Mitigating Risks of Ransomware

University of North Texas
Center for Public Management

Patrick Shinkle
University of North Texas
Center for Public Management
https://cpm.hps.unt.edu/

Session Objectives

- Discuss the nature of Ransomware attacks
- Discuss the best practices for mitigating an attack
  - Administration
  - Employees
  - IT Technology Staff
- Provide resources for additional information

Ransomware

- In a ransomware attack, victims—upon seeing an e-mail addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the e-mail might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.
- Once the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise

Anatomy of an Attack

- The Bait
- The Click
- The Installation
- The Infection
- The Ransom Notification
- The Panic
- The Payment or Restoration
- The Hardening of the Systems

Best Practices

- Administration
- Employees
- Information Technology Staff
- Resources

Administration

- Training & Education
  - Employees without the proper education can defeat the best of technical controls by accident.
  - Establish security awareness campaigns and training that stress the importance of avoiding security vulnerabilities (questionable links and attachments in email).
  - The training program should be tailored for the audience. Developers/IT Staff/Administrators should have different training program and focus on topics relevant to their role compared to the training program for general employees and the management team.
  - User training is the best defense against ransomware.

Administration

- Incident Response Planning (Strategic Level)
  - Organizations need to write an incident response plan and tactical steps to specifically address ransomware including what remediation is necessary to mitigate the incident.
- Multilayer Defense
  - Overall security posture, understanding and defense in depth "The Onion Approach"
  - Secure Connections
  - Protection of Wi-Fi
  - Delegated administration
  - Training development
  - Enforcement of policies and procedures

Administration

- Local Policy Development Should Include:
  - Acceptable Use
  - Authentication
  - Backup
  - Confidential Data
  - Data Classification
  - Encryption
  - Email
  - Guest Access
  - Incident Mgmt./Response
  - Mobile Device
  - Network Access
- Network Security
- Outsourcing
- Password
- Physical Security
- Remote Access
- Data Retention
- Third Party Connection
- VPN Remote/Log-In
- Wireless Access
- IT Specific Account policies
- (Password complexity, account lockout thresholds, whitelisted IP ranges, blocked websites, checking for website publisher certificates, etc.)

Administration

- Strategy Development
  - Compartmentalizing authentication systems and domains (segmentation, firewalls, and network rules).
  - Keeping up-to-date storage snapshots outside the primary storage (dual backup)
  - Enforcing hard limits (rules) on who can access data and when access is permitted.

Administration

- Cyber Insurance
  - Losses following a ransomware attack fall into several categories, including:
    - Business interruption.
    - Costs associated with removing infections from machines.
    - Recovering data that the ransomware makes inaccessible.
    - Possible penalties, fines and fees.

Administration

- Risk Assessment Implications
  - Strategic
    - Prevention from accomplishing objectives.
  - Regulatory
    - Non-compliance with laws and regulation resulting in penalties and fines.
  - Operational
    - Prevention of efficient and effective operations.
  - Financial
    - Final solution results in a negative financial impact.
  - Reputational
    - Negative publicity, public trust and citizen engagement

Administration

- To Pay or Not Pay the Ransom
  - Paying the ransom encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that you will be able to regain access to your files.
  - Spend the money on securing the systems moving forward.
  - FBI Cyber Division Assistant Director:
    - "The FBI does not advocate paying a ransom to an adversary. Paying a ransom does not guarantee that an organization will regain access to their data. In fact, some individuals or organizations were never provided with decryption keys after paying a ransom. Paying emboldens the adversary to target other organizations for profit and offers a lucrative environment for other criminals to become involved."

Employees

- Best Practices
  - Appropriate Use
    - Unauthorized use of an entity owned computer resource is prohibited.
    - Use of an entity owned computer resource is subject to review and disclosure in accordance with the Texas Public Information Act and other laws.
    - You have no reasonable expectation of privacy in regard to any communication or information stored on an entity owned computer.
    - Use of an entity owned computer resource constitutes your consent to security monitoring and testing, as well as administrative review.

Employees

- Best Practices
  - Email, Phishing, & Social Engineering
    - Be careful when responding to or clicking a link in an email that asks you to verify an account or reset a password. If the email appears to be from a reputable source, but you weren't expecting it, or it looks suspicious, contact the reputable source by some other means and verify that they sent the email.
    - If you receive an email with an attachment you weren't expecting, don't open it. These attachments could be infected with malicious code, such as a virus or a worm. Even just opening a document or PDF can be enough to infect your computer or device.
    - Remember - no one should EVER ask you to tell them your password. If you receive such a request, delete the message immediately.
    - Verify unexpected attachments/emails with sender before opening.
    - Never submit financial/personal information online.
    - Employ complex individual passwords for each system.
    - Hovering the mouse pointer over a link displays its hyper-link validity.
    - Destination links to domains that end in ".ru", ".cn", (Russia and China, respectively) and so forth should be suspect.
    - Report any suspicious links, emails, requests, and computer activity to the IT department.

Employees

- Best Practices
  - System Patching and Updating
    - Keep all personal devices and their software current and up to date.
      - If possible, set the software to update automatically. This will ensure that any security vulnerabilities that are found in the software will be patched, making the device more secure.
      - If a device indicates that an update or restart is needed, schedule a time to do so to ensure that the device will always have the latest security applied.
  - Malware Protection
    - A major line of defense for protecting a computer or other devices is utilizing antivirus software, as well as keeping it up to date.

Employees

- Best Practices
  - Backing Up Your Important Information & Data
    - Hardware and software failures occasionally happen, but the impact of a failure can be minimized by maintaining regular backups of important files.
      - While working on documents or other files, save often.
      - Save backups in a secure location.
      - If possible, save to a cloud-based location. These drives are typically backed up to multiple locations, making files recoverable and secure.
  - Using Public WI-FI
    - When using an unfamiliar Wi-Fi network, such as the Wi-Fi at a coffee shop or hotel, it is always best to add an extra layer of protection to prevent others from seeing your online activities. Use a Virtual Private Network, or a VPN.

Employees

- Best Practices
  - Copyright, Software Licenses, & File Sharing
    - Sharing or distributing copyrighted files is illegal. Examples of copyright protected files include music, movies, and other materials.
    - Sharing files that are not protected by copyright is acceptable. Copyrighted materials may be used under the terms of fair use as noted in US copyright laws.
    - Follow the requirements and limitations of software licenses.
    - Read the license agreement!
    - Users caught violating copyright laws or software license agreements may face disciplinary action.

Employees

- Best Practices
  - Identity Theft Protection
    - Identity theft is a major concern in today's digital world. But, by following a few steps, you can greatly reduce your chances of becoming a victim of identity theft:
      - Avoid sending personal information via email, as email can often be relatively easily intercepted by unauthorized individuals.
      - When entering personal information online, make sure your connection is secure (encrypted). Always look for "https://" at the beginning of the web address, and, often, a locked padlock icon to the left of the web address.
      - Watch for unauthorized purchases charged to your credit and debit accounts. Contact the account provider if you notice unauthorized activity.

Employees

- Best Practices
  - If You've Been Compromised
    - If you feel that your personal computer has been compromised or infected, your computer should be taken to a trusted IT Professional.
    - Then, using a different computer that you know is safe, change any passwords that might have been entered into the compromised computer.
    - Keep in mind that prevention is your best option, and repair may result in complete loss of data!
  - Remember:
    - NEVER share your password with anyone.
    - ALWAYS update the software on your computer.
    - ALWAYS run reputable, up-to-date antivirus.
    - ALWAYS back up your most important files.
    - ALWAYS protect your connection when using free, public Wi-Fi.

Information Technology Staff

- An antivirus with a good reputation and support is installed and up to date across all endpoints. (On all desktops/laptops/servers).
  - Additional options are reviewed and enabled such as heuristic scanning, tamper protection, adaptive scanning, behavioral-based threat prevention, etc.
- Backup the data
  - Remove the external storage device once a backup has been taken so that if ransomware does infect the computer, it won't be able to touch the backup.
  - Backup data to an external device using a dedicated backup account.
  - Ransomware encrypts data on all attached and mapped drives, including mapped cloud storage and USB flash drives, these must be backed up as well.
  - Backup restorations must be validated for integrity and recovery testing.
  - Ensure the ransomware is not restored with the backup recovery.
  - Utilization of Cloud Services
    - Many cloud services retain previous versions of files, allowing the entity to "roll back" the previous unencrypted files.

Information Technology Staff

- Restrict Administrative User Rights & Permissions (Least Privilege)
  - Users should only be issued the rights/permissions required for their job role.
  - All users, including IT admin personnel, should log in using a non-privileged account, and escalate privilege as needed using a secondary account.
  - Assign rights to users using security groups in Active Directory (AD). Use of local admin accounts should be limited.
  - Change default built-in admin account passwords (if machines are on a domain, disable local admin accounts).
  - Most of the common tasks any user uses (browsing the internet, checking e-mail, or editing a document) does not require the ability to stop and start services or to edit registry keys (end users should never edit the registry).
  - Administrative accounts have more privileges and introduce heightened risk.
    - Privilege Bracketing - Allowing the administrator accounts only when absolutely needed and for the shortest time necessary and is lifted immediately after it is used.
      - Privilege bracketing can be applied to individual users as well as to systems or processes.

Information Technology Staff

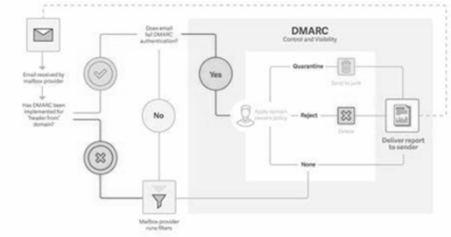
- IP Address / Geo-Blocking for Suspicious Domains and Regions
  - Consider configuring your firewalls to block all incoming and outgoing traffic to these domains and geographical areas.
- Block Outgoing I2P traffic
  - Consider blocking all outgoing I2P (Invisible Internet Project) and other unnecessary peer-to-peer network traffic at the firewalls on the perimeter of your network. This will prevent infected computers communicating with their controllers and receiving further instructions.

Information Technology Staff

- Example tools to enhance email security with DMARC, SPF and DKIM
  - DMARC "Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol. DMARC is only designed to protect against direct domain spoofing.
  - SPF "Sender Policy Framework" is an email authentication protocol that allows the owner of a domain to specify which mail servers they use to send mail from that domain.
  - DKIM "Domain Keys Identified Mail" is an email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain.

DMARC (Domain-based Message Authentication, Reporting & Conformance)

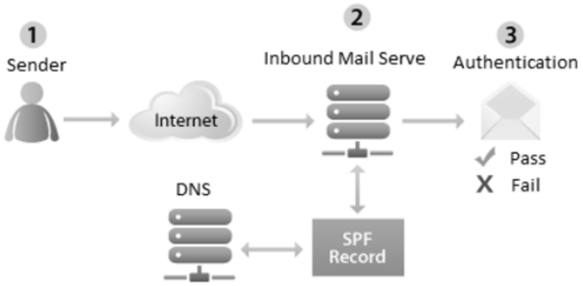
- It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling of authentication failures, and reporting from receivers to senders, to improve and monitor protection of the domain from fraudulent email.



https://dmarc.org/

SPF (Sender Policy Framework)

- Defines a way to validate an email message was sent from an authorized mail server in order to detect forgery and to prevent spam. It was designed to supplement SMTP, the basic protocol used to send email, because SMTP does not itself include any authentication mechanisms.

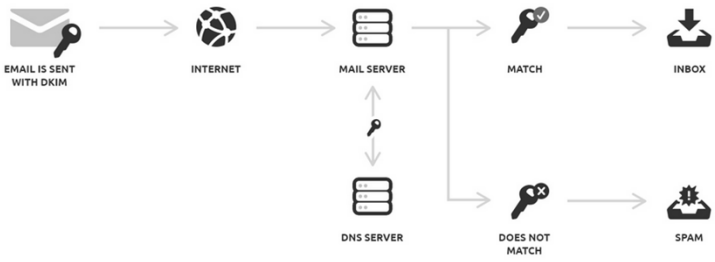


https://www.sparkpost.com/resources/email-explained/spf-sender-policy-framework/

Center for Public Management

DKIM (Domain Keys Identified Mail)

- An email authentication technique that allows the receiver to check that an email was indeed sent and authorized by the owner of that domain. This is done by giving the email a digital signature. This DKIM signature is a header that is added to the message and is secured with encryption.



https://www.dmarcanalyzer.com/dkim/

Center for Public Management

Information Technology Staff

- Block Executable Files From the %APPData% and %TEMP% Paths
  - These folders are often used by malicious software to download and execute the files associated with ransomware and other malicious software.
  - Additional folders to consider restrictions:
    - LocalAppData
    - ProgramData
    - Desktop
- Block Malicious TOR IP addresses (block TOR access for all users unless necessary for job role).
  - TOR "The Onion Router" gateways are the primary means for ransomware threats to communicate with their servers. Blocking those addresses may impede the critical malicious processes from communicating.

Information Technology Staff

- Create Restrictions via GPO (Group Policy Object) on Network
  - GPO has the ability to provide granular control over the execution of files on an endpoint, so adding rules that block activity such as files executing from the 'Appdata' directory or even disabling the ability for executables to run from attachments.
- Create Restrictions via SRP (Software Restriction Policies) on Network
  - (SRP) is a Group Policy-based feature that identifies software programs running on computers in a domain, and controls the ability of those programs to run.
  - Consider deploying Microsoft AppLocker to centrally manage which applications can be run.
    - https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-overview

Information Technology Staff

- Patch Commonly Exploited Third Party Software such as Java, Flash, Adobe etc.
  - Ensure all third party software is kept up to date with latest versions.
- Showing Hidden Extensions in File Manager
  - “PartyPig.jpg” might actually be “PartyPig.jpg.exe”.
- Consider Filtering Files from Email Servers
  - Executable (exe)
  - Password Protected
  - Macro-enabled files (DOCM)
  - Others with the following extensions (SCR PIF CPL DLL SYS FON EFI OCX)

Center for Public Management

Information Technology Staff

- Consider Disabling (RDP) Remote Desktop Protocol Connections
  - Remote Desktop Protocol “RDP” - A proprietary protocol providing a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software.
  - Windows RDP allows you or others to connect to your computer remotely over a network connection, allowing access to everything on your computer.
- Evaluate “Whitelisting” of Software, IP addresses and Domains
  - Allows only specified programs to be run on the company's computers and therefore blocks malware.
  - Configure white listing for plugins and add-ins for your browser.
  - Instead of allowing Flash on every site, block it on every site and whitelist only the sites you trust.

Center for Public Management

Information Technology Staff

- Install ad-blocking Add-ins on Web Browsers.
  - Most web browsers allow the installation of add-in to enhance security and script blocking.
- Enable Unified Threat Management "UTM" on edge devices such as a firewalls
  - UTM virtual firewalls provides enhanced protection and enables users to control and manage network security.
  - UTMs can offer intrusion detection and prevention, web-site filtering where you block access to known or suspected malicious content, and another layer of antivirus.
- Maintain a Patch Management System
  - Have a dedicated WSUS (Window Server Update Services) server that manages security and critical updates.
  - Ensuring all desktop clients are fully patched and updates are pushed.

Information Technology Staff

- Perform Data Leakage Prevention (DLP) and anomaly detection.
  - Make sure no users are leaking data out of the network. Pay close attention to suspicious outbound connections.
- Ensure Windows "Shadow Copy" in enabled
  - It automatically keeps previous versions of documents available.
  - Allows quick restoration of the previous version of any impacted file.
  - Most well written ransomware applications will attempt to disable Shadow Copy.
  - If you are logged in as an admin, ransomware will successfully disable this and alter any previous versions you may have saved.

Information Technology Staff

- Disable ActiveX in Office Files (Disable Macros by default)
  - Disable ActiveX content in the Microsoft Office Suite of applications. Malware often uses macros to take advantage of ActiveX and download files to the computers. Highly recommended for any organization running devices with Microsoft operating system earlier than Windows version 10.
- Enable User Access Control (UAC) in Windows
  - "UAC" prevents unauthorized changes to a computer. Change requests can be initiated by applications, viruses or other users. When UAC is enabled, these changes are made only with approval from the person using the computer or by an administrator.

Information Technology Staff

- Manage Mapped Drives (Map Drives via GPO on Microsoft systems)
  - Mapped drive is just a shortcut to a drive that's physically located on a different computer.
  - Mapped drives can be used to reach resources on different computers on a local network, as well as files on a website or FTP server.
  - Keep critical data in segregated or air-gapped mapped drives or networks that utilize additional firewall protection and controlled access from authorized devices / users.
- Use Penetration Testing to Validate Vulnerability and Patch Management Activity.
  - Penetration test, also known as a "pen test", is a simulated cyber-attack against computer systems to check for exploits and vulnerabilities.
  - Pen testing can involve the attempted breaching of any number of application systems, networks etc.
  - Insights provided by the penetration test can be used to fine-tune security policies and patch detected vulnerabilities.

Information Technology Staff

- Review Active Directory Maintenance
  - With so many moving parts related to AD, it is important to monitor, report, fix, and diagnose issues related to the different supporting technologies.
    - DNS zones (Domain Naming System)
    - AD Replication
    - AD Backups
    - DHCP (Dynamic Host Configuration Protocols)
    - Event Logs, Privileged accounts, inactive users, etc.
  - Identifying bottlenecks and resolving them before issues improves productivity, efficient usage of resources, consistency of data and services, and reduces the number of issues.
  - Setup an AD cleanup schedule (remove/disabled unused accounts/objects).

Information Technology Staff

- Incident Response Planning (Tactical Level)
  - Organizations need to write an incident response plan and tactical steps to specifically address ransomware including what remediation is necessary to mitigate the incident.
- Network Segmentation
  - Allows the ability to isolate infected sections of the network and prevent the infection spreading further.
  - Setup private/isolated networks for nonstandard machines/users.
  - Benefits:
    - Improved Security. Network traffic can be isolated and / or filtered to limit and / or prevent access between network segments.
    - Efficient Access Control. Allow users to only access specific network resources.
    - Improved Monitoring. Provides event logging, monitoring of connections and suspicious activity.
    - Improved Performance. With fewer subnet hosts, local traffic is minimized. Broadcast traffic can be isolated to the local subnet.
    - Incident Containment. When a network issue occurs, its effect is limited to the local subnet.

Information Technology Staff

- Implement Intrusion Detection System / Intrusion Prevention System (IDS/IPS)
  - Intrusion Detection System "IDS" – A hardware device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports and notifications to a management station.
  - Intrusion Prevention System "IPS" - An Intrusion Prevention System (IPS) is a network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
  - IDS / IPS can be:
    - Signature-Based: This is where patterns, or signatures, of known attacks are downloaded by the system. Network traffic is compared against these patterns to identify potential attacks.
    - Anomaly-Based: Intrusion Software learns the "normal" behavior of the network and the types of traffic and network packets it handles. Traffic that is detected that is out of the normal state will alert the monitoring station.
    - Rule-Based: Employs a set of rules or protocols defined as acceptable network behavior. If the network traffic is outside the norm, it is blocked.

Information Technology Staff

- Monitoring
  - Use network scanning application to sniff suspicious traffic (for example WireShark).
    - https://www.wireshark.org/
  - Ensure that the IT team has full visibility of the network traffic and its behavior under normal business conditions. This knowledge can then be used as a baseline to identify any unusual activity which should then be investigated to determine whether it is the result of a potential breach or an issue with the network.
- Evaluate Encryption for Hardware and Files
  - Encrypt hard-drives
  - Consider file encryption of sensitive information.

Resource Links

- **Federal Bureau of Investigations** - https://www.fbi.gov/
  - Ransomware Prevention and Response for CEOs
    - https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-ceos.pdf/view
  - Ransomware Prevention and Response for CISOs
    - https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view
  - FBI Recommendations for the Prevention of Ransomware (News Section)
    - https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise
- **Texas Department of Information Resources (DIR)** - https://dir.texas.gov/
  - Proactive Measures and Response Video
    - https://www.youtube.com/watch?v=MdXogO-4m4s&feature=youtu.be
  - IT Policies and Guidance
    - https://www.dir.texas.gov/View-Resources/Pages/Content.aspx?id=32

Resource Links

- **National Cybersecurity Center of Excellence** - https://www.nccoe.nist.gov/
  - Data Integrity: Recovering from Ransomware and Other Destructive Events
    - https://www.nccoe.nist.gov/projects/building-blocks/data-integrity/recover
      - NIST PDF Version:
        - https://www.nccoe.nist.gov/sites/default/files/library/sp1800/di-nist-sp1800-11-draft.pdf
      - NIST Web Version:
        - https://www.nccoe.nist.gov/publication/1800-11/

Questions?

Thank You!