Ransomware: focus on treating the cause not mopping up the mess

With the frequency of cyber breaches linked to the Covid pandemic on the rise, businesses need to proactively prepare for a potential breach focusing on the cause, not clearing up the mess once it has happened. This is according to ProLion, a best-in-class active ransomware and data protection solution provider for ONTAP centralised file services.

Since the outbreak of the Covid pandemic ransomware attacks have been evolving, becoming ever more sophisticated in terms of their deployment. At its core, ransomware is a financial transaction; if you want your stolen data back, pay for it.

Steve Arlin, VP Sales, UK, Americas & APAC, ProLion, stated: “Once a company’s IT systems have been breached by ransomware, it is immediately left open to the loss of mission critical systems which in its own right could be fatal. But then the threat of data leaks adds another level of pressure with the associated challenge of reputational risk and the threat of information regulators and associated GDPR fines.”

For the overwhelming majority of businesses their first priority is getting their data back and ensuring the business can function again. But the real problem is that ransomware could be a symptom of a far more serious network intrusion.

“Even with the ransomware removed and the system restored from backups, the problem may not have gone away, as the attacker may still have backdoor access to the network and could just as easily re-deploy the ransomware,” continued Arlin.

“Since there's no way to completely protect your organisation against a ransomware attack, businesses should adopt a 'defence-in-depth' approach. This means using layers of defence with several mitigations at each layer. You'll have more opportunities to detect it and then stop it before it causes real harm.”

This continuity of security functions means you should be looking beyond being reactive and dealing with the outcome post-breach to actively monitoring your network to counter opportunist threats.

The recent rise in ransomware incidents is in part due to the pandemic, as businesses have become more vulnerable as a result of the move to working from home. But other factors appear to be at play, not least the rise in hostile actors as a result of increased political tensions, and a rise in organised crime targeting organisations in dire straits.

“Although most organisations have endpoint cybersecurity, ransomware and malware can slip through. Even the best antivirus protection finds it difficult to track internal threats and compromised employees. Our solution is CryptoSpike, which delivers agentless ransomware protection for Central File Services whether in the local data centre, NAS, or in the Cloud, enabling us to deal with the cause before it becomes a mess,” concluded Arlin.

ENDS

Notes to editors

About ProLion

ProLion GmbH is a developer of ransomware protection and data integrity software solutions for any ONTAP centralised file services environment and high-availability solutions for SAP and MetroCluster environments.

Founded in Austria, ProLion’s best-of-breed CryptoSpike solution eliminates system downtime and data loss risk ensures that an organisations’ data remains secure, compliant, manageable and accessible.

www.prolion.com