Security

2018

Quick Take

- Traditional security is only as good as your user community.
- Current approaches are based upon a flawed premise
- Technology needs to do a better job at securing systems.
- Implement multiple steps in safeguarding your environment.

Considerations

Backups, backups, backups

It is not IF it is WHEN

Weigh costs when developing a recovery strategy

Understand your vulnerabilities

Keep up to date on what is available

User community education

Up to date firewalls

Up to date anti-virus software

Cloud technology

IT Security

Reading about the failure of major systems due to encryption or ransomware is unnerving to the public domain. In a time where technology is the cure for most anything, why are our systems so vulnerable to such obvious attacks?

The technology foundation in 2018 is based upon keeping the bad programs out of our processors. We scan programs and try to match their digital footprint against a database of bad programs. This strategy of looking for "bad guys" is a flawed approach and cannot ever be won. But the reality is that this foundation is how our "open" systems are based so we continue to battle this never ending war on malware.

While we wait for technology to come up with a better plan, we must be able to guard an organization from spyware and malicious attacks. Leading edge decisions could be made such as adopting "lock down" or "white list" technology, but in reality, working in a BYOx world with innovation requiring open systems, we must work with what today's technology is giving us to maintain a safe, productive environment.

Good security begins with your user community. Continuous education of the user community on the good practices of using email needs to be maintained. To communicate but not to come off as an alarmist, the IT staff needs to send out regular updates to the user community on safe computing—especially email management.

A comprehensive backup and restore system is the best defense against a malicious attack on an organization's system. When an attack is found, it is usually too late to stop the damage. When this occurs, the best effort is to pause the system, identify the scale of the attack, and restore your system to it's last safe checkpoint. During this effort of restoring the system to a safe checkpoint, expectations must be managed to minimize disruption.

The backup system needs to have numerous versions of each data element. The number of versions is dependent on the environment, but typically 10 generations of backups should be maintained.

The backup system should be granular yet have full system recoveries in place. Restoring a file from two months ago should be available. In addition, restoring an entire server's image from the night before needs to be in place. These options plus many more are requirements for a comprehensive backup and restore system.

Money and time invested in a comprehensive backup / restore system is one of the best defenses against malicious software attacks.

Anti-virus protection software is another layer of your defense against malicious software. Although anti-virus software seldom stops an attack, it can be used to clean up after such event. But deciding whether to flash and restore or try to operate with an anti-virus removal tool, more times I would suggest flash and restore.

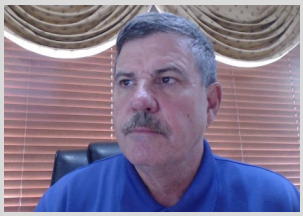
Firewalls and browsing protection software must be kept current to be most effective. Keeping the licenses current and the software updated is paramount to a good security plan. But again, if the virus is new and the website just created, the "black list" approach to stopping the virus will be minimally effective. But nevertheless, keep the firewalls maintained and the subscriptions current to ensure that you have a level of good security for your network.

A fairly quick addition to the defenses against attacks is the use of the cloud. By migrating your data stores and systems to the cloud, the availability of data files to be corrupted are minimized or removed. If an end user gets ransomware on their computer and they are using cloud storage, depending of the timing of the detection, the user may be able to flash and go within an hour or so. Furthermore, the cloud services typically have versioning in place. If the detection is not immediate, restore options are available from the cloud provider so a clean files can be restored to the flashed computer.

There are some technologies and systems available which are very resistant to malicious attacks. But due to our preferences and approach to innovation we use open systems which is vulnerable to viruses. To guard against major catastrophe, we must institute several levels of safeguards to keep the organization's systems running and the company productive.

Tom McCloy

Phone: 513.549.4551
Email: tom.mccloy@outlook.com
Mc-cloy.com



www.mc-cloy.com