«بسمه‌تعالی»

آموزش مقابله با

مهندسی اجتماعی در هک

مترجمان:
ابوالفضل طاهریان دیزی
سمانه فلاح

انتشارات طاهریان

سرشناسه: میتنیک، کوین دیوید، ۱۹۶۳ -م.
Mitnik, Kevin David
نام و عنوان پدیدآور: آموزش مقابله با مهندسی اجتماعی در هک/[کوین دیوید میتنیک، ویلیام ال. سایمون]؛ مترجمان ابوالفضل طاهریان ریزی، سمانه فلاح.
مشخصات نشر: تهران: طاهریان، ۱۳۹۰ .
مشخصات ظاهری: ۲۲٤ ص.
شابک: ۹-۹۷-۰٦-۸٤-۹٦٤-۹۷۸ قیمت: ۷۰۰۰۰ ریال
وضعیت فهرست نویسی: فیپا
یادداشت: عنوان اصلی: The art of deception: controlling the human element of security, c2002.
موضوع: کامپیوترها - ایمنی اطلاعات
موضوع: تکنولوژی اطلاعات - جنبه‌های اجتماعی
موضوع: هکرها
شناسه افزوده: سایمون، ویلیام ال.، ۱۹۳۰ -م.
شناسه افزوده: Simon, William L.
شناسه افزوده: طاهریان ریزی، ابوالفضل، ۱۳۵۲-، مترجم
شناسه افزوده: فلاح، سمانه، ۱۳۶۳-، مترجم
رده بندی کنگره: الف۱۳۸۹ ۹٤م۴ک/QA ۷٦/۹
رده بندی دیویی: ۰۰۵/۸
شماره کارشناسی ملی: ۲۲۳۴۷۷۷

انتشارات طاهریان

«آموزش مقابله با مهندسی اجتماعی در هک»

● مترجمان: ابوالفضل طاهریان ریزی، سمانه فلاح
● ناشر: انتشارات طاهریان ● نوبت چاپ: اول ● سال چاپ: ۱۳۹۰ ● تیراژ: ۵۱۰۰ جلد
● لیتوگرافی: باران ● قیمت: ۸۰۰۰۰ ریال ● طرح جلد: آرزو خسروپور
شابک: ۹-۹۷-۸۴۰۶-۹۶۴-۹۷۸

آدرس: میدان انقلاب، خیابان کارگر جنوبی، خیابان لبافی نژاد، پلاک ۲۶۶، طبقهٔ چهارم، واحد ۱۱
تلفن: ۶۶۴۹۲۷۳۳ تلفکس: ۶۶۹۷۴۱۵۲

سفارش مستقیم از طریق وب سایت ما www.Taherianpress.com

مقدمه‌ای از یک دوست

بشر با یک گرایش درونی برای جستجو در طبیعت و ذات محیط اطراف، به دنیا آمده است. به عنوان دو انسان جوان، کوین میتنیک و من دربارهٔ جهان و اشتیاق به تأیید حوادث آن، شدیداً کنجکاو بودیم. ما اغلب در تلاش برای یادگیری موضوعات جدید مانند حل معماها و پیروزی در بازی بودیم. اما در همان زمان، جهان اطراف ما، قوانین رفتاری را که انگیزهٔ درونی را به سمت تحقیقات بی‌قید و شرط سوق می‌داد را یادآوری می‌کرد. بی‌باک‌ترین دانشمندان و پیشگامان در تکنولوژی، افرادی مانند کوین میتنیک هستند که با انگیزه‌های درونی، مهیج‌ترین موضوعات را ارائه می‌دهند و موفقیت در چیزهایی که قادر به انجام آن نیستند را میسر می‌سازند.

کوین میتنیک یکی از جالب‌ترین افرادی است که من می‌شناسم. از او پرسیدم و او بی‌درنگ پاسخ داد: مهندسان اجتماعی به عنوان افراد معتمد چه کاری انجام می‌دادند؟ اما کوینمیتنیک اشتیاقی برای مهندس اجتماعی شدن نداشت. حتی در زمانی‌که او یک مهندس اجتماعی بود. انگیزهٔ او چنین بود که اصلاً خود را توانگر نمی‌دانست تا به دیگران صدمه وارد سازد. در حالی‌که جنایات ویران کننده و خطرناک در خارج از آنجا وجود داشت. و حتی کسانی‌که به منظور ایجاد خسارات از مهندسی اجتماعی استفاده می‌کردند. در حقیقت، چرا کوین این کتاب را نوشت؟ برای هشدار به شما دربارهٔ دیگران.

این کتاب، چگونگی نیرنگ‌های کارمندان داخلی و پیش‌دستی همهٔ آنها برای حفاظت تکنولوژی را به آسانی نشان می‌دهد. اگر شما برای یک تجارت یا دولت کار می‌کنید، این کتاب یک چشم‌اندازی روشن برای کمک به فهم فعالیت‌های مهندسان اجتماعی را مهیا می‌کند و اینکه چطور می‌توانید آنها را خنثی کنید. با استفاده از داستان‌های در این کتاب که سرگرم‌کننده و هشداردهنده هستند کوین و همکار نویسندداش بیل‌سیمون ، روش‌ها و تکنیک‌هایی از مهندسی اجتماعی را می‌آورند. بعد از هر داستان، آنها نکات امنیتی عملی برای کمک به حفاظت شما بر علیه نفوذها و تهدیدات وصف شده را ارائه می‌دهند. تکنولوژی امنیت، شکاف‌های امنیتی را به افرادی مانند کوین را نشان می‌دهد. این کتاب را بخوانید و سرانجام ممکن است محقق شود که همهٔ ما به راهنمایی میتنیک و اطلاعاتش نیازمند هستیم.

استیو وزنیک یکی از موسسان شرکت Appel-هکر سابق

مقدمه:

بعضی از هکرها همهٔ فایل‌ها یا درایوهای مردم را خراب می‌کنند. آنها خرابکار نامیده می‌شوند. بعضی از هکرهای تازه‌کار زحمت یادگیری روش‌های تکنولوژی را به خود نمی‌دهند و فقط از ابزارهای لازم برای شکستن و ورود به سیستم‌های کامپیوتری استفاده می‌کنند. آنها نمایشنامه‌های کودکانه نامیده شده‌اند. بیشتر هکرهای باتجربه، مهارت‌های خود را از طریق برنامه‌های دیگر هکرها توسعه می‌دهند و آنها را برای وب و سیستم‌های پژوهشی و تبلیغاتی ارسال می‌کنند. افرادی هستند که به تکنولوژی علاقه‌ای ندارند و از کامپیوتر صرفاً به عنوان یک ابزار برای کمک در سرقت پول، کالاها یا خدمات استفاده می‌کنند. علی‌رغم داستان افسانه‌ای کوین میتنیک، من یک هکر بداندیش نیستم بلکه در حال سوق دادن خود در این مسیر هستم.

آغاز مسیر:

مسیر زندگی من خیلی زود مشخص شد. یک کودک شاد و خوش‌شانس ولی خسته، زمانی‌که پدرم از ما جدا شد من سه ساله بودم و مادرم به عنوان یک خدمتکار برای حمایت از ما کار می‌کرد. به نظر من بچه‌ای که فقط با مادر زندگی می‌کند و پرورش می‌یابد در طولانی مدت با همهٔ مسائل کنار می‌آید، گذشت زمان خیلی زود او را به ستوه می‌آورد و اندیشه‌های نامعقول دارد و دمدمی مزاج است و برای دیدن شخصیت درونی خویش ساعت‌ها در ذهن جستجو می‌کند. به طور خلاصه من پرستار خویش بودم. رشد و پرورش من در درهٔ فرناندو، فرصتی برای جستجو در لس‌آنجلس به من داد و در سن دوازده سالگی من راه مسافرت رایگان به سراسر منطقهٔ L.A را کشف کرده بودم. روزی متوجه شدم، هنگامی اتوبوس حرکت می‌کند که امنیت آن تأمین شده باشد. من یک بلیط مهر شده خریدم آن بلیط فقط برای آگاهی راننده از زمان حرکت و مسیر صادره شده بود. از یک رانندهٔ مهربان دربارهٔ محل تهیهٔ نوع خاصی از این مهرها سؤال کردم و او مرا راهنمایی کرد. بلیط‌ها اجازهٔ تغییر اتوبوس‌ها و امکان ادامهٔ سفر بر طبق مقصد شما را آسان می‌ساخت. اما من دربارهٔ چگونگی استفاده از آنها برای مسافرت به هر جایی که رایگان باشد، تحقیق کردم. دستیابی به یک بلیط خالی و بدون متن به سادگی قدم زدن در یک پارک بود. سطل‌های آشغال اتوبوس‌های ترمینال همیشه از تکه‌های کاغذ بلیط که رانندهها مچاله و سپس دور می‌ریختند، پر شده بود. من توانستم با استفاده از یک دفترچه یادداشت خالی و بدون مهر، بلیط‌های خودم را علامت برنم و به هر جایی که اتوبوس‌های L.A می‌رفتند، مسافرت کنم. بعد از یک مدت من تمام برنامهٔ حرکت اتوبوس‌ها را حفظ کردم (این یک مثال ساده از حافظهٔ توانای من برای حفظ اطلاعات بود، من هنوز هم می‌توانم شماره تلفن، کلمه‌های عبور و حتی جزئیات ناچیز رویدادهای کودکی‌ام را خیلی واضح به یاد بیاورم).

دیگر علاقهٔ شخصی من این بود که در همان سنین کودکی، کارهای جادویی و جذاب انجام دهم. زمانی‌که من روش حقه‌های جدید را یاد می‌گرفتم و تمرین می‌کردم و بعضی از تمرینات من باعث شد که من در این مسیر تا مرحلهٔ استادی پیش روم. تا جایی که کسب اطلاعات محرمانه دیگران را در اولویت کار خود قرار دادم.

دزدی از تلفن‌های عمومی تا هکر شدن:

اولین مواجههٔ من، یادگیری تماس گرفتن با مهندسان اجتماعی در طول دوران دبیرستانم بود. هنگامی‌که دانش‌آموزی که به دلیل دزدی از تلفن‌های عمومی، دستگیر شده بود را دیدم. دزدی از تلفن‌های عمومی نوعی از سرقت است که به شما اجازه می‌دهد سیستم شبکه‌های تلفن را خراب و از شرکت و کارکنانش بهره‌برداری کنید. او به من یاد داد که چگونه با استفاده از تلفن، دیگران را فریب دهم. مانند کسب هر اطلاعاتی از مشتریان، شبکهٔ تلفن و استفاده از شماره‌های محرمانه برای برقراری تماس رایگان با دورترین نقاط آن خیلی برایم آسان بود. من متوجه شدم که این شماره‌ها همیشه یکسان نیست. در حقیقت این تماس‌ها به حساب بعضی از شرکت‌های کم‌درآمد MCI، ثبت می‌شد.

این مقدمه‌ای برای مهندسی اجتماعی در دوران کودکی‌ام بود. دوستان من و دیگر سارقان تلفن‌های عمومی به من اجازه می‌دادند که به صحبت‌ها و مکالمه‌هایشان با شرکت‌ها گوش دهم. تمامی مکالمات آنها برای من قابل درک بود. من تلفن ادارات و شرکت‌های مختلف، زبان مخصوص و برنامه‌هایشان را یاد گرفتم. اما تربیت من در این راه زیاد طول نکشید و خیلی زود من همهٔ این فعالیت‌ها را برای خود انجام می‌دادم و حتی بهتر از معلمانم. این دوره از زندگی من تا سن پانزده سالگی به همین طریق سپری شد. در دبیرستان، بیشترین زمان را به کسب دسترسی بی‌اجازه به سوئیچ‌های تلفن و تغییر دستکاری سارق تلفن عمومی[1]، اختصاص دادم.

هنگامی که می‌خواستم از خانه با شرکت تماس بگیرم به ذهنم رسید که تماس با یک سکهٔ ده‌سنتی را کنار بگذارم زیرا سوئیچ‌های تلفن شرکت، ورودی‌ها را دریافت می‌کرد و نشان می‌داد که تماس از یک تلفن سکه‌ای است. من به هر چیز دربارهٔ تلفن مجذوب شدم نه فقط به استفاده ازآن بلکه الکترونیک، سوئیچ و کامپیوتر و همچنین با سازمان و برنامه‌ها و مجموعهٔ اصطلاحات آنها آشنا شدم. بعد از یک مدت، بیشتر چیزها دربارهٔ سیستم‌های تلفن را حتی بهتر از کارمندان آن می‌دانستم. و بالاخره مهارت مهندسی اجتماعی‌ام را گسترش دادم تا به سن هفده‌سالگی رسیدم. من قادر بودم دربارهٔ مخابرات تلفنی صحبت کنم. بعدها من با واژهٔ هکر به معنی شخصی که بیشترین سروکار را

---

[1]- Phone Phreak: شخصی است که از تلفن‌های عمومی بدون هیچ هزینه‌ای استفاده می‌کند (سارقان تلفن عمومی).

با سخت‌افزار و نرم‌افزار، دارد آشنا شدم. اما حالا این واژه یک کلمهٔ تحقیرآمیز و دربردارندهٔ معنای جنایت‌کار بداندیش است. من در این صفحات از این کلمه در مفهوم بی‌خطر استفاده کرده‌ام. بعد از دوران دبیرستان، کامپیوتر را در مرکز یادگیری کامپیوتر لس‌آنجلسیاد گرفتم. بعد از گذشت چند ماه، مدیر مدرسهٔ کامپیوتر متوجه شد که من علت آسیب‌پذیری در سیستم‌های عامل را می‌دانم و همهٔ امتیاز اداری شرکت IBM کامپیوترهای کوچک را به من داد. بهترین کارشناسان کامپیوتر هم نتوانستند کارهایی را که من انجام دادم، تشخیص دهند. زیرا فعالیت‌های من ساده‌ترین مثال از یک هکر بود و من یک تصور در ذهن داشتم که نمی‌توانستم به سادگی از آن بگذرم: انجام یک پروژهٔ ارزشمند برای افزایش امنیت کامپیوترهای مدرسه،یا ایجاد وقفه در سیستم‌های سرقتی هکرها. البته من انجام یک پروژهٔ شایسته را انتخاب کردم و تحقیقاتم را دربارهٔ آن کامل کردم.

مهندس اجتماعی شدن:

بعضی از مردم هر روز صبح با ترس و وحشت از کارهای روزمره‌شان از خواب بیدار می‌شوند. من به اندازهٔ کافی لذت در کارم داشتم که شما نمی‌توانستید رقابت، ارزش و اشتیاق مرا تصور کنید. من همهٔ ساعاتم را صرف تحقیقات شخصی‌ام می‌کردم.

من استعدادم را در اجرای هنری که مهندسی اجتماعی نامیده می‌شد، به کار گرفتم (کارهایی که به نظر مردم آن زمان خیلی عجیب بود و هزینه‌های زیادی را در بر داشت). برای من مهندس اجتماعی ماهر شدن کار سختی نبود و کسب‌وکار خانوادهٔ پدری من فروش زمین و کشتزار بود، بنابراین هنر نفوذ و تحریک و تشویق را از آنها به ارث برده بودم. زمانی که شما رفتار را با یک علاقه و تمایل برای فریب مردم ترکیب کنید، شما بهترین عامل عمده در مهندسی اجتماعی را دارید. بعضی از مردم که از نیرنگ و حقه در تجارت، استفاده می‌کنند و معمولاً اطلاعاتشان را هدف قرار می‌دهند و از روش‌های تخصصی بهره می‌گیرند که در نهایت همان مهندسی اجتماعی است. از زمان حقهٔ من دربارهٔ بلیط‌های اتوبوس و زمانی‌که برای تشخیص درست و غلط خیلی کوچک بودم من این فعالیت‌ها را آغاز کرده بودم و در خود استعدادی برای فهمیدن رازهای مردم را یافتم و در این راه هیچ تردیدی نداشتم و ندارم. من روی حافظه‌ام برای حقه و فریب دانستن زبان مخصوص طبقات خاص و توسعهٔ مهارت کلاهبرداری و دستکاری، کار کردم. روشی که من برای توسعهٔ حافظه‌ام استفاده کردم مهارت در کلک زدن بود. من این را کلک نامیدم، زیرا از طریق آن اطلاعات مردم را بدون اینکه بدانند به دست می‌آوردم، در فکر حقه‌های جادویی بودم، و آنها را تکرار می‌کردم. به زودی من متوجه شدم که می‌توانم هر اطلاعاتی را به طور صددرصد کسب کنم. من در شهادت‌هایم در کنگره قبل از نمایندهٔ مجلس سنای لیبرمن و تامسون در سال گذشته توضیح دادم و مسئولیت دسترسی به سیستم‌های کامپیوتری بعضی از بزرگترین شرکت‌ها را قبول کردم و در نفوذ به بعضی

از سیستم‌های کامپیوتری ارتجاعی توسعه یافته، موفق شدم. من از هر دو عامل تخصصی و علاقه برای کسب کد منبع، برای سیستم‌های عملیاتی متنوع و وسایل مخابراتی برای مطالعهٔ آسیب‌پذیری و فعالیت‌های درونی آنها استفاده کردم. همهٔ این کارها واقعاً حس کنجکاوی مرا راضی می‌کرد. برای دیدن و یا فهمیدن اطلاعات محرمانه دربارهٔ سیستم‌های عملیاتی، تلفن همراه و هر چیز دیگر که حس کنجکاوی‌ام را تحریک می‌کرد تلاش می‌کردم.

آخرین تصورات ذهنی:

من در این رابطه مهارت کسب کرده بودم زیرا پس از دستگیری در کارهای غیرقانونی متوجه شده بودم که باید قبل از تعرض به حریم خصوصی مردم دربارهٔ آن بیاندیشم. پیچیدگی فعالیت‌های خلاف قانون حس کنجکاوی‌ام را تحریک می‌کرد. من می‌خواستم دربارهٔ چگونگی کارکرد شبکه‌های تلفنی و امنیت ورودی و خروجی کامپیوترها بیشتر بدانم. من از دوران بچگی به انجام اعمال فریبنده برای تبدیل شدن به بدنام‌ترین هکر جهان که شرکت‌ها و دولت‌ها از آن هراس داشتند، علاقه داشتم. یعنی کار امروز من، بازتابی از سی سال پیش است. من پذیرفتم که بعضی از تصمیمات معدود و ناچیز را به وسیلهٔ حس کنجکاوی‌ام عملی کنم ، زیرا برای یادگیری تکنولوژی به یک رقابت عقلانی نیاز داشتم. اکنون من تغییر کرده‌ام. من در حال گسترش استعدادها و دانش وسیع خود هستم و اطلاعاتی را دربارهٔ امنیت و تکنیک‌های فنی مهندسی اجتماعی برای کمک به دولت، تجارت و مسائل فردی، کشف و مسئولیت برای تهدید امنیت اطلاعات، کسب کرده‌ام. این کتاب بیشتر از یک روش دربارهٔ اینکه من توانستم از تجربیاتم برای کمک به دیگران و تلاش برای فهم اطلاعات سارقان بداندیش و پلید در دنیا استفاده کنم، ارائه می‌دهد. من فکر می‌کنم که شما داستان‌های جالب و پندآموز زیادی را در این کتاب پیدا خواهید کرد.

این کتاب شامل اطلاعات مفید دربارهٔ امنیت اطلاعات و مهندسی اجتماعی است. فقط کافی است نگاهی گذرا به عناوین فصل‌آن داشته باشید. من در بخش یک ضعیف‌ترین عامل امنیت را افشا کردم و چگونگی حمله‌های مهندسی اجتماعی به عنوان مهمترین خطر برای شرکت‌ها را نشان دادم.

در بخش دو، روش مهندسی اجتماعی با تکیه بر جلب اعتماد، فواید همفکری و موافقت و زودباوری و ساده‌لوحی برای کسب هر آنچه که می‌خواهید را مشاهده می‌کنید. داستان‌های افسانه‌ای و موثر دربارهٔ اینکه مهندسی اجتماعی می‌تواند به هر شکل و صورتی تغییر یابد، اشاره خواهد کرد. اگر شما تصور می‌کنید که هرگز با این نیرنگ‌ها مواجه نمی‌شوید، بدانید در اشتباه بزرگی هستید. آیا شما یک طرح یا زمینه‌ای را که در آن تجربه کرده‌اید و یا قبلاً با مهندسی اجتماعی تماس داشته‌اید را تشخیص نمی‌دهید. اما زمانی‌که فصل دو، قسمت ۹ را خواندید، چگونگی کسب اطلاعات از شرکت‌های رده بالا با استفاده از روش مهندسی اجتماعی را خواهید دانست.

بخش سه، جایی است که فرازونشیب مهندسی اجتماعی. در داستان‌هایی که چگونگی ورود شما داخل فرضیه‌های منطقی یک شرکت را نشان می‌دهد. دزدی و سرقت اطلاعات محرمانه می‌تواند یک شرکت را نابود کند و مقادیر بالای تکنولوژی امنیت را از بین ببرد. طرح و نقشهٔ این بخش شما را از تهدیداتی که در تیررس انتقام کارمندان ساده برای ایجاد ترس و وحشت فیزیولوژیکی است، آگاه می‌کند. اگر شما می‌خواهید ارزش اطلاعاتی که در جریان تجارت مهم و جزئی از داده‌های محرمانه هستند، بدانید باید فصل ده قسمت چهارده از آغاز تا پایان را بخوانید. تمام مطالب این کتاب به استثنای مطالبی که دربارهٔ توضیح کیفیت و حکایت داستان‌های افسانه‌ای است، برای یادداشت‌برداری مفید هستند. در فصل چهار من دربارهٔ چگونگی ممانعت از حمله‌های موفق‌آمیز مهندسی اجتماعی روی سازمان‌ها و شرکت‌ها، بحث کرده‌ام. در فصل پانزده یک برنامهٔ کار دربارهٔ امنیت موفق، تهیه کرده‌ام و فصل شانزده یک سیاست امنیتی که شرکت شما برای حفظ و نگهداری اطلاعات نیاز دارد، ارائه می‌دهد. سرانجام من امنیت را در یک نگاه مهیا کرده‌ام. متنی شامل لیست‌ها و جدول‌ها و دستوراتی که اطلاعات راهنما برای کمک به دفع حملات مهندسی اجتماعی است. همچنین ابزارهایی که ارزش اطلاعات قابل استفاده در ایجاد برنامهٔ امنیت به کار می‌روند را نشان می‌دهد. به طور کلی در این کتاب به اطلاعات مفیدی در مورد مهندسی اجتماعی و کلمات فنی هکرهای کامپیوتری دست خواهید یافت. در جای جای کتاب پیام‌های میتنیک راهنمایی های مفیدی برای کمک به تقویت راهکارهای امنیت را ارائه می‌دهد و نوشته‌ها و مقالات کوتاه، زمینهٔ جالب یا اطلاعات جانبی را فراهم می‌کنند.

موفق باشید

فهرست: