NetDiligence®

Call to Action on Ransomware

Must-Have Ransomware Safeguards

February 2020

Must-Have Ransomware Safeguards

NetDiligence® Call to Action on Ransomware

Ransomware is very difficult to prevent. Not only are the malware and attack vectors constantly changing to slip past traditional security measures but prevention often hinges on human vigilance. Warning people to think before they click is simply not enough to keep the threats at bay.

To prevent or mitigate many types of serious cybersecurity threats, organizations must assume their frontline defenses will be defeated and deploy layers of safeguards.

Antivirus & Endpoint Protection

- **Use antivirus and anti-malware software** to block known payloads from launching. Note that your AV software won't necessarily protect you in scenarios such as a zero-day attack. With ransomware constantly morphing and threat actors regularly tweaking the code, the known signatures may not be flagged by traditional antivirus programs.
- **Deploy next generation anti-malware protection on all endpoints**. This is now a baseline standard of care given the rampant rise of ransomware. Example solutions are Crowdstrike Falcon Prevent and Carbon Black, or Norton360 for consumers. Malwarebytes can be an additional layer of valuable protection that does not conflict with other packages. These solutions often prevent ransomware by flagging malicious behavior rather than static signatures.

Must-Have Safeguards

Call to Action on Ransomware

Backups

- **Segment your backups**. Be sure to make frequent, comprehensive backups of your important files and isolate them from your local and open networks. A good way to do this is by deploying a cloud backup service. Should a ransomware attack occur, the ability to restore from backups may be a vital recourse for recovery.
- **Keep offline copies**. Keep offline backups of your vital data to avoid the accidental spread of malware from publicly connected infected computers. Make sure your external storage drives or cloud backups are properly disconnected from your main corporate network to prevent backups from being accessed/infected by the spread of ransomware. Cybersecurity experts have posited that in up to 80 percent of incidents, certain types of ransomware impacted both regular network/devices and the backups. Timely recovery following a successful ransomware attack is significantly impacted by the efficacy of backup and backup segregation practices.

Segment Your Network

- If possible, **segment your networks** to keep critical computers isolated and to prevent the spread of malware in case of attack.

- **Turn off network shares** (if not necessary).
- **Disconnect systems and segments** where possible. Interconnectivity should be permitted ***based only upon demonstrated business need***—otherwise, ransomware attacks can be accelerated and amplified.

Lock Down Admin Rights on Desktops

- **Turn off admin-level access** for staff users who don't require it. This should be the case for the vast majority of endpoint workstations and will help prevent malware from installing and executing if a staff accidentally clicks/launches on the wrong file or link.
- **Disable RDPs (remote desktop protocols)** unless they are vital and there is multi-factor authentication in place.

Patch Often

- Bad guys often take advantage of known vulnerabilities. Establish a daily process to **install the latest security updates** in your IT environment for desktops, laptops, servers, applications, browsers, mobile devices, and web plugins.
- **Turn on any auto-update feature** for operating systems and applications that have been approved by the business.

Staff Training and Cyber Hygiene

- **Regularly remind staff** to be careful about opening attachments or clicking on links, especially from unknown senders. Keep everyone apprised of the latest email phishing scams that seek to trick employees.
- **Be cautious even with known senders**. Bad guys can and will masquerade as a known friend, senior manager, or anyone with whom you have routine contact and they use this familiar email account to avoid detection and launch an attack.
- **Look closely at attachments**. Email attachments that look like PDF documents or photo images could actually be malware. Legitimate-looking business invoices are also a favored means of entry.
- **Consider investing in phishing training**. A drill can simulate emails from fake employees and test staff reaction, leading to more awareness of this insidious threat.

Have a Crisis Plan

- **Assume that a ransomware attack *will* happen**. Even with best practices in place, there's no way to completely avoid this growing scourge.
- **Create an actionable incident response plan (IRP), that you can access 24/7**. This should allow you to deploy your ransomware crisis strategy, including timely access to known experts to help minimize the damage and restore operations.
- One example of this is our Breach Plan Connect® solution. Learn more at https://netdiligence.com/portfolio/breach-preparedness/.

If you have an urgent issue with ransomware, contact management@netdiligence.com and we will connect you to experts who can help.