KnowBe4

Auch die MFA kann geknackt werden – mithilfe von Social Engineering

Nachdem Cyberkriminelle jahrzehntelang mit Angriffen auf Konten mit einfacher Authentifizierung (d. h. Nutzername + Passwort) erfolgreich waren, wird seit einigen Jahren meist die Multi-Faktor-Authentifizierung (MFA) aktiviert. Heute haben Sie bei beliebten Websites und Services, darunter Google, Microsoft, Facebook und X, die Wahl zwischen der herkömmlichen Lösung aus Nutzername und Passwort und deutlich sichereren MFA-Optionen.

Früher wurde die MFA nur von Organisationen und Websites mit höchsten Sicherheitsanforderungen vorausgesetzt. Heute gehören MFA-Codes zu unserem Alltag und deren Nutzung ist mit nur geringen Kosten verbunden.

Die breite Einführung von MFA-Lösungen ist eine positive Entwicklung. Dadurch können viele Bedrohungen abgewehrt werden, die bei einer einfachen Authentifizierung erfolgreich wären. Die Vorteile der MFA wurden jedoch so häufig hervorgehoben, dass manchmal fälschlicherweise angenommen wird, die MFA sei vor allen Angriffen geschützt. Beispielsweise gehen viele MFA-Administratorinnen und -Administratoren sowie Nutzerinnen und Nutzer davon aus, dass Phishing per E-Mail keine Bedrohung mehr darstellt, da lediglich Anmeldedaten entwendet werden können. Das stimmt jedoch nicht.

Obwohl sich durch MFA-Lösungen bestimmte Sicherheitsrisiken reduzieren lassen, können viele Angriffe genauso erfolgreich durchgeführt werden wie bei herkömmlichen Authentifizierungslösungen. MFA-Lösungen sind sicherer, aber nicht unhackbar.

Hacken der Multi-Faktor-Authentifizierung

Es gibt zahlreiche Möglichkeiten zum Hacken der MFA – egal, was die Anbieter von MFA-Lösungen behaupten. Je höher die Sicherheit eines Kontos (z. B. durch Einführung der MFA), desto größer ist die Belastung für Endnutzerinnen und Endnutzer. Mehr Sicherheit bedeutet immer auch weniger Benutzerfreundlichkeit. Die MFA ist da keine Ausnahme.

Cyberkriminelle haben zum Hacken der MFA im Grunde vier Möglichkeiten: Social-Engineering-Hacks, technische Manipulation, physische Angriffe und gemischte Hacks.

Social Engineering	Technische Manipulation	Physische Angriffe	Gemischte Hacks
Beim Social Engineering sollen Endnutzerinnen und Endnutzer dazu gebracht werden, MFA-Lösungen so einzusetzen, dass diese unbeabsichtigt umgangen oder missbraucht werden.	Technische Manipulation bezieht sich auf technische Exploits und Manipulationen, bei denen es nicht auf menschliche Fehler ankommt.	Bei physischen Angriffen werden z. B. Fingerabdrücke von Geräten oder Tastaturen kopiert.	Bei vielen MFA-Hacks werden zwei oder mehr Methoden kombiniert. Am häufigsten ist die Kombination von Social-Engineering-Hacks und technischer Manipulation.

Die 15 gängigsten Taktiken im Rahmen der vier genannten Möglichkeiten:

Social-Engineering-Hacks

- Gefälschte Authentifizierung
- Angriffe über Sicherheitsfragen zum Zurücksetzen von Passwörtern
- Tarnung als Teammitglied des technischen Supports

Technische Manipulation

- Prognose der eindeutigen Sitzungskennung
- Man-in-the-Endpoint-Angriffe
- Schädliche MFA-Software- oder Hardwareänderung
- Generatoren für doppelte Codes
- Skimming-Angriffe
- Identitätsdiebstahl
- Brute-Force-Angriffe
- Fehlerhafte MFA
- Physische Angriffe

Gemischte Hacks

- Session Hijacking
- SIM-Swap-Angriffe
- Downgrade-/Recovery-Angriffe

Das menschliche Element beim Hacken von MFAs: Social Engineering

Social Engineering stellt bei Versuchen, die MFA zu umgehen, die größte Gefahr dar. Social Engineering und Phishing sind die Premium-Werkzeuge im Repertoire von kriminellen Hackerinnen und Hackern. Cyberkriminelle setzen auf Manipulation und Täuschung, um menschliche Schwächen auszunutzen und Sicherheitsmechanismen wie die MFA zu umgehen.

Beim Phishing, einer weit verbreiteten Social-Engineering-Technik, wird versucht, Personen zu täuschen und zur Herausgabe sensibler Daten wie Nutzernamen, Passwörter oder MFA-Codes zu bewegen. Cyberkriminelle geben sich in E-Mails, Textnachrichten und Telefonaten als Mitglieder vertrauenswürdiger Organisationen aus und drängen die Opfer zu unüberlegten Handlungen, indem ein Eindruck von Dringlichkeit erzeugt wird oder Drohungen ausgesprochen werden. Durch teilweise recht gut gemachte Kopien von E-Mails seriöser Banken, Dienstanbieter oder Teammitglieder schaffen es die angreifenden Personen, ihre Opfer zur Herausgabe der Anmeldedaten und der MFA-Codes zu bewegen.

Häufig werden dafür sogar eigens Websites gefälscht, die den seriösen Websites fast bis aufs Pixel gleichen. Nutzerinnen und Nutzer, die unbedacht eine anscheinend vertraute Website aufrufen, geben dort Anmeldedaten und MFA-Codes ein, die Cyberkriminellen die Tür in das System öffnen. In Phishing-Kampagnen mit E-Mails werden Mitteilungen gesendet, die auf den ersten Blick glaubhaft erscheinen. Die Empfängerinnen und Empfänger werden dazu aufgefordert, auf schädliche Links zu klicken oder infizierte Anhänge herunterzuladen. Doch ein Klick reicht aus, um sensible Daten zu kompromittieren.

Cyberkriminelle nutzen auch aus, dass Autoritätspersonen meist Vertrauen entgegengebracht wird. Hackerinnen und Hacker geben sich als Mitglieder des IT-Supports, Führungskräfte oder Mitarbeitende aus, um Personen MFA-Codes oder andere Angaben zur Authentifizierung zu entlocken. Wir haben einfach gelernt, den Anweisungen von Autoritätspersonen zu folgen. Social Engineers können dadurch jedoch die MFA knacken.

Schutz vor MFA-Angriffen

MFA-Lösungen sind als Cybersicherheitsmaßnahme nicht mehr wegzudenken. Die MFA ist jedoch nicht unhackbar und nicht sicher vor Phishing- oder Social-Engineering-Angriffen. Auch nach der Einführung von MFA-Lösungen bleibt Security Awareness Training in der allgemeinen Sicherheitsstrategie unerlässlich.

Ihre Organisation kann sich wie folgt vor Social-Engineering-Hacks und technischer Manipulation schützen.

Human Firewall

Organisationen und Einzelpersonen müssen sich mit Cybersicherheit auseinandersetzen und ihre Security Awareness stärken. In Trainingsprogrammen lernen die Teilnehmenden, Phishing zu erkennen, E-Mails oder Textnachrichten auf deren Echtheit zu prüfen und eine gesunde Dosis Skepsis an den Tag zu legen. Dies kann die Gefahr von Social Engineering erheblich eindämmen. Fortschrittliche Systeme zur Erkennung von Bedrohungen, die Nutzerverhalten und Kommunikationsmuster analysieren, können ebenfalls die allgemeine Sicherheit erhöhen, indem potenzielle Bedrohungen identifiziert und abgewendet werden, bevor sie zur Offenlegung sensibler Daten führen.

Security Awareness Training schärft darüber hinaus das Verständnis der Bedeutung der Multi-Faktor-Authentifizierung. Die Teilnehmenden erfahren, inwieweit durch die MFA eine zusätzliche Sicherheitsebene geschaffen wird, für die weitere Formen der Identifikation wie Passwörter oder Einmalcodes erforderlich sind. Wissen fördert das Verständnis für bestehende Schutzmaßnahmen und motiviert Einzelne dazu, Best Practices bei der Nutzung von MFA zu befolgen. Dadurch verringert sich die Wahrscheinlichkeit, selbst zum Opfer zu werden.

Sechs wichtige Erkenntnisse:

- Nichts – auch keine MFA-Lösung – ist unhackbar.
- Die Aufklärung über MFA-Hacking gehört in jedes Security Awareness Training.
- Lassen Sie sich nicht zum Klicken auf schädliche Links verleiten.
- Blockieren Sie schädliche Links.
- Stellen Sie sicher, dass Ihre Mitarbeitenden eine URL vor dem Klicken auf deren Echtheit hin prüfen.

Technische Schutzmaßnahmen

- Machen Sie die Verwendung der MFA verpflichtend Voraussetzung fest, sofern möglich.
- Deaktivieren Sie die SMS-basierte MFA, sofern möglich.
- Verwenden Sie „1:1“-MFA-Lösungen, bei denen vorab eine Geräteregistrierung beim Server der Organisation erforderlich ist.
- Aktivieren Sie die Zwei-Wege- bzw. gegenseitige Authentifizierung, sofern möglich.

- Überprüfen Sie, ob Ihre MFA-Lösung gegen den Diebstahl von Sitzungstoken und/oder vor Replay-Angriffen geschützt ist.
- Informieren Sie sich darüber, welchen Schutz vor Social Engineering Ihr MFA-Anbieter bietet.
- Stellen Sie sicher, dass Ihr MFA-Anbieter einem Konzept zur Entwicklung sicherer Software folgt (Secure Development Lifecycle, SDL).
- Stellen Sie sicher, dass bei zu vielen fehlgeschlagenen Anmeldeversuchen eine Kontosperrung erfolgt.
- Übermitteln Sie die Faktoren über verschiedene „Kanäle“ oder „Bänder“ (In-Band/Out-Of-Band).
- Schützen und kontrollieren Sie Identitätsattribute, die bei MFA-Anmeldungen zur eindeutigen Identifizierung verwendet werden.
- Nutzen Sie für Sicherheitsfragen zum Zurücksetzen von Passwörtern keine leicht erratbaren Antworten.
- Aktivieren Sie die dynamische Authentifizierung. Hier werden in Situationen mit höherem Risiko zusätzliche Faktoren verlangt.
- Informieren Sie sich über die Risiken, die von Systemen mit „gemeinsamen Geheimnissen“ ausgehen.
- Senden Sie Nutzerinnen und Nutzern bei transaktionsbasierten Authentifizierungen alle kritischen Angaben „Out-of-Band“, bevor die Bestätigung übermittelt/angefordert wird.

Fazit

Kriminelle Hackerinnen und Hacker setzen bei Angriffen weiterhin auf Social Engineering und Phishing. Dies gilt auch für die Multi-Faktor-Authentifizierung. Auch neuere Technologien sind vor Social Engineering nicht geschützt. Dabei werden die Angriffe immer ausgefeilter. Der Faktor Mensch muss bei der Abwehr von Cyberbedrohungen unbedingt berücksichtigt werden. Die Einführung von umfassenden Programmen für Security Awareness Training ist ein wichtiger Schritt zur Stärkung der Human Firewall.

KnowBe4 Germany | Rheinstr. 45/46 | 12161 Berlin – Deutschland | knowbe4.de | +49 30 34 64 64 60 | kontakt@knowbe4.com