Industry Report highlights the scale of the ransomware challenge

Double Whammy of increased frequency of cyber breaches, coupled with difficulties of recovering from these attacks during a pandemic laid bare

A recent report which has found that the overall proportion of businesses targeted by cyber criminals in the past year has increased to 43 percent up from 38 percent has laid bare the double whammy impact of the Covid pandemic. This is according to ProLion, a best-in-class active ransomware and data protection solution for ONTAP storage.

The Report – the Hiscox Cyber Readiness report 2021 - surveyed over 6,000 companies across the US, UK, Belgium, France, Germany, Spain, the Netherlands and Ireland.

Steve Arlin, VP Sales, UK, Americas & APAC, ProLion, stated: “This Report is one of the most respected in the market, one that not only has starkly illustrated the rise in cyber-attacks over the past year, but also highlighted the financial consequences. According to the research one in six businesses attacked (17 percent) stated that the attack materially threatened their future from a financial perspective.

“Out of the total 16 percent were targeted with ransomware, that is the equivalent of 1 in 6 businesses. A staggering 58 percent paid up a figure that jumped through the roof in the USA where 71 percent paid the ransom. The Report also found that the costs of recovery was almost as high as the ransom itself, making up an average 45 percent of overall cost.”

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.

“The most effective route to combat ransomware lies in what companies are not doing, that is failing to take the threat of ransomware seriously enough in the first place. Organisations seem content to carry on with the mandated once-a-year cyber-security training courses which focus primarily on phishing emails and click-bait. Whilst these are still worthwhile, additional measures are needed due to the impact of Covid-19 which has led to many more people working from home,” continued Arlin.

One undeniable reason why you should care more than ever about Ransomware is the removal of barriers to entry. With the introduction of Ransomware-as-a-Service (RaaS), many more criminals can now operate, and now it's not only large organisations that fall victim, but also SMEs, local government and councils, and even sports teams, resulting in massive business disruption, reduced revenue, and disenfranchised customers.

"The call to action is simple – be proactive. We have seen with the Covid-19 response that most people would not wait till they are infected with a virus before doing something about it. Likewise, with ransomware, do not wait till it is too late! In the famous underlining principle of medicine – prevention is better than cure," concluded Arlin.

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