Financial Service Providers Need to Catch Up on TLPT

Wednesday 30 April, 2025

Keith Poyser on DORA: "A penetration test every three years is ineffective, irrelevant and immediately out of date. Monthly, or weekly testing is far more effective."

London, 30 April 2025 – Since the implementation of the Digital Operational Resilience Act (DORA) on January 17th this year, financial institutions in the EU are required to conduct regular Threat-Led Penetration Testing (TLPT). This involves using real-world cyber-attack techniques to assess IT infrastructures and identify exploitable attack vectors before they are discovered by threat actors. "While this is a positive step, the mandated three-year testing cycle is far too long given the fast-paced nature of cybercrime," said security expert Keith Poyser, Vice President for EMEA at cybersecurity company Horizon3.ai. The company operates the autonomous pentesting platform NodeZero®, where financial service providers can conduct penetration tests on their IT infrastructure, cloud and kubernetes environments, as often as they like to identify potential security gaps. Poyser points to findings from Horizon3.ai's "Cyber Security Report UK 2024/25" according to which 70 percent of organisations questioned have fallen victim to a cyberattack at least once in the past two years.

"Given the increasing frequency of cyberattacks, it is unacceptable for a financial services provider to assess just once every three years whether their IT infrastructure is capable of withstanding an attack or if it will fail," explained Poyser. He further added: "With cybercriminals becoming ever more aggressive, an exploit focused, impact prioritised, high frequency, modern testing regime, with fix actions and re-tests, has to be a key part of any sensible strategy for financial services institutions."

"Like Finding a Needle in a Haystack"

According to the industry veteran, the biggest challenge is identifying which of the vast number of potential IT weaknesses or vulnerability "noise" are real world exploitable within an organisation, and prioritising these for quick remediation. "The list of potential entry points is long, ranging from outdated software somewhere in the system, weak or reused passwords, or excessively broad access rights for individual employees, to threats arising from the software supply chain," explained Poyser, illustrating the scale of the task. He continued: "In this typically heterogeneous and complex IT landscape, finding a security gap is like searching for the proverbial needle in a haystack. Threat actors manage to do it, which is why financial service providers need to use the same methods as cybercriminals to stay one step ahead. And that's exactly what penetration tests are: searching for needles in your own IT haystack before attackers can find them."

Extensive Compliance Requirements

"It's not just about technical protection; compliance is equally important," emphasised cybersecurity expert Keith Poyser. He highlights the extensive obligations for financial service providers under the Digital Operational Resilience Act: ICT risk management, digital operational resilience testing, which includes TLPT, ICT incident reporting, business continuity and emergency management planning, management of ICT third-party risks, and information sharing between entities to collectively enhance resilience.

In relation to all these obligations, financial service providers are subject to increased oversight by national and European authorities, including inspections and audits. "In the event of a serious security incident, the question of how thoroughly the requirements have been implemented at each institution will come to the forefront," Poyser is certain.

"A successful self-attack on one's own IT infrastructure, which is exactly what a penetration test is, provides the best proof of resilience. For this compliance consideration alone, a penetration test is recommended on a monthly, if not weekly, basis."

CTEM und ASM are Key

Cybersecurity leader Poyser strongly recommends extending the Threat-Led Penetration Testing (TLPT) required by DORA to a Continuous Threat Exposure Management (CTEM). This new approach not only continuously monitors the risk but also makes it visible at both the IT level and management level.

A crucial element in this process is Attack Surface Management (ASM), which involves monitoring the portion of the IT infrastructure that is connected to the internet and, therefore, vulnerable to external

Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

Computer :: Cyberattack :: Financial Services ::

Scan Me:

attacks. "In the era of online banking and smartphone apps, continuous ASM is essential for financial service providers," explained Poyser. By integrating the autonomous penetration testing platform NodeZero into their CTEM and ASM strategies, institutions can direct their security efforts towards addressing the actual vulnerabilities that are proven to be exploitable, identified during testing.

Instead of searching for long lists of often low relevance vulnerabilities, Poyser recommends focusing on targeted repairs at critical points. This approach can significantly reduce the so-called Mean Time to Remediation (MTTR), which is the time between discovering a vulnerability and fixing it. In normal practice, this time frame typically ranges from one to three months due to a lack of sufficient staff to fix "all errors at once." However, with NodeZero tests, exploitable weaknesses are prioritised based on their risk to the specific organisation, enabling the IT team to address the most critical entry points for hackers first, and only then tackle the "smaller gaps." The tool then shows how to fix the issue, then re-runs a specific retest to ensure that attack is no longer possible.

"DORA is an important step in the right direction," said Poyser, "but only with significantly shortened pentesting intervals can cybersecurity in the financial sector be made appropriate to the level of criminal energy in the hacker community. And only through an autonomous pentesting platform like NodeZero can this increased frequency be achieved at manageable costs and with a reasonable amount of personnel effort."

For more in-depth insights on DORA and its impact on legal firms and their requirements for demonstrating resilience, read our detailed whitepaper here.

Download your complimentary copy of the 2025 Gartner® Market Guide for Adversarial Exposure Validation here.

About Horizon3.ai and NodeZero: Horizon3.ai provides a cloud-based platform, NodeZero, enabling organisations and public authorities to simulate self-attacks on their IT infrastructure to assess their cyber resilience through penetration testing (pentesting). Thanks to its cloud model, the platform offers affordable, regular pentesting, making it accessible to mid-sized companies. Horizon3.ai continuously monitors the cybercrime landscape to ensure that newly discovered vulnerabilities are swiftly integrated into the cloud system. NodeZero not only identifies security flaws but also offers tailored recommendations for remediation. Through this platform, Horizon3.ai helps organisations meet rising regulatory demands for cyber resilience in Governance, Risk & Compliance (GRC), with guidelines recommending an internal self-attack at least once a week.

Trademark notice: NodeZero is a trademark of Horizon3.ai

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

PR Agency: euromarcom public relations GmbH, Tel. +49 611 973150, Web: www.euromarcom.de, E-Mail: team@euromarcom.de

Company Contact:

_

news aktuell

E. desk@newsaktuell.de
W. https://www.newsaktuell.de/

View Online

Newsroom: Visit our Newsroom for all the latest stories:
https://www.newsaktuell.pressat.co.uk