How CISO's should remediate a ransomware attack

The successful remediation of the impact of a ransomware attack depends entirely on the plan a chief information security officer (CISO) has in place to protect their business, says Stephen Osler, co-founder and business development director at Nclose.

Stephen Osler, co-founder and business development director at Nclose

It's impossible to read the news without seeing at least one headline blaring about a breach, hack or attack. In the USA, the Colonial Pipeline experienced a Darkside ransomware attack that affected more than 10,000 gas stations.

Virgin Active was hit by a hack in early May 2021 and took weeks to re-establish its systems.

Vastaamo, a platform that provided therapy to thousands of patients, lost its data to hackers thanks to an unexpected security flaw. The hackers sent ransom demands to patients – pay up, or your personal information is public knowledge.

As Osler points out, the criminal networks and masterminds behind digital attacks are doing their jobs and have every motivation to do these jobs extremely well.

> *The sheer volume of events is a concern. The threat actors and the methods they use are increasingly sophisticated and complex, taking advantage of even the slightest gap in a company's defences. Many attacks are extremely malicious, and some are driven by intentions other than just money or data. But, and this is really important, don't panic and don't pay the ransom.*

For Osler, the first and most important step that the CISO should take is to set your disaster recovery (DR) and business continuity plan (BCP) in motion by notifying leadership.

Massive ransomware attack hits South African businesses

5 Jul 2021

Transparency is key, as is full insight into how serious the compromise may be, and the challenge that lies ahead. Next step – contain the breach.

Determine which servers and systems have been infected and contain them as quickly as possible to minimise the damage and the spread. Notify the teams and get people off the network as fast as possible – from the mobile device to the server mainframe.

> *Once you've contained as much of the breach as possible, you need to identify the source. It's absolutely critical to identify howthis got into the organisation and the level of access that the hackers have. Even if you switch everything off and rebuild everything from scratch, you still need to knowhowthey got in so you don't add that vulnerability straight back into the business. Find patient zero.*

At this point, you shouldn't have paid the ransom. Hackers are unethical to start with, there's no guarantee that they won't withhold services in spite of payment, as they did in the Colonial Pipeline attack, or simply sell your data anyway. Payment also paints a big, red bullseye on the back of your business, and perhaps your whole industry.

"If you pay, the hackers will look at other companies in your sector and simply replicate their success story with someone else," says Osler.

"And they may come back to you for more. Payment is a risk; non-payment is a risk. Either way, you've been hacked and you need to have plans in place to protect your business and your information."

Check Point Research warns of a further increase in cyberattacks

28 Jun 2021

This means that your BCP and DR strategies need to be tested, as far as they can be, rigorously. That you have put clearly defined processes in place for remediation, and that your detection systems are as cutting edge as they can get.

> *Learn lessons from the attack and use failure as an opportunity to learn from mistakes, to close loops and to add in additional controls. Double-check the policies, see what worked and what didn't, and adapt internal training and systems to improve your security posture as thoroughly as possible. Most importantly, don't panic and pay. Plan, protect, and plan some more."*

No business or system is perfect – it's like hitting a moving target that changes shape every 10 seconds – but having the right procedures in place can help you minimise the damage done.