The £30k Solution to a £1.5M Ransom: A Cybersecurity Cautionary Tale

The £30k Solution to a £1.5M Ransom: A Cybersecurity Cautionary Tale

BIRMINGHAM, WEST MIDLANDS, UNITED KINGDOM, August 29, 2023 /EINPresswire.com/ -- In the cyber landscape, moments of inaction can result in significant setbacks. Many believe that massive cyber attacks are something read about in the news but will never befall them. CyberQ Group has witnessed firsthand the cascade of security lapses that lead to destructive events. Here's a recent example that underscores the importance of proactive cybersecurity measures.

On a seemingly regular Tuesday at 11 am, a company's Managing Director (before they became our client) received an unsettling call: their systems were encrypted by Medusa ransomware. In disbelief, they found that four of their five servers had been compromised.

Though they had security measures in place, like firewalls and SentinelOne (basic) on endpoints, these were not enough.

They believed they were safe; reality proved otherwise. By 11:40 am, CyberQ Group was deep-diving into the issue, analysing the breach's scope and potential consequences.

Our assessment unveiled glaring vulnerabilities. Their network configuration was chaotic, lacking fundamental protections like DMZs, access control policies, multi-factor authentication, and more. Their backups? Encrypted. The Malware software had detected 4,000 vulnerabilities on their network, but no action had been taken.

The aftermath was devastating: customer records, supplier data, maintenance contracts, payroll, and critical Intellectual Property – all encrypted. And there was evidence that much of the data had been exfiltrated.

The ransomware perpetrators, identifying themselves as the Medusa group, demanded a staggering £1.5 million, having assessed the company's financials. CyberQ Group worked

diligently, testing the hackers' decryption capability and initiating cautious negotiations. Meanwhile, our investigation pinpointed the attack origin: a phishing email, inadvertently making our client a secondary target due to their security shortcomings.

Opting against meeting the ransom demand, the company decided to rebuild from the ground up. CyberQ Group provided essential support, deploying new servers and implementing over 300 vulnerability fixes.

However, the challenges were far from over. With the stolen data, the hackers threatened to sell it on the dark web. Within minutes of their dark web advertisement, it garnered 753 views.

Fast forward, the company is still grappling with the ramifications of this event. While the ransom was £1.5 million, the long-term costs, both financial and reputational, are yet to be fully realised. CyberQ Group estimates that a £30k annual investment in comprehensive cybersecurity services would have significantly mitigated such risks.

About CyberQ Group:

CyberQ Group is a leading cybersecurity firm dedicated to helping companies safeguard their assets in an increasingly digital world. With expertise in incident response, dark web monitoring, and a myriad of cybersecurity solutions, we are committed to the protection and recovery of businesses facing cyber threats.

The Team
CyberQ Group
+44 800 061 4725
email us here
Visit us on social media:
Twitter
LinkedIn
