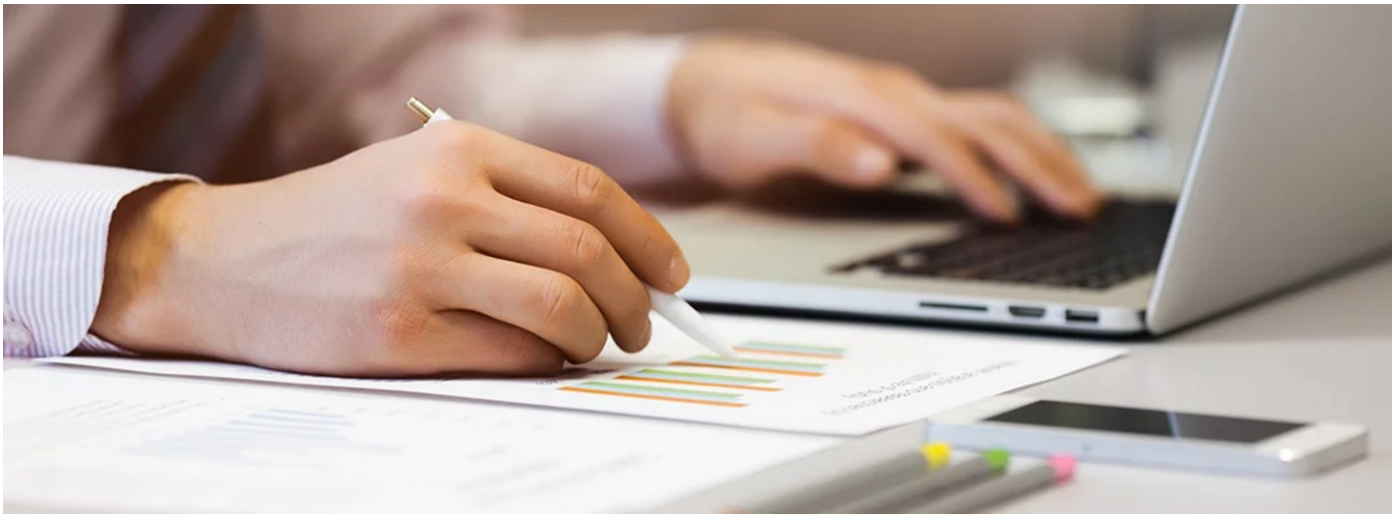

Goodbye Passwort: G+D zeigt wie eine passwortlose Authentifizierung zur Betrugsprävention und Verbesserung der Benutzerfreundlichkeit beiträgt

2023-10-17 | München | Giesecke+Devrient

Passwörter gehören der Vergangenheit an. Sowohl Finanzinstitute als auch zukunftsorientierte Unternehmen suchen nach unkomplizierten und gleichzeitig sicheren Möglichkeiten zur Authentifizierung ihrer Mitarbeiter und Kunden. Giesecke+Devrient (G+D) stellt drei Beispiele vor, die von der passwortlosen Multi-Faktor-Authentifizierung (MFA) profitieren und gleichzeitig einen höheren Schutz vor Cyber-Bedrohungen und eine bessere User Experience bieten.

Die IDC European-Security-Studie 2022 belegt, dass unzureichendes Passwortmanagement in fast jedem zweiten Unternehmen (44%) die größte Herausforderung im Bereich der Identitäts- und Zugangskontrolle darstellt. Besonders besorgniserregend ist die hohe Rate an wiederverwendeten Passwörtern, wobei nicht zwischen privaten und firmeninternen Passwörtern unterschieden wird. Passwörter sind die Hauptursache für über 80 % aller Datenpannen↗. Werden also persönliche Zugangscodes entwendet, entsteht so oft schnell ein Sicherheitsrisiko für das Unternehmen. Abgesehen von Sicherheitsbedenken gibt es oft auch pragmatische oder betriebliche Herausforderungen bei der Eingabe von Passwörtern, etwa bei Mitarbeitern in der Produktion oder an Industriestandorten. Laut IDC kämpft mehr als ein Drittel der Unternehmen damit, ein Gleichgewicht zwischen zuverlässiger Sicherheit und positiver Nutzererfahrung herzustellen.

Im Bankenumfeld ist es nicht anders. Die manuelle Eingabe von Zugangsdaten zur Anmeldung auf einer Website oder in einer App ist ebenfalls nicht mehr zeitgemäß. Laut der FIDO Alliance wurden im Jahr 2021 89 % der Sicherheitsverletzungen bei Webanwendungen durch gestohlene oder kompromittierte Passwörter verursacht. Passwörter sind nicht nur häufig das Ziel von Phishing-Versuchen, sondern es ist für Verbraucherinnen und Verbraucher auch mühsam, sich mehrere Passwörter für sämtliche Online-Konten zu merken. Dies führt dazu, dass sie häufig dasselbe Passwort wiederverwenden, wodurch im Falle einer Datenpanne alle ihre Konten angreifbar sind. Multi-Faktor-Authentifizierungsverfahren, wie Einmalpasswörter und SMS, wurden eingeführt, um die mit schwachen Passwörtern verbundenen Risiken zu verringern. Allerdings bringen diese Verfahren sowohl für Kunden als auch für Banken eine Reihe von Einschränkungen mit sich, wie umständliche Benutzerführung, Anfälligkeit für Phishing, mangelnde Kontrolle und nicht zuletzt versteckte Kosten, denn der Umgang mit betrügerischen Aktivitäten kostet die Banken viel Zeit, Geld und Ressourcen.

„Viele der Vorschriften zur Authentifizierung sind darauf fixiert, ein Problem zu lösen, das im Grunde mit dem primären Authentifizierungsfaktor zusammenhängt, den wir seit 60 Jahren haben – dem Passwort“, sagt Andrew Shikiar von der FIDO

Alliance. „Passwörter sind das Problem."

Die 2013 gegründete FIDO (Fast IDentity Online) Alliance ist ein Zusammenschluss führender Technologie-, Finanz- und Industrieunternehmen – darunter Apple, Google, Microsoft und Mastercard. Die Allianz hat die wachsende Bedeutung des Datenschutzes erkannt und zielt darauf ab, die Abhängigkeit von Passwörtern zu verringern und in Zukunft passwortfreie Anmeldeverfahren einzuführen.

Es ist von entscheidender Bedeutung, dass Authentifizierungslösungen die Komplexität der Sicherheit am Backend bewältigen und gleichzeitig nur einen einzigen, einheitlichen Prozess für den Endbenutzer bereitstellen. Die Optimierung von MFA durch die Kombination von biometrischen Merkmalen (Gesicht, Iris, Fingerabdruck) und Besitzfaktoren schafft einen passwortfreien Mechanismus. Dies ermöglicht es Finanzinstituten und zukunftsorientierten Unternehmen, Benutzerfreundlichkeit und Sicherheit für Mitarbeitende und Kunden zu verbinden.

Anhand von drei praktischen Beispielen zeigt G+D, wie Unternehmen und Finanzinstitute von passwortloser Authentifizierung im Arbeitsalltag profitieren können.

- **Physischer Zugang.** Die Identifikation von berechtigten Mitarbeitern und Mitarbeiterinnen sollte nicht länger nur von Zahleneingaben oder leicht zu stehlenden Zugangskarten am Gebäudeeingang abhängig sein. Hier bieten sich zusätzlich biometrische Verfahren an, etwa das Scannen von Iris oder Fingerabdrücken – insbesondere in Produktionsumgebungen oder in der Schwerindustrie, wo das Personal Schutzkleidung trägt.
- **Authentifizierung am Arbeitsplatz und sichere Kommunikation.** Mit dem Vormarsch hybrider Arbeitsformen müssen sich Mitarbeitende über mehrere Geräte, Systeme, Anwendungen und physische Standorte hinweg authentifizieren, um sicher zu kommunizieren und Daten auszutauschen. Einheitliche und passwortlose Authentifizierungslösungen, die den Benutzerkomfort maximieren und gleichzeitig das richtige Maß an Sicherheit gewährleisten, sind dabei entscheidend.
- **Sicherer Zugang zu Konten und Zahlungen.** Finanzinstitute müssen gesetzliche Vorschriften einhalten und sicherstellen, dass ihre Zahlungssysteme auf allen Ebenen geschützt sind – während in der Finanzbranche weltweit ein massiver Anstieg von Betrug und Scamming zu beobachten ist. Passwortlose MFA garantieren dabei Kundenfreundlichkeit und sichere Prozesse. So können Kunden etwa eine Transaktion mühelos durch einen Gesichts- oder Fingerabdruck-Scan bestätigen. Die Authentifizierung ist damit so einfach wie das Entsperren eines Telefons.

„Da sich Sicherheitsbedrohungen, Kundenverhalten und regulatorische Vorschriften ständig weiterentwickeln, sollte es nicht mehr gängige Praxis sein, sich ausschließlich auf Passwörter zu verlassen. Schwache passwortbasierte Lösungen können durch starke passwortlose Technologien ersetzt werden, um eine vertrauenswürdige Sicherheitsumgebung zu schaffen", erklärt Quintin Stephen, Global Business Lead for Authentication bei G+D. „In einer Zeit, in der sich Kriminelle zunehmend an Sicherheitsmaßnahmen anpassen und gezielt Schwachstellen in Unternehmenssystemen und bei Mitarbeitenden ausnutzen, ist der Verzicht auf Passwörter ein entscheidender Schritt, um die Anfälligkeit eines Unternehmens zu verringern und die Kunden zu schützen."

Über Giesecke+Devrient

Giesecke+Devrient (G+D) ist ein weltweit tätiger Konzern für Sicherheitstechnologie mit Hauptsitz in München. Als verlässlicher Partner für internationale Kunden mit höchsten Ansprüchen sichert G+D mit seinen Lösungen die essenziellen Werte dieser Welt. Dabei entwickelt das Unternehmen maßgeschneiderte Technologie mit Leidenschaft und Präzision in vier Kernfeldern: Bezahlen, Konnektivität, Identitäten und Digitale Infrastrukturen.

G+D wurde 1852 gegründet. Im Geschäftsjahr 2022 erwirtschaftete das Unternehmen mit mehr als 12.600 Mitarbeiterinnen und Mitarbeitern einen Umsatz von 2,53 Milliarden Euro. G+D ist mit 103 Tochtergesellschaften und Gemeinschaftsunternehmen in 33 Ländern vertreten.

Weitere Informationen: www.gi-de.com.