IBM Studie: Pandemie bedingte digitale Abhängigkeit erzeugt anhaltende Sicherheitsnebenwirkungen

• Laut Studie erstellten Verbraucher während der Pandemie durchschnittlich 15 neue Benutzerkonten, wobei 82 % der Befragten ihre Passwörter für mehrere Konten verwendeten

• Mehr als die Hälfte der befragten Millennials würde lieber eine Bestellung über eine potenziell unsichere App oder Website aufgeben, als eine Filiale anzurufen oder persönlich zu besuchen

Cambridge, MA, 15. Juni, 2021 – IBM Security gab heute die Ergebnisse einer globalen Studie bekannt, die das digitale Verhalten von Verbrauchern während der Pandemie sowie deren mögliche langfristige Auswirkungen auf das Sicherheitsverhalten im Internet hin untersucht. Da sich die Gesellschaft zunehmend an digitale Interaktionen gewöhnt, ergab die Studie, dass die Präferenzen für Bequemlichkeit oft die personenbezogenen Sicherheits- und Datenschutzbedenken überwiegen - was negativen Einfluss auf den Umgang mit Passwörtern und dem Sicherheitsverhalten insgesamt hat.

Der laxe Umgang der Verbraucher mit dem Thema Sicherheit, kombiniert mit der beschleunigten digitalen Transformation von Unternehmen während der Pandemie, könnte Angreifern zusätzliche Möglichkeiten liefern, Cyberattacken branchenübergreifend zu forcieren - von Datendiebstahl bis hin zu Erpressung. Laut IBM Security X-Force kann sich laxer Umgang mit Sicherheit vom privaten auf den geschäftlichen Bereich übertragen und kann zu kostspieligen Sicherheitsvorfällen für Unternehmen führen. Kompromittierte Benutzeranmeldedaten stellten 2020 eine der Hauptursachen für Cyberangriffe in Unternehmen dar.[1]

Die weltweite Umfrage[2] unter 22.000 Personen in 22 Märkten, die von Morning Consult im Auftrag von IBM Security durchgeführt wurde, ergab folgende Auswirkungen der Pandemie auf das Sicherheitsverhalten der Verbraucher:

- **Der digitale Boom wird die Pandemie überdauern:** Befragte Verbraucher haben während der Pandemie im Durchschnitt 15 neue Online-Konten erstellt, was Milliarden zusätzlicher Benutzerdaten weltweit bedeutet. Da 44 % angaben, dass sie nicht vorhaben diese neuen Konten nach der Pandemie zu löschen oder zu deaktivieren, werden diese Verbraucher einen größeren digitalen Fußabdruck hinterlassen, welcher die Angriffsfläche für Cyberkriminelle erheblich vergrößert.
- **Eine Zunahme der Benutzerkonten führte zu Passwort-Müdigkeit:** Die Flut an digitalen Konten hat unter den Befragten zu einem laxen Passwortverhalten geführt. 82 % der Befragten geben zu, dass sie ihre Anmeldedaten zumindest manchmal wiederverwenden. Das bedeutet, dass ein Großteil der neuen Konten, die während der Pandemie erstellt wurden, wahrscheinlich auf wiederverwendeten E-

Mail- und Passwort-Kombinationen basierten, die bereits als „bekannt“ einzustufen sein könnten.

- **Bequemlichkeit geht oft vor Sicherheit und Datenschutz:** Mehr als die Hälfte (51 %) der befragten Millennials würde lieber eine Bestellung über eine potenziell unsichere App oder Website aufgeben, als anzurufen oder persönlich in eine Filiale zu gehen. Da diese Nutzer eher bereit sind, Sicherheitsbedenken zugunsten der Bequemlichkeit digitaler Bestellungen zu ignorieren, wird die Verantwortung voraussichtlich stärker auf die Anbieter der Dienste verlagert, um Betrug zu vermeiden.

Da sich die Verbraucher immer mehr auf digitale Interaktionen einlassen, hat dieses Verhalten auch das Potenzial, die Einführung neuer Technologien in einer Vielzahl von Bereichen voranzutreiben - von Telemedizin bis hin zu digitaler Identität.[3]

"Die Pandemie führte zu einem enormen Anstieg neuer Online-Konten, aber die wachsende Vorliebe der Gesellschaft für digitale Bequemlichkeit kann auf Kosten der Sicherheit und des Datenschutzes gehen", sagt Charles Henderson, Global Managing Partner und Leiter von IBM Security X-Force. "Unternehmen müssen jetzt die Auswirkungen dieser digitalen Abhängigkeit auf ihr Sicherheitsrisikoprofil berücksichtigen. Da Passwörter immer unzuverlässiger werden, ist eine Möglichkeit, wie sich Unternehmen über die Multi-Faktor-Authentifizierung hinaus anpassen können, die Umstellung auf einen 'Zero-Trust'-Ansatz. Dabei wird fortschrittliche künstliche Intelligenz (KI) und Analytik während des gesamten Prozesses angewendet, um potenzielle Bedrohungen zu erkennen, anstatt davon auszugehen, dass ein Benutzer nach der Authentifizierung vertrauenswürdig ist."

Verbraucher berichten von hohen Erwartungen an den einfachen Zugang

Die Umfrage beleuchtet eine Reihe von Verhaltensweisen von Verbrauchern, die sich heute und in Zukunft auf die Sicherheitslandschaft auswirken. Da Verbraucher zunehmend digitale Interaktionen in immer mehr Lebensbereichen nutzen, ergab die Umfrage, dass viele auch hohe Erwartungen an einen einfachen Zugang und eine einfache Nutzung haben.

- **5-Minuten-Regel:** Laut der Umfrage erwarten die meisten Verbraucher (59 %), dass sie weniger als 5 Minuten für die Einrichtung eines neuen digitalen Kontos benötigen.
- **Nach drei Fehlversuchen ist Schluss:** Global gesehen würden die Befragten 3-4 Logins versuchen, bevor sie ihr Passwort zurücksetzen. Diese Rücksetzungen kosten die Unternehmen nicht nur Geld, sondern können auch ein Sicherheitsrisiko darstellen, wenn sie in Kombination mit einem bereits kompromittierten E-Mail-Konto verwendet werden.
- **Im Gedächtnis abgelegt:** 44 % der Befragten speichern Online-Kontoinformationen in ihrem Gedächtnis (häufigste Methode), während 32 % diese Informationen auf Papier aufschreiben.
- **Multi-Faktor-Authentifizierung:** Während die Wiederverwendung von Passwörtern ein wachsendes Problem darstellt, kann das Hinzufügen eines zusätzlichen Verifizierungsfaktors für Transaktionen

dazu beitragen, das Risiko einer Kompromittierung des Kontos zu verringern. Die Umfrage ergab, dass rund zwei Drittel der weltweit Befragten innerhalb der letzten Wochen vor der Befragung eine Multi-Faktor-Authentifizierung verwendet haben.

Tiefer eintauchen in das digitale Gesundheitswesen

Während der Pandemie wurden digitale Kanäle zu einer entscheidenden Komponente, um die massive Nachfrage nach COVID-19-Impfstoffen, Tests und Behandlungen zu bedienen. Laut einer IBM Security Analyse[4] könnte die Nutzung einer Vielzahl von digitalen Kanälen für COVID-19-bezogene Dienstleistungen durch die Verbraucher in Zukunft zu einem stärkeren digitalen Engagement bei Gesundheitsdienstleistern führen, indem die Einstiegshürde für neue Nutzer gesenkt wird. Laut der Umfrage:

- 63 % der Befragten haben sich über irgendeine Form von digitalem Kanal (Web, mobile App, E-Mail und SMS) mit pandemiebezogenen Diensten[5] beschäftigt
- Während Websites/Web-Apps die häufigste Methode der digitalen Einbindung waren, wurden auch mobile Apps und Textnachrichten in erheblichem Umfang genutzt - mit 39 % bzw. 20 % Einbindung über diese Kanäle.

Je weiter Gesundheitsdienstleister in der Telemedizin fortschreiten, desto wichtiger wird es, dass ihre Sicherheitsmechanismen so gestalten sind, diesem Wandel standzuhalten - von der Aufrechterhaltung kritischer IT-Systeme über den Schutz sensibler Patientendaten bis hin zur kontinuierlichen Einhaltung gesetzlicher Vorgaben. Dazu gehört die Segmentierung von Daten und die Implementierung strenger Kontrollen, so dass Benutzer nur auf bestimmte Systeme und Daten zugreifen können und die Auswirkungen eines kompromittierten Benutzerkontos oder Geräts begrenzt werden. Um für den Fall von Erpressungsangriffen gewappnet zu sein, sollten Patientendaten im Idealfall zu jeder Zeit verschlüsselt werden und zuverlässige Backups vorhanden sein, damit Systeme und Daten schnell und mit minimaler Unterbrechung wiederhergestellt werden können.

Den Weg für digitale Ausweise ebnen

Das Konzept des digitalen Gesundheitspasses oder des sogenannten Impfpasses zeigte den Verbrauchern einen realen Anwendungsfall für digitale Ausweise auf, die einen technologiebasierten Ansatz zur Verifizierung bestimmter Aspekte unserer Identität bieten. Laut der Umfrage geben 65 % der Erwachsenen weltweit an, dass sie mit dem Konzept der digitalen Ausweise vertraut sind, und 76 % würden sie wahrscheinlich annehmen, wenn sie allgemein akzeptiert würden.

Das Beschäftigung mit der Idee von digitalisierten Identitätsnachweisen während der Pandemie könnte dazu beitragen, eine breitere Akzeptanz von modernisierten Systemen der digitalen Identität zu fördern und könnte den Bedarf an traditionellen Formen der Identifikation wie Pässen und Führerscheinen ersetzen. Digitale

Identitäten würden den Verbrauchern auch eine Möglichkeit bieten, die für eine bestimmte Transaktion erforderlichen begrenzten Informationen bereitzustellen. Während die Nutzung einer digitalen Form der Identität auch das Potential hat, ein nachhaltigeres Modell für die Zukunft zu schaffen, müssen auch Sicherheits- und Datenschutzvorkehrungen getroffen werden, um Fälschungen zu vermeiden - was die Fähigkeiten von Blockchain-Lösungen fordert, um diese Ausweise zu verifizieren und die Möglichkeit zu bieten, sie zu aktualisieren, falls erforderlich.

Wie sich Unternehmen an die sich verändernde Sicherheitslandschaft für Verbraucher anpassen können

Unternehmen, die aufgrund der Pandemie zunehmend auf die digitale Interaktion mit Verbrauchern angewiesen sind, sollten die Auswirkungen auf ihr Cybersecurity-Risikoprofil berücksichtigen. Angesichts der sich ändernden Verhaltensweisen und Vorlieben der Verbraucher in Bezug auf digitale Annehmlichkeiten schlägt IBM Security vor, dass Unternehmen die folgenden Sicherheitsempfehlungen berücksichtigen:

- **„Zero Trust“ Sicherheitsansatz:** Angesichts der zunehmenden Risiken sollten Unternehmen die Umstellung auf einen "Zero Trust"-Sicherheitsansatz in Erwägung ziehen. Zero Trust arbeitet unter der Annahme, dass eine authentifizierte Identität oder das Netzwerk selbst bereits kompromittiert sein könnte, und daher kontinuierlich die Bedingungen für die Verbindung zwischen Benutzern, Daten und Ressourcen zu validieren sind, um die Berechtigung und den Bedarf zu ermitteln. Dieser Ansatz erfordert, dass Unternehmen ihre Sicherheitsdaten und -ansätze vereinheitlichen, mit dem Ziel, den Sicherheitskontext für jeden Benutzer, jedes Gerät und jede Interaktion zur verstehen.
- **Modernisierung des Identity- und Access-Management (IAM)**: Für Unternehmen, die weiterhin digitale Kanäle für die Kundenbindung nutzen wollen, ist ein nahtloser Authentifizierungsprozess wichtig. Die Investition in eine modernisierte IAM-Strategie kann Unternehmen dabei helfen, das digitale Engagement zu erhöhen - durch ein reibungsloses Nutzererlebnis auf allen digitalen Plattformen und die Einbeziehung von Verhaltensanalysen das Risiko eines Missbrauchs zu verringern.
- **Datensicherheit und Datenschutz:** Mehr digitale Nutzer bedeuten, dass Unternehmen auch mehr sensible Verbraucherdaten zu schützen haben. Angesichts der Tatsache, dass Datenschutzverletzungen den untersuchten[6] Unternehmen im Durchschnitt 3,86 Millionen Dollar kosten, müssen Unternehmen strenge Datensicherheitskontrollen einrichten, um sich gegen unbefugten Zugriff zu schützen - von der Überwachung von Daten zur Erkennung verdächtiger Aktivitäten bis hin zur Verschlüsselung sensibler Daten, wo immer sie transportiert werden. Unternehmen sollten auch die lokal notwendigen Datenschutzrichtlinien implementieren und aktuell halten, um das Vertrauen der Kunden zu bewahren.
- **Überprüfung der IT-Sicherheit:** Da sich die Nutzung und die Abhängigkeit von digitalen Plattformen schnell ändern, sollten Unternehmen regelmäßige Tests in Erwägung ziehen. Damit stellen

sie sicher, dass die Sicherheitsstrategien und Technologien, auf die sie sich bisher verlassen haben, auch in dieser neuen Umgebung noch Bestand haben. Die Neubewertung der Effektivität von Reaktionsplänen auf Vorfälle und das Testen von Anwendungen auf Sicherheitslücken sind wichtige Bestandteile dieses Prozesses.

Link zur Pressemitteilung im englischen Original: Link

Link zur weltweiten Studie: Link

Deutschland Report: siehe oben bei Bildern

Über IBM Security: https://www.ibm.com/de-de/security

IBM Security Intelligence Blog: https://securityintelligence.com/

Methodik des Berichts: *Eine globale Umfrage wurde von Morning Consult im Auftrag von IBM im März 2021 durchgeführt. Die Studie wurde unter 22.000 Verbrauchern in 22 Märkten (1.000 Befragte pro Markt) durchgeführt, darunter Argentinien, Australien, Brasilien, Chile, Deutschland, Frankreich, Indien, Italien, Japan, Kanada, Kolumbien, Mexiko, Peru, Singapur, Südkorea, Spanien, Großbritannien, USA, Naher Osten, Mittel- und Osteuropa, Skandinavien und BNL (Belgien, Niederlande und Luxemburg).*

Kontakt für Journalisten:

Barbara Jax

IBM Unternehmenskommunikation

+43.664.618 7237

barbara.jax@at.ibm.com

---

[1] IBM X-Force Threat Index 2021: Kompromittierte Benutzeranmeldeinformationen waren 2020 der drittwichtigste Angriffsvektor für Cyberangriffe und machten 18 % der gemeldeten Vorfälle aus.

[2] Die globale Umfrage wurde im März 2021 von Morning Consult im Auftrag von IBM durchgeführt. Die Studie wurde unter 22.000 Verbrauchern in 22 Märkten durchgeführt.

[3] Vorhersage auf Basis von IBM Security Erkenntnissen

[4] Vorhersage auf Basis von IBM Security Analyse

[5] Beinhaltet finanzielle COVID-19 Unterstützung, Tests, Behandlung und Impfungen

[6] 2020 Cost of a Data Breach Report, Benchmark Studie durchgeführt vom Ponemon Institute, analysiert und gesponsert von IBM Security

---