22.10.2024 – 11:00 Uhr

Cybersecurity Expert Calls for Increased Penetration Testing

Cybersecurity Expert Calls for Increased Penetration Testing

Keith Poyser: “Blind faith in cyber defence systems without constantly putting them to the test is naive.”

London, October 22 2024 – Penetration testing, i.e. the self-assessment of a company's IT infrastructure to test its cyber resilience, is too often neglected in the business world, warns Keith Poyser, Vice President for EMEA at security company Horizon3.ai. He explains: “You only know how resilient an IT network really is to cyberattacks if you put it to the test. Only penetration tests can determine whether hackers can penetrate from the outside or whether an organisation is actually protected against cyber criminals.”

The security expert cites findings from the Government's *Cyber Security Breaches Survey 2024*, which reveals that 50% of businesses experienced a cyber breach or attack in the past 12 months—a figure that climbs to 70% for medium businesses and 74% for large enterprises. While over 70% of organisations have implemented key security measures such as anti-malware, EDR, DLP, password policies, backups and firewalls, Poyser warns that they underestimate how easily cyber criminals can bypass these defences by exploiting vulnerabilities through social engineering, unpatched software, misconfigurations, poor credential security, and insider threats.

He adds: “Many organisations rely on dozens of cyber defence tools, assuming they are fully protected against external and internal attacks. But this is like flying blind, trusting that everything will work perfectly without active testing. And human led testing only delivers a static snapshot, of a small part of the estate. It may work in calm conditions, but it's naive to think that a purely defensive strategy can withstand the relentless and evolving nature of modern cyber threats.” The security expert urges organisations to adopt a more proactive, automated penetration testing approach in defending against cyber attacks. By doing so, companies can better safeguard their systems, ensure best ROI from their existing investments, and show their boards they are “more secure this week than last week” to meet compliance and regulatory requirements.

Keith Poyser: "Human Risk Is Often Neglected"

According to the Government's *Cyber Security Breaches Survey 2024*, a staggering 95% of cyberattacks succeed because of human error – whether it's opening phishing emails or using weak passwords. While identifying technical vulnerabilities and software flaws is critical, neglecting the human factor leaves organisations equally exposed. Both technical and human vulnerabilities must be addressed to ensure a comprehensive cyber defence. Keith Poyser explains: “Hackers generally analyse *all* publicly available information about a company, its employees and even former employees on social networks, for example, in order to track down security-relevant information.”

Furthermore, he cites “configuration errors due to ignorance or oversight in the defence systems” as another frequently encountered consequence of human weaknesses. “With a myriad of security programmes running at the same time, organisations have often lost track of their associated configurations. The need to constantly update security software alone can be overwhelming for many corporate IT teams, not so much in terms of expertise, but in terms of workload. With each update, the entire configuration has to be re-examined, as the interaction of different systems can lead to new vulnerabilities as soon as one component changes even slightly.”

Given the significant effort required, Poyser recommends that organisations adopt autonomous penetration testing platforms, as they are safer and more cost-effective than relying on traditional teams of experts. He clarifies: “Of course, we still need as many highly qualified specialists as possible, but at the same time we need to increase the level of automation in penetration testing as much as possible in order to cope with the constantly growing threat situation.”

This recommendation is closely aligned with Poyser’s work at Horizon3.ai, which offers NodeZero, a cloud-based penetration testing platform. This solution enables companies to conduct simulated cyberattacks on their internal, external, cloud, and hybrid IT infrastructures, providing a comprehensive assessment of their cyber resilience.

Even the 'Demilitarised Zone' Is No Longer Safe

The frequency and depth of penetration testing are crucial to a robust cybersecurity strategy. It’s not just the external perimeter of IT networks that requires comprehensive testing, but also the internal security. The security expert explains: "With remote work, the Internet of Things, and mobile access, more devices are connecting to company networks from external locations, increasing the potential attack surface. Modern security strategies must assume that hackers will breach the outer defences and gain initial access to a network segment, from which they can then launch internal attacks."

Even the so-called ‘demilitarised zone’ (DMZ), which is considered particularly trustworthy because it is shielded several times from other network segments, can no longer be classified as a secure area in Poyser's experience. “A modern penetration test can examine the entire company network in all its ramifications, internal, external and cloud attack surfaces” he emphasises. “It's not just about identifying vulnerabilities, but also assessing their potential impact. For instance, if a break-in to the DMZ exposes the entire network to a hacker, a thorough penetration test will highlight this risk, allowing for immediate and targeted remediation. Repeated automated tests will allow you to find, fix and verify.”

A Shift in Perspective: The Key to Effective Security

While achieving 100% protection is impossible, this era of machine speed attacks means traditional approaches won’t solve the problem. Simply upgrading defence systems isn’t enough though. To truly safeguard against evolving threats, organisations are advised to regularly assess their security through ongoing machine speed, automated penetration tests. Only by continuously testing and evaluating their defences can organisations stay one step ahead and ensure their systems remain secure, reducing risk and cost.

Poyser, Vice President for EMEA at security company Horizon3.ai, urges companies to "conduct penetration tests regularly to consistently monitor and strengthen their cyber resilience." He adds, "I recommend that every board member, managing director, and IT manager across all industries subject their company to this critical assessment, given the current threat landscape."

* https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

About Horizon3.ai and NodeZero™: Horizon3.ai's NodeZero™ Autonomous Security Platform offers integrated threat detection, autonomous pentesting, third-party risk management, and comprehensive governance, risk, and compliance (GRC) insights. It enhances organisational security by proactively identifying and remediating exploitable vulnerabilities, while strategically deploying deception and threat detection through NodeZero Tripwires™. Founded in 2019 by former industry leaders and U.S. National Security veterans, Horizon3.ai is at the forefront of cybersecurity innovation. Request a free demonstration at: www.horizon3.ai.

Trademark notice: NodeZero is a trademark of Horizon3.ai

Further information: Horizon3.AI Europe GmbH, Sebastian-Kneipp-Str. 41, 60439 Frankfurt am Main, www.horizon3.ai

PR Agency: euromarcom public relations GmbH, www.euromarcom.de, Email: team@euromarcom.de

- - - -

Medieninhalte

Image Source: Horizon3.ai