23.01.2024 – 11:57 Uhr

ECB chases Banks in Cyber Stress Test: Autonomous Penetration Testing contributes to European Financial Security

ECB chases Banks in Cyber Stress Test: Autonomous Penetration Testing contributes to European Financial Security

“IT teams around the world must learn to think and act like hackers.” - Rainer M. Richter, Horizon3.ai

Frankfurt / San Francisco, January, 23rd, 2024 – The banking supervisory authority of the European Central Bank (ECB) has begun testing the resilience of banks' IT systems with a large-scale test at around 100 banks in the euro zone. “The ECB's initiative is very welcome and speaks for one thing above all: the paradigm shift in IT security away from purely reactive defense," explains Rainer M. Richter, long-time specialist in IT security and Vice President EMEA & APAC at Horizon3.ai. With NodeZero, Horizon3.ai has developed professional penetration testing into an autonomous SaaS platform that can be used to test IT infrastructures around the clock using the latest hacking methods. The solution could make a significant contribution to European and global financial security, even anticipating further ECB stress tests to verify the security and integrity of financial institutions. "IT teams around the world need to learn to think and act like hackers. This is the only way to find vulnerabilities before hackers exploit them and IT teams are stuck on the defensive," continues Rainer M. Richter of Horizon3.ai.

Spot checks leave room for vulnerabilities

The ECB's tests, which were previously scheduled for a few days and are always announced, leave plenty of room for vulnerabilities: "The attack vectors of the increasingly commercialized hacker gangs are dynamic and include several forms of attacks, for example to capture access data and use criminal engineering to gain insight into the penetration of infrastructures. Conditions change with every update to a network component, and only continuous penetration testing offers maximum security. This cannot be achieved without the technological support of an autonomous pentest solution like NodeZero," says Rainer M. Richter of Horizon3.ai. The financial sector also has to meet the requirements of the EU Regulation 2022/2554 on Digital Operational Resilience in the Financial Sector (Digital Operational Resilience Act - DORA). DORA requires testing of various threat scenarios at least once a year. The German regulator, the Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), also wants banks and insurance companies to implement defenses internally rather than outsourcing them to multi-tenant service providers.

GDPR-compliance and permanent security

Horizon3.ai's NodeZero performs an autonomous penetration test of the entire infrastructure - with no significant loss of performance, daily checks can be performed to determine if there are any vulnerabilities that can be exploited by hackers. Once the vulnerabilities have been fixed, it is immediately possible to check whether the measure was successful. Horizon3.ai calls this principle "find, fix and verify". A pentest can be safely initiated at any time against production systems – both software and hardware - to ensure the integrity of the network. NodeZero is made available in Germany and Europe in full compliance with data protection regulations. "We only use server capacity in Frankfurt for our German and European customers. Another advantage of using NodeZero is that no hardware needs to be integrated into the network to use the platform. The entire platform is a SaaS service and can be administered by a company's internal IT staff via a web interface," says Rainer M. Richter. The focus is on ease of use to provide IT teams, CIOs, CISOs and administrators with detailed analysis of attack vectors with proof of exploitation and prioritized remediation.

About Horizon3.ai and NodeZero

Horizon3.ai's NodeZero™ SaaS platform enables organizations to continuously find, fix, and verify exploitable vulnerabilities in their IT infrastructure with autonomous penetration testing. NodeZero is the flagship product of Horizon3.ai, a company founded in 2019 by seasoned industry and national security veterans. Our mission is to help organizations see their networks through the eyes of the attacker, and proactively remediate issues that previously went undetected and posed a major security risk. This can improve the effectiveness of all security measures, while IT managers can ensure they are prepared for real cyber attacks.

Visit https://www.horizon3.ai/ for a free trial.

Contact: Horizon3.AI Europe GmbH,
Sebastian-Kneipp-Straße 41, 60439 Frankfurt am Main, Germany,
Web: www.horizon3.ai

PR-agency: euromarcom public relations GmbH,
Muehlhohle 2, 65205 Wiesbaden, Germany,
Tel.: +49 611 973150, E-Mail: team@euromarcom.de,
Web: www.euromarcom.de

- - - -