Understanding Cybersecurity Threats

Russ Ward, GSE, CISSP
russ.ward@uah.edu
UAH Chief Information Security Officer (CISO)
Who am I...

• B.S. in Computer Science with Information Assurance Professional Certificate.
• 17 years in IT security in EDU, DoD and Business
• 12 current certifications (9 GIAC, CISSP, CEH, CEI)
• Ex-system, network, storage and HPC administrator.
• DoD Contractor (Assessor, Incident Response/Handling, Forensics, Software Development and Blue team activities)
• Areas of focus:
  – Securing the “unsecurable”, well at least different.
  – SCADA / ICS security
  – HPC security
  – Forensics
  – Education
  – Research
Cybersecurity Threats

WEB ATTACKS

FORMJACKING ATTACKS

ENTERPRISE RANSOMWARE

OVERALL RANSOMWARE

56% up

12% up

20% down

4,800 average number of websites compromised with formjacking code each month

Source: https://www.symantec.com/security-center/threat-report
MALICIOUS EMAIL

78% of malicious email attachments are office files, up from 5% in 2017.

NUMBER OF ATTACK GROUPS USING DESTRUCTIVE MALWARE

25%

AVERAGE NUMBER OF ORGANIZATIONS TARGETED BY EACH ATTACK GROUP

55

Source: https://www.symantec.com/security-center/threat-report
What Do You Have?

- Pictures
- House Layouts
- Contracts
- Loan Applications
- Pre-Approval Letters
- Contact Information
- Access to peoples doors
- Clients schedules and locations
- Bank account information
- Social Network

Image Source: https://www.nar.realtor/data-privacy-security
Human Tendencies:

• People...
  – ...fall for phishing
    • Usually an emotional response.
  – ...let unauthorized users access data
  – ...reuse passwords that may be weak
    • Or might be reused several places.
  – ...are inherently trusting
  – ...are too busy
User Awareness and Education

• Users are the first line of defense.
• Without user education they will not be aware of the issues.
• People
  – Over share information
  – Lack the awareness of how to secure IT resources
  – Don’t consider security, or only as an after thought (me too)
  – Want what is:
    • Easy (How hard is it to tack on security later?)
    • Fast (Does it really save time in the end?)
    • Fun (Is it really fun, if you later have to clean it up?)
    • Free (Is free, really free?)
User Awareness and Education: Who needs it?

• Everyone
  – System Administrators
  – Network Administrators
  – Software Engineers
  – Security Staff
  – Administrators
  – Users
  – Me!!
Attack Surface

Past:
Attack Surface

Present:

Source: https://graquantum.com/wp-content/uploads/2016/07/CyberAttackSurface_blogGraphic_Lindsay-1024x790.jpg
Attack Surface – Data

• Data used to reside on servers
  – Fewer places to secure.
  – Easier to monitor.

• A lot of data now resides in the “cloud” and on end user devices.
  – Many points to secure and monitor.
  – Many not University/company owned and controlled.
  – May not be able to monitor cloud storage.
Attack Surface – What to do.

• Use approved storage locations only.
  – These should have contracts in place for legal and security requirements.

• Verify with officials before storing sensitive data.

• Do not store non-public data in personal storage accounts.
  – Usually does not have proper restrictions.
Cybersecurity Issue – Passwords

• Use a string of text that mixes both numbers, letters that are both upper and lower case and special characters.
• The longer the better, but make at least 8 characters. Think passphrases.
• Change your passwords at least every 180 days.
• Do not reuse passwords amongst different systems. A compromise of one account could lead to access to other accounts with the same username and password.
• Use 2 factor authentication when possible.
  – Make sure it is you before you click approve.
Passphrase examples:

• Four buildings on the row, seven total.
  \textit{4botr,7t.}
    • 9 Characters
      – 2 numbers | 5 lower case letters | 2 special characters

• There are four buildings on Engineering row, seven total.
  \textit{Ta4boEr,7t.}
    • 11 Characters
      – 2 numbers | 5 lower case letters | 2 special characters | 2 upper case letters
Cybersecurity Issue – Phishing

• Attackers send phishing emails/texts/calls to steal information or conduct fraud.

• Check the from addresses closely. If it is not from the person’s verified email address then good chance it is phishing.

• Most phishing contains:
  – Grammar and/or spelling errors.
  – Solicit an emotional response.
  – Fake email addresses similar to person it pretends to be from.

• When in doubt contact the “sender” through other methods.

• Not the “sender’s” fault.
Phishing Example from December 15, 2018

From: Christine Curtis (c.curtis.uah.edu@gmail.com)
Date: Saturday, December 15, 2018 11:00 AM
Subject:

Are you available?

Phishing Example from November 16, 2018

From: Jason Greene (jason.greene.uah.edu@gmail.com)
Date: Fri, Nov 16, 2018 at 9:59 AM
Subject: Re:

Am in a meeting now and that's why am contacting you through here, I should have call you but phone isn't allowed during the meeting. I don't know when the meeting will be rounding up. I need you to help me get google play gift card at the store I will reimburse you when I get back to the office
Cybersecurity Issue – Remote Networks

• Connecting your computer/phone/iPad/device to an untrusted (and possibly unprotected) network can lead to attacks against your device.

• When on untrusted networks utilize VPN connections to encrypt your network traffic on the untrusted network.
Cybersecurity Issue – Wireless Networks

- By default most wireless networks are not encrypted.
- Prefer wired over wireless networks when sensitive data is transferred.
- Attackers can capture the network traffic and extract data that is not encrypted by other means.
- Networks with pre shared network keys (PSK) (single password per network) can be decrypted using the PSK.
- Networks that use 802.1x standards utilize a key per wireless device and changes the key often to reduce this risk.
Cybersecurity Issue – Mobile Devices

• These days mobile devices contain a high amount of sensitive data.

• The devices should:
  – encrypt the storage, so it cannot be easily retrieved.
  – be password protected.

• Remote wipe capabilities are useful in the case of a lost or stolen device.
Cybersecurity Issue – Computer Security Settings

• On computers:
  – Install antivirus programs and keep up to date.
  – Install software updates.
  – Disable automatic login and require a password to log in to the computer and to unlock after being unused.
  – Do not use the computer as an administrative user that can modify the operating system or applications.
Cybersecurity Issue – Backups

• If there is sensitive data, then it needs to be backed up on a frequent basis.
• The backup needs to be stored off-site and not connected to the computer.
• Protects the data from:
  – ransomware encrypting the only copy.
  – hardware failure.
  – human error.
Cybersecurity Issue – Data Security

• Identify sensitive data and protect it as such.
• Use only approved storage locations.
• Do not store on personal devices or personal accounts.
• Consult cybersecurity personnel on contracts to make sure vendors protect the data properly.
• Encrypt sensitive data at rest and transit.
Report Suspicious Activity

• If you see something suspicious, report it.
  – Unexpected data changes.
  – Reports of unknown logins to your account.
  – Changes to account information that you did not make.
  – Files changing on your storage locations that you did not change.

• Often the security teams can discover why these changes occurred and whether they were malicious.
Where to Get Cybersecurity Help:

• Other people.
• When in doubt, stop and think.
• IT support personal.
• https://www.nar.realtor/data-privacy-security
• Cybersecurity experts.
• Cybersecurity aware clients.
Closing Thoughts

• Cybersecurity is
  – a growing problem.
  – everyone’s problem.
  – the new attack vector.
  – difficult, if not impossible
  – a moving target.
  – important.
  – best layered.
  – FUN!!!!
Resources

• [https://www.cybrary.it/](https://www.cybrary.it/)
  – Community to promote free cybersecurity education

  – Describes and defines cybersecurity work across the boundaries of industry/govt

• [https://www.cisecurity.org/](https://www.cisecurity.org/)
  – Center for Internet Security

• [https://isc.sans.edu/](https://isc.sans.edu/)
  – SANS Internet Storm Center

• [http://iase.disa.mil/stigs/Pages/index.aspx](http://iase.disa.mil/stigs/Pages/index.aspx)
  – DISA’s Security Technical Implementation Guides (STIGs)
Resources

- [http://www.uah.edu/oit/services/cybersecurity](http://www.uah.edu/oit/services/cybersecurity)
  - UAH OIT Cybersecurity webpage.
  - Contains UA System IT Risk Bulletins:
    - Issue 1 - Passwords (October 2014)
    - Issue 2 - Social Networking (November 2014)
    - Issue 3 - Phishing (December 2014)
    - Issue 4 - WiFi Dos and Don’ts (January 2015)
    - Issue 5 - Mobile Phone Security (February 2015)
    - Issue 6 - Security Risks (March 2015)
    - Issue 7 - Best Practices (April 2015)
    - Issue 8 - Mobile Apps (Summer 2015)
    - Issue 9 - Protect Your Computer and Personal Information (September 2015)
    - Issue 10 - The Importance of Backing-Up (October 2015)
    - Issue 11 - Preventing Viruses and Malware (November/December 2015)
    - Issue 12 - Social Networking (January 2016)
    - Issue 13 - Phishing (February 2016)
    - Issue 14 – Lessons from Current Data Breaches (Spring 2016)
Threat Predictions

Compromised-Accounts  Malware  IoT  HTML5  BYOD

Insiders  Spam  DDoS  CyberCrime

APT's  Regulations  Privacy  Hacktivism

Insecure-Storage  Zero-Days  Mobile-Threats

Botnets  Security-Engineering  CloudComputing
Questions?

Russ Ward, GSE, CISSP
russ.ward@uah.edu
UAH Chief Information Security Officer (CISO)