Internet Safety

Jaime Martinez, CISA, CISSP
Reserve Deputy #4
jmartinez@mcsdmace.com
(313) 268-5930 cell

Definitions

- **Attack** – an assault on the system from an intelligent threat
- **Exploit** – a defined way to breach the security of an IT system thru vulnerability
- **Security** – a state of well being of info and infrastructure in which the possibility of theft , tampering and disruption of info and services is kept low or tolerable.
- **Threat** – something that might compromise security
- **Vulnerability** – a weakness in design or implementation error that can lead to an unexpected and undesirable event compromising the security of the system
- **Risk** – the likelihood of a threat agent exploiting a vulnerability and the corresponding business impact.
- **Control** – a counter measure (safeguard) put in place to prevent/reduce a potential risk.

What factors define Security and being secure?

- Security
- Functionality
- Ease of Use
- Cost

The Bad

- **Malware** – Software that has a malicious intention ex: to damage, to disable computer system
- **Virus** – a Malware that can duplicate and copy itself onto other computing devices
- **Trojan** – a type of virus that is “hidden” (Trojan like) on a program that is usually offered for free.
- **Worm** – a self-replicating computer virus that changes and moves through a computer network.

The Bad

- **Zombie** – a computer that has been compromised and is controlled by a remote unauthorized user.

- **Rootkit** – a software tool that hides its existence and enables another (hacker) to have administrative (root) access to a computing device

- **Botnet** – a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet.

Security Risks (More Bad)

virus/malware/trojan
keyloggers
botnets
data loss
emerging virus
cyber espionage
zero day exploits
fishing attacks
identity theft
cyber extortion
usb drives
zombie networks
exploits in technology
outsourcing projects
social networking
business interruption

How do we categorize Risk?

- **Quantitative**
  "*How likely*" is something bad to happen?

- **Qualitative**
  Just "*how bad*" would it be?

Top Challenges

- increase in the sophistication of cyber criminals
- data leakage
- multiplication/variation of existing security risks
- New technologies ex: mobile security (all with smart phone with internet) who testing the apps?

Risk on the rise

- New Technologies
- New exploits
- Aging Internet
- More hackers and more foreign governments hacking
- Hackers (criminals) getting more savvy

Who is the hacker/cracker?

- anyone with a computer or phone (sophisticated tool)
- an intelligent person who understands code (can look at code and reverse engineer it)
- person who sees it as a hobby, fun
  "*let's see how this works*"
- hacker also wants to see it used in a way contrary to original usage
- hacker use it for money, malicious to get financial gain
- anybody can be a hacker

What does the hacker do?

- Perform Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Clearing tracks

Security in Measures

- **defense in depth** – strategy in which several protection layers are placed throughout an information system – each layer has its own controls

- **vulnerability research** – process of discovering vulnerability and design flaws
  ex: penetration testing (hiring a white hat hacker to find your organization vulnerabilities)

Controls

- login/access control
- anti-virus/malware removal scan/software
- Firewall
- vulnerability analysis
- penetration testing
- router/switch testing
- IDS/IPS
- Encryption
- security awareness
- patch management
- reviewing logs
- VPN

Types of Controls

- **Physical controls** e.g. fences, doors, locks and fire extinguishers;
- **Procedural controls** e.g. incident response processes, management oversight, security awareness and training;
- **Technical controls** e.g. user authentication (login) and logical access controls, antivirus software, firewalls;
- **Legal and regulatory or compliance controls** e.g. privacy laws, policies and clauses.
- **Detective Controls** – assist in detecting an irregularity (a passive control, they do not prevent unwanted events from occurring).
- **Deterrent Controls** – are designed to prevent an individual from attempting to trespass, steal, destroy, or cause any other unwanted event

Trends

- Ransomware
  - Hacker encrypting a person's hard drives
  - Hacker taking photos utilizing a person's webcam
- Credit Card forgery/duplication
  - Target, POS, credit card vulnerabilities
- Fraudulent tax returns
- Non Trustworthy USB devices

What can you do to keep your home computer safe?

- Never run programs (or open webpage) that you do not know where they came from. Such as an executable (or link) in an email from an unknown sender
- Run virus scan, malware scan often
- Keep your computing device up to date with o/s updates
- Never insert a usb storage device in your computer from an unknown source

What can you do to keep your home computer safe?

- Try a non MS Windows computer
- Delete your cookies
- Delete your history
- Never store passwords within the browser
- Never provide any of your passwords to anyone
- Disable remote assistance/remote desktop

What can you do to keep your home computer safe?

- Never do any confidential computing at a public wifi location
- Always lock your computer
- Monitor the websites that your children visit. Block internet (home router setting) at appropriate times.
- Ask your children about the activity they do on the internet, What sites do they visit? What do they do?

What can you do to keep your home computer safe?

- Be sure to lock down your home router/switch
- Never write your passwords down
- Put your passwords in a safe place
- Never use simple passwords
- Change your passwords

What can you do to keep your home computer safe?

- Be careful what you do with outdated technology
  Retiring old equipment
- Make backups of important data
- Store your backups in a safe place
- Test your backups

What are Organizations doing?

- Accepting the notion they will be hacked
  - They do not appreciate the severity of the risk.
- Hacking back
- Attempting to mitigate the severity of the attack

Outlook

- Has energy grid already been compromised?
- Do we have sufficient "*Security Experts*"?
- Are we in for an "*Internet Pearl Harbor*"?
- Will things get a lot worse before things get better?
- Are we losing the Cyber War?

- THANK YOU!

Reserve Deputy #4
Jaime Martinez, CISA, CISSP
jmartinez@mcsdmace.com
(313) 268-5930 cell