LINK11

Trends 2025

Cyber-Resilienz durch Oberservability,
KI und ganzheitliche Strategien stärken

2024: Ein Jahr der Rekord-DDoS-Angriffe

Das Jahr 2024 markierte einen Wendepunkt in der Welt der Cyberbedrohungen: Nie zuvor wurden so viele und gleichzeitig so massive DDoS-Angriffe verzeichnet. Der Angriff des Mirai-Botnets mit über 2 Tbit/s auf einen asiatischen Hosting-Provider oder die größte europäische Attacke mit 1,4-Tbit/s, die Link11 erfolgreich abgewehrt hat, sind nur zwei Beispiele dafür, wie rasant das Bedrohungsniveau gestiegen ist. DDoS-Angriffe dominieren laut ENISA Threat Landscape 2024 mittlerweile das Feld der Cyberattacken in der EU und machen mit über 40 % den größten Anteil der registrierten Vorfälle aus – sie übertreffen damit sogar Ransomware und Datenvorfälle.

Der Einfluss der Künstlichen Intelligenz

Verantwortlich dafür sind die zunehmende Verfügbarkeit von DDoS-as-a-Service und der gezielte Einsatz von Künstlicher Intelligenz. Obwohl schwer zu quantifizieren, wird Künstliche Intelligenz (KI) bereits heute bei den verschiedensten Cybervorfällen eingesetzt. Der deutliche Anstieg der Angriffshäufigkeit, die enorme Größe einiger dieser DDoS-Angriffe und die orchestrierte Ausführung von Multi-Vektor-Angriffen deuten ebenfalls darauf hin. Das Reverse Engineering von Botnets und Angriffen ist jedoch schwierig und eher von vorübergehender Natur, was eine genaue Analyse erschwert.

Gleichzeitig zeigt sich ein klarer Trend: Unternehmen setzen verstärkt auf agiles Risikomanagement und KI-gestützte Analysetools, um Bedrohungen schneller zu erkennen, Compliance sicherzustellen und ihre Resilienz zu stärken. Für 2025 bedeutet dies: die Cybersicherheit muss intelligenter, agiler und vorausschauender werden, um den immer komplexeren Bedrohungen standzuhalten.

LINK11

Ausblick auf 2025

Neue Ziele,
mehr Überwachung,
stärkere Angriffe

Shift in Targets

Traditionelle Sektoren wie Gaming und Finanzdienstleistungen bleiben attraktive Ziele für Cyberkriminelle. Gleichzeitig beobachten wir eine zunehmende Diversifizierung der Angriffsszenarien. Neue Branchen im Bereich Kryptowährungen und Biotechnologie rücken zunehmend in den Fokus der Angreifer. Die Kryptowährungen stehen aufgrund ihrer hohen Liquidität und den innerhalb des Bereichs dezentralen Strukturen im Fokus. Auch der Biotechnologiesektor wird zunehmend angegriffen, da hier sensible Forschungsdaten und geistiges Eigentum von hohem Wert konzentriert zu finden sind. Diese Entwicklung zeigt, dass sich die Angreifer zunehmend auf Branchen mit hochpreisigen Vermögenswerten und sensiblen Geschäftsprozessen konzentrieren. Zudem spielt die geopolitische Lage eine entscheidende Rolle: Die Bereitschaft zu politisch motivierten Angriffen auf Regierungen und kritische Infrastrukturen ist nach wie vor sehr hoch. Konflikte wie in der Ukraine und in Israel führen zu gezielten Attacken auf staatliche und kritische Infrastrukturen. Diese Entwicklung zeigt, dass Cyberkriminelle ihre Strategien kontinuierlich anpassen und neue Angriffsmöglichkeiten ausloten.

„Ich erwarte für 2025, dass geopolitische Ereignisse im Rahmen bereits bestehender oder erst auftretender Konflikte weiterhin Widerhall im Cyberspace finden werden - mit einer weiter zunehmenden Annäherung kriminell und politisch motivierter Angreifer, etwa auch im Rahmen von technischem Tool-Sharing.“

Dr. Kerstin Zettl-Schabath
Cyberkonfliktforscherin
EuRepoC

„Was ich erwarte? Trinität mit Knock-Out-Potenzial aus KI-gestützten Angriffen, Quanten-bedrohungen und massivem - aber gar nicht so offensichtlichem - staatlichen Sponsoring.“

Annika Wägenbauer
Innovating Cybersecurity
Advocating for Holistic Security Solutions

Bigger and Badder

DDoS-Angriffe werden immer größer, häufiger und raffinierter. Die zunehmende Verbreitung von IoT-Geräten bietet Angreifern eine nahezu unbegrenzte Anzahl von Geräten, die sie für ihre Angriffe missbrauchen können. Botnets entwickeln sich ständig weiter und sind inzwischen in der Lage, riesige Datenmengen zu erzeugen. Dies führt dazu, dass immer mehr Angriffe regelmäßig die 200 Gbps-Marke überschreiten und damit immer größere Auswirkungen auf die Verfügbarkeit von Online-Diensten haben. Unternehmen müssen sich daher auf eine Zunahme von DDoS-Angriffen einstellen und ihre Sicherheitsmaßnahmen entsprechend anpassen.

Bedeutung der Observability

Die zunehmende Komplexität von IT-Umgebungen erfordert eine ganzheitliche Sicht auf die Sicherheit. Observability ermöglicht es Unternehmen, ihre IT-Infrastrukturen (On-Premise, Cloud oder Hybrid) umfassend zu analysieren und potenzielle Bedrohungen frühzeitig zu erkennen. Durch die kontinuierliche Überwachung von Systemen, Anwendungen und Netzwerken können Unternehmen Abweichungen vom Normalbetrieb schnell erkennen und darauf reagieren. Der Schwerpunkt liegt dabei nicht nur auf dem Schutz der Peripherie, sondern auch auf der Messung der Auswirkungen und der Arbeitsbelastung, um regulatorische Anforderungen zu erfüllen und die Auswirkungen und Schwachstellen während eines Angriffs besser zu verstehen. Darüber hinaus hilft Observability, regulatorische Anforderungen zu erfüllen und die Resilienz gegenüber Cyberangriffen zu verbessern. Ein wichtiger Aspekt dabei ist die Integration von Observability in die DevOps-Praktiken, um eine enge Zusammenarbeit zwischen Entwicklung und Betrieb zu gewährleisten. Übergeordnetes Ziel ist die Verbesserung der End-to-End-Sicherheit.

„Künstliche Intelligenz schärft zwar das Schwert der Cyberkriminellen, gleichzeitig können sich Unternehmen durch die intelligente Nutzung von KI-basierter Technologie wie proaktive Überwachung und automatisierte Abwehrmaßnahmen dagegen wehren.“

Jag Bains
VP Solution Engineering
Link11

„2025 sind ganzheitliche Cybersicherheits-konzepte gefragt, Unternehmen initiieren umfassende Sicherheitsprogramme. Dabei sind gesetzliche Regelungen oft der letzte Anstoß. Die Erkenntnis, dass Cybersicherheit und Resilienz durch Organisation, Menschen und Technologie geschaffen werden, setzt sich durch. Es geht um umfassende Programme, die vom C-Level verantwortet werden, und Cybersecurity wird zum Treiber der Digitalisierung.“

Rudolf Preuss
Bereichsleiter IT/OT
Actemium

API-Schutz: Die Achillesferse 2025

2025 wird die API-Sicherheit zu einem zentralen Thema der Cybersicherheitsstrategie – getrieben durch alarmierende Zahlen und neue Bedrohungen. Die Bedeutung der Programmierschnittstellen (Application Programming Interface) wird oft unterschätzt. Dabei sind sie für Cyberkriminelle ein ideales Einfallstor. Laut einer Befragung von Experten aus den USA, UK und Deutschland erleben 84 Prozent der Unternehmen im vergangenen Jahr API-Sicherheitsvorfälle. APIs, die als Schnittstellen die Kommunikation zwischen Anwendungen steuern, sind durch den zunehmenden Einsatz von KI-Systemen und Microservices immer häufiger Angriffsziel von Cyberkriminellen. Gleichzeitig mangelt es vielen Unternehmen an Transparenz: Weniger als ein Drittel der Unternehmen verfügt über ein vollständiges API-Inventar. Fehlende Übersicht erhöht das Risiko, Schwachstellen zu übersehen – und Gartner warnt, dass API-Verstöße im Schnitt zehnmal mehr Daten preisgeben als herkömmliche Sicherheitsverletzungen. Unternehmen müssen 2025 dringend handeln: Neben der Implementierung lückenloser Überwachungs- und Schutzmaßnahmen spielen generative KI und umfassendes Third-Party-API-Monitoring eine Schlüsselrolle.

Smarte Automatisierung hilft bei Fachkräftemangel

Der Fachkräftemangel wird 2025 zu einer der größten Herausforderungen für die Cybersicherheit in Deutschland. Laut der aktuellen ISC2 Cybersecurity Workforce Study sind 62 % der deutschen Organisationen von Personalengpässen betroffen, während 90 % der Cybersicherheitsteams Kompetenzlücken verzeichnen. Besonders kritisch: Der Bedarf wächst weiter, während die Zahl der verfügbaren Fachkräfte sinkt. ISC2 schätzt, dass die Anzahl der Cybersicherheitsexperten in Deutschland von 456.000 im Jahr 2023 auf 439.000 in 2024 zurückgegangen ist. Während Bedrohungen immer komplexer werden und gesetzliche Anforderungen steigen, fehlen in vielen Unternehmen qualifizierte Experten, um den Schutz vor Angriffen zu gewährleisten. Organisationen laufen Gefahr, Schwachstellen zu übersehen und Cyberkriminellen ein Einfallstor zu bieten. Gleichzeitig kämpfen viele Teams nicht nur mit zu wenig Personal, sondern auch mit Kompetenzlücken in Schlüsselbereichen wie Cloud-Sicherheit, künstlicher Intelligenz und Zero-Trust-Architekturen. Hoffnungsträger ist generative KI: Sie kann helfen, Sicherheitsaufgaben zu automatisieren, Risiken schneller zu erkennen und so den Druck auf überlastete Teams zu mildern. Doch damit diese Technologien wirksam werden, müssen Unternehmen stärker in die Aus- und Weiterbildung investieren und neue Wege finden, Talente für die Branche zu gewinnen – etwa durch gezielte Umschulungen oder attraktivere Karrierepfade für Frauen. Fest steht: Wer die Fachkräftelücke nicht schließt, gefährdet die Resilienz des gesamten Unternehmens. 2025 wird es entscheidend sein, gezielt in Kompetenzen und neue Technologien zu investieren.

„Mein Tipp für 2025 ist: KI + Cybersecurity wird das Hauptthema sein. Insbesondere werden viele neuartige sowie verbesserte Security-Werkzeuge mit KI kommen. Auch die Diskussion, wem KI mehr nutzt, den Angreifern oder den Verteidigern, wird weiter Fahrt aufnehmen.“

Andreas Falk
Senior Consultant
Novatec Consulting GmbH

„Cybersicherheit wird 2025 mit NIS2 und DORA endgültig in der Breite ankommen. Allerdings werden die vielen Nachweise erfordern, dass wir unsere Verwaltungsprozesse, wahrscheinlich mit einer Prise KI, optimaler und intelligenter steuern, um gezielt Entlastung zu schaffen. Mit den weltweiten Spannungen, inklusive der wirtschaftlichen Lage in Deutschland, werden wir alle einen realistischen Blick auf die Bewertung von Bedrohungen und den daraus notwendigen Entscheidungen legen müssen. Gut für jeden, der vorgesorgt hat und weiß a) was er hat, b) welche Bedrohungen für ihn relevant sind und c) wie er sich dagegen zu schützen vermag.“

Désirée Sacher
Geschäftsbereichsleiterin für Operative IT-Sicherheit
Finanz Informatik

Cyberpolicen im Wandel: Wer bleibt, wer geht?

AXA Deutschland hat im Sommer 2024 angekündigt, sich aus dem Cyberversicherungsgeschäft zurückzuziehen und keine Policen mehr für Unternehmen von über fünf Millionen Euro Jahresumsatz anzubieten. Auch bestehende Verträge sollen gekündigt werden. Die steigenden Schadenssummen durch Cyber-Angriffe erschweren für Versicherer die Risikoeinschätzung. Die Gefahr von Kaskadenschäden bei großflächigen Cyberattacken belastet die Bilanzen der Versicherer zusätzlich. Experten spekulieren, dass AXA lediglich den Anfang macht und weitere Versicherer diesem Rückzug folgen könnten, da sich bereits in den letzten Jahren mehrere Anbieter aus dem Cyberversicherungsmarkt zurückgezogen oder ihr Engagement deutlich reduziert haben.

Gleichzeitig treibt die steigende Anzahl und Komplexität von Cyberangriffen die Nachfrage nach Cyberversicherungen voran. Unternehmen erkennen zunehmend die Notwendigkeit, sich gegen finanzielle Schäden abzusichern, die durch Cyberattacken entstehen können. Darüber hinaus können Cyberversicherungen dazu beitragen, das Vertrauen von Kunden und Geschäftspartnern zu stärken. Auch die regulatorischen Anforderungen an die Cybersicherheit nehmen zu: Der Abschluss einer Cyberversicherung kann Unternehmen dabei helfen, zu demonstrieren, dass sie ihre Risiken angemessen managen. Der Rückzug von AXA Deutschland und anderen Versicherern steht somit in Kontrast zu einem wachsenden Bedarf an Lösungen für die Absicherung in einer zunehmend digitalen und bedrohten Welt.

Fazit

Die Bedrohungslage durch DDoS-Attacken bleibt ernst. Unternehmen müssen sich auf eine ständige Weiterentwicklung der Angriffsmethoden einstellen und ihre Sicherheitsmaßnahmen entsprechend anpassen. Investitionen in fortschrittliche Technologien wie DDoS-Schutzlösungen, verbessertes Monitoring, ein robustes Risikomanagement sowie ein solides Compliance-Framework sind entscheidend, um den zunehmenden Bedrohungen wirksam zu begegnen. Die vollständige Einhaltung der strengen EU-Datenschutzgesetze ist dabei unerlässlich.

Kontakt

Michael Scheffler
Vice President Sales

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

link11.com

linkedin.com

LINK11