SWGfL

Education that Clicks

Ransomware White Paper

October 2016

South West Grid for Learning Trust Ltd, Belvedere House, Woodwater Park, Pynes Hill, Exeter, EX2 5WS
Registered in England and Wales, Company Number 5589479. Charity Number 1120354. VAT Reg. Number 880 8618 88

Contents

Introduction

A number of organisations have fallen victim to ransomware attacks in recent months. This document provides an overview of the guidance from SWGfL as well as signposts to products and services that can help.

What is Ransomware?

Ransomware is a kind of malware or malicious software that interferes with data on your device. It holds your device or files for "ransom" and will demand that you pay money to get access to your device or files.

There are different types of ransomware which behave in slightly different ways, including:

- Preventing you from accessing Windows
- Encrypting your files so you can't use them
- Stopping certain apps from running, including your web browser

Like other malware, ransomware targets any user, whether at home, work or school. There is also no guarantee that paying the fine or doing what the ransomware tells you will give access to your device or files ever again.

Types of Ransomware

There are thought to be over 120 different variants of ransomware in existence today, and there are two main types – ‘lockscreen’ ransomware and ‘encryption’ ransomware. Lockscreen ransomware shows a full-screen message that prevents you from accessing your device or files. It says you have to pay a “ransom” to get access to your device or files again. Encryption ransomware changes your files so you can’t open them. It does this by encrypting the files, and similarly requests payment of the “ransom” to decrypt them.

Well known examples include CryptoLocker and CryptoWall. Each variant can have a number of different ‘strains’.

What’s the point of Ransomware?

The distribution of ransomware is a criminal activity that involves someone trying to steal money. Some ransomware is operated by criminal gangs, others are available to buy from the underground market.

How does Ransomware infect your device?

Ransomware can get on to your device from nearly any source that any other malware (including viruses) can come from. This includes:

- Visiting unsafe, suspicious, or fake websites
- Opening emails and email attachments from people you don’t know, or that you weren’t expecting
- Clicking on malicious or bad links in emails, Facebook, Twitter and IM chats like Skype

How to reduce your risk of a Ransomware attack

Defence in Depth

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

A good defence in depth strategy should include:

- Firewall – 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

Back up your data, regularly.

If you can restore access to your data easily and quickly, the impact of a ransomware attack is going to be less disruptive. Some types of ransomware will encrypt files on drives that are mapped to your device, so it's 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's 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, reducing vulnerabilities.

Some ransomware will rely on security vulnerabilities in popular software applications, including Office, your browser, Flash etc. so it's important to keep yours up to date with the latest version.

Certain software also recommends that you uninstall older versions when you install the new ones, so that the vulnerabilities are closed.

Anti-malware is vital, keep yours up to date.

Whilst some ransomware is complex and elaborate, others are relatively simple and can be caught by a good, up-to-date anti-malware solution.

SWGfL recommends Sophos solutions and what's more we're able to offer schools top-notch protection from as little as £2.95 per device for 36 months cover. Click here to find out more.

Keep all your passwords sufficiently complex

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).

If you connect to school from home it's 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 against Brute Force attacks).

Only use admin rights when you absolutely have to

It's common for malware to need elevated permissions to do real damage to a device, and gets 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.

When it comes to emails, be suspiciously smart

Don't open emails and email attachments, or click on links, from people or organisations you don't know, or that you weren't expecting. If in doubt, don't open it!

Solutions

SWGfL offer a number of products and services that can support educational establishments to prevent the likelihood of a ransomware attack and minimise the disruption caused if it does happen.

- Remote Data Backup and Restoration
- Remote Access
- Endpoint Protection
- Information and Data security Self Review - 360data
- Cyber Risk Insurance

Remote Data Backup and Restoration

Schools must ensure that electronically stored data is protected, and that a safe and reliable backup strategy is in place.

One part of this strategy should include sending your data (the backed-up files) to an offsite location to ensure that, in case of an emergency, a complete copy of the schools most important data can be recovered quickly.

The RM RemoteSafe service allows schools to automate the backup of their important data to a secure offsite location (within the UK). In the event of an emergency the data is instantly available and can be recovered simply - ensuring that impact to your school operation is kept to a minimum.

http://esi.swgfl.org.uk/shops/swgfl/

Remote Access

If your school allows users to connect from home, it's quite likely that this will be via RDP (Remote Desktop Protocol). Some types of ransomware specifically target machines using RDP so it may be better to opt for a solution with increased security.

RM SSL Connect provides a simple but secure method of remote access to school systems. Securely access file stores, shared areas, network servers and other parts of your local network as if you were in school. As an encrypted Cloud service, there is no device or server installation is required, so once activated you're ready to go.

Simple to use and priced based on concurrent users, RM SSL Connect provides a low cost way for your staff to securely access their most important resources regardless of whether they're planning, marking or updating a server.

Anti-ransomware and Endpoint Protection

It's critical to keep devices protected from malware in general, not just ransomware. SWGfL offer a number of anti-malware solutions at preferential rates from Sophos including:

- NEW! Sophos Intercept X
- Endpoint Protection Advanced
- EndUser Protection Mail and Encryption
- EndUser Protection, Web, Mail and Encryption

We are delighted to introduce the new ground-breaking anti-ransomware solution, Sophos Intercept X, which incorporates powerful ransomware protection that is capable of automatically stopping ransomware attacks as soon as they are detected and rolling back damaged files to a known and safe state.

Sophos Intercept X can be installed alongside existing endpoint protection to fend off unknown exploit variants and stealth attacks that traditional cybersecurity software might miss – all with minimal impact to system performance.

To find out more register for Stop ransomware before it stops you:
Introducing Sophos Intercept X on Oct 13, 2016 12:30 PM BST at:
https://attendee.gotowebinar.com/register/6570332220555258370
Join SWGFL's Julia Adamson and Sophos pro, Matt Cooke as they discuss Sophos Intercept X and its application in schools. Matt will also demonstrate how this new technology can prevent modern cyber-attacks, including crypto ransomware. After registering, you will receive a confirmation email containing information about joining the webinar.

For more information:

For licensing visit https://www.phoenixs.co.uk/swgfl-sophos/

Information and Data Security Self Review – 360Data

Changing whole school culture on security requires a plan that not only has rigour but is well communicated; however, understanding all of those complex components can be difficult to manage.

360data is a unique self-review tool designed to help organisations test and improve their data protection policies and practices. Built on the same approach as the award-winning 360 Degree Safe, this tool will help your organisation understand what systems are currently in place and how to improve these.

During your review, you will be able to generate reports with a list of improvement actions to help you move forward with your organisation's data security. All the resources required to enact those recommendations are included in the tool.

For more details visit https://360data.org.uk/

Cyber Risk Insurance

Whilst we understand that technology in schools adds huge value to a schools' administration, teaching, learning and communication strategies, it can also present unique vulnerabilities and compromise as it offers an additional interface for engagement.

Not all engagement is positive and well-meaning and despite precautions and preventative measures, incidents can occur. A school's effectiveness is often measured in its ability to respond and manage incidents when they arise but, from an operational perspective, these can impact on a school's capacity and budget.

It's at these times that a school may need additional resource; a safety net.

SWGfL have worked with leading UK insurance brokers to create a Cyber & Data insurance policy specifically tailored for schools. It covers:

- Breach costs
- Cyber-business interruption
- Hacker damage
- Cyber-extortion
- Privacy protection
- Media liability

It's available for all schools through the SWGfL website. For more details, visit: http://www.swgflstore.com/products/cyber-and-data-insurance-for-schools-and-colleges. Further cyber risk insurance coverage from Hiscox is available from SWGfL, please contact esafety@swgfl.org.uk

Further Reading

- Ransomware – Don't fall victim
- One phish, two phish, red phish, blue phish…
- The secret to secure passwords
- How to stay protected against ransomware - Sophos Guide
- Microsoft guide to Ransomware
- 'Alarming' rise in ransomware tracked - BBC News article
- University pays $20,000 to ransomware hackers - BBC News article