daisy.

CYBER SECURITY 101: RANSOMWARE

Ransomware continues to be one of the biggest threats to all organisations and shows no signs of going away any time soon. In fact, 66% of organisations were affected by Ransomware in 2023[1]. With recent media reports and vendor scaremongering, it would seem that it may already be too late! However, this is not necessarily the case.

With most hackers looking for any opportunity to gain access, organisations are actively working to guard against ransomware, but despite this, it seems many aren't taking essential precautions. While 78% of organisations believe they are "very" or "extremely" prepared to mitigate an attack, 50% still fell victim to ransomware last year.

This guide helps you to understand the threat and explores the most common ways a ransomware breach happens. It outlines things that your IT staff and users can do to avoid common mistakes and vulnerabilities, as well as reduce the chances of any unwanted intrusions. It also looks at ways you can protect your data so that you can avoid a situation where someone who has broken into your network, can completely deny you access to your live and backed-up data.

CONTENTS

BACK TO MENU

WHAT IS RANSOMWARE?

Ransomware is a malicious software that encrypts files or systems, denying access to victims until a hefty ransom is paid. Hackers typically infiltrate networks through tactics like phishing emails, tricking individuals into clicking on links or attachments to reveal passwords and gain system access. Once inside, they pilfer terabytes of confidential information, establish back doors, and deploy ransomware on multiple IT assets, sometimes crippling entire networks or data centres.

The attackers demand a ransom, often in the millions, constituting 10-20% of a company's cashflow, in exchange for the decryption key. This demand is accompanied by a threat to expose data until the ransom is paid.

Attempts to conceal this information may lead hackers to engage with local press, revealing a compiled list of clients and staff obtained during the breach, with some resorting to public shaming tactics.

The rise of ransomware as a service (RaaS), which was first observed in 2016, marks a shift from automated viruses to deployment by individuals or hacker groups. This surge is propelled by an escalating need for resilience in digital infrastructure across diverse sectors.

Insufficient protection of backups poses a significant vulnerability. Hackers, armed with full admin access, can delete all backups, demonstrating creativity by deleting private keys of encrypted tape backups or manipulating retention periods to delete backups instantly, including its offsite replication.

Whether in online education, government services, ecommerce, or remote work, individuals and businesses heavily depend on smoothly functioning digital infrastructure. Hackers view ransomware attacks as a means to secure substantial payouts or sow chaos in these critical systems.

TYPES OF RANSOMWARE

Since 2020, there have been more than 130 different ransomware strains detected[2], categorised into five main types. However, nowadays when people mention ransomware, they typically refer to ransomware as a service (RaaS).

RaaS - this model involves hackers renting or selling ransomware to create and distribute malicious software, enabling unauthorised individuals to carry out ransomware attacks for financial gain. This approach lowers the entry barrier for executing ransomware attacks, as any criminal can pay a fee to access the necessary tools without the need to develop their own malware.

Crypto ransomware strains - these strains focus on restricting access to individual files and crucial data within systems.

Locker ransomware strains - this type of ransomware affects entire systems, preventing users from performing basic computer functions.

Scareware - is fake software that claims to have detected a virus or issue on your computer and asks you to pay to resolve the problem. Some scareware attacks restrict access to your files by blocking the screen with pop-ups to encourage payment.

Doxware or Leakware - poses a threat by distributing sensitive information online, causing panic and ransom payments to safeguard privacy; one variation masquerades as law enforcement, offering to avoid jail time through a fine.

The primary goal of any ransomware group whilst attacking a network, is to extract data from an IT environment before locking files or systems to gain monetary benefits. These attacks are evolving, introducing a new threat: double extortion, some groups are now attempting quadruple extortion! In this scenario, the first stage involves demanding payment to unlock encrypted files or systems, while the second stage demands a second ransom to prevent the publication of sensitive data online and on the dark web.

There's no guarantee that the data hasn't been shared with anyone, given the involvement of hackers. Whether now or in the future, once the data is gone, it's gone, making it challenging to determine its fate.

BACK TO MENU

WHO IS THE TARGET?

Ransomware attacks pose a threat to all businesses, including charities. Despite common misconceptions that smaller or less-known organisations are immune, the reality is that every business, regardless of size or profile, is susceptible.

Many believe they won't be targeted because they lack sensitive data or are not widely recognised. However, if a business generates revenue and relies on digital assets for its operations, it becomes an attractive target for hackers seeking to profit by ransoming critical information.

Size is not a factor in discrimination; businesses of all sizes, from sole proprietors to billion-pound companies, as well as large to small city councils, universities, and government entities, have all faced ransomware attacks.

The notion that it won't happen to a particular organisation is often a misconception.

Hackers are opportunistic and will exploit any vulnerability to gain access to a network.

WHO IS MOST AT RISK?

It's not a matter of "if" but "when" a ransomware attack may occur. To safeguard against such threats, it is crucial for all organisations, irrespective of their perceived risk level, to adopt proactive measures for protecting their digital assets. Understanding that the potential for attack exists for any business underscores the importance of implementing robust cyber security practices.

However, there are certain factors that can increase the likelihood of being targeted, such as:

Businesses in industries or sectors with low cyber security maturity

Such as transportation, healthcare, higher education, and the energy industry are more prone to be defenceless against ransomware attacks.

Inadequate training and awareness among staff

This lack of understanding can also affect the overall well-being of staff, including factors such as fatigue and the strain of long working hours. This aspect of ransomware is often overlooked or not extensively discussed, emphasising the need for comprehensive training programs that address both the technical and human elements of cyber security.

A lack of dedicated security infrastructure and dedicated security staff

Often when a new app is being developed, ease of use and efficiency is prioritised over security. Security needs to be integrated into all IT solutions and services and should not be considered as an afterthought, in order to create a comprehensive and robust defence against cyber threats.

Lack of multi-factor Authentication (MFA)

Businesses that do not implement MFA, a security protocol requiring users to provide multiple forms of identification before accessing a system, are more susceptible. MFA adds an extra layer of protection by requiring not only a password but also an additional verification method, reducing the risk of unauthorised access.

Insufficient patching practices

Failing to regularly update and patch software and systems creates vulnerabilities that hackers can exploit. Outdated software often contains known security flaws that can be easily targeted, making it crucial for organisations to maintain up-to-date patches to mitigate these risks.

Exposed management protocols

Certain management protocols, such as Remote Desktop Protocol (RDP) or Secure Shell (SSH), or a terminal server, can become easy points for cyber attackers if left exposed and unprotected. It is essential to secure these protocols with strong authentication methods, encryption, and access controls to prevent unauthorised access.

EXAMPLES OF RANSOMWARE ATTACKS

Let's have a look at these attacks in action. Below are six of the most infamous ransomware attacks over the years.

WannaCry (2017) - WannaCry is an example of crypto ransomware. Exploiting a Windows vulnerability, WannaCry spread rapidly across the globe. It encrypted files on infected systems and demanded ransom payouts in Bitcoin.

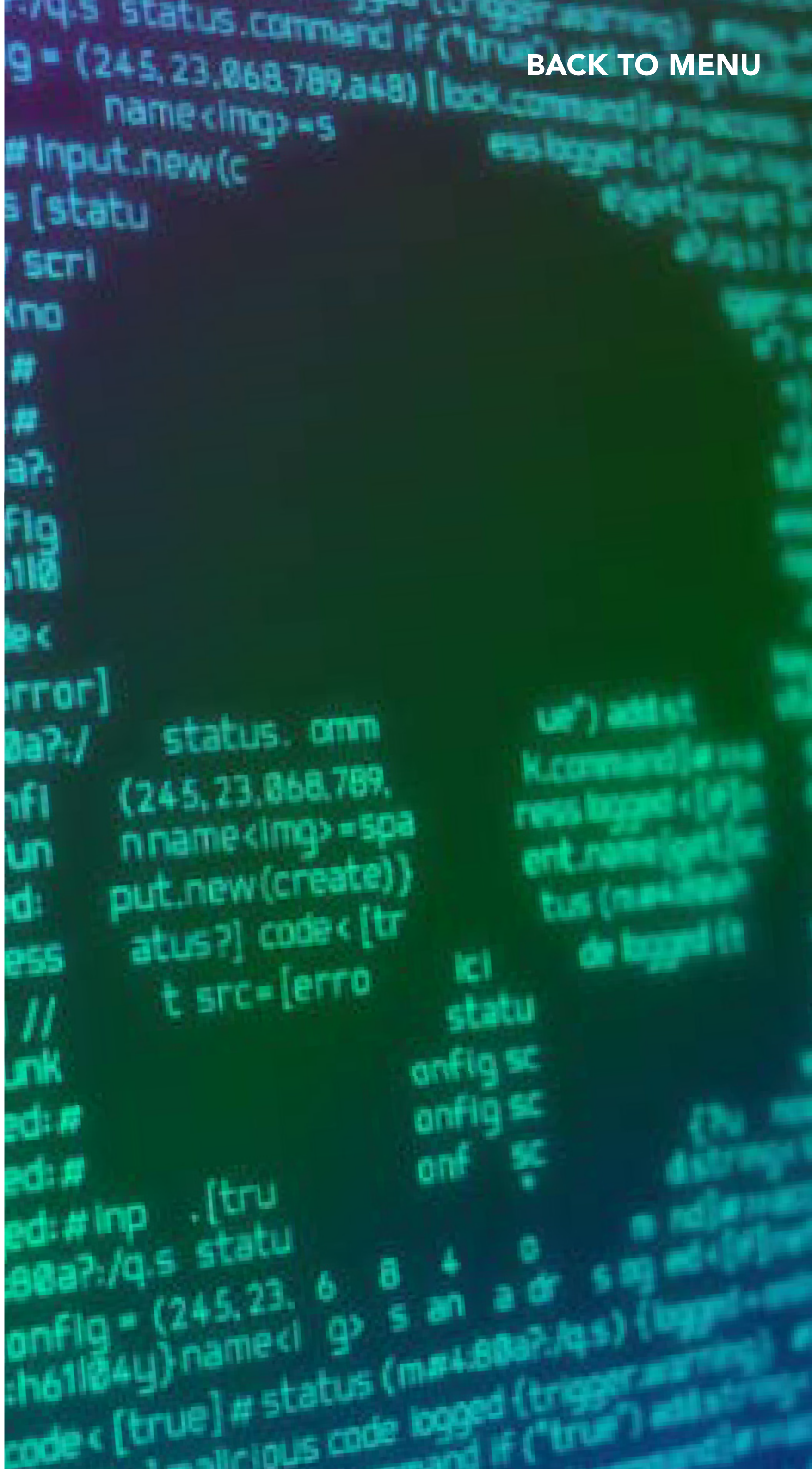
The attack affected more than 200,000 computers in 150 countries and major institutions including the National Health Service (NHS) were disrupted.

Møller-Maersk (2017) - The NotPetya ransomware infected 50,000 endpoints across 130 countries causing an estimated $300 million in losses. Ransomware NotPetya was estimated to have caused a total of £10 billion in damages.

The Guardian (2022) - British Newspaper, The Guardian, experienced a major ransomware attack that shut down part of its IT infrastructure. It was a highly sophisticated attack involving unauthorised third-party access to parts of their network, that was most likely triggered by a successful phishing attempt.

National Health Service (2022) - A ransomware attack on IT supplier, Advanced, caused widespread outages across the NHS. The LockBit 3.0 attack affected services including patient referrals, ambulance dispatch, out-of-hours appointment bookings, mental health services and emergency prescriptions.

Royal Mail (2023) - The Royal Mail service was hit by a LockBit ransomware group, the group hacked into software and blocked international shipments by encrypting files crucial to the company's operations. They made one the largest known ransom demand ever: £67 million. Royal Mail declined to hand over the ransom, as a result the group published the files on the dark web, an investigation is still ongoing.



BACK TO MENU

HOW CAN YOU STOP RANSOMWARE ATTACKS?

There is no silver bullet when it comes to avoiding ransomware. This is why it is necessary to adopt a multi-layered strategy to protect your organisation.

When looking at the overall impact of what ransomware can do to your data, you must tackle everything from user training, prevention, protection, and even understanding the worth and impact of your digital assets, including data.

There is no silver bullet when it comes to avoiding ransomware. This is why it is necessary to adopt a multi-layered strategy to protect your organisation.

When looking at the overall impact of what ransomware can do to your data, you must tackle everything from user training, prevention, protection, and even understanding the worth and impact of your digital assets, including data.

The problem with ransomware is when systems are already hacked. Unless you have got appropriate backups, you are at the mercy of the perpetrator.

This means that from a security perspective, it's more about stopping it happening rather than fixing it once it's happened.

There's no one thing that is guaranteed to stop it happening. The best approach is to have multiple layers of protection, in order to detect an intruder and prevent any further infiltration and damage.

We recommend patching as the first line of defence, followed by multi-factor authentication (MFA), anti-phishing, anti-malware, properly configured firewalls and then vulnerability management and web application firewalls (WAF).

Patching is critical to addressing known vulnerabilities and thwarting exploitation. However, IT teams face challenges in swiftly deploying and testing patches, leading to instances where security updates aren't implemented. This applies not only to Windows but extends to all security patches, including firewalls, VPNs, VDI, and Citrix, posing a risk of compromise. Comprehensive patch management is crucial.

PREVENTATIVE SOLUTIONS

Preventative solutions are a combination of tools such as WAF, email security, firewalls, active directory hardening, and antivirus software are essential. While these tools are important it is equally important to regularly test and validate these defences to ensure their effectiveness and make necessary adjustments to maintain resilience. This includes conducting regular vulnerability assessments and penetration testing to identify any weaknesses or potential entry points that could be exploited by cyber criminals.

After implementing protective measures, next you would deploy additional defence mechanisms such as a security information and event management (SIEM) platform as part of a managed detection and response (MDR) service.

By using a full MDR system featuring SIEM, you can proactively monitor your systems and networks, and detect potential ransomware attacks in real-time, thereby enabling immediate isolation of the infected devices and preventing the spread of the malware to other machines.

It is crucial to note that deploying advanced defence mechanisms is only effective if the basic security foundations are in place.

You must ensure that they have proper network segmentation, strong access controls, regular system backups, and a disaster recovery plan in place as a starting point.

Armed with this information about the entry points and attack vectors used by hackers, you can establish robust security defences and protocols to best protect against ransomware attacks.

PROTECTIVE CONTROLS

First things first, start with protective controls that can help to keep ransomware off your network and minimise the spread should they sneak in:

Moitoring and Patch Management

Monitoring your external digital attack surface is key, this includes asset management, IP addresses, ports, configurations, cloud resources and applications.

Timely and effective patching is essential for promptly addressing vulnerabilities especially internet connected devices, whether they are servers or endpoints. This process should cover all applications, both in-house and third-party, as well as firmware on network-connected devices and operating systems on endpoint workstations. Regular patching mitigates the risk of threat actors exploiting detected vulnerabilities. Lack of patching creates a window of time where hackers have opportunity to break in.

Multiple Layers of Protection

Firewalls, endpoint security, secure email gateways (SEG) and secure web gateways (SWG) solutions are all essential in preventing ransomware from gaining access to your organisation.

Having these protections in place will ensure that you have a robust layer of defence.

Anti-virus software is your last layer of defence, it is essential to review virus alerts for root cause analysis, identifying any security layers that may not have effectively thwarted the threat. This may include shortcomings in the anti-spam filtering system, configuration, or web proxy, among other potential vulnerabilities.

Employee Training

Gaps in cyber security education can be a business's greatest downfall. Ransomware groups know that the common weak link is humans, and without proper training, you'll fall right into their hands.

Ensure that you conduct regular cyber security awareness training, educate your employees on recognising phishing emails, avoiding suspicious downloads, and adhering to safe online practices.

Consider ways to alleviate MFA fatigue, ensuring that security measures don't become burdensome for your staff. Balancing robust security practices with user-friendly approaches is key to maintaining a resilient cyber security posture.

Testing and Security Standards

Regular testing and adherence to security standards, including Cyber Essentials and Cyber Essentials +, are vital for protecting your organisation from cyber attacks. Through vulnerability assessments and penetration testing, weaknesses are identified and addressed. Strong security standards, such as ISO 27001 for information security management, enforce access controls and encryption protocols to enhance defences.

These measures ensure that industry best practices, including those specified in Cyber Essentials and Cyber Essentials +, are consistently followed, reducing the risk of overlooking critical security measures. By combining regular testing with adherence to ISO standards and Cyber Essentials certifications, you can proactively identify vulnerabilities, minimise the impact of attacks, and safeguard sensitive data and systems.

BACK TO MENU

DEFENSIVE CONTROLS

Defensive controls play a crucial role in enhancing the security posture of your organisation:

Security Information and Event Management (SIEM)

SIEM is a powerful cyber security solution designed to protect your organisation from evolving threats and ensure the integrity of digital assets. If you don't have the expertise or resources to operate a SIEM solution yourself, you can purchase it as part of an MDR managed service. SIEM acts as a central hub for collecting, aggregating, and analysing security events and logging data generated by various systems, devices, and applications across an organisation's network. By consolidating this information into a unified platform, SIEM enables IT teams to gain valuable insights into potential security incidents and anomalous activities.

MDR solutions offer the added advantage of outsourcing the monitoring and management of the SIEM platform to a third-party provider with expertise in cyber security. This allows you to leverage advanced threat detection and response capabilities while freeing up internal resources for other critical tasks. MDR, improves your ability to detect and respond to cyber attacks, and enhances your overall security posture.

Active Threat Detection

Advanced threat detection utilises cutting edge technologies, such as AI-based behavioural analytics and machine learning, in order to detect anomalous patterns and behaviours indicative of ransomware attacks. This proactive approach enhances the ability to respond swiftly.

Endpoint Detection

Deploy robust endpoint detection solutions to safeguard devices against malicious activities. This helps in detecting and blocking suspicious behaviour before it leads to a ransomware infection.

RESPONSE CONTROLS

Ensuring that your business has well documented, tried and tested procedures, and supporting solutions in place can make responding to a ransomware attack much easier and faster.

1. Backup and Recovery Processes

For a ransomware attack to work, your security must be breached in the first instance, but this on its own is not enough to bring the organisation to its knees.

Once access to your infrastructure has been gained, the intruder also needs to be able to prevent you from accessing your own data. If you take some basic steps to protect your data you can recover to a point in time prior to any attack.

The Offline Rule

The purpose of an 'offline backup' is that it remains unaffected should any incident impact your live environment. You can ensure an offline backup by:

- Only connecting the backup to live systems when absolutely necessary
- Never having all backups connected at the same time

With at least one backup offline at any given time, an incident cannot affect all your backups simultaneously.

Air Gapping

Air gapping is a network security measure that ensures a secure computer network or device is physically isolated from unsecured networks, such as the public Internet or an unsecured local area network. Next time you book in a penetration test, make sure you maximise the value of your investment and have the testers assess the effectiveness of your air gap by evaluating whether your backup systems are genuinely isolated.

Immutable Data

Once a backup is completed, it assumes a point-in-time status, this means that they cannot be edited or modified. However, it's worth noting that the immutable status is not automatically activated and needs to be manually enabled. It's imperative to activate this feature, as without it, even if the backup system exists within the same virtualised environment, it remains susceptible to encryption during a ransomware attack.

Thus, the immutable status acts as an additional layer of defence, safeguarding the integrity of your backups against potential threats.

BACK TO MENU

RESPONSE CONTROLS

2. Business Continuity Plans

Another important consideration is that, as with any business interruption from any cause, you have the necessary continuity plans in place for any critical communication platforms and operating systems.

Any downtime could negatively affect your organisation, having these in place can help to get your business back up and running.

3. Incident Response Planning and Retainers

Responding to a ransomware attack requires mature incident response procedures. These plans include predefined steps to be taken during a ransomware incident, ensuring a well-coordinated and swift response.

In addition to implementing mature incident response procedures, you can further enhance your ability to respond to ransomware attacks by engaging retained third-party cyber incident responders.

This gives access to expert knowledge, resources, and guidance during a ransomware incident. Their involvement can significantly minimise the damage caused by ransomware attacks and increase the chances of a successful recovery.

This service provides you with a structured form of expertise and support though a security partner, enabling you to respond quickly and effectively in the event of an attack.

> **Before implementing response controls, conducting a management and tabletop exercise is valuable. This exercise aids in gauging the criticality of response controls to the business and provides insights into how effectively they would function in the event of a security incident.**

BACK TO MENU

HOW TO TALK TO THE BOARD ABOUT RANSOMWARE CHALLENGES

Communicating with the board about ransomware challenges is crucial for fostering understanding, support, and proactive decision-making.

By framing the discussion around the business impact, regulatory compliance, and proactive risk management, you can effectively communicate the ransomware challenges and garner support for necessary cyber security initiatives.

For more information, take a look at our resource on how to talk to the board about ransomware challenges.

1. TechTarget
2. The Ransomware in Global Context Report

3. TechTarget

HOW CAN DAISY HELP?

As a leading provider of IT, cloud, and communications solutions, we can help your organisation become more cyber resilient and better defend against cyber attacks. We offer a range of cyber security services, including vulnerability assessments, penetration testing, and managed SIEM solutions, to assess your organisations cyber security posture and identify potential vulnerabilities.

We've also provided business continuity and backup solutions for more than 30 years, that help our customers maintain operations during and after a cyber attack. These solutions include data backup and disaster recovery options that provide redundancy and can restore critical systems and data in case of a disruption. Our disaster recovery solutions are designed to minimise downtime and ensure data integrity through regular testing and maintenance. Our experts can also help you design and implement comprehensive business continuity plans to minimise the impact of cyber attacks and other disruptions.

We also offer retained 24/7/365 cyber incident response services to provide expert guidance and support during a cyber security incident. With our help, you can improve your cyber security posture, better prepare for cyber attacks, and ensure uninterrupted continuity of your business operations.

For more information our specialists are on hand:

Call: **0344 863 3000**

Email: **enquiry@daisyuk.tech**

2024 © Daisy Corporate Services Trading Limited (CRN: 02888250)