Kensington®

Vergiss dein Passwort!

Der sicherste Login ist dein Fingerabdruck.

Mitarbeiter sind die größte Gefahr für die Datensicherheit.

Die Datenschutzverletzungen steigen stetig an. Nach Schätzungen sind im Jahr 2019[1] 8,5 Milliarden Datenschutzverletzungen aufgetreten, 70% mehr als 2018.[2]

Hacking (Ausnutzen von Sicherheitslücken, um Zugang zu sensiblen Informationen zu erhalten) und Phishing (sich als vertrauenswürdige Quelle ausgeben, damit vertrauliche Daten preisgegeben werden) sind die häufigsten Cyberattacken, die zu Datenschutzverletzungen führen. **80 % der Cyberangriffe gehen auf unsichere Kennwortpraktiken zurück.[3]**

“Sichere” Passwörter - mit Groß- und Kleinschreibung, Zahlen und Symbolen - sind sehr leicht zu vergessen. Wenn man bedenkt, dass der durchschnittliche Anwender 191 Passwörter4 für zahlreiche Logins hat, ist dies eine echte Herausforderung, die es zu bewältigen gilt.

Anstatt sich nur auf Benutzernamen und Passwörter zu verlassen, schafft die Multi-Factor-Authentifizierung (MFA) eine zusätzliche Sicherheitsebene. **Die biometrische Authentifizierung ist die sicherste Stufe der MFA und erfordert einen zusätzlichen Faktor, um Zugang zu gewähren.**

Die MFA kann nahtlos in Benutzer-Workflows implementiert werden, wobei Windows Hello die biometrische Anmeldung und den kennwortlosen Zugang zu Online-Diensten unterstützt. Zudem hat die FIDO-Allianz einen Industriestandard geschaffen, um die Kompatibilität zwischen Hard- und Software für die Authentifizierung sicherzustellen.

VeriMark™ USB Fingerabdruckscanner

- Biometrische Anmeldung
- Multi-Factor-Authentifizierung (MFA)
- Windows Hello
- FIDO U2F zertifiziert

Kensington

Sicherheitsrisiko: Ein-Faktor-Authentifizierung

Die Ein-Faktor-Authentifizierung - mit anderen Worten, ein Passwort, das keine zusätzliche Überprüfung erfordert - wird von Hackern als der Weg des geringsten Widerstands angesehen. Wenn ein Phishing- oder ein Replay-Angriff erfolgreich ein Passwort erbeutet, können noch mehr Informationen abgefangen werden, wenn der Zugriff auf das Gerät kompromittiert wird.

Passwörter, selbst starke, reichen nicht mehr aus, um sensible Konten und unternehmensinterne Informationen vor Hacker- und Phishing-Angriffen zu schützen.

Dabei besteht ein enger Zusammenhang zwischen der Passwortsicherheit und Datenschutzverletzungen, welche einen kostspieligen Datenklau begünstigen. Neben dem real entstandenen Schaden, muss mit möglichen Geldbußen gemäß DSGVO-Richtlinien gerechnet werden.

Passwörter allein reichen nicht aus

Ohne zusätzliche Sicherheitsmaßnahmen sind Passwörter anfällig für Diebstahl und abgefangen zu werden. Die **Zwei-Faktor-Authentifizierung (2FA)** oder Multi-Faktor-Authentifizierung (MFA) sollte daher Teil jedes modernen Authentifizierungsprotokollen sein.

Mit der Abfrage einer weiteren Information (= Faktor) neben dem Passwort oder zweier eindeutiger Informationen (Fingerabdruck & Code per Textnachricht) ohne jegliche Passworteingabe, beseitigt die 2FA/MFA die bekannten Komplexitäten und Unzulänglichkeiten bei der Vergabe von Anmeldepasswörtern.

Eine eindeutige biometrische Authentifizierung wie Fingerabdrücke sind herkömmlichen Sicherheitsabfragen mittels SMS-Textnachrichten oder Sicherheitsfragen deutlich überlegen. Diese Sicherheitsabfragen können, ohne das der Benutzer überhaupt davon weiß, abgefangen werden. Die Authentifizierungstechnologie hat sich mit der Einführung biometrischer Anmeldeoptionen wie Microsofts Windows Hello[5] , welche mit dem **Kensingtons VeriMark™ Fingerabdruckscanner** kompatibel ist, weiterentwickelt.

Warum 2FA und MFA?

Das grundlegende Sicherheitsrisiko der Ein-Faktor-Authentifizierung besteht darin, dass ein Unbefugter, wenn er sich korrekt angemeldet hat, vollumfänglich Zugriff auf das passwortgeschützte Konto hat. **Es spielt keine Rolle, ob er das Passwort durch Diebstahl, einen systematischen Wörterbuchangriff oder durch glückliche Vermutungen erlangt hat, dass daraus resultierende Risiko ist das gleiche.**

Die Zwei- und Multifaktor-Authentifizierung verbessert das Authentifizierungsmodell auf zwei verschiedene Arten:

- Nach erfolgreicher Passworteingabe ist die Verifizierung eines weiteren Berechtigungsnachweises erforderlich
- Das Erlauben der Anmeldung ausschließlich durch einen sichereren kennwortlosen Mechanismus

In beiden Fällen wird die Authentifizierungslösung versuchen, die Identität eines Benutzers zu verifizieren, indem sie etwas abfragt, das er **kennt, das er hat oder mit dem er identifiziert werden kann.** Die Möglichkeiten reichen von einem Einmal-Passwort, das per SMS verschickt oder in einer Authentisierungs-App generiert wird, bis hin zu etwas wesentlich Stärkerem wie einem Hardware- oder Fingerabdruck-Schlüssel. Die beiden letzteren bieten eine größere Sicherheit, da sie nicht anfällig für das Abfangen oder Phishing sind.

Die Vorteile der Biometrie für 2FA, MFA und kennwortlose Log-Ins

Biometrische Daten bietet eine einzigartige Kombination aus Komfort und Sicherheit, so zum Beispiel:

- **Sie lassen sich leicht scannen, verifizieren und mit einer bestimmten Identität in Verbindung bringen.**
- **Basierend auf Berechtigungsnachweisen, die schwer zu duplizieren oder zu stehlen sind.**
- **Sie werden durch spezielle Hardware gespeichert oder übertragen, um Fernzugriff oder Diebstahl zu verhindern.**

Biometrische Authentifizierung kann mehr als nur ein besseres Anmeldeerlebnis für Endbenutzer bieten.

Die Biometrie ermöglicht eine kennwortlose Anmeldung, die die Belastung des IT-Helpdesks durch das Zurücksetzen von Kennwörtern verringert. Jede Passwortzurücksetzung kostet schätzungsweise mehr als 60€[6] - und mehr als 40 % der Benutzer benötigen mehr als 50 Zurücksetzungen pro Jahr.[7]

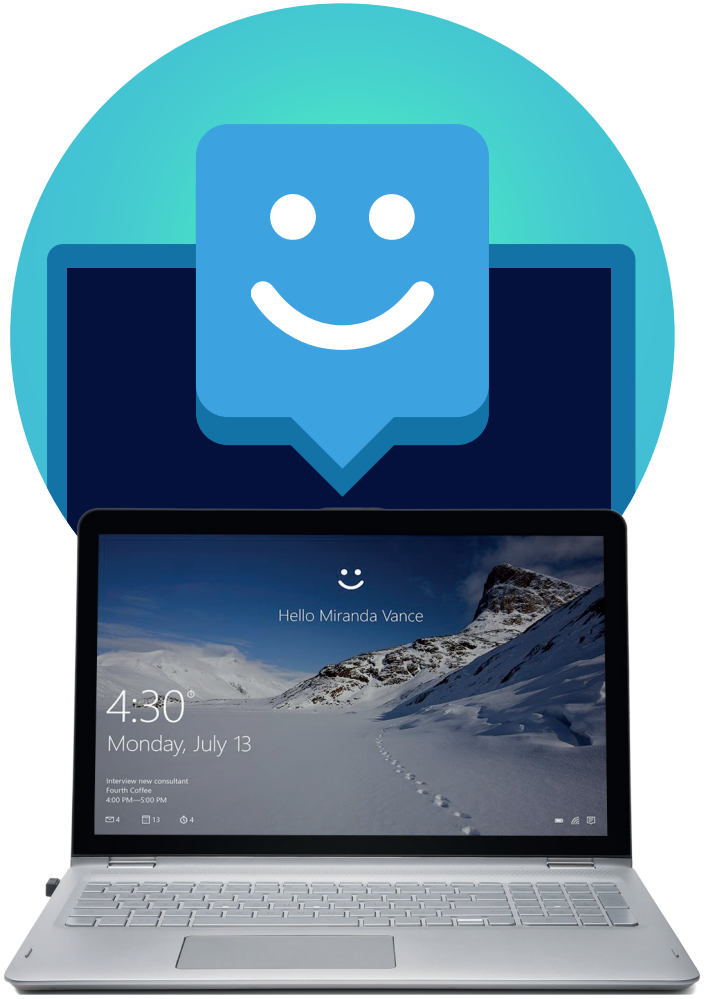
In einem Unternehmen mit 1.000 Anwendern ergibt das 1,2 Million € pro Jahr an verlorener Zeit und Produktivität.

Windows Hello unterstützt die direkte biometrische Anmeldung

Windows Hello, das zu den Standardfunktionen von Windows 10 gehört, unterstützt die direkte biometrische Anmeldung. Zu diesen biometrischen Optionen gehören Gesichtserkennung, Iris-Scan und Fingerabdruckscan, **letzteres über FIDO U2F-zertifizierte Hardware wie der Fingerabdruckscanner von Kensington VeriMark™.**

Windows Hello eliminiert die Unannehmlichkeiten, die das Erstellen und Merken komplexer Kennwörter mit sich bringt. Noch wichtiger ist, dass es die üblichen Schlupflöcher in der kennwortbasierten Sicherheit vermeidet, wie z.B. die Offenlegung von Zugangsdaten durch Phishing.

Das Anmeldeverfahren für Windows Hello ist sehr unkompliziert. Eine erfolgreiche biometrische Authentifizierung gibt den Zugriff auf ein unterstütztes Windows-Gerät frei.



Was ist FIDO?

Die **Fast IDentity Online (FIDO) Alliance** wurde gegründet, um Standards sowohl für 2FA/MFA als auch für die kennwortlose Authentifizierung zu setzen.

FIDO Universal Second Factor (U2F) ist ein offener Standard, der Spezifikationen für 2FA unter Verwendung eines starken und manipulationssicheren, nicht passwortgeschützten zweiten Faktors definiert. Da er standardisiert ist, ist FIDO U2F weitgehend kompatibel mit beliebten Online-Diensten wie Gmail, Facebook, Github, Dropbox und vielen anderen.

Biometrischer Fingerabdruck und Hardwareschlüssel mit USB-, NFC- oder Bluetooth-Technologien sind die typischen zusätzlichen Faktoren für Dienste, die U2F nutzen.

VeriMark™ - der erste Fingerabdruckscanner von Kensington, der ein starkes, effizientes 2FA gewährleistet

VeriMark™ arbeitet sowohl mit der Windows-Hello- als auch mit der FIDO U2F-Authentifizierung, um eine sichere und nahtlose Möglichkeit zu bieten, sich bei Windows 7, 8.1 und Windows 10 anzumelden und bei wichtigen Konten 2FA zu ermöglichen.

Der VeriMark™ Fingerabdruckscanner bietet die beste biometrische Leistung seiner Klasse in einem praktischen, kompakten und standardkonformen Paket.

Falschrückweisungs- (3 %) und Falschakzeptanzraten (0,002 %), die durch den Einsatz der TLS1.2/AES256-Verschlüsselung und der Anti-Spoofing Protection (ASP)-Technologie die Industriestandards übertreffen.

VeriMark™ ist die perfekte Lösung für Personen, die eine biometrische Authentifizierung benötigen, die mit aktuellen oder älteren Windows-Betriebssystemen funktioniert und gleichzeitig die U2F-Authentifizierung für Cloud-basierte Dienstleistungs- und Softwareanbieter wie Facebook, Google, GitHub, Dropbox und andere.

VeriMark™ USB Fingerabdruckscanner

- **Die moderne Fingerabdrucktechnologie** kombiniert höchste biometrische Leistung und 360°-Lesbarkeit mit Antispoofing-Schutz und bietet mit einer universellen Zwei-Faktoren-Authentifizierung Schutz Ihrer Daten vor Cyberdiebstahl.
- **Die universelle Integration** ermöglicht einen skalierbaren, sofort einsatzbereiten Zugang für Windows-Computer und -Plattformen, einschließlich der biometrischen Anmeldung für Windows Hello™.
- **FIDO U2F-zertifiziert,** um eine nahtlose Interoperabilität zu gewährleisten und die Anmeldeanforderungen für den 2-Faktor-Sicherheitsschlüssel für Anbieter von Cloud-basierten Diensten und Software, einschließlich Google, Dropbox, GitHub und Facebook, zu erfüllen.
- **Kompaktes Design,** das sich leicht an einem Standard-Schlüsselanhänger befestigen lässt und somit bequem tragbar ist.

Artikel-Nr. K67977WW

Kensington

Weitere Informationen, Testgeräte oder Projektpreise erhalten Sie unter:


www.kensington.com/forget-your-password


contact@kensington.com

Quellen:

1. Risk Based Security's Q3 2019 Data Breach QuickView Report
2. darkreading.com/threat-intelligence/2018-was-second-most-active-year-for-data-breaches/d/d-id/1333875
3. Verizon 2019 Data Breach Investigations Report
4. securitymagazine.com/articles/88475-average-business-user-has-191-passwords
5. symantec.com/content/en/uk/enterprise/other_resources/b-is-your-data-safe-security-non-compliance-infographic-21330416-UK.pdf
6. infosecurity-magazine.com/opinions/how-much-passwords-cost
7. plan-net.co.uk/blog/password-reset-processes