Security Update

NEOnet

Northeast Ohio Network for Educational Technology

NEOnet

How to Identifying Risk

- Identify and classify technology assets
- Develop a threat model based on that data
- Start with the highest risk applications and work down the list
- Time consuming and expensive
  - Requires people time and money

NEOnet

What are the biggest threats?

- Phishing – sending official looking, and sounding, emails to end users to trick them into providing sensitive information.
- Malware – malicious software used to gain control of an end user's computer in order to gather sensitive information or to conduct similar attacks on other entities.
- Ransomware – malware that uses cryptography to take a victim's data hostage in return for monetary gain.
- Dictionary attacks – an intruder's automated attempt at guessing a simple password so they can gain access to sensitive information.

What can be done now?

- End user awareness – training for end users on what to look for in these phishing and malware attacks so they will not fall victim as easily. This is also an opportunity to train them on what to do if they are questioning the validity of a request.
- A consistent message you want to send to your end users – **You will NEVER be asked for your credentials via email or over the phone by anyone managing your technical assets.**

What can be done now?

- Establish password policies – simple passwords can lead to data breaches that cost real dollars. The more complex a password is the harder is to guess. The harder it is to guess, the harder it is for end users to remember. Use phrases instead of hard to remember characters. Long passwords containing multiple easy to remember words is hard to crack.
- Password management tools are also a good idea to help end users remember and keep complex passwords safe.

NEOnet

What can be done now?

- Backups – maintaining good backups is a very important aspect of reducing the liability of ransomware. If you can restore to a point in time with limited loss, then your liability is reduced and the ransomware is less effective.

NEOnet

Malware Protection Statistics

Consortium Level Requests – 30 Days

- 375 Million requests total
- Malware
  - 489k blocked malware connections
- Botnets
  - 244k blocked botnet connections
- Phishing
  - 2700 blocked phishing connections

NEOnet

Consortium Level Requests – 24 Hours

- 6 million requests total
- Malware
  - 10k blocked malware connections
- Botnets
  - 2700 blocked botnet connections
- Phishing
  - 37 blocked phishing connections

NEOnet

Disitrict Level Requests – 24 Hours

- 326k requests total
- Malware
  - 62 blocked malware connections
- Botnets
  - 0 blocked botnet connections
- Phishing
  - 0 blocked phishing connections

NEOnet

NEOnet

700 Graham Road
Cuyahoga Falls, OH 44221
www.neonet.org
P: 330.926.3900
F: 330.926.3901
E: helpdesk@neonet.org