THE RISE AND RISE OF RANSOMWARE

Ransomware made worldwide headlines with the devastating WannaCry attack of May 2017. WannaCry cost the NHS £92 million and forced the cancellation of 19,000 medical appointments. Nevertheless, two years later, over a million computers remain vulnerable to WannaCry and similar types of malware. Anyone who thinks ransomware has gone away is very much mistaken.

Massive increase in ransomware attacks

This year has seen a massive increase in ransomware attacks across the globe. Local government, schools, universities and hospitals have all been victims in a wave of highly successful ransomware attacks. Certainly, ransomware has become more sophisticated and insidious. However, pitiful security has left many organisations needlessly exposed to attack. Failure to patch applications for known vulnerabilities remains one of the main reasons cyber-attacks are so successful.

RDP attacks growing steadily

There is a new generation of ransomware designed to exploit open network ports to the Internet. RDP lets remote workers connect to company systems when they are out of the office. However, RDP can also be easily exploited if it's not configured properly. Open ports are an open invitation to cyber criminals and ransomware.

One born every minute

Every minute of every day, new malware is being released. In fact, the numbers are astonishing. AV-Test institute recorded 18 million new malware instances in the month of September 2019. While ransomware evolves and grows in sophistication, its preferred delivery method remains stubbornly the same: email.

Phishing as popular as ever

Nine out of ten cyber-attacks start with a phishing email. Unfortunately, unwary employees remain easily duped into opening email attachments and clicking on malicious links. Security Awareness Training that teaches employees to spot suspicious emails is infinitely cheaper than the costs of a successful cyber-attack.

£92 MILLION

the cost of the WannaCry attack to the NHS.

118%

increase in ransomware attacks this year.

18 MILLION

instances of new malware every month and growing.

NINE OF TEN

cyber-attacks start with a phishing email.

Pay up, lose out

The costs of ransomware attacks has tripled this year. Ransom payments have jumped from an average £10,600 to £29,451. The amount of downtime caused by ransomware attacks has also increased to 10-days. Of course, paying a ransom is no guarantee that you will get all your data back. On average, 8% of all data encrypted by ransomware is permanently lost during decryption.

Security isn't rocket science

Protecting your organisation from ransomware and cyber-attacks isn't rocket science. You need a robust IT policy, ensure your systems are correctly configured, regularly patched and user access is properly controlled. All your employees need to take regular Security Awareness Training. We also recommend you use mock-phishing attacks to test their alertness.

You need some basic security tools such as enterprise firewalls, anti-virus, spam filtering, Web protection, two-factor authentication, password management and encryption. Finally, you must ensure that all your data is reliably backed up and can be fully recovered should the worst happen.

If you have questions about IT security and data protection then talk to Modern Networks today.

£29,451

the average ransom demand to release encrypted data.

10 DAYS

the average loss of productivity due to a ransomware attack.

Sources:

Malware Statistics, Trends and Facts in 2019, www.safetydetectives.com
Ransomware preys on SMBs via RDP attacks, spam emails, www.carbonite.com
WannaCry Two Years On, www.techcrunch.com
Ransomware Attacks Costs Nearly Triple in 2019 to over $36K Per Attack, www.blog.knowbe4.com
Ransomware: Why we're still losing the fight – and the changes you need to make, before it's too late, www.zdnet.com

modernnetworks