LINK11

Trends 2025

Cyber resilience through observability, AI, and holistic strategies.

2024: A Year of Record DDoS Attacks

The year 2024 marked a turning point in the world of cyber threats: never before had so many simultaneous DDoS attacks been recorded, nor had they been so massive. The attack by the Mirai botnet with over 2 Tbps on an Asian hosting provider and the largest European attack with 1.4 Tbps, which Link11 successfully defended against, are just two examples of how rapidly the threat level has increased. According to the ENISA Threat Landscape 2024, DDoS attacks now dominate the field of cyber attacks in the EU, accounting for the largest share of recorded incidents at over 40% – even surpassing ransomware and data breaches.

The Influence of Artificial Intelligence

The increasing availability of DDoS-as-a-service offerings and the use of artificial intelligence are major factors behind the growing frequency and sophistications of DDoS attacks. Although difficult to quantify, artificial intelligence (AI) is already being used in a wide range of cyber incidents. The significant increase in attack frequency the unprecedented scale of some DDoS attacks, and the orchestrated execution of multi-vector attacks all point to this influence. However, reverse engineering botnets and attacks is challenging and often temporary, which complicates accurate analysis.

At the same time, there is a clear trend: companies are increasingly relying on agile risk management and AI-based analysis tools to detect threats faster, ensure compliance and strengthen resilience. In 2025, cybersecurity must evolve to become smarter, more agile, and more proactive to withstand increasingly complex threats.

LINK11

Outlook for 2025

New Targets,
More Surveillance,
Stronger Attacks

LINK11

Shift in Targets

Traditional sectors such as gaming and financial services remain attractive targets for cyber-criminals. At the same time, attack scenarios are diversifying. Emerging industries, such as cryptocurrency and biotechnology are increasingly being targeted. Cryptocurrencies draw attention due to their high liquidity and decentralized structures, while the biotechnology sector faces risk due to its concentration of sensitive research data and intellection property. This shift highlights a growing focus on industries with valuable assets and critical business processes.

The geopolitical situation also plays a pivotal role. The willingness to carry out politically motivated attacks on governments and critical infrastructures remains high. Conflicts like those in Ukraine and Israel have led to targeted attacks on state and critical infrastructures. These developments show that cybercriminals are continuously adapting their strategies and exploring new attack vectors.

“In 2025, I expect that geopolitical events in the context of existing or emerging conflicts will continue to resonate in cyberspace – with a further increase in the convergence of criminally and politically motivated attackers, for example in the context of technical tool sharing.”

Dr. Kerstin Zettl-Schabath
Cyber Conflict Researcher
EuRepoC

“What do I expect? A potentially devastating trinity of AI-based attacks, quantum threats, and massive – but not so obvious – state sponsorship.”

Annika Wägenbauer
Innovating Cybersecurity
Advocating for Holistic Security Solutions

Bigger and More Sophisticated DDoS Attacks

DDoS attacks are becoming larger, more frequent, and increasingly complex. The proliferation of IoT devices provides attackers with a near-endless supply of devices to exploit. Modern botnets can now generate unprecedented traffic. As a result, attacks exceeding the 200 Gbps are becoming more common, severely impacting the availability of online services. Companies must prepare this escalation by adapting their security measures accordingly.

The Importance of Observability

The increasing complexity of IT environments requires a comprehensive approach to security. Observability enables companies to analyze their entire IT ecosystem—on-premises, cloud, or hybrid— to detect potential threats early. By continuously monitoring systems, applications, and networks, businesses can identify and respond to anomalies proactively. Beyond perimeter protection, observability provides insights into the impact and workload of attacks, helping companies meet regulatory requirements and improve overall resilience. Integrating observability into DevOps practices ensures closer collaboration between development and operations teams, strengthening end-to-end security.

“While Artificial Intelligence sharpens the sword of cybercriminals, companies can defend themselves through the intelligent use of AI-based technology such as proactive monitoring and automated defenses.”

Jag Bains
VP Solution Engineering
Link11

“Holistic cybersecurity concepts will be essential by 2025 as companies launch comprehensive security programs. Regulations will provide the final push, but it‘s clear that cybersecurity and resilience are built through organization, people, and technology. Comprehensive, C-level-driven initiatives are transforming cybersecurity into a driver of digitalization.”

Rudolf Preuss
Head of IT/OT
Actemium

API Protection: The Achilles Heel in 2025

In 2025, API security will become a cornerstone of cybersecurity strategy, driven by alarming trends. APIs, which control communication between applications, are increasingly targeted by attackers, particularly with the rise of AI systems and microservices.

A recent survey found that 84% of companies in the US, UK, and Germany experiences API security incidents last year. Despite this, fewer than one-third of companies maintain a complete API inventory. This lack of visibility exacerbates vulnerabilities, with API breaches disclosing ten times more data on average than traditional security breaches, according to Gartner,

As we move into 2025, immediate action will be essential for companies. Continuous monitoring, generative AI tools, and comprehensive third-party API monitoring will be crucial in staying ahead of escalating cyber threats.

Intelligent Automation to Bridge the Skills Gap

In 2025, the shortage of skilled cybersecurity professionals will become one of the biggest challenges for cybersecurity in Germany. According to the 2024 ISC2 Cybersecurity Workforce Study, 62% organizations in Germany face staff shortages, and 90% of cybersecurity teams report skills gaps.

Despite rising demand for qualified professionals, the number of available cybersecurity workers has declined from 456,000 in 2023 to 439,000 in 2024. As threats become increasingly complex and regulatory requirements grow, organizations risk overlooking vulnerabilities and leaving themselves exposed to cybercriminals—particularly in key areas like cloud security, AI, and zero-trust architectures. Generative AI offers a silver lining. It can help to automate security tasks, identify risks more efficiently, and alleviate pressure on overstretched teams. However, for these technologies to be effective, companies must invest in training, professional development, and finding new ways to attract and retain talent. A good example would be through targeted retraining or more career paths for women.

“My prediction for 2025 is rather: AI + cybersecurity will be the main topic. In particular, many new and improved security tools will come with AI. The discussion about who benefits more from AI, attackers or defenders, will also continue to gain momentum.“

Andreas Falk
Senior Consultant
Novatec Consulting GmbH

“Cybersecurity will finally arrive on a broad scale in 2025 with NIS2 and DORA. However, the abundance of evidence will require us to manage our administrative processes more optimally and intelligently, probably with a dash of AI, in order to provide targeted relief. With global tensions running high, including the economic situation in Germany, we will all have to take a realistic look at how we assess threats and the decisions we need to make as a result. This is good news for anyone who has taken precautions and knows a) what they have, b) which threats are relevant to them and c) how they can protect themselves against them.”

Désirée Sacher
Head of Operational IT Security
Finanz Informatik

Cyber Policy in Transition

In the summer of 2024, AXA Germany announced its withdrawal from the cyber insurance market for companies with annual turnovers exceeding five million euros, including the termination of existing contracts. The rising costs of damages from cyber attacks have made risk assessment more challenging for insures, and the risk of cascading damage from large-scale attacks further strains their balance sheets. Experts suggest that AXA’s move may signal a broader trend, as several insurers have already withdrawn from or scaled back their cyber insurance offerings in recent years.

At the same time, the increasing number and complexity of cyber attacks are driving demand for cyber insurance. Companies are increasingly aware of the need to protect themselves against financial losses due to cyber attacks. Additionally, cyber insurance can help to build trust with customers and business partners. As regulatory requirements for cyber security grow, obtaining cyber insurance demonstrated that companies are actively managing their risks. The withdrawal of AXA Germany and other insurers highlights the contrast between decreasing availability of coverage and the rising need for protection in an increasable digital and vulnerable world.

Conclusion

The threat of DDoS attacks continues to grow with attack methods constantly evolving. Companies must stay ahead by adapting their security strategies to address emerging threats. Investing in advanced solutions, including DDoS protection, enhanced monitoring, comprehensive risk management, and a solid compliance framework is essential for mitigating these risks. Ensuring full compliance with stringent EU data protection laws is a critical component of safeguarding against evolving cyber threats.

Contact

Michael Scheffler
Vice President Sales

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

link11.com

linkedin.com