## NEN – The Education Network

# Guidance Note: Ransomware

### What is ransomware?

Ransomware is a form of malware which enables criminals to lock computers and files from a remote location. The user is then informed that the computer and/or files will not be unlocked until a ransom fee is paid. Ransomware can be activated in a number of ways, for example, by opening a malicious email attachment, clicking a malicious link or visiting a corrupt website. Often ransomware is distributed through phishing emails containing apparently authentic email attachments or links to apparently genuine websites. Such emails purport to be from genuine sources, such as social media sites, banks or sometimes even another individual from the same organisation (spoofing).

Ransoms are often demanded in the form of Bitcoins to protect the identity of the attacker. See further guidance from GetSafeOnline, the UK National Cyber Security Centre and the US Computer Emergency Readiness Team (US-CERT, more ransomware guidance here) for more detail. Recent months have seen a significant number of reports of ransomware attacks and incidents, many focussing on the healthcare sector (see these examples from PublicTechnology, BBC News, Ars Technica and SecurityInfoWatch). UK councils have also been targeted, again see PublicTechnology.

This document provides introductory guidance on how to prevent ransomware attacks and what to do if you are a victim of one. Also see the NEN's e-security advice for more guidance on how to keep your network and users secure. Your broadband service provider should also be able to provide further advice.

### How to protect against ransomware attacks

Recovering from a ransomware attack is non-trivial so it makes sense to take precautions to prevent them as far as possible. The following suggestions reference the 20 Critical Security Controls (CSCs) set out in the NEN School e-Security Checklist.

**Back up your data, regularly:**

- Make sure you have frequent, regular and tested backup and recovery procedures in place (see CSC 8). A key defence against an initiated ransomware attack is having the capability to restore files and data quickly from the most recent backup, before the ransomware attack commenced. This removes the ransomware threat whilst minimising the amount of data lost.
- Some types of ransomware will encrypt files on drives that are mapped to your device, so it is important to opt for an external drive or remote backup service, one that is not assigned a drive letter or is disconnected when it is not doing a backup.
- Remember that replication of data is different to backing up data: data replication may be useful for retrieving files under normal circumstances, but it is possible ransomware would infect the replicated data location too. A backup is a copy of the data at a point in time, which (on the assumption it is working correctly) can be restored to the source at a later time.

**Keep software up to date:**

- Ransomware often exploits weaknesses in application or operating system software; regular and timely installation of patches and software updates can help to prevent this (see CSC 3, 4, 5, 6 and 10).
- Some malware installs via features in applications that many users do not require; configuring software to disable such features can prevent this (see CSC 2, 3 and 6).

**Manage permissions appropriately:**

- Restricting users' ability (permissions) to install and run unwanted software applications and access network services may prevent malware from running or limit its capability to spread through the network (see CSC 12 and 15).
- It is common for malware to need elevated permissions to do real damage to a device, and it can obtain this through administrator level accounts. Don't give yourself more permission than you need. Don't stay logged in as an administrator any longer than is strictly necessary, and avoid browsing, opening documents or other "regular work" activities while you are logged in with administrator rights.

**Make sure anti-malware software is up to date:**

- Make sure that all anti-malware software is kept up to date; tools that look for and alert about unusual activity on networks as well as for known attack signatures can provide the most effective defence (see CSC 4 and 5).
- Whilst some ransomware is complex and elaborate, others are relatively simple and can be caught by a good, up-to-date anti-malware solution.

**Educate your users:**

- Educate all users (staff and learners) on the importance of cyber security and promote a culture of good cyber hygiene. A ransomware attack typically requires input from a user in order to be initiated (such as clicking on a link or opening an attachment), so encouraging users to be suspicious and to ask or check before clicking can help to prevent ransomware instances (see CSC 9). Tell-tale signs include web or email addresses that look unusual or suspicious, unfamiliar or incorrect language and demands that something is done immediately/urgently.
- Most malware spreads as a result of user action (or inaction). A common cause is the use of poor passwords (e.g. very simple words or phrases, or indeed the use of the same password by the same user across many different services).

**Make sure remote access is secure:**

- If you connect to school from home it is quite likely that you'll be doing so using RDP (Remote Desktop Protocol). Some types of ransomware specifically target machines using RDP. As a user, the best way to defend yourself is to ensure that your password is sufficiently strong. As an organisation you can also take steps to harden RDP against attack (including limiting the number of login attempts on the server to mitigate brute force attacks).

**What to do in the event of a ransomware attack**

US-CERT's advice *Ransomware: What it is and what to do about it* suggests the following in the event of a ransomware attack:

- Isolate the infected computer immediately. Infected systems should be physically removed (disconnected) from the network as soon as possible to prevent ransomware from attacking network or shared drives. Also isolate or power-off affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
- Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware (CSC 8).
- Contact law enforcement immediately. The UK National Crime Agency (NCA) encourages anyone who thinks they may have been subject to online fraud to contact Action Fraud. It is a matter for the victim whether to pay the ransom, but the NCA encourages industry and the public not to pay.
- If available, collect and secure partial portions of the ransomed data that might exist.
- If possible, change all online account passwords and network passwords after removing the system from the network. Furthermore, change all system passwords once the malware is removed from the system.
- Delete Registry values and files to stop the program from loading.
- Implement your security incident response and business continuity plan (CSC 8 and 18).

**Should I pay the ransom?**

US-CERT suggests ransomware victims may wish to consider the following factors, echoing the NCA's views outlined above:

- Paying a ransom does not guarantee an organization will regain access to their data; in fact, some individuals or organizations were never provided with decryption keys after paying a ransom. After paying the originally demanded ransom, some were asked to pay more to get the promised decryption key. Some victims who paid the demand were then targeted again.
- Paying could inadvertently encourage this criminal business model.

**The importance of defence in depth**

No security device or approach is 100% effective, 100% of the time, so it is important to take a "defence in depth" approach: the use of multiple different layers of security to protect school data and systems.

A good defence in depth strategy should include:

- **Firewa**ll – an enterprise-class, professionally-managed 'next generation' firewall provides a strong perimeter defence.
- **Web Filtering** – blocking user access to sites that contain malware is an effective means of reducing the likelihood of issues.
- **Anti-malware** – good anti-malware software on clients and servers reduces the likelihood of malware infection.

- **User awareness and training** – ensuring that users have the knowledge to spot and avoid threats is vital.

Whilst this may seem daunting and complex at first, the UK National Cyber Security Strategy 2016 – 2021 highlights that taking even straightforward precautions can make a huge impact on the success or failure of a cyber attack:

> "Cyber attacks are not necessarily sophisticated or inevitable and are often the result of exploited – but easily rectifiable and, often, preventable – vulnerabilities. In most cases, it continues to be the vulnerability of the victim, rather than the ingenuity of the attacker, that is the deciding factor in the success of a cyber attack."

Regardless of whether they procure and manage their own broadband services or subscribe to services provided by a local authority or regional broadband consortium (RBC), all schools need to ensure they have an appropriate and up to date strategy in place to ensure the security and integrity of their networks and systems.

All schools should draw up a policy for how cyber security is managed, maintained and reviewed in the light of new and emerging issues and risks. Cyber security is not something that can be "fixed" on a one-off basis; the changing nature of the threat landscape means that e-security policies and strategies require regular review and update if they are to remain effective.

Key to managing cyber security is an understanding of where the responsibilities for different aspects reside. Schools' responsibilities will differ depending on the nature of their broadband service. For example, some schools may rely upon in-house expertise to maintain their firewalls locally while others may choose to subscribe to a managed firewall service provided by a third party. The NEN School e-Security Checklist can help schools manage this.

Local authorities and RBCs provide cyber security protections as part of the services they provide to schools. It is essential that schools understand how their network is protected and by whom (including what the school is responsible for and what service providers and other third parties are responsible for) if security incidents are to be understood and dealt with effectively. See the NEN's e-security advice for more guidance on how to keep your network and users secure.

The increasing number of security threats and schools' increasing reliance on broadband networks and applications as "mission critical" services mean this is now more important than ever.