21.05.2024 – 08:00 Uhr

Cybersecurity: Self-attack is the best Defence

Cybersecurity: Self-attack is the best Defence

Security expert: "Companies should regularly attack themselves to test their cyber resilience."

Rainer M. Richter: "Today's autonomous penetration testing solutions from the cloud are affordable for every medium-sized company."

With the surge of cyber threats in 2023, European companies must seek proactive solutions to confront their system security challenges.

Frankfurt am Main, May 21 2024 – When it comes to cybersecurity, the economy is relying too heavily on defensive measures and neglecting self-assessments using autonomous penetration testing solutions to assess its cyber resilience. This is the criticism of Rainer M. Richter, Head of Europe and Asia at the cybersecurity company Horizon3.ai. He points out that the European Central Bank (ECB) has been conducting stress tests to measure cyber resilience in the financial sector for years. "Companies in all sectors would be well advised to voluntarily undergo regular stress tests," Rainer M. Richter advises.

In a stress test, known in technical jargon as a "penetration test" or "pentest" for short, so-called white hat hackers are hired by the company to crack into its own computer network to uncover vulnerabilities and other weaknesses. Rainer M. Richter points out: "White hat hackers are no longer needed because there are autonomous pentesting solutions used for stress testing that are available from the cloud at a reasonable price. The German Federal Office for Information Security (BSI) writes in its 2023 situation report "The threat from cybercrime is higher than ever before.", underscoring the urgent need for robust cybersecurity measures.

Increasing demands for measuring Cyber Resilience

Rainer M. Richter points to the increasing demands being placed on the economy in terms of cyber resilience as a result of ever more stringent EU legislation. In addition to specific security requirements for the financial sector, many other sectors of the economy that are part of the “European Programme for Critical Infrastructure Protection” (EPCIP) are affected, says Rainer M. Richter. As an example, he cites the new NIS2 (Network and Information Security) Directive, the EU-wide legislation on cybersecurity that came into force in 2023. Cyber risks exist not only within a company's own operations, but also with suppliers and distribution partners, emphasises security expert Rainer M. Richter. He points out: "An attack on a business partner or supplier can spread directly to all associated companies. That's why NIS2 covers the entire supply chain.

However, security breaches can also be fatal for companies that are not EPCIP-rated, Rainer M. Richter points out. He explains: "When a company, regardless of sector or size, falls victim to a cyber attack, it not only can cause significant damage, but also raises the question of who's to blame. Board members and managing directors who neglect the issue of cyber security will find themselves with one foot, if not both, in court".

Pentests are "affordable for every SME"

The security expert emphasises that autonomous pentests from the cloud are "affordable for every medium-sized company". "The costs scale with the number of workstations and the size of the computer network," Rainer M. Richter adds. According to him, the operation is so simple that the pentest procedure, which was originally developed primarily for the corporate world, can now also be easily used by SMEs without having to hire external hackers.

The pentest costs must also be considered alongside the potential financial repercussions of cyber attacks, stresses the security expert. With the European Union Agency for Cybersecurity (ENISA) estimating the total annual cost of cybercrime to the EU economy at approximately 180 billion Euros*, investing in pentesting solutions becomes a prudent financial decision, offering invaluable protection against devastating losses.

Checking all connected devices and machines

In addition to the low cost and ease of use, he categorises the fact that cloud-based pentesting solutions can also assess other connected machines and devices in the test as a further advantage. "If hackers take control of the security cameras on the factory premises, it jeopardises the security of the entire company," says Rainer M. Richter, giving a concrete example of how the call for greater cyber resilience extends far beyond companies' computer systems.

What's more, the time between the discovery of a security vulnerability and its exploitation by criminals is becoming increasingly shorter. As a result, companies have less and less time to check whether their own computer networks are at risk. "Given the complexity of today's IT landscapes, it is basically impossible for companies to determine in good time whether they are potentially affected by every new vulnerability that emerges, not to mention the enormous costs involved," analyses Rainer M. Richter.

Home working and AI driving attack scenarios

Companies of all sizes are too careless, warns Rainer M. Richter. Most IT departments have long since lost track of all the potential vulnerabilities in their computer networks, says the security expert. This is understandable "because computer and network constellations are becoming increasingly complex, and attacks are becoming more sophisticated and faster". Rainer M. Richter has identified two main drivers for the rapid growth of cybercrime: the trend towards working from home, which is integrating more and more poorly secured PCs into corporate structures, and the weaponization of artificial intelligence (AI), which is making cyber-attacks "faster and more dangerous than ever before".

As Horizon3.ai has discovered in attack scenarios commissioned by companies using its own autonomous pentest platform, NodeZero™, companies' defences can usually be breached within minutes. According to the company, NodeZero also uses Open-Source Intelligence (OSINT) to exploit human weaknesses, such as when an employee reveals the name of their dog on social networking sites and uses it as a password for the company network. "Typically, a single vulnerability is all it takes for attackers to gain access to a company's digital infrastructure," says Horizon3.ai's head of Europe and Asia.

Europe: Epicenter of 2023 Cyber Threats

Rainer M. Richter is certain that the majority of businesses are well aware of the threat situation, but are relying solely on defensive measures alone. "Many companies have 20 to 40 separate security systems running at the same time to defend against cyber attacks, but have no way of measuring how well they will work when the company comes under attack," says Rainer M. Richter. He refers to the IBM Security X-Force Threat Intelligence Index 2024, according to which Europe was the most frequently attacked region in the world.** "Given the heightened risk of cyber attacks, stress tests, i.e. penetration tests, are recommended every day, but definitely once a week," advises the expert.

Many companies rely on so-called vulnerability scanners to uncover know vulnerabilities in the software they use, but the feeling of security associated with this is deceptive, says Rainer M. Richter. The scanners do find vulnerabilities that should be patched; however, they do not assess the ‘exploitability’ of such vulnerabilities. "No IT department is in a position to plug all the security gaps that become known," says Rainer M. Richter. “Rather, it is important to focus on the vulnerabilities and weaknesses that can be exploited by attackers. This focus is only possible by using solutions like NodeZero that are designed to safely attack your own company, because only then will the relevant risks come to light," emphasises Rainer M. Richter.

The security expert quotes from the BSI status report on IT security in Germany, which states: "The BSI is observing a shift in attacks involving cyberattacks with ransomware: The focus is no longer only on large, solvent companies, but increasingly also on small and medium-sized organisations as well as state institutions and local authorities. The citizens of our country are often directly affected by successful cyberattacks on municipal administrations and municipal businesses in particular: this can result in citizen-centred services being unavailable for a period of time or personal data falling into the hands of criminals."***

*https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

**https://www.ibm.com/reports/threat-intelligence

*** https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

About Horizon3.ai and NodeZero: Horizon3.ai offers a cloud-based platform called NodeZero that enables companies and public authorities to carry out continuous self-assessments on their IT infrastructure to check their cyber resilience (known as penetration tests or pentests). The costs are low due to the cloud concept, making regular pentesting affordable even for medium-sized companies. Horizon3.ai constantly analyses emerging vulnerabilities and adds new attack content to NodeZero so companies can uncover their truly exploitable issues. Once identified, NodeZero also provides specific advice on how to rectify them. With this platform, Horizon3.ai helps companies and authorities to fulfil the increasing regulatory requirements for measuring cyber resilience, which suggest that a self-assessment should be carried out in-house at least once a week. Free trial version: www.horizon3.ai.

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

PR Agency: euromarcom public relations GmbH,
Mühlhohle 2, 65205 Wiesbaden, Deutschland,
Phone: +49 611 973150, Email: team@euromarcom.de,
Web: www.euromarcom.de

- - - -