Horizon3.AI Europe GmbH

25.11.2024 – 10:22 Uhr

Cybersecurity Under Threat: New Study Exposes 'Security Chaos'

London (ots) -

- **'Cyber Security Report 2024/2025' by Horizon3.ai for the United Kingdom**
- **Cybersecurity Expert Keith Poyser sounds alarm over "Security Chaos in UK Organisations": "Almost two-thirds of companies in the UK have been targeted by hackers at least once in the past two years. Nearly half have experienced two or more cyberattacks in that time. Shockingly, almost a quarter are unaware if they've even been breached. The growing gap between the level of threat and the protection in place is a serious concern for organisations across the country."**

70 percent of companies in the UK have fallen victim to a cyberattack at least once in the past two years. This is according to the "Cyber Security Report UK 2024/25" by security firm Horizon3.ai.

For the report, a sample of 100 UK-based companies was surveyed. According to the findings, 53 percent of companies reported a specific incident of damage. 16 percent detected a hacker attack but claimed to have successfully defended against it. 23 percent of the companies contacted by Horizon3.ai were unsure whether they had been the victim of a cyberattack in the past 24 months. Only 8 percent of companies stated, "We are certain that we were not attacked."

Nearly Half of Companies Targeted by Two or More Cyberattacks

Nearly half of the companies (44 percent) were targeted by a cyberattack twice or more during the two-year period examined, according to the "Cyber Security Report UK 2024/2025."

"The true extent of the issue is likely far greater," warns Keith Poyser, Vice President for EMEA at cybersecurity firm Horizon3.ai, which conducted the study, pointing to the near quarter of respondents unaware of any cyberattacks. He continues, "With almost 20,000 new vulnerabilities in software identified by the European Union Agency for Cybersecurity (ENISA) in just one year, alongside the increasing complexity of IT and network environments, many organisations have lost sight of how vulnerable they truly are and how frequently they are targeted. There are numerous instances where attackers have silently infiltrated corporate networks for months, extracting sensitive data without being detected. It's only when an attack disrupts operations or a ransom demand appears that many companies become aware of the breach."

Downtime, Financial Losses, Legal Consequences, and Data Theft

According to the "Cyber Security Report DACH 2024/2025," 62 percent of the surveyed organisations experienced downtime due to a cyberattack over the two-year period examined. 42 percent (multiple answers were allowed) suffered financial losses as a result. 15 percent faced legal consequences, while data theft occurred in 35 percent of cases. Alarmingly, 54 percent of companies received a ransom demand to recover data encrypted by hackers.

Cybersecurity expert Keith Poyser is concerned: "Many executives, CEOs, and IT leaders seem unaware of the potential damage that cyberattacks can cause to their organisations. The consequences can escalate exponentially, negatively impacting every part of the organisation. Both the financial losses and the resources required for recovery can inflict significant harm. UK companies working with EU partners must also be aware that they are subject to European regulations like NIS2 and risk operational disruptions if they fail to meet cybersecurity compliance standards."

Key Executives' Lack of Understanding of Risks and Their Personal and Corporate Impact

The participants selected for the survey predominantly hold responsible positions within their companies: IT team leaders (21 percent), Chief Information Security Officers (18 percent), Chief Technology Officers (14 percent), Chief Information Officers, and IT Managers (12 percent each). "According to the survey, more than half of the executives who would be personally affected in the event of a cyber incident do not believe they could be held liable for potential damage," says Keith Poyser, highlighting the lack of understanding among key executives about the risks and their potential personal and corporate impact.

The cybersecurity expert warns: "Organisations must urgently step up their efforts on cybersecurity. With artificial intelligence driving increasingly rapid and aggressive cyberattacks, and the growing use of remote work and the increase of Internet of Things (IoT) devices being connected to corporate networks, the opportunities for threat actors are expanding. The gap between the growing threats and the level of protection organisations have in place is widening at an alarming rate."

Keith Poyser advises organisations to "conduct penetration tests frequently to continuously assess their cyber resilience." A penetration test involves a company-commissioned simulated attack to identify security vulnerabilities. In the financial sector, the European banking regulator regularly conducts penetration tests, known as "stress tests," to assess financial institutions' ability to defend against cyberattacks. "I recommend that every board member, CEO, and IT leader across all industries subject their company to such a rigorous test," says the Vice President for EMEA at Horizon3.ai, whose company operates NodeZero, a platform aimed at making these penetration tests accessible and affordable for mid-sized organisations.

About Horizon3.ai and NodeZero: Horizon3.ai provides a cloud-based platform, NodeZero, enabling organisations and public authorities to simulate self-assessments 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-assessment at least once a week.

Contact:

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