ProLion warns of increased ransomware attacks over the busy festive season

Amid growth in online activity, expect an increased number of cyber threats to your business

Forecasts by eMarketer predict that this year ecommerce revenues over the holiday period will increase by 11.3%. In order to successfully navigate expected extraordinary levels of online activity, it's vital that all businesses are protected over the festive busy season. This is according to ProLion, a best-in-class proactive ransomware solution.

The annual shopping frenzy is fast approaching and is officially kicked off by Black Friday on November 26th. This is quickly followed by Cyber Monday, and the inevitably busy Christmas period. It's predicted that as a result of the effects of both the pandemic and worldwide supply chain crises that the majority of shopping this year will take place in a similar way to the working lives of many, from the comfort of homes across the country.

The events of the last two years have served to accelerate the predicted shift from high street retail to ecommerce. In fact, in 2020 online sales reached their highest in 13 years, with a 37% increase in online sales in December 2020 alone.

With increased online activity comes an increased threat of cyber-attack. Not only for organisations in the retail space, but for what is always a busy period for businesses across many industries. Data from the Gambling Commission has revealed that over last year's festive period, the number of bets placed online rose by 12 per cent, with the number active online gamblers rising by 6 per cent.

Steve Arlin, VP Sales, UK, Americas & APAC, ProLion said: "It's no secret that we've seen an increase in online and digital activity over the past two years. But as a result of widespread media coverage of supply chain issues and a shift in attitudes and behaviours towards online shopping, we can expect criminals to be meeting the festive period with increased levels of cyber-attacks this year."

"When it comes to ransomware, there's no room for complacency. Once a business's IT systems have been breached, it is immediately left open to the loss of mission critical systems which could mean missing out on huge revenues and potentially lead to the loss of business entirely. Even if an organisation is able to successfully restore their systems after

an attack, the threat of data leak and reputational damage is enough to destroy a business altogether," said Arlin.

"The most effective way to combat ransomware is by being proactive, take the threat of ransomware seriously enough in the first place and build your defences. 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 newfound levels of digital activity," continued Arlin.

"The call to action is simple – be proactive and be vigilant. There are many simple practices that can limit the likelihood of attack. Don't store proprietary data on personal laptops, be sensible with your digital profiles, encourage good password practice. But most importantly, do not wait till it is too late! Investing in a proactive ransomware solution is the best way to combat the threat," concluded Arlin.