60% of UK workers affected by some kind of cyberattack, but only 10% consider it their problem, shows Armis research

Armis analysed the public perception of cybersecurity and cyber resilience to understand the public's cybersecurity awareness

Armis Security

LONDON, UK, December 16, 2021 /EINPresswire.com/ -- Armis, the leading unified asset visibility and security platform provider, has today released the findings of a nationwide study of 2,000 UK employees that analysed their thoughts on the country's cyber resilience and their own attitudes to security.

The results demonstrate the lack of awareness towards cybersecurity in the UK. Despite 60% admitting to having been impacted by a cyber-attack, the study found a general lack of awareness towards cybersecurity, revealing that only 27% are aware of the associated risks, while 1 in 10 (11%) admitted to not worrying about them at all and the same amount confessing that cybersecurity is someone else's problem.

Unfortunately, the public's confidence in the government to prevent large-scale cyber-attacks appears to be divided as well. In fact, just over half are confident, whilst the remaining 45% are either not confident at all or are unsure, while 30% confessed to thinking the UK is more equipped to deal with another pandemic over a cyber-attack.

Other key findings include:
- The top three worries for the UK's future were:
- Economic recession (54%)
- Another pandemic (50%)
- Climate change (48%)
- A large-scale cyber-attack on the UK's critical infrastructure came in fourth at 21%
- 21% of the UK workforce thinks Britain going to war is as much of a worry as the country facing

a large-scale cyberattack on its critical infrastructure
- 46% said the UK is more capable to deal with a cyberattack since leaving the EU, 34% said less capable, and 1 in 5 didn't know
- 1 in 5 (20%) people will pay for online security (AV/password manager etc) while 1 in 3 (33%) pay for home security, 1 in 4 (25%) for car security and 1 in 4 (25%) for phone security
- 1 in 5 (20%) think Russian-backed cybercriminals are the biggest threat to the UK's cybersecurity, followed by financially motivated cybercriminals (17%) and Chinese-backed cybercriminals (16%)

The pandemic saw a spike in cyberattacks on both organisations and individual people, with ransomware attacks alone doubling over the course of the past year. The survey also revealed that 27% of workers had experienced a phishing attack on themselves or their organisations, while 23% suffered a data breach and 20% experienced malware. Insufficient cyber resilience puts UK organisations and individuals at a high risk of falling victim to cyber criminals and suffering immense damage when it comes to business operations and reputation. With the increase in threats, the public are relying more on the government to provide support, resulting in 40% believing that a minister for cybersecurity should be instated to focus more on the issue.

Andy Norton, Chief Cyber Risk Officer at Armis commented: "It's alarming to think that so many individuals will pay extra to invest in home, car or phone security yet will refuse to protect their online identities. With remote working and so much of ourselves being stored online, individuals risk being targeted in a variety of scams and attacks. To make matters worse, with only 1 in 5 people paying for online security, organisations are put at risk of breach as attackers can use individual devices and accounts to gain access to corporate networks."

"It's clear that cybersecurity awareness and training must be made a priority within the UK government," said Conor Coughlan, CAO and General Manager for EMEA at Armis. "This is an issue that must be addressed from the top down. Moving forward, more emphasis should be placed on security awareness training as well as technology controls that give organisations a full picture of risk exposure. Organisations need to understand the importance of investing in the right security to protect themselves and their customers and to avoid experiencing any downtime."

About Armis
Armis the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

Bethany Smith
Armis
email us here
Visit us on social media:
Facebook
Twitter
LinkedIn
Other
