Nearly half of London’s councils have taken preventative action to counter the growing threat of ransomware

Four councils (12%) confirmed they have been impacted by ransomware but did not pay the demand, with 42% taking preventative measures to counter the growing threat

A Freedom of Information (FoI) request by ProLion has revealed that nearly half of London’s borough councils (**42%**) have taken preventative action to counter ransomware, with four (**12%**) confirming they had been either impacted, or targeted by ransomware, but did not pay a demand.

The remaining 19 (**58%**) refused to confirm if they had been impacted by ransomware or have taken measures to counter attacks, citing Section 31 as a qualified exemption that ‘could prejudice the prevention, or detection of crime’.

Steve Arlin, VP Sales, UK, Americas & APAC, ProLion, stated: “With the problem of ransomware on the rise, it’s good to see almost half of London’s borough councils have taken preventative action. With four of boroughs confirming they have already been impacted by an attack, we would advise the other 58% to follow suit as a matter of urgency.

“The fact that 58% of the councils refused to answer if they had been affected by ransomware suggests they may have been victims of ransomware but do not want to publicly state this for fear of another attack. Organisations of all sizes and sectors are viable targets for opportunistic cybercriminals but the public sector is likely to hold more sensitive data, including Council Tax, medical records, and other financial records. This may explain why they are a preferred target and more likely to pay any ransom demands.”

The research also discovered the top preventative measures councils are implementing to counter future ransomware attacks, include antivirus solutions, multi-factor identification (MFA), web filtering, email scanning, firewalls, red team testing and cybersecurity training programs for all staff.

Arlin added: “It’s incredibly positive that a number of councils confirmed the measures they are taking to prevent ransomware, such as implementing cybersecurity training programs to all staff. However, despite authorities doing as we suggest by adopting a layered approach, there is no mention of any dedicated protection for file sharing, and many seem to be relying on basic endpoint protections, firewalls, and backups. This means that if something does get through their defences, there is no next step protection.

“Additionally, these measures don’t protect against insider threats, so with the increase in remote working and staff using their personal devices, the chances of being compromised are now even higher, as many employees don’t even know they’ve been hacked. There is a real need to have more rigorous IT policies around who can access, edit, copy and delete data, by having effective transparency tools and file share protections in place.”

Arlin concluded: “We would advise any organisation to make sure they are using the latest file protection solutions, as these can automatically block known ransomware signatures and files that have not been approved, while simultaneously monitoring users for any unusual behaviour. This is a vital final layer of cyber defence if all other security solutions fail.”

ENDS

Notes to editors

About ProLion

ProLion GmbH is a developer of ransomware protection and data integrity software solutions for any ONTAP focused storage 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

For further information
Alex Sowden/ Christian Stevens
Spreckley PR
T +44 (0)20 7388 9988
E: prolion@spreckley.co.uk