفاده‌شان.

● به نظر شما همین مشکل موجود در میان قانونگذاران، ناشی از عدم آگاهی آنان از محتوای قضیه و نبود درک صحیحی از آن نمی‌باشد؟

○ به نظر من اگر نتوانیم به درستی مشکلی را درک کنیم هیچ‌گاه نخواهیم توانست از پس حل آن بر آییم.

● توصیه کلی شما در رابطه نحوه برقراری امنیت کامل شبکه‌های کامپیوتری چیست؟

○ ببینید امروزه ابزارآلات متعددی وجود دارند که همه مراحل نفوذ را برای شما انجام می‌دهند. شما می‌توانید بدون کوچک‌ترین اطلاعاتی از نحوه عملکرد آن‌ها فقط با دانستن آسیب‌پذیری‌های موجود در هدف خود، به‌راحتی به سیستم نفوذ نمایید. این در حالیست که در زمان من برای انجام هر کاری، خودمان باید نرم‌افزار مربوطه را می‌نوشتیم. دقیقاً به همین دلیل است که می‌گویم امروزه امنیت نه تنها شامل مقابله بلکه شامل محافظت و عکس‌العمل سریع نیز می‌شود. برای ایجاد امنیت با ضریب بالا باید تا حد امکان حفره‌ها و پنجره‌های ارتباطی موجود را محدودتر ساخته و همیشه در حال مانیتور نمودن تمامی انتقالات صورت گرفته در طول شبکه باشیم.

خودم براین باورم که به جای بررسی کلی شبکه و داشتن یک دید کلی، باید تک تک نرم‌افزارها و سخت‌افزارهای موجود را به صورت جداگانه مورد بررسی قرار دهیم. به نظر من بهترین روش حفظ امنیت، شناسایی و کشف حملات در حال اجرا و خنثی نمودن آن قبل از انجام هر کاری می‌باشد.

بعضی از افراد فکر می‌کنند که فناوری همیشه جوابگوی مشکلات بوده و ضامن حفظ امنیت آنان می‌باشد. به طور مثال همه به شبکه تلفن عمومی اعتماد کامل دارند در حالی‌که من به شما نشان می‌دهم که این امر چندان صحیح نیست.

در ادامه گفتگو، کوین شماره تلفن همراهم را از من پرسید. گوشی تلفن خودش که یکی از انواع گوشی‌های معمولی بود بیرون آورد و تعدادی دکمه را فشار داد. سپس از من سؤال کرد که دوست دارم چه شماره‌ای با من تماس بگیرد؟ من هم در جواب شماره تلفن مرکز اطلاعات تلفن نیویورک را اعلام کردم. وی دوباره چند دکمه دیگر را بر روی گوشی موبایل خود فشار داد. پس از چند ثانیه تلفن من به صدا درآمد و شماره مرکز اطلاعات تلفن را نشان داد. وقتی که به تلفن پاسخ دادم، کوین پشت خط بود.

در ادامه کوین توضیح داد که چگونه این کار توسط یکسری از کدهای XML که توسط خود وی نوشته شده‌اند صورت گرفته است و این‌که چگونه بسیاری از افراد و سیستم‌ها که فقط برحسب شماره تماس‌گیرنده به صحت تماس برقرار شده اطمینان می‌کنند در اثر این اعتماد غلط خود ممکن است مورد سوء استفاده قرار گیرند.