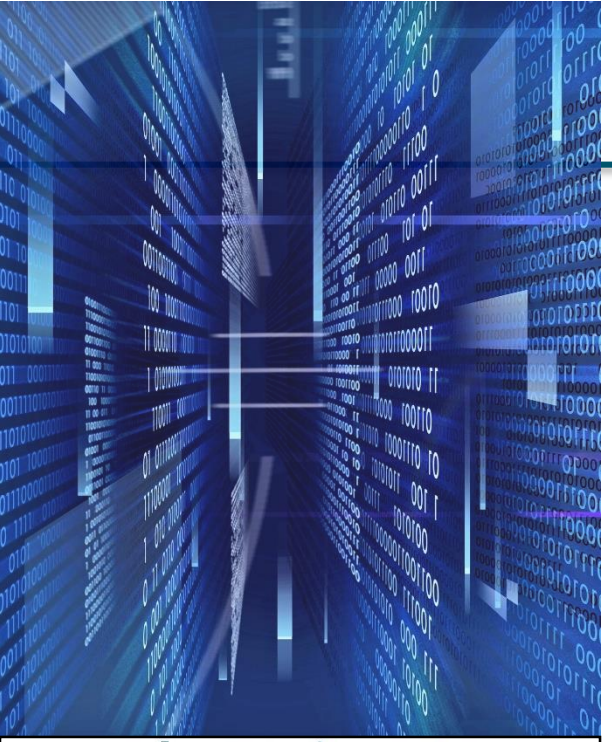


cybersecurity centre
GCHQ Academic Centre of Excellence EPSRC

Cybersecurity Southampton

Cyber Security Research Group

blog | twitter

UNIVERSITY OF Southampton

COMP6224 2019-20
Foundations of Cyber Security

Corporate Security #2

Week 9 – Tuesday 26th November 2019

Dr Leonardo Aniello

l.aniello@soton.ac.uk

Link with previous lectures

UNIVERSITY OF Southampton

Cyber Security

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

Cyber Space

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

Cyber Attacks

Cyber Actors

. . .

. . .

. . .

- Law

Multi-disciplinary Aspects

Learning Outcomes

At the end of this lecture you should be able to

- LO1 Explain what additional security measures corporations can use (i.e. advanced cyber defences)
- LO2 Discuss the effectiveness of advanced cyber defences against specific cyber attacks

Outline

- **Advanced Cyber Defences**
  - Data Protection
  - Segregation of Duties
  - Network Fragmentation & Monitoring
  - Honeypots
  - Pentesting
  - Standards
- Are Advanced Cyber Defences effective (against a specific cyber attack)?

Data Protection

- Understand the risk
  - What data?
  - Who would want it?
  - What would be the impact?
- Use encryption
  - Data at rest and in transit
  - Key management
- Fragmentation
  - Split data into multiple pieces, stored in diverse locations
  - Harder for an attacker to collect all the fragments
- Data Backup
  - Frequently make copies of data
  - Keep backup data on different, separate devices
- Privacy protection
  - Sanitize information to remove PII

Segregation of Duties

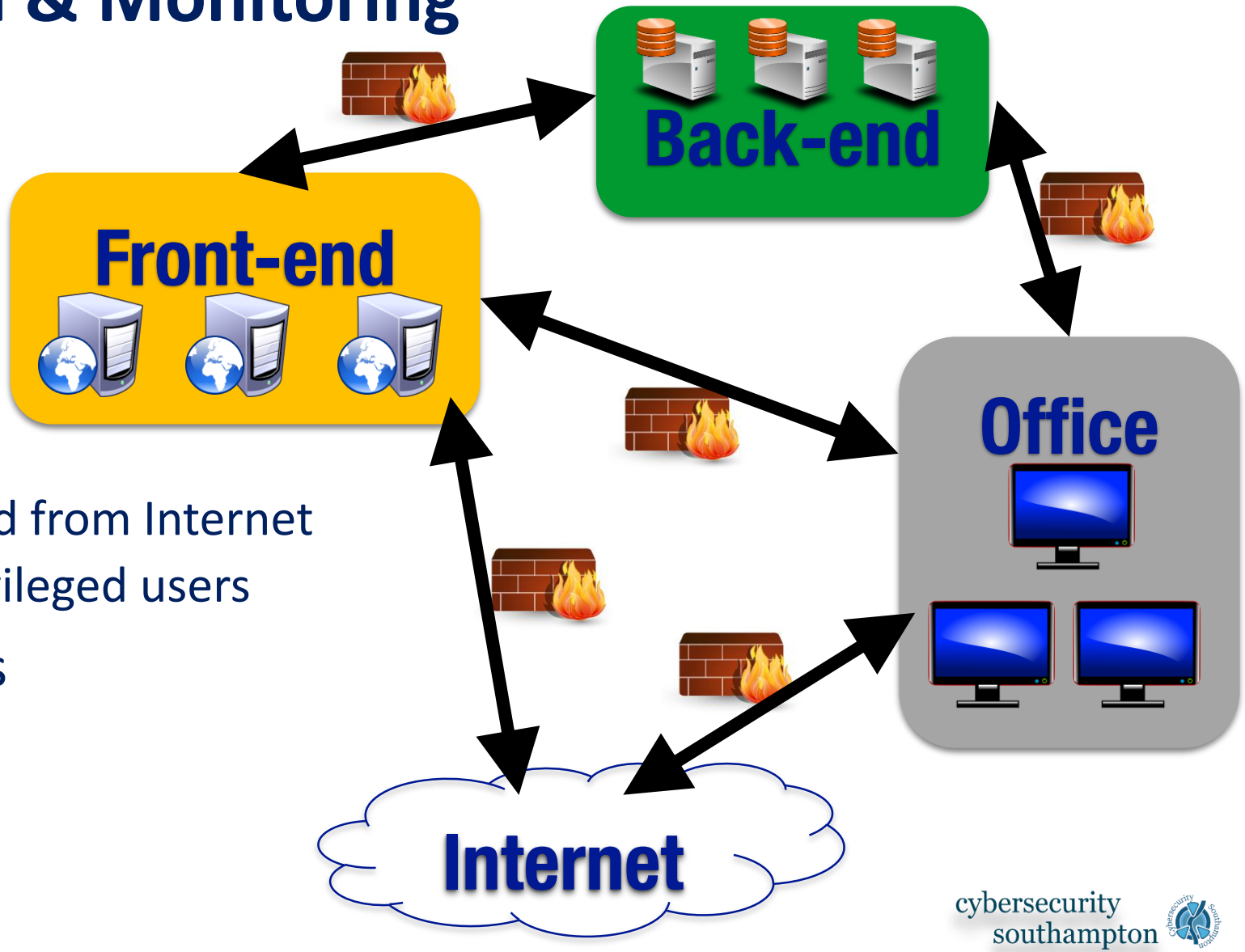
- Basic Idea: have more than one person required to complete a critical task

- Application in Cyber Security
  - If N accounts are required to execute a security-critical task, then N accounts should be compromised to undermine that task

- Example in banking
  - Every sensitive order has to be signed off by at least 2 different people, from 2 different departments

Network Fragmentation & Monitoring

- Split infrastructure based on
  - Business processes
  - Necessary exposure
  - Risk levels
- Example
  - Offices need access to Internet
  - Front-end needs to be accessed from Internet
  - Back-end only accessed by privileged users
- Use firewalls at all boundaries
  - Beware of reconfigurations



Network Fragmentation & Monitoring

- Network monitoring – Intrusion Detection/Prevention Systems (ID/PS)
  - Observe/record all traffic on a given network
  - Detect/block malicious traffic
  - Signature-based vs anomaly-based
  - Alert on suspicious traffic
- Example: an unknown computer starts scanning the whole address space
  - An intruder?
  - An administrator using a new machine?
  - A third party contractor doing maintenance?
- Use machine learning techniques…
  - Accuracy
  - Explainability
  - Adversarial learning

Honeypots

- A decoy to lure attackers
  - HW, SW and data to simulate a real system, actually isolated
  - Attack detection
  - Deflect attackers
  - Gather valuable info on attack strategies
- Research/production honeypots
  - Beware of effective isolation in production honeypots!
- High-interaction/low-interaction honeypots
- Different deployments
- The Honeynet Project https://www.honeynet.org/

Pentesting

- Authorised simulated attack, aimed at assessing the security of a system
  - One of the most effective way to find vulnerabilities
  - Can identify how an attacker could compromise the system
  - Frameworks exist to automate and ease common pentesting operations (e.g. Metasploit)

> *"Imagine that sometime in the not-so-distant future an attacker decides to attack a multinational company's digital assets, targeting hundreds of millions of dollars worth of intellectual property buried behind millions of dollars in infrastructure. Naturally, the attacker begins by firing up the latest version of Metasploit."*
>
> Metasploit - The Penetration Tester's Guide, Introduction

Pentesting

- Penetration Testing Execution Standard (PTES) [http://www.pentest-standard.org]
  - Adopted by several authoritative members of security community
  - Goals
    - Fostering awareness about the importance of penetration testing
    - Establishing fundamental principles for carrying out a penetration testing
- Phases of a Penetration Testing
  - Pre-engagement interactions (goals definition)
  - Intelligence Gathering (what security mechanisms are being used?)
  - Threat Modelling (how can the target be attacked?)
  - Vulnerability Analysis (how can I attack the target in practice?)
  - Exploitation (the actual attack)
  - Post Exploitation (what can I do once the target has been compromised?)

Standards

- ISO 27000 series, NIST 800 series
  - Big, generic and complicated
  - Appropriate for big businesses only
  - In comparison: cyber essentials ~ 10 pages
- Specific standards for specific industries
  - Payment Card Industry Data Security Standard (PCI DSS)
  - Health Insurance Portability and Accountability Act (HIPAA)
- Compliance-driven security is dangerous!
- Yet standards are an efficient stick to drive adoption

Outline

- Advanced Cyber Defences
  - Data Protection
  - Segregation of Duties
  - Network Fragmentation & Monitoring
  - Honeypots
  - Pentesting
  - Standards

➢ **Are Advanced Cyber Defences effective (against a specific cyber attack)?**

Group Activity on Advanced Cyber Defences

UNIVERSITY OF Southampton

Scenario: targeted attack against a big health organisation which manages a large amount of customer personal data

First Attack: email to an employee with malicious attachment, which installs a malware allowing the attacker to control the infected machine remotely; the attacker then scans the internal network searching for the computers where customer personal data are stored

Second Attack: the attacker bribes an insider who has physical access to the data centre of the corporation and can steal customer personal data

Cyber Essentials Analysis

- Split into groups of 4/5 students
- For each advanced cyber defence (no standards) and for each cyber attack, discuss if it might have
  - Prevented the attack
  - Mitigated the impact of the attack
  - Been ineffective
- Give an explanation!!!
- 8 min group discussion
- 5/10 min open discussion

Data Protection

Segregation of Duties

Network Fragmentation & Monitoring

Honeypots

Pentesting

Group Activity on Advanced Cyber Defences

UNIVERSITY OF Southampton

First Attack

- Data protection: can mitigate by encrypting/fragmenting data
- Segregation of duties: can mitigate by requiring two different accounts to gain access to customer personal data
- Network fragmentation & monitoring: can mitigate by making it harder for the attacker to scan the internal network
- Honeypots: could deceive the attacker in the internal network
- Pentesting: can mitigate by providing valuable feedback on how to harden the internal network

Second Attack

- Data protection: encrypting/fragmenting data can make it harder for the insider to collect customer personal data
- Segregation of duties: can mitigate by requiring two different accounts to gain access to customer personal data
- Network fragmentation & monitoring: ineffective
- Honeypots: ineffective
- Pentesting: ineffective

Corporate Security #2 – Recap

- Advanced Cyber Defences
  - Data Protection
  - Segregation of Duties
  - Network Fragmentation & Monitoring
  - Honeypots
  - Pentesting
  - Standards

➢Are Advanced Cyber Defences effective (against a specific cyber attack)?

Corporate Security #2 - References

- Segregation of Duties
  - Stallings, W. and Brown, L., 2018. Computer Security, Principles and Practice, 4: th ed. (sec 17.2, pag 559)
- Network monitoring, Intrusion Detection and Prevention
  - Stallings, W. and Brown, L., 2018. Computer Security, Principles and Practice, 4: th ed. (chapters 8 and 9)
- Honeypots
  - Stallings, W. and Brown, L., 2018. Computer Security, Principles and Practice, 4: th ed. (sec 8.8)
- Pentesting
  - Andress, J., Cyber Warfare, *Techniques, Tactics and Tools for Security Practitioners*, Syngress, 2013. (chapter 11, pag 202)
- Standards
  - Stallings, W. and Brown, L., 2018. Computer Security, Principles and Practice, 4: th ed. (sec 14.1)
  - Payment Card Industry Data Security Standard https://www.pcisecuritystandards.org/pci_security/
  - Health Insurance Portability and Accountability Act https://www.hipaaguide.net/