International Center for Enterprise Preparedness (InterCEP)

Latest on Ransomware and Other Escalating Cyber Threats

Web Forum

On September 12, 2017, **Jason Fricke**, Senior Cybersecurity Engineer at Carnegie Mellon SEI CERT, and **Jay Braun**, Manager, Incident Control and Response, United States Postal Service (USPS), discussed the latest on Ransomware and Other Escalating Cyber Threats, with a special focus on preparedness and response to ransomware attacks to the USPS.

Introduction

Ransomware is a variety of malware that restricts access to a computer system's data until a ransom is paid. This typically happens as a random infection via phishing email or drive-by, in which case the ransom is usually a few hundred dollars. An example of this kind of scenario is the CryptoLocker ransomware attack.

The most dangerous ransomware attacks involve targeted attacks to a company or institution. These can be delivered via email, or as part of more targeted and complex, spear phishing. These kinds of targeted attack can involve thousands or millions of dollars. Examples include attacks on hospitals and financial institutions.

There are other cases where the attack can look like ransomware but they turn out to be destructive malware. There are some examples that have used the Eternal Blue exploit. Wiper malware can overwrite files and these attacks may sometimes be a distraction from other malicious activity.

Cyber preparedness at the United States Postal Service (USPS)

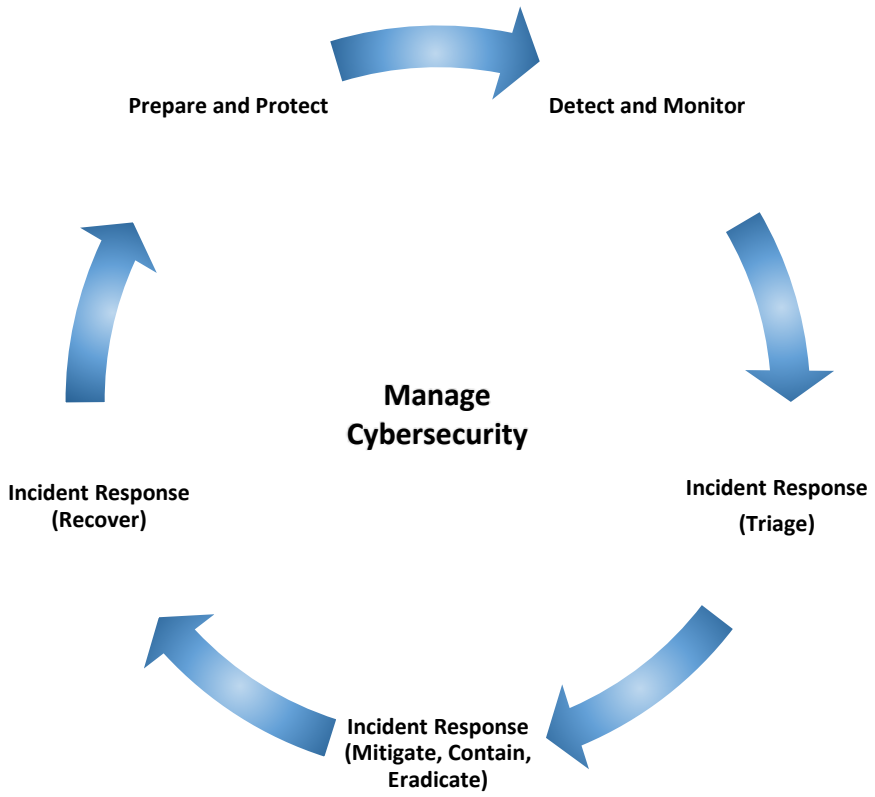
In an organization such as the USPS, a lot of the cyber risk comes from individuals checking their personal e-mail accounts. In a given year there are between one and twenty laptop infections. In 2016, there were 12 confirmed infections. So far, in 2017, no infections have been recorded, although two people clicked on a WannaCry link. In both instances controls prevented an infection.

Preventing an infection is a significant challenge as there are 21,000 laptops in use. That's where all infections have come from so far, and they typically involve drive-by, phishing emails, and checking personal email accounts. The infections take place when laptops are taken outside the organization and they are used to surf the Internet without using USPS VPN.

To reduce the risk of ransomware, the USPS has implemented a training program for employees. In addition, employees that are repeat offenders are tracked and made to take the training again.

The ransomware response framework used by USPS is a decision-support tool, developed by the Software Engineering Institute, that can be tailored to an organization's needs. It is based on five incident response process steps derived from NIST 800-61. Figure 1 shows a schematic of the framework.

Figure 1. Incident Response Life Cycle



Key aspects of the framework:

- Prepare and Protect: Preparation and protection of an organization's network and network dependent functions for handling computer security incidents
- Detect and Monitor: Activities to detect and monitor anomalous activity of an organization's network
- Response: Triage: Process by which an event is categorized as an incident and prioritized for handling
- Respond: Mitigate: Reduction or elimination of an incident's effects

- Respond: Contain: Process by which an incident's damaging attributes are prevented from spreading to other vulnerable parties or infrastructure
- Respond: Eradicate: Removal of the artifact or vulnerability responsible for the incident
- Respond: Recover: Process of returning systems, networks, or other infrastructure to a normal operating state

The framework includes key questions that an organization must be prepared to answer if their goal is to build a comprehensive incident mitigation and response plan.

Recommendations

Recommendations to organizations addressing the risk of ransomware include:

- Encourage employees to report infections not hide them.
- Utilize threat intelligence to understand risks, help allocate resources, and be predictive in order to prevent something from happening.
- Conduct regular tests and drills – organizations can have a great plan but unless they are tested there is always the possibility that the plan may not work. Plans need to be tested and drilled.
- Define RTOs and RPOs: amount of acceptable time loss without operations due to network failure and amount of acceptable data loss.
- If an organization is affected by ransomware, a part of the strategy should be to determine data recoverability and to develop a course of action. Just because an organization's data is encrypted doesn't mean it's lost. Sometimes poor code allows for data recovery.
- Employees in areas related to operations, response, and the technical side of IT should work together on addressing cyber risks as this is an enterprise level effort.
- Recovery is part of the process. After a ransomware event, it is important to have an After Action Review and discuss the issues involved.

Organizations that adopt a policy of no payment will do okay if they have a good policy of backups. Maintaining back-ups and exercising ransomware/cybersecurity plans are critical. If an organization has good back-ups it may only lose a day or so of data, and that is usually recoverable for an organization.

A response plan should also establish an interface with contacts to law enforcement and other agencies in the event of a cyber-attack.

Additional Resources

- CERT Division of the Software Engineering Institute (SEI), Carnegie Mellon University: http://www.cert.org/about/
- Volynkin, Alexander; Morales, Jose Andre; & Horneman, Angela. Ransomware: What It Is and How to Combat It Technical Report. Software Engineering Institute, Carnegie Mellon University (CMU/SEI-2017-SR-017).

- Fricke, Jason; McIntire, David; & Ruefle, Robin. Ransomware Response Framework. Software Engineering Institute, Carnegie Mellon University (CMU/SEI-2017-SR-013).
- CERT Resilience Management Model (CERT-RMM): http://www.cert.org/resilience/products-services/cert-rmm