Intrusion, Detection and Prevention

An increase in cyber-attacks involving ransomware affecting the education sector has had devastating effects. Loss of control, loss of data, loss of money- it’s a real threat to schools that don’t have the appropriate defences.

Hackers use Ransomware to encrypt files by luring staff and pupils to open seemingly innocent emails that contain Ransomware viruses. The following advice explains what Ransomware is and what your school can do to mitigate the risks.

What is Ransomware?

Ransomware is Malware that affects “endpoints.” These are your computer devices. There are two main types of Malware: one inhibits the operation of your device, and one encrypts user files, making it impossible to use your files or emails unless you agree to pay the ransom, or unless you have a back-up.

A user may click on an unsuspecting link, website or malvertising; once the infected link has been clicked, malicious code is then downloaded onto the user’s computer. The Ransomware is initiated into the user’s system.

Common Types of Ransomware

The most common technique is through Phishing attacks, via emails. The emails can contain malicious links or files, which once clicked will execute malicious code. Some emails do not need to be opened for encryption to take place. Files then become unusable and pop-up messages demand payment.

Adobe and Microsoft operating systems are common favourites amongst the professional cyber attackers, especially if users have outdated protection and do not regularly update it. Once the vulnerabilities are discovered in the endpoint (your computer or device) they are immediately exploited by infecting the system with Malware.

What Problems can Ransomware Cause?

A ransomware attack can result in a user's computer being held hostage. The attacker can threaten to publish the victim's data or block access until the ransom is paid. The attacks are typically carried out by a Trojan, a type of malware, which is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment.

Ransomware Protection

Ransomware can be difficult to detect as it is constantly changing. Offenders are continually testing new ransomware against the world's top security vendors using Exploit Kits to look for vulnerabilities in users' systems.

Schools Broadband's Intrusion Prevention System (IPS) safeguards customer networks from all known and unknown threats, protecting critical applications from external and internal attacks.

Backed by automatic, real-time updates delivered by FortiGuard Services, our Multi Threat Protection blocks new exploit kits every day, leveraging a database of thousands of unique attack signatures to stop attacks that might evade conventional firewall defences.

Anomaly-based detection also enables the system to recognise threats for which no signature has yet been developed by monitoring and blocking malicious network activity.

Fortinet is officially one of the industry's most effective enterprise firewalls, blocking over one million URL exploit kits every single day.

Endpoint Protection

Since the increase in ransomware, it is important you have extra Endpoint Protection for your desktops, laptops, tablets and mobiles to safeguard any vulnerable access points to your network. Endpoint protection is software that sits on your end device, e.g. PCs and AppleMacs. This strengthens the security of applications such as web browsers, PDF readers, email clients or MS office components which are commonly exploited.

Top Tips:

✓ The National Cyber Security Centre advises never to pay a ransom as there is no guarantee your files will be restored.

Paying a Ransom also fuels the cyberattack infrastructure.

✓ Report any scam or attack to Action Fraud: **0300 123 2040 www.actionfraud.police.uk**

✓ If you suffer a ransomware attack, there may be a way to unlock your devices without paying the ransom. Visit **www.nomoreransom.org**

✓ You can help prevent ransomware attacks by advising staff not to open unsolicited emails, attachments or SMS messages.

Find out more. Call or email:

0113 222 333

info@schoolsbroadband.co.uk

schools broadband™