CKAHU Symposium

Cyber-Security

Technical Director of Security

Scott Logan

Position: Technical Director of Security

Employment: NetGain Technologies (6+ years)

- NetGain is a Regional partner with 7 locations
- I am one of 153 associates who are trained and certified
- NetGain Technologies is SOC 2 type II certified
- NetGain is ranked in the top 60 in the WORLD with our managed services program

Security Certifications: CISSP “Certified Information Systems Security Professional”

Engineering Certifications: MCSE, MCITP, MCTS, ASE, AIS, Sophos Certified Engineer, Barracuda Certified Engineer

Today's Security Agenda

- Basic Security Weakness (TOP 10)
- New Cyber Security Threats for 2016
- How to improve security against ransomware attacks
- Latest Threats/Attacks
- What Types of Businesses should be Concerned
- What can NetGain provide

Basic Security Weakness TOP 10

#10 Don’t leave the safe open

- Server areas kept unlocked or access not restricted
- Work areas not secure from prying eyes
- Workstations not locking down access after inactivity

#9 You can’t prove it!

- Missing auditable access record or an audit log is not maintained
- Use of key locks instead of card swipes or fobs that can document access

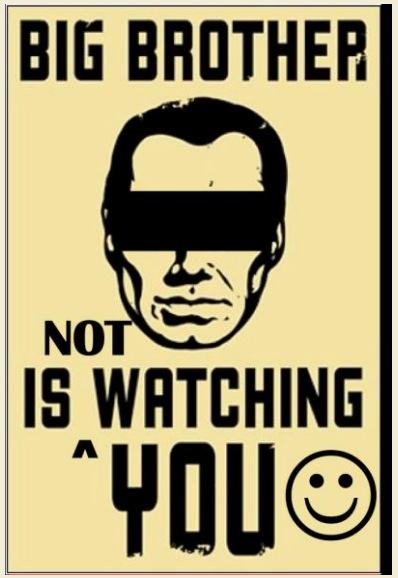
Basic Security Weakness TOP 10

#8 Do you smell smoke?

- No environmental controls (Smoke, Water, Humidity)
- The use of water to protect computers
- Absence of proper power protection (UPS, Generator)

#7 Big brother's NOT watching?

- No surveillance systems in place
- Surveillance records not kept or maintained
- DVRs have no or poor retention



Basic Security Weakness TOP 10

#6 It worked yesterday?

- Warranties absent or expired
- Equipment too old to repair (no parts available)

#5 Patches, We don't need no stinking Patches!

- Operating systems no longer supported
  - XP – Expired Apr 2014
  - Exchange 2003 – Expired Apr 2014
  - Server 2003 – Expires July 2015
  - SQL 2005 – Expires Apr 2016

Basic Security Weakness TOP 10

#4 Easy… To Forget

- Copiers and Network printer drives not erased
- Hard drives not properly destroyed
- Removable media usage

#3 Administration Aggravation

- Weak or missing SLAs
- No security training provided to employees
- Weak or missing security policies
- No sanctions imposed for violations

Basic Security Weakness TOP 10

#2 What was IT thinking?

- Weak passwords (no complexity)
- Network equipment using default passwords
- Stale Active Directory, not maintained
- Delinquent or missing “updates”
- Third Party applications like Java not updated
- Event logs and Syslogs not reviewed

Basic Security Weakness TOP 10

#1 Is that the Best you got?

- Not using business class firewalls
- Missing IDPS protection
- Missing 24x7x365 support
- Missing web protection
- Missing Email security scanning
- No Encryption in use
  - Data in motion
  - Data at rest
- Weak user endpoint protection
  - Weak anti-virus, also missing elements like HIPS, DLP, Device Control and Application control

New Security Threats

- **Internet of Things (IoT)**
  - In 2014 there was more evidence that manufacturers of Internet of Things (IoT) devices have failed to implement basic security standards, in 2016 there will be even more

- **Major flaws in widely-used software**
  - From Heartbleed to Shellshock, it became evident that there are significant pieces of insecure code used in a large number of our computer systems today

New Security Threats

- **Regulatory Landscape forces greater disclosure and liability**
  - A staggering 77% of the surveyed businesses didn't even know if they were compliant with present data protection regulations

- **Third-Party Attacks**
  - Major data breaches at retailers like Target and Home Depot occurred because attackers were able to obtain valid network credentials from trusted, third-party providers, and just walk right in.

New Security Threats

- **Ransomware**
  - Ransomware “Crypto Locker” continues to threaten many businesses with new variants making it even harder to prevent attacks. Plus more and more victims are falling prey to the attacks and paying the ransom to restore access to company sensitive information. This fuels the attackers to expand the volume of attacks and create even more deviant methods of attack “ex. zero day attacks”.

  - Ransomware attacks grew 113 percent in 2014, driven by a more than 4,000 percent increase in crypto-ransomware attacks in 2015. These numbers will continue to grow in 2016.

How to improve security against ransomware attacks

- **Backup, Backup, Backup:** This cannot be stressed enough. Backup restorations are the BEST method to recover files that become inaccessible from a Ransomware attack. It is also a very good idea to expand the retention period for data backups if possible.

- **Social Engineering Training:** Improve your employees knowledge and understanding about phishing attacks. Provide training on how to recognize attacks and enforce rules about opening unknown attachments.

How to improve security against ransomware attacks

- **Expand web filtering to create a blacklist/whitelist:** Exclusively deny access to sites that promote malware. Category filtering is a start, but an aggressive white/black list can assure that certain elements are just not allowed.

- **Access to shares:** Make sure that users, that do not require admin (modify/delete) access, don't have it. Some users may only require read access, this may prevent spread during an attack.

How to improve security against ransomware attacks

- **Restrict access to personal email from company resources:** Filters that may protect company email systems from infection are easily defeated when allowing access to Gmail, Yahoo and other personal email systems from the corporate network. A good defense it to segregate from the private network a workstation (or two), maybe in the break room that has access to personal email and social media sites.

How to improve security against ransomware attacks

- **Step up the perimeter protection:** Advanced persistent threat protection can deny recognized signature attacks at the edge, never allowing the attacks to enter the network. Best in class UTM products now include APT protection.

- **IDPS protection:** Firewalls just do not have the capability to protect against these types of attacks. Adding Intrusion detection and intrusion prevention services can provide a stronger level of defense.

How to improve security against ransomware attacks

- **Country blocking:** Some threats can occur from foreign markets, so if your business does not require access to entities outside the US, then adding country blocking is a good method to improve security.

- **Improved Endpoint protection:** Advanced AV/Spam/Malware protection plus other advanced controls like Device Control, Application Control, and Data Loss Protection.

Latest Attacks

- **Healthcare Security – Insider Blunders Still a Common Breach Culprit**
  - While 2015 will be remembered as the year of major hacker attacks in the healthcare sector, most of the health data breaches added so far this year to the official federal tally have involved insider blunders, including improper disposal of paper records and lost or stolen unencrypted laptop computers.
- **Beacon Health – Hacker Victim**
  - Phishing leads to email compromise, exposing PHI

Latest Attacks

Latest Attacks

- **Ransomware Variants – “Locky”**
  - The new piece of malware is being distributed via fake invoice emails that contain Word document attachments with malicious macros. When the user enables macros to view the content of the document, the Locky ransomware is downloaded from a remote server and executed, and it immediately begins encrypting files on the compromised system.
- **Tech Support Scams**
  - This scam involves a criminal posing as a computer support technician who makes an unsolicited call to trick a potential victim into believing his/her computer is infected with malware

What Types of Businesses Should Be Concerned?

- Any business that has possession of private and/or confidential data
- Any business concerned about an outsider causing their business to simply stop
- Common industries are:
  - Finance (banks, insurance co's & brokers, wealth mgr.'s)
  - Healthcare
  - Education
  - Retail (e.g. Target, Home Depot)
  - Manufacturers, Suppliers and Distributors

What can NetGain provide?

- **Assess** – Comprehensive Risk Assessments
- **Recommend/propose** – Strategic Security Solutions
- **Implement** – Certified Engineered Deployments
- **Remediate** – Security Correction and Verification
- **Monitor** – Complete Awareness
- **Manage** – Worry Free Control

If You Need Help

Contact us: SecurityTeam@NetgainIT.com

859-255-0155