گذار واژه‌ها؛ آیا راهی هست؟

توانگران

سیستم‌های امنیتی همواره عرصه مصالحه بوده‌اند. مصالحه میان هزینه‌ای که نفوذگر باید بپردازد (زمانی که صرف می‌کند، یا خطری که می‌پذیرد) و دارایی (ثروت، قدرت یا اطلاعاتی) که به دست می‌آورد. هیچ سیستم صددرصد امنی وجود ندارد. اما نفوذ به هر سیستمی هم به اندازه ارزش چیزی که از آن محافظت می‌کند، باید سخت‌تر باشد.

یک بانک هیچ‌گاه برای تامین امنیت گاوصندوقش از قفل‌های آویز معمول بازار استفاده نمی‌کند و هیچ‌کس هم برای بستن در کیف دستی‌اش از قفل زمان‌دار سه محوری استفاده نخواهد کرد. اکنون سؤال این است که ارزش دارایی‌های دیجیتال شما چقدر است؟ یا به عبارت ساده‌تر گذرواژه‌ها و سیستم‌های امنیتی شما از چه چیزی محافظت می‌کنند؟

ارزش حساب‌کاربری ایمیل‌های شما چقدر است؟ حساب‌تان در شبکه‌های اجتماعی چطور؟ آیا فکر می‌کنید فقط باید از حساب‌های آنلاین بانکداری‌تان محافظت کنید؟ به احتمال زیاد شما هم داستان هک شدن حساب‌های کاربری مت هونان (نویسنده وایرد که اتفاقا نویسنده یکی از مقالات همین پرونده نیز هست) و نابود شدن زندگی دیجیتالش ظرف کمتر از دو ساعت را خوانده‌اید(شرح این داستان در مقاله «تا جهنم و بازگشت» در شماره ۱۳۷ ماهنامه شبکه منتشر شده است). اگر جذابیت یک نام کاربری سه‌حرفی مثلا @mat را در یک کفه ترازو و هر آن‌چه شما در دنیای آنلاین و ابری‌تان ذخیره کرده‌اید، را در کفه دیگر بگذاریم، به نظر شما کدام کفه سنگین‌تر خواهد بود؟

گمان می‌کنم که شما هم به این نتیجه برسید که خطر چندان هم دور نیست. به عبارت دیگر همه ما «ثروتمندانی بالقوه» هستیم که باید از ثروت خود در برابر مهاجمان محافظت کنیم. آن هم مهاجمانی که هزینه حمله و تلاش برای نفوذ روز به روز برای‌شان کمتر می‌شود.

زنجیر

قدرت یک زنجیر همواره به اندازه ضعیف‌ترین حلقه آن است و تا کنون تصور بر این بود که در حوزه امنیت سیستم‌ها، به‌خصوص انواع دیجیتالش، این انسان است که ضعیف‌ترین حلقه زنجیر را می‌سازد. اما به نظر می‌رسد که این ادعا دیگر اعتبار چندانی نداشته باشد. تا پیش از این سیاست‌های غلط در انتخاب، نگهداری و استفاده از گذرواژه‌ها عامل اصلی انواع هک‌ها و لورفتن اطلاعات بود. اما اکنون نقطه‌ضعف سیستم بنیان و شالوده اصلی آن است. اینترنت و فضای آنلاین موجودی در حال تکامل است و مدام فرم عوض کرده

و جنبه‌های گوناگونش در هم می‌پیچد و ترکیب‌های جدیدی به‌وجود می‌آورد. در این میان اما اصول حفاظت از اطلاعات و حساب‌های کاربری هنوز هیچ تغییری نکرده است.

کلیت سیستم این‌گونه است که شما برای حساب‌های کاربری‌تان گذرواژه‌ای تعیین می‌کنید. اگر آن را ساده انتخاب کنید، قابل حدس زدن خواهد بود و اگر آن را دشوار در نظر بگیرید به‌یاد آوردن آن برای خودتان هم دشوار خواهد بود. پس به عنوان چاره‌ای برای روز مبادا، حساب کاربری دیگری می‌سازید تا پشتیبان گذرواژه شما باشد و بعد حساب دیگری برای پشتیبانی از حساب دوم و بعد... .حلقه آخر این زنجیر در واقع ضعیف‌ترین حلقه و محل نفوذ است. یعنی حسابی که شما برای بازیابی گذرواژه آن به جای یک حساب‌کاربری پشتیبان به داده‌هایی از دنیای واقعی (مثلا آدرس پستی، شماره تامین اجتماعی، پلاک خودرو، شماره کارت اعتباری) تکیه می‌کنید. اینجا است که هم شما و هم شرکتی که به شما خدمات می‌دهد، فراموش می‌کنید که در دنیای کنونی ما «حریم خصوصی» کم‌و بیش مرده است. تلفن، آدرس، شماره خودرو، نام دوستان و بسیاری از موارد خصوصی دیگر، اکنون به لطف شبکه‌های اجتماعی و بانک‌های داده آنلاین به راحتی در دسترس همگان است. پس از خواندن مقالات این پرونده، شما هم به این نتیجه خواهید رسید که اعتماد تنها به رشته‌ای حداکثر ۲۰ حرفی از کاراکترها برای محافظت از دارایی‌های آنلاین ما چندان عاقلانه نیست. زیرا اگر قابل شکستن نباشد، با انواع تکنیک‌های مهندسی اجتماعی قابل بازنشانی خواهد بود.

گردباد

هرچه دنیای ما بیشتر به ابزارها و فناوری‌های الکترونیک وابسته می‌شود، مجبور می‌شویم اطلاعات حساب‌های کاربری بیشتر و بیشتری را نگهداری کنیم. هرچه تعداد حساب‌های کاربری‌مان بیشتر شود، سیاست‌های ضعیف‌تری را برای ایجاد، حفظ و نگهداری و تعویض منظم گذرواژه‌های آن‌ها در پیش خواهیم گرفت. هرچه دقت ما در این زمینه کمتر شود، آمار نفوذ به حساب‌های کاربری بالاتر خواهد رفت. اما بدترین نکته قسمت آخر این توالی است. هرچه حساب‌های بیشتری لو برود، کار نفوذگران ساده‌تر شده و با داده‌ها و الگوهای به دست آمده الگوریتم‌های شکستن رمزهای عبور قدرتمندتر می‌شوند. گردبادی پیش روی ما است که هرچه بیشتر می‌بلعد، قدرتمندتر می‌شود و به راستی مشخص نیست کجا و چگونه فرو خواهد نشست.

هابیل و قابیل

اما آیا همه این تمهیدات لازم است؟ اگر همه ما می‌توانستیم متعهد شویم که به حریم خصوصی دیگران سرک نکشیم، از جیب دیگران پول برنداریم و از اطلاعاتی که از آن‌ها داریم سوءاستفاده نکنیم، به هیچ کدام از این تمهیدات نیازی نبود.

سه دهه پیش اینترنت بر اساس مشارکت جمعی انسان‌ها پایه‌ریزی شد. موجودی به وجود آمد که هیچ متولی و صاحبی نداشت. سازندگان آن همان استفاده‌کنندگانش بودند. برقراری امنیت، مسیریابی، صدور مجوزهای تایید صلاحیت و اعتبارسنجی در آن به افراد و شرکت‌هایی سپرده شد که ما آن‌ها را قابل اعتماد فرض کرده و می‌کنیم. اما داستان خلقت نشان می‌دهد که بزه‌کاری از ابتدای تاریخ همراهی جداناشدنی بوده است. حتی اگر شما بهترین شیوه‌های رمزنگاری و قدرتمندترین سیاست‌های انتخاب و مدیریت گذرواژه‌ها را اتخاذ کنید، کافی است شرکت صادرکننده مجوزهای امنیتی (درست مثل اتفاقی که یکی دو ماه پیش برای گوگل رخ داد) مجوزهای اشتباهی را صادر کند، تا تمام ارتباطات مثلا رمزنگاری‌شده شما توسط شخص ثالث و به احتمال زیاد نامربوطی شنود شود.

داستان تنها توجه و دقت شما نیست، کل بستر و جامعه درگیر اینترنت به بازنگری در سازوکارهایشان نیاز دارند.

پرونده

شاید به این فکر افتاده باشید که راه‌حل چیست؟ این احتمالا سؤالی است که حتی با خواندن دو مقاله این پرونده هم جواب مستقیمی برای آن نخواهید یافت. مسئله این است که هدف ما از این پرونده طرح مشکل و نه حل آن بوده است. در مقاله اول این پرونده خواهید دید که چگونه شکستن و یافتن گذرواژه‌ها با تلاش‌های کور روز به روز ساده‌تر و سریع‌تر می‌شود. در مقاله دوم هم خواهید دید که اگر گذرواژه‌ای با این روش‌ها قابل شکستن نباشد، با تکنیک‌های مهندسی اجتماعی قابل بازنشانی است. معضل امنیت تنها با تلاش و سیاست‌گذاری ما کاربران قابل حل شدن نیست. اما امیدواریم دانستن این نکات و ضعف‌ها حساسیت شما را برانگیخته و شما در زمان وقوع آن نفوذ عظیم زندگی‌تان یاری کند.