Loss Prevention Standards – Cross Classes

Cyber - Ransomware

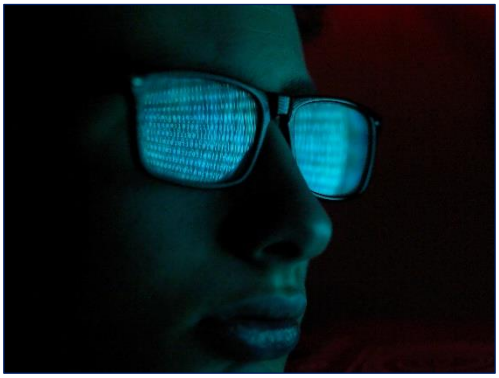
Version: 1.3
Date: 24th October 2024

The rapid increase of ransomware means any organisation could be a target for this type of cyber-attack. This document is intended to provide guidance on protecting against a ransomware attack.

AVIVA

Cyber - Ransomware

Introduction



To protect against ransomware, it is important to understand what it is.

Ransomware, in simple terms, is malicious software (malware) that infiltrates a network, system, or computer and prevents access to certain elements, until a ransom is paid to the attackers.

Cyber criminals will find a weakness to exploit, and the ransomware will encrypt or deny access to key data. Criminals will set a time frame, within which the victim is told to pay the ransom, usually in an untraceable cryptocurrency, such as Bitcoin, to have access restored, or data de-crypted.

Ransomware is not a new development, and the first recorded example was in the late 1980s, but there was a real explosion in cybercrime during the 2019 pandemic. History shows that fraudsters attempt to take advantage of any disaster. This saw many IT systems, network and support functions stretched, with many businesses moving to working from home. This, unfortunately, saw cybercrime increase greatly and ransomware attacks become more rampant.

History

The WannaCry attacks in Spring 2017 and the NotPetya attack a few months later, showed the world the potential impact of ransomware attacks. Both attacks were attributed by the National Cyber Security Centre (NCSC) as the work of state actors (hackers representing a Nation State). The ransomware spread independently and at pace throughout networks, impacting almost every device they encountered.

WannaCry was the name of a cryptoworm that targeted computers running the Microsoft Windows operating system. It encrypted data and the attackers demanded ransom payments in the Bitcoin cryptocurrency. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organisations that had not applied these patches or were using older Windows systems that were past their end-of-life.

The attack was halted within a few days of its discovery, due to emergency patches released and the discovery of a kill switch that prevented infected computers from spreading WannaCry further. The WannaCry ransomware attack was estimated to have affected more than 200,000 computers across 150 countries, impacting hugely on the UK's NHS. The attack is believed to have originated from a country in the Far East or actors working for the country (see BBC News 16/07/2017).

NotPetya was like WannaCry in that it used the penetration tool, or exploit, EternalBlue, created by the US National Security Agency (NSA) and leaked by a group called the Shadow Brokers. It is widely believed that this was a state-sponsored Russian cyber-attack on Ukraine that spread globally, causing widespread impact on businesses and infrastructure (see BBC News 15/02/2018). In the NotPetya ransomware attack, businesses with strong trade links with Ukraine, such as the UK's Reckitt Benckiser, Dutch delivery firm TNT and Danish shipping giant Maersk were affected, and the attack is estimated to have cost more than £850m.

Protecting against Ransomware

One of the big misconceptions around cybercrime and ransomware, is businesses assuming they are not really a target and that ransomware attacks are only perpetrated by organised crime groups, against major targets. This is not true, as like all cybercrime, ransomware is aimed generally at any business where a weakness may invite an opportunity of financial gain for the criminal(s). The first part of protecting against ransomware attacks is to understand that anyone could be a target. As with general cyber security, the best defence is to put as many barriers as possible to attack or infiltration, in place as soon as possible. This will help to slow the spread of a virus and give businesses a chance to act on what has happened and mitigate its impact.

Backup Data Regularly

- Make regular data backups.
    - Backing up data, especially key aspects is essential. There should be a regime in place for data backups, so a business knows exactly what has been affected by an incident.
    - Reinstating from these backups should be tested to ensure it works and in a timely manner, and any learning from these tests can be acted on before they are required in a 'real event'.
- Keep offline copies of backups.
    - Keeping a copy of the backup offline means any infiltration into the network and systems will not affect this copy.
    - Cloud storage could offer an ideal solution.
    - Any standalone hard drives used for data backup should be disconnected from the network once the backup is completed.
    - The NCSC blog on 'Offline backups in an online world' provides useful additional advice for organisations.
- Scan backups before reinstating data.
    - Check for malware before reconnecting to the network.
    - Malware can remain hidden and could have replicated.

Block Delivery and Spread of Malicious Software

- Use of multi-factor authentication for access to networks and use of a virtual private network (VPN).
- Ensure firewalls are in place and that these are adequate and up to date.
- Have a pro-active control over user privileges.
    - Ensure users only have access to what they need to do their job.
    - Ensure access is immediately removed when a user leaves the company.

Updates to Software

It is essential that updates are actioned as soon as they become available, as these will not only update the software, but also include security improvements.

- Enable automatic updates where possible.

Plan

Put a plan in place to act on and manage any incident and to cater for activity necessary to recover. Dealing with incidents and securing data can be key to protecting operations, its reputation, and its future.

- A plan should consider what the critical assets are and the likely impact, should these be attacked.
- Have a response to any ransom demand pre-prepared and a communication plan in place.
    - This will ensure the right messages are delivered from an organisation out to customers, suppliers, other business partners, media, etc.
- In planning any incident management and the business recovery, service level agreements and regulatory requirements should be considered.
- Business impact analysis is at the centre of business continuity management and this concept applies here.
    - Understanding what the impact could be, what resources and activities need to be prioritised to get the business running again, will help to provide focus in the right areas.
    - Considering what needs restoring first, and in what time scale, is essential.

Steps to Take if Your Organisation is Infected

The following 9 steps have been published by the NCSC and may help limit the impact of an attack:

1. Immediately disconnect the infected computers, laptops, or tablets from all network connections, whether wired, wireless, or mobile phone based.
2. In very serious cases, consider:
    - Turning off wi-fi or disabling any core network connections (including switches).
    - Disconnecting from the internet.
3. Reset credentials including passwords (especially for administrator and other system accounts).
    - Verify this action does not lock users out of systems that are needed for recovery.
4. Safely wipe (clean) the infected devices and reinstall the operating systems.
5. Before restoring from a backup, verify that the backup is free from any malware.
    - Only restore from a backup if there is a high level of confidence that the backup and the connecting device are both clean.
6. Connect devices to a clean network - to download, install and update the operating system and all other software.
7. Install, update, and run antivirus software.
8. Reconnect to the network.
9. Monitor network traffic and run antivirus scans to identify if any infections remain.

Do Not Pay a Ransom!

In the UK law enforcement strongly advise against the payment of ransom demands. If the ransom is paid:

- There is no guarantee that an organisation will get access to their data or computer back.
- The computer/network will still be infected.
- It will probably be funding criminal activities.
- An organisation is more likely to be a future target for cyber criminals.

Attackers will also threaten to publish data if payment is not made. To counter, this organisation should take measures to minimise the impact of data being released. The NCSC's guidance on protecting bulk personal data gives more guidance on this and is available here.

Reporting Incidents

In the UK, cyber security incidents can be reported to the NCSC by visiting here.

Action Fraud is the UK National Fraud & Cyber Crime Reporting Centre. Reporting the information to this website not only gives the Police key details in attempting to apprehend criminals, but it also raises awareness of the incident that could help other people/businesses avoid a similar attack.

Cyber Essentials Certification

Cyber Essentials Certification is a UK Government-backed scheme, which helps businesses achieve a satisfactory level of cyber protection.

The scheme will help businesses avoid, or at least minimise, the impact on their business of:

- Phishing attacks
- Malware
- Ransomware
- Password guessing
- Network attacks

Specialist Partner Solutions

Aviva Risk Management Solutions can offer access to a wide range of risk management products and services via our network of Specialist Partners who are reputable companies offering agreed discounted rates for Aviva customers.

For more information please visit:

Aviva Risk Management Solutions-Specialist Partners

Sources and Useful Links

- National Cyber Security Centre (NCSC)
- ActionFraud

Additional Information

Relevant Loss Prevention Standards include:

To find out more, please visit Aviva Risk Management Solutions or speak to one of our advisors.

Email us at riskadvice@aviva.com or call 0345 366 6666. *

*Calls may be recorded and/or monitored for our joint protection.

Please Note

This document contains general information and guidance only and may be superseded and/or subject to amendment without further notice. Aviva has no liability to any third parties arising out of ARMS' communications whatsoever (including Loss Prevention Standards), and nor shall any third party rely on them. Other than liability which cannot be excluded by law, Aviva shall not be liable to any person for any indirect, special, consequential or other losses or damages of whatsoever kind arising out of access to, or use of, or reliance on anything contained in ARMS' communications. The document may not cover every risk, exposure or hazard that may arise and Aviva recommend that you obtain specific advice relevant to the circumstances.

24th October 2024

Version 1.3

ARMSGI262023