How to improve cyber hygiene and prevent ransomware

UK Finance information sheet for members and their suppliers

Executive Summary and Resources

- Ransomware incidents increased significantly in 2019. These threats are neither new or declining: firms need to understand what ransomware is, the different types and how they can best defend themselves against it, especially in the current climate as attackers try to take advantage of disruption to firms' operational activities.
- The National Cyber Security Centre (NCSC) has published guidance on preventing malware and ransomware attacks that explains how firms can reduce the likelihood of becoming infected and how to mitigate any potential impact if they are.
- The NCSC's Cyber Essentials certification is a government backed scheme that helps firms protect themselves against the most common cyber attacks, including ransomware and is a useful starting point for firms to develop and improve their cyber hygiene.
- The NCSC Board Toolkit is designed to encourage cyber security discussions between a board and their technical experts and ensures that robust and effective challenge is provided in firms before decisions are made.
- The Financial Sector Cyber Collaboration Centre (FSCCC) is working with its members and the NCSC to actively share intelligence on threats to the sector, which include ransomware.

Traditional Ransomware

- Traditional ransomware relies on exploiting user vulnerabilities and is self-spreading. It is delivered through targeted and enticing phishing attacks or through the download of malicious software (malware).
- Criminals use the malicious content within emails that, when opened, allows ransomware to run, compromising the user's computer. This can also occur even if the email is only viewed, i.e., without opening attachments or clicking links, because security weaknesses can be exploited in the operating system or the software that is installed.
- There is specific software that can be used to detect phishing emails and malicious attachments that can prevent the propagation of the ransomware. Without these preventions in place, malware may spread rapidly through a firm's network, encrypting files, resulting in victims being left without access to systems and files. These may then be held for ransom and stolen information may be published on the internet. Even if a ransom is paid, there is no guarantee the hacker will unencrypt your data.

Human Operated Ransomware

- Human operated ransomware incidents are not always immediate or obvious. Attackers are often adept at systems administration and identifying security misconfigurations and can therefore adapt to the path of least resistance they find in a compromised network to establish a silent foothold, before triggering the ransom at a later date. This can occur even after critical patches have been applied.
- Vulnerabilities in remote access software (that allow you to work from home) are a common path for attackers to establish a foothold in a firm before activating ransomware further down the line. Common examples being targeted are Virtual Private Networks (VPN) or Remote Desktops.
- It is important not to assume there is no risk just because it has not happened thus far. If your firm has not applied a security patch in a timely manner it is possible your network may have already been compromised, because criminals typically investigate their victim for months before acting.
- To prevent this type of attack, it is equally important that you constantly monitor for anomalous activity within your network and that business continuity and recovery plans are in place to minimise the impact of a successful attack.
- Your remote service provider can give guidance on how to identify if you have been compromised and whether a vulnerability is particularly serious.

Detection and Prevention

- Ensure software patching is up to date including operating systems such as Windows, MacOS, Android and iOS; web browsers such as Edge, Chrome and Firefox; and any email software.
- Run up to date antivirus software and endpoint protection and use an 'email filter service' to scan and block malicious messages before they reach you.
- Ensure that staff receive appropriate training to never open attachments they are not expecting or are unsure of the contents.
- Stay closely apprised of alerts from official sources, such as the NCSC and other relevant organisations in countries in which your firm operates.

Preventing Vulnerabilities from becoming Breaches

- Ensure systems are well maintained with the latest security updates applied.
- Configure systems following best practice guidance.
- Commission penetration and vulnerability testing to identify and address any weaknesses.
- Apply Identity and Access Management controls to ensure that only the people that need access receive it.
- Ensure you are receiving and applying advice and intelligence on critical vulnerabilities from suppliers.
- Include two factor authentication for any remote access software where an additional layer of protection is required and which will prevent harm if passwords are leaked.

More Information

Please contact Joel.Wilson-Hunt@ukfinance.org.uk if you have any questions or feedback on this information sheet.

Previous information sheets can be found here.