TIPS & TACTICS | PREPARING YOUR ORGANIZATION FOR RANSOMWARE ATTACKS

HOW DO I STAY PREPARED?

What do you do if your computer suddenly displays a countdown clock and a message telling you that your files have been encrypted and will be permanently lost to you unless you pay a ransom by a specified date and time? Whether you are responsible for protecting computers and data for a small business, hospital, local government, or other organization, it's vital that you be prepared for ransomware attacks. This guidance from the National Institute of Standards and Technology (NIST) includes basic practices for protecting against and recovering from ransomware attacks. Be sure to consult an expert if one is available to you.

PROTECTING AGAINST THE THREAT

The computers and information on which we rely are under constant threat from disruptive and potentially destructive ransomware. **NIST recommends that organizations take these basic steps to help thwart ransomware**:

- **Use antivirus software at all times**—and make sure it's set up to automatically scan your emails and removable media (e.g., flash drives) for ransomware and other malware.
- **Keep all computers fully patched**.
- **Use security products or services that block access to known ransomware sites** on the internet.
- **Configure operating systems or use third-party software to allow only authorized applications** to run on computers, thus preventing ransomware from working.
- **Restrict or prohibit use of personally owned devices** on the organization's networks and for telework/remote access without taking extra steps to assure security.

Users should follow these tips for their work computers:

- **Use standard user accounts** instead of accounts with administrative privileges whenever possible.
- **Avoid using personal applications and websites**, such as email, chat, and social media, from work computers.
- **Avoid opening files, clicking on links, etc. from unknown sources** without first checking them for suspicious content. For example, you can run an antivirus scan on a file, or look at a link to see if it goes to the site it claims to be going to.

NIST's National Cybersecurity Center of Excellence (NCCoE) has collaborated with the private sector on projects that can help organizations protect themselves against future ransomware attacks. An example is *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events (NIST Special Publication [SP] 1800-25)*.

Learn more about NIST NCCoE projects to improve data security practices at: https://nccoe.nist.gov/projects/building-blocks/data-security.

Organizations without dedicated cybersecurity professionals should consider establishing relationships with third-party cybersecurity service providers and using their expertise to assist in improving their protection against ransomware and preparing to recover from ransomware attacks.

Updated May 2021

RECOVERING FROM RANSOMWARE ATTACKS

Unfortunately, even though the recommended protective measures may be in place, a ransomware attack against your organization may still succeed. Organizations can prepare for this by taking steps to ensure that their information will not be corrupted or lost, and that normal operations can resume quickly. **NIST recommends that organizations follow these steps to accelerate their recovery:**

- **Develop and implement an incident recovery plan** with defined roles and strategies for decision making, then regularly exercise that plan.
- **Carefully plan, implement, and regularly test a data backup and restoration strategy**. It's important not only to have secure backups of all your important data, but also to make sure that backups are kept isolated so ransomware can't readily spread to them.
- **Maintain an up-to-date list of internal and external contacts** for ransomware attacks, including law enforcement, and understand the role of each contact in recovery efforts.

NIST's NCCoE has collaborated with industry on ransomware recovery guidance. For example, *Data Integrity: Recovering from Ransomware and Other Destructive Events (SP 1800-11*) describes how to recover operating systems, databases, user files, applications, and software systems configurations. The guide covers a variety of practices and technologies that can help organizations recover from incidents and investigate how they occurred.

NIST's *Guide for Cybersecurity Event Recovery (SP 800-184)* also provides guidance to help organizations plan and prepare recovery from ransomware and other cyber events. It offers technology-neutral ways for organizations to improve cyber event recovery plans, processes, and procedures, with the goal of resuming normal operations more quickly. Section 7 of the guide walks through a scenario for recovering from a ransomware attack.

Additionally, the Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide provides an adaptable ransomware response checklist with detailed steps to consider during detection and analysis, containment and eradication, and recovery and post-incident activity.

For more information about what you can do for ransomware attack protection and recovery, see https://csrc.nist.gov/ransomware and https://www.cisa.gov/ransomware.