Practical Application

The Cryptolocker incident

It was a Monday…ugh Mondays

- Around 10am users started to call in that they could not access some files on a server
- Narrowed down to a few departmental folders
- Looked at the files, they are encrypted
- We knew we were being hit with Locky

Step 1a – Cut off access, from the server

- Windows allows rights and permissions to objects such as processes and users
- Since Locky operates via a user infection, we had to kill the access to the server
- We made the server Read Only, which meant no objects could write data to it.

Step 1b – Cut off access, from the user

- We knew it was a user that was infected
- We looked at who had permissions on those folders and looked at access logs
- Found the user
- Called user and told her to unplug her Ethernet cable (if there is an incident – never shutdown the computer. There may be vital information running in memory that will be deleted if you pull the power)

Step 2 – Assess the damage

- Due to confidentiality, the damage was only done to a small part of the server.
- Only 2 out of 100’s of folders were encrypted. Still 84,000 files though
- Integrity allowed us to ensure that the files from the previous several hours were the only files damaged by the malware

Step 3 - Recovery

- During a major incident – availability becomes attacked as well since you are trying to ensure confidentiality and data from becoming breached
- We pulled the backups that took place 4 hours prior and restored them
- This was availability
- I guarantee not a lot of organizations are this lucky

Putting it all together

- Confidentiality limited the damage through permissions
- Integrity assured the correct files that had been compromised
- Availability allowed us to get the systems functional again

A word for the wise

- Unless you can say we have covered CIA on every system and process, you are going to have issues at one time or another
- If one of those pillars was not in place, the incident would have been much worse
- I don’t think it could have gone any better
- However…
  - I had my key staff on hand
  - We have great logs
  - We have great backups
  - Everyone worked together