How To Protect Yourself From Ransomware Attacks

RANSOMWARE ATTACK

Your personal files are encrypted

You have 5 days to submit the payment!!!

To retrieve the Private key you need to pay

Your files will be lost

Ransomware is the second most common type of malware attack, according to Verizon's 2019 Data Breach Investigations Report (DBIR). Ransomware prevention is a complex topic that security experts are continuing to learn about, let alone small and medium-sized businesses.

What is a Ransomware Attack?

Ransomware is a multi-staged attack that has some common elements. The basics are the same: infiltrate the target's network, encrypt data, and extort the target for a ransom.

1. Infection

Attackers need to deliver malware to the target, which often occurs through a phishing attack. The malware might be included in the file attachment. From there, the ransomware works locally or replicates itself to other computers on the network.

2. Security Key Exchange

After the malware has infected a company's systems, it reaches out to attackers to let them know and get the cryptographic keys. With these keys, the ransomware can encrypt the victim's data.

3. Encryption

Now, the ransomware begins to encrypt the files on the victim's computer or network. It might start with a local disk and then probe the network for shared files. There are also other types of ransomware:

- Non-encrypting ransomware, which restricts access to data but doesn't encrypt them
- Leakware or extortionware, which exfiltrates data that attackers then threaten to release if the ransom isn't paid
- Mobile ransomware, which infects cell phones through fake apps

4. Extortion

This is the moment when you receive the message asking for a ransom. Usually, there is a dollar figure or Bitcoin amount attached, with threatening messages like "pay us or you will lose all your data." There are many variations on this message, but generally speaking, they will include instructions for paying and a deadline.

5. Unlocking and Recovery

Will the criminal send over the decryption keys once the ransom is paid? Sometimes yes, and sometimes no. When a cyber forensic expert is there to help, it's easier to determine which threat actor you're dealing with. Some threat actors are known to honor their word, while other variants may not come through with the decryption key even after payment. In either case, it's best not to try to negotiate with the attacker because they may raise the ransom amount in retaliation.

One option is to choose not to pay the ransom and attempt to restore the data from backups. However, this depends on having sufficient backups and on knowing that the attacker won't release the data to the public.

How to Protect Yourself from Ransomware Attacks

There are many things that a company can do to build a defense against ransomware and mitigate the damage in the event of an attack. Here are seven methods to protect yourself from a ransomware attack:

1. Keep Your Antivirus Software up to Date

It sounds simple, but antivirus software can stop malware in its tracks. The first line of defense is to install a high-quality antivirus program with ransomware protection.

2. Employee Education

Clicking on a bad link is still the most common way ransomware attacks occur. Educating users is one of the most powerful tools you can implement to prevent an attack. There are many ways to do this effectively. Companies can choose from any number of computer-based training programs to drill employees on recognizing phishing emails and responding to a simulated attack. Many of these programs will also include data metrics to track progress over time.

3. Make it Harder to Roam Your Networks

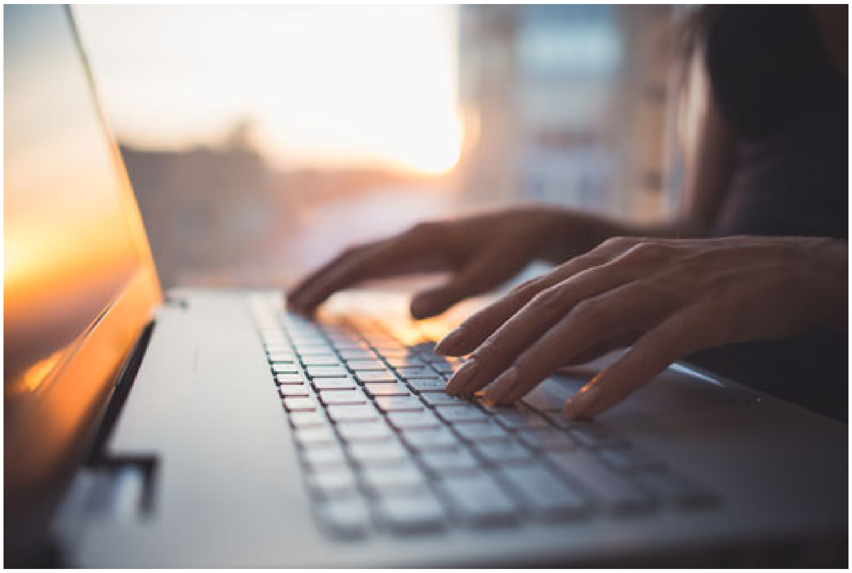
Ransomware groups are looking for the biggest return on their activities. Encrypting the data from just one computer won't make them rich, so their goal is to gain access to a large network where they can spread the malware before encrypting all your data.

Companies can make this harder by segmenting networks and by limiting the number of administrator accounts. Keep proper internal controls on administrator accounts to ensure that access remains limited. That means updating passwords regularly, creating complex passwords, allowing only three login attempts at a time, and defining who and when these accounts are to be used.

4. Change Passwords Across Access Points

While clicking on a bad link in an email is a common way to get infected by malware, it's not the only way. Ransomware can be distributed through remote desktop protocol (RDP) attacks, meaning that the hacker attempts to access the server by using as many passwords as possible. Often, this is done with the aid of bots. If a company fails to change default passwords or relies on easily-guessed combinations, brute force attacks will likely succeed at one point. A company can reduce the risk of an RDP by using only strong passwords, changing the RDP port, and limiting its availability to only those devices that need it.

5. Patch Software Vulnerability
Patching software is a time-consuming and tedious job, but it’s vital to any security strategy. Malware groups will take advantage of any software vulnerabilities and use them to enter a network before the business has had a chance to deploy patches. Though patching is a stop-gap measure until a new version of the software is released, it can save an organization from being breached. The IT department should be scanning for and patching any system vulnerabilities to keep systems safe.



6. Enable Multi Factor Authentication
Multi factor authentication is any security system that verifies a user’s identity by requiring multiple credentials. The user typically must present at least two types of information to the authentication mechanism: either knowledge (something only the user knows), possession (something only the user has), or inherence (something only the user is). So for example, you’ve probably used MFA before when you logged into your bank portal or a Google account. Typically, you would input your name and password. Then as a second factor, you might have to use an authenticator app or a one-time code sent to your phone.

As you can see, multi factor authentication can be a powerful tool to enhance security. While there are many ways for hackers to acquire your username and password, it’s much more difficult to get access to another of your credentials. Use MFA wherever possible in your systems, especially on email. Email remains the number one method of communication for most organizations. It’s also the number one way that hackers will try to infiltrate your network and plant malware. While MFA isn’t foolproof, a two-step verification process can keep the bad guys out even if they have your password.

7. Utilize a Secure Email Gateway
Because email is one of the biggest sources of exposure to hacking threats, you should invest in a secure email gateway. Methods of attack are becoming more targeted, sophisticated, and dangerous –which is why you shouldn’t rely only on employee education to shield from phishing

and other threats. A secure email gateway offers a robust framework of technologies that acts as a firewall for email. It scans both outbound and inbound email for malicious content. By blocking, filtering, and quarantining potential threats, a secure email gateway significantly reduces the number of successful compromises involving company data.

Cyber Insurance as Protection From the Fallout of an Attack

Even if a company does everything right (though that’s hard to do when it comes to cybersecurity), there’s no substitute for keeping a cyber insurance policy in force. A cyber policy covers the vast array of costs that come with a data breach, including IT forensics, data restoration, legal defense, systems repair, and more.

Cyber insurance policies vary widely, which is why it’s helpful to be able to tailor them to the unique needs of each business. Minnesota Insurance Group offers some of the best-in-class insurance providers of cyber liability insurance through our relationship with ProWriters. We offer a simple quick comparison quote across multiple carriers through our CyberQuickRate Portal. Many businesses may not realize that they are at risk for a cyber breach. Ask us for resources that can help you develop your cyber security plan.