SNG Grant Thornton

Rise in Ransomware Cyber-attack - what you need to know.

There has been a rise in ransomware attacks across the world with organisations of different sizes being targeted. The attacks resulted in a huge impact on the organisations concerned.

The impact of the Colonial Pipeline attack attracted so much attention in the US and globally:

- Colonial Pipeline, in running one of the biggest pipeline operations in the United States, delivers approximately 45% of the fuel for the US east coast, including gasoline, diesel fuel, heating oil, jet fuel and the fuel used by the military.
- The impact of Colonial Pipeline suspending fuel supplies as a result of the attack was severe. In addition to actual widespread shortages at gas stations along the east coast, four US states – North Carolina, Virginia, Georgia, and Florida – declared a state of emergency. For the first time since 2014, the average price of a gallon of gasoline across the US rose to almost US$3 (price exceeded $3 per gallon in 2014).

The other high-profile cyber-attack this year was on JBS S.A. The Sao Paulo, Brazil based company, is a meat processing company that is behind the supply of nearly 25% of the world's meat (and 23% of the US meat supply). It was the target of a cyber-attack, which it became aware of on May 30 2021. The attack resulted in the shutdown of all the company's fed-beef and regional beef plants in the US and disrupted animal slaughter operations across Australia. JBS operates in six countries and sells beef and pork through major retailers in these countries.

In July 2021, South Africa's largest logistics company Transnet SOC was hit by a disruptive cyber-attack that halted its operations at all the port's terminals. The company declared force majeure after the attack.

In the past, in May 2017, the WannaCry ransomware attack spread around the world, impacting over 10,000 organizations and 200,000 individuals in over 150 countries, according to European authorities. In the same year June 2017, a new variant of Petya was used for a global cyberattack, primarily targeting Ukraine.

Over and above these examples, there -have been numerous other attacks with both private and public institutions being targeted, with most not being publicized.

In light of these attacks, what is ransomware and how can organisations and individuals protect themselves from such attacks?

What is ransomware?

Ransomware is a malicious program that locks a computer's files. The attacker(s) usually demand a ransom in exchange to unlocking the files. For instance, the WannaCry virus takes control of users' files and demands a payment to restore access. It exploits security flaws on Microsoft computers, and once it infects a computer, it encrypts the files and spreads to other computers. Victims receive a demand for a payment of $300 in Bitcoin to regain access.

Should you pay the demanded ransom?

You should be discouraged from paying the requested ransom as paying will only incentivise criminals to keep targeting you with no guarantee that you or your company will get your data back.

How can organisations and individuals protect themselves from such attacks?

Ransomware exploits security weaknesses in computers. For organisations to protect themselves from such attacks they should ensure that their antivirus, patch management, and back-up processes are effective. Antivirus software can detect and block viruses before they infect your computers and patches are security updates that addresses fixes weaknesses in your computers that can be exploited by viruses. Organisations should consider the following countermeasures:

1. Ensure that the latest security updates and patches are applied on all computers and systems in their network. Updating software should be done regularly not only when there is a threat. In a blog post, Microsoft stressed the importance of doing this, writing: "As cybercriminals become more sophisticated, there is simply no way for customers to protect themselves against threats unless they update their systems."
2. Ensure that antivirus and anti-spyware software's installed on all servers and workstations.
3. Ensure that the antivirus and anti-spyware software have up-to-date definitions (ideally have a central antivirus server that downloads the definitions regularly and deploys them across the network to all computers).
4. Ensure that the email gateway is configured to scan for malware, spam, and spyware on all incoming and outgoing emails.
5. Ensure that the email gateway is configured to block all suspicious attachments e.g., executable files.
6. Block accessing of malicious websites and downloading of suspicious files.
7. Ensure that computers are configured to auto-scan for malware and spyware when external or portable media e.g., Memory sticks, hard drives are connected.
8. Consider segmenting the network to slow the spread of malware. Segmenting the network and keeping critical applications and devices isolated on a separate network or virtual LAN can limit the spread.
9. Conduct periodic security awareness training – educating employees (including Executive Team) against opening suspicious attachments, accessing malicious websites.
10. Backup up critical data and keep it offline and separate from the network in case ransomware spreads.
11. Conduct periodic vulnerability and virus scans to detect security weaknesses and infected machines.
12. Consider taking cyber insurance to cover your business against Internet-based liability and cyber risks.

How can we help you?

At SNG Grant Thornton, we advise our clients on how to effectively manage cyber-risks, highlighting measures to secure and protect information stored and processed on computers. We help clients build cyber resilience against mounting cyber-attacks.

Contact us

Please get in contact with our professional team should you require any further information about Cyber Security.

Kudakwashe Charandura
Head of Cyber Advisory

T +27 11 231 0600
E Kudakwashe.Charandura@sng.gt.com

SNG Grant Thornton

sng-grantthornton.co.za