Cybersecurity BootCamp
week 3

ZERNA Lesly

October 2017

1 Introduction

Cybersecurity BootCamp by CyberWayFinder SPRL consists in a four week training in topics to be introduced into the cyber security field. This training is mainly focused on women.

This document contains my personal notes and extra info about the topics involved during the 4 weeks.

2 Class 7 - Risk assessment (Practice)

Study case with:

- multi-tiered system architecture
- private cloud solutions

What do you need to assess?

- threads
  - potential danger
- inherent risk (raw)
  - cost is on a yearly basis
  - probability * impact = risk
  - impact:
    - significant
    - major
    - catastrophic, financial loss > 1million EUR
- type:
  - strategic (out of scope)

  - operations
  - architecture
  - access control

What to do?

- excel sheet
- network diagram
- mr-know-it-all (ask?!)

We analyzed two networks. The first one typical with a firewall in front of the Data Bases, Middle ware and Front. The second network involved Virtual Machines and only a firewall at the input of the local network.

Differences between: system stand-by vs. loading balance **loading balance** preferable when you have multiples data centers. Normally 1 data center should not have more than 40% of work or load.
When using the excel for analysis:

- thread agents
- **thread scenario** -> when you make presentation to CEO, board, etc
- **exploitable**
- **impact** -> board might know about this impact
- **control**
  - detect
  - prevent
  - reactive

Example study case in excel!

Acronyms

- **SOC** -> Security Operation Center
- **SIEM** -> Security Incident Event Management
- **BCP** -> Business Continuity Plan
- **DRP** -> Disaster Recovery Plan
- **IPS** -> Intrusion Prevention System
- **IR** -> Incident response
- **ISO27000** -> standard

- **UPS** -> Uninterrupted Power Supplies
- **RPO** -> Recovering Point Objective
- **RTO** -> Recovering Type Objective
- **PUAM** -> Privilege User Access Management
- **HSM** -> Hardware Security Module
- **RAP** -> Remote Access Protocol

3 Class 8 - NVISO IOT & Threat Hunting

4 Class 9 - Application Security (Enterprise Architecture)

References