LINK11

Trends 2026

Web Application Security,
Resilienz, Digitale Souveränität

2025: Cyberangriffe erreichen neue Dimensionen

Die Bedrohung durch DDoS-Angriffe erreichte im Jahr 2025 ein bislang unbekanntes Ausmaß. So haben wir im ersten Halbjahr eine Steigerung der Attacken im Link11-Netzwerk um 225 Prozent gegenüber dem Vorjahr beobachtet. Dabei ist nicht nur die Anzahl, sondern auch die Komplexität und die Größe der Angriffe gestiegen.

Doch die technische Dimension ist nur ein Teil dieser Entwicklung. Politisch motivierte Angriffe, die zunehmend orchestriert und automatisiert durch den Einsatz künstlicher Intelligenz durchgeführt werden, zielten verstärkt auf kritische Infrastrukturen – oftmals im Kontext geopolitischer Spannungen. Die Grenzen zwischen staatlichen Akteuren und Cyberkriminellen verschwimmen zunehmend, während Unternehmen mit wachsenden Angriffsflächen, veralteten Technologien und mangelnder Resilienz kämpfen.

Wendepunkt in der Sicherheitspolitik

Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) betont, dass der Schutz der eigenen Angriffsflächen der Schlüssel zur Stärkung der Cybersicherheit ist. Die Erkenntnis ist klar: Wer seine digitale Widerstandsfähigkeit nicht stärkt, bleibt verwundbar in einem Umfeld, das so professionell, vernetzt und dynamisch ist wie nie zuvor.

Für Unternehmen, Verwaltungen und kritische Infrastrukturen in Europa könnte das Jahr 2026 einen Wendepunkt in der Sicherheitspolitik markieren. Die Bedrohungslage verschärft sich, da Cyberangriffe immer dynamischer, KI-gesteuerter und geopolitisch aufgeladener werden. Gleichzeitig wächst der regulatorische Druck und mit ihm der Bedarf an resilienten, souveränen Sicherheitsarchitekturen.

Ausblick auf 2026

Web Application Security,
Resilienz, Digitale Souveränität

LINK11

Web Application Security der nächsten Generation

Webanwendungen und APIs bilden heute das funktionale Zentrum moderner Geschäftsprozesse: von Login-Mechanismen und Bezahlprozessen bis hin zur Kommunikation zwischen internen und externen Systemen. Gerade deshalb rücken sie zunehmend in den Fokus von Angreifern, die nicht nur technische Schwachstellen ausnutzen, sondern auch Geschäftslogiken gezielt manipulieren. Vor diesem Hintergrund wird WAAP (Web Application and API Protection) zu einem zentralen Baustein digitaler Resilienz.

Im Unterschied zu klassischen WAFs (Web Application Firewalls) vereint WAAP vier Schutzdisziplinen – WAF, DDoS-Abwehr, Bot-Management und API-Schutz – in einer integrierten Plattform. Diese Konsolidierung senkt die Komplexität, verbessert die Bedrohungsanalyse und bietet effektiven Schutz vor kombinierten Angriffen.

Die Weiterentwicklung von WAAP wird durch mehrere Trends geprägt:

- **API-First-Security:** Vollständige Transparenz über alle APIs durch Discovery, Schema-Validierung und Schutz vor Business-Logic-Angriffen, Scraping, Credential Stuffing und API-spezifischen Schwachstellen.
- **Konsolidierung:** Ein einheitliches, plattformbasiertes Modell korreliert Bedrohungen über alle Ebenen und vereinfacht das Management.
- **Positive Security Models:** Erlaubtes Verhalten wird klar definiert, was Zero-Day-Angriffe und neue Exploit-Muster effektiver abwehrt.
- **KI-gestützte Verhaltensanalyse:** ML-basierte Systeme erkennen komplexe Bot-Aktivitäten und Anomalien im API-Verkehr in Echtzeit.
- **DevSecOps-Integration:** Sicherheitsrichtlinien werden als Code verwaltet und automatisiert in CI/CD-Prozesse eingebunden.
- **Client-Side-Security:** Schutz vor Angriffen im Browser, etwa Magecart oder manipulierten Third-Party-Skripten, gewinnt an Bedeutung.

Damit entwickelt sich WAAP zu einem umfassenden Ökosystem, das Webanwendungen, APIs und Nutzerinteraktionen ganzheitlich schützt. In einer Zeit zunehmender Automatisierung und Angriffskomplexität wird es zu einem zentralen Fundament digitaler Sicherheit.

„KI ist ein Beschleuniger – und eine Herausforderung zugleich. Wir nutzen KI-basierte Technologien, um Angriffsmuster in Echtzeit zu erkennen, Anomalien besser zu verstehen und unsere Schutzmechanismen kontinuierlich zu optimieren. Ich halte es jedoch für entscheidend, dass wir KI nicht als „Black Box“ einsetzen. Sicherheit braucht Erklärbarkeit.“

Marc Lamik
Chief Product Officer
Link11

„DDoS-Angriffe werden 2026 nicht nur größer, sondern präziser. Wir sehen eine klare Entwicklung hin zu Multi-Vektor- und API-zentrierten Attacken, die klassische Abwehrmechanismen überfordern. Nur KI-gestützte, cloudnative Schutzsysteme, die Angriffe in Echtzeit erkennen und autonom reagieren, können dieser neuen Dynamik standhalten.“

Jag Bains
VP Solution Engineer
Link11

KI-getriebene DDoS-Dynamik

Auch im Jahr 2026 zählen DDoS-Attacken zu den sichtbarsten und unberechenbarsten Bedrohungen. Während das Volumen und die Frequenz der Angriffe weiter steigen, verändern sich die Attacken grundlegend: KI-gestützte Botnetze agieren autonom, testen Abwehrmechanismen in Echtzeit und wechseln innerhalb von Sekunden ihre Muster. Klassische, signaturbasierte Systeme sind damit überfordert.

Hybride Angriffe auf Layer 3, 4 und 7 werden zum Standard, Hyper-Scale-Attacken über IoT-Botnetze erreichen neue Rekorde und Ransom-DDoS-Kampagnen setzen Unternehmen zusätzlich unter Druck. Gleichzeitig rücken APIs stärker in den Fokus, da Angreifer gezielt ressourcenintensive Endpunkte überlasten, um mit minimalem Aufwand maximale Ausfälle zu erzeugen.

Die Abwehr verlagert sich zunehmend in Always-on- und Cloud-first-Architekturen: Globale, cloudnative Netzwerke mitigieren Angriffe direkt am Edge ab, reduzieren Latenzen und schützen zentrale Systeme vor Überlastung.

Zwei Entwicklungen werden die Zukunft prägen: Erstens wird KI zur Grundlage moderner DDoS-Mitigation, da autonome Systeme Angriffsmuster in Echtzeit erkennen und selbstständig reagieren. Regelbasierte Legacy-Lösungen verlieren dabei schnell an Wirksamkeit. Zweitens dienen DDoS-Attacken immer häufiger als Ablenkungsmanöver für komplexere Vorfälle wie Datendiebstahl oder Malware-Installationen. Security-Teams müssen daher DDoS als Teil mehrstufiger Angriffe betrachten.

Damit wird der DDoS-Schutz im Jahr 2026 zu einem strategischen Sicherheitsfaktor: Unternehmen benötigen automatisierte, vorausschauende und robuste Abwehrsysteme, um der neuen Angriffsdynamik standzuhalten.

Digitale Souveränität im Fokus

Europa steht an einem sicherheitspolitischen Wendepunkt: Die Fähigkeit, zentrale digitale Infrastrukturen und Sicherheitsmechanismen selbst zu kontrollieren, wird im Jahr 2026 ein entscheidender Bestandteil moderner Resilienzstrategien sein. Digitale Souveränität ist längst mehr als ein politisches Versprechen – sie entwickelt sich zu einem operativen Schutzprinzip, das im Ernstfall über die Handlungsfähigkeit eines Staates entscheidet.

Geopolitischer Druck, wirtschaftliche Abhängigkeiten und extraterritoriale Gesetzgebungen zwingen Unternehmen zu einer grundlegenden Neubewertung ihrer Infrastrukturen. Wo werden Daten verarbeitet? Welche Sicherheitsplattformen steuern kritische Abwehrmechanismen? Welche Provider haben im Ernstfall Zugriff auf sensible Systeme? Souveräne Sicherheitsarchitekturen, die auf europäischer Infrastruktur basieren und eine vollständige Kontrolle über Datenflüsse, Schlüsselmanagement und KI-gestützte Schutzmechanismen bieten, werden zunehmend zum Wettbewerbsvorteil – insbesondere für kritische Sektoren wie Energie, Finanzen, Gesundheitswesen und öffentliche Verwaltung.

Was digitale Souveränität 2026 vor allem ausmacht, ist: die Fähigkeit, Angriffe unabhängig, transparent und in Echtzeit abzuwehren – auch unter geopolitischem oder regulatorischem Druck.

„Digitale Souveränität bedeutet vor allem eines: unsere Entscheidungsfreiheit im digitalen Raum zu bewahren. Dafür müssen wir Risiken und Abhängigkeiten realistisch bewerten und viel genauer hinschauen, welche Technologien und Anbieter wir einsetzen. Es geht nicht um Autarkie, sondern um die Fähigkeit, in einer vernetzten Welt handlungsfähig zu bleiben – technisch, rechtlich und strategisch.“

Prof. Dr. Dennis-Kenji Kipker
Research Director and Gründer
des Cyberintelligence.institute

„NIS2, das KRITIS-Dachgesetz und der CRA kommen nicht, um zu nerven, sondern um die Handlungsfähigkeit unserer Wirtschaft zu sichern. Sicherheit ist längst kein Nice-to-have mehr, sondern Daseinsvorsorge.“

Uwe Bergmann
Geschäftsführer
Nethinks GmbH

Regulationsdruck steigt

Parallel zur wachsenden Bedrohungslage intensivieren Regierungen weltweit ihre Regulierungsvorgaben, was spürbare Auswirkungen auf Unternehmen aller Branchen hat. 2026 wird deshalb zum Jahr, in dem Compliance von einer organisatorischen Pflicht zu einem strategischen Erfolgsfaktor wird. Vorgaben wie NIS2, DORA oder die verschärften Meldepflichten setzen klare Erwartungen in Bezug auf Transparenz, Incident Response und sichere Softwareentwicklung.

Insbesondere die verpflichtende 72-Stunden-Benachrichtigung wird die operative Realität vieler Organisationen verändern. Es reicht nicht mehr aus, Angriffe zu erkennen – sie müssen auch sauber dokumentiert, bewertet und mit belastbaren Prozessen gemeldet werden können. Gleichzeitig rückt die Verantwortung der Softwareanbieter stärker in den Fokus. Secure-by-Design, SBOM-Erstellung und die Absicherung von Software-Lieferketten werden regulatorisch eingefordert und verändern die Art und Weise, wie digitale Produkte entwickelt und betrieben werden. Unternehmen müssen Compliance als kontinuierlichen Prozess begreifen, der technologische, organisatorische und strategische Entscheidungen gleichermaßen beeinflusst.

Die Sicherheitsarchitektur von morgen

Organisationen stehen an einem Wendepunkt. Die folgenden Maßnahmen bilden die Grundlage für eine widerstandsfähige Sicherheitsarchitektur:

- **WAAP als festen Bestandteil in der IT-Sicherheit verankern.** Inklusive API-Discovery, Verhaltensanalyse und positiver Sicherheitsmodelle.
- **DDoS-Schutz modernisieren.** Autonome, KI-gestützte Technologien einsetzen, die Multi-Vektor-Angriffe in Echtzeit abwehren.
- **Souveräne Infrastrukturentscheidungen treffen.** Europäische Hosting-Modelle und kontrollierte Sicherheitsplattformen priorisieren.
- **Compliance vereinheitlichen.** Security-Plattformen nutzen, die kontinuierliche Transparenz über Risiken und Vorgaben bieten.
- **Ein Resilienz-Programm auf C-Level verankern.** Cybersicherheit 2026 ist keine technische Frage mehr, sondern Teil der Unternehmensstrategie.

Fazit

2026 wird zur Bewährungsprobe für die digitale Souveränität Europas. Angesichts KI-gesteuerter Cyberattacken und steigender geopolitischer Risiken müssen Unternehmen die Kontrolle über ihre Infrastruktur zurückgewinnen. Sicherheit sollte kein Kostenfaktor mehr sein, sondern das strategische Fundament für Innovation und Wachstum. Wer jetzt auf dynamische, integrierte Sicherheitsarchitekturen, autonome Abwehr und souveräne Technologie setzt, schafft regulatorisch geforderte Transparenz und gewinnt entscheidenden unternehmerischen Handlungsspielraum für nachhaltigen Erfolg.

Kontakt

Michael Scheffler
Vice President Sales

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

link11.com

linkedin.com


LINK11