29.05.2024 – 10:45 Uhr

New Rapid Response Service against current Cyber Threats

New Rapid Response Service against current Cyber Threats

- **Enables organisations to immediately check which new vulnerabilities affect them**
- **Significant cost savings as only the vulnerabilities that affect the organisation are patched**

Frankfurt am Main, 29 May, 2024 - According to the Qualys Trurisk Research Report, 26,447 vulnerabilities were reported in 2023*, leaving organisations asking the question: Could we be affected, too?

"Given the complexity of computer and network environments, plus the sheer number of vulnerabilities being discovered in today's software, no organisation has the ability to completely defend against a highly targeted attack," says Rainer M. Richter, Head of Europe and Asia at security company Horizon3.ai. He hopes to remedy this with the new "Rapid Response Service", which works quite simply - with a self-attack on the organization itself, using currently discovered vulnerabilities. "Within a few minutes, you can see whether your organization is affected, and which remedial measures are urgently recommended," says security expert Rainer M. Richter.

Attack team continuously uncovers vulnerabilities

Horizon3.ai maintains an attack team that both identifies software vulnerabilities itself and continuously monitors vulnerability publications from other sources. Each new potential entry point for hackers is assessed for its ease of exploitation, and if warranted, is added to the Horizon3.ai's NodeZero penetration testing platform. From this platform, organisations can launch an autonomous self-attack ("penetration") on their own computers and networks to find out which current vulnerabilities affect them. "Instead of trying in vain to close all potential security holes, NodeZero allows organizations to test which ones they are actually vulnerable to and focus on those," explains Rainer M. Richter.

The new Rapid Response Service ensures that organizations are notified immediately when the attack team discovers a new vulnerability and adds it to NodeZero. This allows organizations to test their own IT infrastructure for the current hacker gateway and fix it, if necessary, often before the vulnerability becomes public knowledge.

"The time advantage, which often amounts to several days, can make the difference between an organization falling victim to a hacking attack and all that entails, or being able to protect itself in good time," says Rainer M. Richter. He describes the new service as a "proactive defence mechanism for the pre-emptive mitigation of newly discovered vulnerabilities before they are fully exploited by threat actors".

In technical jargon, there are two types of vulnerabilities: zero-days and n-days. The former is a potential security vulnerability for which a workaround (patch) is not yet available. The second is a known vulnerability that has a patch, but it has not yet been applied.

"The window of opportunity between the public disclosure of a vulnerability and its exploitation by criminals is getting smaller and smaller. It is therefore becoming increasingly important to fix the vulnerabilities that are actively being exploited by threat actors as quickly as possible," says Rainer M. Richter, emphasising the benefits of the new Rapid Response Service.

Increases security, reduces costs

Horizon3.ai argues that self-attacking to assess if an organization is at risk not only strengthens security, but also reduces the massive costs that organizations are spending today to protect themselves against cybercrime. In a study commissioned by the company last year entitled "The Total Economic ImpactTM of the NodeZero Platform, October 2023", Forrester Consulting concluded in a sample calculation that a company with 2,000 employees and an annual turnover of 455 million euros would benefit financially from NodeZero to the tune of almost one million euros within three years. Rainer M. Richter points out: "This doesn't even include the potential damage of an actual attack."

The security expert notes that in the face of an ever-increasing threat landscape, organizations "spend time and money trying to close all possible security gaps without even knowing whether their own organization is actually at risk". Whether or not a software vulnerability actually poses a threat depends on the computer and network configuration, which is different for every organisation. "This is why self-attacking your own infrastructure is basically the only way to find out which software vulnerabilities should be dealt with as quickly as possible and which can safely be ignored," concludes Rainer M. Richter.

* https://www.qualys.com/tru/

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.

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,
Phone: 0611/97315-0, Web: www.euromarcom.de,
Email: team@euromarcom.de

- - - -