Caltech

Cybersecurity Month - Week 3

RANSOMWARE

What is Ransomware?

Ransomware is a type of malicious software that prevents you from accessing your computer files, systems, or networks and demands you to pay a ransom for their return. By fostering a culture of ransomware awareness, research and higher education institutions can better protect their data, comply with regulations, and maintain their reputation and financial stability.

Ransomware Impact

- Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.
- **Infection Methods:** You can unknowingly download ransomware by opening an email attachment, clicking on an ad, following a link, or visiting a website embedded with malware.
- **Effects:** Once the code is loaded on a computer, it can lock access to the computer or encrypt files and folders on local drives, attached drives, and even networked computers.
- **Detection:** Most of the time, you do not know your computer has been infected until you can no longer access your data or see messages demanding ransom payments.

Prevention Tips

- **Keep Systems Updated:** Ensure Operating Systems, software, an applications are current and up to date with patches and security updates.
- **Use Anti-Virus and Anti-Malware Solutions:** Set these solutions to automatically update and run regular scans.
- **Perform Regular Backups:** Back up data regularly and double-check that those backups are completed. Test your backups often.

Prevention Tips (continued)

- **Secure Your Backups:** Ensure backups are not connected to the computer and networks they are backing up.
- **Create a Continuity Plan:** a continuity plan helps organizations prepare for, respond to, and recover from potential disruptions or disasters. It should include a business impact analysis, recovery strategies, documentation & procedures, and testing & training.
- **Create an Incident Response Plan (IRP):** an IRP is a structured approach for handling and managing security incidents. Key components include: identifying potential security incidents, measures to contain incidents and prevent further damage, steps to eradicate the cause of the incident, restoring and validating system functionality and conducting a post-incident review.

Next Week in the Series: Research Best Practices for Protecting Sensitive, Proprietary, and Classified Information on Campus