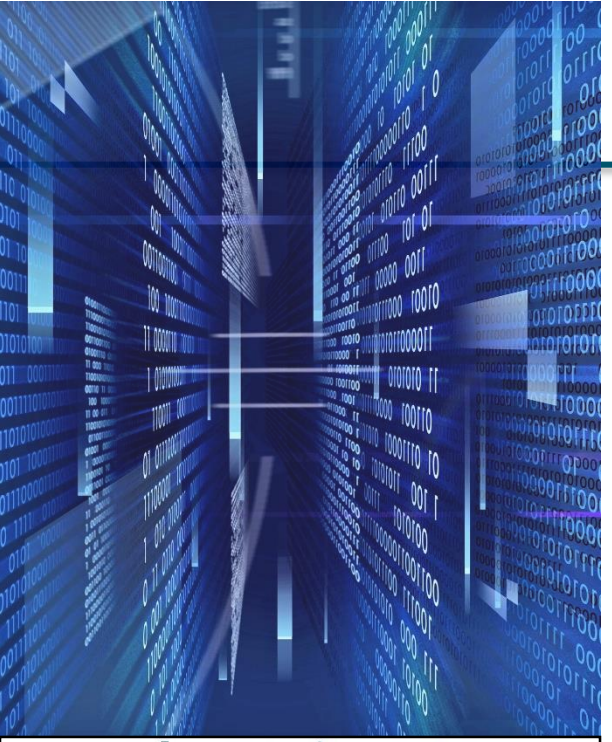


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

Cyber Security Research Group

blog | twitter

UNIVERSITY OF Southampton

COMP6224 2019-20
Foundations of Cyber Security

Corporate Security #1

Week 8 – Friday 22nd November 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

Link with previous lectures

UNIVERSITY OF Southampton

Cyber Security

Cyber Space

- . . .
- . . .
- Access Control
- Confidential/anonymous data/communication
- Authentication (include passwords)
- Cryptography
- Applications
- Data at rest
- Data in transit
- Machines
- Network

Cyber Attacks

- Social Engineering
- Web defacements
- Influence campaigns
- DDoS
- Data breaches
- Ransomware
- Money theft
- Pervasive Passive Monitoring
- Cyber Attack Life Cycle

Cyber Actors

Multi-disciplinary Aspects

- . . .
- . . .
- . . .
- Law

Learning Outcomes

At the end of this lecture you should be able to

- LO1 Describe the basic security measures any organization should put in place (i.e. Cyber Essentials)
- LO2 Discuss the effectiveness of Cyber Essentials against specific cyber attacks

Outline

- **Cyber Essentials**
  - Firewalls
  - Secure Configuration
  - User Access Control
  - Malware Protection
  - Patch Management
- Group Activity on Cyber Essentials

Cyber Essentials

More than half of British firms 'report cyber-attacks in 2019’

Mean cost of all incidents for UK firms: $243K

[Hiscox Cyber Readiness Report 2019]

What basic security controls can be used?

UK Cyber Essentials

- Main goal: protection against the most common cyber threats

- Not effective against advanced attacks
  - Zero-day vulnerabilities
  - Social engineering
  - Advanced Persistent Threats
  - …

Cyber Essentials

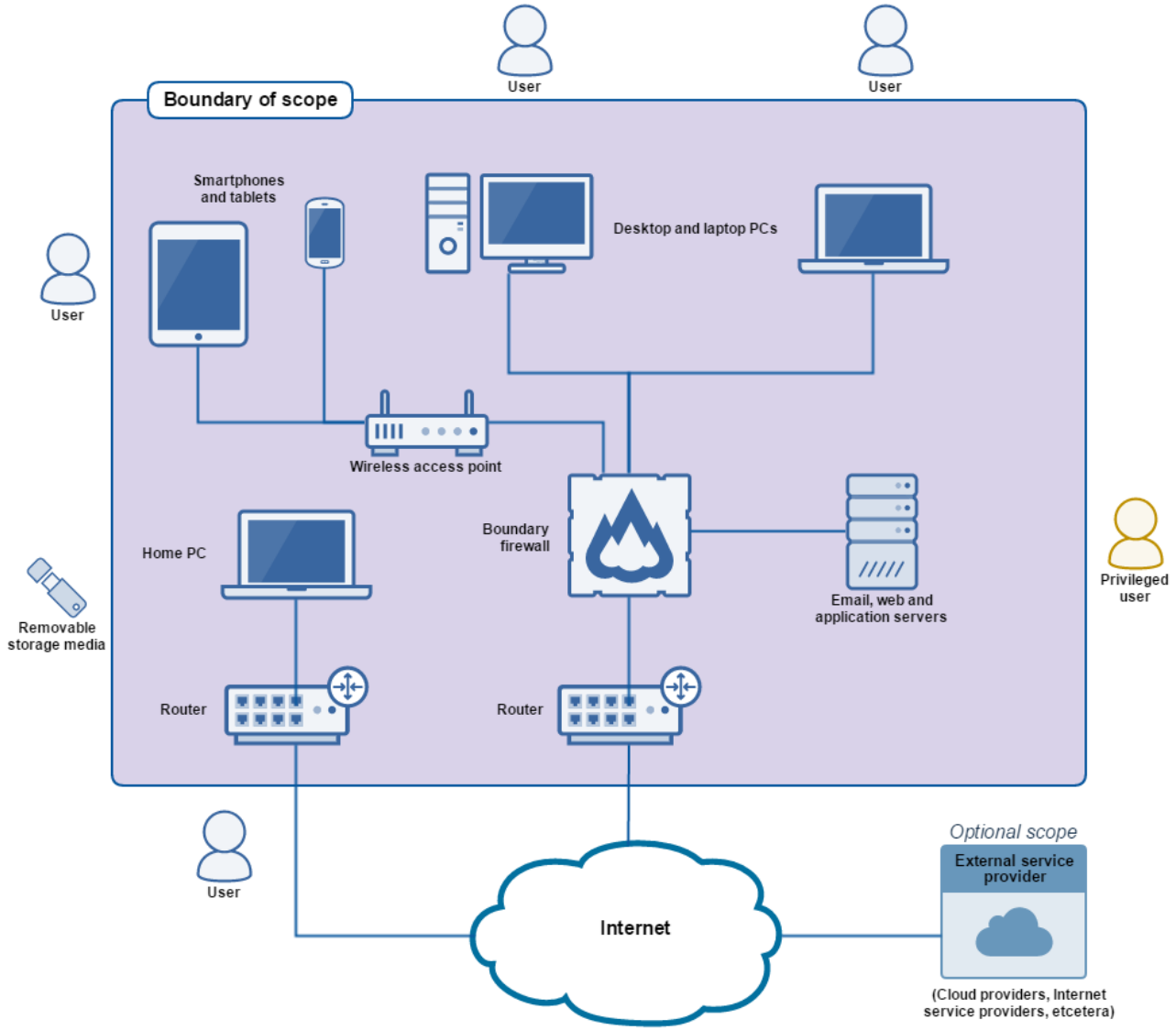
- What are the basic requirements to protect the IT Infrastructure?
  - Firewalls
  - Secure configuration
  - User access control
  - Malware protection
  - Patch management

Cyber Essentials

- First step: define the scope
  - What are the boundaries of the IT Infrastructure to protect?

- The requirements apply to all software/devices within this boundary that
  - Accept incoming connections via Internet from untrusted hosts
  - Establish outbound connections via Internet
  - Control the flow of data between these devices and the Internet

Cyber Essentials



- Bring your own device (BYOD)
- Wireless devices
- Externally managed services
  - Cloud
  - Other
- Web applications developed by third parties

#1 Firewalls

- Objective: ensure that only safe and necessary network services can be accessed from the Internet
- Network security device
- Reduce exposure to attacks (boundary FW vs host-based FW)
- Firewall rules to block/allow traffic on the basis of src, dst, protocol, …
- Requirements
  - Block unauthenticated inbound connections
  - Every inbound rule that accepts connections must be motivated and documented

#2 Secure Configuration

- Objective: ensure that computers/devices are configured to reduce vulnerabilities and provide only strictly required services
- Set of best practices for the configuration of computers/devices
- Default configurations are not always secure
  - Administrative account with known default password
  - Unnecessary applications and services
- Requirements
  - Remove/disable unnecessary software
  - Change default/guessable passwords
  - Disable auto-run features
  - Authenticate users before allowing Internet-access to sensitive data

#3 User Access Control

- Objective: ensure user accounts are assigned to authorised individuals only and provide access to actually required resources only
- Set of processes and techniques to manage accounts and authorisations
- Reduce the risk of information being stolen or damaged
- Compromised accounts with high privileges can result in severe damage
- Requirements
  - Setup a process to create and approve a new user account
  - Always authenticate users before grating access to applications/devices
  - Remove/disable accounts when no longer required
  - Use two-factor authentication
  - Use administrative accounts to perform administrative activities only

#4 Malware Protection

- Objective: restrict execution of known malware and untrusted software
- Verify if software is malicious
- Reduce the risk of damage caused by harmful code
- Potential source of malware infection: email attachments, downloads, direct installation of unauthorised software
- Problems deriving from malware infection: malfunctioning, data loss/leakage
- Requirements
  - Anti-malware software
    - Always up to date, at least daily
    - Automatic scan when files are downloaded, opened or accessed from a network folder
    - Automatic scan of visited web pages, blacklisting of malicious/suspicious websites
  - Application whitelisting
  - Application sandboxing for code of unknown origin

#5 Patch Management

- Objective: ensure devices/software are not vulnerable to known security issues for which fixes are available
- Set of best practices for the maintenance and update of software
- Known vulnerabilities are likely to be exploited soon by attackers
- Vendors release patches for product they still support
  - As soon as new vulnerabilities are discovered
  - Periodically
- Requirements
  - Keep all software updated
  - Keep all software licensed and supported

Outline

- Cyber Essentials
  - Firewalls
  - Secure Configuration
  - User Access Control
  - Malware Protection
  - Patch Management

➢ **Group Activity on Cyber Essentials**

Group Activity on Cyber Essentials: WannaCry

The ransomware self-propagates as a worm over the local network and to random machines on the Internet. The EternalBlue exploit is used for the exploitation of a known vulnerability of Windows' SMB, which listens on TCP port 445. The patch for that vulnerability was released two months before. This allows to install the DoublePulsar backdoor in infected machines, which in turn drops and executes the WannaCry ransomware with high privileges.

After gaining persistence via registration as auto-start service, WannaCry (downloads and) installs Tor to establish an anonymous connection to track infections and obtain unique Bitcoin addresses for ransom payments. It then starts propagating as explained before, encrypts files with specific extensions and shows instructions for the victim to pay the ransom in Bitcoin.

Cyber Essentials Analysis

- Split into groups of 4/5 students
- For each cyber essential, discuss if it might have
  - Prevented the attack
  - Mitigated the impact of the attack
  - Been ineffective
- Give an explanation!!!
- 5 min group discussion
- 5/10 min open discussion

Firewalls

Secure Configuration

User Access Control

Malware Protection

Patch Management

Group Activity on Cyber Essentials

- Firewalls
  - If there is no need to access SMB from the Internet, a boundary FW configured to block TCP traffic to port 445 can prevent the attack
  - Otherwise, a host-based FW configured to block TCP traffic to port 445 where non necessary can mitigate the attack
- Secure Configuration
  - Can mitigate if SMB service is disabled where non necessary
  - Can prevent is SMB service is not required at all
- User Access Control
  - Can mitigate if it is possible to reduce what files can be accessed by the user. However, note that the WannaCry executes with high privileges
- Malware Protection
  - Likely ineffective because anti-malware software could not detect WannaCry when it was first launched
  - Although more advanced anti-malware techniques could have detected WannaCry (e.g. see references), Cyber Essentials require a basic level of anti malware sophistication (i.e. signature-based); as WannaCry was new and no signature was available when the infection started to spread, it is reasonable to state that Cyber Essentials malware protection would have been ineffective
- Patch Management
  - Can prevent the attack if the patch for that SMB vulnerability was installed

Corporate Security #1 – Recap

- Cyber Essentials
  - Firewalls
  - Secure Configuration
  - User Access Control
  - Malware Protection
  - Patch Management
- Are Cyber Essentials effective (against a specific cyber attack)?

Corporate Security #1 - References

- Hiscox Cyber Readiness Report 2019
  - https://www.hiscox.co.uk/sites/uk/files/documents/2019-04/Hiscox_Cyber_Readiness_Report_2019.PDF
- Cyber Essentials for organizations
  - https://www.cyberessentials.ncsc.gov.uk/
  - https://www.cyberessentials.ncsc.gov.uk/advice/
- WannaCry detection
  - Chen, Q. and Bridges, R.A., 2017, December. Automated behavioral analysis of malware: A case study of wannacry ransomware. In 2017 16th IEEE International Conference on Machine Learning and Applications (ICMLA) (pp. 454-460). IEEE.