The Ultimate Checklist To Preventing And Fighting Ransomware Attacks

2016 is the year of ransomware, says a recent report by the Institute for Critical Infrastructure Technology, an industry think tank. When it comes to battling ransomware, your best offense is a good defense. Is your organization prepared to ward off an attack? Don't waste hours pondering a defense strategy. Use this checklist instead to shield your business from sophisticated attacks.

☐ 1. Back Up All Your Data

Your most powerful weapon to defeat ransomware is a regularly scheduled backup. In the event of an attack, power down the endpoint, then reimage it and reinstall a recent backup to prevent the ransomware from spreading to other systems on your network.

Eliminating ransomware will require wiping the system, so a system-state backup or snapshot is essential to rapidly recover from an attack. The more frequent the backup, the less data is lost. Backup frequency should be based on the
strategic importance of the data and how much data the organization can afford to lose. Since any attached device will be encrypted, the storage must be external and not mapped or connected to the device after the backup is completed.

☐ 2. Patch, Patch, Patch

Ransomware attackers frequently rely on people running outdated software with known vulnerabilities, which they can exploit to silently get into your network. Inconsistent patching and outdated software leave organizations exposed. Make a habit out of updating your software regularly. Patching commonly exploited third-party software such as Java and Flash will undoubtedly prevent many attacks from being successful.

☐ 3. Educate Your Users On Attack Sources

The weakest link in the security chain is usually human. By falling for a phishing email or other social engineering scheme, an employee could
leave your organization exposed. Educate your users around social engineering threat scenarios. Criminals use these tactics because it's usually easier to exploit people's natural inclination to trust than it is to discover ways to hack your software.

Security is all about knowing who and what to trust. Train your users to ask themselves these questions when reading their email:

1. Do I know the sender?
2. Do I really need to open that file or go to that link?
3. Did I really order something from this company?

☐ 4. Protect Your Network

Keep your network protected by deploying a layered approach. Use technologies such as a next-generation firewall (NGFW) and an intrusion prevention system (IPS). A layered defense can give you multiple approaches to enforcing security measures at multiple areas within a network. By removing single points of failure, you can effectively secure and safeguard your network and data.

☐ 5. Segment Network Access

Network segmentation limits the volume of resources that an attacker can access. It logically groups network assets, resources, and applications into compartmentalized areas. By dynamically controlling access at all times you help ensure that your entire network is not compromised in a single attack.

The majority of corporate networks are "flat," with little to no segmentation between business units, between users and data, between data specific to business units, and so on. Segmentation can be used to stop or slow the lateral movement of malware as well as contain threats.

☐ 6. Keep a Close Eye on Network Activity

You cannot protect what you cannot see. Gaining in-depth network visibility may sound like a daunting task, but it is a crucial one. The ability to see everything happening across your network and data center can help you uncover attacks that bypass the perimeter and infiltrate your internal environment.

Protect the perimeter by deploying and hardening a so-called demilitarized zone (DMZ). The DMZ is a physical or logical subnetwork that contains and exposes your organization's external-facing services to a usually larger and untrusted network, such as the Internet. It adds another layer of security to your local area network (LAN). It gives an external network node direct access only to servers in the DMZ rather than any other part of your internal network.

☐ 7. Prevent Initial Infiltration

Sometimes your users may innocently access compromised sites or emails that contain malvertising, thereby exposing your network to malware. Initial ransomware infections occur typically through an email attachment or a malicious download. By diligently blocking malicious websites, emails, and attachments sent by attackers as part of their ransomware campaign, you can keep your network protected.

Consider investing in a company-sanctioned file-sharing program for exchanging files between users in the organization and company partners. Using a file-sharing solution and instructing users to never share or accept files over email can almost completely mitigate phishing attacks that include attachments.

☐ 8. Arm Your Endpoints

Deploying an antivirus solution on your endpoints is not a sufficient defense against ransomware. Bring-your-own-device (BYOD) workplaces are increasingly popular, and you must find a solution that gives you control over the laptops, mobile devices, and tablets that enter your network. Critically, your solution should do two things: give you visibility into what's connected on your network, and help you enforce policies that prevent users from accessing compromised websites or downloading suspicious files.

Consider practicing the "least privilege" concept. That is, any given account should have the least amount of privilege required to perform appropriate tasks. Common places where this concept can be applied, but often is not, include user permissions on endpoints and user permissions on network shares. The key to this concept is that malicious software most often runs using the privilege level of the currently logged in user. If that user is an administrator, so is the attacker. Always use two-factor authentication. A hacker may steal passwords, but it's nearly impossible to steal those and a smartphone or token at the same time.

☐ 9. Gain Real-Time Threat Intelligence

To proactively combat a threat, it is important to know your enemy. Threat intelligence provides security practitioners with advance warning of cybercriminals targeting their region, industry, or even specific firms so that you have time to take action.
So, how do you gain real-time threat intelligence? By keeping your ear to the ground and learning from threat-intelligence organizations such as Talos.

The Talos team is composed of more than 250 full-time threat researchers who work to protect against known and emerging cybersecurity threats. The team publicly shares security information through blog posts, newsletters, social media, community forums, and instructional videos to help make the Internet safer for everyone. You can benefit from their work by following their content closely and updating your organization when a threat hits close to home.

☐ 10. Say NO to Ransoming

Although many businesses are tempted to pay the ransom to regain control over their systems, this should be the last option for you to consider. Contact the authorities instead and refrain from funding these cybercriminals by paying the ransom.

For More Information

For more information on network visibility and Cisco Ransomware, visit http://www.cisco.com/go/ransomware.