3 Steps to Protect Critical Business Data from WannaCry Ransomware Attack

On Friday, May 12, an unprecedented ransomware attack hit more than 200,000 computers in 150 countries. Experts warn that attacks like this will increase, and copycat versions of the initial ransomware have already been detected. Protect your organization's critical data now by implementing these key security measures.

In April, Symantec released its annual Internet Security Threat Report. The report warned that ransomware posed one of the most significant threats facing organizations. Just weeks later, cyber criminals launched a widespread ransomware attack. The attack crippled the hospital system in Great Britain and affected business and government networks globally.

Using a hacking tool stolen from the N.S.A., the WannaCry attack exploits a vulnerability in Microsoft Windows servers. As with many attacks, the malware entered victim organizations through an email attachment. Once opened, it spread to other vulnerable computers on the organizations' networks.

Users of infected computers found their data held hostage with unbreakable encryption. Attackers demanded ransom payment in bitcoin, threatening to destroy the data after a deadline passed. However, according to experts at Norton, in 2016 only 47 percent of victims who paid ransoms recovered their data.

To safeguard your data and ensure business continuity, start with these three basic but vital steps.

1. Back Up Your Data

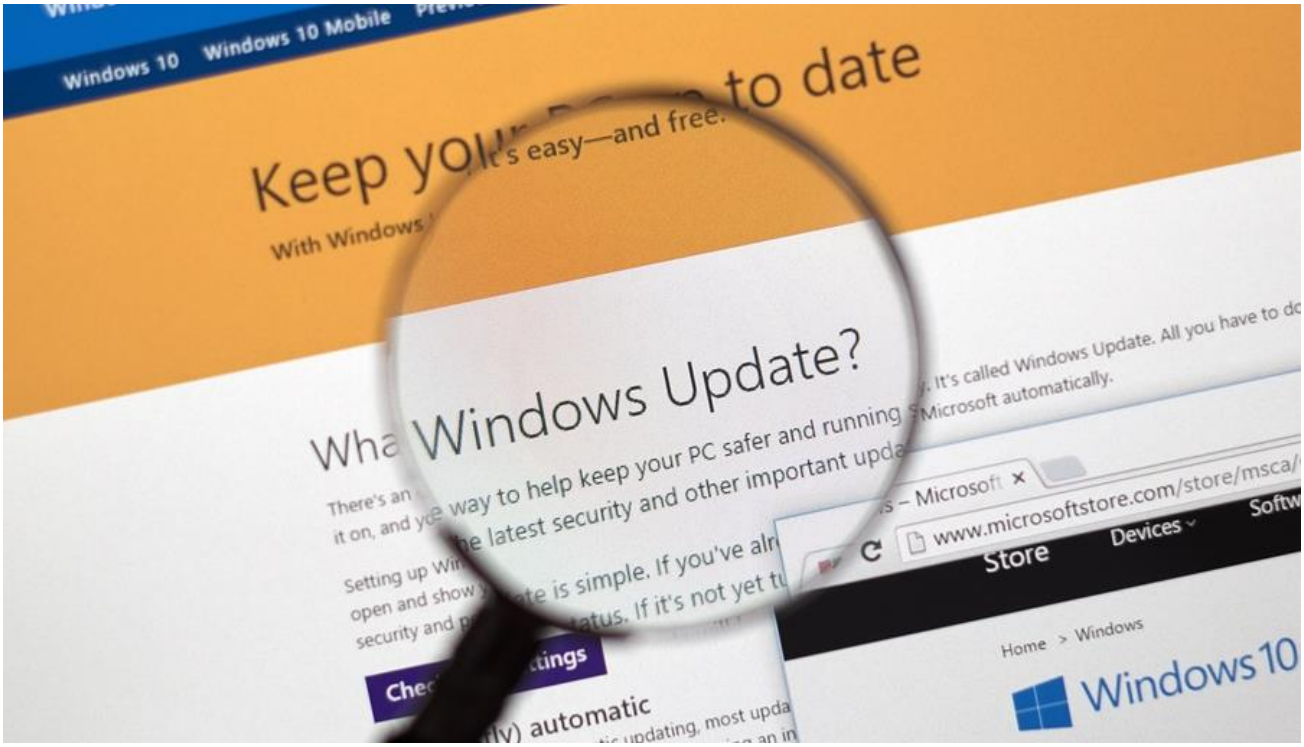
The most important step to take to defend against ransomware is to back up your data regularly and keep a copy of the backup off the network. Apply this simple rule of thumb: if you cannot live without the data, back it up.

Ransomware attackers gain leverage by making important files inaccessible. Businesses can easily remove that leverage by storing copies of critical data. With proper backups, a ransomware attack may disrupt operations temporarily during infection cleanup, but data loss is minimized.

2. Keep Your Software Updated

Not only is it critical to keep anti-virus software updated, but be sure to also update your operating system and other software. This helps to guard against recently uncovered vulnerabilities that attackers can exploit.

Two months prior to the May 12 attack, Microsoft received a tip regarding the server vulnerability. The company quickly released a patch that would have protected computers from the ransomware. Unfortunately, many organizations delayed implementing the patch.



In some cases, organizations delay deploying patches because of cost, compatibility issues with existing systems, or workflow disruption. Often, the cost of infection in lost data, crippled productivity and customer relations far outweighs the cost of updating.

If a legacy system absolutely cannot be updated, take measures to isolate the system on a strictly controlled segment of the network.

3. Practice Safe Email

The WannaCry attack employed a basic phishing email, an often used and effective method. Security systems failed to detect the encrypted file attached to the email. However, as soon as one user clicked the infected attachment, the wormlike nature of the malware allowed it to spread with unusual speed.

Simple email safety measures help guard against threats that find their way past security systems. Delete any suspicious emails, particularly if they include attachments. Be particularly cautious with Microsoft Office, JavaScript and .wsf attachments. And make sure any link sent by email is legitimate before you click on it.

More Ransomware Attack and Defense Strategies

While email currently represents the most common infection method, attackers employ a variety of strategies, including compromised web pages, malicious advertisements, secondary infections, third-party app stores and more.

In addition to the tips above, browse only trusted web sites and never download software from unknown providers. Avoid clicking on a banner or link without knowing its true source.

Peace of Mind with eMazzanti

Staying on top of emerging internet threats can tax your organization, diverting energy away from the core business. eMazzanti offers 24/7 protection for critical business assets with customized managed services. Count on multi-level security, software update management, email monitoring and more.

With proactive security measures in place, threats like the recent ransomware attacks will not leave you scrambling to recover vital business data held hostage. Minimize business disruptions and gain the peace of mind that comes with knowing that your data is more secure.