Insight Space

cyber insights programme

nccgroup

Is ransomware an exponential threat to society?

Ade Clewlow, Senior Advisor at NCC Group

Ransomware is one of the most common types of cyber attack for organisations around the world, and it is showing no signs of slowing down. According to our research, the number of ransomware attacks on organisations of all sizes across every sector has increased in the last 12-18 months by 45%.

From humble beginnings in 1989, when the first attack was allegedly distributed via a floppy disk and demanded that the victim send $189 to a post box in Panama, ransomware has developed into a hugely profitable and sophisticated business.

Although the end goal of extortion has remained, the tactics, techniques and procedures have all evolved to cause catastrophic damage to organisations.

In our latest Big Three webinar, Quentyn Taylor, Director of Information Security at Canon Europe, Keith McDevitt, Cyber Security Integrator at the Scottish Government and Kat Sommer, Head of Public Affairs at NCC Group, joined me to discuss this exponential threat.

We asked whether ransomware was an inevitable threat for organisations, whether it made protecting your crown jewels data more important and what organisations can do to address it.

AN INEVITABLE EVENT?

Threat actors have realised that ransomware generates big returns for relatively little effort, so they use a combination of methods to generate as many opportunities to profit as possible. For example, many organisations fall victim to 'drive-by' attacks where threat actors compromise a supply chain to access multiple targets indiscriminately.

Alternatively, many attacks are manually deployed and targeted at specific organisations that are particularly lucrative or that threat actors believe will pay the ransom. These attacks use bespoke methods to cripple operations and exfiltrate sensitive information to use as leverage and as a threat to damage the organisation.

This dual approach means that any organisation with money or data must consider a ransomware attack as inevitable and prepare accordingly. Practically, this means deploying good cyber hygiene by regularly patching vulnerabilities and increasing your resilience against indiscriminate and targeted attacks.

PROTECTING YOUR CROWN JEWELS DATA

Protecting assets and systems has always been important to organisations, but the threat of ransomware makes it crucial to identify your most critical assets so that you can prioritise their recovery in the event of an attack. However, many IT, security and business leaders disagree on what those assets are, so it's vital to find common ground here. Organisations should also pin down the system or network that would need to be restored first to enable normal operations to resume.

It's also important to remember that ransomware attacks are carried out by real people that can adapt their methods to cause maximum disruption to your organisation at any one time. For example, a sales website could be the most important asset to an e-commerce retailer in the months leading up to Christmas, but throughout the rest of the year it is of normal importance. Ransomware threat actors will know this, so it's important that organisations protect their assets accordingly.

ADDRESSING THE THREAT

Currently, there are three conditions that favour ransomware threat actors: they can operate safely from geographies like Russia, they can take advantage of systemic human and technical weaknesses across organisations and crypto currency enables easy ransom payments. Many ransoms are still being paid by organisations in the knowledge that they are likely to claim a proportion of the payment back from their cyber insurance policy. This perpetuates the proven ransomware business model.

Paying ransoms is discouraged because it funds further criminal activity and provides a viable business model for threat actors. Banning payments is one option, but it could lead to criminals intensifying their efforts in other areas, making this a controversial issue for organisations to consider, and a complex policy challenge for governments to address.

With all of this in mind, it's clear that addressing the ransomware threat requires leadership and a multi-pronged approach, ranging from improved international cooperation and pressure against those countries that harbour ransomware criminal groups, to organisational and individual responsibility for good cyber hygiene. Governments around the world are taking the threat seriously, with the Ransomware Task Force in the US encompassing elements from the entire cyber community just one example. However, organisations can protect themselves and slow the growth of this exponential threat by increasing their resilience to ransomware. Here are six key steps which should be considered as a minimum:

1. Employ multi-factor authentication (MFA) on all external facing internet connections (remote access points)
2. Segregate legacy operating systems from the network
3. Backup your files, ideally offline in multiple locations (and rehearse deploying them)
4. 'Patch, patch, patch!'
5. Invest in your people to improve their awareness, culture and behaviours
6. Write and rehearse your incident management plan

To find out more about how you can increase your resilience against the exponential threat of ransomware, you can watch the full webinar, 'Is ransomware an exponential threat to society?' here.

Insight Space

cyber insights programme

nccgroup

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 14,000 customers worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses assess, develop and manage the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With circa 2,000 colleagues in 12 countries, NCC Group has a significant market presence in North America, Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia, Japan and Singapore.

To discuss how you can reduce your ransomware risk, speak to our team today.

+44 (0)161 209 5111

response@nccgroup.com

www.nccgroup.com