Ouch! ژانویه 2023

SANS SECURITY AWARENESS

OUCH!

ماهنامه آگاهی از امنیت اطلاعات برای شما

احراز هویت بایومتریک - امنیت را ساده کنید

مقدمه

آیا از رمزهای عبور متنفر هستید؟ آیا از ورود مداوم به وب سایت های جدید خسته شده اید یا نمی توانید همه رمزهای عبور پیچیده خود را به یاد بیاورید؟ آیا از لزوم ایجاد رمزهای عبور جدید برای حساب‌های جدید یا تغییر رمزهای عبور قدیمی برای حساب‌های موجود خودتان ناامید شده‌اید؟ ما خبرهای خوبی برای شما داریم. راه حلی به نام بایومتریک وجود دارد که کمک می کند امنیت سایبری برای شما آسان تر شود. در زیر توضیح می‌دهیم که احراز هویت بایومتریک چیست، چگونه زندگی شما را ساده‌تر کرده و به چه دلیل بیشتر از قبل آنها را مشاهده و از آنها استفاده خواهید کرد.

در ابتدا، چرا رمزهای عبور؟

رمزهای عبور بخشی از چیزی به نام احراز هویت هستند، فرآیند اثبات اینکه شما کی هستید. معمولاً دو چیز وجود دارد که می توانید برای اثبات هویت خود ارائه دهید: چیزی که می دانید (مانند رمزهای عبور) و چیزی که دارید (مانند کارت عابر بانک یا دستگاه تلفن همراه تان). احراز هویت به طور سنتی با رمزهای عبور انجام می شود. رمزهای عبور در ابتدا به دلیل اینکه یکی از آسانترین راهکارهای احراز هویت کاربردی بودند مورد استفاده قرار گرفتند. با این حال، در طول سال‌ها، زندگی های ما با وجود حسابهای کاربری فراوان، به شکلی که هیچکس انتظار نداشته، پیچیده تر شده است. این بسیار عادی است که یک فرد در کار یا زندگی شخصی خود بیش از 100 رمز عبور داشته باشد.

علاوه بر این، مهاجمان سایبری در حدس زدن، سرقت یا شکستن (هک) رمزهای عبور بسیار خوب عمل کرده اند. به همین دلیل است که قوانین زیادی در مورد رمزهای عبور مشاهده می کنید، مانند طولانی کردن آنها (که حدس زدن آنها دشوارتر شود) و استفاده از یک رمز عبور منحصر به فرد برای هر حساب (که اگر یکی از حساب های شما هک شود، حساب های دیگر شما همچنان امن باقی بمانند). مشکل الزامات فراوان رمز عبور این است که آنها امن بودن سایبری را دشوارتر می کنند. مدیران گذرواژه به طور چشمگیری کمک حال مان هستند زیرا آنها همه رمزهای عبور شما را به صورت ایمن به خاطر می آورند و شما را به وب سایت مورد نظرتان وارد می کنند، اما آیا راه بهتری وجود دارد؟ اینجاست که بایومتریک می‌تواند با ارائه یک چیز سوم برای اثبات هویت شما کمک کند - چیزی که هستید.

بایومتریک ها

مانند رمزهای عبور، احراز هویت بایومتریک راه دیگری برای اثبات اینکه چه کسی هستید میباشد. تفاوت آن دراین است که به جای اینکه مجبور باشید چیزی را به خاطر بسپارید (مثل رمزهای عبور) از عنصری که در اختیار دارید برای اثبات هویت خود استفاده کنید، مانند استفاده از اثر انگشت برای دسترسی به تلفن خودتان.

بایومتریک بسیار ساده‌تر است، زیرا لازم نیست چیزی را به خاطر سپرده یا تایپ کنید، فقط با استفاده از چیزی که هستید احراز هویت می‌کنید. انواع مختلفی از احراز هویت بایومتریک وجود دارد مانند صدای شما، نحوه راه رفتن یا اسکن چشمی شما . با این حال، اثر انگشت و تشخیص چهره دو مورد رایج هستند، به خصوص برای دستگاه های تلفن همراه. در حالی که بایومتریک مزایای بسیار زیادی دارد، معایبی نیز دارد، یکی از بزرگترین معایب آن این است که اگر اثر انگشت یا چهره شما توسط مهاجمان سایبری کپی برداری شده باشد، نمی توانید آنها را تغییر دهید.

کلیدهای عبور

در ماه‌ها و سال‌های آینده، باید شاهد جایگزینی رمزهای عبور با بایومتریک‌ها و با فناوری جدیدی به نام کلیدهای عبور(Passkeys) باشید. این فناوری توسط مایکروسافت، اپل و گوگل پذیرفته شده است و به زودی و با گذشت زمان باید شاهد استفاده از آن در وب سایت های بیشتری باشید. کلیدهای عبور جایگزین رمزهای عبور می شوند و به شما این امکان را می دهند که با استفاده از بایومتریک همراه با دستگاه تلفن همراه خود ثابت کنید که چه کسی هستید. هنگامی که یک حساب کاربری در یک وب سایت (مانند Google یا Apple) ایجاد می کنید به جای ایجاد رمز عبور، دستگاه تلفن همراه خود را ثبت می کنید. در ادامه، با احراز هویت با دستگاه تلفن همراه خود با استفاده از بایومتریک، مانند اثر انگشت یا تشخیص چهره، وارد آن وب سایت می شوید. وب‌سایت به دستگاه تلفن همراه شما اعتماد داشته و دستگاه تلفن همراه تان با استفاده از بایومتریک هویت شما را تائید میکند. علاوه بر این، اطلاعات بایومتریک شما (اثر انگشت یا چهره) به هیچ وبسایتی ارسال نخواهد شد. درعوض، بایومتریک شما به صورت محلی و امن در دستگاه شما ذخیره می شود. این فقط برای باز کردن قفل "Passkey" استفاده می شود، یک کلید منحصر به فرد، ایجاد شده برای هر سایت، که دستگاه شما در حالی که از داده های بایومتریک شما محافظت می کند، به سایت ارسال می کند. در حالی که هیچ راهکاری کامل و بدون نقص نیست، بایومتریک و راه حل‌هایی مانند Passkeys می‌توانند به حفظ امنیت شما و در عین حال ساده‌سازی امنیت کمک کنند.

سردبیر مهمان

دکتر یوهانس اولریچ رئیس تحقیقات کالج موسسه فناوری SANS است. او با بیش از 20 سال تجربه در صنعت، در حال حاضر تهدیدات فعلی را با راه اندازی مرکز طوفان اینترنت SANS نظارت می کند. او SEC522 (امنیت برنامه های وب) و SEC503 (تشخیص نفوذ) را تدریس می کند.

آدرس توئیتر: @johullrich & آدرس لینکدین: https://www.linkedin.com/in/johannesullrich

منابع

برنامه های مدیریت رمز عبور: https://www.sans.org/newsletters/ouch/password-managers

توضیحات بیشتر درمورد کلیدهای عبور: https://www.sans.org/blog/what-is-phishing-resistant-mfa

ترجمه شده برای عموم توسط: مجید هدایتی، هومن خجاو