

The background is a dark field filled with white binary code (0s and 1s). Overlaid on this are several large, overlapping circles. Some circles are solid black, while others are white with a black outline. A horizontal band of color, transitioning from orange on the left to pink on the right, runs across the middle of the image, serving as a backdrop for the title text.

# Die 50 größten **Cybersecurity- Bedrohungen**

splunk®

# Inhalt

|                                        |    |                                                |    |                                               |     |
|----------------------------------------|----|------------------------------------------------|----|-----------------------------------------------|-----|
| Account-Übernahme . . . . .            | 5  | Insider-Bedrohungen. . . . .                   | 39 | Router- und Infrastrukturangriffe . . . . .   | 73  |
| Advanced Persistent Threat . . . . .   | 7  | IoT-Bedrohungen . . . . .                      | 41 | Schädliche PowerShell . . . . .               | 75  |
| Angriff auf die Lieferkette . . . . .  | 9  | Kompromittieren privilegierter Benutzer. . . . | 43 | Schatten-IT . . . . .                         | 77  |
| Application Access Token . . . . .     | 11 | Kompromitierte Zugangsdaten. . . . .           | 45 | Sim-Jacking. . . . .                          | 79  |
| AWS-Angriffe . . . . .                 | 13 | Kryptojacking-Angriff . . . . .                | 47 | Social-Engineering-Angriff. . . . .           | 81  |
| Brute-Force-Angriff. . . . .           | 15 | Makroviren. . . . .                            | 49 | Spear Phishing . . . . .                      | 83  |
| Business Email Compromise . . . . .    | 17 | Malware. . . . .                               | 51 | Spyware . . . . .                             | 85  |
| Cloud-Kryptomining . . . . .           | 19 | Man-in-the-Middle-Angriff. . . . .             | 53 | SQL Injection . . . . .                       | 87  |
| Command-and-Control-Angriffe . . . . . | 21 | Masquerade-Angriff . . . . .                   | 55 | Typosquatting . . . . .                       | 89  |
| Credential Dumping . . . . .           | 23 | Meltdown-and-Spectre-Angriff . . . . .         | 57 | Verdächtige Cloud-Speicheraktivitäten . . . . | 91  |
| Credential-Reuse-Angriff. . . . .      | 25 | Network Sniffing . . . . .                     | 59 | Watering-Hole-Angriff. . . . .                | 93  |
| Cross-Site Scripting . . . . .         | 27 | Open Redirection . . . . .                     | 61 | Web Session Cookie-Diebstahl . . . . .        | 95  |
| DNS Amplification. . . . .             | 29 | Pass the Hash. . . . .                         | 63 | Whale Phishing (Whaling). . . . .             | 97  |
| DNS Hijacking. . . . .                 | 31 | Phishing. . . . .                              | 65 | Zero-Day-Exploit . . . . .                    | 99  |
| DNS Tunneling . . . . .                | 33 | Phishing Payloads. . . . .                     | 67 | Mehr erfahren. . . . .                        | 101 |
| DoS-Angriff . . . . .                  | 35 | Ransomware . . . . .                           | 69 |                                               |     |
| Drive-by-Download-Angriff . . . . .    | 37 | Rechnungsbetrug. . . . .                       | 71 |                                               |     |

# Vorwort

Cybersicherheit ist heute wichtiger als jemals zuvor. Denn sie ist unverzichtbar, um all das zu schützen, worauf wir uns tagtäglich verlassen. Von Bankgeschäften und Online-Handel über die Entwicklung von Medikamenten und Impfstoffen bis hin zu einfacheren Dingen wie dem Schutz unserer Streaming-Dienste. Doch im Zuge der Massenmigration in die Cloud und der digitalen Transformation haben viele Unternehmen ihr optimales Sicherheitsniveau aufgrund vier maßgeblicher Herausforderungen noch längst nicht erreicht: In erster Linie zählt hierzu eine sich ständig weiterentwickelnde Bedrohungslandschaft, in der wir mit kreativen, finanziell gut ausgestatteten Akteuren zu tun haben. Aber auch die zunehmende Komplexität hybrider sowie Multi-Cloud-Umgebungen spielt eine Rolle. Ebenso Sicherheitsteams, die durch eine schier endlose Flut an monotonen Aufgaben und manuellen Prozessen ausgebremst werden. Nicht zu vergessen die unzähligen Datensilos, welche durch den Tool-Wildwuchs entstehen und Ineffizienz sowie blinde Flecken begünstigen.

Zusammen machen diese vier Herausforderungen eines deutlich: Sicherheit ist ein Datenproblem. Aus diesem Grund ist ein datenzentrierter Ansatz entscheidend. Denn dieser versorgt uns zur richtigen Zeit mit den richtigen Informationen. Und ermöglicht die gezielte Verbindung von Tools und Teams – trotz der Flut an Warnmeldungen und der Komplexität. Der Schlüssel zum Erfolg jedes Unternehmens ist eine analysegestützte Lösung, die sich auf End-to-End-Transparenz und Machine Learning (ML) stützt. Diese fortschrittlichen Fähigkeiten vermitteln Ihnen nicht nur ein vollständiges Bild Ihrer Umgebung. Ebenso lassen sich Prozesse weg von menschlichen Eingriffen und einfachen Diagnosen hin zu automatisierten, leistungsstarken Abwehrmechanismen verlagern.

Und wie soll das gelingen? Durch die gemeinsame Auswertung und Kontextualisierung riesiger Mengen hochkomplexer Datensätze. Durch das schnellere Reagieren auf Bedrohungen mithilfe automatisierter Abläufe. Durch das Entdecken anomalen Verhaltens mithilfe von sofort einsatzbereiten ML-Modellen und -Algorithmen. All dies hilft Unternehmen, ihre Cyber-Resilienz zu optimieren – also die Fähigkeit, Kompromittierungen oder Angriffen zuvorzukommen und sich auf etwaige Bedrohungen einzustellen. So können Sie die Sicherheitsprozesse in Ihre Unternehmen effektiver automatisieren und es besser schützen, während Sie gleichzeitig Wachstum und Innovation weiter vorantreiben.

Wir bei Splunk sind begeistert von den Möglichkeiten, die in Daten stecken – für eine *bessere und sicherere* Zukunft. Doch um dieses Ziel zu erreichen, müssen wir gewappnet sein. Wir müssen wissen, womit wir es zu tun haben – das gilt auch für die großen Bedrohungen, die sich zunehmend abzeichnen. Genau deshalb haben wir Ihnen in diesem Katalog die aktuell relevantesten Cyber-Sicherheitsbedrohungen zusammengestellt. Damit Sie die verschiedenen Arten von Angriffen besser erkennen, das Risiko mindern und den Schutz Ihres Unternehmens weiter stärken können.



**Gary Steele**

President und CEO, Splunk



Es wird wohl noch eine ganze Weile dauern, bis sich die Auswirkungen der Pandemiejahre auf die weltweite InfoSec-Landschaft erfassen lassen. Denn allein in diesem Zeitraum hat sich mehr getan, als viele Sicherheitsexperten in ihrer gesamten Laufbahn bis 2020 erlebt haben. Fakt ist: Die Herausforderungen, mit denen wir konfrontiert sind, sind größer als jemals zuvor.

Die große Kündigungswelle und die Burn-out-Problematik haben die Lage noch verschärft. Und das zu einem Zeitpunkt, in dem die IT-Sicherheitsbranche dringend Spitzenkräfte finden und halten sollte. Weil jene, die bisher noch nicht aufgegeben haben, von mehr Warnmeldungen als jemals zuvor überschwemmt werden und viel zu viel Zeit für wiederkehrende, manuelle Aufgaben aufwenden müssen. Eine Entwicklung, die der Arbeitsmoral nicht gerade zuträglich ist. Zudem fehlt ein umfassender Einblick in dringend benötigte Daten, um die größten Bedrohungen überhaupt verstehen zu können.

**Doch die Lage ist nicht aussichtslos. Zwar haben es die meisten SecOps-Plattformen bisher versäumt, das Thema Sicherheit als grundlegendes Datenproblem anzugehen. Doch genau hier verbirgt sich zugleich auch die größte Chance für Sicherheitsexperten.**

Weil die Fähigkeit, eine resiliente Cybersicherheit aufzubauen, direkt mit der Quantität und Qualität der gesammelten, analysierten und implementierten Daten zusammenhängt. Daten, die es für die Reduzierung des Unternehmensrisikos braucht. Gerade im Hinblick auf eine ungewisse Zukunft investieren viele Unternehmen in Resilienz, um auf aktuelle Bedrohungen reagieren und gestärkt daraus hervorgehen zu können.

In diesem Kontext bedeutet Resilienz: Flexibilität. Schnell. Vorbereitet. Proaktiv. Resiliente Unternehmen besitzen in der Regel eine starke Daten- und Technologiebasis, dank der sie schnell auf alles reagieren können. Resiliente Sicherheitsteams stellen Cyber-Sicherheitslösungen bereit, um jeden Aspekt des Unternehmens zu schützen, die Innovationskraft zu fördern und das Unternehmen zu stärken. Sie gehen Herausforderungen an, in dem sie Daten in den Mittelpunkt all ihrer Handlungen stellen. Mit dem Ergebnis, dass datenzentrierte Security Operations das Risiko von Datenschutzverletzungen, IP-Diebstahl und Betrug um bis zu 70 % senken können.

Vorausgesetzt man weiß, nach welchen Bedrohungen man Ausschau halten sollte. Und genau hier setzt dieses E-Book an. Auf der Grundlage von Untersuchungen des [Splunk Threat Research Teams](#) präsentieren wir Ihnen auf den folgenden Seiten die 50 größten Cyber-Sicherheitsbedrohungen, um Ihre Sicherheitsprofis dabei zu unterstützen, uns allen ein Gefühl von mehr Sicherheit zu geben.

# Account-Übernahme



Die Übernahme eines Accounts gilt als eine der gefährlichsten und skrupellosesten Methoden, um auf den Account eines Benutzers zuzugreifen. Dabei gibt sich der Angreifer in der Regel als echter Kunde, Benutzer oder Mitarbeiter aus und verschafft sich so Zugang zu den Accounts jener Person, für die er sich ausgibt.

Allein im Jahr 2022 wurden **84 % der Unternehmen Opfer identitätsbezogener Kompromittierungen**. 96 % gaben an, dass die Vorfälle durch die Implementierung identitätsbezogener Sicherheit hätte vermieden oder minimiert werden können.

Ohne die richtigen Technologien und Richtlinien (z. B. Zero Trust und Anbieter-Management) können Anomalien im User-Verhalten unglaublich schwierig zu entdecken sein. Daher bleiben derartige Angriffe oft unentdeckt, denn die Authentifizierung eines Schadakteurs sieht unter Umständen genauso aus wie die eines legitimen Benutzers, je nachdem, wie gründlich das Identitäts- und Zugriffsmanagement (IAM) ist (falls es überhaupt existiert).



## Was Sie wissen müssen:

Bei einer Account-Übernahme werden die Kreditkarten- oder Zugangsdaten nicht einfach direkt gestohlen. Vielmehr erfolgt der Angriff heimlich und schleichend, damit der Angreifer die Daten so oft wie möglich nutzen kann, bevor verdächtige Aktivitäten entdeckt werden. Häufige Ziele sind Banken, große Marktplätze und Finanzdienste wie PayPal. Ebenso sind all jene Websites anfällig, bei denen eine Anmeldung erforderlich ist.

Unternehmen müssen sich von der Netzwerksicherheit verabschieden, wenn sie Identitäten besser schützen und authentifizieren wollen. Bis vor Kurzem fehlte es oft einfach an den notwendigen Integrationsmöglichkeiten, sodass die Sicherheit der Ressourcen insgesamt kaum zentral zu managen war. Inzwischen gibt es unzählige Technologien rund um die Zugangskontrolle, speziell die Multi-Faktor-Authentifizierung (MFA).

Um eine unzulässige Authentifizierung bei Cloud-Anwendungen zu vermeiden, sollte keinem User und keinem Gerät – egal ob intern oder extern – a priori vertraut werden. Der Zugang zu sämtlichen Ressourcen sollte explizit und kontinuierlich authentifiziert und autorisiert werden.

## Wie der Angriff funktioniert:

Zu den gängigsten Methoden zählen proxy-basierte „Checker“-One-Click-Apps, Brute-Force-Angriffe mit Bot-Netzen, Phishing und Malware. Auch das sogenannte „Dumpster Diving“ ist nicht selten, bei dem in weggeworfenen Postsendungen nach personenbezogenen Daten gesucht wird. Darüber hinaus gibt es noch den direkten Kauf von Listen per „Fullz“, einem Slang-Begriff für Pakete mit vollständigen Identifizierungsdaten, die auf dem Schwarzmarkt angeboten werden. Sobald dann ein Profil des Opfers gekauft oder erstellt wurde, kann ein Identitätsdieb diese Informationen dazu nutzen, um wissensbasierte Authentifizierungssysteme gezielt auszuhebeln.

Eine Bedrohung bzw. ein Angreifer kann auch dann leicht ins Netzwerk eindringen bzw. den Perimeter durchdringen, wenn das IAM-Framework zu schwach ist bzw. ganz fehlt und wenn sich das Unternehmen immer noch auf Netzwerk-/Endpunktsicherheit verlässt. In beiden Fällen kann sich ein Angreifer mit gestohlenen Zugangsdaten angesichts der laxen Identitätszugangskontrollen problemlos anmelden, ohne entdeckt zu werden – und hat damit letztlich freie Hand.

## Woher der Angriff erfolgt:

Ein Großteil unserer finanziellen und sonstigen Transaktionen findet heute online statt. Für Cyberkriminelle ist der Erwerb von Zugangsdaten und personenbezogenen Daten (wie z. B. Sozialversicherungsnummern, Privatadressen, Telefonnummern, Kreditkartennummern oder andere Finanzdaten) ein lukratives Geschäft. Unabhängig davon, ob sie die erworbenen Daten letztendlich verkaufen oder für ihre eigenen Vorteile nutzen.

Angesichts der wachsenden Zahl von Phishing-Angriffen, der zunehmenden Menge von Benutzeridentitäten und der fortschreitenden Cloud-Migration kann diese Art von Angriffen letztlich von überallher erfolgen, auch von Drittanbietern, Mitarbeitern, Beschäftigten im Homeoffice oder von Auftragnehmern.

# Advanced Persistent Threat



Für Aufsehen sorgte der Angriff, bei dem einem [chinesischen Advanced Persistent Threat](#) (APT) u. a. die Kompromittierung von 25 Microsoft-Exchange-Konten bei verschiedenen US-Behörden gelang. [Berichten zufolge](#) ermöglichte der Angriff der APT-Gruppe den Zugriff auf „mehrerlei Azure-Active-Directory-Anwendungen, einschließlich aller Anwendungen, die eine persönliche Account-Authentifizierung unterstützen, wie SharePoint, Teams, OneDrive, Kunden-Apps, die die Funktion ‚Mit Microsoft anmelden‘ unterstützen, sowie unter Umständen mandantenfähige Anwendungen“.



## Was Sie wissen müssen:

Mit Advanced Persistent Threat (APT) wird eine hoch entwickelte, verdeckte Bedrohung eines Computersystems oder Netzwerks bezeichnet. Dabei gelingt es einem unbefugten Benutzer, unentdeckt in das Zielsystem einzudringen und Informationen abzuschöpfen – sei es nun aus finanziellen oder politischen Motiven.

Die Angriffe werden in der Regel von Kriminellen oder Nationalstaaten durchgeführt. Die Hauptziele: finanzieller Gewinn oder politische Spionage. APTs werden vor allem mit nationalstaatlichen Akteuren in Verbindung gebracht, die Regierungs- oder Industriegeheimnisse stehlen wollen. Aber auch Cyberkriminelle, die nicht im Auftrag einer bestimmten Organisation handeln, setzen auf APT-Angriffe, um sich unerlaubt Daten oder geistiges Eigentum anzueignen.

## Wie der Angriff funktioniert:

Eine APT kann sowohl durch hoch entwickelte Taktiken, einschließlich einer umfangreichen Sammlung von Informationen, als auch durch weniger ausgefeilte Methoden (z. B. Malware und Spear-Phishing) erfolgen. Dabei kommen verschiedenste Verfahren zum Einsatz, um zum Ziel des Angriffs vorzudringen, es zu kompromittieren und Zugriff darauf zu erhalten.

Der häufigste Angriffsplan besteht darin, von einem einzelnen Computer aus ein ganzes Netzwerk anzugreifen. Hierfür wird eine Authentifizierungsdatenbank ausgelesen, um all jene Accounts ausfindig zu machen, die über entsprechende Berechtigungen verfügen. Mithilfe eben jener Accounts werden anschließend die Ziele kompromittiert. Dem nicht genug installieren APT-Hacker zudem Backdoor-Programme auf kompromittierten Computern in der erfolgreich angegriffenen Umgebung. Um sich ähnlich einem Trojaner den erneuten Zugriff zu sichern, selbst wenn die Zugangsdaten bereits geändert wurden.

## Woher der Angriff erfolgt:

Die meisten APT-Gruppen stehen in Verbindung mit Regierungen souveräner Staaten oder handeln in deren Auftrag. Eine APT kann aber auch von einem professionellen Hacker ausgeführt werden, der für einen der oben erwähnten Akteure arbeitet. Diese staatlich gesponserten Hackerorganisationen verfügen in der Regel über die dafür benötigten Ressourcen und Fähigkeiten, um ihr Ziel genau zu analysieren und den besten Angriffspunkt zu identifizieren.

# Angriff auf die Lieferkette



Die [SolarWinds-Angriffe](#), die von manchen Experten als die schlimmste Serie von Cybersicherheitsangriffen der Geschichte bezeichnet wurden, sind ein Paradebeispiel für den Schaden, den Angriffe auf die Lieferkette (Supply Chain-Angriffe) anrichten können. Im Jahr 2020 wurde die SolarWinds-Software von raffinierten Angreifern, die vermutlich mit dem russischen Geheimdienst in Verbindung standen, kompromittiert. Dabei betteten sie Malware ein, die über ein Produkt-Update verteilt wurde, sodass die Angreifer über eine Backdoor Zugang zu den Netzwerken aller Kunden der Orion-Plattform von SolarWinds erhielten. Bis zu 18.000 Kunden installierten Updates, die sie für Hacker anfällig machten, darunter Fortune 500-Unternehmen und mehrere Behörden der US-Regierung. Tim Brown, Vice President für Sicherheit bei SolarWinds, [sagte](#): „Das war ein echter Albtraum.“



### Was Sie wissen müssen:

Ein Angriff auf die Lieferkette ist ein mächtiger Cyberangriff, der selbst die ausgefeiltesten Sicherheitsvorkehrungen durch legitime Drittanbieter durchbrechen kann. Da Anbieter Zugriff auf sensible Daten benötigen, um sich in die internen Systeme ihrer Kunden zu integrieren, sind bei einem Cyberangriff oft auch die Daten ihrer Kunden betroffen. Und da Anbieter vertrauliche Daten für zahlreiche Kunden speichern, verschafft ein einziger Angriff auf die Lieferkette Hackern Zugang zu den sensiblen Daten vieler Unternehmen, quer durch viele Branchen. Die Schwere von Angriffen auf die Lieferkette kann nicht hoch genug eingeschätzt werden. Und die jüngste Flut dieser Angriffe deutet darauf hin, dass diese Methode zurzeit die Angriffsart der Wahl für staatliche Akteure ist.

### Wie der Angriff funktioniert:

Ein Angriff auf die Lieferkette nutzt legitime, vertrauenswürdige Prozesse, um vollständigen Zugriff auf die Daten von Unternehmen zu erlangen, indem er auf den Software-Quellcode, Updates oder Build-Prozesse des Anbieters abzielt. Sie sind schwer zu erkennen, da sie mit einem gewissen Abstand zur Angriffsfläche stattfinden. Kompromittierte Anbieter übertragen dann unwissentlich Malware in ihr Kundennetzwerk. Die Opfer können durch Software-Updates von Drittanbietern, Anwendungsinstaller und durch Malware auf angeschlossenen Geräten verletzt werden. Ein einziges Software-Update kann Tausende von Unternehmen infizieren, und das mit minimalem Aufwand für den Hacker, der nun „legitimen“ Zugang hat, um sich seitlich durch Tausende von Unternehmen zu bewegen.

### Woher der Angriff erfolgt:

Bei Supply Chain-Angriffen handelt es sich um groß angelegte, ausgeklügelte Angriffe, die von raffinierten Bedrohungsakteuren verübt werden, die oftmals von Nationalstaaten unterstützt werden und ideologisch motiviert sind, obwohl auch der finanzielle Gewinn ein wichtiges Motiv ist.

# Application Access Token



Ein aktiver, unbekannter Bedrohungsakteur setzte verschiedene Strategien ein, um an verwertbare Informationen von wichtigen Zielen zu gelangen. Eine Methode war der Missbrauch von OAuth-Tokens (Open Authorization) zum [Angriff auf Repositories prominenter Unternehmen und Organisationen](#), darunter die Produktionsinfrastruktur von Github npm sowie Apps, die in Heroku- und Travis-CI-Cloud-Produkte integriert sind.



### Was Sie wissen müssen:

Mit einem [OAuth-Zugriffstoken](#) kann ein Hacker die vom Benutzer gewährte REST-API verwenden. In erster Linie, um Funktionen wie die E-Mail-Suche und die Auflistung von Kontakten durchzuführen. Bei einem Cloud-basierten E-Mail-Dienst erhält eine schädliche Anwendung nach Gewährung eines OAuth-Token potenziell langfristigen Zugriff auf Funktionen des Benutzerkontos. Vor allem wenn ein „Refresh“-Token vergeben wurde, über den ein Zugriff im Hintergrund erfolgen kann.

### Wie der Angriff funktioniert:

Angreifer verwenden Application Access Token, um den normalen Authentifizierungsprozess zu umgehen und Zugriff auf eingeschränkt verfügbare Konten, Informationen oder Dienste auf entfernten Systemen zu erhalten. Diese Token werden in der Regel von Benutzern gestohlen und anstelle von Zugangsdaten verwendet.

### Woher der Angriff erfolgt:

Kompromittierte Access Token können einen ersten Schritt hin zur Kompromittierung anderer Dienste darstellen. Wenn ein Token z. B. Zugriff auf die primäre E-Mail-Adresse eines Opfers gewährt, kann der Angreifer den Zugriff auch auf alle anderen Dienste ausweiten, die das Ziel abonniert hat. Hierfür muss der Angreifer nur die Routineprozesse für vergessene Passwörter anstoßen.

Der direkte API-Zugang über ein Token hebt die Wirksamkeit eines zweiten Authentifizierungsfaktors auf und kann gegenüber Gegenmaßnahmen wie das Ändern von Passwörtern immun sein.

# AWS- Angriffe

Die Zahl der kreativen Angriffe auf virtuelle Umgebungen ist mit dem Aufkommen des Cloud-Computing regelrecht explodiert. Als einer der größten Anbieter von Cloud-Services war Amazon Web Services (AWS) mit Sicherheit ein beliebtes Ziel dieser Bedrohungen.

Es existieren gleich mehrere Schwachstellen, welche die Sicherheit von Cloud-Anbietern gefährden. So hat z. B. ein Unternehmen für digitales Marketing seinen Amazon S3-Bucket nicht **mit einem Passwort geschützt**, nachdem es den Betrieb eingestellt hatte. Ein folgenschwerer Lapsus, bei dem die Daten von 306.000 Personen preisgegeben wurden. Allein durch dieses Datenleck wurden 50.000 Dateien mit einer Größe von insgesamt 32 GB offengelegt – inklusive vollständigen Namen, Standorten, E-Mail-Adressen, Telefonnummern und verschlüsselten Passwörtern von Kunden wie Patrón Tequila.





### Was Sie wissen müssen:

Das Modell der „geteilten Verantwortung“ von Amazon besagt, dass AWS für die Umgebung außerhalb der virtuellen Maschine verantwortlich ist. Demgegenüber ist innerhalb des S3-Containers der Kunde selbst dafür verantwortlich, für Sicherheit zu sorgen.

Dadurch sind Bedrohungen zu einem immer größeren Problem geworden. Weil sich diese gezielt Schwachstellen durch Konfigurations- und Bereitstellungsfehler zunutze machen.

Begünstigt durch die Tatsache, dass Cloud-Technologien bei vielen Unternehmen schnell eingeführt wurden und AWS-Kunden selbst für die Sicherung ihrer Umgebung verantwortlich sind. Problem dabei ist nur, dass es in Zukunft immer mehr Bedrohungen geben wird, welche die AWS-Kunden im Blick behalten müssen.

### Wie der Angriff funktioniert:

Ein Angriff auf eine AWS-Instanz kann auf verschiedenste Art und Weise erfolgen. Es ist wichtig, auf Aktivitäten zu achten, bei denen es sich um verdächtiges Verhalten innerhalb einer AWS-Umgebung handeln könnte. Aktivitäten, auf die geachtet werden sollte, sind S3-Zugriffe von unbekannten Standorten und durch unbekannte Benutzer.

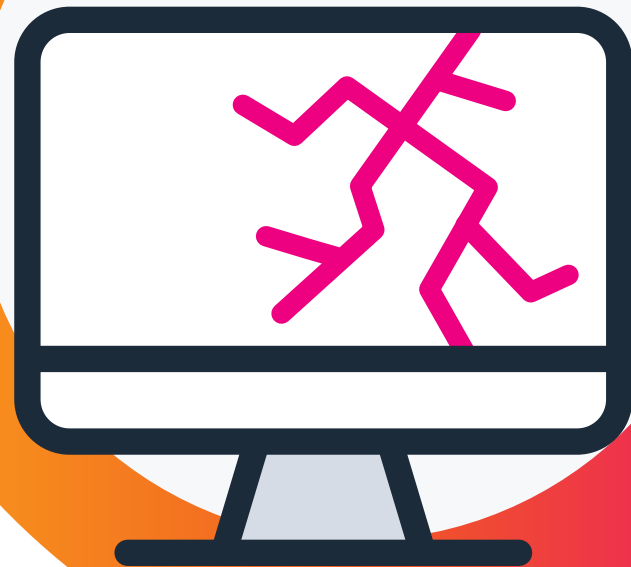
Unbedingt überwacht und kontrolliert werden sollte auch, wer alles Zugriff auf die AWS-Infrastruktur eines Unternehmens hat. Die Erkennung verdächtiger Anmeldungen bei der AWS-Infrastruktur bietet ideale Ausgangspunkte für weitere Untersuchungen. Nur so lassen sich Aktivitäten wie etwa die missbräuchliche Nutzung aufgrund kompromittierter Anmeldeinformationen verhindern, die direkt zu monetären Kosten führen können. Weil alle vom Angreifer erstellten EC2-Instanzen den Benutzern in Rechnung gestellt werden.

### Woher der Angriff erfolgt:

Aufgrund der Vielfalt der auf AWS gehosteten Dienste und der tagtäglich hinzukommenden, neuen Arten von Cloud-Bedrohungen, können diese Angriffe praktisch von überall aus erfolgen und von jedem vorgenommen werden.

# Brute-Force-Angriff

Brute-Force-Angriffe können bei ganz unterschiedlichen Services auftreten – ein jüngeres Beispiel betrifft das Remote Desktop Protocol (RDP) von Windows. Seit etwa Anfang 2020 und bis heute verzeichnet Microsoft [einen deutlichen Anstieg der Brute-Force-Angriffe auf RDP](#). Der Grund dafür liegt in der großen Anzahl ungeschützter Endpunkte. Schadakteure können dort schwache oder häufig verwendete Passwörter durchprobieren und sich auf diese Weise unbefugten Zugang zu einer Vielzahl von Systemen verschaffen.





### Was Sie wissen müssen:

Ein Brute-Force-Angriff zielt in erster Linie darauf ab, per Trial & Error-Ansatz in den Besitz personenbezogener Daten zu gelangen – insbesondere Benutzernamen und Passwörter. Eine der vielleicht unkompliziertesten Möglichkeiten, um sich Zugang zu einer Anwendung, einem Server oder einem passwortgeschützten Konto zu verschaffen. Weil der Angreifer lediglich verschiedene Kombinationen von Benutzernamen und Passwörtern ausprobieren muss. Bis er schließlich Erfolg hat. Sofern der Angriff überhaupt erfolgreich ist, da für ein sechstelliges Passwort nahezu Milliarden möglicher Kombinationen existieren.

### Wie der Angriff funktioniert:

Die einfachste Form des Brute-Force-Angriffs ist ein sogenannter Wörterbuchangriff. Dabei arbeitet sich der Angreifer systematisch durch ein Wörterbuch oder eine Wortliste und probiert jeden einzelnen Eintrag aus. Bis er schließlich Erfolg hat.

Mitunter ergänzen Angreifer dabei sogar Wörter mit Symbolen und Ziffern oder verwenden spezielle Wörterbücher mit geleakten und/oder häufig verwendeten Passwörtern. Und sollte ihnen doch einmal Zeit und Geduld ausgehen, erledigen automatisierte Tools die Arbeit für sie. Natürlich viel schneller und mit viel weniger Aufwand.

### Woher der Angriff erfolgt:

Dank der unkomplizierten und einfachen Natur von Brute-Force-Angriffen können sich Hacker und Cyberkriminelle auch mit wenig oder gar keiner technischen Erfahrung einen Zugang zu einem Account verschaffen.

Die Menschen hinter diesen Kampagnen haben entweder genug Zeit oder sind in Besitz der erforderlichen Rechenleistung, um ihre betrügerischen Ziele zu erreichen.

# Business Email Compromise



Business Email Compromise (BEC) bzw. CEO Fraud funktioniert ähnlich wie Rechnungsbetrug und hat sich im Laufe der Jahre kräftig weiterentwickelt, insbesondere mit der Zunahme von Videotelefonaten seit der Covid-19-Pandemie. Der Angriff wird häufig von Schadakteuren durchgeführt, die sich mit gefälschten Meeting-Einladungen als legitime Geschäftskontakte ausgeben. In einer [Bekanntmachung des FBI Internet Crime Complaint Centers](#) heißt es, das IC3 habe „eine zunehmende Menge an BEC-Beschwerden erhalten, bei denen virtuelle Meeting-Plattformen genutzt wurden, um die Opfer anzuweisen, unberechtigte Geldüberweisungen auf betrügerische Konten zu tätigen“.



## Was Sie wissen müssen:

Bei BEC versuchen die Schadakteure, ihre Opfer dazu zu bringen, eine falsche (aber überzeugende) Rechnung zu begleichen, die an das Unternehmen adressiert ist. In Wirklichkeit gehen die Gelder an Betrüger, die sich als Lieferanten, Kollegen oder Geschäftspartner ausgeben. Diese Angriffe gehen oft über gewöhnlichen Betrug hinaus und zielen z. B. auf Banken in Schwellenländern ab, die nur eine begrenzte Cybersicherheitsinfrastruktur und unausgereifte operative Kontrollen haben. Oder sie locken prominente Ziele mit ausgeklügelten und täuschend echten Phishing-Mails. Diese Cybercrime-Syndikate sind nur auf eines aus: Geld. Und zwar möglichst viel.

## Wie der Angriff funktioniert:

In einem Angriffsszenario verwenden die Cyberkriminellen ausgeklügelte Malware, um die Sicherheitssysteme vor Ort zu umgehen. Von dort aus verschaffen sie sich dann Zugang zu einem Messaging-Netzwerk und versenden betrügerische Nachrichten, um Überweisungen von Konten bei größeren Banken zu veranlassen. In einem anderen Szenario werden Stakeholder durch gezieltes Spear-Phishing dazu gebracht, größere Geldbeträge an die Betrüger zu überweisen. Mit gefälschten Rechnungen versuchen die Schadakteure, Geld zu stehlen – in der Hoffnung, dass die Opfer nicht allzu genau auf die Prozesse ihrer Kreditorenbuchhaltung achten.

Die Hacker suchen sich ihre Opfer nach Unternehmensgröße, nach Standort und nach Lieferanten aus und produzieren dann gefälschte Rechnungen, die legitim erscheinen. In der Hoffnung, dass die Kreditorenbuchhaltung des Opfers überlastet ist, versenden sie falsche Rechnungen mit hohen Forderungen à la „90 Tage überfällig, jetzt begleichen!“

## Woher der Angriff erfolgt:

Zwar gibt es eine Vielzahl von Einzeltätern, die BEC betreiben. Doch viele gehören zu größeren Betrügerorganisationen, die über die nötige Organisation und entsprechende Ressourcen verfügen, um das jeweilige Bankinstitut der Betrugsopfer ausfindig zu machen und überaus gut gefälschte Rechnungen zu erstellen. Derartige Banden gibt es überall auf der Welt.

Durchorganisierte internationale oder nationalstaatliche Cybercrime-Gruppen wie APT38 bzw. die Lazarus-Gruppe sind die Klassiker des Überweisungsbetrugs. Diese Gruppen verfügen über die notwendige Infrastruktur und die Ressourcen, die nötig sind, um solche komplexen und vielschichtigen Angriffe durchzuführen. Es ist zwar nicht klar, wer genau hinter diesen Gruppen steckt, aber manches deutet darauf hin, dass sie Verbindungen zu Nordkorea haben könnten. Doch auch Hackergruppen aus China und aus Nigeria wurden bereits als Urheber ausgemacht. Ein Warnhinweis: Bei groß angelegten Angriffen auf Einrichtungen mit robusteren Sicherheitssystemen sind vermutlich Insider im Spiel, die den Tätern Zugang zu den Systemen verschaffen.

# Cloud-Kryptomining



Als Antrieb für Cloud-Kryptomining braucht es kein Benzin. Das musste auch Github bereits feststellen. Das Cloud-Repository für Softwarecode wurde [Opfer eines Cloud-Kryptomining-Angriffs](#), als Bedrohungsakteure eine umfangreiche Freejacking-Kampagne durchführten – sie umfasste 30 GitHub-Konten, 2.000 Heroku-Konten und 900 Buddy-Konten sowie 130 Docker-Hub-Images – und eine große Anzahl kostenloser Accounts mit minimalem menschlichen Aufwand missbrauchten.



### Was Sie wissen müssen:

Aus guten Gründen ist Kryptomining ein schwieriges und ressourcenintensives Business. Denn durch die Komplexität soll sichergestellt werden, dass die Anzahl der täglich „geminten“ Blocks möglichst konstant bleibt.

Daher war es nur eine Frage der Zeit, dass sich ebenso ehrgeizige wie skrupellose Miner irgendwann die Rechenleistung großer Unternehmen anzueignen versuchen – eine unter Cyberkriminellen gängige Praxis, die als Kryptojacking bezeichnet wird.

### Wie der Angriff funktioniert:

Kryptojacking hat mit der explosionsartigen Zunahme im Herbst 2017 auch die Aufmerksamkeit der Medien auf sich gezogen. Seitdem haben sich die Angriffe von Browser-Exploits und Mobiltelefonen hin zu Cloud-Diensten für Unternehmen wie Amazon Web Services (AWS), Google Cloud Platform (GCP) und Microsoft Azure verlagert.

Es lässt sich nicht genau bestimmen, wie weit verbreitet diese Praxis ist. Gerade weil die Angreifer ihre Fähigkeiten ständig weiterentwickeln, um unentdeckt zu bleiben. Indem sie z. B. nicht gelistete Endpunkte einsetzen, ihre CPU-Nutzung drosseln und die IP-Adresse des Mining-Pools hinter einem kostenlosen Content Delivery Network (CDN) verstecken.

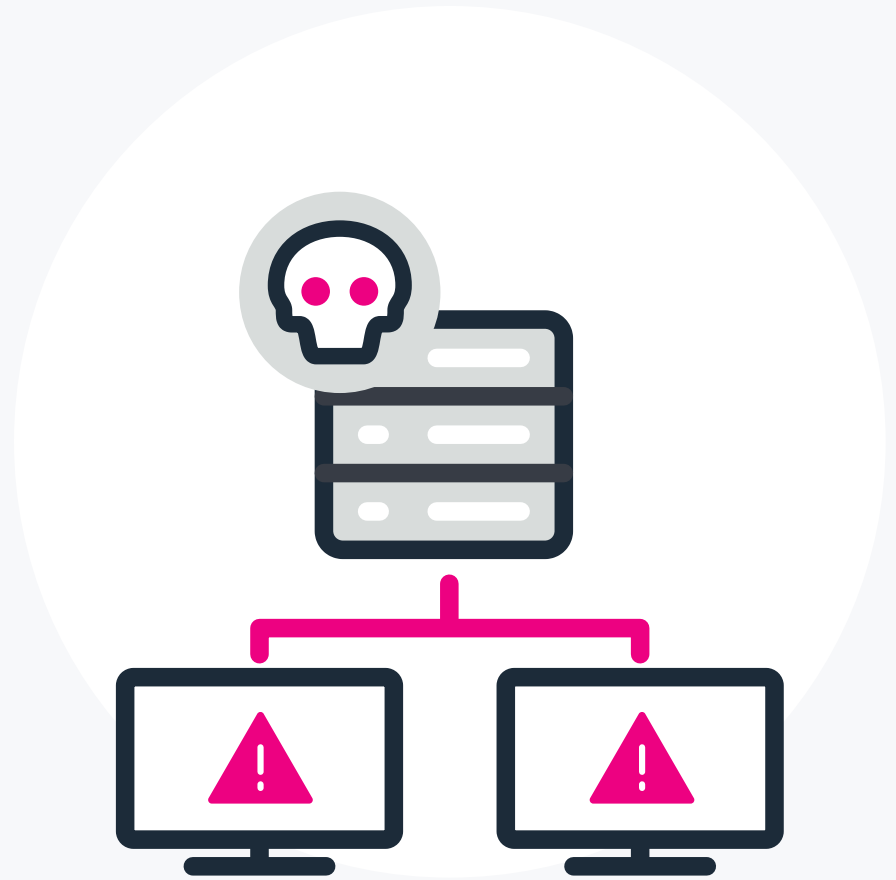
Wenn sich kriminelle Miner eine Cloud-Instanz aneignen und dabei oft Hunderte neue Instanzen aufsetzen, können die Kosten für den Account-Inhaber in astronomische Höhen steigen. Grund genug, die Systeme auf verdächtige Aktivitäten zu überwachen, die auf ein infiltriertes Netzwerk hindeuten.

### Woher der Angriff erfolgt:

Da es sich bei Kryptowährungen um eine globale Ware handelt, können diese Angriffe von jedem Ort der Welt ausgehen. Anstatt sich jedoch darauf zu konzentrieren, woher die Angriffe kommen, ist es wichtiger, Cloud-Computing-Instanzen auf Aktivitäten im Zusammenhang mit Kryptojacking und Kryptomining zu überwachen.

Darunter fallen z. B. neue Cloud-Instanzen, die aus bisher unbekannten Regionen stammen, Benutzer, die eine ungewöhnlich hohe Anzahl von Instanzen starten, oder Computing-Instanzen, die von bisher unbekannten Benutzern gestartet werden.

# Command-and-Control-Angriffe



Cobalt Strike ist ein kommerzielles Penetrationstest-Tool, das Cybersicherheitsexperten einsetzen, um das Verhalten fortgeschrittener Bedrohungen zu simulieren und die Sicherheitslage eines Unternehmens zu bewerten. Es bietet eine Reihe von Funktionen, darunter Aktivitäten der Aufklärung, der Ausnutzung und der Post-Exploitation. Das beachtlichste Feature ist allerdings die Payload namens Beacon.

In den letzten Jahren konnte man mit Beacon **kompromittierte Hosts unter Command and Control (C2) bringen**, sodass verdeckte Kommunikation, Seitwärtsbewegungen und diverse speicherinterne In-memory-Angriffstechniken möglich wurden. Cobalt Strike ist zwar ein legitimes Tool, das für Red-Team-Übungen und die Emulation von Bedrohungen gedacht ist, doch aufgrund seiner leistungsstarken Funktionen und Ausweichfähigkeiten haben Schadakteure sich geknackte Versionen dieser Software beschafft und für Cyberangriffe verwendet.



## Was Sie wissen müssen:

Bei einem Command & Control-Angriff übernimmt ein Hacker die Kontrolle über einen Computer, um Befehle oder Malware an andere Systeme im Netzwerk zu senden. In einigen Fällen führt der Angreifer Aufklärungsaktivitäten durch, indem er sich lateral im Netzwerk bewegt und sensible Daten sammelt. Derartige Angriffe werden immer beliebter, und [die Menge der C2-Server hat allein im Jahr 2022 um unglaubliche 30 % zugenommen](#).

Bei anderen Angriffen können Hacker diese Infrastruktur wiederum nutzen, um die eigentlichen Angriffe zu starten. Eine der wichtigsten Funktionen dieser Infrastruktur ist die Einrichtung von Servern, die mit Implantaten in kompromittierten Endpunkten kommunizieren. Diese Angriffe werden oft auch als C2- oder C&C-Angriffe bezeichnet.

## Wie der Angriff funktioniert:

Zumeist verschaffen sich Angreifer über Phishing-E-Mails und die Installation von Malware einen entsprechenden Zugang zum System.

Dadurch wird ein Command & Control-Kanal eingerichtet, über den Daten zwischen dem kompromittierten Endpunkt und dem Angreifer ausgetauscht werden.

Diese Kanäle leiten dann Befehle an den kompromittierten Endpunkt weiter und die Ausgabe dieser Befehle anschließend wieder zurück an den Angreifer.

## Woher der Angriff erfolgt:

In der Vergangenheit erfolgten prominente Command & Control-Angriffe aus Russland, dem Iran und sogar den USA. Aber natürlich können die Angreifer auch aus jedem Land der Welt stammen. Allerdings wollen sie nicht, dass Sie das wissen.

Da die Kommunikation von entscheidender Bedeutung ist, verwenden Hacker spezielle Techniken, um die wahre Natur ihrer Korrespondenz zu verschleiern. In der Regel versuchen sie, ihre Aktivitäten so lange wie möglich zu loggen, ohne dabei entdeckt zu werden. Indem sie eine Vielzahl von Techniken einsetzen, um über Kanäle zu kommunizieren und dabei möglichst unauffällig zu bleiben.

# Credential Dumping



Im Herbst 2022 wurde erstmals eine [neue Ransomware namens Trigona](#) bemerkt, die es auf Windows abgesehen hat und dabei auf ganz eigene Weise vorgeht, insbesondere mit dem Mimikatz-Tool für Anmeldeinformationen. Mit dessen Hilfe werden sensible Daten aus Windows ausgeschleust; betroffen sind u. a. der Windows-Arbeitsspeicher, der Local Security Authority Subsystem Service (LSASS) und die Windows-Registry. Mimikatz extrahiert die Anmeldedaten und packt sie in eine Datei – von User-Namen und Passwörtern über Hash-Werte bis zu Kerberos-Tickets.



### Was Sie wissen müssen:

Credential Dumping bezeichnet in erster Linie einen Angriff, der auf dem Sammeln von Zugangsdaten von einem Zielsystem beruht. Auch wenn die Zugangsdaten nicht im Klartext vorliegen – sie sind oft gehasht oder verschlüsselt –, kann ein Angreifer die Daten dennoch extrahieren und im Anschluss offline auf seinen eigenen Systemen knacken. Genau deshalb wird diese Art von Angriff auch als „Dumping“ bezeichnet.

Oft versuchen Hacker, Passwörter von Systemen zu stehlen, in die sie bereits eingedrungen sind. Das Problem verschärft sich allerdings zusehends, wenn Nutzer ein und dasselbe Passwort für gleich mehrere Konten in verschiedenen Systemen verwenden.

### Wie der Angriff funktioniert:

Zu den auf diese Weise erlangten Zugriffsdaten gehören in der Regel auch solche von privilegierten Nutzern, die möglicherweise Zugang zu sensiblen Informationen und Systemoperationen haben.

Hacker zielen oft auf eine Vielzahl von Quellen ab, um Zugangsdaten abzugreifen. Hierzu zählen z. B. Konten des Security Accounts Manager (SAM) oder der Local Security Authority (LSA), NTDS von Domain Controllern oder Group-Policy-Preference-Dateien (GPP).

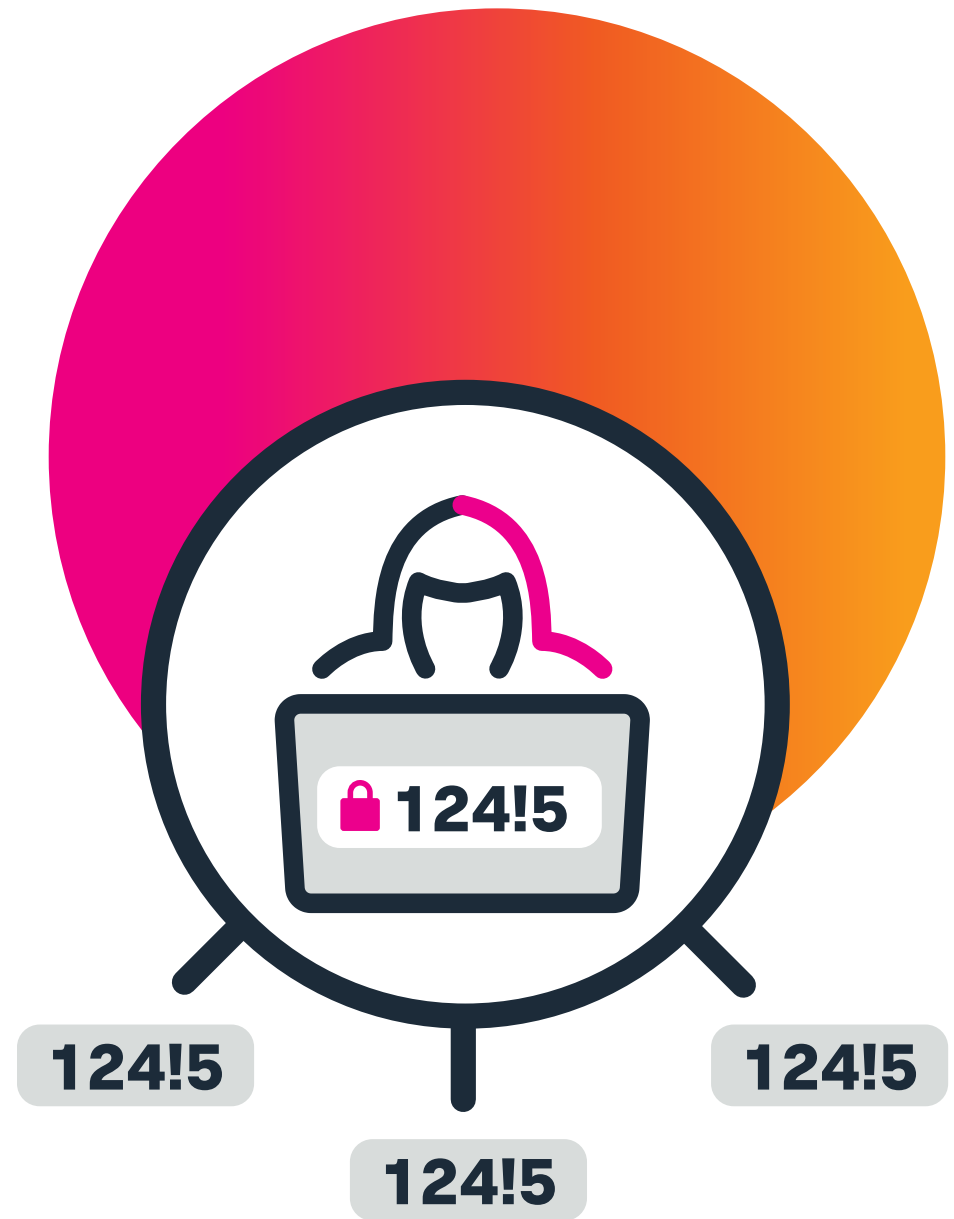
Sobald die Angreifer in den Besitz gültiger Zugangsdaten sind, können sie sich damit problemlos im Zielnetzwerk bewegen, neue Systeme ausfindig machen und für sie interessante Objekte identifizieren.

### Woher der Angriff erfolgt:

Credential Dumping kann von jedem Ort der Welt aus stattfinden. Und gerade weil wir alle unsere Passwörter gerne wiederverwenden, lassen sich Informationen dieser Art auch für zukünftige Angriffe problemlos weiterverkaufen.

# Credential-Reuse-Angriff

Zu den bemerkenswerteren Credential-Reuse-Angriffen zählt die [Attacke auf PayPal](#), bei der 2022 über einige Monate hinweg über 30.000 Konten kompromittiert wurden, zum Leidwesen des Online-Bezahldienstleisters. Die Bedrohungsakteure erlangten Zugang zu persönlichen Daten, darunter – laut einer E-Mail, die PayPal nach dem Angriff verschickte – „Name, Adresse, Sozialversicherungsnummer, Steueridentifikationsnummer (ITIN) und/oder Geburtsdatum“.





## Was Sie wissen müssen:

Credential Reuse (also die Wiederverwendung von Zugangsdaten) ist in allen Unternehmen und Benutzergruppen ein allgegenwärtiges Problem. Heutzutage haben die meisten Benutzer Dutzende (wenn nicht Hunderte) von Accounts und müssen sich unzählige Passwörter merken, die außerdem alle vielen strengen Anforderungen genügen müssen. Das führt dazu, dass sie immer wieder das gleiche Passwort verwenden, in der Hoffnung, dass sie ihre Zugangsdaten für verschiedene Accounts leichter verwalten und sich einprägen können. Es ist wohl nicht verwunderlich, dass dies zu großen Sicherheitsproblemen führen kann, wenn diese Zugangsdaten kompromittiert werden.

## Wie der Angriff funktioniert:

Theoretisch ist der Angriff an sich einfach, unkompliziert und überraschend unauffällig (wenn keine Zwei-Faktor-Authentifizierung aktiviert ist). Sobald die Zugangsdaten eines Benutzers gestohlen wurden, kann der Täter denselben Benutzernamen und dasselbe Passwort auf anderen Verbraucher- oder Bank-Websites ausprobieren, bis er schließlich Erfolg hat – daher der Begriff „Reuse“ (Wiederverwendung) in der Bezeichnung „Credential-Reuse-Attack“.

Sich überhaupt Zugang zu verschaffen, ist jedoch ein wenig komplizierter. Um an privilegierte Informationen zu gelangen, beginnen Angreifer in der Regel mit einem Phishing-Versuch, bei dem sie mithilfe von täuschend echt aussehenden E-Mails und Websites Benutzer zur Herausgabe ihrer Zugangsdaten verleiten.

## Woher der Angriff erfolgt:

Diese Art von Angriff kann gezielt erfolgen, wenn die Person das Opfer kennt und aus persönlichen, beruflichen oder finanziellen Gründen Zugang zu dessen Accounts erlangen möchte. Er kann jedoch auch von einem völlig Fremden ausgehen, der die personenbezogenen Daten des Nutzers über einen Kanal für Cyberkriminalität gekauft hat.

# Cross-Site Scripting

Kürzlich wurde [in der Collaboration-Suite Zimbra eine Cross-Site-Scripting-Schwachstelle entdeckt](#), durch die Bedrohungsakteure mit einem gezielten Angriff sensible Benutzerdaten stehlen konnten.

Cross-Site Scripting (XSS) ist eine Art von Injection-Angriff, bei dem schädliche Skripte in ansonsten harmlose und vertrauenswürdige Websites eingeschleust werden. Das Konzept ähnelt einer SQL Injection – bei der bösartiger Code in ein Formular eingegeben wird, um Zugriff auf die Datenbank der Website zu erhalten – mit dem Unterschied, dass im Falle von XSS der schädliche Code so konzipiert ist, dass er im Browser eines anderen Besuchers der Website ausgeführt wird. Dies ermöglicht dem Angreifer, User Cookies zu stehlen, Session-IDs auszulesen, den Inhalt einer Website zu ändern oder Benutzer auf eine schädliche Website umzuleiten.





### Was Sie wissen müssen:

XSS-Angriffe treten auf, wenn ein Angreifer eine Webanwendung nutzt, um schädlichen Code – im Allgemeinen in Form eines browserseitigen Skripts – an einen anderen Endbenutzer zu senden. Schwachstellen, die diese Angriffe ermöglichen, sind weit verbreitet und treten überall dort auf, wo eine Webanwendung Eingaben eines Benutzers generiert, ohne sie zu validieren oder zu verschlüsseln.

Der Browser des Endbenutzers hat keine Möglichkeit zu erkennen, dass das Skript nicht vertrauenswürdig ist, und führt es automatisch aus. Da er glaubt, das Skript stamme aus einer vertrauenswürdigen Quelle, kann es auf Cookies, Session Token oder andere vertrauliche Informationen des Browsers zugreifen. Diese Skripte können sogar den Inhalt der HTML-Seite umschreiben.

### Wie der Angriff funktioniert:

Es gibt zwei Arten von XSS-Angriffen: gespeicherte und reflektierte. Gespeicherte XSS-Angriffe liegen vor, wenn ein injiziertes Skript an einem festen Ort auf dem Server gespeichert ist, z. B. in einem Forenbeitrag oder Kommentar. Jeder Benutzer, der auf der infizierten Seite landet, ist von dem XSS-Angriff betroffen. Bei einem reflektierten XSS-Angriff wird das eingeschleuste Skript dem Benutzer als Antwort auf eine Anfrage, z. B. als Suchergebnisseite, angezeigt.

### Woher der Angriff erfolgt:

XSS-Angriffe kommen zwar nicht mehr so häufig vor wie in der Vergangenheit, was in erster Linie auf Verbesserungen bei Browsern und Sicherheitstechnologien zurückzuführen ist, sie sind jedoch immer noch so weit verbreitet, dass sie vom Open Web Application Security Project unter den zehn größten Bedrohungen geführt werden. Die Datenbank Common Vulnerabilities and Exposures listet fast 14.000 Schwachstellen im Zusammenhang mit XSS-Angriffen auf.

# DNS Amplification



Im Februar 2022 starteten Übeltäter massive DDoS-Angriffe (Distributed Denial-of-Service) über Mitel, einen globalen Anbieter von Kommunikationssystemen für Unternehmen. [Der Angriff](#) richtete sich u. a. gegen Finanzinstitute, Breitband-ISPs sowie Logistik- und Gaming-Unternehmen. Da Angreifer das DDoS-Bombardement bis zu 14 Stunden mit einem rekordverdächtigen Verstärkungsfaktor von fast 4,3 Milliarden zu eins aufrechterhalten können, sind sie in der Lage, die Sprachkommunikation und andere Dienste ganzer Unternehmen mit einem einzigen böartigen Netzwerkpaket lahmzulegen.



### Was Sie wissen müssen:

DNS Amplification, eine Art von DDoS-Angriffen, gibt es schon recht lange, doch die Nutzung wird ständig weiterentwickelt. Diese Art von Angriff ähnelt dem DNS Hijacking dahingehend, dass sie sich das Internet-Verzeichnis zunutze macht, indem sie es falsch konfiguriert. Die Art und Weise, wie der Angriff erfolgt, unterscheidet sich dabei jedoch.

Bei einem DNS-Amplification-Angriff wird in der Regel eine kleine Menge an Informationen an einen anfälligen Netzwerkdienst gesendet, die diesen dazu veranlasst, mit einer viel größeren Datenmenge zu antworten. Wenn der Angreifer diese umfangreiche Datenantwort zu seinem Opfer lenkt, erreicht er mit relativ geringem Aufwand, dass fremde Rechner die ganze Arbeit übernehmen und ein ausgewähltes Ziel durch Überlastung offline setzen.

### Wie der Angriff funktioniert:

Bei einem DNS-Amplification-Angriff überflutet der Angreifer eine Website mit so vielen gefälschten DNS-Abfragen, dass die Netzwerkbandbreite nicht ausreicht und die Website schließlich ausfällt. Während ein DNS-Hacking den Traffic auf eine andere Website umleiten kann, verhindert ein DNS-Amplification-Angriff, dass die Website überhaupt geladen wird.

Der Unterschied zwischen den beiden Angriffen wird durch das Wort „Amplification“ (Verstärkung) verdeutlicht. Bei diesem Angriff stellen die Hacker die DNS-Abfragen so, dass eine intensivere Antwort erforderlich ist. So könnte ein Hacker z. B. mehr als nur den Domain-Namen anfordern. Der Angreifer könnte die gesamte Domain anfordern, auch bekannt als „ANY-Eintrag“, der die Domain zusammen mit der Subdomain, den Mail-Servern, den Backup-Servern, den Aliasen und mehr anfordert.

Stellen Sie sich nun einmal vor, dass mehrere dieser ANY-Anfragen gleichzeitig eingehen. Der verstärkte Traffic reicht aus, um die Website lahmzulegen.

### Woher der Angriff erfolgt:

Ähnlich wie bei einem DNS-Hijacking-Angriff bedeutet die relativ primitive Natur des Angriffs, dass er von jedem Ort der Welt ausgehen kann, sei es von Hackern im Auftrag einer Regierung oder von Einzelpersonen.

# DNS Hijacking

Ende 2022 wurde das Blockchain-Interoperabilitätsprotokoll Celer Network, das als Cross-Chain-Bridge fungiert, [Opfer eines DNS-Hijacking-Angriffs](#). Die gekaperte cBridge-Oberfläche leitete um zu Phishing Smart Contracts auf Avalanche, Ethereum und Polygon und bediente sich so aus den Kontoguthaben argloser User.



## DNS Hijacking



### Was Sie wissen müssen:

Das DNS wird oft als Achillesferse oder Telefonbuch des Internets bezeichnet, da es eine entscheidende Rolle bei der Weiterleitung des Internet-Traffic spielt. DNS ist das Protokoll, über das Domain-Namen mit IP-Adressen verknüpft werden. Es hat sich gezeigt, dass es für die ihm zugedachte Funktion sehr gut geeignet ist. Das DNS ist jedoch notorisch anfällig für Angriffe, was zum Teil auf seinen verteilten Charakter zurückzuführen ist. DNS stützt sich auf unstrukturierte Verbindungen zwischen Millionen von Clients und Servern über inhärent unsichere Protokolle.

Es ist zweifellos enorm wichtig, das DNS vor Angriffen zu schützen. Die Folgen einer DNS-Kompromittierung können katastrophal sein. Hacker könnten nicht nur ganze Unternehmen vom Netz nehmen, sondern auch vertrauliche Informationen, E-Mails und Anmeldedaten abfangen.

### Wie der Angriff funktioniert:

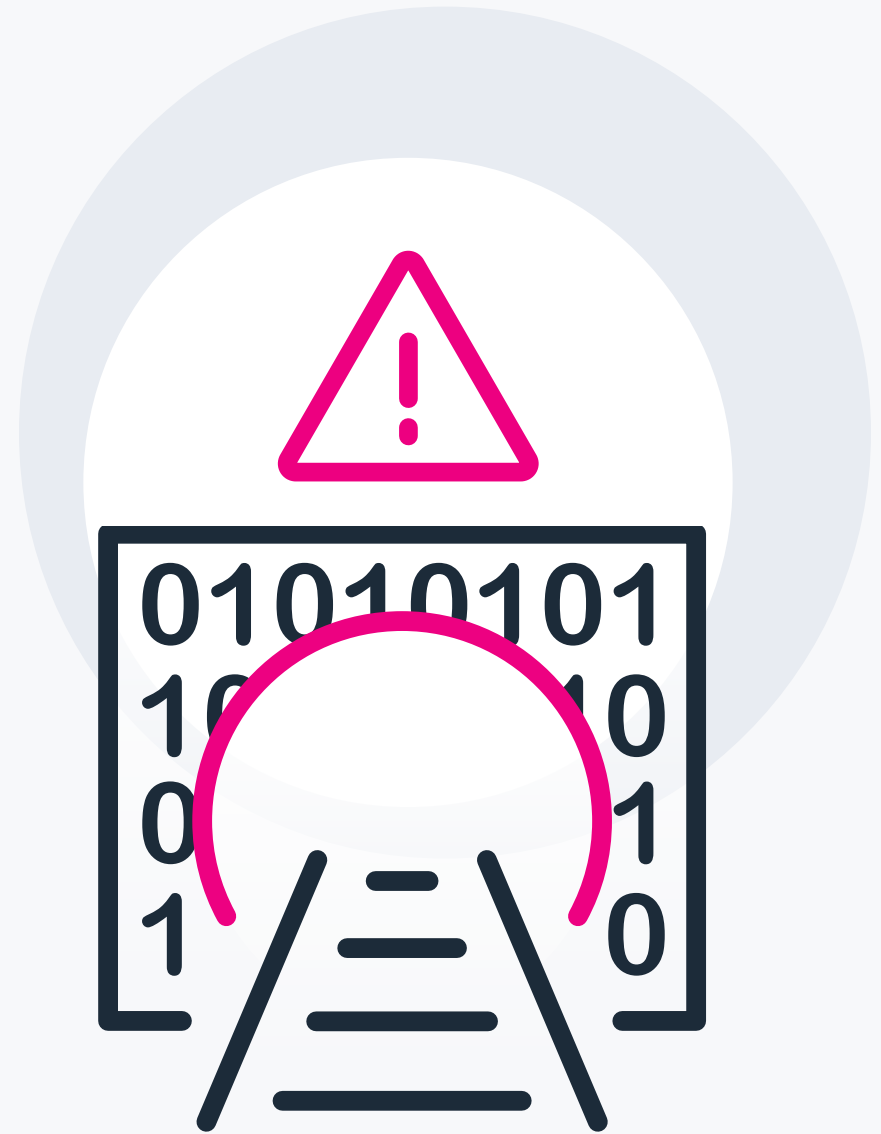
Der Angriff funktioniert, wenn Hacker die Art und Weise ausnutzen, wie DNS mit einem Internet-Browser kommuniziert. Das System verhält sich wie ein Telefonbuch und übersetzt eine Domain – wie NYTimes.com – in eine IP-Adresse. Das DNS sucht und findet dann den globalen Server, auf dem diese Website gehostet wird, und leitet den Traffic dorthin. Der Angriff erfolgt, wenn ein Hacker in der Lage ist, den DNS Lookup zu stören und dann entweder die Website offline zu schalten oder den Traffic auf eine Website umzuleiten, die der Hacker kontrolliert.

### Woher der Angriff erfolgt:

Es gibt kein einheitliches Profil eines DNS-Hijackers, was zum Großteil daran liegt, dass ein solcher Angriff genauso leicht erfolgen kann wie ein Social-Engineering-Angriff, bei dem jemand einen Domain-Anbieter kontaktiert und ihn dazu bringt, einen DNS-Eintrag zu ändern.

# DNS Tunneling

Seit ein paar Jahren hat eine Hackergruppe namens OilRig **regelmäßig Angriffe** auf verschiedene Regierungen und Unternehmen im Nahen Osten durchgeführt und dabei eine Vielzahl von Tools und Methoden eingesetzt. Ein wesentliches Element ihrer Bemühungen, den täglichen Betrieb zu stören und Daten zu exfiltrieren, ist die Aufrechterhaltung einer Verbindung zwischen ihrem Command & Control-Server und dem System. Das gelingt mithilfe von DNS Tunneling.





### Was Sie wissen müssen:

Der Dienst, der die URLs, die wir in unsere Webbrowser eingeben, in numerische IP-Adressen umwandelt, Domain Name System (DNS). Er ist sozusagen das Telefonbuch für das Internet. Der Traffic, der über das DNS läuft, wird oft nicht überwacht, da es nicht für die Datenübertragung ausgelegt ist. Dadurch ist es anfällig für verschiedene Arten von Angriffen, einschließlich DNS Tunneling, bei dem ein Angreifer schädliche Daten in eine DNS-Abfrage – eine komplexe Zeichenfolge am Anfang einer URL – packt.

Es gibt gute Gründe für DNS Tunneling: Anbieter von Antivirensoftware nutzen es z. B., um aktualisierte Malware-Profile im Hintergrund an ihre Kunden zu senden. Da die Möglichkeit einer legitimen Nutzung besteht, ist es für Unternehmen wichtig, ihren DNS-Traffic sorgfältig zu überwachen, damit nur vertrauenswürdiger Traffic durch das Netzwerk fließt.

### Wie der Angriff funktioniert:

Durch DNS Tunneling kann ein Angreifer die Sicherheitssysteme umgehen (bildlich gesprochen einen Tunnel unter ihnen hindurchgraben), indem er den Traffic auf seinen eigenen Server umleitet und eine Verbindung zum Netzwerk eines Unternehmens herstellt. Sobald diese Verbindung aktiv ist, sind Command & Control- oder Datenexfiltrationsangriffe ebenso möglich wie eine Reihe anderer Angriffe.

### Woher der Angriff erfolgt:

Es gibt zwar DNS-Tunneling-Tools zum Herunterladen, aber Angreifer, die mehr tun wollen, als die Paywall eines Hotels oder einer Fluggesellschaft für den Internetzugang zu umgehen, benötigen anspruchsvollere Kenntnisse. Da das DNS nur für die Auflösung von Webadressen konzipiert wurde, ist die Datenübertragung in diesem System außerdem sehr langsam.

# DoS-Angriff

Vor fast zwei Jahrzehnten führte [ein 16-jähriger Hacker mit dem Spitznamen Mafiaboy](#) einen der berühmtesten Denial-of-Service-Angriffe (DoS) aus, der die Websites einiger großer Unternehmen wie CNN, eBay, Amazon und Yahoo vom Netz nahm. Berichten zufolge drang Mafiaboy in Dutzende Netzwerke ein und installierte dort Malware, die die Ziele mit Traffic überfluten sollte. Da viele Websites auf einen solchen Angriff nicht vorbereitet waren, dauerte es etwa eine Woche, bis die betroffenen Organisationen herausfanden, was passiert war und wie sie wieder online gehen konnten. Mafiaboy wurde schließlich verhaftet und zu einer Jugendhaftstrafe verurteilt.

Zwanzig Jahre später sind DoS-Angriffe – bei denen es sich in vielen Fällen um DDoS-Angriffe handelt (Distributed Denial-of-Service), mit denen Hacker, Hacktivist\*innen oder Cyberspione Websites und Online-Dienste lahmlegen – weiterhin auf dem Vormarsch. Sie zählen mittlerweile zu den Angriffen, die Unternehmen am häufigsten erleben: [2022 hat die Menge der DDoS-Attacken weltweit um 150 % zugenommen](#).





## Was Sie wissen müssen:

Bei einem DoS-Angriff versuchen Cyberangreifer, einen Computer oder ein Netzwerk für die vorgesehenen Benutzer unzugänglich zu machen. DoS-Angriffe können entweder durch die Überflutung von Netzen mit Traffic oder das Senden von Informationen erfolgen, die eine Verlangsamung oder einen vollständigen Absturz des Systems bewirken. Wie bei DDoS-Angriffen konzentrieren sich DoS-Angriffe in der Regel auf wichtige Organisationen oder solche mit beliebten, öffentlich zugänglichen Websites, wie Banken, E-Commerce-Unternehmen, Medien oder staatliche Einrichtungen. DoS-Angriffe verhindern, dass Nutzer auf den gewünschten Dienst zugreifen können, und verursachen erheblichen Schaden, da den betroffenen Organisationen für die Erhöhung der Sicherheit, die Wiederherstellung des Dienstes, durch Rufschädigung, den Verlust von Umsatzerlösen und Kundenschwund hohe Kosten entstehen.

## Wie der Angriff funktioniert:

DoS-Angriffe können auf zwei Arten erfolgen: durch Flooding oder den gezielten Absturz eines Zielnetzes. Bei Flooding-Angriffen bombardieren Cyberkriminelle die Computer der Opfer mit mehr Traffic als sie bewältigen können, damit sie langsamer werden oder komplett ausfallen. Zu den verschiedenen Flooding-Angriffen gehören Buffer-Overflow-, ICMP-Flooding- und SYN-Flooding-Angriffe.

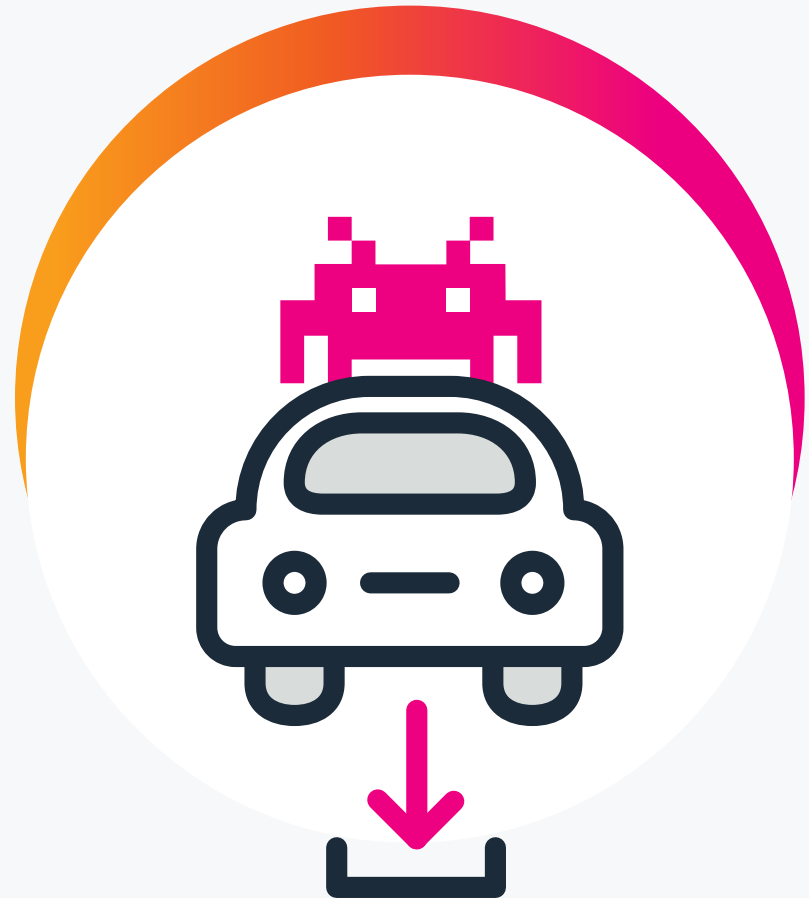
Die Schadakteure hinter den DDoS-Angriffen sind darauf aus, Schaden anzurichten, Web-Assets zu sabotieren, die Markenreputation zu schädigen und für finanzielle Verluste zu sorgen, indem sie die User am Zugriff auf eine Website oder eine Netzwerkressource hindern. DDoS-Angriffe nutzen dazu Botnetze aus Hunderten oder Tausenden von infizierten Computern auf der ganzen Welt. Damit eine DDoS-Attacke mit voller Wucht trifft, führen diese Armeen kompromittierter Computer den Angriff alle gleichzeitig aus.

## Woher der Angriff erfolgt:

DoS-Angriffe können von jedem Ort der Welt ausgehen. Angreifer können ihren Aufenthaltsort leicht verschleiern und damit die Computer ihrer Opfer übernehmen, Malware ausführen oder andere böswillige Aktionen durchführen, ohne entdeckt zu werden.

Wie der Name schon sagt, sind DDoS-Angriffe verteilt (distributed), die Traffic-Flut, die das Netzwerk des Opfers überschwemmt, rührt also aus einer Vielzahl von Quellen her. Die Schadakteure, die hinter derartigen Angriffen stehen, können tatsächlich von überallher sein. Darüber hinaus ist es aufgrund der verteilten Natur der Angriffe unmöglich, sie zu stoppen, indem man eine einzelne Quelle sichert bzw. blockiert.

# Drive-by-Download-Angriff



Im [Januar 2020](#) wurde Besuchern der legendären Magazin- und Blog-Website Boing Boing ein gefälschtes Google Play Protect-Overlay angezeigt, das sie zu einem Download aufforderte, bei dem es sich im Endeffekt um ein böses Angler-Exploit-Kit (APK) handelte, das einen Banking-Trojaner auf Android-Geräten installierte. Für Windows-Benutzer sah das Ganze wie eine (gefälschte) Adobe Flash-Installationsseite aus, die andere schädliche Programme verbreitete. Das Content Management-System von Boing Boing war gehackt worden. Selbst wenn der Besucher den Köder nicht schluckte, wurden die Drive-by-Downloads trotzdem automatisch durch ein in die Seite eingebettetes JavaScript-Skript ausgelöst. Boing Boing entdeckte den Angriff zwar relativ schnell und konnte das Skript zügig entfernen, doch angesichts der fünf Millionen Benutzer der Website – zu denen auch der ehemalige US-Präsident Barack Obama zählt – hätten die Auswirkungen katastrophal sein können.



### Was Sie wissen müssen:

Unter einem Drive-by-Download versteht man das unbeabsichtigte Herunterladen von schädlichem Code auf einen Computer oder ein mobiles Gerät, wodurch der Benutzer verschiedenen Arten von Bedrohungen ausgesetzt wird. Cyberkriminelle nutzen Drive-by-Downloads, um personenbezogene Daten zu stehlen und zu sammeln, Banking-Trojaner einzuschleusen oder Exploit-Kits bzw. andere Malware auf die Geräte der Nutzer zu laden. Zum Schutz vor Drive-by-Downloads sollten Systeme regelmäßig mit den neuesten Versionen von Anwendungen, Software, Browsern und Betriebssystemen aktualisiert oder gepatcht werden. Außerdem ist es ratsam, sich von unsicheren oder potenziell schädlichen Websites fernzuhalten.

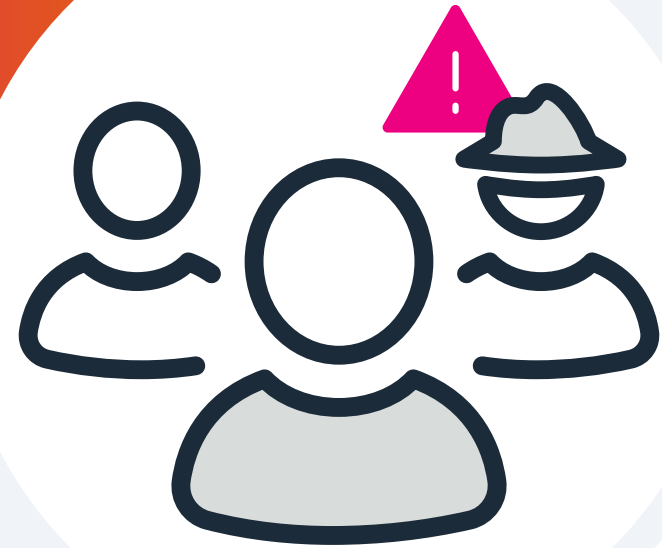
### Wie der Angriff funktioniert:

Das Besondere an Drive-by-Downloads ist, dass Benutzer nichts anklicken müssen, um den Download zu starten. Schon das Aufrufen oder Durchstöbern einer Website kann den Download aktivieren. Der schädliche Code ist so konzipiert, dass er ohne das Wissen des Benutzers schädliche Dateien auf das Gerät des Opfers herunterlädt. Bei einem Drive-by-Download werden unsichere, anfällige oder veraltete Anwendungen, Browser oder sogar ganze Betriebssysteme ausgenutzt.

### Woher der Angriff erfolgt:

Die Zunahme von vorgefertigten Drive-by-Download-Kits ermöglicht es Hackern jeglicher Erfahrungsstufe, diese Art von Angriffen durchzuführen. Diese Kits können gekauft und eingesetzt werden, ohne dass der Hacker seinen eigenen Code schreiben oder eine eigene Infrastruktur für die Datenexfiltration oder andere illegale Aktivitäten aufbauen muss. Die Leichtigkeit, mit der diese Angriffe ausgeführt werden können, sorgt dafür, dass sie praktisch von jedem Ort der Welt ausgehen können.

# Insider-Bedrohungen



Rache – die älteste Geschichte der Welt. 2022 wurde ein IT-Spezialist angeklagt, weil er angeblich [den Server einer Gesundheitseinrichtung in Chicago gehackt](#) hatte. Als Auftragnehmer hatte er Zugang zu dem Server, und er hatte ein Motiv. Seine Stellenbewerbung bei der Organisation war abgewiesen worden, und ein paar Monate später wurde ihm von der beauftragten IT-Firma gekündigt. Dieser persönliche Racheakt führte zu einem Cyberangriff, der die medizinischen Untersuchungen, Behandlungen und Diagnosen vieler Patienten spürbar beeinträchtigte. Im Falle einer Verurteilung muss der Angreifer mit bis zu zehn Jahren Bundesgefängnis rechnen.



### Was Sie wissen müssen:

Ein Insider-Angriff, auch bekannt als Insider-Bedrohung, ist ein schädlicher Angriff, der von Insidern mit autorisiertem Zugriff auf das Computersystem, das Netzwerk und die Ressourcen Ihrer Bank durchgeführt wird. Bei diesen Angriffen zielen die Angreifer häufig darauf ab, geheime, geschützte oder anderweitig sensible Informationen und Vermögenswerte abzugreifen, um sich selbst zu bereichern oder Informationen an Wettbewerber weiterzugeben. Angreifer könnten auch versuchen, Ihr Unternehmen durch Systemunterbrechungen zu sabotieren, was Produktivitäts-, Rentabilitäts- und Reputationsverluste zur Folge haben kann.

### Wie der Angriff funktioniert:

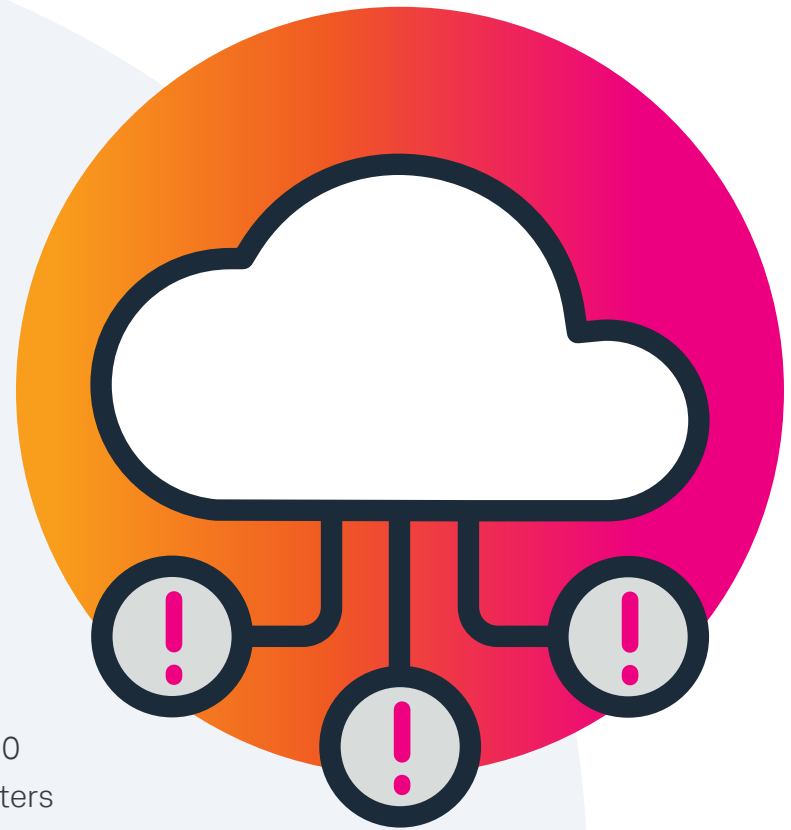
Insider besitzen einen klaren Vorteil: Sie haben bereits autorisierten Zugriff auf das Netzwerk, die Informationen und die Vermögenswerte Ihres Unternehmens. Sie können über Accounts verfügen, die ihnen Zugang zu wichtigen Systemen oder Daten geben, wodurch es für sie ein Leichtes ist, diese ausfindig zu machen, die Sicherheitskontrollen zu umgehen und sie an einen Standort außerhalb des Unternehmens zu versenden.

### Woher der Angriff erfolgt:

Die Urheber von Insider-Angriffen können böswillige Mitarbeiter in Ihrem Unternehmen oder Cyberspione sein, die sich als Auftragnehmer, Lieferanten oder externe Mitarbeiter ausgeben. Sie können sowohl eigenständig als auch als Teil von Nationalstaaten, Verbrecherbanden oder konkurrierenden Organisationen agieren. Es kann sich aber auch um externe Lieferanten oder Auftragnehmer handeln, die überall auf der Welt ansässig sind und in gewissem Umfang legitimen Zugang zu den Systemen und Daten des Unternehmens haben.

# IoT- Bedrohungen

Nachdem ein Datenleck die persönlichen Informationen von mehr als 3000 Benutzern von Haussicherheitstechnik des zu Amazon gehörenden Anbieters Ring offengelegt hatte, nutzten Hacker das Leck aus und kaperten die Video-türklingeln und intelligenten Kameras in den Häusern der Benutzer. **Tausende Unternehmen sind durch ihre Ring-Geräte einem Risiko ausgesetzt** – und Experten zufolge sind diese dokumentierten Angriffe nur die Spitze des Eisbergs. Inzwischen setzt Ring End-to-End-Verschlüsselung zum Schutz vor künftigen Hackerangriffen ein, doch mit der zunehmenden Verbreitung von IoT-Geräten wird dies wohl nicht der letzte Angriff dieser Art gewesen sein.





### Was Sie wissen müssen:

Weltweit gibt es schätzungsweise **15,14 Milliarden vernetzte IoT-Geräte** – eine Zahl, die bis 2030 voraussichtlich auf 30 Milliarden ansteigen wird. Allerdings fehlt es diesen Geräten oft an einer Sicherheitsinfrastruktur, was zu eklatanten Schwachstellen im Netzwerk führt, die ihre Angriffsfläche exponentiell vergrößern und sie anfällig für Malware machen. Zu den Angriffen, die über IoT-Geräte ausgeführt werden können, gehören DDoS-, Ransomware- und Social-Engineering-Angriffe.

### Wie der Angriff funktioniert:

Hacker und Nationalstaaten können Schwachstellen in vernetzten IoT-Geräten mit ausgeklügelter Malware ausnutzen, um sich Zugriff auf ein Netzwerk zu verschaffen, damit sie Benutzer überwachen oder geistiges Eigentum, geheime oder personenbezogene Daten und andere wichtige Informationen stehlen können. Sobald sie in ein IoT-System eingedrungen sind, können Hacker ihren neu gewonnenen Zugriff auch dafür nutzen, sich lateral zu anderen angeschlossenen Geräten zu bewegen oder sich für verschiedene schädliche Zwecke Zugriff auf ein größeres Netzwerk zu verschaffen.

### Woher der Angriff erfolgt:

Diese Angriffe können von jedem Ort der Welt ausgehen. Da jedoch viele Bereiche wie Regierungen, die Fertigungsindustrie und das Gesundheitswesen IoT-Infrastrukturen ohne angemessene Sicherheitsvorkehrungen einsetzen, sind diese Systeme leichte Ziele für Angriffe feindlicher Nationalstaaten und Organisationen für Cyberkriminalität. Im Gegensatz zu Angriffen auf die technische Infrastruktur könnten Angriffe auf vernetzte Bürger- oder Gesundheitssysteme zu weitreichenden Störungen, Panik und der Gefährdung von Menschenleben führen.

# Kompromittieren privilegierter Benutzer



[2022](#) prahlte die kriminelle Hackerbande Lapsus\$, die angeblich von einem Teenager aus dem britischen Oxford angeführt wird, öffentlich mit dem erfolgreichen Hack von Okta, einem Single-Sign-on-Anbieter, der weltweit von Tausenden Unternehmen und Regierungen genutzt wird. Lapsus\$ verschaffte sich über einen externen Supporttechniker Zugang zu einem „Super User“-Administratorkonto für Okta und hatte fünf Tage lang Zugriff auf den Laptop des Mitarbeiters mitsamt privilegiertem Zugriff auf einige Okta-Systeme. Die Hackergruppe informierte auf ihrem Telegram-Kanal über den Angriff und postete sogar Screenshots, die zeigten, dass sie in die Systeme von Okta eingedrungen waren. Das eigentliche Ziel war jedoch gar nicht Okta, sondern die 15.000 Okta-Kunden. Eine Woche später verzeichnete der Telegram-Kanal der Hacker 15.000 zusätzliche Follower, was viele weitere Angriffe befürchten ließ.



## Was Sie wissen müssen:

Es ist allgemein bekannt, dass sich viele schwerwiegende Datenschutzverletzungen auf den Missbrauch privilegierter Zugangsdaten zurückführen lassen. Es handelt sich dabei um Accounts mit weiterreichenden Rechten, wie z. B. Benutzer mit Domänenadministrator- oder Root-Berechtigungen. Angreifer nutzen immer öfter die Zugangsdaten privilegierter Benutzer, um auf die Ressourcen und Informationen eines Unternehmens zuzugreifen und sensible Daten zu exfiltrieren. Ein Angreifer, der sich Zugriff auf Anmeldeinformationen privilegierter Benutzer verschafft, kann die Kontrolle über die Infrastruktur eines Unternehmens übernehmen und damit Sicherheitseinstellungen ändern, Daten exfiltrieren, Benutzerkonten erstellen und vieles mehr. Dabei scheint er ein legitimer Benutzer zu sein und ist daher schwerer zu entdecken.

## Wie der Angriff funktioniert:

Angreifer versuchen, durch Social-Engineering-Methoden, Spear-Phishing-Nachrichten, Malware oder „Pass the Hash“-Angriffe Zugriff auf privilegierte Accounts zu erhalten. Unternehmen haben ihre Netzwerke geöffnet, um dem zunehmend mobilen, dezentralen Arbeitsstil gerecht zu werden und ein komplexes Netz aus Fernzugängen für Lieferanten und Dienstleister zu ermöglichen. Bei vielen dieser Verbindungen, einschließlich der Cloud, erfolgt der Zugriff über weitreichende privilegierte Accountzugangsdaten. Es ist schwierig, sie alle zu festzulegen, zu kontrollieren und zu überwachen, was Angreifern Angriffspunkte bietet.

Sobald die Angreifer sich Anmeldeinformationen beschafft haben, infiltrieren sie das System und stehlen, was sie können, z. B. SSH-Schlüssel, Zertifikate und Hashes für die Domänenverwaltung. Ein einziger erfolgreicher Angriff auf ein Account genügt, um eine weitreichende Datenschutzverletzung zu verursachen, die ein Unternehmen in die Knie zwingen kann.

## Woher der Angriff erfolgt:

Da Angreifer durch das Kompromittieren privilegierter Benutzer schwer zu entdeckenden, weitreichenden Zugang zu allen Arten von Datenprivilegien bekommen, ist diese Angriffsart für sie sehr attraktiv und wird häufig für verschiedene Arten von Cyberangriffen genutzt – sei es für politisch-ideologisch motivierte Cyberspionage von Nationalstaaten oder für raffinierte finanziell motivierte Cyberkriminelle wie Lapsus\$.

# Kompro- mittierte Zugangsdaten



[Group-IB](#), ein weltweit führender Cybersecurity-Anbieter, entdeckte 2023 eine sechsstellige Zahl von kompromittierten Geräten mit darauf gespeicherten ChatGPT-Anmeldeinformationen. Es dürfte kaum überraschen, dass der auf einem Large Language Model basierende Chatbot bei Cybercrime-Syndikaten sehr beliebt ist, besonders, wenn es darum geht, sich unbefugten Zugang zu Konten zu verschaffen und [sensible Informationen aus den ChatGTP-Interaktionen](#) für groß angelegte Kampagnen gegen Unternehmen und deren Mitarbeiter abzugreifen.



## Was Sie wissen müssen:

Die meisten Menschen verwenden bei der Anmeldung von ihnen genutzter Dienste nach wie vor auf die Ein-Faktor-Authentifizierung (was in puncto Cybersicherheit ein absolutes No-Go ist).

Zwar werden inzwischen strengere Anforderungen an Passwörter gestellt (z. B. hinsichtlich der Länge in Zeichen, der Kombination von Symbolen und Zahlen oder der Erneuerungsintervalle). Doch die meisten Endbenutzer verwenden ihre Anmeldedaten für gleich mehrere Konten, Plattformen und Services. Und versäumen es obendrein, diese regelmäßig zu aktualisieren.

Allein diese Tatsache macht es Angreifern ungemein leicht, Zugriff auf ein Nutzerkonto zu erhalten. Mit dem Ergebnis, dass sich eine Vielzahl der heutigen Sicherheitsverletzungen auf solche Sammelvorgänge von Zugangsdaten zurückführen lassen.

## Wie der Angriff funktioniert:

Ausgespähte Passwörter, Schlüssel oder andere Identifikatoren können von Angreifern dazu verwendet werden, sich unbefugten Zugang zu Informationen und Ressourcen zu verschaffen. Wobei entweder nur ein einzelner Account oder sogar ganze Datenbanken betroffen sein können.

Mit Hilfe eines vertrauenswürdigen Accounts können sich Angreifer Zugriff auf ein Unternehmen schaffen und unentdeckt sensible Datensätze exfiltrieren, ohne dass es jemandem auffällt. Gängige Methoden zum Sammeln von Zugangsdaten sind der Einsatz von Passwort-Sniffen, Phishing-Kampagnen oder Malware-Angriffen.

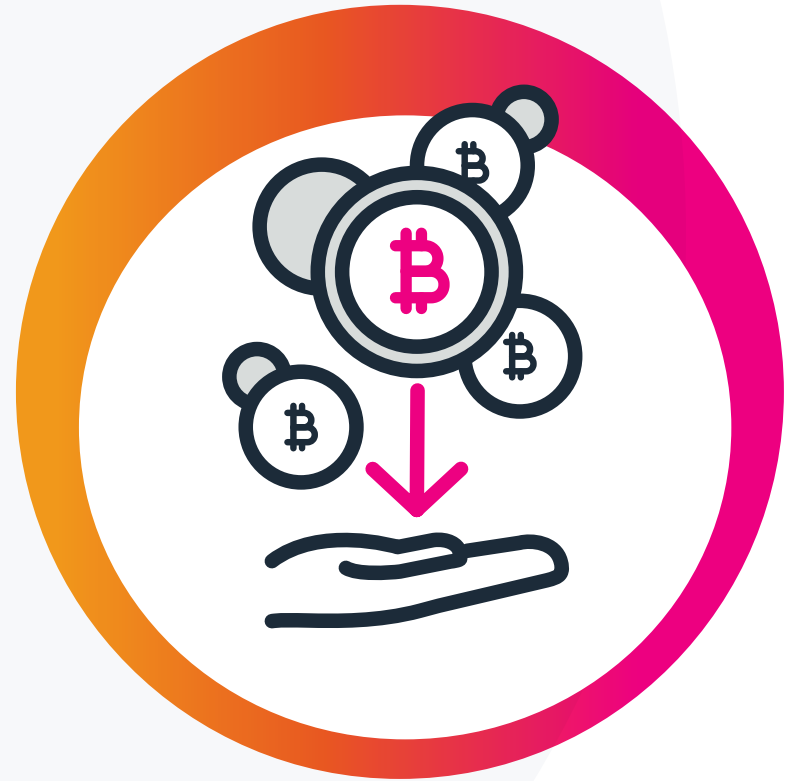
## Woher der Angriff erfolgt:

Kompromittierte Zugangsdaten stellen einen sehr großen Angriffsvektor dar. Weil sich Angreifer dadurch relativ leicht Zugang zu Computern, passwortgeschützten Accounts und der Netzwerkinfrastruktur eines Unternehmens verschaffen können.

Häufig sind die Angreifer gut organisiert und haben es auf bestimmte Unternehmen oder Personen abgesehen. Dabei muss es sich nicht zwingend um externe Akteure handeln. Ebenso können es auch Insider sein, die in gewissem Umfang einen legitimen Zugang zu den Systemen und Daten eines Unternehmens haben.

# Krypto-jacking-Angriff

Im Juli 2023 missbrauchten Cyberhacker Cloud-Workloads in bis zu 200 Fällen, um **heimlich und ohne Erlaubnis oder Wissen der User Kryptowährungen zu schürfen**. Dieser Kryptojacking-Angriff begann damit, dass dateilose Nutzdaten unauffällig in den Speicher des Zielsystems geladen wurden, sodass sie der Entdeckung erfolgreich entgingen.





### Was Sie wissen müssen:

Kryptojacking bezeichnet einen Angriff, bei dem ein Hacker Computersysteme mit Malware angreift, die sich auf einem Gerät versteckt und dessen Rechenleistung ausnutzt, um Kryptowährungen wie Bitcoin oder Ethereum zu minen – und zwar auf Kosten des Opfers. Das Ziel der Angreifer ist es, mit Computerressourcen anderer wertvolle Kryptowährungen zu erzeugen.

### Wie der Angriff funktioniert:

Eine Möglichkeit für Angreifer, Kryptojacking-Angriffe auszuführen, besteht darin, einen schädlichen Link in einer Phishing-E-Mail zu versenden, der Benutzer dazu verleitet, Kryptomining-Code direkt auf ihren Computer herunterzuladen.

Eine andere Möglichkeit besteht darin, einen JavaScript-Code in eine besuchte Webseite einzubetten – auch bekannt als Drive-by-Angriff. Beim Besuch der Website wird automatisch schädlicher Code zum Mining von Kryptowährungen auf den Computer des Besuchers heruntergeladen. Der Kryptomining-Code arbeitet dann unbemerkt im Hintergrund. Der einzige Hinweis darauf, dass etwas nicht stimmt, ist dann die Tatsache, dass der Computer langsamer ist als üblich.

### Woher der Angriff erfolgt:

Diese Angriffe können von jedem Ort der Welt ausgehen. Heutzutage sind für Kryptojacking keine besonderen technischen Fähigkeiten erforderlich. Im Deep Web sind Kryptojacking-Kits für nur 30 US-Dollar erhältlich. Dies ist eine niedrige Einstiegshürde für Hacker, die mit relativ geringem Risiko schnelles Geld verdienen wollen.

# Makro- viren

Einer der bekanntesten Virenvorfälle aller Zeiten, das [Melissa-Virus](#) Ende der 1990er Jahre, war nichts anderes als ein Makrovirus. Ein mit Melissa infizierter Computer kaperte das E-Mail-System Microsoft Outlook des Benutzers und verschickte mit Viren verseuchte Nachrichten an die ersten 50 Adressen in den Mailinglisten. Das Virus verbreitete sich mit unglaublicher Geschwindigkeit und verursachte weltweit einen Schaden von schätzungsweise 80 Millionen US-Dollar für die Wiederherstellung und Reparatur der betroffenen Systeme und Netzwerke. Auch wenn die Blütezeit von Makroviren zu Ende ist, gibt es diese Angriffe weiterhin, und sie zielen nicht mehr nur auf Microsoft Windows ab: [Jüngste Angriffe](#) galten auch Mac-Benutzern.





### Was Sie wissen müssen:

Ein Makrovirus ist ein Computervirus, das in der gleichen Makrosprache geschrieben ist, die auch für Softwareanwendungen verwendet wird. Einige Anwendungen wie Microsoft Office, Excel und PowerPoint ermöglichen die Einbettung von Makroprogrammen in Dokumente, sodass die Makros automatisch ausgeführt werden, wenn das Dokument geöffnet wird. Dadurch entsteht ein spezifischer Mechanismus, über den sich schädliche Computerbefehle schnell verbreiten können. Dies ist ein Grund, warum es gefährlich sein kann, unbekannte Anhänge in E-Mails oder E-Mails von unbekannten Absendern zu öffnen. Viele Antivirenprogramme können Makroviren erkennen, aber ihr Verhalten lässt sich auch dann immer noch nur sehr schwer analysieren.

### Wie der Angriff funktioniert:

Makroviren werden häufig über Phishing-E-Mails verbreitet, die Anhänge enthalten, in die das Virus eingebettet ist. Da die E-Mail den Anschein erweckt, als stamme sie von einer glaubwürdigen Quelle, wird sie von vielen Empfängern geöffnet. Sobald ein infiziertes Makro ausgeführt wird, kann es auf jedes andere Dokument auf dem Computer des Benutzers überspringen und dieses infizieren. Makroviren verbreiten sich immer dann, wenn ein Benutzer ein infiziertes Dokument öffnet oder schließt. Sie laufen auf Anwendungen und nicht auf Betriebssystemen. Die Verbreitung von Makroviren entsteht häufig durch die gemeinsame Nutzung von Dateien auf einem Datenträger oder in einem Netzwerk und durch das Öffnen einer an eine E-Mail angehängten Datei.

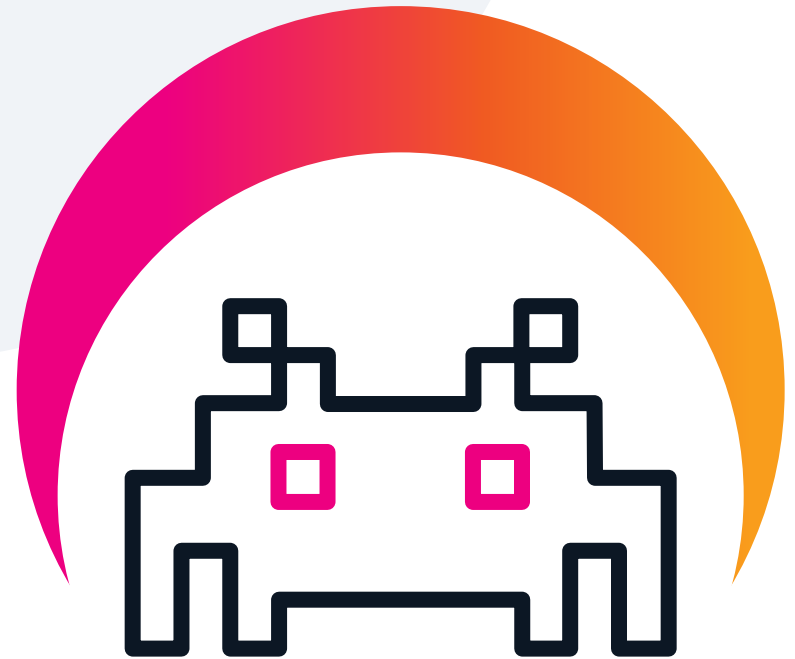
### Woher der Angriff erfolgt:

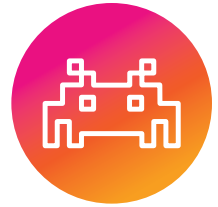
Obwohl Makroviren als schädliche Angriffe aus der Mode gekommen sind – vor allem, weil Antivirensoftware sie besser erkennen und deaktivieren kann – stellen sie noch immer eine große Bedrohung dar. Eine flüchtige Google-Suche nach „Makrovirus“ führt zu Anleitungen für die Erstellung von Makroviren und zu Tools, die Personen ohne Programmierkenntnisse bei der Erstellung dieser Viren unterstützen. Theoretisch kann also jede Person mit Internetzugang mit Leichtigkeit ein Makrovirus erstellen.

# Malware

Emotet wurde erstmals 2014 als Banking-Trojaner identifiziert, der es auf Verbraucher abgesehen hatte. Seitdem hat sich diese Malware vielfach neu erfunden und als eine ausgesprochen hartnäckige, weit verbreitete Bedrohung sowohl für die Privatwirtschaft als auch für die öffentliche Hand erwiesen.

Nach [Angaben der US-Staatssicherheit](#) ist Emotet eine der teuersten und zerstörerischsten Formen von Schadsoftware – die Kosten pro Incident belaufen sich auf mehr als 1 Million US-Dollar. Emotet hat [Behörden](#) in Frankreich, Japan, Kanada und Neuseeland ebenso attackiert wie Unternehmen, u. a. [Pharmahersteller](#), Fertigungs- und Technologieunternehmen sowie Finanzdienstleister. Im Februar 2021 haben die Strafverfolgungsbehörden in den USA und in Europa das Emotet-Netzwerk stillgelegt und damit die Kommunikation unterbrochen und die weitere Ausbreitung unterbunden. Doch schon [2023 war Emotet wieder da](#), und das üble Botnet treibt erneut sein Unwesen.





### Was Sie wissen müssen:

Malware gibt es in zahllosen Ausprägungen – sie spioniert, verschafft sich Admin-Rechte durch Hintertüren und ermöglicht ungehinderten unautorisierten Fernzugriff auf das Zielgerät. Sobald ein Angreifer die Kontrolle über den bzw. die fraglichen Rechner erlangt hat, kann er Programme installieren und entfernen, Webcams kapern, Dateien manipulieren sowie Anmeldeinformationen und andere sensible Daten abgreifen. Hacker können sich auch als legitime Benutzer ausgeben, dann weitere Malware herunterladen und so noch andere Computer und Geräte im Netzwerk kompromittieren.

### Wie der Angriff funktioniert:

Malware, die durch moderne Phishing-Methoden verbreitet wird, ist darauf ausgelegt, vertrauliche Informationen zu stehlen – dazu zählen Benutzeranmeldeinformationen, Screenshots, Webcam-Zugänge, Audio-, Standort- und Keylogging-Daten. Eine der gängigsten Phishing-Taktiken besteht darin, User dazu zu verleiten, eine Datei zu öffnen, die als Microsoft-Office-Dokument verpackt ist, namentlich PowerPoint und Word. Die Angreifer können Malware auch über Spearphishing-Kampagnen und per Drive-by-Download in Unternehmen einschleusen, aber auch mit herkömmlichen Attacken über Remote-Services.

### Woher der Angriff erfolgt:

Angesichts der Beliebtheit und der weiten Verbreitung von Malware ist diese Taktik ebenso heimtückisch wie üblich. Wenn Sie in Ihrem Posteingang eine verdächtige E-Mail mit einem Dateianhang finden, sollten Sie sich gründlich vergewissern, dass sie von einer vertrauenswürdigen Adresse stammt, bevor Sie sie öffnen, damit Sie nicht unbeabsichtigt Malware in Ihr Netzwerk einschleusen.

# Man-in-the-Middle-Angriff



Anfang 2022 entdeckte Microsoft eine [Phishing-Kampagne](#), deren Ziel Benutzer von Office365 waren. Die Angreifer leiteten die Benutzer auf eine gefälschte 365-Anmeldeseite und sammelten Anmeldeinformationen, um diese später für böswillige Zwecke zu missbrauchen. Die Angreifer verwendeten dabei ein [Evilginx2](#)-Phishing-Kit. Dieses MITM-Angriffsframework (Man-in-the-Middle) wird zum Phishing von Anmeldeinformationen zusammen mit Session Cookies verwendet und ermöglicht Angreifern, die Zwei-Faktor-Authentifizierung zu umgehen, um den Authentifizierungsprozess zu kapern. Microsoft wies in seinem [Blog-Beitrag](#) darauf hin, dass es sich nicht um eine Schwachstelle von MFA handelt – da beim AiTM-Phishing das Session Cookie gestohlen wird, wird der Angreifer im Namen des Benutzers für eine Sitzung authentifiziert, unabhängig davon, welche Anmeldemethode der Benutzer verwendet.



### Was Sie wissen müssen:

Bei Man-in-the-Middle-Angriffen (auch Adversary-in-the-Middle oder AiTM genannt) wird ein Proxy-Server eingerichtet, der die Anmeldesitzung des Opfers abfängt, sodass sich der Angreifer zwischen die beiden Parteien oder Systeme schalten kann, um Zugang zu sensiblen Informationen zu erhalten bzw. diese zu entwenden. Man-in-the-Middle-Angriffe ermöglichen Cyberkriminellen, Daten abzufangen, zu senden und zu empfangen, die für eine andere Person bestimmt sind – oder die gar nicht verschickt werden sollen –, und zwar ohne dass eine der beiden Parteien etwas davon mitbekommt, bevor es zu spät ist.

### Wie der Angriff funktioniert:

Praktisch jeder kann einen Man-in-the-Middle-Angriff ausführen. Seit der Implementierung von [HTTPS Everywhere](#) sind diese Arten von Angriffen jedoch schwieriger auszuführen und damit seltener geworden. Bei einem MITM-Angriff schaltet sich der Hacker zwischen den Benutzer und die eigentliche Website (oder einen anderen Benutzer) und leitet die Daten zwischen den Parteien weiter, wobei er beliebige Daten aus der Interaktion exfiltrieren kann.

### Woher der Angriff erfolgt:

Da die Durchführung von MITM-Angriffen durch die Verbesserung der Sicherheitstechnologien mittlerweile schwieriger geworden ist, sind die einzigen Gruppen, die solche Angriffe heute noch versuchen, sehr versierte Hacker oder staatliche Akteure. 2018 entdeckte die niederländische Polizei vier Mitglieder der russischen Hackergruppe Fancy Bear vor der Organisation für das Verbot von Chemiewaffen in den Niederlanden. Sie versuchten dort, durch MITM-Infiltration die Zugangsdaten von Mitarbeitern zu stehlen. Später im selben Jahr gaben die Regierungen der USA und Großbritanniens [Warnungen](#) heraus, dass russische staatlich unterstützte Akteure aktiv Router in Privathaushalten und Unternehmen zum Zweck der MITM-Exfiltration anvisieren.

# Masquerade-Angriff

Betrüger geben sich oft als Vertreter von Softwarefirmen aus, wenn sie ahnungslose Benutzer dazu verleiten wollen, Malware in Form von E-Mail-Anhängen herunterzuladen. Ein [aktueller Trend](#) betrifft Microsoft und Adobe. „Betrüger verschicken an ihre Opfer Microsoft-OneNote-Dateien als E-Mail-Anhänge, die Malware-Downloads auslösen, wenn jemand den Anhang öffnet“, berichtete Avast, ein bekanntes Antiviren- und Sicherheitsunternehmen, Anfang 2023. Seitdem sind Masquerade-Angriffe weiter auf dem Vormarsch.





### Was Sie wissen müssen:

Ein Masquerade-Angriff liegt vor, wenn ein Hacker eine gefälschte oder legitime (aber gestohlene) Identität verwendet, um sich über eine legitime Zugangskennung unbefugten Zugriff auf den Computer einer Person oder das Netzwerk eines Unternehmens zu verschaffen. Je nachdem, wie weit die Zugriffsrechte reichen, können Angreifer mithilfe von Masquerade-Angriffen Zugriff auf ein komplettes Netzwerk erhalten.

### Wie der Angriff funktioniert:

Ein Masquerade-Angriff kann erfolgen, nachdem die Zugangsdaten eines Benutzers gestohlen wurden, oder durch Authentifizierung auf unbewachten Rechnern und Geräten, die Zugang zum Zielnetzwerk haben.

### Woher der Angriff erfolgt:

Aus der Sicht von Insidern können sich Angreifer Zugriff verschaffen, indem sie Anmelde-Domains fälschen oder Keylogger verwenden, um legitime Authentifizierungsdaten zu stehlen. Die Angriffe können auch physisch erfolgen, wenn Rechner unbewacht gelassen werden, z. B. wenn ein Mitarbeiter auf den Laptop eines Kollegen zugreift, während dieser abwesend ist. Im Allgemeinen sind schwache Authentifizierungsmethoden, die von externen Parteien überlistet werden können, die Ursache dieses Problems.

# Meltdown- and-Spectre- Angriff



Die meisten Angriffe auf die Cybersicherheit nutzen eine Schwachstelle aus, z. B. einen Programmierfehler oder schlechtes Design. Doch nicht alle Angriffe sind gleich. So entdeckten zwei Google-Forscher eine Art von Angriff, die [alle Computerchip-Hersteller](#) betraf und potenziell Milliarden von Menschen dem Meltdown-and-Spectre-Angriff aussetzte.



## Was Sie wissen müssen:

Der Meltdown-and-Spectre-Angriff nutzt Schwachstellen in Computerprozessoren aus. Diese Schwachstellen ermöglichen es Angreifern, fast alle Daten zu stehlen, die auf dem Computer verarbeitet werden. Dieser Angriff **trifft den Kern der Computersicherheit**, die auf der Isolierung des Speichers beruht, um die Daten eines Benutzers zu schützen. Als „Meltdown“ bezeichnet man den Zusammenbruch der Schutzbarriere zwischen einem Betriebssystem und einem Programm, während „Spectre“ den Zusammenbruch der Barriere zwischen zwei Anwendungen bezeichnet, die Informationen voneinander fernhalten.

## Wie der Angriff funktioniert:

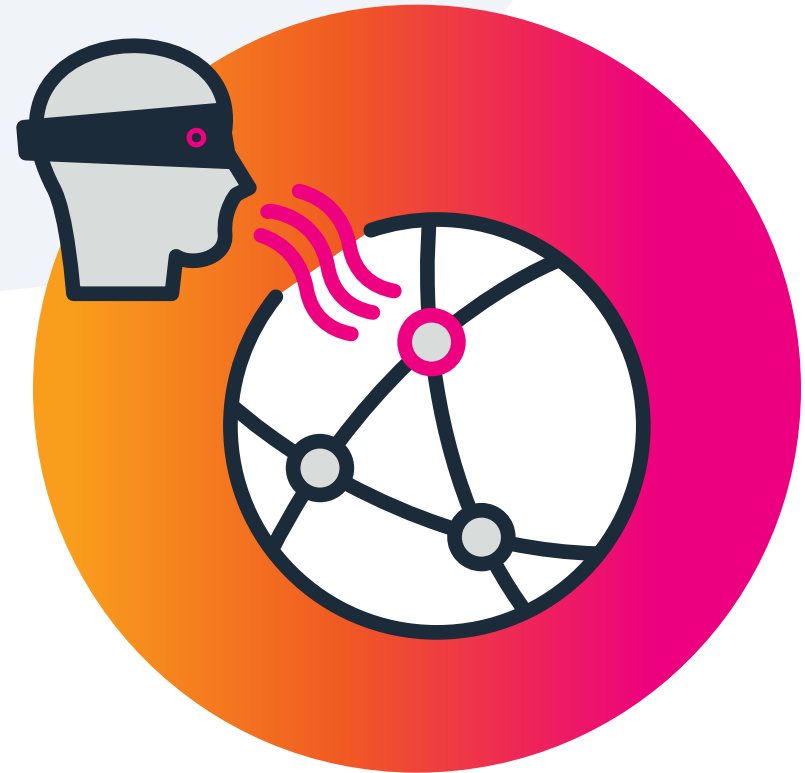
Ein Meltdown-and-Spectre-Angriff nutzt kritische Schwachstellen in modernen CPUs aus, die einen unbeabsichtigten Zugriff auf Daten im Arbeitsspeicher ermöglichen. Der Angriff bricht mit der Computernorm, nach der es Programmen nicht erlaubt ist, Daten von anderen Programmen zu lesen. Zu den Informationen, auf die es Angreifer typischerweise abgesehen haben, gehören in einem Passwort-Manager oder Browser gespeicherte Passwörter sowie E-Mails, Finanzdaten sowie personenbezogene Daten wie Fotos und Sofortnachrichten. Dieser Angriffstyp ist jedoch nicht auf PCs beschränkt. Er kann vielmehr auf fast jedes Gerät mit einem Prozessor abzielen, z. B. auch auf ein Mobiltelefon oder ein Tablet.

## Woher der Angriff erfolgt:

Der Meltdown-and-Spectre-Angriff kann von fast jedem Ort ausgeführt werden, und ein Großteil der Forschung hat sich bisher auf die einzigartige Natur dieses Angriffs konzentriert und nicht darauf, wer dahinter steckt.

# Network Sniffing

Smart Locks sind eine neue Art von Geräten, die Ihr Haus schützen und den Zugang zu ihm mit einem Klick (oder besser gesagt: einem Tippen) auf eine Taste erleichtern sollen. Doch die futuristische Herangehensweise an die Haussicherheit kann ernste Folgen haben, wie Sicherheitsforscher herausgefunden haben. Ein Smart Lock, das nicht ganz passend als „intelligentestes Schloss aller Zeiten“ vermarktet wurde, konnte über das [Abfangen des Netzwerk-Traffics](#) zwischen der mobilen App und dem Schloss selbst geknackt werden. Noch erschreckender war, dass dies durch preiswerte, leicht erhältliche Network Sniffer geschehen konnte.





### Was Sie wissen müssen:

Network Sniffing, auch Packet Sniffing genannt, bezeichnet das Erfassen, Überwachen und Analysieren von Daten, die in einem Netzwerk fließen, in Echtzeit. Ob über Hardware, Software oder eine Kombination aus beidem: Angreifer verwenden Sniffing-Tools, um unverschlüsselte Daten aus Netzwerkpaketen abzufangen, z. B. Anmeldedaten, E-Mails, Passwörter, Nachrichten und andere sensible Informationen.

### Wie der Angriff funktioniert:

Ähnlich wie beim Abhören von Telefongesprächen, bei dem jemand nach sensiblen Details sucht, arbeitet das Network Sniffing im Hintergrund und hört unbemerkt mit, wenn Informationen zwischen zwei Parteien in einem Netzwerk ausgetauscht werden. Dies geschieht, wenn Angreifer durch die Installation von Software oder Hardware, die an ein Gerät angeschlossen wird, einen Sniffer in einem Netzwerk platzieren, der es ermöglicht, den Traffic über das kabelgebundene oder drahtlose Netzwerk, zu dem das Host-Gerät Zugang hat, abzufangen und aufzuzeichnen. Aufgrund der Komplexität der meisten Netzwerke können sich Sniffer lange Zeit darin aufhalten, ohne entdeckt zu werden.

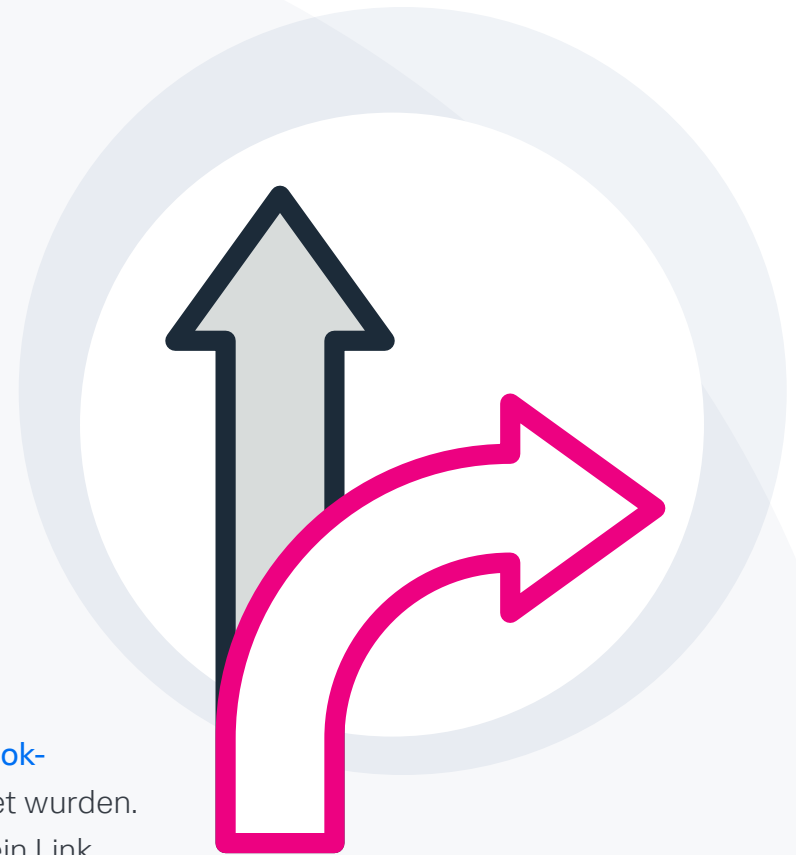
### Woher der Angriff erfolgt:

Network Sniffing wird oft legal von Organisationen wie Internetanbietern, Werbeagenturen, Regierungsbehörden und anderen durchgeführt, die den Netzwerkverkehr überprüfen müssen.

Es kann jedoch auch von Hackern rein aus Spaß oder von Nationalstaaten durchgeführt werden, die sich geistiges Eigentum aneignen möchten. Wie Ransomware können auch Network Sniffer in das Netzwerk eingeschleust werden, indem die richtige Person auf den richtigen Link klickt. Auch Insider mit Zugang zu sensibler Hardware können einen Angriffsvektor darstellen.

# Open Redirection

2022 wurde eine weitere [Phishing-Kampagne aufgedeckt, die auf Facebook-Nutzer abzielte](#) und bei der Hunderte Millionen von Zugangsdaten erbeutet wurden. Dabei wurde eine gängige Methode verwendet: Per Sofortnachricht wird ein Link von einem kompromittierten Facebook-Konto gesendet. Dieser Link führt dann eine Reihe von Umleitungen durch, oft über Malvertising-Seiten, um Aufrufe und Klicks (und Einnahmen für den Angreifer) zu generieren und schließlich auf einer gefälschten Seite zu landen. Host Redirection, auch Open Redirection genannt, ist zwar als Angriffsmethode nicht neu, doch die Größenordnung dieser Phishing-Kampagne ist wirklich bemerkenswert. Untersuchungen zeigten, dass nur eine von rund 400 Landing Pages, die für Phishing-Zwecke eingesetzt wurde, im Jahr 2021 2,7 Millionen Besucher hatte und im Juni 2022 dann 8,5 Millionen. In einem Gespräch mit Experten prahlte der Angreifer damit, dass er pro tausend Besuchen von US-Facebook-Nutzern 150 US-Dollar verdiene, womit seine Gesamteinnahmen bei 59 Millionen US-Dollar liegen würden.





### Was Sie wissen müssen:

Host Redirection-Angriffe sind weit verbreitet und werden immer subversiver, da die Hacker immer kreativer werden, um ihre Ziele zu ködern. Angreifer nutzen URL-Umleitungen, um das Vertrauen der Benutzer zu gewinnen, bevor sie schließlich zuschlagen. In der Regel verwenden sie eingebettete URLs, eine .htaccess-Datei oder sogar Phishing-Taktiken, um den Traffic auf eine schädliche Website umzuleiten.

### Wie der Angriff funktioniert:

Hacker könnten einen Phishing-Versuch unternehmen und eine E-Mail mit einer nachgemachten URL der Website an ihre nichts ahnenden Opfer senden. Wenn die Website seriös erscheint, kann es vorkommen, dass Nutzer beim Ausfüllen von Eingabeaufforderungen oder Formularen versehentlich personenbezogene Daten weitergeben. Angreifer können diese Art von Angriff ausweiten, indem sie gefälschte Command & Control-Domains in Malware einbetten und schädliche Inhalte auf Domains hosten, die Unternehmensservern zum Verwechseln ähnlich sind.

### Woher der Angriff erfolgt:

Die Ursprünge dieser Art von Angriff sind nicht so wichtig wie das Ziel. Dieser Angriff zielt in der Regel auf unbedachte Internetnutzer ab, die nicht bemerken, dass die URL ihrer Lieblingsdomain um einen oder zwei Buchstaben geändert wurde. Und da dieser Angriff aufgrund seiner Einfachheit so beliebt ist (er kann z. B. einfach über die Registrierung eines Domain-Namens erfolgen), kann er von fast jedem Ort der Welt ausgehen.

# Pass the Hash

Der berühmte Hack der Accounts von über 40 Millionen Target-Kunden war u. a. dank der **bekannten Angriffstechnik** Pass the Hash (PtH) erfolgreich. Die Hacker nutzten PtH, um sich Zugang zu einem NT-Hash-Token zu verschaffen, mit dem sie sich ohne das Klartext-Passwort beim Active Directory-Administratorkonto anmelden konnten. Dadurch erhielten sie die notwendigen Berechtigungen, um ein neues Administratorkonto für die Domain zu erstellen und es später zur Gruppe der Domain-Admins hinzuzufügen. Diese Verankerung im System gab ihnen die Möglichkeit, personenbezogene Daten und Zahlungskartendaten von Target-Kunden zu stehlen.





### Was Sie wissen müssen:

PtH ermöglicht es einem Angreifer, das Passwort eines Benutzers mit dem zugrunde liegenden NTLM- oder LanMan-Hash anstelle des zugehörigen Klartext-Passworts zu authentifizieren. Sobald der Hacker einen gültigen Benutzernamen zusammen mit den Hash-Werten des Passworts besitzt, kann er sich problemlos mit dem Account des Benutzers anmelden und Aktionen auf lokalen oder entfernten Systemen durchführen. Im Wesentlichen ersetzen Hashes die ursprünglichen Passwörter, aus denen sie generiert wurden.

### Wie der Angriff funktioniert:

Auf Systemen, die NTLM-Authentifizierung verwenden, wird das Passwort oder die Passphrase eines Benutzers niemals im Klartext übermittelt. Stattdessen wird es als Hash-Wert als Antwort auf ein Challenge-Response-Authentifizierungsverfahren gesendet. In diesem Fall werden gültige Passwort-Hashes für das verwendete Konto mithilfe einer Technik erfasst, die Zugriff auf die Zugangsdaten ermöglicht.

### Woher der Angriff erfolgt:

Diese Art von Angriff ist ausgefeilter als andere Methoden und wird in der Regel von Hackergruppen durchgeführt, die gut organisiert sind, es auf eine bestimmte Organisation oder Person abgesehen haben und auf politische Einflussnahme oder finanziellen Gewinn aus sind.

# Phishing

Im Juni 2022 kam es bei der Cloud-Kommunikationsplattform Twilio zu einer **(zweiten) großen Kompromittierung**. Die Hacker von „Okta-pus“, die für beide Vorfälle verantwortlich waren, verschafften sich mithilfe von Voice-Phishing Zugang zu Kundendaten: Sie gaben sich telefonisch als die IT-Abteilung von Twilio aus und täuschten damit einen Mitarbeiter. Im Glauben, er spreche mit einer legitimen Twilio-Vertretung, übermittelte der Angestellte den Bedrohungsakteuren die Anmeldedaten seines Unternehmens. Dieser Verstoß führte zum unbefugten Zugriff auf eine gewisse Anzahl von Kundenkontaktdaten.





### Was Sie wissen müssen:

Bei einem Phishing-Angriff werden Verbraucher, Benutzer oder Mitarbeiter dazu verleitet, auf einen böswilligen Link zu klicken, der sie meist zu einer gefälschten Website bringt, wo sie personenbezogene Daten wie Bankkontennummern, Kreditkartendaten oder Passwörter eingeben sollen. Die Angriffe erfolgen per E-Mail, Sofortnachricht oder über eine andere Kommunikationsart. Seien Sie auf der Hut, denn diese gefälschten Websites sehen zwar überzeugend echt aus, die Angreifer fangen jedoch alle Informationen ab, die Sie dort übermitteln. Oder sie bringen Malware in Umlauf, die darauf abzielt, Geld von Ihren Konten, persönlich identifizierbare Kundendaten oder andere wichtige Vermögenswerte zu stehlen.

### Wie der Angriff funktioniert:

In der Regel werden Sie durch eine E-Mail ausgetrickst, deren Absender sich als jemand ausgibt, den Sie kennen – z. B. ein Vorgesetzter oder ein Kollege – und in der Sie dazu verleitet werden, schädliche Anhänge zu öffnen oder auf Links zu klicken, die Sie zu Webseiten führen, die legitimen Websites zum Verwechseln ähnlich sind.

### Woher der Angriff erfolgt:

Noch vor wenigen Jahrzehnten konnte eine große Anzahl an Phishing-Angriffen nach Nigeria zurückverfolgt werden. Diese Angriffe waren unter dem Namen 419-Scams bekannt – in Anlehnung an den Code für Betrug im nigerianischen Strafgesetzbuch.

Heute haben Phishing-Angriffe ihren Ursprung in aller Welt, wobei laut dem InfoSec Institute [viele in den BRIC-Ländern](#) (Brasilien, Russland, Indien und China) auftreten. Aufgrund der einfachen Verfügbarkeit von Phishing-Toolkits sind selbst Hacker mit nur geringen technischen Kenntnissen in der Lage, Phishing-Kampagnen zu starten. Die Hintermänner dieser Kampagnen reichen von einzelnen Hackern bis hin zu organisierten Cyberkriminellen.

# Phishing Payloads

Es ist ein Phishing-Angriff aufgetaucht, der in seiner Art einzigartig ist und der Bedrohungsgruppe [TA866](#) zugeschrieben wird. Er erste Malware-Ladung macht dabei Screenshots von den Geräten der Opfer. So können die Angreifer den potenziellen Wert des Opfers abschätzen und entscheiden, ob sie weitere Malware einbringen wollen. Diese Kampagne hat bislang über 1000 Unternehmen und Organisationen in den USA und Deutschland getroffen.





### Was Sie wissen müssen:

Trotz ihrer einfachen Natur bleibt die Phishing-Methode die am weitesten verbreitete und gefährlichste Cyberbedrohung. Untersuchungen haben ergeben, dass 91 % aller erfolgreichen Angriffe über eine Phishing-E-Mail eingeleitet werden.

Diese E-Mails verwenden betrügerische Domains, E-Mail-Scraping-Techniken, bekannte Kontaktnamen als Absender und andere Taktiken, um die Zielpersonen dazu zu verleiten, auf einen schädlichen Link zu klicken, einen Anhang mit einer schädlichen Payload zu öffnen oder sensible personenbezogene Daten einzugeben, die die Täter abfangen können. Die „Payload“ ist hierbei ein Verweis auf die übermittelten Daten, die die beabsichtigte Nachricht darstellen. Kopfzeilen und Metadaten werden nur gesendet, um die Zustellung der Payload an die richtige Person zu ermöglichen.

### Wie der Angriff funktioniert:

Dieser Angriff folgt einem typischen Muster: Zunächst versendet der Angreifer eine Phishing-E-Mail, und der Empfänger lädt die angehängte Datei herunter, bei der es sich in der Regel um eine .docx- oder .zip-Datei mit einer eingebetteten .lnk-Datei handelt. Danach führt die .lnk-Datei ein PowerShell-Skript aus, und schließlich führt das Powershell-Skript eine Reverse Shell aus. Damit ist der Angriff erfolgreich abgeschlossen.

### Woher der Angriff erfolgt:

Da für diese Art von Angriffen kein hohes Maß an Raffinesse erforderlich ist und Phishing im Mittelpunkt der meisten Cyberangriffe steht, können sie von jedem Ort der Welt ausgehen.

# Ransomware



Nach Angaben des Cybersecurity-Unternehmens Emsisoft waren 2019 mindestens 948 Regierungsbehörden, Bildungseinrichtungen und Anbieter im Gesundheitswesen in den USA **von Ransomware-Angriffen betroffen**, wobei sich der potenzielle Schaden auf mehr als 7,5 Milliarden US-Dollar belief.

Im medizinischen Bereich können solche Angriffe dazu führen, dass Patienten in andere Krankenhäuser verlegt werden, dass Krankenakten unzugänglich gemacht werden (oder dauerhaft verloren gehen) und dass Notrufzentralen auf gedruckte Karten und Papierprotokolle angewiesen sind, um den Überblick über die Einsatzkräfte zu behalten. Bei Regierungsbehörden können z. B. die lokalen Notrufdienste unterbrochen werden. Laut dem Staatsanwalt von Manhattan, Cyrus Vance Jr., könnten **die Auswirkungen von Ransomware** genauso verheerend und kostspielig sein wie eine Naturkatastrophe in der Größenordnung von Hurrikan Sandy.



### Was Sie wissen müssen:

Ransomware ist ein Angriff, bei dem ein infizierter Host die Daten eines Opfers verschlüsselt und sie als eine Art Geisel hält, bis dem Angreifer ein Lösegeld gezahlt wird. Die jüngsten Ransomware-Angriffe haben gezeigt, dass Hacker inzwischen damit drohen, die gestohlenen Daten weiterzugeben oder zu verkaufen, was den potenziellen Schaden dieser Art von Angriffen um ein Vielfaches steigert.

Es gibt unzählige Arten von Ransomware, doch bestimmte Gruppen sind besonders bösartig. Eine berühmte Gruppe namens **Blackmatter** hat verschiedene Organisationen angegriffen, die für die US-Wirtschaft und -Infrastruktur von entscheidender Bedeutung sind, darunter auch Unternehmen aus der Lebensmittel- und Agrarindustrie. Eine weitere Art von Ransomware, vor der Sie sich in Acht nehmen sollten, ist **Ryuk**. Bis 2019 war Ryuk mit 12,5 Millionen US-Dollar die Ransomware mit dem höchsten Lösegeld, das jemals gezahlt wurde.

### Wie der Angriff funktioniert:

Angreifer können Ransomware über Spear-Phishing-Kampagnen und Drive-by-Downloads sowie über herkömmliche, auf Remote-Diensten basierende Angriffe auf den Rechnern von Unternehmen und Privatpersonen installieren. Sobald die Malware auf dem Rechner des Opfers installiert ist, informiert sie den Benutzer mit einem Popup-Fenster oder durch Weiterleitung auf eine Website darüber, dass seine Dateien verschlüsselt sind und erst wieder entschlüsselt werden, wenn er ein Lösegeld zahlt.

Bei Ransomware as a Service (RaaS) liegt das Geschäftsmodell zwischen Ransomware-Betreibern und Ransomware-Partnern: Die Partner zahlen für die Ausführung von Ransomware-Angriffen, die von Betreibern entwickelt wurden. Mit speziellen RaaS-Paketen können auch Partner, die nicht die erforderlichen Skills oder die nötige Zeit haben, eigene Ransomware-Varianten zu entwickeln, schnell und kostengünstig loslegen. Ein solches RaaS-Kit kann Rund-um-die-Uhr-Support, Kombinationsangebote, Nutzerbewertungen, Foren und andere Funktionen enthalten, die sich von denen legitimer SaaS-Anbietern in nichts unterscheiden.

### Woher der Angriff erfolgt:

Ransomware ist in der Regel das Werk professioneller Cyberkrimineller, denn um anonym zu bleiben, nachdem sie Regierungen oder Großunternehmen erpresst haben, ist technologische Raffinesse erforderlich. Seit dem Aufkommen von Kryptowährungen, die anonyme Transaktionen vereinfachen, ist die allgemeine Bevölkerung jedoch einem größeren Risiko von Ransomware-Angriffen ausgesetzt.

Weil RaaS-Kits relativ einfach zu nutzen und ganz leicht im Dark Web zu finden sind, wo sie großflächig beworben werden, könnte ein solcher Angriff von jedem angehenden Hacker ausgehen, der Geld genug hat, ein Kit zu kaufen.

# Rechnungs- betrug

Paypal ist ein Finanzdienst und Online-Zahlungssystem, mit dem Kunden problemlos Geld senden und empfangen können. Doch gerade jene Funktionen, die Paypal so schnell und effizient machen, werden **von Cyberdieben gezielt ausgenutzt**. Hacker und Betrüger nutzen das System, um den Verbrauchern im Rahmen eines Zahlungsbetrugs Geld zu stehlen oder manchmal sogar ganze Bankkonten leer zu räumen.





### Was Sie wissen müssen:

Mit dem Begriff Rechnungsbetrug bzw. Zahlungsbetrug wird jede Art von gefälschter oder illegaler Transaktion bezeichnet, bei denen Dritte unerlaubt Geld von Verbrauchern abzweigen. Und diese Methoden funktionieren – laut jüngsten Erhebungen der FTC haben Verbraucher 2022 **fast 8,8 Milliarden US-Dollar durch Betrug verloren**, was einem Anstieg von über 30 % gegenüber dem Vorjahr entspricht.

### Wie der Angriff funktioniert:

Bei einem solchen Angriff soll eine möglichst große Anzahl von Personen dazu bewegt werden, wiederholt kleinere bzw. zumutbare Geldbeträge zu zahlen. Beträge, die geringfügig genug sind, damit der Betrug nicht auffällt. Bei dieser Masche verschicken Angreifer gefälschte, aber echt erscheinende Rechnungen, in denen Kunden dazu aufgefordert werden, Geld zu überweisen.

Da die meisten Kunden regelmäßig kostenpflichtige digitale Dienste in Anspruch nehmen, spekulieren die Angreifer einfach darauf, dass ihre Opfer fälschlicherweise annehmen, die gefälschte Rechnung sei für einen Dienst, den sie tatsächlich nutzen. Daraufhin veranlassen die Verbraucher eine Überweisung oder Kreditkartenzahlung, um die falsche „Rechnung“ zu begleichen.

### Woher der Angriff erfolgt:

Rechnungsbetrug findet überall auf der Welt statt. Zumeist handelt es sich um organisierte Angreifer, die über entsprechende Finanzmittel, die nötige Bandbreite und Technologien zum Erstellen gefälschter Rechnungen verfügen. Ähnlich dem „Phishing“ wird auch beim Rechnungsbetrug in der Regel eine breite, zufällig ausgewählte Gruppe von Personen ins Visier genommen.

# Router- und Infrastrukturangriffe



Cisco wurde [Opfer eines Router- und Infrastrukturangriffs](#), bei dem ein Router-„Implantat“ namens SYNful Knock auf 14 Routern in vier verschiedenen Ländern gefunden wurde. Bei SYNful Knock handelt es sich um persistente Malware, die es einem Angreifer ermöglicht, die Kontrolle über ein betroffenes Gerät zu erlangen und seine Integrität mit einem modifizierten Cisco IOS-Software-Image zu kompromittieren. Laut Mandiant hat SYNful Knock verschiedene Module, die über das HTTP-Protokoll aktiviert und durch manipulierte TCP-Pakete, die an das Gerät gesendet werden, ausgelöst werden.



### Was Sie wissen müssen:

Router-Implantate sind selten, und es wurde allgemein angenommen, dass sie eher theoretischer Natur seien. [Laut neueren Herstellerhinweisen](#) kommen sie in der Praxis jedoch durchaus vor. Die Angreifer verschaffen sich wahrscheinlich Zugang zu diesen Geräten, indem sie bekannte Schwachstellen ausnutzen oder Geräte anvisieren, bei denen das Passwort schwach und leicht zu erraten oder gar nicht geändert ist. Aufgrund seiner Rolle im Netzwerk ist ein Router ein ideales Ziel, das wiederholtes Eindringen und weitere Infizierungen ermöglicht.

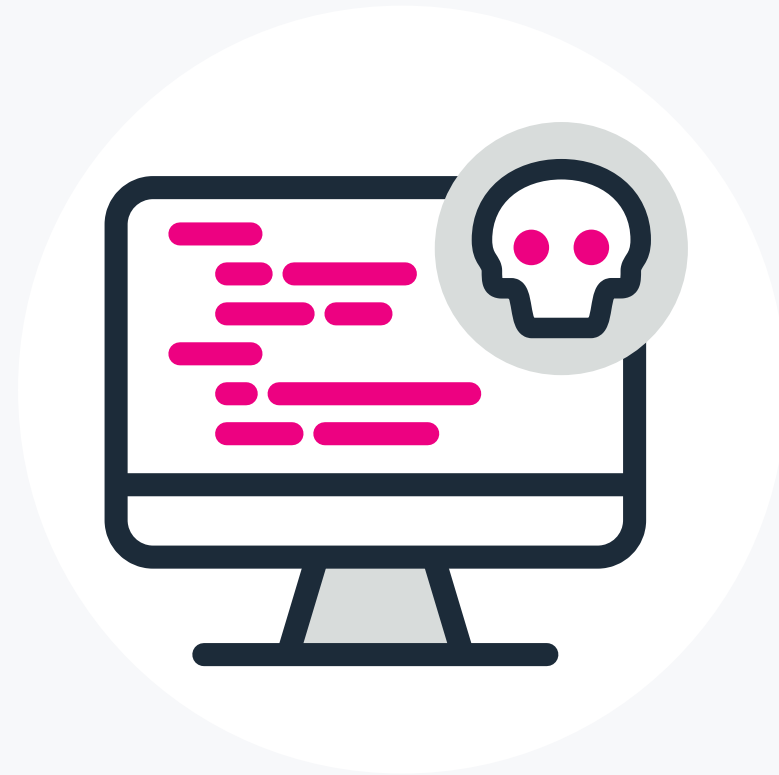
### Wie der Angriff funktioniert:

Netzwerkgeräte, wie Router und Switches, werden oftmals als Ressourcen übersehen, die Angreifer zum Kompromittieren von Unternehmen nutzen können. Angreifer kompromittieren Netzwerkgeräte und erhalten dann möglicherweise direkten Zugriff auf die interne Infrastruktur des Unternehmens, womit sie die Angriffsfläche effektiv vergrößern und Zugriff auf private Services bzw. Daten bekommen.

### Woher der Angriff erfolgt:

Bei komplexen Bedrohungen nehmen Angreifer gerne diese kritischen Assets ins Visier, um so Netzwerk-Traffic abzufangen und umzuleiten, Betriebssysteme über eine Backdoor zu flashen und schwächere kryptografische Algorithmen zu implementieren, damit der Netzwerk-Traffic leichter entschlüsselt werden kann.

# Schädliche PowerShell



Angriffssequenzen, die die viel genutzte PowerShell ausnutzen, werden dank ihrer Fähigkeit, Viren über ein Netzwerk zu verbreiten, bei Cyberkriminellen und Cyberspionen immer beliebter. Berühmte Bösewichte wie [APT29](#) (auch bekannt als „Cozy Bear“) verwenden PowerShell-Skripte, um wichtige Informationen für immer noch raffiniertere Cyberangriffe zu sammeln. [2020](#) nutzte die berühmte Bedrohungsgruppe APT35 (alias „Charming Kitten“) Powershell für einen Ransomware-Angriff auf eine Wohltätigkeitsorganisation und zum Abfangen und Exfiltrieren von Daten einer US-Kommunalverwaltung.



### Was Sie wissen müssen:

PowerShell ist ein von Microsoft entwickeltes Befehlszeilen- und Skripting-Tool, das auf .NET (ausgesprochen „dot net“) basiert und es Administratoren und Benutzern ermöglicht, Systemeinstellungen zu ändern und Aufgaben zu automatisieren. Das Command Line Interface (CLI) bietet viele Tools und hohe Flexibilität, was es zu einer beliebten Shell- und Skriptsprache macht. Auch Angreifer haben die Vorzüge von PowerShell erkannt – nämlich die Möglichkeit, unbemerkt auf einem System als Code-Endpunkt zu operieren und Aktionen im Hintergrund auszuführen.

### Wie der Angriff funktioniert:

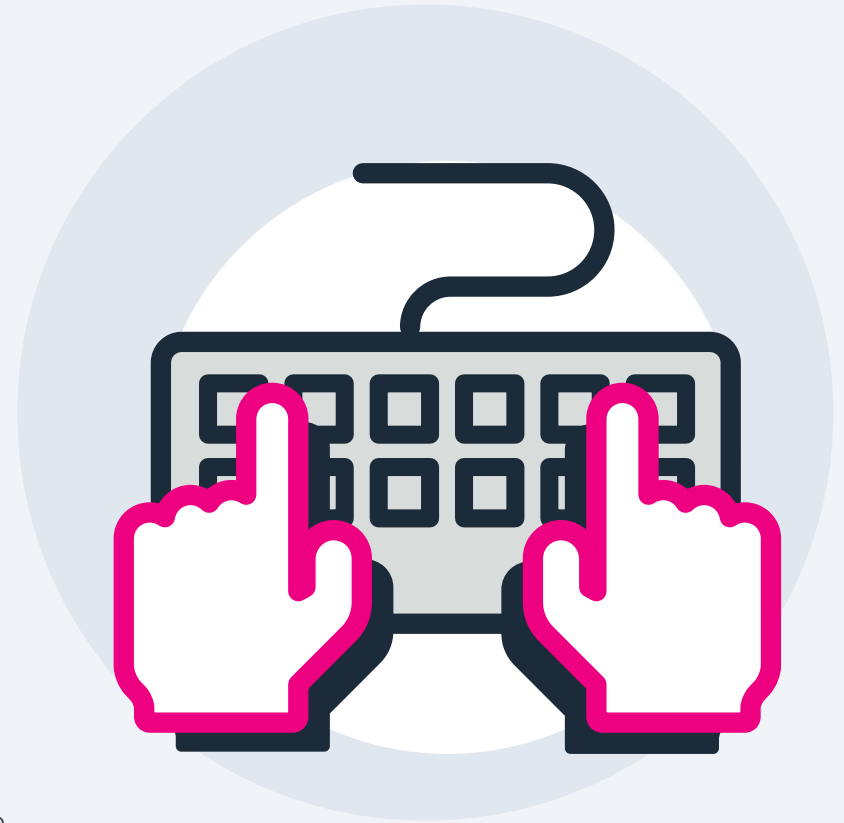
Da PowerShell eine Skriptsprache ist, die auf den meisten Unternehmenscomputern ausgeführt wird, und da die meisten Unternehmen ihre Code-Endpunkte nicht überwachen, wird die Logik hinter dieser Art von Angriff sehr schnell klar. Es ist für Angreifer einfach, Zugriff zu erhalten, und noch einfacher, sich in das System einzubetten. Es muss keine Malware installiert werden, um das schädliche Skript zu starten oder auszuführen. Das bedeutet, dass der Hacker die Entdeckung mühelos vermeiden kann, indem er die Analyse der ausführbaren Dateien umgeht und anschließend nach Belieben Schaden anrichtet.

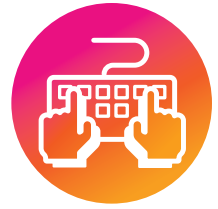
### Woher der Angriff erfolgt:

Diese Art von Angriff ist ausgefeilter als andere Methoden und wird in der Regel von einem Powerhacker ausgeführt, der genau weiß, was er tut (im Gegensatz zu Amateuren, die eher auf Brute-Force-Angriffe zurückgreifen). Hacker gehen stets unauffällig vor, verwischen geschickt ihre Spuren und wissen, wie sie sich lateral im Netzwerk bewegen können.

# Schatten-IT

Da Software-as-a-Service-Anwendungen (SaaS) heute immer schneller und einfacher zu nutzen sind, können Mitarbeiter nun Lösungen auf ihre Arbeitsplätze herunterladen, die sie bei der Erledigung ihrer Aufgaben unterstützen. Viele nutzen diese Anwendungen jedoch mit wenig Rücksicht auf die Sicherheit. Es überrascht daher nicht, dass eine Forbes Insights-Befragung mit dem Titel „[Cyber Resilience Perception Gaps: What Could Go Wrong?](#)“ hat ergeben, dass mehr als jedes fünfte Unternehmen von einem Cybervorfall betroffen war, der von einer nicht autorisierten Schatten-IT-Ressource ausging.





### Was Sie wissen müssen:

Der Begriff Schatten-IT bezieht sich auf IT-Anwendungen und -Infrastrukturen, die Mitarbeiter ohne das Wissen und/oder die Zustimmung der IT-Abteilung ihres Unternehmens nutzen. Dazu können Hardware, Software, Webdienste, Cloud-Anwendungen und andere Programme gehören. In der Regel laden Mitarbeiter diese Anwendungen in guter Absicht herunter und nutzen sie, um ihre Arbeit zu erleichtern oder effizienter zu gestalten. Dieses Phänomen ist so weit verbreitet, dass laut einer [Schätzung von Gartner](#) ein Drittel aller Angriffe auf die Cybersicherheit in Unternehmen von Schatten-IT-Ressourcen ausgehen. Da die Benutzer weitgehend unbemerkt auf diese Anwendungen zugreifen, öffnen sie oft ungewollt die Schleuse für Insider-Bedrohungen, Datenschutzverletzungen und Compliance-Verstöße.

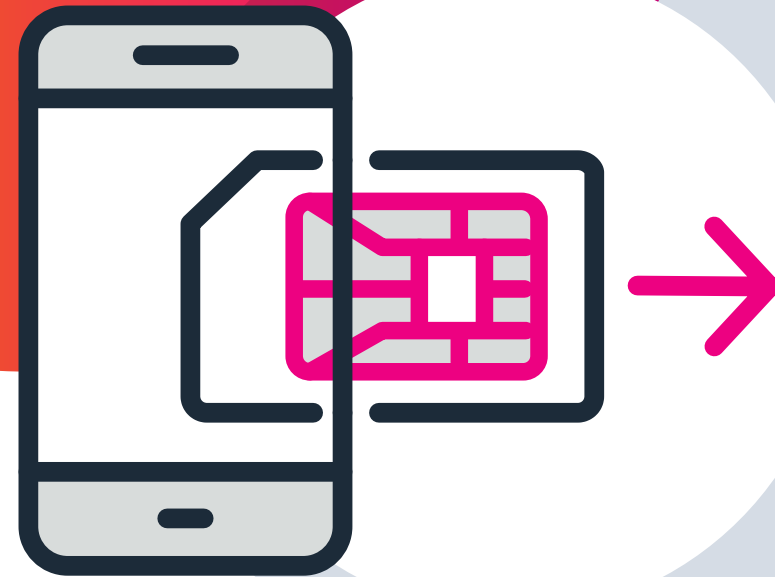
### Wie der Angriff funktioniert:

Wie der Name schon vermuten lässt, ist die Geheimhaltung der Schatten-IT darauf zurückzuführen, dass Mitarbeiter Daten auf nicht autorisierten Cloud-Diensten freigeben oder speichern, was zahlreiche Sicherheits- und Compliance-Risiken mit sich bringt. Verstöße können auftreten, wenn Mitarbeiter kritische oder regulierte Daten in Schatten-IT-Anwendungen hochladen, freigeben oder speichern, ohne dass geeignete Sicherheits- und Data-Loss-Prevention-Lösungen (DLP) vorhanden sind. Die offengelegten Informationen sind dann ein leichtes Ziel für Insider-Bedrohungen und Datendiebstahl und können darüber hinaus zu kostspieligen Compliance-Verstößen führen. Außerdem können die Anwendungen selbst Endpunktschwachstellen und Sicherheitslücken aufweisen.

### Woher der Angriff erfolgt:

In diesem Fall geht die Bedrohung von einer Organisation selbst aus. Mitarbeiter, die Schatten-IT-Apps verwenden, tun dies oft, um Richtlinien zu umgehen oder ihre Arbeit schneller zu erledigen, und nicht unbedingt, um ihre Arbeitgeber und Kollegen zu gefährden. Letztlich öffnen sie dadurch jedoch Insidern oder externen Hackern, die Sicherheitslücken in diesen Systemen ausnutzen wollen, Tür und Tor.

# Sim-Jacking



Am 30. August 2019 wurden die 4,2 Millionen Follower von Twitter-CEO Jack Dorsey von einer Hackergruppe, die sich „Chuckling Squad“ nannte, mit **äußerst beleidigenden Nachrichten** überschwemmt. Die Gruppe nutzte SIM-Jacking, um die Kontrolle über Dorseys Telefonnummer zu erlangen, und verwendete dann einen von Twitter übernommenen Text-to-Tweet-Dienst, um die Nachrichten zu veröffentlichen. Obwohl die Nachrichten weniger als zehn Minuten lang online sichtbar waren, wurden Millionen von Menschen den beleidigenden Tweets ausgesetzt.



### Was Sie wissen müssen:

SIM-Jacking (auch bekannt als SIM-Swap-Scam, Port-out-Betrug, SIM-Splitting oder SIM-Swapping) ist eine Art der Account-Übernahme, die in der Regel eine Schwachstelle bei der Zwei-Faktor-Authentifizierung und der zweistufigen Verifizierung ausnutzt, wobei der zweite Faktor eine Textnachricht (SMS) oder ein Anruf an ein Mobiltelefon ist. Einfach ausgedrückt bedeutet SIM-Jacking, dass sich ein Angreifer beim Mobilfunkanbieter als die Zielperson ausgibt und deren Handynummer stiehlt, indem er sie auf eine andere SIM-Karte übertragen lässt, die sich bereits in seinem Besitz befindet.

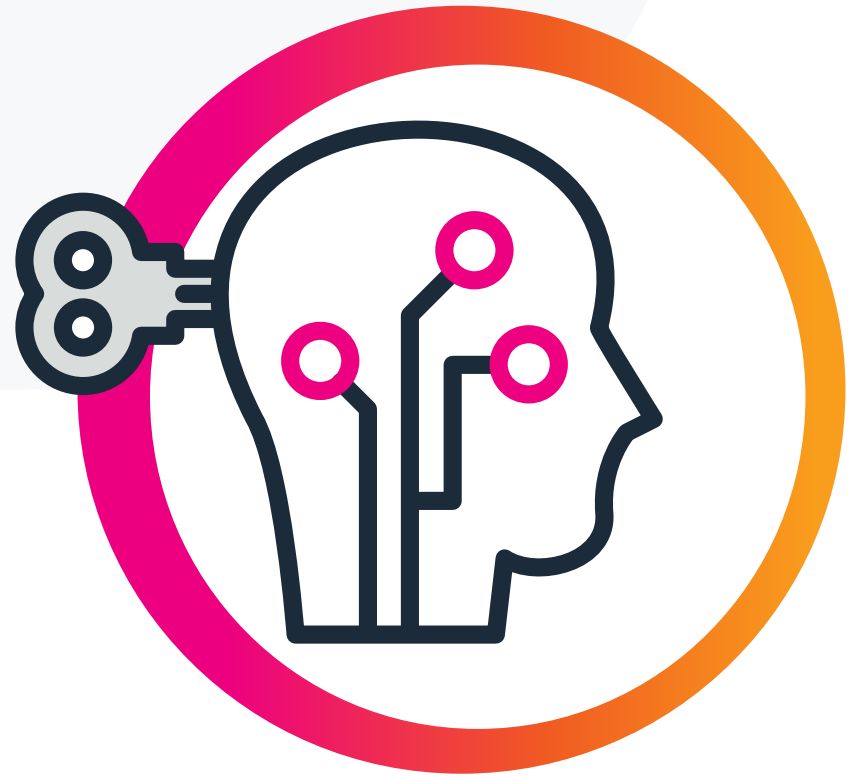
### Wie der Angriff funktioniert:

Ein Hacker ruft bei der Support-Hotline des Mobilfunkanbieters an, gibt sich als die Zielperson aus und behauptet, er habe seine SIM-Karte verloren. Der Angreifer kann die Identität der Zielperson nachweisen, da er durch einen der vielen Datenbank-Hacks der letzten zehn Jahre in den Besitz einiger personenbezogener Daten (Adresse, Passwörter oder Sozialversicherungsnummer) gelangt ist. Der Mitarbeiter des Serviceanbieters kann nicht wissen, dass es sich bei dem Anrufer nicht wirklich um die Zielperson handelt, und nimmt die Umstellung vor. Und damit wird diese Telefonnummer – die normalerweise der Schlüssel zu einem Großteil des digitalen Lebens ist – nun plötzlich von einer anderen Person kontrolliert.

### Woher der Angriff erfolgt:

SIM-Jacker versuchen in der Regel, etwas Wertvolles von ihren Opfern zu erpressen – wie Bitcoin- oder andere Kryptowährungs-Wallets oder wertvolle Social Media-Konten – oder ihren Ruf zu beschädigen, wie Chuckling Squad bei Jack Dorsey. Diese Hacker können von überall auf der Welt kommen und Mitglieder von organisierten Banden oder Einzelpersonen sein.

# Social-Engineering-Angriff



Im Juli 2022 verlor CoinsPaid, ein Zahlungssystem für Kryptowährungen, durch einen Social-Engineering-Angriff **37 Millionen US-Dollar**. Die Bedrohungsakteure machten einem Mitarbeiter ein vorgebliches Jobangebot und brachten ihn dazu, Schadsoftware auf seinem Firmenrechner zu installieren. „Man möchte zwar meinen, dass ein solcher Versuch, Schadsoftware auf dem Computer eines Mitarbeiters zu installieren, doch allzu offensichtlich ist“, notiert das geschädigte Unternehmen. „Aber die Hacker hatten ganze sechs Monate darauf verwendet, alle möglichen Einzelheiten über CoinsPaid, unsere Teammitglieder, unsere Unternehmensstruktur usw. in Erfahrung zu bringen.“



### Was Sie wissen müssen:

Social Engineering ist der Sammelbegriff für ein breites Spektrum an schädlichen Aktivitäten, die auf psychologische Manipulation setzen, um Benutzer dazu zu bringen, Sicherheitsfehler zu begehen oder sensible Informationen preiszugeben. Was Social Engineering besonders gefährlich macht, ist die Tatsache, dass es auf menschlichem Versagen beruht und nicht auf Schwachstellen in Software und Betriebssystemen. Fehler, die von legitimen Benutzern begangen werden, sind viel weniger vorhersehbar und daher schwieriger zu erkennen und zu vereiteln als ein auf Malware basierender Angriff.

### Wie der Angriff funktioniert:

Social-Engineering-Angriffe gibt es in vielen verschiedenen Formen. Sie können überall dort erfolgen, wo menschliche Interaktion Teil eines Prozesses ist. Im Folgenden stellen wir Ihnen die fünf häufigsten Formen digitaler Social-Engineering-Angriffe vor. Ein Täter spioniert das anvisierte Opfer zunächst aus, um die für den Angriff erforderlichen Hintergrundinformationen zu erhalten, wie etwa potenzielle Einstiegspunkte und schwache Sicherheitsprotokolle. Dann gewinnt der Angreifer das Vertrauen des Opfers und liefert Anreize für nachfolgende Handlungen, die gegen Sicherheitspraktiken verstoßen, z. B. sensible Informationen preiszugeben oder Zugriff auf wichtige Ressourcen zu gewähren.

### Woher der Angriff erfolgt:

Social Engineering kann viele Formen haben, aus verschiedensten Richtungen kommen und unterschiedlich motiviert sein. Am häufigsten erfolgen Social-Engineering-Angriffe in Form von Phishing-E-Mails. Andere Formen sind das „Pretexting“, bei dem der Angreifer einen guten Vorwand schafft, um wichtige Daten zu stehlen; das „Baiting“ bzw. „quid pro quo“, bei dem der Angreifer dem Opfer etwas Begehrtes im Austausch für die Herausgabe von Zugangsdaten anbietet; und der als „Tailgating“ oder „Piggybacking“ bezeichnete Miteintritt, bei dem ein Angreifer Zugang zu einem geschlossenen Bereich eines Unternehmens erhält, indem er einem authentifizierten Mitarbeiter durch gesicherte Türen folgt.

# Spear Phishing



Heutzutage haben es Spear Phisher nicht nur auf die großen Fische abgesehen, sondern machen sich auch Praktiken aus dem Bereich der Romance Scams zunutze: Sie verleiten ihre Opfer nämlich mit attraktiven gefälschten Profilen dazu, Malware auf ihre Computer herunterzuladen. Ein Beispiel ist der jahrelange, gezielte Social-Engineering- und Malware-Angriff, der auf die bekannte Hackergruppe TA456 zurückgeht, der Verbindungen zum iranischen Staat nachgesagt werden. Mit dem gefälschten Social Media-Profil „Marcella Flores“ **baute TA456 eine romantische Beziehung** zu einem Mitarbeiter einer kleinen Tochtergesellschaft eines Rüstungsunternehmens im Luft- und Raumfahrtsektor auf. Einige Monate später nutzten die Hacker diese Beziehung aus, indem sie eine große Malware-Datei über eine laufende E-Mail-Kommunikationskette des Unternehmens verschickte, mit der sie das Unternehmen ausspähen wollten. Sobald die Malware, LEMPO genannt, den Computer infiziert hatte, exfiltrierte sie Daten und schickte hochsensible Informationen an die Angreifer, während sie gleichzeitig ihre Spuren verwischte, um nicht entdeckt zu werden.



### Was Sie wissen müssen:

Spear Phishing ist eine Unterart des Phishing, bei der Cyberkriminelle Zielpersonen in einer speziellen, personalisierten E-Mail-Nachricht gezielt ansprechen, um Sie oder Ihre Mitarbeiter dazu zu bringen, finanzielle oder geschützte Daten preiszugeben oder den Zugriff auf das Netzwerk freizugeben. Spear Phisher haben es auf Personen abgesehen, die entweder Zugriff auf sensible Informationen haben oder eine Schwachstelle in dem Zielnetzwerk darstellen. Hochrangige Zielpersonen, wie z. B. Führungskräfte, Vorstandsmitglieder oder Administratoren sind besonders gefährdet, da sie Zugriff auf wichtige Systeme und geschützte Informationen eines Unternehmens haben.

### Wie der Angriff funktioniert:

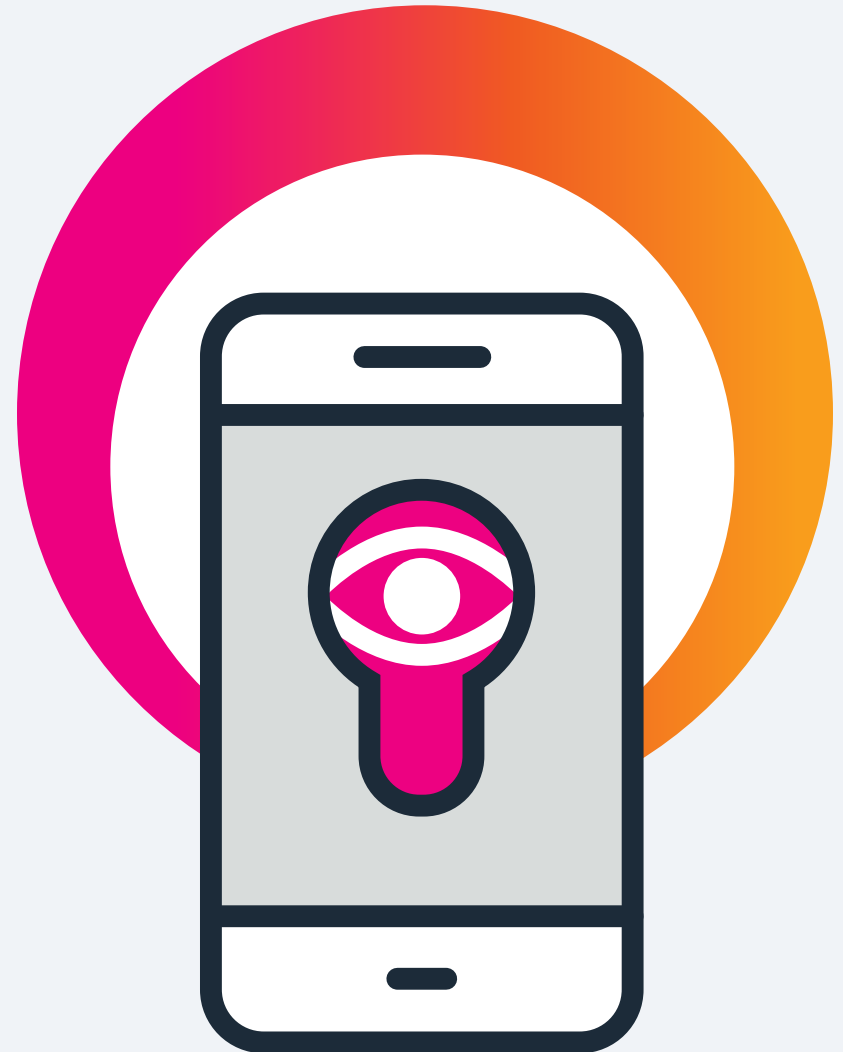
Spear Phisher recherchieren auf Social Media-Seiten wie LinkedIn, um ihre Zielpersonen und deren berufliche Positionen zu identifizieren. Anschließend fälschen sie Adressen, um hochgradig personalisierte, authentisch aussehende Nachrichten zu versenden, mit denen die Infrastruktur und Systeme ihrer Zielpersonen infiltriert werden sollen. Sobald die Hacker Zugriff auf die Umgebung haben, versuchen sie, noch weiter gehende Pläne umzusetzen.

### Woher der Angriff erfolgt:

Hinter dieser Art von Angriff können sowohl Einzelpersonen als auch Organisationen stehen. Viele hochkarätige Spear Phishing-Versuche gehen auf staatlich finanzierte kriminelle Cyberbanden zurück, die über die erforderlichen Ressourcen verfügen, Zielpersonen auszuspionieren und strenge Sicherheitsfilter zu umgehen.

# Spyware

Es ist kein Geheimnis, dass Spyware-Angriffe weiterhin erschreckend oft auftreten. Aber wenn Sie eine hochgestellte Persönlichkeit sind, ist Ihr Risiko dafür wahrscheinlich größer. So wurden die Mobiltelefone des spanischen Premierministers Pedro Sánchez und der Verteidigungsministerin Margarita Robles [Ziel mehrerer Angriffe mit der Spyware Pegasus](#), die zu einem erheblichen Datendiebstahl von beiden Geräten führten und gleichzeitig Schäden in den spanischen Verwaltungs- und Regierungssystemen anrichteten.





### Was Sie wissen müssen:

Spyware ist eine Art von Malware, die darauf abzielt, personenbezogene Daten oder vertrauliche Daten einer Organisation zu sammeln, Webaktivitäten (wie etwa Suchvorgänge, Verlauf und Downloads) einer Zielperson zu verfolgen oder zu verkaufen, ihre Bankkontodaten zu erfassen oder gar ihre Identität zu stehlen. Es gibt viele Arten von Spyware und jede von ihnen verwendet eine einzigartige Taktik, um die Zielperson auszuspähen. Letztlich kann Spyware ein Gerät übernehmen und Daten exfiltrieren oder personenbezogene Daten ohne vorherige Zustimmung oder Kenntnis an eine unbekannte externe Partei senden.

### Wie der Angriff funktioniert:

Spyware kann sich auf verschiedene Weise auf dem Gerät einer Zielperson installieren, fasst aber in der Regel Fuß in einem System, indem sie den Benutzer täuscht oder vorhandene Schwachstellen ausnutzt. Dies kann passieren, wenn ein Benutzer unvorsichtigerweise einer plötzlich erscheinenden Aufforderung oder einem Pop-up-Fenster zustimmt, Software oder Upgrades von einer nicht zuverlässigen Quelle herunterlädt, E-Mail-Anhänge von unbekannten Absendern öffnet oder Filme und Musik von illegalen Sites streamt.

### Woher der Angriff erfolgt:

Dank inzwischen leicht erhältlicher Crimeware-Kits kann diese Art von Angriff von jeder Person und jedem Ort ausgeführt werden. In den meisten Fällen stammt Spyware jedoch von böswilligen Organisationen, die die Daten ihrer Opfer an Dritte verkaufen möchten.

# SQL Injection

Structured Query Language (SQL) ist die Standardprogrammiersprache, die für die Kommunikation mit relationalen Datenbanken – Systeme, die jede datengetriebene Website und Anwendung im Internet unterstützen – verwendet wird. Ein Angreifer kann sich dieses (weit verbreitete) System zunutze machen, indem er eine bestimmte SQL-Abfrage in das Formular eingibt (und sie in die Datenbank einspeist), woraufhin der Hacker auf die Datenbank, das Netzwerk und die Server zugreifen kann. Und SQL Injection-Angriffe sind weiterhin als Angriffsmethode beliebt. Erst [im August 2020 gab das Unternehmen Freepik eine Datenschutzverletzung bekannt](#), die die Zugangsdaten von mehr als acht Millionen Benutzern betraf und durch eine SQL Injection in eine globale Datenbank mit anpassbaren Symbolen entstand, die es den Übeltätern ermöglichte, die Anmeldedaten und personenbezogene Informationen der Benutzer zu stehlen.





### Was Sie wissen müssen:

SQL Injection ist eine Art von Injektionsangriff, bei dem Datenbanken mit schädlichen SQL-Statements manipuliert oder zerstört werden. SQL-Statements steuern die Datenbank Ihrer Webanwendung und können zur Umgehung von Sicherheitsmaßnahmen verwendet werden, wenn die Benutzereingaben nicht ordnungsgemäß bereinigt werden.

### Wie der Angriff funktioniert:

Bei einem SQL-Injection-Angriff wird eine SQL-Abfrage über die Eingabedaten vom Client in die Anwendung eingeschleust oder „injiziert“. Ein erfolgreicher SQL-Injection-Exploit kann sensible Daten aus der Datenbank auslesen, Datenbankdaten ändern, Verwaltungsoperationen in der Datenbank ausführen, den Inhalt einer bestimmten Datei im DBMS-Dateisystem wiederherstellen und in manchen Fällen Befehle an das Betriebssystem senden.

### Woher der Angriff erfolgt:

Da das Internet zu einem großen Teil auf relationalen Datenbanken basiert, sind SQL-Injection-Angriffe sehr häufig. Wenn man in der Datenbank „[Common Vulnerabilities and Exposures](#)“ nach „injection“ sucht, erhält man 15.000 Ergebnisse.

# Typo-squatting

Noblox.js ist ein Wrapper für die Roblox-API, die von vielen Gamern genutzt wird, um Interaktionen mit der beliebten Gaming-Plattform Roblox zu automatisieren. Die Software scheint aber auch für andere attraktiv zu sein. 2021 starteten Hacker [Typosquatting-Angriffe über das noblox.js-Paket](#), indem sie verwirrend ähnliche, mit Ransomware bestückte Pakete in eine Registry für Open-Source JavaScript-Bibliotheken hochluden und die infizierten Dateien dann über einen Chat-Dienst verbreiteten. Seit September 2021 gehen Josh Muir und andere Gamer aktiv gegen die Angreifer vor und versuchen, die Verbreitung von Ransomware durch das noblox.js-Paket und andere Code-Bibliotheken zu verhindern und weitere Angriffe auf die Gaming-Community zu vereiteln.





### Was Sie wissen müssen:

Typosquatting ist ein Phishing-Angriff, bei dem sich Angreifer häufig falsch geschriebene Domain-Namen zunutze machen. Oftmals möchten die Täter gar keinen Angriff ausführen, sondern hoffen, dass ein Unternehmen, eine Marke oder eine Person ihnen die Domain abkauft. In anderen Fällen erstellen die Diebe schädliche Domains, die denen legitimer Marken zum Verwechseln ähnlich sind.

### Wie der Angriff funktioniert:

Hierbei handelt es sich nicht um einen ausgeklügelten Angriff. Typosquatting kann z. B. auch einfach von einem 14-Jährigen begangen werden, der eine Domain registriert und dort anschließend schädlichen Code installiert. Bei der bösartigen Form dieses Angriffs verwendet ein Hacker in der Regel gefälschte Domains, um Benutzer zur Interaktion mit einer schädlichen Infrastruktur zu verleiten.

Selbst wenn die Benutzer ausführlich über diese Risiken aufgeklärt werden, lässt sich menschliches Versagen nie ganz ausschließen. Dieser Tatsache sind sich die meisten Angreifer nur allzu bewusst und sie nutzen sie gerne aus – z. B. beim Phishing mit ähnlichen Adressen, dem Einbetten von gefälschten Command & Control-Domains in Malware und dem Hosten schädlicher Inhalte auf Domains, die Unternehmensservern sehr ähnlich sind.

### Woher der Angriff erfolgt:

Die Ursprünge dieser Art von Angriff sind nicht so wichtig wie das Ziel. Dieser Angriff zielt in der Regel auf unbedachte Internetnutzer ab, die nicht bemerken, dass die URL ihrer Lieblingsdomain um einen oder zwei Buchstaben geändert wurde. Und da dieser Angriffstyp so einfach ist (er kann z. B. einfach über die Registrierung eines Domain-Namens erfolgen), kann er von fast jedem Ort der Welt ausgehen.

# Verdächtige Cloud-Speicheraktivitäten



Laut dem [Verizon Data Breach Investigations Report](#) (DBIR) aus dem Jahr 2022 ist bei erstaunlichen 82 % der Datenschutzverletzungen der „Faktor Mensch“ beteiligt, wobei „verschiedene Fehler“ aufgrund von falsch konfiguriertem Cloud-Speicher zunehmen. Darüber hinaus ergab der Bericht „[Sensitive Data in the Cloud](#)“, dass die Mehrheit der Sicherheits- und IT-Experten (67 %) sensible Daten in öffentlichen Cloud-Umgebungen speichert, wobei ein Drittel der Befragten angab, dass sie kein oder nur wenig Vertrauen in ihre Fähigkeiten haben, sensible Daten in der Cloud zu schützen.

Genau diese Art von technischen und professionellen Schwachstellen – sei es durch eine falsch konfigurierte Datenbank oder Sicherheitsteams, denen das nötige Know-how fehlt – sind der Grund, warum Cloud-Accounts im Zeitalter der Remote-Arbeit zu einem der Hauptziele für Cyberangriffe geworden sind.



## Was Sie wissen müssen:

Da die Daten heute weit (und allzu oft willkürlich) über die Cloud verteilt sind, haben Angreifer reichlich Gelegenheit, bekannte und unbekannte Schwachstellen zu finden und auszunutzen. Dies ist ganz besonders der Fall, wenn Unternehmen überstürzt in die Cloud migrieren, und bestimmte Sicherheitskontrollen dabei möglicherweise kompromittiert oder falsch konfiguriert werden.

Erschwerend kommt hinzu, dass Ressourcen und Anwendungen nach dem [Modell der geteilten Verantwortung](#) gesichert werden müssen, bei dem Cloud-Serviceanbieter (CSPs) den Schutz für bestimmte Elemente, Prozesse und Funktionen übernehmen, der Kunde aber gemäß der [Cloud Security Alliance](#) (CSA) für die Sicherheit seiner eigenen Daten, seines Codes und anderer wichtiger Ressourcen zuständig ist. Wird diese Aufgabe jedoch nicht in ausreichendem Maß erfüllt, ruft dies unweigerlich Hacker auf den Plan.

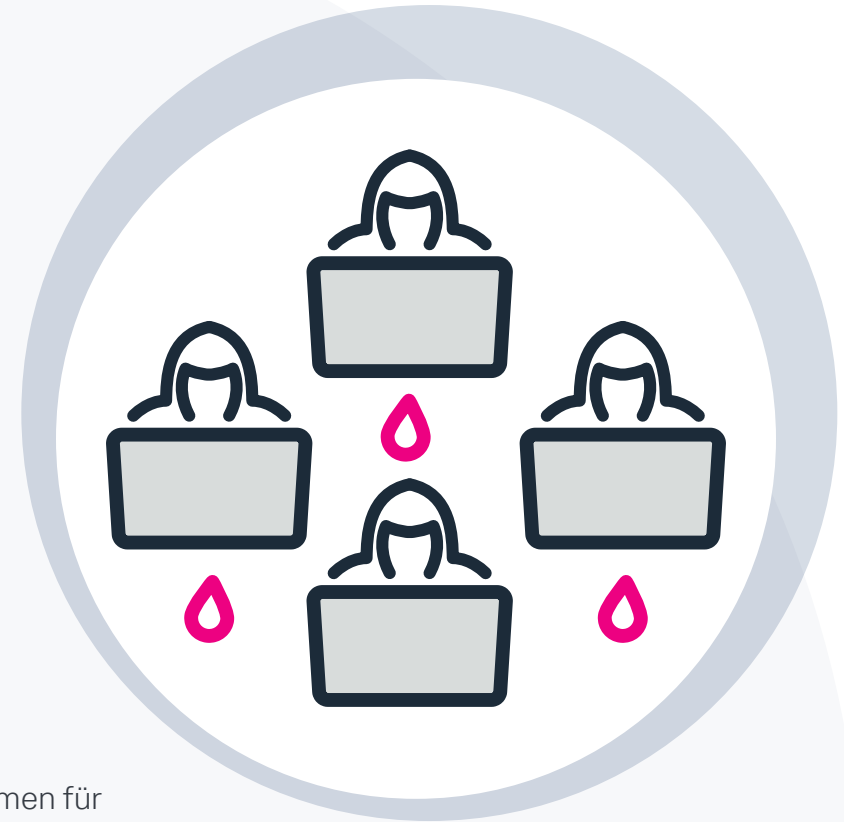
## Wie der Angriff funktioniert:

Ein Angriff auf den Cloud-Speicher kann erfolgen, wenn ein Angreifer durch falsche, laxe oder nicht vorhandene Sicherheitseinstellungen in der Cloud-Infrastruktur des Unternehmens Fuß fasst. Wenn das System erst einmal infiltriert ist, deaktivieren die Angreifer bestimmte Kontrollen, wie etwa das Zugriffs-Monitoring. Sie legen eventuell neue Accounts an, um sich den weiteren Zugang zu sichern, und führen gleichzeitig Befehle aus, die für den betreffenden Benutzer oder das System nicht typisch sind. Sie könnten auch die Richtlinien für bestimmte Storage Buckets ändern, sodass die Dateien eines Unternehmens öffentlich zugänglich sind und Daten exfiltriert werden können. Glücklicherweise sind dies alles relevante Ereignisse, die in den Auditlogs des Cloud-Serviceanbieters protokolliert werden.

## Woher der Angriff erfolgt:

Zu verdächtigen Cloud-Speicheraktivitäten kann es z. B. kommen, wenn ein Entwickler eine veraltete Instanz einer Cloud-Funktion oder -Anwendung ausführt. Diese könnte bekannte Sicherheitslücken enthalten, die in einer späteren Version gepatcht wurden. Da jedoch eine ältere Programmversion ausgeführt wird, können Angreifer dies als Einstiegspunkt nutzen, bevor sie sich lateral in der Cloud-Umgebung bewegen.

# Watering-Hole-Angriff



Im Rahmen eines klassischen Watering-Hole-Angriffs hat ein Unternehmen für Wasser- und Abwasseraufbereitungsanlagen in Florida [unwissentlich böartigen Code auf seiner Website gehostet](#), was 2021 dann zu dem [Hack des Wasserwerks Oldsmar](#) führte. Die Cyberkriminellen, die hinter dem Angriff steckten, hatten offensichtlich eine bestimmte Zielgruppe im Visier: Der Schadcode, der auf der Website des Unternehmens gefunden wurde, schien auch auf andere Wasserversorgungsunternehmen in Florida abzielen und wurde genau am Tag des Hacks von einem Browser aufgerufen, dessen Ursprung in das Städtchen Oldsmar zurückverfolgt werden konnte. Die Website startete zwar keinen Exploit-Code, injizierte aber Malware, die als Browserauflistungs- und Fingerprinting-Skript fungierte, um Informationen von Website-Besuchern zu sammeln, wie etwa Betriebssystem, Browsertyp, Zeitzone sowie Angaben zu Kamera und Mikrofon, die dann an eine Remote-Datenbank gesendet wurden, die auf der Website einer Heroku-App gehostet wurde, auf der auch das Skript gespeichert war.



### Was Sie wissen müssen:

Bei einem Watering-Hole-Angriff wird der Computer des Benutzers durch den Besuch einer infizierten Website mit Malware kompromittiert, die darauf abzielt, das Netzwerk zu infiltrieren und Daten oder finanzielle Vermögenswerte zu stehlen. Bei der eingesetzten Technik handelt es sich im Grunde genommen um einen Zero-Day-Angriff mit dem Ziel, das Computersystem zu infizieren, um sich Zugriff auf das Netzwerk zu verschaffen und so finanzielle Vorteile oder geschützte Informationen zu erlangen.

### Wie der Angriff funktioniert:

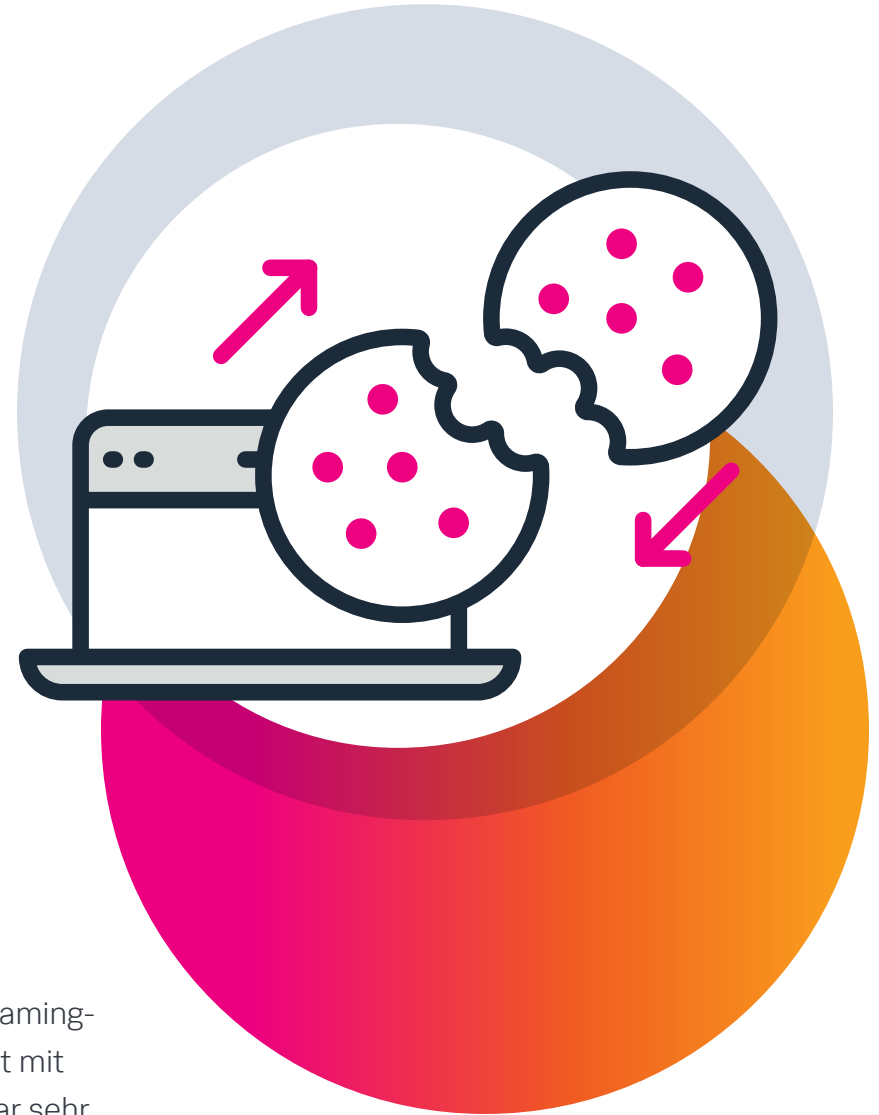
Zunächst erstellen die Angreifer ein Profil ihrer Zielperson, um festzustellen, welche Websites sie häufig besucht, und suchen anschließend nach Schwachstellen, die sie ausnutzen können. Durch die Ausnutzung dieser Schwachstellen kompromittiert der Angreifer diese Websites und wartet dann in dem Wissen ab, dass es nur eine Frage der Zeit ist, bis der betreffende Benutzer sie besucht. Die kompromittierte Website infiziert wiederum das Netzwerk der Zielperson, sodass die Angreifer in das System eindringen und von dort aus auf andere Systeme zugreifen können.

### Woher der Angriff erfolgt:

Zwar können diese Angriffe von jedem Ort der Welt ausgehen, viele der Cyberkriminellen, die hinter diesem Angriff stecken, stammen jedoch aus Ländern, in denen organisierte Hackergruppen derzeit florieren, wie z. B. Russland und China. Im Jahr 2018 wurde ein Watering-Hole-Angriff auf Länderebene der chinesischen Bedrohungsgruppe „LuckyMouse“ (auch bekannt als „Iron Tiger“, „EmissaryPanda“, „APT27“ und „[Threat Group 3390](#)“) zugeordnet, die dafür bekannt ist, dass sie mit zahlreichen Arten von Angriffen, darunter auch Watering-Hole-Angriffen, auf Regierungen, den Energiesektor und die Fertigungsindustrie abzielt.

# Web Session Cookie- Diebstahl

Fast jede von uns genutzte Webanwendung, von Social Media- und Streaming-Plattformen bis hin zu Cloud-Diensten und Finanzanwendungen, arbeitet mit Authentifizierungs-Cookies. Cookies machen das Surfen im Internet zwar sehr viel bequemer, sie stellen jedoch auch eine Schwachstelle dar, die mit großem Erfolg ausgenutzt werden kann. Ende 2019 machte sich ein lose verbundener Kreis von Hackern einen Namen: Sie führten Malware aus, [die Cookies stahl, um verschiedene YouTube-Kanäle zu kapern](#), und köderten dann nichts ahnende Besitzer mit gefälschten Angeboten, um sie für Kryptowährungsbetrug zu missbrauchen oder die Accounts an den Höchstbietenden zu verkaufen.





### Was Sie wissen müssen:

Wenn ein Angreifer erfolgreich ein Session Cookie stiehlt, kann er alle Aktionen durchführen, zu denen der ursprüngliche Benutzer berechtigt ist. Eine Gefahr für Unternehmen besteht darin, dass Cookies zur Identifizierung authentifizierter Benutzer in Single-Sign-on-Systemen verwendet werden können, wodurch der Angreifer möglicherweise Zugriff auf alle Webanwendungen erhält, die das Opfer nutzen kann, wie Finanzsysteme, Kundendatensätze oder Branchensysteme, die möglicherweise vertrauliches geistiges Eigentum enthalten.

### Wie der Angriff funktioniert:

Nachdem ein Nutzer auf einen Dienst zugegriffen und seine Identität bestätigt hat, wird ein Cookie für einen längeren Zeitraum auf seinem Rechner gespeichert, damit er sich nicht jedes Mal neu anmelden muss. Hacker können Session Cookies mithilfe von Malware stehlen und das Cookie in einen von ihnen kontrollierten Browser importieren, sodass sie die Website oder Anwendung nutzen können, solange das Session Cookie aktiv ist. Ist er einmal auf der Website angemeldet, kann ein Angreifer auf sensible Daten zugreifen, E-Mails lesen oder Aktionen durchführen, für die das Konto des Opfers eine Berechtigung besitzt.

### Woher der Angriff erfolgt:

Cookie-Diebstahl erfolgt in der Regel durch Malware, die die Cookies des Opfers kopiert und direkt an den Angreifer sendet. Die Malware kann auf verschiedene, in diesem Handbuch behandelte Arten auf dem Computer des Opfers landen, z. B. durch Phishing, Makroviren, Cross-Site-Scripting und mehr. Viele Hacker, die Cookies stehlen, gehören zu größeren Netzwerken, die von Russland oder China aus operieren. Die Hintermänner des YouTube-Angriffs gehörten z. B. zu einer Gruppe von Hackern, die über ein russischsprachiges Forum verbunden waren.

# Whale Phishing (Whaling)



Warum kleine Fische „phishen“, wenn man auch Wale fangen kann? Der australische Hedgefonds Levitas Capital musste dies am eigenen Leib erfahren, als Angreifer einen **heimlichen Whaling-Angriff** starteten, der direkt auf einen der Gründer abzielte. Die Angreifer verschafften sich Zugang zum Netzwerk des Hedgefonds, indem sie dem Vorstandsmitglied einen gefälschten Zoom-Link schickten, der beim Anklicken Malware installierte. Der schädliche Code ermöglichte es den Hackern, das E-Mail-Konto der Zielperson zu infiltrieren und anschließend gefälschte Rechnungen an den Treuhänder und den externen Verwalter des Fonds zu senden, die daraufhin Bargeldtransfers in Höhe von 8,7 Millionen US-Dollar an die Angreifer veranlassten und genehmigten. Die gefälschten Rechnungen enthielten auch eine Aufforderung zur Zahlung von 1,2 Millionen US-Dollar an die verdächtige Privatkapitalgesellschaft Unique Star Trading. Das enorme Ausmaß der Verluste zwang das Unternehmen schließlich zur Geschäftsaufgabe.



### Was Sie wissen müssen:

Whaling bedeutet, dass Hacker ein einzelnes, hochrangiges Ziel, wie etwa einen CEO eines Finanzdienstleisters, ins Visier nehmen. Das Ziel ist dabei immer eine bestimmte Person, wohingegen eine einfache Phishing-E-Mail auf jeden Mitarbeiter eines Unternehmens abzielen kann. Die Hacker haben es in der Regel deswegen auf hochrangige Zielpersonen abgesehen, da diese möglicherweise über wichtige oder sensible Informationen verfügen.

### Wie der Angriff funktioniert:

Die bei einem Whaling-Angriff verwendete Technik ist das klassische Phishing. Die Zielperson erhält eine authentisch aussehende E-Mail, in der sie in der Regel aufgefordert wird, auf einen Link zu klicken, der schädlichen Code enthält oder zu einer Website führt, auf der vertrauliche Informationen, wie z. B. ein Passwort, abgefragt werden.

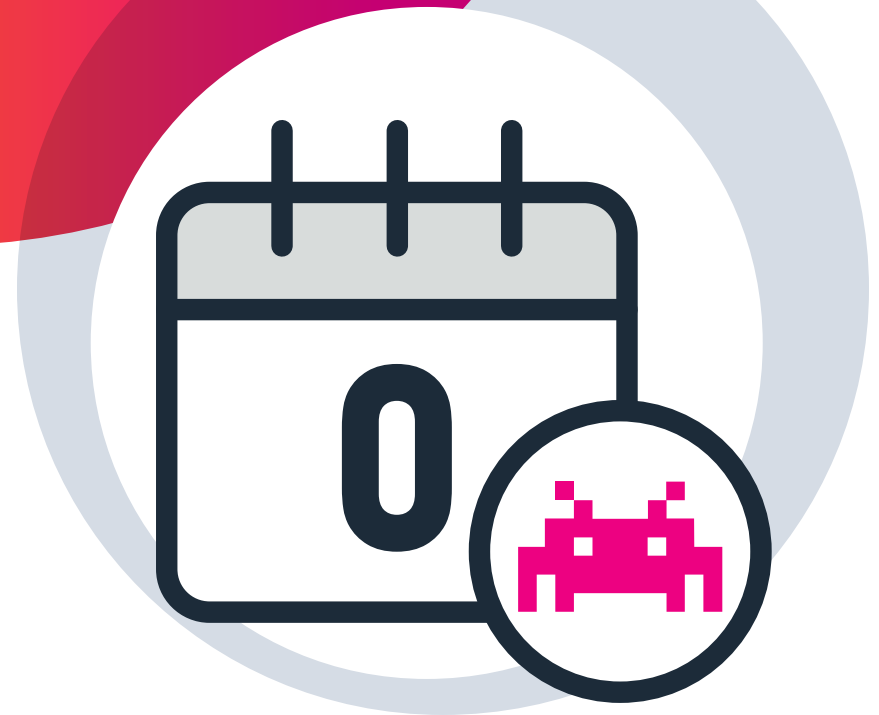
### Woher der Angriff erfolgt:

Phishing ist der häufigste Einstiegspunkt für einen Cyberangriff, was bedeutet, dass ein Whaling-Angriff von jedem Ort der Welt ausgehen kann.

Der Angriff auf Levitas Capital wurde z. B. von einer Gruppe von Cyberkriminellen aus verschiedenen Regionen ausgeführt, wobei die Zahlungen an die Bank of China und die United Overseas Bank in Singapur gingen.

# Zero-Day-Exploit

Es ist kaum verwunderlich, dass die Zahl der Zero-Day-Schwachstellen immer weiter zunimmt. Das Jahr 2021 war jedoch bis jetzt mit Abstand das schlimmste, da Angreifer **insgesamt 58 neue Zero-Day-Bedrohungen** ausnutzten, gegenüber 25 Schwachstellen im Jahr 2020 und 21 im Jahr 2019. Und mit der zunehmenden Vernetzung kritischer Systeme steht auch zweifellos immer mehr auf dem Spiel. In den letzten Jahren haben Hacker Zero-Day-Angriffe genutzt, um Microsoft-Server zu kompromittieren und hoch entwickelte Spyware auf Smartphones zu installieren, mit der sie Journalisten, Politiker und Menschenrechtsaktivisten ausspionieren konnten.





### Was Sie wissen müssen:

Eine Zero-Day-Schwachstelle ist im Kern eine Sicherheitslücke. Dabei handelt es sich um eine Schwachstelle in einer Software oder einem Computernetzwerk, die Hacker kurz (oder sofort) nach der allgemeinen Verfügbarkeit oder Veröffentlichung des Produkts ausnutzen – der Begriff „Zero“ bezieht sich auf das Zeitfenster des ersten Tages, an dem diese Schwachstellen ausgenutzt werden.

### Wie der Angriff funktioniert:

Die Art der Schwachstelle hat Einfluss darauf, wie der Angriff durchgeführt wird. Zero-Day-Angriffe folgen jedoch einem bestimmten Muster. Zunächst prüft der Hacker (oder die Hackergruppe) den Code auf Schwachstellen. Sobald sie eine Schwachstelle gefunden haben, erstellen sie einen eigenen Code, der diese Schwachstelle ausnutzt. Sie infiltrieren das System (mit einer oder mehreren der in diesem Handbuch beschriebenen Methoden), infizieren es mit ihrem schädlichen Code und starten dann den Exploit.

### Woher der Angriff erfolgt:

Die heutige Verbreitung von Technologie hat zu einer explosionsartigen Zunahme von Zero-Day-Angriffen geführt. Diese Angriffe können zwar von überall aus gestartet werden, doch sie werden oft über Nationalstaaten oder Regionen mit ausgedehnten cyberkriminellen Netzen und Infrastrukturen verbreitet.

# Erfahren Sie mehr.

Entdecken Sie, wie Ihr Unternehmen unzählige Bedrohungen abwehren kann und wie Sie **mit analysegestützter Security** von Splunk **Ihr SOC modernisieren**.

Splunk, Splunk> und Turn Data Into Doing sind Marken und eingetragene Marken von Splunk Inc. in den Vereinigten Staaten und anderen Ländern. Alle anderen Markennamen, Produktnamen oder Marken gehören den entsprechenden Inhabern.  
© 2023 Splunk Inc. Alle Rechte vorbehalten.

23-337536-Splunk-Top 50 Cybersecurity Threats-EB-110\_GER

**splunk>**