Ransomware Attacks – what you need to know

Each day in the news we are hearing more and more about ransomware attacks. These attacks lock you out files and systems by adding encryption that blocks access. The malware carrying the encryption can be introduced to files and spread across networked computers in a number of ways including email- based attacks and hacking through remote access to computers.

Unfortunately, the attacks are not limited to big business or government agencies and attackers do not have a social conscience. Libraries and library consortia have been victims of ransomware attacks. What can a library do to protect themselves against these potentially disastrous attacks? The steps below will help you protect and respond the threat of Ransomware.

Security is an ongoing prevention and active awareness plan. Mid-Hudson Library System has a security plan in place and it is regularly reviewed and tweaked. Our plan includes infrastructure, scheduled upgrades, and awareness training for every single staff person. We test our plan regularly and are rigorous about managing risk. While there are many solutions that you might adopt, we thought it would be useful to share the methods we have adopted, not as advice, but simply to provide an example.

Prevention:

- It is strongly suggested by cybersecurity professionals that you use a cloud-based file hosting service with automatic backup. This provides you with clean copies of your files that can later be restored, once you have removed the "infection" source and files. Attackers are banking on the fact that you cannot replace your files, and must pay their ransom to restore your access. Backing up off network to the cloud acts as an insurance policy against this threat.
  What is MHLS doing?
  - *MHLS uses Microsoft Office 365 which includes MS OneDrive and MS SharePoint cloud storage options.*

- Separate and secure backups are key. Hackers look to detect your backups and will spread the encryption to those sources as well if they are not stored remotely and behind password protection.
  What is MHLS doing?
  - *MHLS uses local and online/cloud storage option to backup files. Local backups are rotated with only 1 is on the network at any time.*

- Retain several rolling backups to avoid overwriting your last good copy.
  What is MHLS doing?

- *MHLS retain 2 weeks of local backups. MS Onedrive retains 30 days.*

- Protect your computers and devices with security software and keep it up to date. Windows security does offer some protection and even has a ransomware element that can be engaged.
  What is MHLS doing?
  - *MHLS use Windows Defender*

- Awareness is key to reducing the threat from within. Provide staff with information about email scams and phishing. Ransomware is changing, so awareness is an ongoing process.
  What is MHLS doing?
  - *MHLS provides training and documentation on security.*
  - *MHLS requires password changes at 180 days*
  - *MHLS uses a product called KnowB4 to test vulnerability to email Phishing. Each staff member receives regular email tests to see if they are vulnerable. The emails use the same elements to snare hopeful victims. Staff who fail to recognize the email as a threat are required to complete training on that form of email scam.*
- The internet is another point of concern. Be wary of sites that offer downloads and applications and limit access to downloading. Public computers should be managed on separate networks from your own library network.
  What is MHLS doing?
  - *MHLS separates staff computers from unknown "public" computers. MHLS's firewall blocks incoming attacks.*

Responding to an attack:
MHLS has been the target of a ransomware attack. Included below is how we respnded.

- Do not engage with your attacker.
  What did MHLS do?
  - *Ignored any ransom demand and went directly to work on removal and replacement processes*

- Isolate the infection as quickly as possible by removing the device(s) from your network. It may be a hardwired connection or a Wi-Fi connection, but getting the device quarantined is the first response. If you are unsure of how to disconnect, power off the device.
  What did MHLS do?
- *Unplugged the network cable and powered down the PC.*

- Ransomware spreads fast. You should then move to computers on your network and test for corrupted files. Computers who share drives, networked files and software are at the highest risk. You should check all computers on your network or with access to files.
  What did MHLS do?
    - *MHLS disable the network connection on all computes and scanned all computers on the network for any signs of Ransomware or Malware. Only reconnecting to the network after completing all scans.*

- Finding the original cause or "patient zero" may be difficult. Sorting files by updates and Enabling "Show file extensions" will help you to identify encrypted files. You may need to work with staff to track down when and where noticed changes took place.
  What did MHLS do?
    - *MHLS identified the cause by working with staff to determine what happened. When were signs first noticed? What were recent changes? Was anything new installed? Are there any security/password vulnerabilities on this computer/staff member's accounts?*

- You will need to review your cloud-based files also. It may be possible that infection, even through your password protection has happened inadvertently through regular access
  What did MHLS do?
    - *MHLS reviewed cloud-based files. Infected files were deleted.*

- Cleaning up the files thoroughly is important. You can fully reformat and restore from backup.
  What did MHLS do?
    - *MHLS reformed the infected computer and deleted all infected files.*

- Once you have disinfected, it is time to look at backed up files, by downloading a copy, ensuring the originals remain intact.
  What did MHLS do?
- *MHLS scanned the backup for any signs of Malware. Actively observing the network and restore files for any signs of a continued attack.*

What about Sierra?

- Sierra is hosted by Innovative in Amazon's cloud network. Access to the Sierra Desktop application is protected in by allowing access from approved IP addresses. Logins and passwords meet strong password security measures and must be updated every 180 days. Our security is at its best when we are running the most

current OS versions and the Sierra software itself is current. Innovative's ISO 27001 certification requires regular testing and for vulnerabilities by a 3rd party with a passing outcome. Any incident or suspected attack should be reported in the ticketing system as soon as possible. MHLS will in turn alert Innovative. In the event that Sierra has been breached a new instance of Sierra will be created from back ups dating before the incident.