VERBESSERUNG DER DIGITALEN SICHERHEIT

MIT MULTI-FAKTOR-AUTHENTIFIZIERUNG

WAS IST MULTI-FAKTOR-AUTHENTIFIZIERUNG?

Die Multi-Faktor-Authentifizierung (MFA) ist eine Sicherheitsmethode, bei der Benutzer zwei oder mehr Verifizierungsfaktoren für den Zugriff auf eine Ressource wie etwa eine Anwendung, ein Online-Konto oder ein VPN benötigen. Angesichts der wachsenden Anzahl an Cyberbedrohungen und Datenschutzverletzungen ist es von entscheidender Bedeutung, über starke Authentifizierungsmethoden zu verfügen, um Online-Konten und sensible Informationen zu schützen.

MFA kombiniert zur Erhöhung der Sicherheit oft etwas, das Sie kennen (ein Passwort), etwas, das Sie haben (ein Sicherheitstoken) und Ihr physisches Abbild (biometrische Daten). Dies fügt eine zusätzliche Schutzebene hinzu, die über ein einzelnes Passwort hinausgeht.

ARTEN DER MULTI-FAKTOR-AUTHENTIFIZIERUNG

1. SMS-BASIERTE AUTHENTIFIZIERUNG

So funktioniert's: Ein Einmal-Passcode (OTP) wird per SMS auf Ihr Mobiltelefon gesendet. Diesen Code geben Sie in das System ein, um Zugang zu erhalten.

Vorteile: Einfach zu verwenden, keine besondere Hardware erforderlich.

Nachteile: Kann von Hackern abgefangen werden, ist von der Verfügbarkeit des Mobilfunknetzes abhängig.

2. E-MAIL-BASIERTE AUTHENTIFIZIERUNG

So funktioniert's: Ein OTP oder ein Verifizierungslink wird an Ihre registrierte E-Mail-Adresse gesendet.

Vorteile: Bequem, keine zusätzlichen Geräte erforderlich.

Nachteile: Anfällig für Phishing-Angriffe, kann verzögert werden, wenn die E-Mail-Server langsam sind.

3. AUTHENTIFIZIERUNGS-APPS

So funktioniert's: Softwareanwendungen generieren zeitbasierte OTPs, die Sie nach Ihrem Passwort eingeben.

Vorteile: Sicherer als SMS, funktioniert ohne Internetverbindung.

Nachteile: Erfordert ein Smartphone, kann unpraktisch sein, wenn das Gerät verloren geht.

4. BIOMETRISCHE AUTHENTIFIZIERUNG

So funktioniert's: Verwendet Fingerabdruck, Gesichtserkennung oder Netzhautscan zur Überprüfung der Identität.

Vorteile: Hochsicher, schnell und bequem.

Nachteile: Erfordert spezielle Hardware, kann zu Datenschutzbedenken führen.

5. HARDWARE-TOKEN

So funktioniert's: Physische Geräte generieren OTPs oder verwenden zur Authentifizierung USB/NFC-Tags.

Vorteile: Äußerst sicher, immun gegen Phishing.

Nachteile: Kostspielig, kann verloren gehen oder gestohlen werden.

GRÜNDE FÜR DIE VERWENDUNG VON MULTI-FAKTOR-AUTHENTIFIZIERUNG

- **Verbesserte Sicherheit:** Die Implementierung von MFA bietet eine zusätzliche Sicherheitsebene, die über Passwörter hinausgeht.
- **Schützt sensible Daten:** Es ist entscheidend für Schutz persönlicher und geschäftlicher Informationen.
- **Compliance:** Hilft bei der Einhaltung von Unternehmens- und behördlichen Anforderungen an den Datenschutz.
- **Reduziert Betrug:** Minimiert das Risiko von unbefugtem Zugriff und Betrug.

MFA ist ein einfaches, aber leistungsstarkes Werkzeug, mit dem Sie Ihre Online-Sicherheit erheblich verbessern können. Durch die Nutzung einer oder mehrerer der verschiedenen Arten von MFA können Sie sich und Ihr Unternehmen vor unbefugtem Zugriff und potenziellen Cyberbedrohungen schützen.

SO ERKENNEN SIE EINE PHISHING-NACHRICHT

Die Fähigkeit, eine Phishing-E-Mail zu identifizieren, ist entscheidend, um sensible Informationen vor Cyberkriminellen zu schützen. Da Phishing-E-Mails darauf abzielen, Empfänger dazu zu verleiten, vertrauliche Informationen wie Passwörter, Kreditkartendaten und andere persönliche Daten preiszugeben, stellen sie erhebliche Gefahren dar.

Betrüger tarnen sich oft als vertrauenswürdige Unternehmen, wodurch diese Betrügereien schwer zu erkennen sind. Opfer eines Phishing-Angriffs zu werden, kann schwerwiegende Folgen haben, darunter Identitätsdiebstahl, finanzielle Verluste und unbefugter Zugriff auf persönliche und Unternehmenskonten.

Die Fähigkeit, Phishing-E-Mails effektiv zu erkennen und zu melden, ist entscheidend, um sich und Ihr Unternehmen vor einem Cyberangriff zu schützen. Zu den wichtigsten Indikatoren einer Phishing-E-Mail gehören:

1. VERDÄCHTIGE ADRESSE DES ABSENDERS:

Oft stammen Phishing-E-Mails von einer Adresse, die legitim aussieht, aber leichte Rechtschreibfehler oder zusätzliche Zeichen enthält.

2. UNBEKANNTE ODER ALLGEMEINE BEGRÜSSUNGEN:

Phishing-E-Mails verwenden in der Regel allgemeine Anreden wie „Sehr geehrte Kunden“, anstatt Sie mit Namen anzusprechen.

3. DRINGENDE ODER BEDROHLICHE SPRACHE:

Cyberkriminelle versuchen oft, ein Gefühl von Dringlichkeit hervorzurufen, indem sie beispielweise andeuten, dass Ihr Konto geschlossen wird oder Sie sofort handeln müssen, um ein Problem zu beheben.

4. UNGEWÖHNLICHE ANHÄNGE ODER LINKS

Phishing-E-Mails können unerwartete Anhänge oder Links enthalten. Um die Legitimität eines Links zu bestätigen, bewegen Sie den Mauszeiger darüber, bevor Sie darauf klicken.

5. ANFRAGE NACH PERSÖNLICHEN INFORMATIONEN:

Seriöse Organisationen werden Sie niemals darum bitten, vertrauliche Informationen wie Passwörter, Kreditkartendaten oder Sozialversicherungsnummern per E-Mail anzugeben. Wenn der Absender Sie auffordert, diese Art von Informationen per E-Mail preiszugeben, handelt es sich wahrscheinlich um einen Phishing-Versuch.

6. RECHTSCHREIB- UND GRAMMATIKFEHLER:

Viele Phishing-E-Mails enthalten auffällige Rechtschreib- und Grammatikfehler, die in einer professionellen Kommunikation unüblich sind.

7. NICHT ÜBEREINSTIMMENDE URLS:

Eine Phishing-E-Mail kann URLs enthalten, die nicht mit dem Text übereinstimmen, auf den sie verlinkt sind, oder sie leiten Sie möglicherweise auf eine andere als die erwähnte Website weiter.

Wenn Sie sich dieser Indikatoren bewusst sind, können Sie vermeiden, Opfer von Phishing-Betrug zu werden. Sobald Sie wissen, wie Sie einen Phish erkennen, können Sie mehr fangen.

WIE HACKER VERSUCHEN, SIE AUSZUTRICKSEN

Da Cyberangriffe immer ausgefeilter werden, müssen Mitarbeiter wachsam sein und sich der Vielzahl von Möglichkeiten bewusst sein, wie Hacker Zugriff auf sensible Informationen erhalten können. Von Phishing-Angriffen bis hin zu Deepfakes entwickeln Cyberkriminelle ihre Methoden ständig weiter.

HIER SIND EINIGE DER MÖGLICHKEITEN, WIE SIE EINEM RISIKO FÜR CYBERKRIMINALITÄT AUSGESETZT SEIN KÖNNTEN:

SCANNEN EINES QR-CODES

QR-Codes sind überall, von Restaurants über Werbung bis hin zu Visitenkarten. Sie sind zwar sehr praktisch, stellen aber auch ein erhebliches Risiko dar. Cyberkriminelle verwenden bösartige QR-Codes, die direkt auf Phishing-Websites verlinken, um Ihre persönlichen Daten zu stehlen oder Ihr Gerät mit Malware zu infizieren.

Drei Möglichkeiten, um sicher zu bleiben:

- Überprüfen Sie die Quelle des QR-Codes.
- Vermeiden Sie das Scannen von QR-Codes von unbekannten oder verdächtige Quellen.
- Verwenden Sie QR-Code-Scanner, die URLs überprüfen können, bevor Sie sie öffnen.

PER SMS

Hacker versenden irreführende Textnachrichten, um Menschen dazu zu verleiten, private Daten weiterzugeben oder auf einen bösartigen Link zu klicken. Diese Nachrichten scheinen oft aus einer vertrauenswürdigen Quelle zu stammen, z. B. von einer Bank oder einer Regierungsbehörde.

Drei Möglichkeiten, um sicher zu bleiben:

- Seien Sie vorsichtig bei unerwünschten Textnachrichten, insbesondere diejenigen, die nach persönlichen Informationen fragen.
- Klicken Sie nicht auf Links und laden Sie keine Anhänge von unbekannten Absendern herunter.
- Überprüfen Sie die Legitimität des Textes, indem Sie sich direkt an die Organisation wenden.

ÜBER DAS TELEFON

Betrüger rufen oft Personen an und geben sich als berechtigte Personen aus, um vertrauliche Informationen zu erlangen. Diese Anrufer verwenden oft eine manipulative Sprache, um ein Gefühl der Dringlichkeit oder Angst zu erzeugen.

Drei Möglichkeiten, um sicher zu bleiben:

- Geben Sie keine personenbezogenen Daten über das Telefon weiter, solange Sie sich nicht über die Identität des Anrufers im Klaren sind.
- Überprüfen Sie die Anmeldeinformationen des Anrufers, indem Sie sich direkt an die Organisation wenden.
- Seien Sie skeptisch bei unerwünschten Anrufen, die nach sensiblen Informationen fragen.

ÜBER DIE SCHULTER

Angreifer schauen Ihnen über die Schulter, um Ihren Bildschirm oder Ihre Tastatur zu beobachten und vertrauliche Informationen wie Passwörter und PINs zu stehlen. Diese Taktik, die als „Shoulder Surfing“ oder „Schulter-Surfen“ bezeichnet wird, kann an öffentlichen Orten wie Cafés, Flughäfen oder sogar in Ihrem Büro auftreten.

Drei Möglichkeiten, um sicher zu bleiben:

- Achten Sie auf Ihre Umgebung, wenn Sie sensible Informationen eingeben.
- Verwenden Sie einen Sichtschutz auf Ihren Geräten und sperren Sie sie, wenn sie unbeaufsichtigt sind.
- Schirmen Sie Ihre Tastatur ab, wenn Sie Passwörter oder PINs eingeben.

DURCH DIE AUSGABE VON JEMANDEM, DEM SIE VERTRAUEN

Deepfakes nutzen künstliche Intelligenz, um hyperrealistische, aber gefälschte Videos oder Audioaufnahmen zu erstellen. Cyberkriminelle können Deepfakes verwenden, um sich als Führungskräfte oder andere vertrauenswürdige Personen auszugeben, was zu erheblichen Sicherheitsverletzungen führt.

Drei Möglichkeiten, um sicher zu bleiben:

- Seien Sie vorsichtig bei unerwarteten oder ungewöhnlichen Anfragen, auch wenn sie von bekannten Personen zu stammen scheinen.
- Überprüfen Sie die Identität der Person, die die Anfrage stellt, über mehrere Kanäle.
- Bleiben Sie auf dem Laufenden über die neuesten Entwicklungen in der Deepfake-Technologie.

PHISHME
COFENSE
E-MAIL-SICHERHEIT

SO BLEIBEN SIE SICHER

BEI DER VERWENDUNG VON KI-CHATBOTS

Chatbots mit künstlicher Intelligenz (KI) bieten Komfort, können aber auch Sicherheitsrisiken bergen. Mit dem zunehmenden Einsatz von KI-Chatbots wie ChatGPT müssen Sie Folgendes tun, um Ihre Privatsphäre zu schützen und eine Sicherheitsverletzung zu vermeiden.

1. DIE RISIKEN VERSTEHEN

- ***Phishing-Angriffe:*** Bösartige Bots geben sich als legitime Dienste aus, um Ihre Daten zu stehlen.
- ***Verbreitung von Malware:*** KI-Bots können verwendet werden, um schädliche Software zu verbreiten.
- ***Datenschutz:*** Vertrauliche Informationen, die an Bots weitergegeben werden, können abgefangen oder missbraucht werden.

2. VERTRAUENSWÜRDIGE DIENSTE VERWENDEN

- ***Überprüfen Sie die Legitimität:*** Verwenden Sie nur Chatbots von renommierten Unternehmen.
- ***Achten Sie auf Sicherheitssiegel:*** Stellen Sie sicher, dass der Dienst über angemessene Sicherheitszertifizierungen verfügt.

3. IHRE PERSÖNLICHEN DATEN SCHÜTZEN

- ***Vermeiden Sie die Weitergabe sensibler Daten:*** Geben Sie niemals persönliche, finanzielle oder Anmeldedaten an KI-Chatbots weiter.
- ***Verwenden Sie sichere Passwörter:*** Stellen Sie sicher, dass Ihre Passwörter komplex und einzigartig sind.

4. REGELMÄSSIG AKTUALISIEREN

- ***Halten Sie die Software auf dem neuesten Stand:*** Stellen Sie sicher, dass Ihre Antiviren- und andere Sicherheitssoftware auf dem aktuellen Stand ist.
- ***Nach Bot-Updates suchen:*** Verwenden Sie Chatbots, die ihre Sicherheitsprotokolle regelmäßig aktualisieren.

5. AKTIVITÄT ÜBERWACHEN

- ***Überprüfen Sie regelmäßig die Kontoauszüge:*** Überwachen Sie Bank- und Kreditkartenabrechnungen auf nicht autorisierte Transaktionen.
- ***Bleiben Sie informiert:*** Bleiben Sie auf dem Laufenden über die neuesten Nachrichten zur Cybersicherheit, um sich über neue Bedrohungen im Klaren zu sein.

6. VERDÄCHTIGE AKTIVITÄTEN MELDEN

- ***Kontaktieren Sie den Support:*** Wenn Sie den Verdacht haben, dass ein Bot bösartig ist, melden Sie dies sofort dem Dienstanbieter.
- ***Warnen Sie die Behörden:*** Benachrichtigen Sie lokale oder nationale Cybersicherheitsbehörden über Sicherheitsverletzungen.