Protecting your Networks from Ransomware

In light of the unfortunate Ransomware attacks experienced by some NHS hospital trusts, we thought it would be helpful to outline how Talk Straight Ltd protects our customers' networks, and give advice on what you and your staff can to do to further strengthen the protection.

What is Ransomware?

Ransomware is Malware that affects "endpoints." These are your computer devices. There are two main types of Malware: one which inhibits the operation of your device, even inhibiting the boot-up process and one which encrypts user files, making it impossible to use your files or emails etc. unless you agree to pay the ransom, or unless you have an alternative back-up.

How is Ransomware Distributed?

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

The most common Ransomware Techniques

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, when files become unusable and pop-up messages demand payment of the ransom.

Ransom Collection

Ransom payments are made via Bit Coins. Often the Ransomware is accompanied by instructions on how to purchase the Bit Coins, however it is advised NOT to pay the Ransom as this fuels the cyberattack infrastructure.

How do you protect yourself against Ransomware?

From a technical point of view, Ransomware is difficult to detect because it is constantly changing. Offenders are continuously testing new Ransomwares against the world's top security vendors. Exploit kits are used to look for vulnerabilities in users' systems, Adobe and Microsoft operating systems are commons 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 end system (your computer or device) they are immediately exploited by infecting the system with Malware.

WannaCry Ransomware

The WannaCry attack was particularly damaging, as so many systems were either out of date, or had not received the SMB patch update, despite the fact it was released by Microsoft in March this year.

Continues

How does Talk Straight protect your network?

Fortinet's Multi Threat Protection, (FortiGate and FortiGuard), continuously blocks new exploit kits every day. Our Intrusion Prevention System (IPS) safeguards customer networks from known and unknown threats, protecting critical applications from external and internal attacks.

Backed by automatic, real-time updates delivered by FortiGuard Services, FortiGate leverages a database of thousands of unique attack signatures to stop attacks that might evade conventional firewall defences, plus anomaly-based detection that enables the system to recognise threats for which no signature has yet been developed. It provides a wide range of features that can be used to monitor and block malicious network activity.

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

Extra Endpoint Protection

Since the rapid 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 Apple Macs.

Talk to us and we will recommend what we believe to be the best solution for you.

Educate Staff

- Let your staff know they should NOT open unsolicited emails, attachments or SMS messages
- Do NOT pay the ransom. There is no guarantee your files will be restored
- Report any scam or attack to: Action Fraud: 0300 123 2040 / www.actionfraud.police.uk

For more information please contact 01133 222 333

What to do if you suffer a Ransomware attack

If you ever suffer a Ransomware attack, the following website provides useful information on possible ways to unlock your digital devices without having to pay the ransom.

www.nomoreransom.org

May 2017
01133 222 333