HOW TO PROTECT YOUR BUSINESS FROM RANSOMWARE

Take these proactive steps to keep your company’s files from being held hostage
Three levels of ransomware

Ransomware: A type of malicious software designed to block access to or threaten exposure of sensitive data.

**Scareware**
Fake antivirus tools pretend to detect malware issues and demand payment to fix them.

**Browser or screen locking ransomware**
Attackers use fake FBI or US Department of Justice messages to claim they’ve detected illegal activity on your computer for which you need to pay a fine.

**Encrypting ransomware**
Starts as malware, spreads laterally to other endpoints, captures and encrypts files. Attackers demand ransom for encryption key and “promise” not to expose data.
How dangerous is encrypting ransomware to your business?

**Relevance**
Ransomware attacks now occur every eleven seconds and 69 percent of firms worldwide have experienced a ransomware breach in recent years. Virtually every organization, small or large is at risk from an attack.

**Recovery**
Almost 60 percent of endpoints harbor hidden threats including harmful Trojans, rootkits, and obfuscated malware that can lead to ransomware. Many industry experts concur that breaches may be inevitable, making recovery as important as detection and prevention.

**Ransom**
In 2016, businesses could expect to lose a few thousand dollars in a ransomware attack. Today, the average ransom exceeds $312,000 and some firms have paid tens of millions. As the size of the breach increases, so does the cost to your business.

**Reputation**
IBM and Ponemon studies show that delayed response and slow recovery after a ransomware attack can be costly. Remediation can take months and the average cost is now almost $4M, however, brand and reputation damage can be even more costly.

Sources: 2021 Study, Cybersecurity Ventures; 2020 EDR Study, Ponemon Institute; Combating ransomware, Ransomware Task Force
Should you pay the ransom?

FBI and other law enforcement agencies strongly encourage individuals and businesses to not pay the ransom. Doing so encourages more attacks and there's no guarantee that paying will give you access to your files again, or prevent public exposure. Also, it can make you an even greater target for future malware infection.
You’re vulnerable if...

- You only use traditional antivirus.
- Your remote desktops are unprotected.
- You operate with outdated systems.
- You don’t have a comprehensive resiliency plan.
- You lack a detailed cybersecurity framework.
Proactive prevention

The best prevention is to be proactive. Take these steps to keep ransomware from harming your business.

1. **Patch your systems**
   - Keep browsers, OS’s, and other software applications up-to-date.

2. **Educate users**
   - One of the most common ways that computers are infected with ransomware is through email phishing. Educate users on how to detect phishing campaigns, suspicious websites, and other scams.
3. Stop brute force attacks

Attacks use brute force attacks to discover remote desktop passwords. Employ solutions to prevent these attacks.

4. Backups are important

Backups are your last line of defense and attackers will delete them if they can. Protect your organization by keeping a copy of your data off-site and offline where ransomware can't reach it.

5. Invest in layered security

Employ multiple layers of endpoint cybersecurity that extend beyond only detection and prevention. These are critical, but resilient recovery is just as important.
How do you know if you’re infected?

Malware can spread laterally and lead to ransomware. The National Institute of Standards and Technology (NIST) and similar agencies recommend implementing a Zero Trust Architecture (ZTA) by frequently scanning endpoints for infections, and then removing all executables, artifacts, and changes before trusting an endpoint.

Take your first step in proactive prevention and try out Malwarebytes business products. Go to malwarebytes.com/business to learn more.