CUSTOMER GUIDE

Avoiding Ransomware

Essential tips and strategies for protecting against ransomware

At the heart of nearly all successful ransomware attacks is human error, which accounts for more than 80% of these incidents, according to several surveys. When unaware employees fall victim to well-constructed social engineering attacks, attackers can quickly steal credentials and gain access to sensitive systems. Read on to learn the best practices that we recommend, to help provide protection against ransomware.

Whilst you cannot eliminate human error, you can mitigate the severity of these attacks by educating your staff about essential cybersecurity hygiene, best password management practices and how to spot and report phishing emails. Companies also need proactive monitoring and threat detection through regular security assessments.

This type of monitoring can help mitigate the damage of these attacks through early detection. In many cases, the threat actors in these attacks are active on the network for as long as **180 days before anyone notices**.

There are several best practices that we recommend businesses follow to provide comprehensive protection against ransomware.

Asset inventory

Cataloguing all hardware, software, and Cloud assets in an organisation to establish a robust security infrastructure. This foundational step helps in designing concentric rings of security, creating multiple defence layers to safeguard critical assets. A well-maintained asset inventory enhances incident response, ensures compliance and optimises resource allocation for better operational efficiency.

Establish endpoint protection with 24/7 monitoring

Modern endpoint solutions look at behaviour at the endpoint, which provides good first-layer protection.

Update security patches

Unpatched systems can provide easy access to cybercriminals. Businesses need to understand their assets and what needs to be protected. Automated patch management solutions can help keep the entire environment up-to-date.

Block malicious IP addresses

Using geo-blocking and other restrictions can help harden systems against attack.

Maintain a strong password policy

This requires balancing security with user convenience, but regular password updates can mitigate many attacks. Stolen credentials are worthless if they are changed regularly.

SCG®
Midlands

Multi-Factor Authentication (MFA)

MFA is a security mechanism that requires users to provide two or more forms of identity verification before granting access to a system.

These factors can include something you know like a password, something you have like a smartphone or security token, and something you are like a fingerprint or other biometric data.

By requiring multiple forms of identification, MFA significantly enhances security by making it more difficult for attackers to gain unauthorised access, even if they manage to compromise one of the authentication factors.

Provide security awareness training

Staff need to be aware of how to spot a malicious email, and there should be clear policies around credentials, payment and invoicing processes, and other activities so that social engineering attacks are less likely to succeed.

Establish a data protection strategy

This means offering a solid backup solution and ensuring the backup is secure and everyone understands how restoration processes will work in the event of an attack. Businesses should have an incident response plan and regularly run drills to test it.

Least privilege

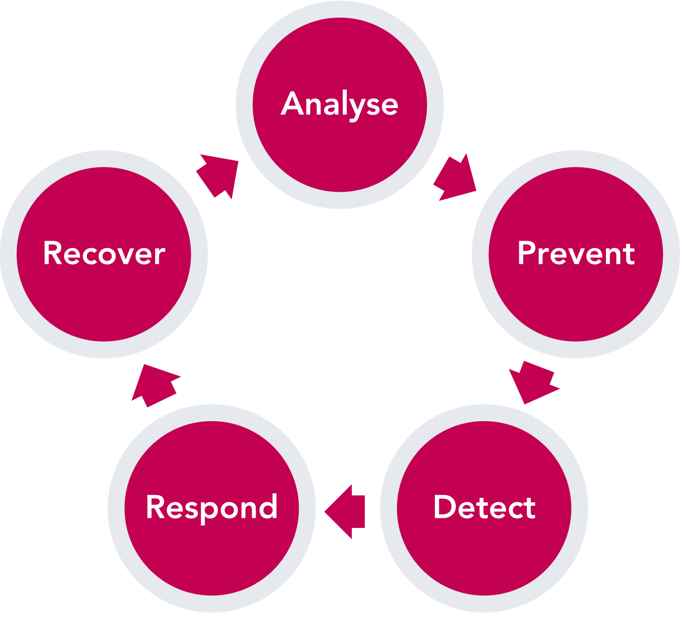
Providing individuals or systems with the minimal levels of access or permissions needed to accomplish their tasks. This proactive measure minimises potential damage in the event of a security breach, as malicious actors or processes are limited in what they can access.

Implementation requires a thorough analysis of what access rights are necessary for each user or system component, along with regular reviews and adjustments to maintain a tight security posture.

How SCG can help

Good cyber hygiene, robust backup and recovery systems, endpoint security, 24/7 monitoring, strong password policies, and automated detection and response can help businesses avoid having their opertions disrupted by these attacks and help avoid paying ransoms.

SCG can offer advice and assist in providing solutions for this multi-layered security approach, reducing the risks to your business as the ransomware problem continues to grow.



Contact us:
0330 333 0001 ☎
info@scgmidlands.co.uk ✉
www.scgmidlands.co.uk 🌐