Sicherheit nur noch gegen Aufpreis? – Twitter schränkt 2FA ein

Twitter hat in letzter Zeit viele Schlagzeilen durch den Umgang mit Angestellten und Nutzern gemacht. Nun hat das soziale Netzwerk entschieden, seine Zwei-Faktor-Authentifizierung mit SMS-Login zu deaktivieren, weil diese von Betrügern missbraucht würden. Sophos Sicherheitsexperte Paul Ducklin ordnet das Risiko ein und gibt Tipps für Nutzer.

Die Änderung der Zwei-Faktor-Authentisierung (2FA) bei Twitter kommt überraschend: Da Textmeldungen zu unsicher seien, um 2FA durchzuführen, müsse man für diesen Service bei dem sozialen Netzwerk in Zukunft bezahlen. Ab wann genau die Nutzer (nur diejenigen, die nicht den zahlungspflichtigen Twitter Blue-Dienst verwenden) mit dieser Umstellung rechnen müssen, wird nicht so ganz deutlich. Twitter selbst hat den Nutzern von SMS-basierter 2FA mit seiner Verkündung am 15. Februar „30 Tage Zeit zur Deaktivierung dieser Methode und Anmeldung einer neuen“ gegeben. Fest steht: nach dem 20. März wird die 2FA-Methode via SMS für Konten, die noch aktiviert sind, deaktiviert.

Warum wird die SMS für die 2FA als unsicher angesehen?
Twitter hat entschieden, dass einmalige Sicherheitscodes, die via SMS verschickt werden, nicht mehr sicher sind, da sie der Erfahrung nach bereits missbräuchlich verwendet wurden. Der Haupteinwand gegen SMS-basierte 2FA ist, dass Cyberkriminelle schlichtweg Mitarbeiter von Mobilfunkunternehmen austricksen, überreden oder bestechen, damit sie ihnen Ersatz-SIM-Karten aushändigen, die mit der Telefonnummer einer anderen Person programmiert sind. Legales Ersetzen einer verlorenen, kaputten oder gestohlenen SIM-Karte ist natürlich ein wünschenswerter Service des Mobilfunknetzwerkes, sonst müsste man bei jeder neuen SIM auch immer die Telefonnummer ändern

Nachdem Betrüger aber mit geschickten Social Engineering-Fähigkeiten die Telefonnummern von Bürgern „übernommen“ haben – normalerweise, um deren 2FA-Codes abgreifen zu können – sank das Ranking der Textnachricht als sichere 2FA-Quelle. Diese kriminelle Art des „SIM-Swapping“ ist in Wahrheit aber gar kein Tausch, denn eine SIM-Karte kann nur mit einer einzigen Telefonnummer programmiert werden. Wenn also ein Mobilfunkunternehmen eine SIM-Karte austauscht, dann findet hier kein Wechsel statt, sondern, die alte SIM-Karte ist tot und funktioniert nicht mehr.

Für den Nutzer, der seine eigen SIM-Karte austauscht, weil sein Handy gestohlen wurde, ist das eine sehr nützliche Sicherheitsfunktion, da er so seine eigene Nummer zurückerhält und der Dieb nicht auf seine Kosten telefonieren oder Nachrichten und Anrufe abhören kann. Aber: wenn die SIM-Karte illegal in Betrügerhände gerät, wird diese Funktion gleich zweifach gefährlich. Kriminelle erhalten dann die Nachrichten, die für den Nutzer bestimmt sind, inklusive Login-Codes und der Nutzer kann sein eigenes Telefon nicht verwenden, um das Problem zu melden.

Geht es bei diesem Verbot wirklich um Sicherheit?
Geht es Twitter wirklich um Sicherheit oder nur um eine Verschlankung seiner IT, indem es die versendeten Textnachrichten reduziert? Es ist verwunderlich, dass nicht alle Nutzer von der SMS-basierten 2FA hin zu einer sichereren Methode geleitet werden, sondern nur diejenigen, die nicht den kostenpflichtigen Twitter Blue-Dienst verwenden. Diese dürfen weiterhin die SMS-Methode nutzen.

SIM-Swapping ist für Cyberkriminelle mit einigem Aufwand verbunden und daher keine Massenware. Immerhin müssen sie ihre Anonymität verlassen und physisch in einem Mobilfunkgeschäft versuchen, eine bestimmte Nummer zu bekommen. Diese Art des Betrugs ist geplant und zielgerichtet für ein ganz bestimmtes Konto, für das die Kriminellen bereits Benutzernamen und Kennwort haben, und bei dem sie annehmen, dass der Wert des Kontos das Risiko, ertappt zu werden, übersteigt. Daher raten wir: Wenn man sich für den Twitter Blue Dienst entscheidet, sollte man keine SMS-basierte 2FA mehr verwenden, selbst wenn man dazu berechtigt ist.

Das sollten Twitter-Nutzer jetzt tun:

- Wer Twitter-Blue-Mitglied ist oder jetzt werden will, sollte sich von der SMS-basierten 2FA verabschieden. Denn wenn diese Methode für die große Anzahl der nicht Blue-Nutzer sicherheitsbedenklich ist, dann natürlich auch für die kleinere Gruppe der Blue-Mitglieder.
- Wer kein Blue-Anwender mit aktivierter SMS-2FA ist, sollte zur App-basierten 2FA wechseln. Auf keinen Fall die 2FA auslaufen lassen und zur veralteten Passwort-Authentifizierung zurückkehren. Schließlich hat der Nutzer erst einmal die unbequeme Hürde zur 2FA genommen und sollte jetzt auch an der Sicherheitsfront vorn dabeibleiben.
- Wer Twitter zur 2FA-Bestimmung seine Telefonnummer gegeben hat, sollte diese nun löschen, da das Unternehmen das nicht selbst automatisch macht.
- Nutzer von App-basierter Authentifikation sollten sich bewusst machen, dass ihre 2FA Codes nicht sicherer gegen Phishing sind als eine SMS. App-basierte 2FA Codes sind allerdings generell durch den Sperrcode des Telefons geschützt und können nicht auf dem Telefon einer anderen Person berechnet werden – selbst, wenn diese die Nutzer-SIM-Karte ins Handy legt.
- Anwender sollten hellhörig werden, wenn das Telefon unerwartet den Mobilfunkdienst verliert. Hier sollten sie nachforschen, ob die SIM-Karte ausgetauscht wurde. Selbst wenn Nutzer das Telefon nicht für 2FA-Codes verwenden, kann ein Betrüger, der die Kontrolle über die Telefonnummer des Opfers hat, trotzdem Nachrichten in seinem Namen senden und empfangen sowie Anrufe tätigen oder annehmen – und das alles, während er vorgibt, das Opfer zu sein. Wenn der Verdacht einer Übernahme besteht, sollte der Nutzer seinen Mobilfunkanbieter kontaktieren oder am besten persönlich in einem Mobilfunkgeschäft vorstellig werden, inklusive Ausweis und Kontobelegen.
- Wer noch keinen PIN-Code auf seiner SIM-Karte eingerichtet hat, sollte das jetzt tun. Ein Dieb, der das Telefon stiehlt, wird es wahrscheinlich nicht entsperren können. Er könnte aber die SIM-Karte herausnehmen, in ein anderes Gerät einlegen und Anrufe und Nachrichten übernehmen. Die PIN für die SIM-Karte muss man nur beim Neustart oder nach dem Ausschalten eingeben.

Noch ein kurzer Nachtrag zum Wechsel auf die App-basierter 2FA: Diese ist von ihren Schritten nicht wesentlich aufwändiger als die Legitimation via SMS: denn auch hier muss man das Handy in die Hand nehmen, den Code aber statt als Textnachricht von der App ablesen. Also kein größerer Aufwand, aber mit hoher Wirkkraft.

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