nccgroup

Executive Viewpoint: Defending your organisation from Ransomware. Tim Rawlins, Senior Adviser at NCC Group.

Jul 20, 2021 11:05 BST

Executive Viewpoint: Defending your organisation from ransomware

The ransomware threat landscape is becoming increasingly complex. Changing ways of working and the increasing commoditisation of ransomware mean that ransomware is more of a threat to business resilience than ever before.

One factor contributing to this increasing threat is the way that working life has changed. At the beginning of the pandemic, many organisations quickly transformed their operating model to allow employees to work from home, often onboarding new solutions and ways of working without taking the time

to consider any security gaps that would open up as a result.

The adoption of new technology has meant that we've increasingly seen criminals taking advantage of unsecured solutions. It's common for ransomware groups to take advantage of business web applications with vulnerabilities and remote access solutions such as Virtual Private Networks (VPN) and Remote Desktop Protocols (RDP) to gain a foothold on a corporate network.

Social engineering attacks are another common route for criminals. While email phishing attacks remain at the top of the list, LinkedIn, WhatsApp, and text messages are increasingly used as ways to reach unwitting employees. Highly targeted and well-crafted phishing attacks are more likely to be successful if employees are working away from the office and are therefore less likely to question any requests that are even slightly out-of-character.

A global issue

The threat of ransomware spans borders and sectors, with the targets of ransomware gangs ranging from IT suppliers and software companies to critical national infrastructure providers, local and national governments and financial institutions, where stakes and potential rewards for hackers are high.

In the past few months alone, the world has seen several large-scale ransomware attacks. These include the attack on Kaseya, an IT solutions company, which leveraged vulnerabilities in its VSA product for managed service providers (MSPs) to impact between 800-1,500 businesses in July 2021.

Another particularly notable example was a ransomware attack that targeted the Colonial Pipeline, a 5,500-mile fuel pipeline covering the US East Coast in May 2021, severely disrupting fuel supplies across the country. The impact of the attack quickly became apparent as increased fuel demand and shortages led to panic buying and fuel price increases. When added to the $4.4 million (£3.1 million) ransom paid by the Colonial Pipeline Company to Eastern-European based ransomware gang, Darkside, the true cost quickly becomes apparent.

The lucrative nature of ransomware attacks means that businesses are experiencing ever-more aggressive and highly targeted approaches from criminals. This is particularly true for the financial sector, which is frequently targeted by a banking malware family known as Gozi, characterised by an aim to cause financial losses through transactional fraud or targeted ransomware activity. NCC Group's Research and Intelligence Fusion Team (RIFT) found that 136 financial institutions had been targeted by threat groups using RM3, an advanced variant of the Gozi ransomware family, since 2017 - just one small aspect of a vast threat landscape.

The evolution of ransomware

As well as an increase in targeted ransomware attacks, the last year has led to a rise in ransomware-as-a-service attacks, in which ransomware variants are sold to criminals in a subscription model.

This means that many criminals target victims simply by scanning for vulnerable applications or remote access ports. Often, these gangs seek to go after irreplaceable business assets as well as devices connected to a business network, which could include file servers, database services, virtual machines and cloud environments. The theft of data is also a common element of today's ransomware attacks, with criminals often using the threat of publication as leverage.

The determination of today's criminals makes it much harder for organisations to recover from ransomware attacks. In many cases, attacks go undetected until the damage is done. The timeline of attacks can often span weeks from the initial breach to full control of the victim's corporate network.

Building a security strategy fit for the new normal

Prevention is better than a cure, which is why it's vital for organisations to build a proactive security strategy. As organisations step back and review their processes, people and technology for the post-COVID world, it's crucial for them to also consider the security measures they have in place.

1) Creating a security-aware team

People are a critical line of defence for businesses, and the way that

colleagues respond to security challenges can be the difference between ongoing resilience and a damaging cyber attack.

It's therefore crucial for organisations to provide regular security awareness training to staff members, covering best practice when it comes to dealing with phishing and scam attempts. This training should also cover reporting to regulatory bodies, strong password security and how to store sensitive credentials.

In addition to this, individuals can play a key role in helping a business recover quickly after an incident – it's important for organisations to have individuals that are given the authority to make decisions during an incident as part of a robust incident management policy.

2) Minimising risk

Having robust controls in place and limiting access to business networks wherever possible can help to reduce an attacker's chances of breaching corporate systems.

This includes only providing privileges that employees require for business functions, such as only having access to specific folders on a shared drive or server. This means that if a user's account is compromised, the attacker would be able to access a smaller amount of information, and data is less likely to be deleted or modified.

Ensuring that a process is in place for regularly updating software and solutions in line with the release of security patches or improvements is also important. This minimises the risk of vulnerabilities appearing in your system from out-of-date solutions.

3) Maintaining visibility over your IT estate

To ensure that any ransomware attacks can be managed and swiftly resolved, it's crucial to keep logs and backups of critical services, files and networks. This includes logging events into a Security Information and Event Management (SIEM) system, and storing this information for at least 90 days.

As well as increasing the chances of continued access to business-critical

systems, this will also make investigating, tracking and remediating the damage caused by an attacker a far more streamlined process.

Tim Rawlins, Senior Adviser at NCC Group

Insight Space – Ransomware

This Executive Viewpoint is part of our latest edition of Insight Space, which analyses the ransomware landscape and what it means for your organisation.

We've put together technical and executive insights, case studies and practical advice about how you can protect yourself from ransomware, and what to do if you do fall victim to an attack to ensure you recover as effectively as possible.

Find out more here.

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 to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience, and investment in research and innovation, it is best placed to help organisations assess, develop and manage their cyber resilience posture.

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.

Contacts

NCC Group Press Office
Press Contact
All media enquires relating to NCC Group plc
press@nccgroup.com
+44 7824 412 405
+44 7976 234 970