MYRA

CYBERSECURITY REPORT H1 2024:

KRITISche Prozesse im Fokus

In Zusammenarbeit mit:

zeroBS

Vorwort

In Zeiten zunehmender geopolitischer Spannungen erfährt die Cybersicherheit eine immer stärkere Bedeutung für das gesellschaftliche Wohl. Im Jahr 2024 warten neue Herausforderungen und Risiken, aber auch Chancen auf Unternehmen, öffentliche Einrichtungen und Einzelpersonen gleichermaßen.

Der Hacktivismus erlebt einen besorgniserregenden Aufschwung, angetrieben durch weltweite Konflikte und soziale Krisen. Politisch motivierte Gruppierungen nutzen vermehrt Cyberattacken als Werkzeug, um ihre Ziele und Forderungen durchzusetzen. Parallel hierzu beobachten wir eine fortschreitende Professionalisierung von Angriffsmethoden und -technologien. Cyberkriminelle setzen immer ausgefeiltere Techniken ein, um Schwachstellen in Systemen und Netzwerken auszunutzen.

Der anhaltende Trend zu „Cybercrime as a Service" ist besonders alarmierend. Diese Form der Cyberkriminalität zielt auf eine unmittelbare Monetarisierung von Angriffen ab, indem diese über Darknet-Foren als Dienstleistung angeboten werden. Hierdurch erhält ein breites Publikum krimineller Akteure Zugang zu Cyberattacken. Mit gezielten Angriffen auf Behörden und andere öffentliche Einrichtungen oder die Politik selbst verfolgen Cyberkriminelle das Ziel, für Unsicherheit in der öffentlichen Wahrnehmung zu sorgen.

Im Superwahljahr 2024 könnte dies weitreichende Folgen für demokratische Prozesse haben.

Künstliche Intelligenz (KI) spielt abseits des aktuellen Hypes um die Technologie eine ambivalente Rolle in der Cybersicherheit. Einerseits ermöglicht KI verbesserte Abwehrmaßnahmen und automatisierte Sicherheitsprozesse. Andererseits eröffnet sie Cyberkriminellen neue Möglichkeiten für noch raffiniertere Angriffe.

Angesichts dieser Entwicklungen sehen sich Unternehmen und öffentliche Einrichtungen mit enormen Herausforderungen konfrontiert. Die Umsetzung neuer Regulierungen wie der NIS-2-Richtlinie und die anhaltenden Diskussionen um Datenschutz und grenzüberschreitende Datenübertragungen erhöhen den Druck zusätzlich.

Im vorliegenden Report von Myra erhalten IT-Entscheidende einen umfassenden Überblick über die aktuellen Trends und Herausforderungen im Bereich der Cybersicherheit – mit einem besonderen Fokus auf die Risiken von schädlichem Traffic. Damit wollen wir aufzeigen, wie Organisationen ihre Abwehrstrategien stärken können, um den vielfältigen Bedrohungen zu begegnen.

Inhalt

Executive Summary

DDoS-Bedrohungslage und Angriffstrends

Die Zahl schädlicher Webanfragen ist im ersten Halbjahr 2024 um 53,2 Prozent im Vergleich zum Vorjahreszeitraum gestiegen.

Neue Angriffstechniken wie „HTTP/2 Continuation Flood“ stellen eine erhöhte Bedrohung dar.

Öffentliche Verwaltungen und kritische Infrastrukturen (KRITIS) sind europaweit verstärkt Ziel von Cyberangriffen. Im Jahresvergleich stieg die Zahl der Angriffe in der EU um 31 Prozent.

Angriffe auf Webseiten, Webapplikationen und APIs bereiten Unternehmen aufgrund steigender technischer Komplexität die größten Schwierigkeiten bei der Abwehr.

Künstliche Intelligenz in der Cybersicherheit

Künstliche Intelligenz (KI) spielt eine ambivalente Rolle in der Cybersicherheit. Sie bietet erhebliche Chancen zur Verbesserung der Sicherheitsmaßnahmen, birgt jedoch auch Risiken, da sie gleichermaßen von Cyberkriminellen genutzt werden kann. KI-basierte Angriffe bereiten vielen Unternehmen Sorgen, während gleichzeitig KI-Systeme zur automatisierten Identifikation von Anomalien und Echtzeit-Monitoring eingesetzt werden.

Cybervorfälle
sind **Risikofaktor Nr. 1**

Allianz Risk Barometer 2024

Wirtschaftliche Belastung: 148 Milliarden Euro Schaden

Die Professionalisierung von Cyberkriminellen und der zunehmende Einsatz von Cybercrime-as-a-Service-Plattformen verschärfen die Bedrohungslage zusehends. Die Kosten durch Cyberkriminalität sind enorm, mit geschätzten 148 Milliarden Euro jährlich für die deutsche Wirtschaft und 8,6 Billionen Euro weltweit für das Jahr 2024 – dies entspricht in etwa der Hälfte des Bruttoinlandproduktes der Europäischen Union aus dem Jahr 2023.

Compliance-Herausforderungen

- NIS-2 steht vor der Tür: Die EU-Richtlinie NIS-2 soll ein einheitlich hohes Cybersicherheitsniveau in der gesamten EU gewährleisten. Sie erweitert ab Oktober den Anwendungsbereich erheblich und stellt strengere Anforderungen. Allein in Deutschland sind davon rund 30.000 Organisationen betroffen. Viele Unternehmen sind jedoch bislang nicht ausreichend auf die Umsetzung vorbereitet, die besonders für den Mittelstand eine Herausforderung darstellt.
- DSGVO vs. FISA 702: Die DSGVO hat zu Verbesserungen in der Datensicherheit geführt, aber aufgrund kontroverser Gesetzgebungen bestehen weiterhin rechtliche Unsicherheiten bezüglich grenzüberschreitender Datentransfers, insbesondere zwischen der EU und den USA.

7 von 10
Organisationen erwarten schwere Schäden durch DDoS-Attacken.

Lünendonk 2023

Mehr als die Hälfte
aller Organisationen fühlen sich in Ihrer Existenz bedroht.

Bitkom 2023

Trends und Prognosen

Die Cybersicherheitslandschaft wird auch weiterhin von geopolitischen Spannungen, zunehmender Professionalisierung von Cyberkriminellen und der Entwicklung neuer Angriffstechniken geprägt sein. Unternehmen und Organisationen müssen ihre Sicherheitsmaßnahmen kontinuierlich anpassen und verbessern, um mit den sich entwickelnden Bedrohungen Schritt zu halten. Für Gesetzgeber und Aufsichtsbehörden gilt es indessen, die passenden Rahmenwerke zu liefern, um die Gesellschaft resilient gegenüber diesen Risiken aufzustellen.

KRITISche Prozesse im Fokus

Cybervorfälle auf Organisationen aus dem Bereich der kritischen Infrastruktur (KRITIS) haben Hochkonjunktur. Allein im ersten Quartal 2024 wurden dem Bundesamt für Sicherheit in der Informationstechnik (BSI) 181 Vorfälle gemeldet. Im Schnitt verzeichnete jede sechste KRITIS-Organisation einen Cybervorfall – besonders betroffen waren die Sektoren Energie, Finanz- und Versicherungswesen, Transport und Verkehr sowie das Gesundheitswesen.[1]

Bedrohungslage in der EU

Ebenfalls verstärkt unter Druck stehen Einrichtungen der öffentlichen Verwaltung. Durch die geopolitischen Entwicklungen seit Beginn des Ukraine-Krieges sehen sich Behörden zunehmend mit Angriffskampagnen politisch motivierter Gruppierungen konfrontiert.

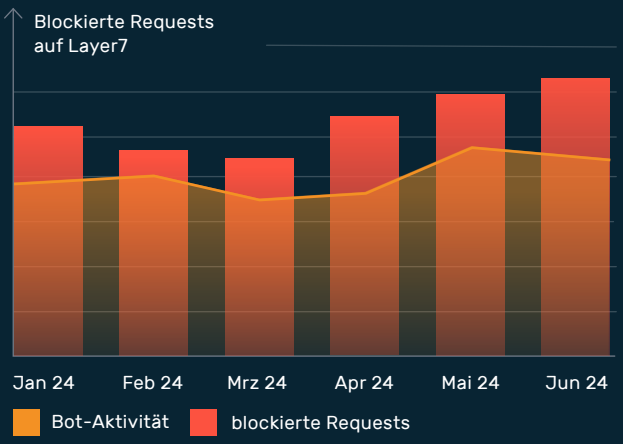
Im März traf eine massive DDoS-Angriffswelle französische Regierungswebseiten. Nach eigenen Angaben wollen die Angreifer 17.000 IP-Adressen und Geräte sowie mehr als 300 Domains lahmgelegt haben. Anfang April sorgten Cyberkriminelle mit einer breit angelegten DDoS-Kampagne für Ausfälle von Webseiten verschiedener deutscher Landes- und Polizeibehörden in Berlin, Brandenburg, Mecklenburg-Vorpommern, Niedersachsen, Saarland, Sachsen-Anhalt, Schleswig-Holstein und Thüringen.

DDoS-Attacken, Cyberangriffe und Bad Bots: Schädliche Requests nehmen um 53,2 Prozent zu

Diese Trends lassen sich auch anhand der Mitigationsdaten aus dem Security Operations Center (SOC) von Myra nachvollziehen. Als spezialisierter Schutzdienstleister für Organisationen aus hochregulierten Sektoren können wir ein detailliertes Lagebild der Entwicklungen in den Bereichen Finanz- und Versicherungswesen, Gesundheitswesen, öffentlicher Sektor sowie KRITIS zeichnen.

Für das erste Quartal 2024 ist eine Zunahme von bösartigen Requests auf Webseiten, Online-Portalen und Web-APIs um 29,8 Prozent im Vergleich zu 2023 festzuhalten. Im zweiten Quartal fällt der Zuwachs mit 80 Prozent nochmals deutlicher aus. Über das gesamte erste Halbjahr 2024 hinweg beträgt der Anstieg bösartiger Requests 53,2 Prozent gegenüber dem Vorjahreszeitraum. Dieser schädliche Traffic setzt sich zusammen aus DDoS-Angriffen, Attacken auf Schwachstellen in Online-Anwendungen und Bot-basierten Angriffen. Vor allem für Mai und Juni belegt das Traffic Monitoring aus dem Myra SOC eine hohe Aktivität von schädlichen Bots.

Angriffe und Bot-Aktivität



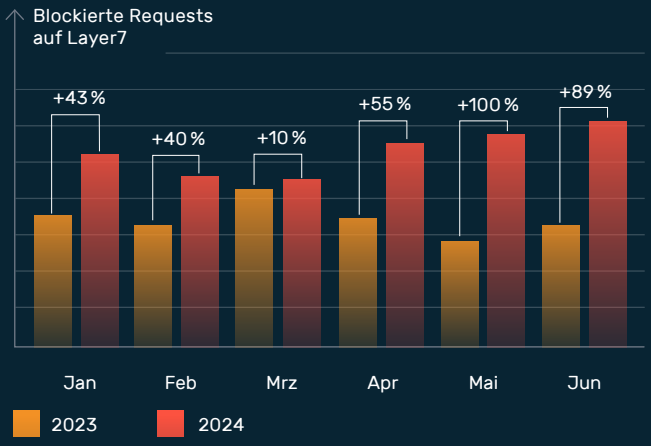
Nach einem leicht rückläufigen Trend im ersten Quartal 2024 steigt die Zahl schädlicher Anfragen ab April wieder kontinuierlich. Autonome Zugriffe durch schädliche Bots folgen weitestgehend diesem Trend, wobei zum Ende des zweiten Quartals ein leichter Rückgang festzustellen ist.

Mit ein Grund für die angespannte Bedrohungslage ist die zunehmende Professionalisierung von Cyberkriminellen, auf die bereits das BSI hingewiesen hat. Durch Cybercrime-as-a-Service-Plattformen werden kriminelle Dienstleistungen wie DDoS-Angriffe über das Darknet kostengünstig vermittelt – simple Attacken sind dort bereits ab 10 US-Dollar erhältlich.[3] Hierdurch sind Angriffe auch für Akteure ohne besondere technische Fähigkeiten möglich.

Ein weiteres Beispiel für die massenhafte Verbreitung von Angriffstools ist das Projekt DDoSia der kriminellen Gruppierung NoName057(16). Das Tool wird Anhängern der Gruppe per Telegram-Messenger zur Verfügung gestellt. Einmal installiert, fungiert der Client-Rechner als Teil eines Botnets, um DDoS-Angriffe auszuführen.

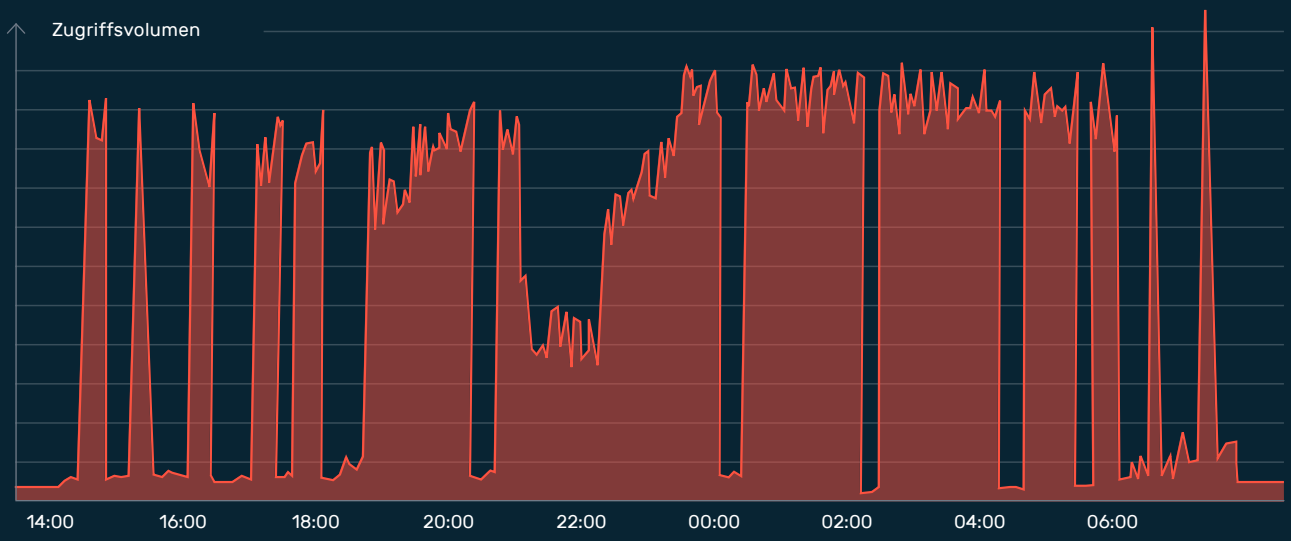
Wie massiv die Schlagkraft von DDoSia mittlerweile ist, zeigt ein Blick in das Myra SOC: Im Juni verteidigten die Abwehrsysteme von Myra vollautomatisch eine 17-stündige DDoS-Attacke auf die digitalen Prozesse eines deutschen KRITIS-Unternehmens. Der Angriff erfolgte typisch über mehrere Wellen und führte zu einer Verhundertfachung des Zugriffsvolumens.

Angriffsaktivität: H1 2023 vs. H1 2024



Im Jahresvergleich zeigt sich vor allem im zweiten Quartal 2024 ein enormer Zuwachs blockierter Requests. Im Mai blockierten die Schutzsysteme von Myra doppelt so viele schädliche Anfragen wie noch 2023.

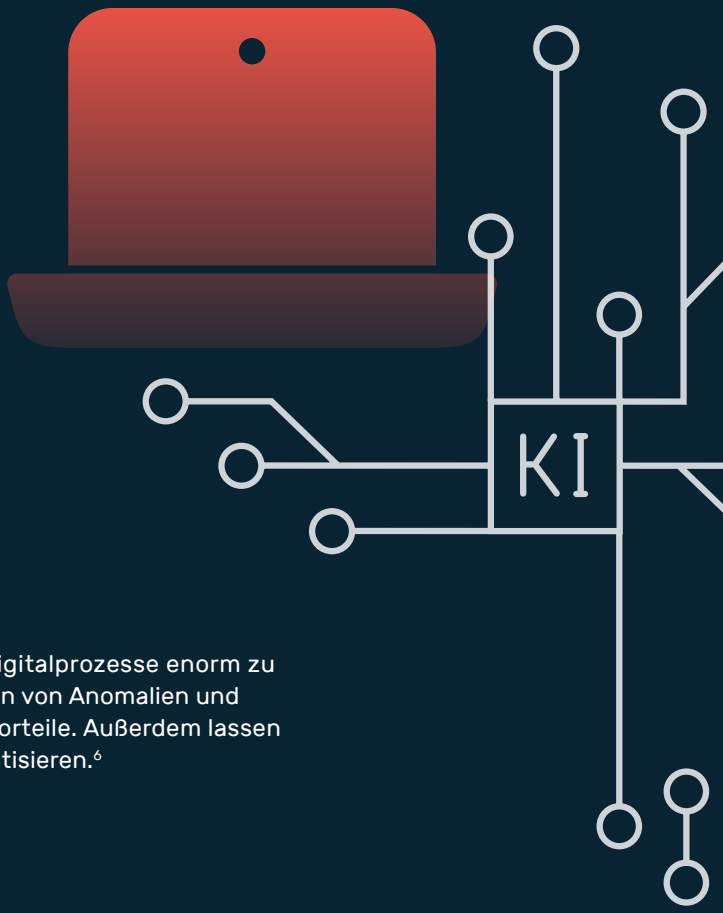
Verlaufsanalyse einer DDoSia-Attacke



Die von dem DDoSia-Botnet ausgehende Attacke erfolgte in mehreren Wellen über einen Zeitraum von 17 Stunden.

Licht und Schatten rund um KI und Cybersecurity

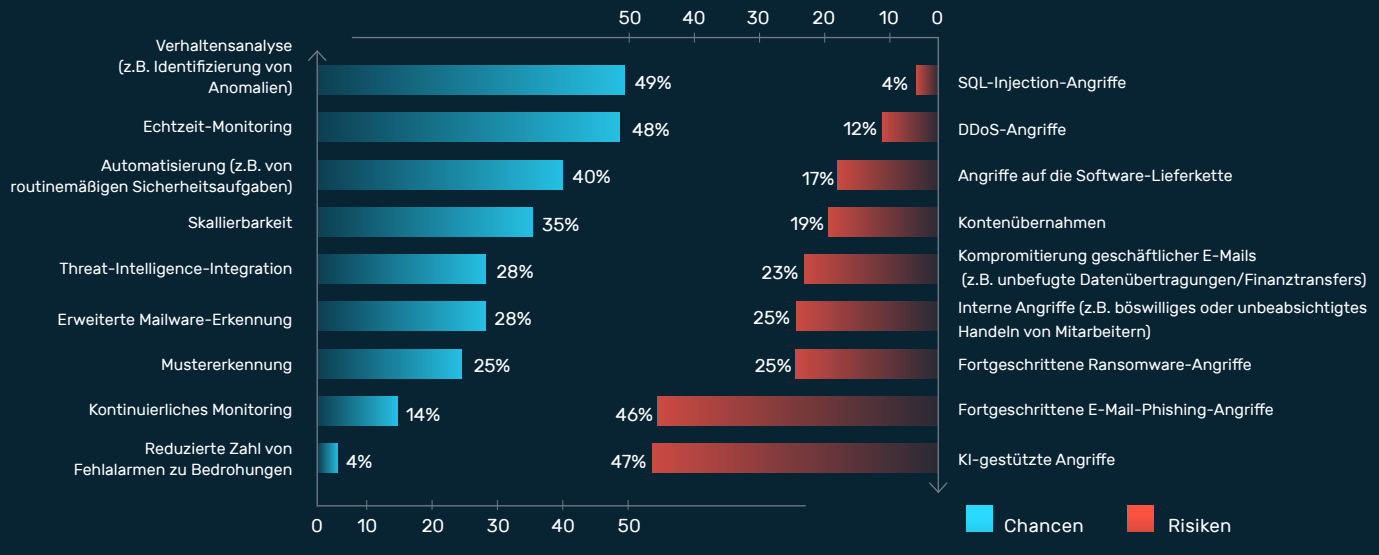
Künstliche Intelligenz (KI) birgt enorme Chancen, aber auch erhebliche Risiken für die Cybersicherheit. KI-Systeme können Bedrohungen in einigen Szenarien schneller erkennen und effektiver bekämpfen als Menschen. Gleichzeitig sind sie selbst ein potentes Angriffswerkzeug für Cyberkriminelle.



Die fortschreitende Entwicklung von KI-Lösungen droht die Bedrohungslage weiter zu verschärfen. Während Angreifer aktuell mehrheitlich für Phishing-Kampagnen auf Large Language Models (LLMs) wie GPT 3.5 zurückgreifen, eignen sich neue LLM-Generationen auch zur automatisierten Erstellung von Schadcode für neu gefundene Softwarefehler. Das Beheben und Schließen von Sicherheitslücken wird dadurch zu einem zeitkritischen Unterfangen, wenn bereits KI-gestützte Analysen von Security Advisories ausreichen, um zielgerichtete Exploits für die betroffene Software zu erstellen.[4] Kein Wunder, dass KI-basierte Angriffe jedem zweiten Unternehmen Sorgen bereiten.[5]

Indes ermöglichen KI-Systeme, die Absicherung kritischer Digitalprozesse enorm zu verbessern. Insbesondere bei der automatisierten Identifikation von Anomalien und dem Echtzeit-Monitoring sehen Sicherheitsfachleute große Vorteile. Außerdem lassen sich durch KI viele routinemäßige Sicherheitsprozesse automatisieren.[6]

Chancen und Risiken von KI in der Cybersicherheit



Cybersecurity-Fachleute sehen beim Einsatz von KI in der Cybersicherheit vor allem Potenzial bei der Erkennung, dem Echtzeit-Monitoring und der Automatisierung von Routinemaßnahmen. Demgegenüber stehen Risiken durch KI-gestützte Angriffe und fortschrittliches Phishing via E-Mail.

Cybercrime, Hacktivismus und Milliardenkosten

Der Kampf gegen organisierte Cybergruppierungen hält weiterhin nationale wie internationale Ermittlungsbehörden in Atem. Im Mai gelang dem Bundeskriminalamt in Zusammenarbeit mit Strafverfolgungsbehörden aus den Niederlanden, Frankreich, Dänemark, Großbritannien, Österreich sowie den USA im Rahmen der „Operation Endgame" ein schwerer Schlag gegen verschiedene Cybergruppierungen – dabei wurden 100 Server beschlagnahmt, 1.300 Domains gesperrt und 10 Haftbefehle erlassen. Gegen die Betreiber der Infrastruktur wurde zudem ein Vermögensarrest in Höhe von 69 Millionen Euro erwirkt und 99 Krypto-Wallets mit einem aktuellen Gesamtvolumen von mehr als 70 Millionen Euro bei zahlreichen Kryptobörsen beschlagnahmt.

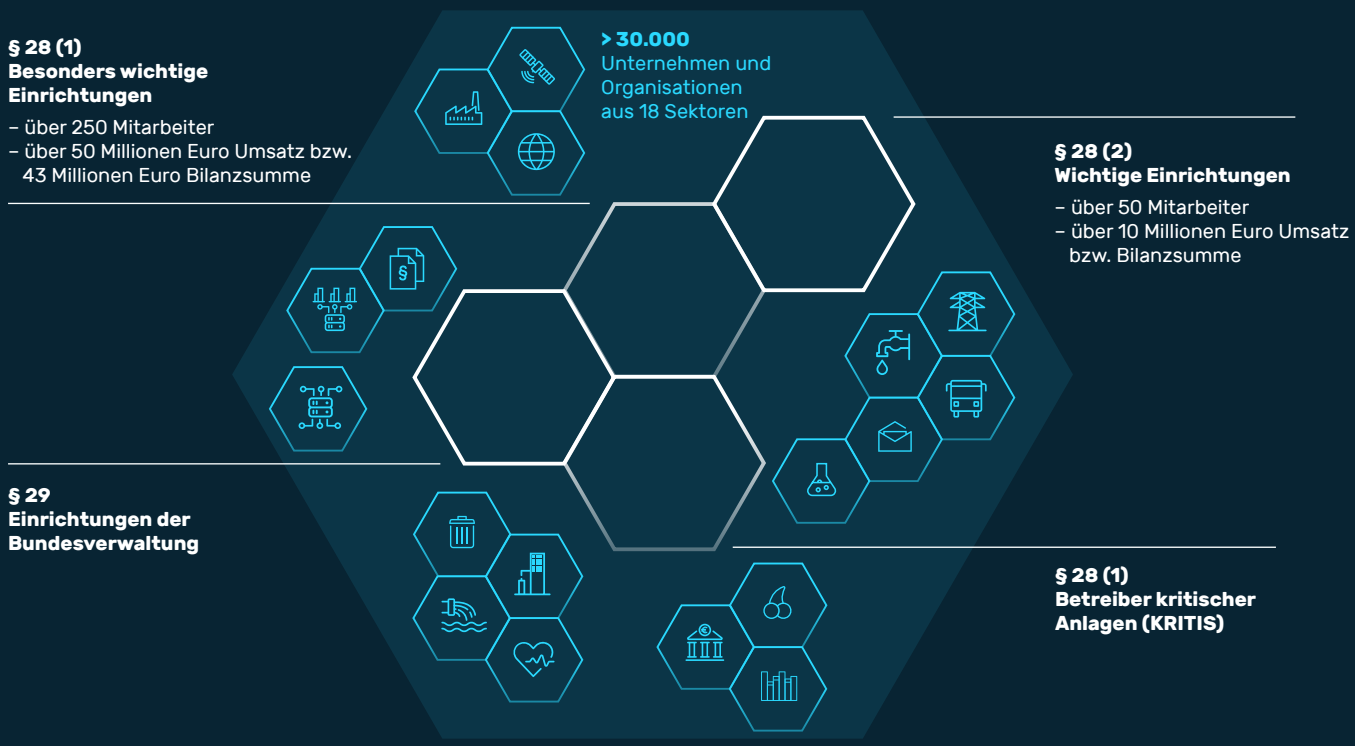
Wie jedoch die Lockbit-Razzia aus dem Februar zeigt, sind solche Erfolge oft nur von kurzer Dauer.[7] Innerhalb weniger Tage meldeten sich die Cyberkriminellen rund um Lockbit mit neuen Angriffstools zurück. Damit gleicht das Vorgehen der Behörden gegen Cyberkriminelle dem Kampf gegen die Hydra – dem Ungeheuer aus der griechischen Mythologie, dem zwei Köpfe nachwachsen, wenn man ihm einen abschlägt.

Vor diesem Hintergrund verwundert es nicht, dass die durch Cyberkriminalität verursachten Kosten immense Ausmaße erreichen. Während sich die Schäden für die deutsche Wirtschaft auf jährlich 148 Milliarden Euro belaufen, werden die globalen Kosten für das Jahr 2024 auf 8,6 Billionen Euro geschätzt.[8,9]

Herausforderung NIS-2-Compliance

Als Reaktion auf die sich seit Jahren verschärfende Bedrohungslage hat die EU mit der NIS-2-Richtlinie die nächste Evolutionsstufe ihrer Cybersicherheitsstrategie auf den Weg gebracht. Die Richtlinie erweitert den ursprünglichen Anwendungsbereich erheblich und definiert strengere Anforderungen an Unternehmen und Organisationen in kritischen Sektoren wie Energie, Verkehr, Gesundheitswesen und digitale Infrastruktur.

NIS-2-Scope im Überblick



Durch die NIS-2-Richtlinie erhöht sich die Zahl hochregulierter Organisationen immens. Je nach Unternehmensgröße und Sektorenzugehörigkeit gilt es unterschiedlich straffe Vorgaben für das IT-Risikomanagement, die Meldung von Cybervorfällen und die sichere Zusammenarbeit mit Dienstleistern zu befolgen.

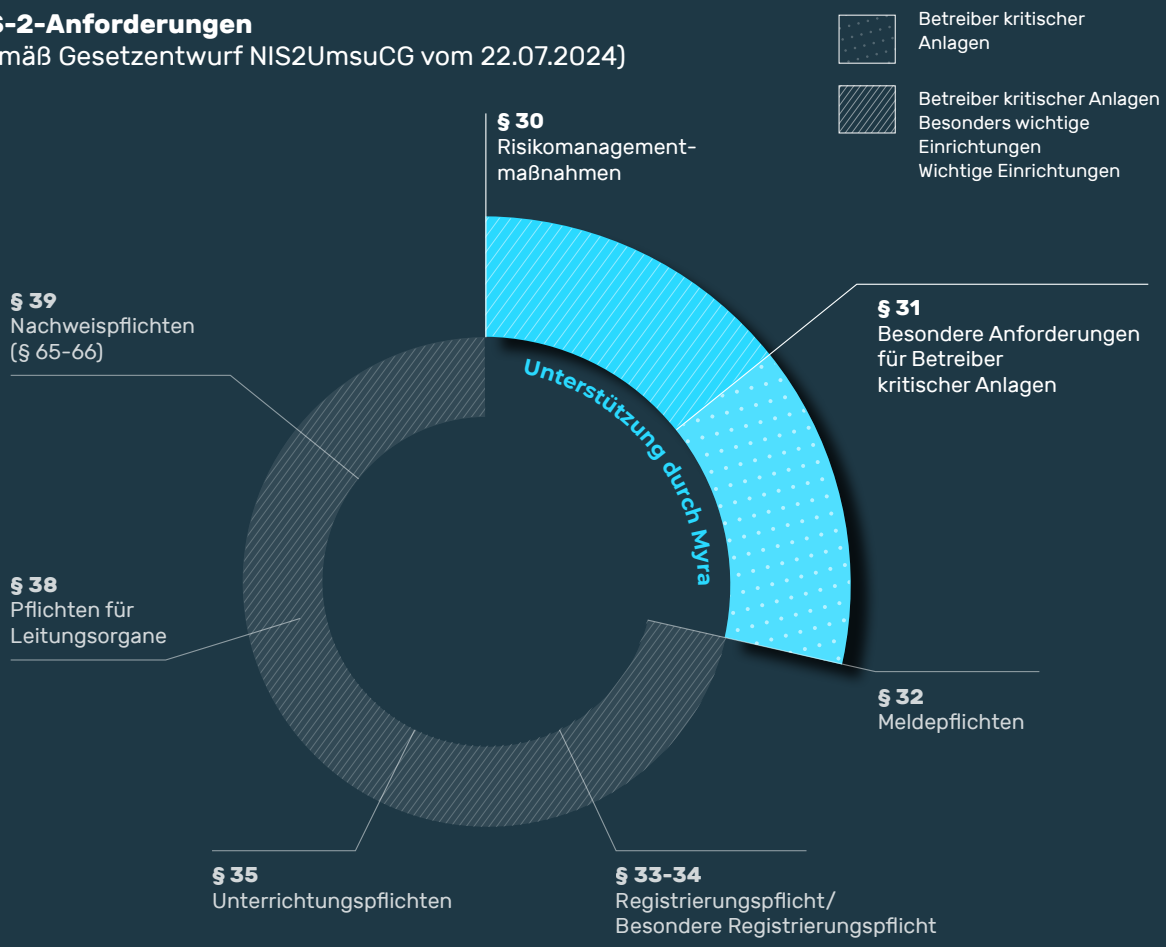
Ziel ist es, ein einheitlich hohes Cybersicherheits-niveau in der gesamten EU zu gewährleisten und die Widerstandsfähigkeit gegen Cyberangriffe zu stärken.

Dabei geht NIS-2 über die bloße Erweiterung des Anwendungsbereichs hinaus. Die Richtlinie legt einen starken Fokus auf das Cybersicherheits-Risikomanagement, die Meldung von Sicherheitsvorfällen und die Informationssicherheit entlang der Lieferkette. Unternehmen müssen gemäß NIS-2 umfassende Maßnahmen ergreifen, um ihre Systeme und Daten zu schützen, und im Falle eines Angriffs schnell und effektiv reagieren.

Bis Mitte Oktober muss NIS-2 in deutsches Recht umgesetzt sein und Anwendung finden. Trotzdem haben sich viele der rund 30.000 betroffenen Unternehmen in Deutschland noch nicht hinreichend mit den künftigen Anforderungen auseinandergesetzt, wie aus einer Umfrage des eco-Verbands hervorgeht. Jedes dritte Unternehmen gab bei der Umfrage an, noch keine Maßnahmen für die NIS-2-Umsetzung getroffen zu haben. Erst 13,2 Prozent der IT-Entscheidenden haben das IT-Risikomanagement entsprechend NIS-2 ausgebaut.

Insbesondere für den Mittelstand stellen die neuen Vorgaben eine Herausforderung dar, da die Umsetzung viele zusätzliche Ressourcen erfordert und das benötigte Fachpersonal nur schwer zu finden ist. Der Bitkom rechnet für das Jahr 2024 mit einer IT-Fachkräftelücke von rund 153.000 offenen Stellen über alle Sektoren hinweg.[10] Im Schnitt suchen Unternehmen mehr als sieben Monate, bis sie eine geeignete IT-Fachkraft gefunden und rekrutiert haben.[11]

NIS-2-Anforderungen
(gemäß Gesetzentwurf NIS2UmsuCG vom 22.07.2024)



Im Zentrum der NIS-2 steht das Risikomanagement. Es umfasst gemäß § 30 NIS2UmsuCG die Durchführung von Risikoanalysen, die Sicherheit von Informationssystemen, die Bewältigung von Sicherheitsvorfällen sowie die Aufrechterhaltung des Betriebs einschließlich Wiederherstellung und Krisenmanagement.

Darüber hinaus müssen die betroffenen Organisationen die Lieferketten absichern, die Sicherheit bei der Entwicklung und Wartung gewährleisten, das Risikomanagement evaluieren und das Personal in Cyberhygiene und Cybersicherheit schulen. Kryptografie, Personalsicherheit, Zugangskontrollen und Multi-Faktor-Authentifizierung sind weitere ergänzende Maßnahmen.

Das Risikomanagement von Betreibern kritischer Anlagen muss gemäß § 31 höheren Anforderungen genügen und aufwändigere Maßnahmen umfassen. Zudem sieht das NIS2UmsuCG hier den Einsatz von Angriffserkennungssystemen nach dem Stand der Technik vor.

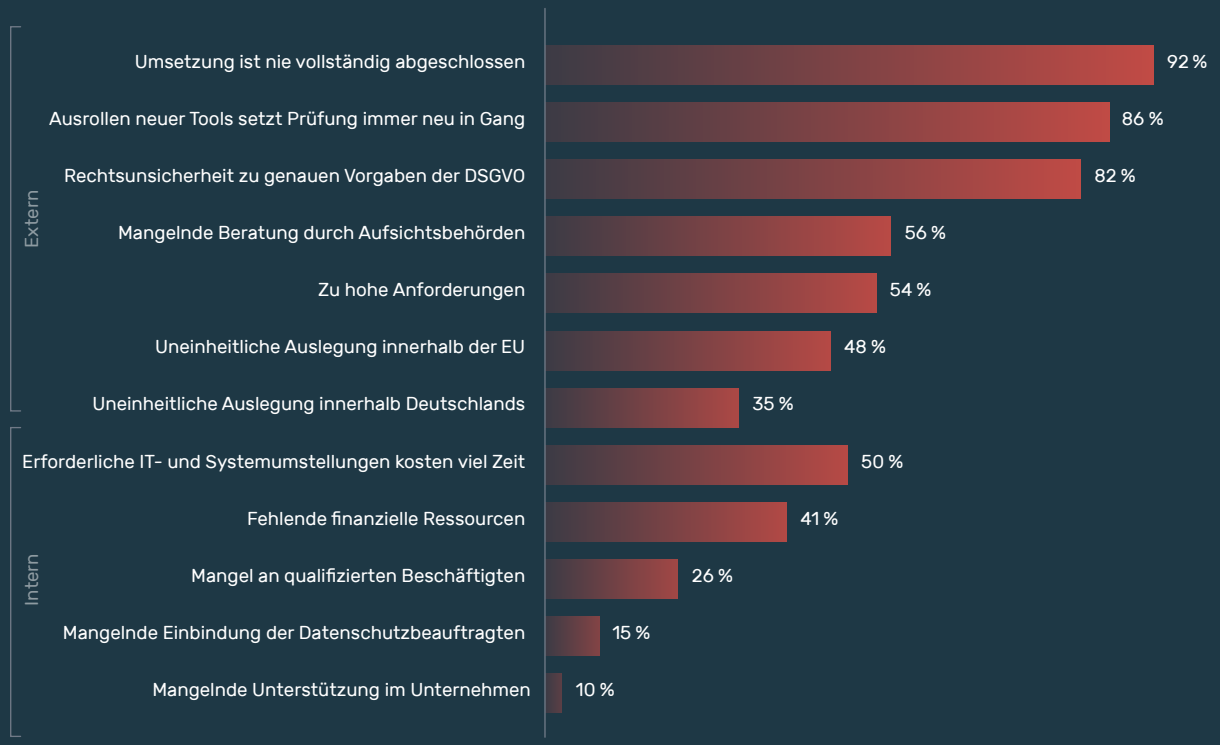
DSGVO und US-Datentransfer

Während NIS-2 auf einen Ausbau der Cybersicherheit abzielt, soll die Datenschutz-Grundverordnung (DSGVO) für eine bessere Absicherung sensibler Informationen sorgen – mit Erfolg. Seit Einführung der DSGVO im Jahr 2018 haben 61 Prozent der deutschen Unternehmen ihre Datensicherheitsmaßnahmen optimiert. Dennoch sind sich viele Organisationen weiterhin unsicher im Umgang mit grenzüberschreitender Datenübertragung, insbesondere vor dem Hintergrund von Rechtsunsicherheiten im transatlantischen Datenverkehr.[12]

Die DSGVO definiert strenge Standards für die Verarbeitung personenbezogener Daten. Demgegenüber verpflichtet der im April 2024 verlängerte Foreign Intelligence Surveillance Act (FISA) in Section 702 US-amerikanische Organisationen zur Kooperation mit Ermittlungsbehörden und der Herausgabe von Daten von Nicht-US-Bürgern. Diese kontroverse Positionierung der Gesetzgebung in Europa und den USA führt zwangsläufig zu juristischen Spannungen und Rechtsunsicherheit.
In der Vergangenheit wurden mit Safe Harbor (2015) und Privacy Shield (2020) bereits zwei Datenschutzabkommen zwischen Europa und den USA vom Europäischen Gerichtshof (EuGH) kassiert. Auch der aktuelle Angemessenheitsbeschluss auf Grundlage des neuen EU-US Data Privacy Framework wird in Fachkreisen kontrovers diskutiert. Der Datenschützer Max Schrems hat bereits angekündigt, juristisch dagegen vorzugehen, da es „keine substanzielle Änderung des US-Überwachungsrechts" biete.

Vor diesem Hintergrund verwundert es kaum, dass nahezu alle in Deutschland ansässigen Unternehmen (99 Prozent) beim Einsatz von Cloud Services einen Anbieter mit Rechenzentren in Deutschland bevorzugen.

Unternehmensumfrage: Die größten Herausforderungen bei der DSGVO-Umsetzung[13]



IT-Entscheidende sehen bei den externen Belastungen vor allem die anhaltende Umsetzung der Datenschutzvorgaben, die ständige Prüfung neuer Tools sowie die anhaltende Rechtsunsicherheit als Herausforderung. Intern bilden die erforderlichen Ressourcen hinsichtlich Zeit, Kosten und Personal die größten Schwierigkeiten.

DDoS Threat Insights by zeroBS

7 Fragen zur DDoS-Bedrohung an zeroBS CTO Markus Manzke

Markus Manzke ist Chief Technology Officer (CTO) von zeroBS, einem in Deutschland ansässigen Pentesting-Unternehmen. zeroBS hilft seinen Kunden, die Risiken beim Betrieb von internetbasierten Infrastrukturen zu verstehen und zu adressieren. zeroBS ist rein technologiegetrieben und betreibt eigene Lösungen für die verschiedenen Arten von Verfügbarkeitstests (Avydos, DDoS-Stresstests). Markus verfügt über 15 Jahre Erfahrung als Sicherheitsspezialist im deutschen E-Commerce-Ökosystem und ist an einigen Open-Source-Lösungen wie Naxsi (nginx-basierte WAF) und Emerging-Threats (Open Source Snort Signatures) beteiligt. Er ist regelmäßiger Sprecher auf Security-Konferenzen (CeBIT, SLAC, diverse BSides, Solutions HH).

DNS-Angriffe scheinen prominenter zu werden, welche Methoden sind hier führend?
Seit 2023 wird eine Zunahme der sogenannten DNS-Flood-Angriffe von verschiedenen Herstellern beobachtet. Dabei werden die DNS-Server dermaßen unter Last gesetzt, dass diese den Betrieb einstellen und das angegriffene Target quasi digital ausradiert wird.

Welche Angriffsvektoren bereiten Unternehmen bei der Abwehr am meisten Schwierigkeiten?
Über den Applikationslayer finden momentan die erfolgreichsten Angriffe statt, da dieser aufgrund einer Kombination von Angriffsoberfläche (Anzahl und Verteilung der Ziele) und eingesetzter Technologie (klassische Webanwendungen, APIs, API-generierte Webseiten) einen extrem hohen Grad an Komplexität aufweist.

Haben DDoS-Angriffe durch staatliche Akteure zugenommen?
Direkt staatliche Akteure sind bei DDoS-Angriffen selten zu sehen. Eine Zunahme von Hacktivismus, der durch geopolitische Ereignisse getrieben wird, sehen wir aber weltweit (Europa, USA, Israel, Naher Osten, Südostasien).

Markus Manzke
Chief Technology Officer (CTO)
von zeroBS

Gibt es neue Angriffstools oder -techniken, die besonders besorgniserregend sind?
Zum einen sind APIs in den Fokus geraten, die durch IoT-Botnetze immer noch gut anzugreifen sind, zum anderen sehen wir eine starke Zunahme von Angriffen mittels Browsern und Proxyfarmen, die klassische Abwehrverfahren und Geoblocking unterlaufen. Wir rechnen weiterhin mit einer starken Zunahme von Protokollangriffen gegen HTTP/2, da hier zwei neue Angriffsvektoren in den letzten sechs Monaten publiziert wurden (RapidReset, Continuation Flood) und neue Vektoren zu erwarten sind.

Welche Rolle spielt heute schon KI und maschinelles Lernen bei der Durchführung und Abwehr von DDoS-Angriffen?
Wir sehen KI schon im Einsatz, vornehmlich auf der Verteidigerseite, um sich gegen neuartige Angriffe zu wappnen. Einerseits funktioniert KI-Unterstützung gut gegen IoT-Botnetze, andererseits lässt sich diese von intelligenten Angreifern effektiv nutzen, um den Angriffstraffic zu „lernen".

Wie ausschlaggebend ist die maximale Abwehrbandbreite bei der Mitigation von Angriffen wirklich?
Wenn man sich die Reports der namhaften Hersteller anschaut, dann liegt die Bandbreite von 90 Prozent der Angriffe unter 100 GB/s, und die High-Volume-Angriffe werden mit 300 bis 500 GB/s durchgeführt. Es gibt einige wenige Angriffe pro Jahr, die im TB-Bereich zu verorten sind, dies sind aber Einzelfälle. Die maximale Bandbreite spielt erst dann eine Rolle, wenn tatsächlich so ein Angriff stattfindet oder zumindest hoch wahrscheinlich wird.

Welche Entwicklungen und Trends erwarten Sie in Bezug auf DDoS-Attacken in naher Zukunft?
Da sich die geopolitische Lage in absehbarer Zukunft nicht ändern wird, bleibt der sogenannte Hacktivismus ein ernstzunehmender Faktor. Des Weiteren erwarten wir eine weiterhin zunehmende Professionalisierung sowohl der Angriffsmethoden (Browser, Proxies, APIs, WAF, Stack/Protokolle) als auch der Zielauswahl seitens der Angreifer.

HTTP/2-Angriff „Continuation Flood“

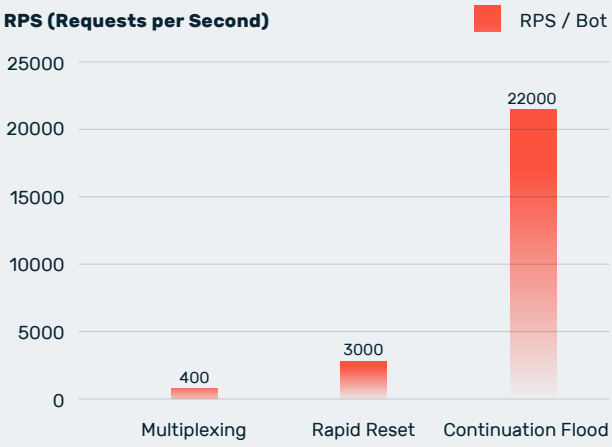
Anfang April 2024 wurde die neue DDoS-Angriffstechnik namens „HTTP/2 Continuation Flood“ entdeckt, die Schwachstellen in zahlreichen HTTP/2-Protokollimplementierungen ausnutzt.

In vielen Fällen stellt die Continuation Flood eine größere Bedrohung dar als die im vergangenen Jahr entdeckte Rapid-Reset-Methode: Es genügt ein einzelner Rechner (und in bestimmten Fällen sogar eine einzelne TCP-Verbindung oder eine Handvoll Frames), um einen Webserver zu überlasten. Dabei sind die schädlichen Anfragen der Attacke nicht einmal in HTTP-Zugriffsprotokolldateien sichtbar, da ähnlich wie bei Slowloris-Attacken die Anfragen nie abgeschlossen werden.

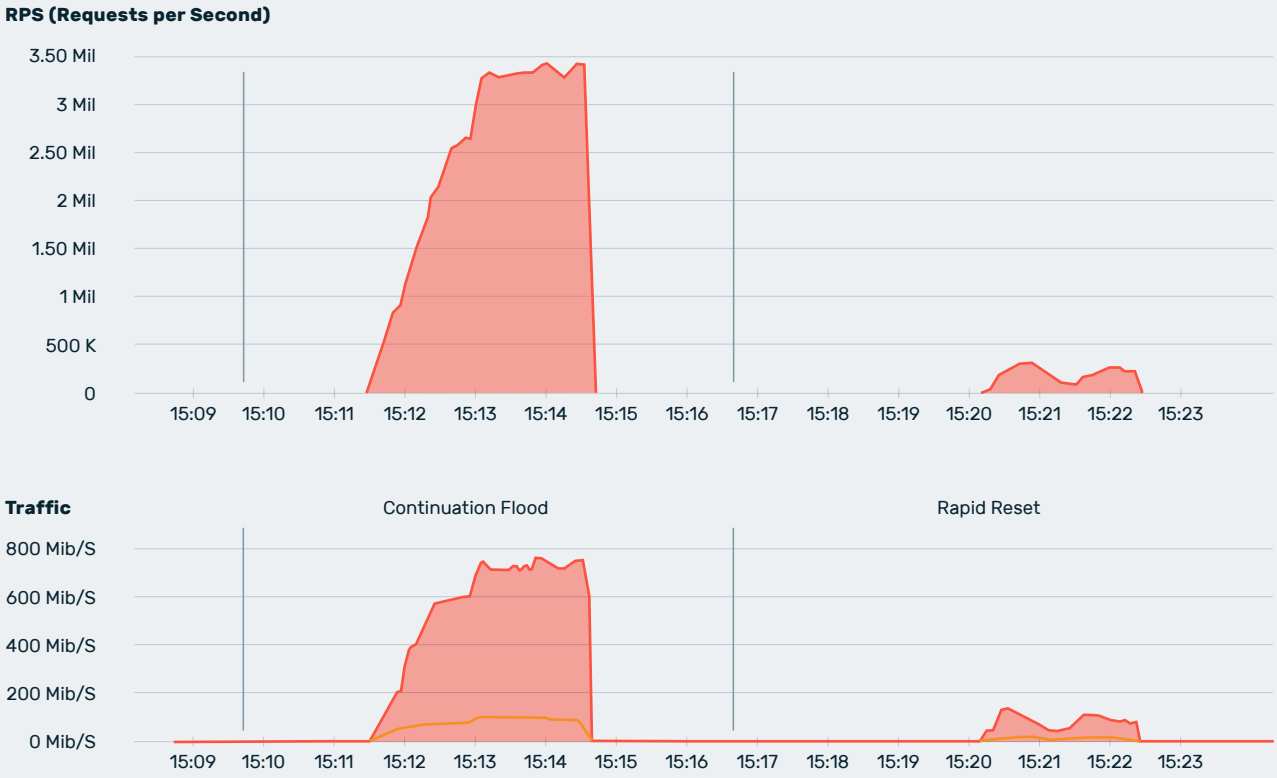
zeroBS hat den neuen Vektor untersucht und kann seine Wirksamkeit gegen mehrere getestete Systeme bestätigen. Beim Vergleich einer Continuation Flood mit Rapid Reset, wird das enorme Schadpotenzial deutlich: Während Rapid Reset im Vergleich zu normalen HTTP/2-Multiplexing-Angriffen fast achtmal so stark war, ist die Continuation Flood in Bezug auf reine Requests per Second (RPS) pro Bot nochmals siebenmal stärker als Rapid Reset – oder 55-mal stärker als Multiplexing.

Bis zu 55-mal stärker: Im Vergleich zu herkömmlichen Multiplexing-Angriffen und der Rapid Reset-Methode aus dem Vorjahr zeigt sich die enorme Schlagkraft der Continuation Flood.

HTTP/2-Angriffsvektoren im Vergleich



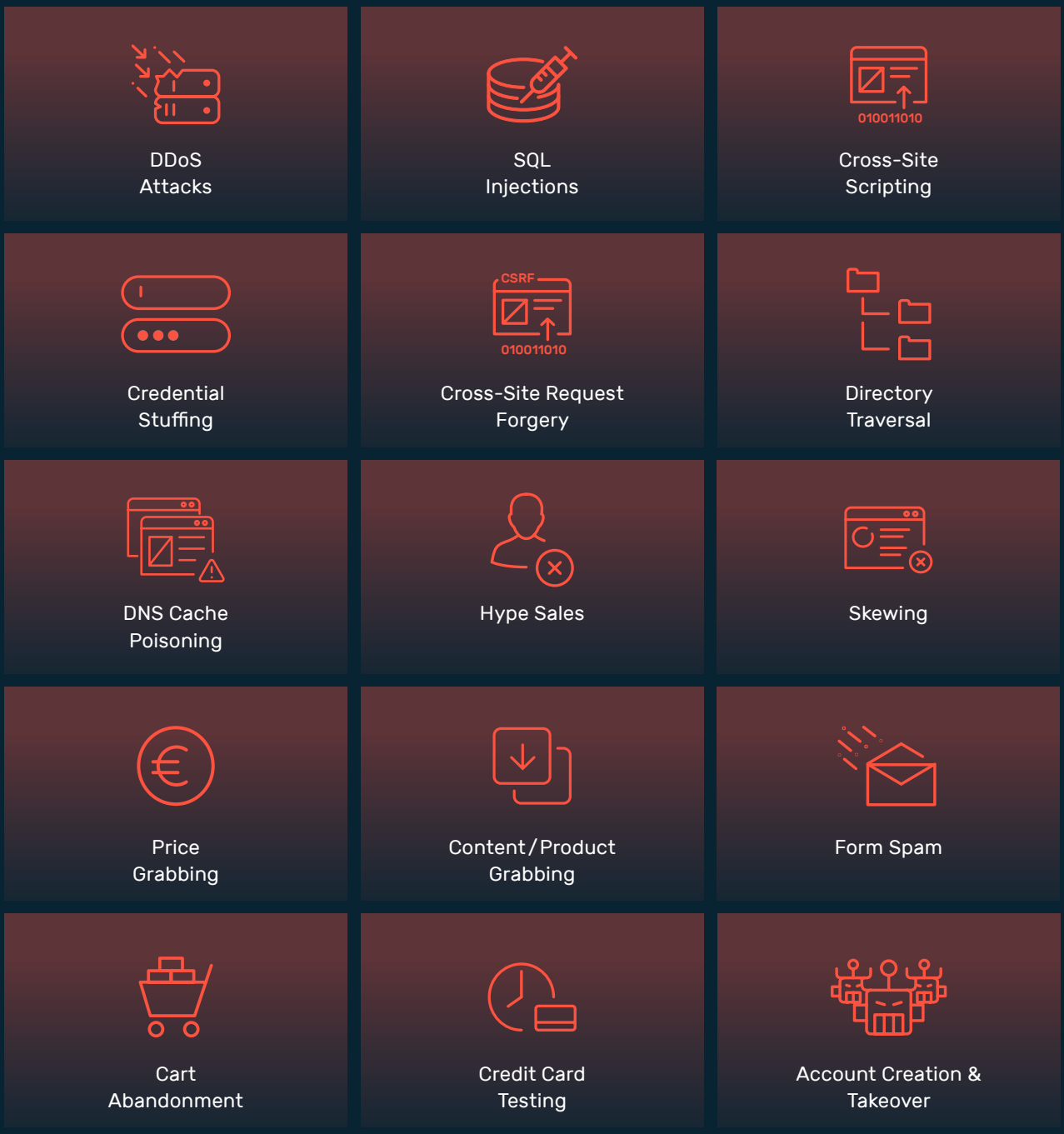
Analyse der Continuation Flood



Sowohl hinsichtlich Paketrate (RPS) als auch Traffic-Volumen übertrifft die Continuation Flood die Rapid-Reset-Methode bei weitem.

Unternehmen stehen täglich einer Fülle digitaler Bedrohungen gegenüber. Myra bietet effektive Schutzlösungen, um dieser Herausforderung zu begegnen.

Die Security-as-a-Service-Plattform von Myra ist zur Absicherung geschäftskritischer Onlineprozesse konzipiert. Unsere Kunden profitieren von hocheffizienten Schutzlösungen zur Abwehr von DDoS-Attacken, schädlichen Bot-Zugriffen, Zero-Day-Exploits, Angriffen auf Datenbanken und vieler weiterer Bedrohungen.



Umfassender Schutz vor schädlichem Traffic

Im Bereich Applikations- und Infrastrukturschutz liefert Myra alle von Gartner definierten Funktionalitäten – von DDoS-Abwehr auf allen relevanten Ebenen über Secure CDN, Web Application und API Protection (WAAP) bis hin zu DNS Security.

Zentrale Funktionen	
Erkennung und Mitigation von volumetrischen Angriffen auf Layer 3	✓
Amplification/Reflection-Attacken (via DNS, NTP, SSDP, CLDAP, Memcached etc.)	✓
Carpet bombing	✓
ICMP flood attacks etc.	✓
Erkennung und Mitigation von Protokoll-Attacken auf Layer 4, die zu Ressourcenüberlastung führen	✓
Flood-Attacken (UDP, TCP SYN, ACK, SYN/ACK, RST, UDP Fragmentation etc.)	✓
Erkennung und Mitigation von Angriffen auf Anwendungsebene (Layer 7)	✓
HTTP-Flood-Attacken (GET, POST, HEAD, Recursive GET Flood etc.)	✓
Low-and-slow-Angriffe (Slowloris etc.), ReDoS, Denial of Wallet Attacks	✓
Erkennung und Mitigation von Multivektor-Attacken	✓

Optionale Funktionen	
Echtzeit-Protokollierung und Reporting-Schnittstelle	✓
Security Operations Center (SOC) and Managed Security Services (MSS)	✓
CDN	✓
Web Application und API Protection (WAAP)	✓
Bot Mitigation	✓
Domain Name System (DNS) Security	✓

Quellen

1 BSI: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html
2 IBM: 2024 X-Force Threat Intelligence Index
3 Privacy Affairs Dark Web Price Index 2023
4 Richard Fang, Rohan Bindu, Akul Gupta, Daniel Kang: LLM Agents can Autonomously Exploit One-day Vulnerabilities | Cornell University
5 Capterra Sicherheitsreport 2024
6 Capterra Sicherheitsreport 2024
7 Europol: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
8 Bitkom Wirtschaftsschutz 2023
9 Statista Market Insights
10 Bitkom 2024: IT-Fachkräfte 2040:Wo steht die deutsche Wirtschaft?
11 Bitkom 2024: Trotz Krieg und Krisen: In Deutschland fehlen 137.000 IT-Fachkräfte
12 Bitkom Research 2023: https://www.bitkom.org/Presse/Presseinformation/5-Jahre-DS-GVO-nur-Note-ausreichend#_
13 Bitkom Research 2023

Deshalb entscheiden sich CISOs für Myra

Security

Durch Cyberangriffe werden Daten gestohlen, Systemausfälle provoziert und Kommunikationskanäle gestört. Myra wehrt Angriffe auf Ihre digitalen Prozesse in Echtzeit ab.

Performance

Traffic-Peaks durch Sales- Kampagnen, Livestreaming oder unplanbare Ereignisse überfordern Web-Anwendungen. Myra liefert Ihren Content immer hochperformant aus.

Business Continuity

Myra gewährleistet den größtmöglichen Schutz für Ihr Unternehmen, indem es direkte und georedundante Verbindungen zu Ihrer Infrastruktur nutzt, ohne von externen Faktoren abhängig zu sein.

Compliance

Gesetzliche und unternehmensspezifische Vorgaben zu IT-Sicherheit und Datenschutz erfordern auditierte Prozesse. Myra ist Ihr Garant für strengste Anforderungen.

BSI-zertifizierte IT-Sicherheit

Die Myra-Technologie ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Standard ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Zudem erfüllen wir als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | BSI C5 TESTAT TYP 2 | Trusted Cloud SERVICE | ISAE 3402 IDW PS 951 TYPE 2 | DIN EN 50600 zertifiziert BETRIEBSSICHERES RECHENZENTRUM

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard (PCI DSS) | KRITIS-qualifiziert nach §3 BSI-Gesetz | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600

Myra schützt, was zählt. In der digitalen Welt.

Bundesministerium für Gesundheit | Bundeszentrale für gesundheitliche Aufklärung (BZgA) | llb 1861 | msc Munich Security Conference | CANCOM | DSV IT Service | Barmenia EINFACH. MENSCHLICH. | flatex DEGIRO

Made in Germany

Myra Security ist der neue Maßstab für globale IT-Sicherheit.

Sie wollen mehr darüber erfahren, wie Sie mit unseren Lösungen Ihren Umsatz steigern, Ihre Kosten minimieren und Ihre Anwendungen vor bösartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihr Unternehmen. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

Kostenlose Schutzberatung anfordern →

Myra Security GmbH

+49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com