The rise of ransomware attacks during 2019

Cyberattacks, specifically ransomware, during 2019 have been on the rise, and it's become such a problem that recently, the ACSC (Australian Cyber Security Centre) stated that they are currently investigating an extensive malware campaign that uses emails to deliver a virus. This virus looks just like a normal file, but once opened allows cyber criminals access to your systems.

This increase in cyber attacks is backed up by one of the largest insurers, Chubb, who have stated that by the third quarter of this year, the number of ransomware attacks in Australia exceeded the total number in 2018. There was reference that the sophistication of these attacks has not only increased, but that some of the ransomware demands have reached six and seven figures. It was also stated that companies providing professional services are more at risk than those in the manufacturing industry, simply because they rely more heavily on emails to run their operations.

How do these viruses spread?

These Trojan viruses move very quickly and aggressively. If the file attached to the email is opened, the virus is sent to all email addresses in that person's mailbox. Once opened by these third parties, it accesses their mail boxes, and the cycle continues. This malicious spam can keep spreading, even if it's been cleared from your systems, and it can come back again via a third party email.

New generation of trojan viruses

These viruses keep evolving and are so invasive that the international law firm, Clyde & Co, issued a public warning about the rising number of attacks. Their briefing stated that these viruses have even attacked banks, as well as the public and private health services in Victoria. Datto, a cybersecurity firm, have stated that SMEs have become prime targets for these types of cyber attacks. In a recent survey they found that out of 1400 managed service providers, 91% have suffered from these types of attacks in the previous two years.

They also found that many SMEs in the Pacific region have reported attacks focusing on applications such as Office 365, Dropbox and G-suite. In fact, Datto found that Australia and NZ have the highest rate globally with 37% of survey respondents reporting cyber attacks.

SMEs need a proactive approach to cyber attacks

Referenced in the report issued by Chubb, it was found that 23% of all cyber claims for ransomware attacks came from SMEs with an annual revenue of less than $25 million USD. This means that owners, managers and supervisors of SMEs must take a proactive stance and ensure that they fully educate their employees about the dangers of ransomware and how to recognise suspicious emails. They must also have in place a system that deals with the aftereffects - if these ransomware emails are actually opened.

As you can appreciate, the increasing number of cyber attacks on Australian SMEs can have devastating effects on the reputations and operation of many businesses. It's imperative that business owners and senior management understand the increased risks posed by these attacks. They also need to learn how to mitigate these risks with the correct type of cyber insurance and how to prevent further damage occurring, if an attack is realised. To discuss how cyber insurance can help your business recover from a ransomware attack, talk to an insurance specialist today.