mimecast

RANSOMWARE SURVIVAL
Top 10 Ways to Protect Your Organization from Ransomware

RANSOMWARE IS SKYROCKETING AS AN ATTACK TECHNIQUE ACROSS MANY INDUSTRIES.

No organization is exempt from ransomware attacks as it continues to be one of the most prominent malware threats used by cybercriminals. To survive a ransomware attack, you must be prepared.

More than **4 million** new ransomware samples were discovered in 2016.*

Global ransomware damages are predicted to exceed **$5 billion** in 2017.**

Within a day, **WannaCry** reportedly infected more then **200,000 computers** in over **150 countries**. ***

What can you, as a security IT professional, do to help protect your organization from ransomware?

PROTECTIVE CONTROLS

Start with protective controls that can help keep ransomware off your network and minimize the spread should it sneak in. Remember that ransomware can gain access to the network in a variety of ways – including email, drive-by-downloads, web-facing systems vulnerabilities, and even USB drives – so it's important to use multiple layers of protective controls.

1. **SECURE EMAIL GATEWAYS (SEG), SECURE WEB GATEWAYS (SWG)/FIREWALLS, AND ENDPOINT SECURITY** solutions are the first line of defense in preventing ransomware from gaining access to your organization. Multiple layers of protection are necessary for a robust defense.

2. The best protective solutions still require **CONSTANT VIGILANCE** in terms of assessing potential gaps. Vulnerability scanning and timely patching to fix discovered vulnerabilities that ransomware might exploit are essential, especially for systems running Microsoft Windows.™ It's vital that all security hotfixes from Microsoft are applied to all systems as soon as possible.

3. Some ransomware will attempt to move from the initial point of compromise to other PCs, network drives and servers. **AIR GAPPING THE CORPORATE NETWORK** from other critical infrastructure systems can prevent ransomware from spreading to where it could do significant damage.

4. **USER SECURITY AWARENESS TRAINING** can significantly reduce the risk of employees making mistakes that can enable a ransomware attack. Make sure the "human firewall" at your organization is sufficiently trained to spot and alert IT to potential attacks.

5. **ENSURE THAT IT SECURITY IS PART OF THE PROCESS** when reviewing new or existing vendors/suppliers that supply or maintain network-enabled systems because many breaches originate from third-party vulnerabilities.

6. Take steps to reduce credential harvesting attacks as compromised insider accounts are in a position to help land and expand a ransomware attack. **USE MULTI-FACTOR AUTHENTICATION** to make it far more difficult for attackers to obtain and use stolen credentials.

7. **NETWORK AND ENDPOINT MONITORING** can detect ransomware infections and provide an early warning. Systems might include a security information and event management system (SIEM) that is capable of combining and analyzing multiple data feeds to increase visibility across the organization. Next-generation endpoint security products can also play an important role in detecting ransomware attacks.

RESPONSE CONTROLS

Well-documented procedures and supporting solutions can make responding to a ransomware attack far easier and faster.

8. **BACKUP & RECOVERY PROCESSES** supported by immutable backups of all critical systems enables IT to bring infected systems back online much faster. It's imperative that these backups are isolated and can't themselves be impacted in the event of an attack. In addition, backups should be periodically tested to ensure data can be restored quickly and easily.

9. For critical communication platforms and operating systems, any downtime could negatively impact the organization. Make sure that these systems have the **NECESSARY CONTINUITY PLANS** in place.

10. Responding to a ransomware attack requires mature incident response procedures that are rehearsed regularly so that every team member knows their responsibilities. This should go beyond the obvious IT and security personnel to **INCLUDE MANAGEMENT, HR, PR, LEGAL AND OTHER IMPORTANT STAKEHOLDERS**.

A ransomware attack can disrupt business operations, render critical infrastructure unusable and significantly damage the organization's brand. Prepare your organization to prevent, detect and respond quickly to ransomware.

Mimecast makes email safer for business.

LEARN MORE

* 2017 Verizon Data Breach Report, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
** Cybersecurity Ventures, https://cybersecurityventures.com
*** NHS, BBC, http://www.bbc.com/news/world-europe-39907965 200K computers, NBC News, http://www.nbcnews.com/news/us-news/blockbuster-wannacry-malware-could-just-be-getting-started-experts-n759356