The Risk of Ransomware

PRACTICAL TIPS TO AVOID CYBERATTACKS

INTRODUCTION

The team at Integotec has packaged seven tips to help organizations across the globe protect themselves from the threat of ransomware. The tips provided do not require advanced technical knowledge to implement and are guaranteed to provide additional layers of security to every business's data.

RANSOMWARE DEFINED

Ransomware is a type of malware that attacks a user's files through encryption. When this happens, a user's data is inaccessible. The data is scrambled, corrupted, or deleted until a ransom is paid to the hacker -- thus, giving it the name *ransom*ware.

Ransomware occurs in various forms. Some hackers threaten to release the data to the public, while others infect the user's computer with malicious programs. In either case, the same principle is involved -- hackers gain access to a user's computer and demand thousands of dollars in payment for the issue to be resolved.

THE DANGERS OF RANSOMWARE

Businesses may find themselves in major financial loss when they become victims of ransomware. Loss of data can be damaging to any business, not only to those that deal with sensitive information. It can take weeks to recover years' worth of work that is critical to the organization's day-to-day operations.

In addition, organizations that experience a ransomware attack will have to spend thousands of dollars to replace infected computers. They will need to hire an IT company to strengthen their systems, preventing future attacks from happening.

SPAM EMAILS: THE LEADING CAUSE OF RANSOMWARE

According to MSPs, spam and phishing emails were the leading cause of ransomware attacks in 2020. Phishing is a method employed by cybercriminals to gain access to sensitive information. This is typically done by impersonating legitimate organizations in emails that include seemingly genuine links. These links lead the user to a website where they are required to fill in their information such as their email address, credit card number, and password. In some cases, phishing emails contain viruses in the form of links or attachments that the user then download unknowingly.

When this happens, ransomware locks down the user's data -- and in some cases their entire computer. The problem with ransomware is that it utilizes military-grade encryption that prevents users from decrypting the data by themselves.

Ransomware can infect anyone at any time, which is why it is crucial for organizations to know how to prevent this ever-evolving virus from impacting their activities.

HOW ORGANIZATIONS CAN AVOID RANSOMWARE ATTACKS

#1 TRAIN EMPLOYEES ON CYBERSECURITY

The second and third leading causes of ransomware are gullibility and lack of cybersecurity training. It takes only one employee to click the wrong link for your organization's entire system to fall victim to ransomware. Employee education can help prevent ransomware attacks from happening within your organization, as well as make your team more cyber-aware.

#2 AVOID OPENING SUSPICIOUS LINKS & ATTACHMENTS

Train your team not to click suspicious links even if the email came from someone with whom they are familiar. Hackers often compromise a user's account to send out malicious links to the person's contacts. Bad links could originate from someone whom you trust, such as a colleague, friend, or family member. If you suspect that your contact's account has been compromised, use other means of communication (e.g. calls, text messaging) to verify.

#3 BLOCK CERTAIN FILE EXTENSIONS

Most ransomware attacks spread through emails that contain malware-infected attachments. These attachments come in seemingly harmless forms, such as Microsoft Office documents that are commonly used in your organization. Regardless of how you and your team come across file formats that you've never seen before (e.g. exe, vbs, and xls), configure your email server to block certain filename extensions.

#4 TURN THE WINDOWS FIREWALL ON AT ALL TIMES

The Windows Firewall is there for a reason. Always enable the Windows Firewall to protect your computer from unauthorized access such as a cybercriminal attempting to infect your system with ransomware.

#5 PERFORM REGULAR BACKUPS

Your organization must perform regular system backups to ensure that data is not entirely lost in the event of a breach. Securely store these backups off-network and conduct regular scans of the backups to ensure that they are free of malware. As a rule of thumb, it is best to create three copies of the backup. Store one of the backups offsite and away from the network.

#6 USE STRONG PASSWORDS

Weak passwords such as password123 allow malicious individuals to hack into your organization's network. Once they've gained access, they can do whatever they want, including deploying ransomware. Require your employees to use strong passwords that:

- Contain more than eight characters (the longer, the better)
- Mix uppercase and lowercase letters
- Use numbers and symbols
- Are unrelated to the business
- Do not contain personal information
- Do not contain words found in the dictionary

#7 INSTALL ANTI-VIRUS SOFTWARE

One of the best ways to prevent ransomware is by installing strong anti-virus software. This security solution blocks malicious activity from infecting your systems, as well as shows administrators which devices are at risk of being compromised. Make sure that your organization’s anti-virus software is always updated, as cyber threats are constantly evolving.

BE PREPARED FOR RANSOMWARE ATTACKS

Statistics from the Federal Bureau of Investigation (FBI) show that since 2016, there have been more than 4,000 ransomware attacks per day. According to the report, one of the common targets of cybercriminals is businesses. With the shift to remote work, this number is expected to grow exponentially. The need for security is stronger than ever.

It is time to take your organization’s cybersecurity seriously. If you do not have security systems in place, Integotec offers cutting-edge solutions that will safeguard your network from even the most sophisticated cyberattacks. With more and more threats emerging each day, it is essential that you treat your organization’s data, as well as your customers’ data, with the utmost security.

CONTACT INFORMATION

Learn more about how you can defend your organization from ransomware. Visit us at integotec.com today or dial **541-527-4460** to get in touch with one of our IT experts.

Follow us on Twitter: https://twitter.com/integotec
Connect with us on Facebook: https://www.facebook.com/integotec/