SOPHOS

Security made simple.

CHECKLIST: HOW TO STOP RANSOMWARE

Key Technologies and Security Best Practices

Ransomware attacks start in two main ways. A booby-trapped email with a malicious attachment or via a compromised website; which then work their way down to your endpoints and servers. To stop these attacks, it's critical that you have advanced protection technology in place at each stage of the attack and combine this protection with good user security practices.

Securing your Endpoints and Servers

If ransomware makes it onto your endpoints and servers it's vital that you block and remove it as quickly as possible. Get the following technologies:

□ CryptoGuard Technology (available in Sophos Intercept X)

Secures your endpoints and servers with unique technology that stops ransomware in its tracks. CryptoGuard complements your existing security, blocking processes that attempt to make unauthorized changes to your data.

- Effective against CryptoLocker, Locky, Zepto, Cerber and much more
- Works against both local and remote encryption
- Automatically rolls back changes – no loss of data

□ Exploit Prevention (available in Sophos Intercept X)

Stops ransomware taking advantage of weaknesses in other software products.

□ HIPS Behavior Analysis/File Analytics

Examines the components/structure of files for malicious elements and checks if it contains code trying to modify the registry.

□ Web Security

Scans web content for ransomware code.

□ Malicious Traffic Detection (MTD)

Detects traffic to ransomware Command & Control servers and blocks it.

□ Application Control

Restricts what applications are allowed to run and can block Wscript – which is often used by ransomware.

□ Application Whitelisting

Establishes a "default deny" policy on servers so that only trusted applications can run – stopping ransomware from gaining a foothold.

Stopping Email Threats

The Email Gateway is your primary defense against malicious emails carrying ransomware. Make sure it includes:

□ Anti-Spam/Anti-Virus Technology

Blocks ransomware emails, including those with booby-trapped macro attachments and stops other email-borne threats.

□ Time-Of-Click Protection

Stops users from clicking on links to websites hosting ransomware – even if the link was safe when it entered the inbox.

□ Cloud-Sandboxing

Catches zero-day threats including ransomware, by testing files in a safe environment before the user runs them.

Stopping Web Threats

The Web Gateway blocks web-borne ransomware before they hit your users' endpoints. Look for the following:

□ URL Filtering

Blocks websites that are hosting ransomware and stops ransomware communicating with its Command & Control servers.

□ Web Filtering

Enforces strict controls on ransomware-related file types, stopping them from being downloaded.

□ Cloud-Sandboxing

Catches zero-day threats including ransomware, by testing files in a safe environment before the user runs them.

Nine best security practices to apply now

Good IT security practices including regular training for employees are essential components of every single security setup. Make sure you're following these nine best practices:

□ Backup regularly and keep a recent backup copy off-line and off-site

Offline and off-site means ransomware can't get to it. With recent backups data loss can be minimized.

□ Enable file extensions

Enabling extensions makes it much easier to spot file types that wouldn't commonly be sent to you and your users, such as JavaScript.

□ Open JavaScript (.JS) files in Notepad

Opening a JavaScript file in Notepad blocks it from running any malicious scripts and allows you to examine the file contents.

□ Don't enable macros in document attachments received via email

A lot of infections rely on persuading you to turn macros on, so don't do it!

□ Be cautious about unsolicited attachments

If you aren't sure – don't open it. Check with the sender if possible.

□ Don't have more login power than you need

Admin rights could mean a local infection becomes a network disaster.

□ Consider installing the Microsoft Office viewers

These viewer applications let you see what documents look like without opening them in Word or Excel.

□ Patch early, patch often

The sooner you patch the fewer holes there are for ransomware to exploit.

□ Stay up-to-date with new security features in your business applications

For example Office 2016 now includes a control called "Block macros from running in Office files from the internet".

Stay secure with Sophos

To stop ransomware before it stops you, you need the right protection in place. Use CryptoGuard technology in Sophos Intercept X to stop ransomware from encrypting your files. And make sure you have the right anti-ransomware technologies at your email gateway, web gateway, firewall, and servers to stop these threats before they ever get to your endpoints. Together they give you the very best chance of stopping ransomware from holding your data – and your business – hostage.

For more information on staying protected against ransomware

visit Sophos.com/ransomware

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS