حملات سایبری و آسیب‌پذیری گذر واژه‌ها

اگر عبارت «حمله سایبری به گذرواژه» را در موتور جستجوی وبگاه «گوگل نیوز» تایپ کنیم، نتایج جستجو نشان خواهند داد مجرمین سایبری با چه تناوبی یعنی هرچند وقت یک‌بار داده‌های مهم شرکت‌ها و افراد را می‌ربایند. گذرواژه‌های ضعیف بخش بزرگی از مشکل هک شدن است. برای مثال، در سال ۲۰۲۳ یک شرکت امنیت فناوری به نام «نوردپَس» (Nordpass) گزارش کرد که «۱۲۳۴۵۶» متداول‌ترین گذرواژه در نیجریه و دومین گذرواژه پرکاربرد در تمامی دنیا است.

با افزایش حملات سایبری که منجر به نفوذ به سیستم‌های رایانه‌ای و نشت داده‌ها شده‌اند، بازبینی و تجدیدنظر روی راهبردهای کنترل دسترسی اجتناب‌ناپذیر به نظر می‌رسد. برای مثال، در سال ۲۰۲۳ تعداد حملات سایبری به صاحبان تجارت و کسب‌وکار در آفریقای جنوبی، کنیا و زامبیا ۷۶ درصد افزایش یافت.

گذر واژه‌ها و نام‌های کاربری همچنان مانند گذشته آسیب‌پذیر هستند؛ چون هنوز برای دسترسی به ایمیل، حساب کاربری و احراز هویت از آن‌ها استفاده می‌شود. عده بسیار زیادی از افراد گذر واژه‌هایی با امنیت پایین یا گذرواژه‌هایی که قبلاً استفاده شده‌اند را انتخاب می‌کنند.

سالانه منابع مختلف فهرستی از پرکاربردترین گذر واژه‌ها را منتشر می‌کنند. طبق تحقیق انجام شده توسط نوردپس، گذرواژه‌های قابل پیش‌بینی که اغلب کاربرها انتخاب می‌کنند مانند admin ،۱۲۳۴۵۶، ۱۲۳۴۵۶۷۸ و خود واژه‌ی password هستند. هکرهای بسیار ماهر و افرادی که مهارت‌های اولیه هک کردن را یاد گرفته‌اند می‌توانند این گذرواژه‌ها را در کمتر از یک دقیقه کرَک کنند. در نتیجه، اطلاعات محرمانه در معرض سرقت، حذف، تغییر و تحریف قرار می‌گیرند. ابزارهای هوش مصنوعی یکی پس از دیگری کار هکرها را آسان‌تر می‌کنند.

در برخی سازمان‌ها، گذر واژه‌ها منقضی نمی‌شوند و این فرصت‌هایی را برای افراد سودجو فراهم می‌آورد تا به اطلاعات سایرین دسترسی پیدا کنند. در بسیاری موارد، گذر واژه‌ها در معرض «سرقت هویت آنلاین» قرار می‌گیرند. امکاناتی که وب‌سایت‌ها هنگام ایجاد حساب کاربری جدید برای ذخیره گذرواژه ارائه می‌دهند نیز راه‌حل عاری از عیبی نیستند؛ درست است که این ویژگی ورود به وب‌سایت‌ها را برای کاربرها آسان می‌کند اما احتمال این که گذرواژه‌ها در دسترس شخص ثالث قرار گیرند را افزایش می‌دهد.

بنابراین لازم است برای حفظ امنیت گذرواژه‌ها و اطلاعات شخصی افراد سیاست‌ها و استانداردهای مربوطه تنظیم شوند و به اجرا درآیند تا اهداف شرکت تأمین‌کننده امنیت سایبری محقق شوند. نحوه انجام این کار به سازمان مورد نظر و نوع کسب‌وکار بستگی دارد. برای مثال، موسسه‌های مالی و شرکت‌های صادرکننده کارت اعتباری، «استاندارد امنیت داده صنعت پرداخت کارت» (PCIDSS) را مناسب‌ترین گزینه می‌دانند که یک استاندارد امنیت اطلاعات برای سازمان‌هایی است که تراکنش‌های کارت‌های اعتباری عمده ازجمله ویزا، مسترکارد، امریکن اکسپرس، دیسکاور و جی‌سی‌بی را پردازش می‌کنند. این استاندارد به‌منظور بالا بردن میزان کنترل روی داده‌های دارنده کارت و کاهش جعل کارت‌های اعتباری ایجاد شده است.

برخی نیز راهنمایی‌ها و توصیه‌های «مؤسسه ملی فناوری و استانداردها» (NIST) یا استانداردهای امنیتی ایزو/آی ای سی ۲۷۰۰۱ را کافی و سودمند می‌دانند. این استانداردها در سراسر دنیا مورد استفاده هستند.

وظیفه شرکت‌های فناوری در حفظ امنیت گذرواژه‌ها

شرکت‌ها باید اطمینان حاصل کنند که کارکنانشان به‌طور کامل از سیاست‌ها و روندهای مرتبط با استفاده از گذرواژه و نیز از مسؤولیت‌های خود آگاهی دارند. بنابراین لازم است به‌طور مداوم کمپین‌های آگاهی‌دهنده برگزار کنند تا اقدامات لازم برای انتخاب گذرواژه‌های امن را ترویج دهند و با تهدیدهایی که امنیت گذرواژه‌ها را به خطر می‌اندازند مقابله کنند. همچنین باید بهترین استانداردهای امنیتی به‌منظور مدیریت حساب‌های کاربری و کنترل گذرواژه‌ها را اتخاذ کرده و تابع آن‌ها باشند. دیگر این‌که باید روش احراز هویت چندعاملی را به کار گیرند؛ چون در این روش تأیید هویت کاربر با ارائه دو یا چند شاهد اثبات‌کننده هویت امکان‌پذیر می‌شود. برای مثال، کاربرها را ملزم به استفاده از گذرواژه و سیستم تشخیص چهره یا تشخیص شبکیه چشم کنند. علاوه‌براین، باید اطمینان حاصل کنند که فایل‌های حاوی ذرواژه‌ها رمزگذاری‌شده هستند.

نبایدهایی برای کاربرها

کاربرها نباید گذرواژه‌های کوتاه را انتخاب کنند. گذر واژه‌های انتخابی آن‌ها نباید کمتر از ۱۲ حرف باشند و باید از ترکیب حروف الفبا، اعداد، علائم، حروف بزرگ و حروف کوچک تشکیل شده باشند. مهم‌تر این‌که باید آن‌ها را محرمانه نگه دارند.

کاربرها نباید از یک گذرواژه برای ورود به چند حساب کاربردی استفاده کنند.

نباید گذرواژه خود را در وب‌سایت‌ها ذخیره (save) یا از گزینه auto-fill استفاده کنند؛ به‌خصوص اگر رایانه به‌طور مشترک با افراد دیگر استفاده می‌شود.

نباید از گذرواژه مشترک استفاده کنند یا آن را به سایرین به‌ویژه همکاران در محل کار اعلام کنند. اگر ناچار هستند با فرد یا افراد دیگری یک گذرواژه مشترک داشته‌باشند باید مطمئن شوند که مدیر یا رئیس اداره از این موضوع باخبر است.

نباید جزئیات گذرواژه خود را بدون صحت‌سنجی پشت تلفن به افرادی بدهند که ادعا می‌کنند تکنسین فناوری اطلاعات (IT) هستند.

چند راه برای اطمینان از این‌که تماس دریافتی اعتبار و صحت دارد به کاربرها پیشنهاد می‌شود: یکی از آن راه‌ها به‌ویژه اگر برای دسترسی به رایانه مشکلی ندارند این است که از فرد تماس‌گیرنده بخواهند یک ایمیل رسمی به‌حساب کاربری آن‌ها ارسال کند. اگر فرد تماس‌گیرنده با شماره تلفن اینترنتی تماس گرفته است، صحت تماس را چک کنند. همچنین باید مشخصات فرد تماس‌گیرنده از قبیل نام، محل دفتر کار، اداره یا سازمان را از او بخواهند.

توصیه‌هایی به کاربرها برای مراقبت از گذر واژه‌ها

هر کدام از کاربرها به‌نوبه خود می‌توانند امنیت محیط آنلاین خود را هم در محل کار و هم در زندگی خصوصی بالا ببرند. کافی است تمامی مدت مراقب و گوش‌به‌زنگ باشند و خود را از تازه‌ترین تهدیدهایی که ممکن است امنیت گذرواژه آن‌ها را به مخاطره بیاندازند مطلع نگه دارند. اگر افراد در محیط‌های اداری و سازمانی کار می‌کنند باید چند نکته را برای حفظ گذرواژه خود به خاطر بسپارند.

نخست این‌که از سیاست‌ها و استانداردهای سازمانی برای استفاده ایمن از گذرواژه مطلع باشند. دوم، در جلساتی که برای آگاهی و آموزش دادن برگزار می‌شوند شرکت کنند. سوم، هرگونه اتفاق امنیتی مشکوک را گزارش کنند. همچنین حتماً باید اطلاعات login خود را امن و دور از دسترس نگه دارند و پس از اتمام کارشان logout کنند؛ به‌ویژه اگر از رایانه مشترک استفاده می‌کنند. دیگر این‌که ضروری است گذرواژه‌ای مستحکم انتخاب کنند به‌طوری که افراد مهاجم نتوانند آن را حدس بزنند. به‌علاوه، نباید از حروفی که به ترتیب هستند یا عبارات تکراری به‌عنوان گذرواژه استفاده کنند. باید از گذر واژه‌هایی مثل واژه‌های لغتنامه که به‌راحتی حدس زده می‌شوند نیز اجتناب کرد. هر وقت کاربرها به عدم امنیت گذرواژه خود مظنون می‌شوند، باید آن را تغییر دهند و سرانجام این‌که توصیه می‌شود از ابزارهای مدیریت گذرواژه رمزگذاری‌شده کمک بگیرند تا گذرواژه‌های خود را با امنیت ذخیره کنند.