FPN FRONT PAGE NEWS | CYBER EDITION

Advisen Cyber FPN - Tuesday, November 22, 2022

Advisen

Over one-third of organizations experience a second cyberattack after paying ransom

By Erin Ayers, Advisen

Paying a ransom demand won't necessarily result in a quick fix – it won't even prevent cybercriminals from coming back for a second attack, according to data from Hiscox's 2022 Cyber Readiness Report.

In a special focus on ransomware, Hiscox found that only 59% of companies that paid a ransom successfully recovered their data. While the attackers do provide a decryption key, it can take weeks to fully decrypt systems and the malicious attack may well negatively affect the data integrity.

Worse, Hiscox found that 36% of firms who paid a ransom experienced another attack and nearly a third (29%) still saw data leaked.

"Ransomware is still the most prevalent and damaging form of cyberattack and it is not uncommon for a company to be hit multiple times," said Gareth Wharton, cyber CEO for Hiscox. "Even if a business owner makes the decision to pay the ransom, often they cannot fully restore their systems or prevent a data breach. That is why it is vital that businesses take the necessary steps to protect their data and systems against a cyberattack; making it harder for cyber criminals to gain entry to their

systems by keeping software up-to-date, running regular in-house training, and frequently backing-up data."

Phishing emails are the most likely vector for ransomware actors, Hiscox added, followed by credential theft (44%), a third-party supplier (40%), unpatched server (28%), and brute force credential efforts, such as password guessing (17%).

Some sectors hit by ransomware seem more prepared to weather an event without paying a ransom – Hiscox found just 18% of professional services firms pay and 62% of food and drink companies pay. Also on the more prepared end were construction at 19% and financial services at 23%. Joining food and drink companies were travel/leisure at 50% and manufacturing at 51%.

Overall, frequency and severity of cyberattacks has increased, according to the insurer's broader cyber report, with the number of companies reporting an event rising to 48% from 43%. One-in-five of the nearly 5,000 firms surveyed said the cyber event threatened their firm's financial solvency and the median cost of an event rose 30% to nearly $17,000, Hiscox found.

Cybercriminals also cast a wider net when it comes to their targets, with small firms very much at risk and seeing a nearly four-fold rise in the average number of attacks.

"While the cyber criminals have long targeted high-value companies, it is clear they are now moving down the food chain. International agencies have recently warned that more mid- and small-sized businesses are being targeted and this is borne out in this year's report. Companies with revenues of $100,000 to $500,000 can now expect as many cyberattacks as those earning $1m to $9m annually," said Wharton.

Cybercriminals also branched out in term of industry sector. Where energy firms and transport/distribution saw the highest number of attacks one year ago, this year's most-targeted sectors were travel and leisure, professional services, and retail/wholesale.

Managing Editor Erin Ayers can be reached at erin.ayers@zywave.com