Die größten Cybersecurity-Bedrohungen 2026

Die gefährlichsten Bedrohungen sind nicht immer die lautesten, sondern diejenigen, die sich unauffällig einfügen und das Vertrauen in das System ausnutzen. Da sich Angreifer an bessere Kontrollen und den zunehmenden Einsatz von KI anpassen, legen einige Bedrohungsmuster schneller an Tempo zu, als Unternehmen Schritt halten können.

Social Engineering in großem Stil

Generative KI ermöglicht hyperpersonalisierte Phishing-, Vishing- und Identitätsnachahmungs-Kampagnen, die für Benutzer (und Filter) nur schwer erkennbar sind.

- Deepfakes von Führungskräften und Anbietern
- Kontextbezogene Köder, trainiert mit öffentlichen Daten
- Automatisiertes Testen und Optimieren von Kampagnen

Bedeutung: Vertrauen (nicht Technologie) wird zur primären Angriffsfläche.

Identitätszentrierte Angriffe

Angreifer verschaffen sich zunehmend Zugang, indem sie sich als Mitarbeiter oder bekanntes Unternehmen anmelden, anstatt das Unternehmen direkt anzugreifen.

- MFA-Ermüdung und Token-Diebstahl
- Übernahmen von SaaS-Accounts
- Missbrauch von Identitäten mit übermäßigen Privilegien

Bedeutung: Herkömmliche Perimeter- und Endpunkt-verteidigungsmaßnahmen werden gar nicht ausgelöst.

Seitwärtsbewegung in Cloud/SaaS

Kompromittierte Zugangsdaten werden verwendet, um unbemerkt zwischen Cloud-Apps zu wechseln, den Zugriff auszuweiten und Daten ohne Malware zu exfiltrieren.

- Missbrauch von OAuth-Tokens
- Erweiterung von Schatten-SaaS
- Datenexfiltration über legitime APIs

Bedeutung: Sicherheitsverstöße sehen wie normale Benutzeraktivität aus.

Ransomware-Kampagnen mit Mehrfach-Erpressung

Ransomware-Praktiken haben sich über die bloße Verschlüsselung hinaus weiterentwickelt und umfassen jetzt Datendiebstahl, Belästigung und Androhung von Reputationsschäden.

- Doppelte und dreifache Erpressung
- Angriffe auf Backup- und Recovery-Systeme
- Datenlecks werden so geplant, dass sie maximale Wirkung zeigen

Bedeutung: Der Sicherheitsvorfall lässt sich nicht mehr allein nur durch Wiederherstellen beheben.

splunk>
a CISCO company

Angriffe auf Software und Lieferkette

Angreifer nutzen vertrauenswürdige Software, Updates und Anbieter aus, um sich Erstzugriff zu verschaffen.

- Kompromittierte Abhängigkeiten
- Böswillige Updates
- Missbrauch von Drittanbieterzugriff

Bedeutung: Vertrauenswürdige Beziehungen werden zu Angriffspfaden.

Living-off-the-Land-Angriffe (LotL)

Bedrohungsakteure bleiben unauffällig, indem sie native Tools und Administrations-Dienstprogramme missbrauchen.

- Missbrauch von PowerShell, WMI und CLI
- Minimaler Malware-Fußabdruck
- Forensische Sichtbarkeit ist schwierig

Bedeutung: Es gibt keine Auffälligkeiten, bis es zu spät ist.

API-zentrierte Angriffe

Da APIs die Grundlage moderner Anwendungen und Integrationen sind, nehmen Angreifer schwache Authentifizierungsmechanismen und ungewöhnlich weitreichende Berechtigungen ins Visier.

- Fehlerhafte Autorisierung auf Objektebene
- Geleakte Tokens
- Missbrauch undokumentierter Endpunkte

Bedeutung: APIs geben Daten und Funktionalität in großem Maßstab preis.

Ausnutzung neu bekannt gegebener Schwachstellen

Die Time to Exploit (TTE) sinkt massiv.

- Instrumentalisierung als Waffe innerhalb von Stunden
- Automatisiertes Scannen und Ausnutzen
- Patch-Lücken werden in großem Stil ausgenutzt

Bedeutung: Erkennungs- und Reaktionszeit sind genauso wichtig wie Vorbeugung.

Verwandeln Sie Bedrohungs-bewusstsein in Taten

Laden Sie unsere neueste Ausgabe von Die 50 größten Cybersecurity-Bedrohungen herunter, um die gängigsten Bedrohungstypen kennenzulernen, zu erfahren, wie und warum sie sich weiterentwickeln, sowie Tipps für eine zielgerichtete Abwehr zu erhalten. Wenn Sie dann bereit sind, Ihr Wissen in die Tat umzusetzen, kann Splunk Ihnen helfen, Ihren Sicherheitsbetrieb mit Transparenz und Geschwindigkeit zu optimieren.

splunk> a cisco company

26_CMP_cheat sheet_Top-cybersecurity-threats_v11_digital