ZYXEL

Defend Your Data from Ransomware Attacks

The threat of Ransomware

Take action now

Recent years have been challenging in networking and data security. The cryptoworm WannaCry and numerous other malware threats caused significant data breaches around the world to businesses and individuals. Malware attacks have resulted in huge financial losses in business productivity and reputational damage as personal data is compromised. For many this threat was new, but with increased media spotlight on data security and GDPR regulations, protecting data from malware and the ability to demonstrate it, should be a top priority for all businesses of all sizes.

The WannaCry attack was the turning point in the awareness of security threats. Suddenly malware was not about slowing down or compromising a few work stations. Malware and particular ransomware was now blocking entire networks in a matter of minutes across the globe.

The real cost of ransomware to business

Ransomware costs businesses around the word millions of dollars from the ransom itself to loss of productivity and their reputation. According to a study by IBM, 70 percent of targeted companies pay the required ransom - half of the more than 10,000 US dollars and 20 percent even over 40,000 US dollars, but paying the ransom does not guarantee the files will be released.

The real cost to businesses is downtime and loss of productivity. With restricted access to files and data, businesses can experience huge delays in accessing data, which can easily run to millions of dollars. Then there is the cost to the company's reputation if personal data is stolen or compromised.

Businesses of all sizes seem to be taking action but more needs to done. Most are reviewing their network security and have started to upgrade insufficient security protection, using the most up-to-date security technology and improving employee education of the threats. The demand for UTM (Unified Threat Management) and USG (Unified Security Gateways) has grown significantly and many have focused on upgrading Anti-Virus and Intrusion detection. But there are still many firms, especially SMBs, that are not taking the necessary action and should not consider themselves safe.

What is ransomware?

Ransomware is a form of malware (malicious software) and is also referred to as blackmail mail or a trojan. Ransomware encrypts files on a computer, device or smartphone and often on connected network drives via a security flaw or from an employee receiving and accessing malicious emails or websites.

The affected data becomes encrypted by the malware so the user cannot access files. The cybercriminals will then often demonstrate they have control of the files and will demand the victim transfers a certain sum (often in the form of cybercurrency) to them. Only then would the files be decrypted. But there is no guarantee that paying the ransom will allow the victim to regain access.

SMEs are increasingly under attack

Cases of ransomware infections are no longer only restricted to major companies. Even small businesses and even micro businesses are increasingly under attack. In 2015, SMEs were the most attacked companies with 43% of all cases. The common opinion of many SMEs that only large companies are in danger of falling victim to Ransomware is definitely wrong.

10 ransomware protection tips

What should IT administrators and employees consider to protect themselves against ransomware?

01. Backups! Backups! Backups!

Make regular backups of your data and save them separately from the wider network. Otherwise, the backups could also be encrypted. If your data is compromised, you will still have access to the backup.

02. Stay Up-to-date

Whether it is the operating system or applications make sure they have the latest manufacture updates. Manufacturers always update their latest software versions first. Therefore it is best to use the latest software versions as much as possible.

03. Unsafe Websites

Avoid visiting unsafe websites. Particular caution should be made when visiting blogs as they are the most frequently infected websites. Firewalls with protection mechanisms increase the security of surfing the web. In particular, content filters can help by blocking contaminated sites and the associated databases are constantly updated. Therefore, even “newly” infected websites are quickly marked and can no longer be accessed.

04. Take special care with emails

Always be suspicious of unsolicited email and above all do not open attachments. Fraudsters are becoming ever more sophisticated - be it fictitious job applications or authentic looking emails from financial service providers. If you are not expecting an email from a firm be skeptical and never reply, click on a link or open attachments.

05. Protection by hardware and software

Among the most effective protection mechanisms are firewalls. Combined with various software solutions, firewalls offer comprehensive protection against ransomware and other malicious programs - from gateway to endpoint protection (client). SSL inspection, VPN application intelligence, intrusion detection prevention, single-sign-on and content filters are now common functions of firewalls. In terms of software, anti-virus solutions as well as special anti-ransomware programs are a good idea. It is important that the programs and firewalls are coordinated so that there is no conflict.

06. Working without admin rights

Do not share the user profiles of the employees with admin rights. Many programs cannot be installed with normal rights and can minimise networks from being compromised by malicious software being installed.

07. Script blockers

Install a script blocker for web browsers to prevent the execution of malicious code on websites.

08. Raise awareness

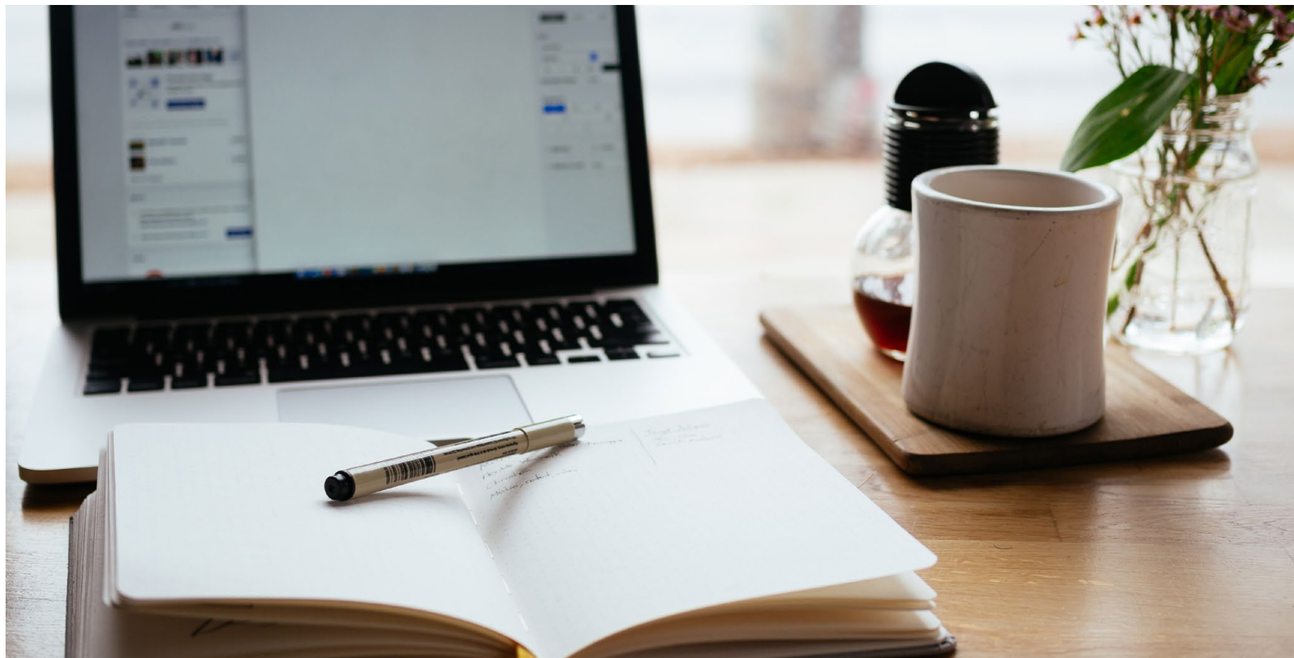
Set up regular training sessions for employees to reminded them of the potential threat of ransomware and their responsibilities to take action.

09. Be prepared

Plan for the worst case scenario and make sure everyone if aware of the crisis plan. What should employees do if their computers are infected and who should they contact? By making sure everyone is prepared, the crisis can be mitigated.

10. In case of an infection

Immediately disconnect the affected computer from all networks. Check if other computers on the network are infected and understand the source of the infection to minimise its spread. Then reinstall the system and change all passwords. Now load the backup. Paying ransom to the blackmailers is not recommended - there is no guarantee that the encrypted data will actually be decrypted.



The big questions

The Zyxel Training Course Leader Patrick Hirscher answers some of the big questions about ransomware.

Q. What is the threat posed by ransomware?

The threat is very severe, ever growing, and still difficult to assess. There is not one comprehensive solution that can solve all threats, but it is imperative that businesses of all sizes protect their networks as best they can, with up-to-date software and security networking devices such as the USG series from Zyxel.

Q. How can awareness of the issue be increased?

It is very easy to be infected with ransomware and it only takes one instance to severally impact your business. Everyone in an organisation needs to be aware of the threat and what action to take.

A large majority of infections come from email. Criminals are becoming increasingly sophisticated and clever in infecting networks using email as a route. Employees need to be aware not to open any unsolicited emails, click on any suspicious links or download anything unless they are completely sure it is legitimate. Businesses need to take a greater responsibility for training staff and making threats known and what action to take if they are infected, as well as relying on their technology/IT team to ensure their network security is robust and up-to-date.

Q. How can ransomware be blocked in incoming email?

An anti-spam solution with an integrated virus scanner is a good first step. However, ransomware attacks are becoming increasingly sophisticated and are, unfortunately, often not recognised by all anti-spam solutions despite the latest security technology.

If emails with suspicious attachments are blocked and quarantined it can however lead to negative consequences. The quarantining is often manually executed by an IT employee who checks the mail for its trustworthiness and then releases it to the addressee. This can lead to delays in emails being received by the recipient if the email is legitimate and lead to employee frustrations, but a cautious approach can identify threats before infection.

For public mail accounts, dedicated mailboxes can be used. These can deal with many general and potentially dangerous e-mails. The logged-in user works with very restricted rights on the file server. In case of a ransomware attack, the damage would be limited and kept under control.

Q. How can systems become immune to ransomware?

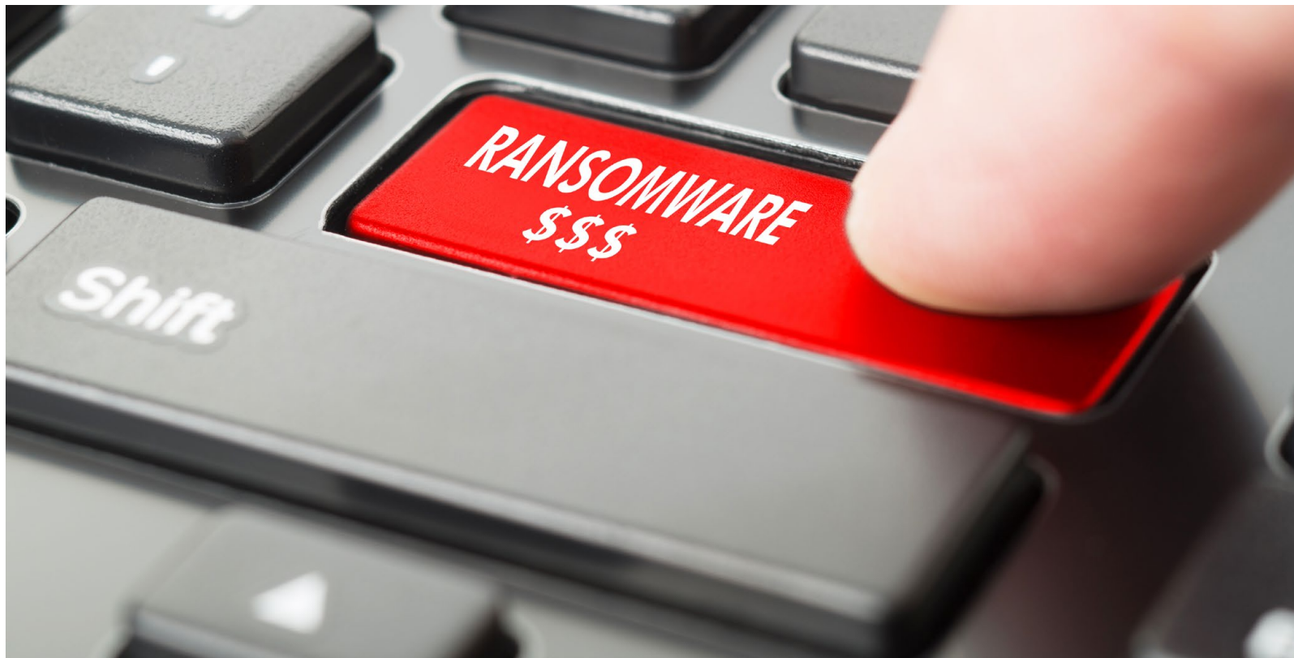
Make sure you continually upgrade your operating systems, applications and have the most up-to-date technology. As soon as new updates are made available by manufacturers, implement them as quickly as possible to ensure you are fully protected.

Q. Securing data with backups?

Make sure you are continuously backing up your data and files separate from the main corporate network. Try to ensure files are not stored locally on an individual's device.

Q. How can IT departments help?

IT departments should make sure the security of the company IT networks is operating as required, is well maintained and fully functioning. They can also have a role with training employees on the importance of security and building awareness throughout the organisation to ensure employees do not compromise the network.



Solving the ransomware problem

The number of cases involving ransomware and other malicious programs are growing rapidly and attacks are becoming increasingly more sophisticated, but so is the software and hardware fighting against them.

Robust affordable solutions

Businesses of all sizes can now opt for affordable solutions offering reliable protection against ransomware and other malicious software. Several security options exist to protect personal and enterprise networks from being compromised. Unified Security Gateways (USGs) provides a comprehensive solution for protecting against ransomware attacks through features including: anti-spam to block phishing emails, content filtering to prevent access to suspicious links, anti-virus to protect users from malware-infected files, and Intrusion Detection and Prevention (IDP) to detect and stop intruders from gaining control of your system.

Security “by design”

Zyxel’s Unified Security Gateway series offers highly integrated defence technology to provide the best protection for small, medium and large businesses against ransomware and other malware attacks via IDP inspection. Your data encryption requirements are met through IPSec and SSL VPN tunnel technology.

Security “by design” means a comprehensive, powerful and scalable solution that is at the core of the solution. Through licensing, you have the freedom to select and design the functionality that fits with your business.

Zyxel Unified Gateway Series integrated security defense technology

Anti-Virus

Prevent the latest content layer threats by detecting and removing malware.

Firewall

Monitor and control the incoming and outgoing network traffic

Anti-Spam

Reduce the number of spam messages, control attacks and virus infections via email

Application Intelligence

Allows or deny the use of web applications to prevent threats from entering the network

Intrusion Detection & Prevention

Check against network traffic flow to prevent known and unknown stealth cyber threats

WLAN Controller

Integrated in a WLAN control gateway to the radio receiver, reducing the cost of multi-machine deployment

Content Filtering

Prevent inappropriate content and dangerous sites on the Internet by blocking connections

VPN

High-end encryption technology to ensure mobile users have a safe connection to your network

Next steps to take action against ransomware

Take our security audit to understand your security requirements

For more information on how Zyxel can support your network security needs, request a call back from a Zyxel Security Specialist or visit zyxel.com