Neue IBM Studie zur „Zukunft der Identitätsfeststellung im Web“: Millennials setzen auf biometrischen Identitätsschutz, Generation 55+ auf starke Passwörter

Für die IBM Security Studie „Future of Identity“ wurden 4.000 Erwachsene in Europa, den USA und in Asien befragt

Sicherheit geht vor Bequemlichkeit

Millennials präferieren Biometrie zum Identitätsschutz

Cambridge, MA, USA - 29 Jan 2018: Ob bei der Anmeldung in Anwendungen oder an Geräten – Sicherheit hat bei Verbrauchern weltweit mittlerweile höchste Priorität. Das zeigt eine neue globale Studie mit knapp 4.000 Befragten aus den USA, APAC und der EU, die von IBM Security in Auftrag gegeben wurde. Unterschiede ergeben sich vor allem in Bezug darauf, wie die Befragten ihre Online-Accounts und Daten absichern: Während die ältere Generation eher auf traditionelle Passworthygiene setzt, nutzen junge Erwachsene eher Biometrie, Multifaktor-Authentifizierung und Passwort-Manager, um ihre Geräte und Profile zu schützen. Die Zukunft des Identitätsschutzes liegt daher in Plattformen, die ein breites Spektrum zielgruppengerechter Authentifizierungsmöglichkeiten bieten. Komplexe Passwörter, bestehend aus Zahlen, Groß- und Kleinbuchstaben und Sonderzeichen, am besten maximal chaotisch zusammengestellt – das ist jungen Erwachsenen angesichts der wachsenden Password-Flut zu anstrengend. Sie suchen vielmehr nach innovativeren Lösungen, um der Sache Herr zu werden. Darauf sollten insbesondere Arbeitgeber mit alternativen Sicherheitskonzepten reagieren. Denn die Generation der „Millennials“ wird schon bald zur größten Arbeitergruppe aufsteigen und Bedrohungen für die digitale Identität werden weiter zunehmen. Die jüngeren Befragten sprechen sich vor allem für biometrische Technologien wie Fingerabdruckleser, Gesichtsscans und Spracherkennung aus.

Die wichtigsten Ergebnisse auf einen Blick - Für die Studie "IBM Security: Future of Identity" wurden knapp 4.000 Erwachsene aus den USA, dem asiatisch-pazifischen Raum (APAC) und der EU nach ihrer Einstellung und ihren Verhaltensweisen rund um die Authentifizierung gefragt. In der EU wurden Menschen aus Großbritannien, Frankreich, Deutschland, Italien und Spanien befragt. Die wichtigsten Erkenntnisse sind:

Sicherheit überwiegt den Komfort - Bei den meisten Anwendungen hat Sicherheit die höchste Priorität, vor allem wenn es um Apps geht, die für Finanztransaktionen genutzt werden.

Biometrie wird Mainstream - 67 Prozent der Befragten fühlen sich heute bereits mit biometrischer Authentifizierung wohl. Insgesamt 87 Prozent sind sich sicher, dass sie sich auch in Zukunft mit biometrischen Technologien wohlfühlen werden.

Identitätsschutz geht bei Millennials über reine Passwörter hinaus - Weniger als die Hälfte der Millennials benutzen komplexe Kennwörter, um ihre Accounts und Geräte zu sichern. Nur 41 Prozent nutzen überhaupt Kennwörter zum Identitätsschutz. Dagegen vertrauen 75 Prozent der Jungen auf Biometrie. Bei der älteren Generation ergibt sich hier ein ganz anderes Bild: Sie zeigt bei der Passwort-Erstellung mehr Sorgfalt, ist jedoch weniger offen für Biometrie und Multi-Faktor-Authentifizierung.

EU beim Thema Biometrie im Mittelfeld - In der EU nutzen bereits 65 Prozent der Befragten gerne biometrische Verfahren zur Authentifizierung. Vorreiter sind hier die APAC-Länder mit 78 Prozent Biometrie-Anhänger, während die USA mit 57 Prozent zurückbleiben. 88 Prozent der EU-Bürger sind außerdem daran interessiert, Biometrie in der nahen Zukunft zu nutzen und immerhin 40 Prozent haben bereits Wissen über die verschiedenen biometrischen Identifizierungsarten.

"Im letzten Jahr haben Datenlecks hochsensible, personenbezogene Daten wie Passwörter oder Sozialversicherungsnummern von Millionen von Verbrauchern offen gelegt. Es besteht kein Zweifel mehr daran, dass traditionelle Strategien zum Identitätsschutz von Hackern zunehmend öfter durchschaut und effektiv umgangen werden", sagt Christian Nern, Head of Security Software DACH bei IBM Deutschland. "Kleine und mittelständische Unternehmen sind daher genauso wie Großkonzerne aufgefordert, einer effektiven Authentifizierung ihrer Mitarbeiter und Kunden höchste Priorität einzuräumen und fortschrittlichere Technologien wie Biometrie und Multi-Faktor-Authentifizierung anzubieten."

Befragte sind sich einig: Sicherheit geht vor - Umfrageergebnisse der IBM Security Studie zu den Themen Sicherheit, Komfort und Privatsphäre widersprechen der lang gehegten Weisheit, dass "Bequemlichkeit König ist". Die lange geltende Attitüde, sich möglichst schnell bei möglichst geringem Aufwand zu registrieren, gilt nicht mehr. Die aktuellen Umfrageergebnisse zeigen vielmehr, dass Sicherheit von den Befragten mittlerweile als oberste Priorität eingestuft wird – insbesondere wenn es um Finanztransaktionen geht.

Sicherheit wurde bei Banking-, Investitions- und Budgetierungs-Apps von durchschnittlich 70 Prozent der Befragten als oberste Priorität eingestuft. Dahinter weit abgeschlagen mit 16 Prozent der Datenschutz und mit 14 Prozent der Komfort.

Auch für Online-Marktplätze, Arbeitsplatz-Apps und E-Mail gilt Sicherheit als oberste Priorität.

Bei Social-Media-Apps sind die Prioritäten weniger klar – Bequemlichkeit siegt hier mit einem leichten Vorsprung (36 Prozent) vor Sicherheit (34 Prozent) und Datenschutz (30 Prozent).

44 Prozent der Befragten bewerten Fingerabdruck-Biometrie als eine der sichersten Authentifizierungsmethoden. Passwörter und PINs wurden als weniger sicher angesehen (27 Prozent bzw. zwölf Prozent).

Die größten Sicherheitsbedenken der Befragten in Bezug auf die biometrische Authentifizierung bestehen bei Fragen der Privatsphäre, also wie Daten gesammelt und genutzt werden (55 Prozent). Gefolgt vom Thema Sicherheit, also der Gefahr, dass gefälschte biometrische Daten verwendet werden (50 Prozent).

Generation-Gap: Passworthygiene versus neue Technologien - Der generationsübergreifende Blick der IBM Security Studie auf Meinungen zur Sicherung der Online-Identität belegt: ältere Menschen haben in erster Linie eigene Strategien zur Passworterstellung entwickelt, die jüngere Generation ist dagegen eher geneigt, neue Technologien wie Passwort-Manager, Biometrie und Multifaktor-Authentifizierung zu verwenden, um ihre Online-Accounts zu sichern. Das könnte ein Hinweis darauf sein, dass jüngere Menschen weniger Vertrauen in Passwörter haben und stattdessen lieber auf alternative Methoden zurückgreifen.

Nur 42 Prozent der Millennials verwenden komplexe Passwörter, die Sonderzeichen, Zahlen und Buchstaben kombinieren. Bei den über 55-Jährigen sind es dagegen noch 49 Prozent. Außerdem verwenden 41 Prozent der Millennials dasselbe Passwort mehrmals, während bei der Generation 55 plus nur 31 Prozent ein solches Sicherheitsrisiko in Kauf nehmen.

Im Durchschnitt verwenden die über 55-Jährigen insgesamt zwölf Passwörter, die Generation Z (18 bis 20 Jahre) durchschnittlich nur fünf Passwörter. Das könnte auf eine häufigere Wiederverwendungsrate hindeuten.

Millennials benutzen doppelt so häufig einen Passwort-Manager (34 Prozent) wie die Generation 55 plus (17 Prozent).

Fast die Hälfte der unter 24-Jährigen zieht eine schnellere Anmeldung einer sichereren Form der Authentifizierung vor. Bequemlichkeit spielt für die junge Generation also eine größere Rolle. Das könnte auch der Grund dafür sein, dass junge Erwachsene häufiger auf biometrische Verfahren setzen. 75 Prozent der Millennials sind mit der biometrischen Authentifizierung vertraut. Bei den über 55-Jährigen sind es gerade einmal 58 Prozent.

Rund um die Welt: Perspektivwechsel bei Passwort und Authentifizierung - Beim Blick auf die verschiedenen Länder ergab die IBM Security Studie, dass der geografische Standort einen starken Einfluss auf die Wahrnehmung von und die Vertrautheit mit aufkommenden Authentifizierungstechniken hat. Dabei ist die asiatisch-pazifische Region am besten mit Taktiken wie der Multifaktor-Authentifizierung und Biometrie vertraut. Die EU-Bürger sind dagegen am wenigsten bereit, im Arbeitsalltag Biometrie zu nutzen.

Weitere wichtige Ergebnisse:

APAC-Befragte gaben am häufigsten an, dass sie mit Biometrie vertraut sind. Immerhin 61 Prozent halten sich für sachkundig. In der EU waren es dagegen nur 40 Prozent, in den USA sogar nur 34 Prozent.

Studienteilnehmer aus den APAC-Staaten fühlten sich mit Biometrie am wohlsten. Von ihnen gaben 78 Prozent an, diese Methode sei für sie komfortabel. In der EU waren es 65 Prozent und in den USA 57 Prozent.

EU-Bürger haben dagegen die stärksten Passwort-Praktiken. 52 Prozent der Befragten verwenden komplexe Passwörter. In den APAC-Ländern sind es 46 Prozent, in den USA 41 Prozent.

Zukunft der Identität: Vielfalt und Komfort - Die Studie „IBM Security: Future of Identity“ hat zudem ermittelt, dass die Vorlieben der Studienteilnehmer in Fragen der Authentifizierung weltweit stark auseinandergehen: Generell nimmt die Akzeptanz neuer Authentifizierungsverfahren, wie beispielsweise der Biometrie, zu. Bei älteren Menschen und bei US-Bürgern bestehen jedoch weiterhin Bedenken. Sie bevorzugen den herkömmlichen Passwortschutz.

Die Daten zeigen auch, dass jüngere Generationen weniger Wert auf traditionelle Passworthygiene legen. Dies stellt insbesondere diejenigen Unternehmen vor neue Herausforderungen, die den Datenzugriff von Millennial-Nutzern über Passwörter verwalten: Da die Mitarbeitergruppe der Millennials und Generation Z zukünftig den größten Teil ihrer Belegschaft stellen werden, sollten sie sich an den neuen Gewohnheiten der jüngeren Generationen orientieren. Das bedeutet, primär mobile Endgeräte zur Authentifizierung zu verwenden und klassische Passwörter gegen biometrische Methoden oder Tokens auszutauschen.

IBM empfiehlt daher Unternehmen generell, sich den Präferenzen ihrer Zielgruppen anzupassen und Identitätsplattformen einzuführen, die den Benutzern die Wahl zwischen mehreren Authentifizierungsoptionen bieten. So sollten Nutzer beispielsweise die Wahl haben, ob sie lieber eine mobile Push-Benachrichtigung, die einen Fingerabdruck-Scan auf ihrem Mobiltelefon aufruft, oder einen einmaligen PIN-Code zugeschickt haben wollen.

Weitere Einzelheiten zur Studie und Tipps für Unternehmen, wie sie sich auf die Zukunft der Authentifizierung vorbereiten können, finden Sie im vollständigen Bericht unter: www.ibm.biz/FutureOfIdentity

Über die Studie - Die Studie wurde in Zusammenarbeit mit Ketchum Global Research and Analytics entwickelt. Durchgeführt wurde die Datenerhebung von Research Now zwischen dem 21. Oktober und dem 5. November 2017 mit einer Fehlerquote von +/- 2,0 für die US-Stichprobe und +/- 3,07 für die EU- und APAC-Stichproben bei einem Konfidenzniveau von 95 Prozent.

Die 15-minütige Online-Umfrage umfasste Antworten von 3.977 Erwachsenen in den Regionen der Vereinigten Staaten (USA), der Europäischen Union (EU) und Asien-Pazifik (APAC), darunter: 1.976 Befragte in den USA, 1.004 Befragte in der EU (Vereinigtes Königreich, Frankreich, Italien, Deutschland, Spanien) und 997 Befragte aus der APAC-Region (Australien, Indien, Singapur).

Die englische Originalmeldung finden Sie hier:

https://www-03.ibm.com/press/us/en/index.wss

Eine Infografik finden Sie unter: http://www-03.ibm.com/press/us/en/photo/53647.wss

Illustration zu biometrischer Authentifizierung: http://www-03.ibm.com/press/us/en/photo/53649.wss

---

https://de.newsroom.ibm.com/2018-01-29-Neue-IBM-Studie-zur-Zukunft-der-Identitatsfeststellung-im-Web-Millennials-setzen-auf-biometrischen-Identitatsschutz-Generation-55-auf-starke-Passworter