Approach Cyber

PRESS RELEASE

Brussels, May 2025

Approach Cyber's 2025 Report Reveals Alarming Spike in Vulnerabilities

Approach Cyber, a leading cyber security company, has published the fifth edition of its highly anticipated Annual Penetration Testing Report, revealing a sharp and troubling rise in critical cyber security vulnerabilities.

The report draws on a hundred real-world penetration tests conducted across 13 sectors in 2024 and provides an unfiltered look into the state of digital defences.

> **"Attackers don't need to exploit zero-days when they can simply act as admin due to access control issues," says Laurent Deheyer, Head of SOC at Approach Cyber.**

Among the most alarming findings:

- **Critical vulnerabilities in web, API, and infrastructures have doubled since 2023.**
- **Nearly 2 out of 5 vulnerabilities pose high to critical risks**, representing a significant threat to organisations due to their potential for causing substantial damage.
- **Low-risk vulnerabilities should not be underestimated**, as they often leveraged to broaden impact of more critical ones. Broken access controls and misconfigured authentication systems dominate the landscape of exploited flaws.

The report includes real-world case studies where our ethical hackers compromised external assets and fully compromised internal networks - demonstrating the same techniques used in major breaches worldwide - with only one client successfully preventing us from obtaining the keys to their digital home.

Infrastructure Weaknesses: Opening Pathways to Digital Compromise

Findings in infrastructure testing underscore fundamental security gaps:

- Outdated software and poor patch management persist.
- Weak authentication and poor network segmentation provide easy access.
- Nearly 60% of infrastructure flaws are rated high or critical.

Regulations vs. Reality

The report warns that many organisations are not ready for the practical impact of regulations like DORA and NIS2, now being enforced in the EU.

“The gap between regulation and real-world security posture suggests many companies are unprepared for the operational, legal, and reputational risks of 2025,” Deheyer adds.

Key Takeaways from the Report

- Recurring clients who undergo regular testing see 70% fewer critical issues than first-time clients.
- Real attack scenarios show predictable, repeatable patterns exploited by threat actors.
- Weak or reused credentials expand the external attack surface, while credential reuse internally amplifies the impact of breaches.

Looking Ahead: 2025 Predictions

- AI-specific vulnerabilities will rise as businesses integrate generative tools.
- Threat intelligence-based ethical red-teaming (TIBER) will become the preferred approach for critical sectors.
- Access control & business logic flaws will remain a top threat vector.
- Supply chain risks, such as Vulnerabilities in third-party libraries and software components, will continue to dominate attacker strategies.

Get the Full Report or Book an Interview

The 2025 Penetration Testing Report is a must-read for CISOs, IT leaders, and journalists covering cybersecurity, regulation, or enterprise risk.

About us

Approach Cyber is a pure-play cyber security and privacy trusted partner, dedicated to bringing cyber serenity to organisations.
With over 25 years of experience, a multidisciplinary team of 100+ experts across Belgium and Switzerland, and ISO 27001 and ISO 27701 certifications, we deliver tailored solutions that safeguard operations, ensure compliance, and protect reputation.
Our comprehensive services include advisory, SOC-driven managed security, and technology integration, ensuring businesses stay secure around the clock.

PRESS CONTACT

Marie-France Rousseau
Marketing and Communication Director

✉ mariefrance.rousseau@approach-cyber.com
☎ +32 498 919 456