Food Defense – Cyber Security Ransomware

What would you do if your computer suddenly displayed a countdown clock and a message conveying that your files are encrypted and will be permanently lost to you unless you pay a ransom by a specified date and time? As a member of the Food and Agriculture Critical Infrastructure Sector, it is vital that you are prepared for ransomware attacks. This guidance provides basic practices for safeguarding and recovering from ransomware attacks. You can also consult an expert if one is available to you.

What is Ransomware?

Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access.

Here's an example of how a ransomware attack can occur:

1. A user clicks on a malicious link that downloads a file from an external website.
2. The user executes the file, not knowing that the file is ransomware.
3. The ransomware takes advantage of vulnerabilities in the user's computer and other computers to propagate throughout the organization.
4. The ransomware simultaneously encrypts files on all the computers, then displays messages on the screens demanding payment in exchange for decrypting the files.

Ransomware disrupts or halts an organization's operations and poses a dilemma for management: does the organization pay the ransom and hope that the attackers restore access, or does the organization not pay the ransom and restore operations themselves?

Organizations can take steps to prepare for ransomware attacks. This includes protecting data and devices from ransomware and being ready to respond to any ransomware attacks that succeed.

Preventing Ransomware Attacks

The computers and information on which we rely are under constant threat from disruptive and potentially destructive ransomware. The Department of Commerce, National Institute of Standards and Technology (NIST), recommends that organizations take these basic steps to help thwart ransomware:

- Always use antivirus software 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 with recommended security and software updates.
- Use security products or services that block access to known ransomware sites.
- 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.
- 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.

Responding to a Ransomware Attack

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 review and refine 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.

Victims of ransomware should **report it immediately** to:

- CISA at www.us-cert.gov/report
- a local FBI Field Office - https://www.fbi.gov/contact-us/field-offices
- a Secret Service Field Office - http://www.secretservice.gov/contact/field-offices/

Helpful Links

- The Cybersecurity & Infrastructure Security Agency (CISA) Ransomware Guide: https://www.cisa.gov/publication/ransomware-guide
- CISA Ransomware Readiness Assessment: https://github.com/cisagov/cset/releases/tag/v10.3.0.0
- CISA Cyber Hygiene Services – At no financial cost, CISA offers several scanning and testing services to help organizations assess, identify, and reduce their exposure to threats, including ransomware: https://www.cisa.gov/cyber-hygiene-services

- NIST Small Business Cybersecurity Corner: https://csrc.nist.gov/projects/small-business-cybersecurity-corner