Bequemlichkeit versus Sicherheit – Das digitale Leben verlangt neue Einsichten

Der Sicherheitsvorfall um LastPass zu Beginn des Jahres spült einmal mehr die grundsätzliche Auseinandersetzung mit dem Thema Multi-Faktor-Authentifizierungen und die Abwägung von Bequemlichkeit und Sicherheit nach oben. Gründe dagegen werden vielfach ins Feld geworfen. Aspekte wie Kosten oder vorherrschende Standards sind potenzielle Hindernisse für den Einsatz universeller Multi-Faktor-Authentifizierungen. Ein genauerer Blick zeigt warum das so ist und warum dennoch kein Weg um eine effektive Zweitabsicherung herumführt.

1. Kosten und Benutzerfreundlichkeit
Wäre ein Token eine geeignete Passwort-Alternative? Sollte jeder einzelne Nutzer damit ausgestattet werden, sind sie recht kostspielig. Zudem kann und will sich nicht jeder ein Smartphone leisten und viele der Systeme, die auf Telefon oder Bildschirme angewiesen sind, sind für Menschen mit Behinderungen nicht nutzbar. Weiteres Problem: die meisten App-Lösungen sind durch Proxy-Angriffe „phishbar“, was zu ihrer zukünftigen Ineffektivität führt, da Kriminelle sich anpassen und immer raffiniertere Phishing-Techniken verwenden. Ein Gegenmittel wäre U2F (Universeller Zweiter Faktor). Microsoft, Google und Apple versuchen erste Schritte mit Passkeys, aber diese Lösung ist in der Tat sehr verbraucherorientiert und es ist noch völlig unklar, ob Normalsterbliche diese verstehen oder annehmen werden.

2. Standards
Wir haben den Industriestandard UF2, aber was wir nicht haben, sind Standards zu Authentifizierungsstandards und -praktiken (die außerhalb der nationalen Regierungen durchgesetzt werden). Webseiten haben unterschiedlichste Anforderungen an die Passworterstellung – die Kombinationsmöglichkeiten von Zahlen, Sonderzeichen oder der Länge für Passwörter sind schier unendlich. Wir müssen jeden einzelnen Web-Entwickler davon überzeugen, Unterstützung für den U2F-Authentifizierungscode, Passkeys oder andere Standards zu implementieren.
Die Ansätze von Google, Apple, Facebook, Microsoft & Co. sind bereits sehr vielversprechend, aber das ist nur der Anfang. Wir brauchen Websites, die nicht nur Unterstützung bieten, sondern diese idealerweise auch auf eine einheitliche Weise kommunizieren.

3. Akzeptanz
Bequemlichkeit ist Verbrauchern wichtig. So antwortete der CISO eines großen Unternehmens in Kanada auf die Frage, warum sie keine MFA anbieten würden: „Wenn es optional ist, werden sich nur etwa zwei Prozent der Kunden dafür entscheiden. Wenn es nicht optional ist und die Kunden die Unannehmlichkeiten nicht mögen, werden sie zu einer anderen Bank wechseln. Ich mache mir keine Sorgen um die zwei Prozent, die sich anmelden würden, da sie ihr Online-Leben wahrscheinlich bereits sehr gut schützen. Ich mache mir Sorgen um die 98 Prozent und kann es mir nicht leisten, diese Kunden zu verprellen.“ Online-Dienste würden lieber Konten kompromittieren, als Kunden zu verlieren.

4. Freie Märkte
Wenn Märkte wie das Bankwesen nicht so reguliert sind, dass sie MFA zwingend umsetzen müssen, werden sie es nicht tun. Wenn Konkurrenten eine reibungslosere Nutzung bieten, dann wird niemand seinen Kunden die sicherere Sache aufzwingen. Die Banken wollen zufriedene Kunden. Und Kunden, die ihren Token in ihrer Ferienwohnung in Fort Lauderdale vergessen haben, sind ein sehr teures Problem.

„Verbraucher sollten Passwörter als Geheimnisse betrachten und sich vor Augen halten, wie gut Menschen darin sind, Geheimnisse zu bewahren“, so Chet Wisniewski, Cybersecurity-Experte bei Sophos. „Dieser Gedankengang führt unweigerlich zu einem Gespräch über Multi-Faktor-Authentifizierung, denn wenn ein Passwort nur ein Geheimnis ist, dann kann es gestohlen, belauscht oder sogar erraten werden. Im Gegensatz dazu kann etwas, das schwerer zu stehlen ist, z.B. ein Token oder eine 2FA- App, das digitale Leben mit einer im Verhältnis sehr kleinen ‚Unannehmlichkeit‘ viel sicherer machen. Mein grundlegender Rat ist deshalb: die Verwendung eines zweiten Authentifzierungsfaktors lohnt sich immer, da sie die Immunität gegen Angriffe auf fast 98 Prozent erhöht. Wer das zu unbequem findet, sollte 2FA zumindest für Dienste implementieren, bei denen die eigene Identität sehr ausgeprägt ausgestellt wird, wie E-Mail, Social Media oder Online-Banking. Die Menschen müssen begreifen, dass ihre Online- und Offline-Identitäten nicht länger zwei verschiedene Dinge sind. Die Kompromittierung eines einzigen E-Mail-Kontos könnte schließlich das gesamte Berufs- und Privatleben durcheinanderwirbeln.“

Abschließend noch eine Rangfolge der sichersten bis zu den unsichersten Optionen zur Authentifizierung:

1. USB/ Bluetooth-Token (U2F)
2. Biometrisch (Fingerabdruck/FaceID/etc.)
3. Authentifizierungs-Smartphone-App (Microsoft, Google, Deo, etc.)
4. SMS
5. Nur ein Passwort

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de