The Ultimate Checklist for Preventing and Fighting Ransomware Attacks
Ransomware has become the most lucrative type of malware ever seen. It’s expected to exceed $5 billion in damages in 2017 alone.¹ And it is continuously evolving to penetrate more networks: attacks have been growing by 300 percent a year.² If you’re worried about ransomware, it’s with good reason. But you can take these steps to reduce its risk to your business.

1. **Back up all your data**
   Your most powerful weapon to defeat ransomware is a regularly scheduled backup. Backup frequency should be based on the strategic importance of the data and how much your organization can afford to lose. It is vital to test your backups to make sure that the system is working and the correct data is being saved. Finally, backups should be stored offline so they cannot be compromised or deleted during an attack.

2. **Patch, patch, patch**
   Ransomware attackers frequently rely on people running outdated software with known vulnerabilities, which they can exploit to silently get into a network. Inconsistent patching and outdated software will leave you exposed. Having a set patching schedule helps you keep systems up to date and provides visibility into those that cannot be patched. This way, you can better understand and address risks before they become a problem.

3. **Educate your users on attack methods**
   The weakest link in the security chain is usually human. By falling for a phishing email or other social engineering scheme, an employee may leave your organization exposed. Reinforce your users’ knowledge with regular testing and focus their training on specific areas where needed.

4. **Protect your network**
   Keep your network protected by deploying a layered approach; protecting your endpoints, network, email, and DNS layer. 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.

¹ – Cybersecurity Ventures, *Ransomware Damage Report*, May 2017
² – The United States Department of Justice, “How to protect your networks from ransomware”
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.

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

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. Your solution should 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.

9. Gain real-time threat intelligence
To proactively combat a threat, you must know your enemy. Threat intelligence provides you with advance warning of cybercriminals targeting specific regions, industries, or firms so that you have time to take action.

10. Don’t pay the ransom
Although you may be tempted to pay the ransom to regain control over your system, remember that there is no promise you will be granted access back. Contact the authorities instead and refrain from funding these cybercriminals.