If you doubt the naysayers on ransomware look to Colonial Pipeline

Ransomware hits cashflow, operations, customers and reputation so take steps now

The Colonial Pipeline ransomware attack is a new and devastating kind type of threat against critical infrastructure. It is not just the financial and operational impact on the business, it is an attack that has directly impacted millions dependent on oil and gas delivery. This is according to ProLion, a best-in-class active ransomware and data protection solution provider for ONTAP centralised file services.

Steve Arlin, VP Sales, UK, Americas & APAC, ProLion, stated: “Ransomware can completely disable your computer or mobile device, locking down the hard drive, blocking access to all your files and data. For any enterprise it can be devastating for productivity and as we have seen in the US it can and does put lives at risk.

“Imagine all your projects on hold as you fight to regain control of your IT system and leaving all that data open to being stolen at best or erased at worse. This is a potential reputational disaster and paying up may not be the solution you think. There are no guarantees it won’t be done again and certainly no guarantee the information has not been copied already.

Arlin added: “For businesses in the UK it is now clear that the government will not step in and pay ransoms. Only this week Home Secretary Priti Patel, speaking at the National Cyber Security Centre's (NCSC) CYBERUK 2021 virtual conference warned that the government doesn't support victims of ransomware attacks paying the ransom.”

Speaking at the conference the Home Secretary stated “Government has a strong position against paying ransoms to criminals, including when targeted by ransomware.” Patel went on to say "Paying a ransom in response to ransomware does not guarantee a successful outcome, will not protect networks from future attacks, nor will it prevent the possibility of future data leaks. In fact, paying a ransom is likely to encourage criminality to continue to use this approach.”

“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,” added Arlin.

“Given the Home Secretary is now calling on organisations to take this threat seriously businesses must now start thinking that a ransomware attack is not just about the loss of data, it can put supply chains at risk, and lives on the line.

“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.

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