As AI advances, cyber threats increase. Are businesses prepared to handle the situation?

To protect vital business data from ransomware attacks, it is imperative to identify key vulnerabilities and develop comprehensive defences to protect the organisations, and recovery plans in the event of an attack. According to Kyocera, this is even more crucial as cybercriminals leverage AI to ever greater effect when constructing and carrying out their campaigns.

Temps de lecture : minute

19 July 2024

According to a recent whitepaper report, *Building a Cyber-Resilient Data Recovery Strategy* by Veeam, businesses will continue to be at high risk for emerging cyber threats until they establish practical frameworks for ransomware protection and minimise the chances of falling prey to cybercriminals.

Andrew Smith, Chief Information & Strategy Officer at *Kyocera Document Solutions U.K.* commented: "Planning is crucial when it comes to cybersecurity for businesses. Just like with any potential disaster, you can't protect against something you don't know about.

“The first step is understanding what needs to be protected and how vital each asset is. Cataloguing and categorising assets might seem less critical than more active forms of cyber defence, but the practice is essential to effective cybersecurity.

It’s especially important when you consider how rapidly cybercriminals’

capabilities are evolving as they take advantage of AI, with the UK's *National Cyber Security Centre* warning of this threat earlier in the year

"A robust secure backup infrastructure is crucial for IT environments. It provides data security and stores multiple copies of all data, including deleted data from production. This, however, also makes it a prime target for criminals seeking to steal data and eliminate a company's safety net, to increase the chances of a ransom being paid out."

Andrew Smith continued:, "Ransomware is designed to avoid detection by frontline cyber defences. To infect as many systems as possible, small changes must be made to evade notice. Attackers frequently delete backups, shorten backup retention times, or disable backup jobs to prevent access to data that they want to hold for ransom. It's important to be aware of these tactics and take necessary measures to prevent them.

"Regular and thorough testing of recovery plans is also an essential practice in cybersecurity since it helps identify the potential damage caused by ransomware. By testing a complete recovery plan, including verifying applications, any failures encountered can reveal areas within the infrastructure where a critical file can be encrypted or a configuration file inappropriately modified. This testing can be particularly useful in learning to detect malware that runs during a system's boot-up sequence."

Given the increasing use of AI by cybercriminals and the growing sophistication of their methods, it is impossible for businesses to guarantee they will never be compromised.

Andrew Smith added: "To that end, removing the threat and restoring any compromised data quickly is crucial. All decisions should aim to meet the recovery time objectives (RTO), similar to preparing for a natural disaster.

Act decisively by stopping and eliminating ransomware from the environment, and optimise your defences to prevent repeat attacks. This will minimise cleanup effort and improve recovery time.

“Speed is of the essence. If dwell time is prolonged, cybercriminals may find ways to infect recovery points, making it necessary to go further back to find a clean restore point, in turn leading to further disruption and financial and reputational damage.

Andrew Smith concluded: "Cybercriminals continue to up their game, but if the right preparations are in place, there’s no need to panic. Take the necessary steps as a priority, and you’ll be well-placed to stay resilient well into the future.”

Andrew Smith is a cybersecurity expert and CISO at *Kyocera Document Solutions UK*

Article by Andrew Smith