Digitalisierung / IT-Sicherheit VII

Warum es ohne Passwort am sichersten ist

Wer Phishing-Übergriffe vermeiden will, sollte menschliches Fehlverhalten eliminieren. Konkret bedeutet das, bei der Multifaktorauthentifizierung die Passwörter wegzulassen. Stattdessen helfen betrugssichere Passkeys, den Cyberkriminellen das Handwerk zu legen.

› Patrick Trevisan, Fabian Mauricio

Phishing gehört zu den häufigsten Cyberangriffsmethoden weltweit, und das auch in der Schweiz. Dabei werden den nichts ahnenden Nutzern Zugangsdaten für Benutzerkonten im Internet oder des Unternehmens entlockt.

Einmal erwischt, können sensible Informationen wie Kreditkarten- oder Zugangsdaten zu Online-Accounts oder ins Unternehmenswerk abgegriffen, Unternehmensinformationen gestohlen oder manipuliert und Nutzeraktivitäten ausspioniert werden.

Aus diesem Grund gehört neben dem eigentlichen Schutz der Benutzerkonten die Sensibilisierung der Mitarbeitenden zu den wichtigsten Massnahmen im Kampf gegen Cyberkriminalität. Mitarbeitende wissen denn auch zwar meistens, dass sie Passwörter verwenden sollen, die schlecht nachvollzogen und gehackt werden können. Auch IT-Sicherheitsverantwortliche kennen die Notwendigkeit der Multifaktorauthentifizierung.

Dabei wird in der Regel zusätzlich zu einem Benutzernamen und dem Passwort ein weiterer Faktor wie ein Einmal-Code aus Ziffern, ein QR-Code oder eine Authenticator-App verlangt.

Auf Passwörter verzichten

Leider sind solche per Push-Nachricht, SMS oder E-Mail versandten Codes für die Mehrfaktor-Authentisierung nach wie vor unbeliebt, teilweise ist das Verfahren zeitaufwendig. Ausserdem können solche Methoden auch dazu führen, dass Nutzende von ihren Konten ausgesperrt werden, wenn das Smartphone verlustig geht.

Alles in allem führt das oft dazu, dass eine Zweifaktorauthentifizierung möglichst einfach gehalten wird (unsichere Passwörter inklusive) – und damit zwangsläufig die Kontosicherheit leidet. Zweifaktorauthentifizierungsmethoden bilden ausserdem keinen Schutz vor Phishing.

Denn solange Informationen von Menschen für den Zugang zu einem Konto eingegeben oder übertragen werden müssen, können diese auch fälschlicherweise Betrügern in die Hände geraten. Deswegen gilt es, zwischen Sicherheit und Benutzerfreundlichkeit abzuwägen und eine verlässliche Alternative zur herkömmlichen Absicherung der Konten in Betracht zu ziehen.

Weil Menschen mit der irrtümlichen Weitergabe von Passwörtern Fehler machen können, ist es aber eigentlich besser, den Menschen ganz aus der Gleichung zu entfernen und auf Passwörter zu verzichten.

Kompliziert oder unsicher

Passwörter richtig zu verwenden, ist umständlich. Deshalb setzen viele Nutzer lieber auf kürzere, unsichere Passwörter statt sichere. Nach wie vor ist es sogar üblich, dass für viele Zugänge dasselbe Passwort verwendet wird. Hinzu kommt, dass Passwörter mit Phishing in Erfahrung gebracht werden können. Cyberangriffe beginnen denn auch oftmals mit einem breit angelegten Auswerfen der «Phishing-Netze» auf alle Mitarbeitenden. Es genügt, wenn nur jemand auf den Versuch hineinfällt und sein Passwort fälschlicherweise auf einer getürkten Webseite eingibt. Einmal in der Unternehmens-IT eingeloggt, können die Cyberkriminellen zur nächsten Phase übergehen, Daten stehlen oder verschlüsseln, Schadsoftware installieren, Systeme zerstören und vieles mehr.

Auch bieten Passwort-Manager und Ähnliches keine Hilfe. Sie erlauben zwar, Passwörter sicher zu verwalten und zu

verschlüsseln. Einen wirklichen Schutz gegen Phishing bieten sie allerdings auch nicht. Selbstverständlich gibt es auch die Möglichkeit, mit Zertifikaten zu arbeiten. Diese mit Verschlüsselung funktionierenden Verfahren ermöglichen es, zum Beispiel Personen oder auch Webseiten eines Unternehmens zu authentifizieren, um Informationen auszutauschen. Digitale Zertifikate eigenen sich besonders, wenn eine breite Palette an Services vielen Personen passwortlos zugänglich gemacht werden sollen, etwa Outlook oder Teams.

Passkey statt Passwort

Eine einfachere Methode, die auch benutzerfreundlicher ist als herkömmliche Zertifikate, bilden Passkeys respektive Security Keys. Wie der Name vermuten lässt, handelt es sich um Schlüssel (Key), mit denen man (zum Beispiel ein Online-Portal eines Benutzerkontos) passieren kann. Passkeys wurden von der FIDO Alliance, einem Zusammenschluss namhafter Technologieunternehmen wie Amazon, Apple, Google, Microsoft et cetera entwickelt. Die Idee dahinter ist, dass man mit Passkeys statt Passwörtern Zugang zu allen Online-Konten haben kann. Eigentlich handelt es sich nicht nur um einen Schlüssel, sondern um ein Schlüsselpaar mit einem öffentlichen und einem privaten Schlüssel. Während der öffentliche Schlüssel zur Webseite oder der App gehört, die den Dienst anbietet, in den

man sich einloggen will, ist der private Schlüssel auf den Endgeräten der Nutzenden hinterlegt. Dies kann das Notebook, das Smartphone oder ein USB- oder NFC-Token wie etwa von Kensington, Swissbit oder Yubico oder anderen Anbietern sein.

Passkeys oder Security Keys ersetzen also das Passwort. Zusätzlich kann auch noch ein zweiter Faktor wie etwa eine Identifikation mittels Fingerabdruck oder Gesichtserkennung verlangt werden. Je nach Compliance-Anforderungen kann der zweite Faktor natürlich auch ein PIN sein, der via SMS verschickt wird und nur kurze Zeit gültig ist.

Am sichersten jedoch ist es, wenn ein Faktor für die Authentifikation etwas ist, das der Nutzer besitzt (Handy, Laptop, Hardware-Token) und der andere Faktor etwas ist, das den Nutzenden explizit persönlich zugeordnet werden kann wie beispielsweise mit der Erkennung des Gesichts oder dem Scan des Fingerabdrucks.

Damit schliesst man auch ausdrücklich das Problem des «Man in the Middle» (Mann in der Mitte) aus, dem Betrugsschema also, bei dem sich der Bösewicht zwischen Nutzer und Nutzerkonto einschleicht und Verhalten manipuliert und ausspioniert.

Fazit

Mit Passkeys oder Security Keys verfügt der Nutzer über einen persönlichen Sicherheitscode. Dieser jedoch ist unbekannt. Der ganz grosse Vorteil dieses Verfahrens ist aber seine bestechende Einfachheit in der Anwendung. Denn der Abgleich mit dem öffentlichen Schlüssel des Online-Services findet im Hintergrund ohne Zutun des Anwenders statt.

Der persönliche Schlüssel ist zum Beispiel auf dem Smartphone oder einem Hardware-Stick gespeichert. Anstatt sich mit Benutzernamen, Passwort und einem zweiten Faktor zu identifizieren, braucht es lediglich den Security- oder Passkey, der auf dem Smartphone oder Laptop gespeichert ist. Auf Letzteren identifiziert man sich ganz unkompliziert mittels Fingerabdruck oder Gesichtserkennung.

Das Verfahren heisst denn auch nicht von ungefähr FIDO (mittlerweile zu FIDO 2 weiterentwickelt). Die Abkürzung steht für Englisch «Fast Identity Online» oder zu Deutsch «schnelle Online-Identität».

Ein weiteres Plus in Sachen Einfachheit ist, dass sich auf Endgeräten gesicherte Passkeys über die Cloud synchronisieren lassen, vorausgesetzt natürlich, die Sicherheitsrichtlinien des Unternehmens lassen das zu. Der Nutzer hat dann auf dem Smartphone, Tablet und Laptop oder dem Hardware-Token immer denselben privaten Schlüssel gespeichert – ein Schlüssel notabene, den weder er noch sonst jemand kennt.

Einziges Manko: Längst nicht alle Online-Dienste bieten Passkey-Authentifizierung. Aus diesem Grund dürften Password- und Zweifaktorauthentifizierung noch eine Weile zum Alltag gehören. Sicherer als Passwörter und einfacher obendrein sind Passkeys aber alleweil. Eine Liste der Dienste, die Passkeys unterstützen, gibt es unter www.passkeys.directory. «

Porträt

Patrick Trevisan
Leiter Verkauf und Produktmanagement, Nomasis

Fabian Mauricio
Mobile-Security-Ingenieur, Nomasis

Nomasis Cyber Security, nach eigenen Angaben Marktführer für Unternehmensmobilität in der Schweiz und in Liechtenstein, bietet Lösungen für digitale Nomaden, also Menschen, die ortsunabhängig, flexibel und mobil arbeiten. Nomasis unterstützt ihre Kunden und deren Endbenutzer seit rund 20 Jahren mit IT-Services und sicheren Lösungen, die speziell auf die Bedürfnisse der modernen Arbeitswelt und mobilen Geräteplattformen ausgerichtet sind.

Kontakt

info@nomasis.ch
www.nomasis.ch