Anticipating the attacks: 92% of enterprises unprepared for security challenges of AI wave

92 per cent of enterprise PCs are left vulnerable amidst the AI revolution, according to new research from Absolute Security, a leading cybersecurity professional solutions provider.

Temps de lecture : minute

18 April 2024

No matter how untouchable we think we are, we will never be fully prepared for all the catastrophes we will encounter throughout our life, which doesn't mean we cannot try to be as ready as possible.

This is reflected early-on in our education. Take for example the post-it on the side of the fridge, on which our parents wrote down the emergency numbers. What seemed to be a random series of numbers when we were children turned out to be an invaluable piece of information once reached adulthood.

Not only what we do, but what we create also comes with risks. Mankind's inventions, no matter how useful, altruistic and convenient, will always come with their share of challenges. Cars allowed us to travel the world and free ourselves from the invisible borders surrounding our neighbourhoods, but we later came to create speed limits, road safety rules, security belts, airbags, to protect ourselves and others.

Even if the AI wave is deluging the world with innovation, irrigating the realm of possibilities and breaking the dams forced upon us by previous technological limitations, it also comes with its share of risks, such as

flooding the world in cyber attacks.

To help us better understand and anticipate the potential dangers brought by AI, *Absolute Security*, a leading cybersecurity professional solutions provider, analysed data from over 5 million end point devices to create the *'Absolute Security Cyber Resilience Risk Index 2024' report*.

New technology requires new equipment

Despite the rush to leverage AI on endpoints, the report highlights that 92% of PCs have insufficient RAM capacity that leading industry groups say is needed to support it. Organisations that want to take advantage of AI will need to replace entire devices, requiring them to ensure that mass deployments can remain secure against threats, and compliant with internal and external security policies.

The research also revealed that most industries continue to run weeks, even months, behind in patching software vulnerabilities, endpoints remain vulnerable to threats, and most enterprise PCs will need to be replaced to support AI-based technologies. All factors creating numerous compliance and security challenges. Education and government are the top sectors with the worst patching records, taking 119 and 82 days respectively to patch.

Adapting before Adopting

> *"As an industry we are intently focused on the inevitable attack coming, breach waiting to happen, and disruption around the next corner. Not enough attention is paid to the simple strategies that can dramatically increase your*

> *resilience to ensure you remain resistant to vulnerabilities and can recover quickly." says Christy Wyatt, CEO of Absolute Security*

Another concern the report highlights is that when not supported by automated remediation technologies, PC Endpoint Protection Platforms (EPP) and network access security applications fail to operate effectively 24% of the time. On almost 14% of devices, unsupported EPPs are not even present, opening high-risk security gaps.

"Cyber Resilience is a paradigm that extends beyond traditional cybersecurity. It's about ensuring that your digital operations, which are the heart of your organisation, can withstand and quickly recover from cyberattacks, technical malfunctions, deliberate tampering, and new deployments.” adds Christy.

Article by Paul Ferretti