DigitalXRAID
CYBER SECURITY EXPERTS

RANSOMWARE ON THE RISE

Understanding the What, Why and How of this Growing Threat

Ransomware attacks are a significant threat to businesses, and their frequency is on the rise

Ransomware is a persistent threat that has been around for over 30 years, yet it continues to evolve and cause havoc. With more people working remotely and companies rushing to implement new systems and processes, this is leaving companies vulnerabilities to ransomware attack.

According to industry reports, the number of successful ransomware attacks on businesses have increased by 485% compared with the previous year. One common misconception about ransomware attacks is that they only affect large corporations.

However, SMEs are increasingly being targeted, with a report by Verizon stating 28% of ransomware attacks were aimed at small businesses in the last year.

In fact, cybercriminals often target small businesses because they tend to have weaker security systems and are more likely to pay the ransom. These statistics show that ransomware attacks are becoming increasingly prevalent, and that no organisation is safe.

The increase in ransomware attacks can be attributed to several factors. Firstly, the cultural shift to remote and hybrid working, which has created new vulnerabilities for cybercriminals to exploit. Secondly, the rise of cryptocurrencies such as Bitcoin has made it easier for cybercriminals to receive ransom payments anonymously.

The increasing sophistication of ransomware attacks means that cybercriminals can now target specific organisations and individuals with greater accuracy.

To protect against ransomware attacks, it is important to follow best practices and implement robust cybersecurity measures.

Proactive protective measures include regularly backing up data, ensuring that all software is up to date, and training employees to recognise and report suspicious activity.

Additionally, organisations should consider implementing cybersecurity frameworks such as ISO 27,001 and Cyber Essentials to help identify and mitigate potential risks.

In this ebook, we will explore the ‘what, why and how’ of ransomware attacks, including common misconceptions, reasons behind the increase in attacks, and the techniques used by cybercriminals to target their victims.

Common Misconceptions

Ransomware is a type of malicious software that is used by hackers for various reasons: Political, shock value, proving a point, or for financial gain. Financial gain is the most common reason for ransomware attacks, and attackers often use cryptocurrency for anonymous payments.

Despite its prevalence, there are still several common misconceptions about ransomware.

One of the most common misconceptions about ransomware is that it only affects large corporations. However, recent statistics show that small businesses are becoming increasingly vulnerable to ransomware attacks.

This is likely due to the fact that many small businesses lack the resources to implement robust cybersecurity measures, making them an easy target for cybercriminals.

Another misconception is that anti-virus software can fully protect against ransomware attacks.

While anti-virus software can provide some protection, it is not enough on its own. Cybercriminals constantly find new ways to bypass anti-virus software, making it important to implement multiple layers of cybersecurity measures to protect against ransomware attacks.

This includes regularly backing up data, implementing strong passwords and policies, and providing regular cybersecurity training to employees.

It is also important to note that ransomware attacks can have significant financial implications beyond the ransom payment.

Downtime due to a ransomware attack can result in lost revenue, lost productivity, and reputational damage. In fact, the average cost of downtime due to a ransomware attack was found to be $274,200, according to recent statistics.


Ransomware attacks on businesses have increased by 485%

The Why

Ransomware attacks have been on the rise in recent years, and one of the main reasons behind this is the emergence of double extortion attacks.

In such attacks, hackers not only encrypt the victim's data but also steal sensitive information to blackmail them into paying the ransom. According to a report by a leading ransomware response firm, the average ransom payment increased by 171% in just 3 months.

One factor that has contributed to the increase in ransomware attacks is the cultural change of workforces working remotely or as part of new hybrid policies.

With more people working remotely, even in part, there has been a surge in the use of online collaboration tools and cloud-based services, which has created new opportunities for hackers to exploit.

In addition, many companies have had to rush to implement new systems and processes to enable remote work, leaving them more vulnerable to attacks.

Another reason behind the rise of ransomware attacks is the increasing availability of ransomware-as-a-service (RaaS).

This has made it easier for cybercriminals to access sophisticated malware without having to develop it themselves, lowering the bar for entry into the ransomware market. RaaS has also enabled hackers to monetise their attacks more effectively, as they can now offer their services to other cybercriminals.

Another contributing factor to the rise in ransomware attacks is the failure of companies to address basic cybersecurity deficiencies.

According to a report by the Ponemon Institute, 70% of organisations surveyed admitted to having paid a ransom in the past, and 57% believed that paying the ransom was the most cost-effective solution. This attitude only encourages cybercriminals to continue their attacks.

To gain entry points into a system, attackers use various methods, including using USB drives or exploiting public information and data breaches.

However, the most common method of entry is through phishing attacks, which account for 90%+ of security breaches.

By tricking users into downloading and executing malicious files, attackers can spread ransomware across the network, encrypting files and infecting as many machines as possible.

The best defence against ransomware attacks is to have strong user training and security awareness. This can help prevent users from downloading malicious files or falling victim to phishing attacks.

Companies should also implement strong security measures, such as multi-factor authentication (MFA), regular data backups, and network segmentation, to minimise the risk of a successful attack.

By taking a proactive approach to cybersecurity, organisations can reduce their vulnerability to ransomware attacks and better protect their sensitive data.

The average cost of a ransomware attack has risen to $1.85 million globally

The How

Cybercriminals use several techniques to target their victims.

One common method is Phishing, where they send emails that appear to be from a legitimate source to trick the recipient into clicking on a link or downloading an attachment.

Once the malware is downloaded, it can spread throughout the system, encrypting files and demanding payment for their release.

Another method is to exploit vulnerabilities in systems or software, allowing the malware to enter undetected.

Once in the system, cybercriminals can use legitimate tools such as Cobalt Strike or PS Exec to move laterally through the network, gathering information and planning their attack.

In addition to phishing and exploiting vulnerabilities, cybercriminals also use other techniques such as social engineering and brute force attacks to target their victims.

Social engineering is a method where attackers use psychological manipulation to trick people into giving them sensitive information or performing actions that may compromise their security.

This could involve posing as a trusted entity or using fake login pages to steal credentials.

Brute force attacks are another common technique used by cybercriminals to gain access to systems or applications.

This method involves trying multiple combinations of usernames and passwords until the correct one is found, allowing the attacker to gain access to the system.

According to recent statistics, ransomware attacks have become more frequent and more damaging.

In the last year, the average cost of a ransomware attack rose to $1.85 million globally, with the average ransom payment being $570,000.

The healthcare sector has been particularly hard hit since the pandemic, with 79% of ransomware attacks in the last year being targeted at healthcare organisations alone.

In addition, the frequency of attacks has increased, with a 62% increase in the number of attacks in just 6 months.

To protect against these attacks, companies should take a multi-layered approach to security, including regular backups, strong access controls, and employee training.

It is also important to stay up to date with the latest threats and vulnerabilities, and to ensure that all software and systems are patched and updated regularly.

With the right defenses in place, businesses can reduce the risk of falling victim to ransomware attacks and protect their sensitive data.

Prevention and Response

Preventing ransomware attacks requires a multi-faceted approach.

One critical aspect of preventing ransomware attacks is employee education and training.

A recent survey found that 68% of organisations identified employee training as the most effective method for reducing the risk of a ransomware attack.

Regular security awareness training for employees can help them identify potential phishing emails and other tactics used by cybercriminals to gain access to the company network.

Another essential step is to keep software and systems up to date with the latest security patches.

Unpatched software or systems with outdated security measures can provide cybercriminals with an easy entry point into a network.

According to a report by the Center for Internet Security, patching systems within two weeks of a security patch being released can prevent up to 85% of targeted attacks.

Using strong passwords is also critical to preventing ransomware attacks. The use of weak or easily guessable passwords is a common entry point for cybercriminals.

Password policies should be enforced, such as requiring the use of a combination of upper and lowercase letters, numbers, and special characters, and encouraging employees to change their passwords regularly.

Regular data backups are essential to mitigating the impact of a ransomware attack.

Backing up data to a separate location and performing regular data recovery drills can help ensure that companies can recover their data quickly in the event of an attack.

Government agencies across the world recommend that companies back up their data frequently and store it in a location that is not connected to their network to prevent it from being encrypted by ransomware.

However, with the progression and proliferation of cybercrime – ransomware in particular – back-ups are less efficacious in the face of increasingly sophisticated cyberattacks so can't be taken as the only mitigation step.

Organisations should consider adopting cybersecurity frameworks like ISO 27001 and Cyber Essentials to protect their business against ransomware attacks.

These frameworks provide a comprehensive set of guidelines and controls to identify and mitigate potential risks to their information security.

ISO 27001 is an international standard for information security management systems that covers a wide range of topics, including risk assessment and management, access control, and incident management.

Cyber Essentials is a UK government-backed scheme that provides a set of basic controls for organisations to implement to help protect against common cyber threats.

By adopting these frameworks, organisations can demonstrate to their customers and partners that they take cybersecurity seriously and have measures in place to protect their data.

In the event of a ransomware attack, companies must have a plan in place for responding quickly and effectively.

This plan should include isolating infected devices, identifying the type of ransomware, and assessing the extent of the damage.

Companies should also consider involving law enforcement and other relevant authorities in their response efforts.

What should you do next?

Cybersecurity is a pressing concern for businesses of all sizes, as attackers are always looking for vulnerabilities to exploit. Whether you're a financial institution or a service business with a low IP footprint, someone out there is looking to take advantage of any weaknesses in your infrastructure. Luckily, there are actionable steps you can take:

Risk Assessment

The first step in protecting your organisation from cyberattacks is to conduct a risk assessment.

Consider the types of transactions you're processing and the size of your business. Identify potential vulnerabilities, such as disgruntled employees who may take action against your organisation.

Assess your organisation's ability to identify and recover from serious infections. Do you have the necessary skill set, tools, and technology to respond effectively?

Incident Response Framework

An incident response framework is crucial for minimising the impact of a cyberattack.

Conduct roundtable exercises to identify roles and responsibilities within your organisation and third-party service providers.

Consider the potential impact of downtime, such as the loss of revenue or damage to your reputation. When an organisation is breached, rapid threat detection and incident response are critical to prevent the spread of malware and minimise damage.

Best Practices

Following best practices is an effective way to protect your organisation from cyber threats.

The UK's National Cyber Security Centre (NCSC) provides guidance on cybersecurity, and frameworks such as ISO 27001 and Cyber Essentials are useful for organisations that are just starting on their cybersecurity journey.

By implementing best practices, you can reduce the risk of a cyberattack and minimise the impact if one occurs.

It's essential to stay informed about cybersecurity trends and to be proactive in identifying and addressing vulnerabilities before they can be exploited by attackers.

How can we help?

The more successful ransomware attacks that occur, the higher the likelihood that more businesses will be targeted by hackers.

Cyberattacks are no longer an 'if' but a 'when'. Implementing a proactive cybersecurity strategy has never been more important for organisations of all sizes.

DigitalXRAID is a leading cybersecurity service provider that specialises in protecting businesses from ransomware and cyberattacks.

With over 25 years' experience in the industry, DigitalXRAID has the expertise to identify vulnerabilities and provide comprehensive solutions to prevent attacks.

We take a proactive approach to cybersecurity. Rather than simply responding to attacks after they occur, we help you to stay a step ahead of cybercriminals, preventing ransomware attacks and other cybersecurity threats before they happen.

By partnering with DigitalXRAID, you can confidently take proactive measures in protecting your systems and data against ransomware attacks.

We can support you with information security certifications such as ISO 27001, penetration testing to identify potential weaknesses in your networks and systems, and a fully managed, CREST accredited Security Operations Centre (SOC), for 24/7/365 monitoring and protection.

DigitalXRAID

CYBER SECURITY EXPERTS

Need the Best Defence Against Cyber Threats?

Call us now on 0800 090 3734

info@digitalxraid.com digitalxraid.com

ISO 27001 INFORMATION SECURITY MANAGEMENT

ISO 9001 QUALITY MANAGEMENT

CYBER ESSENTIALS CERTIFIED PLUS

IASME CONSORTIUM

CREST

Assured Service Provider in association with National Cyber Security Centre CHECK Penetration Testing