Ist das P.ass7wort= ein Auslaufmodell? Chester Wisniewski von Sophos über die Rolle der Technikriesen, Umdenken beim User und sein Ideal

Passwörter gehören zu unserem Leben und jeder hat mittlerweile sein eigenes System entwickelt. Manche nutzen Algorithmen, sämtliche Namen ihrer Vorfahren, kryptische Zahlenkombinationen oder übergeben diese Aufgabe einem nüchternen Passwort-Manager. Chester Wisniewski, Principal Researcher bei Sophos gibt Einblicke in eine Welt ohne Passwort. Leider dauert das noch.

Das größte Problem mit Passwörtern? Sie werden zu leicht kopiert, gestohlen und vergessen. Ein wirklich gutes Passwort ist immens schwer zu merken. Zudem brauchen wir einfach zu viele davon. Sie müssen also immer wieder „neu“ und doch zu merken sein.

Diese Schwierigkeiten sind bekannt und Unternehmen arbeiten bereits an anderen Modellen, zum Beispiel an einer simpleren Authentifizierung und Überprüfung von Nutzeridentitäten. Diese Lösungen werden sich allerdings voraussichtlich erst in der Zukunft gegen das „altmodische“ Passwort durchsetzen. Wichtig ist, dass viele der Technologieriesen die Forschung nach solchen Alternativen unterstützen. Microsoft, Google, Facebook, Apple, Twitter oder Wordpress bieten ihren Anwendern bereits einfachere Authentifizierungstechnologien an.

Die Tech-Konzerne müssen Pionierarbeit leisten
In den nächsten 18 bis 36 Monaten werden die meisten großen Cloud-Anbieter wahrscheinlich die Migration zu einer eher passwortlosen Phase vornehmen. Das hängt aber davon ab, wie die Nutzer sich an die neuen Methoden gewöhnen, oder auch gewöhnen müssen. Da viele dieser Dienste werbefinanziert sind, sind naturgemäß Widerstände gegen Änderung zu erwarten, man sieht sich dann nach anderen Anbietern um. Deswegen müssen die größten Anbieter für diesen Wandel Pionierarbeit leisten und geschlossen vorangehen, um die Menschen von den neuen Modellen jenseits des klassischen Passworts zu überzeugen.

Wie könnte eine Welt ohne Passwörter aussehen?
Im Idealfall ist der neue Ansatz etwas Bekanntes, ähnlich wie ein Passwort. Denkbar wäre ein einziges komplexes Gebilde oder eine kurze PIN plus etwas Haptisches, wie ein USB-/ Bluetooth-Token oder ein Telefon, wenn man sich über den PC anmeldet.
Das Entscheidende ist: es muss sichergestellt werden, dass das vom Nutzer verwendete Tool nicht verwendet werden kann, ohne dass es vom Anwender aktiv „entsperrt“ wird. Das bedeutet aber auch – und das ist zugleich das größte Problem dieses Modells – dass man eine Art Gerät besitzen muss, um die Sicherheit zu erhöhen. Schwierig wird es dann nämlich bei Verlust des technischen Helferleins, beziehungsweise es muss immer und überall mit dabei sein – das uralte Spannungsverhältnis von komfortabel und sicher.

Die Verbesserung der Benutzerfreundlichkeit muss hier unbedingt im Vordergrund stehen, um die Vorteile einer Passwortfreiheit nutzen zu können. Es ist aber davon auszugehen, dass die Akzeptanz durch die Erleichterung der Login-Prozesse zunehmen wird. Eine Vorbildrolle kommt dabei den großen Anbietern wie Google und Facebook zu, die mit einer proaktiven Herangehensweise die öffentliche Akzeptanz beschleunigen können, indem sie zeigen, dass die Alternativen zu Passwörtern sicherer und einfacher sind. Dann gelingt der Wandel.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de