UK Companies Face Increasing Cyber Security Risks Across a Range of Threats, New Report Reveals

Monday 16 December, 2024

- **‘Cyber Security Report 2024/2025’ by Horizon3.ai for the United Kingdom**
- **"Thinking that software can be made completely invulnerable or that conventional cyber security defences are sufficient is a common misjudgement," warns cyber security expert Keith Poyser. "Most organisations today use dozens, if not hundreds, of software applications and solutions, creating an expansive attack surface. A vulnerability remains harmless only until a hacker uncovers how to exploit it. Real world exploitable vulnerabilities are chained together to form effective attack paths, with clear business impact. This very real risk presents numerous potential threats, underscoring the importance for companies to strengthen their defences before an attack occurs, across all attack surfaces…and that means testing from an attacker's perspective."**

London, December 16 2024 – Hackers employ a wide range of tactics, techniques, and procedures to exploit vulnerabilities in software. At the same time, they use targeted phishing attacks, third-party data breaches, and open-source information (OSINT) to gain access to a user’s credentials, which can provide the much needed gateway to valuable systems and data. This is a key takeaway from the "Cyber Security Report UK 2024/25" by Horizon3.ai, which surveyed 150 organisations across the United Kingdom. The findings reveal that almost half of these organisations (48%) regard stolen user and admin credentials as one of the most significant cyber security threats they face. Additionally, an overwhelming 42% of respondents (who could select multiple threats) identify insufficiently secured data and/or unknown data stores as a significant potential risk to their organisations.

Another key finding reveals that more than a quarter (29%) of companies consider attacks via unpatched but known security vulnerabilities in corporate networks to be a major threat. These are software vulnerabilities that are already known, with a patch available from the vendor, but have yet to be patched by the companies using the software. An additional 27% are concerned about incorrectly configured software and/or hardware devices as a source of potential risk to their organisations. "These issues are a prime opportunity for cybercriminals. At the end of the day, a considerable proportion of the successful cyberattacks are the result of human error," Keith Poyser, Vice President for EMEA at cyber security company Horizon3.ai, explains.

Penetration Testing as a Solution to Cyber Threats

“With hundreds of programmes in use, most organisations can no longer keep up with the vulnerabilities being discovered in the software they use, plus the other security gaps that emerge almost daily," says Poyser. To address this, he recommends continuous penetration testing—self-assessments of an organisation’s infrastructure to identify vulnerabilities and other weaknesses in advance. According to the survey, nearly a third of organisations (32%) do not conduct penetration tests. “Autonomous penetration tests are easy to implement, cost-effective, and most importantly, proactively test your environment from an attacker’s perspective —exactly what is needed in the face of the rapidly increasing cybercrime threat,” argues Poyser.

The "Cyber Security Report UK 2024/25" underscores the growing severity of cyber threats: 69% of the companies surveyed revealed they had fallen victim to a cyberattack at least once in the past two years. The survey, which gathered insights from 150 executives and IT professionals, covers a diverse range of industries and critical infrastructures, including telecommunications, manufacturing, automotive, healthcare, education, and research.

Diverse Cyber Threats Pose Growing Challenges to Organisations

Other potential threats identified by the surveyed executives include: Zero-day and/or N-day vulnerabilities (20%), poor or inadequate security controls (16%), shadow IT—using software or hardware unknown to the company’s IT team (14%), weak and/or unenforced security policies (5%), insufficient security budgets (4%), and little or no attention to security (2%).

"Managers are recognising that a combination of cyber risks within their organisations is becoming increasingly difficult to manage," says security expert Keith Poyser. In his view, a a solution is clear: "Companies must regularly test the security of their IT infrastructures through self-initiated attacks in the

Related Sectors:

Business & Finance :: Computing & Telecoms ::

Related Keywords:

Computer :: Software :: IT Security ::

Scan Me:

form of continuous, autonomous penetration testing that focuses on real world exploitable attack paths, prioritises, shows remediation and then verifies that the attack path is fixed. Simulation and vulnerability scanning had their place, but real world, production environment testing is what is needed for modern threats."

Cyberattacks Threaten Business Continuity and Financial Stability

"It is no surprise that Richard Horne of the NCSC recently issued such a stark warning on cyber security," says Poyser. The new CEO of the National Cyber Security Centre (NCSC) said in a recent speech that cyber risk in the UK is "widely underestimated" and that the gap between the exposure and threat we face and the defenses that are in place to protect us is widening. "The increasing frequency and complexity of these attacks highlights the urgent need for organisations to strengthen their cyber security defences and remediate exploitable weaknesses to protect themselves from financial and reputational damage," adds Poyser.

If critical data falls into the hands of cybercriminals, it can result in major outages and significant financial losses. This is evident as 62% and 54% of surveyed companies reported experiencing downtime and ransom demands, respectively. Additionally, the costs associated with data recovery are considerable, alongside the extra workload and potential legal ramifications for the business. Data breaches are especially damaging to critical infrastructures, as they can compromise the functionality of vital systems.

Majority of Companies Underequipped Against Attacks

Shocking 66% of the surveyed companies admitted that they have little to no adequate protection against cyberattacks, while only 17% have taken measures but consider them insufficient. Just 9% were confident that their protection against cyberattacks is complete.

"These results show that while awareness of the importance of robust protection against cyberattacks is growing, resources to meet the challenge are often lacking. For years, cyber security has been defined by defensive and reactive measures that are simply too slow in an environment of aggressive, increasingly AI-driven cyberattacks," says Keith Poyser. Instead, the security expert is urging organisations to adopt a more proactive approach in order to stay one step ahead of cybercriminals. This is the only way companies can effectively protect their systems and deal with the ever-growing threats in cyberspace.

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.

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