Developing CSIRT Infrastructure

Name | Job Title

Event | Location | Date

European Union Agency for Network and Information Security

Exercise overview

Introduction

Task 1 - Discuss the proposed infrastructures for the incident handling – incident analysis service

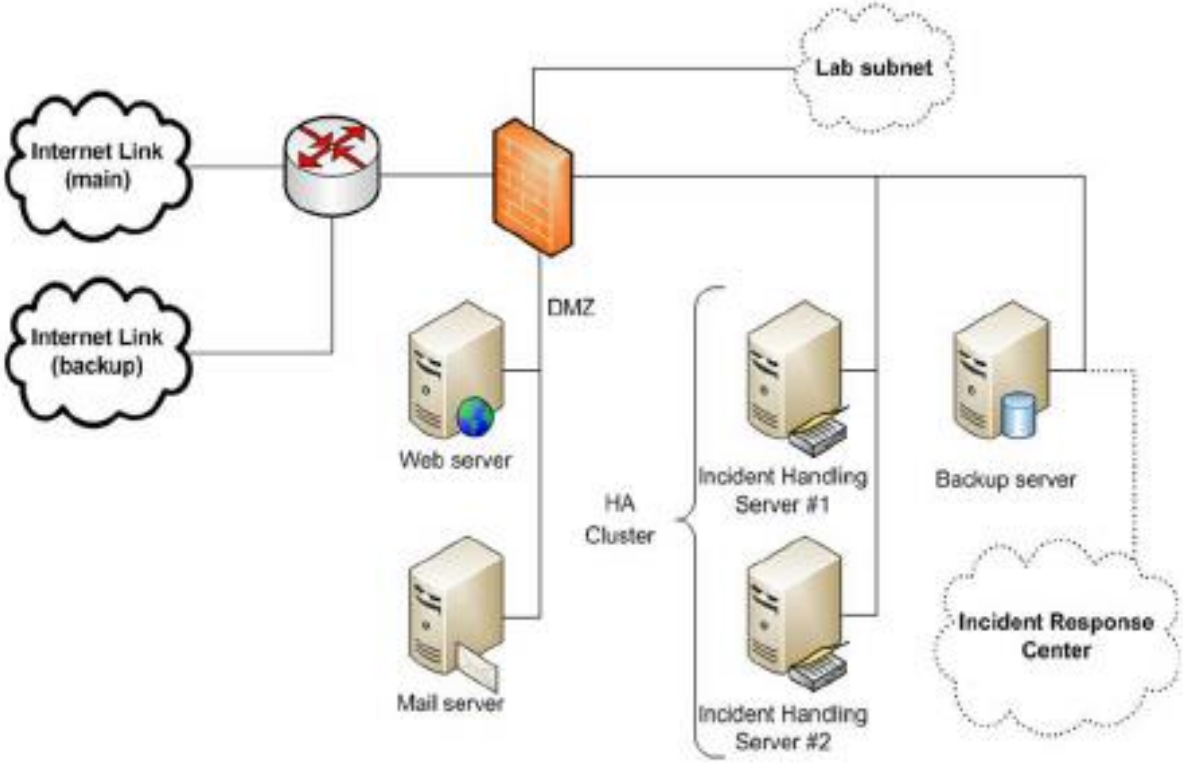
Task 2 - Discuss the proposed infrastructure for a further 3-5 services

Conclusion

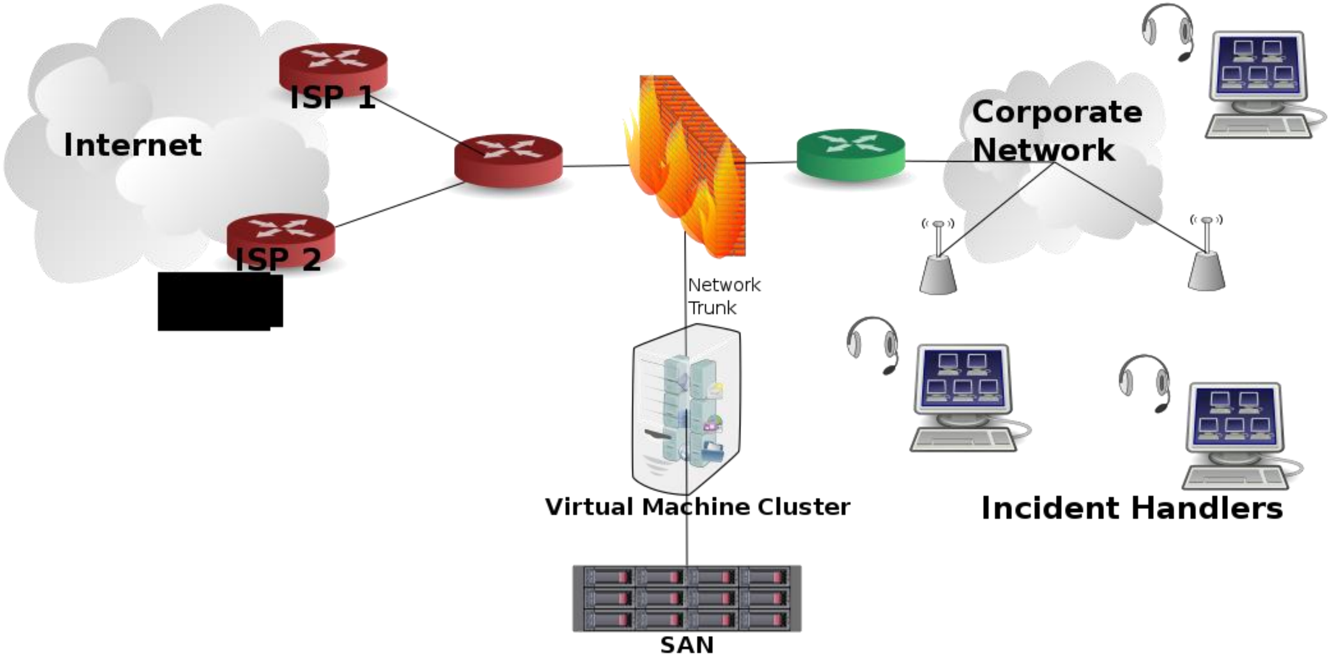
CSIRT services

Reactive Services	Proactive Services	Security Quality Management Services
- Alerts and Warnings - Incident Handling - Incident analysis - Incident response on site - Incident response support - Incident response coordination - Vulnerability Handling - Vulnerability analysis - Vulnerability response - Vulnerability response coordination - Artefact Handling - Artefact analysis - Artefact response - Artefact response coordination	- Announcements - Technology Watch - Security Audits or Assessments - Configuration and Maintenance of Security Tools, Applications, and Infrastructures - Development of Security Tools - Intrusion Detection Services - Security-Related Information Dissemination	- Risk Analysis - Business Continuity and Disaster Recovery Planning - Security Consulting - Awareness Building - Education/Training - Product Evaluation or Certification

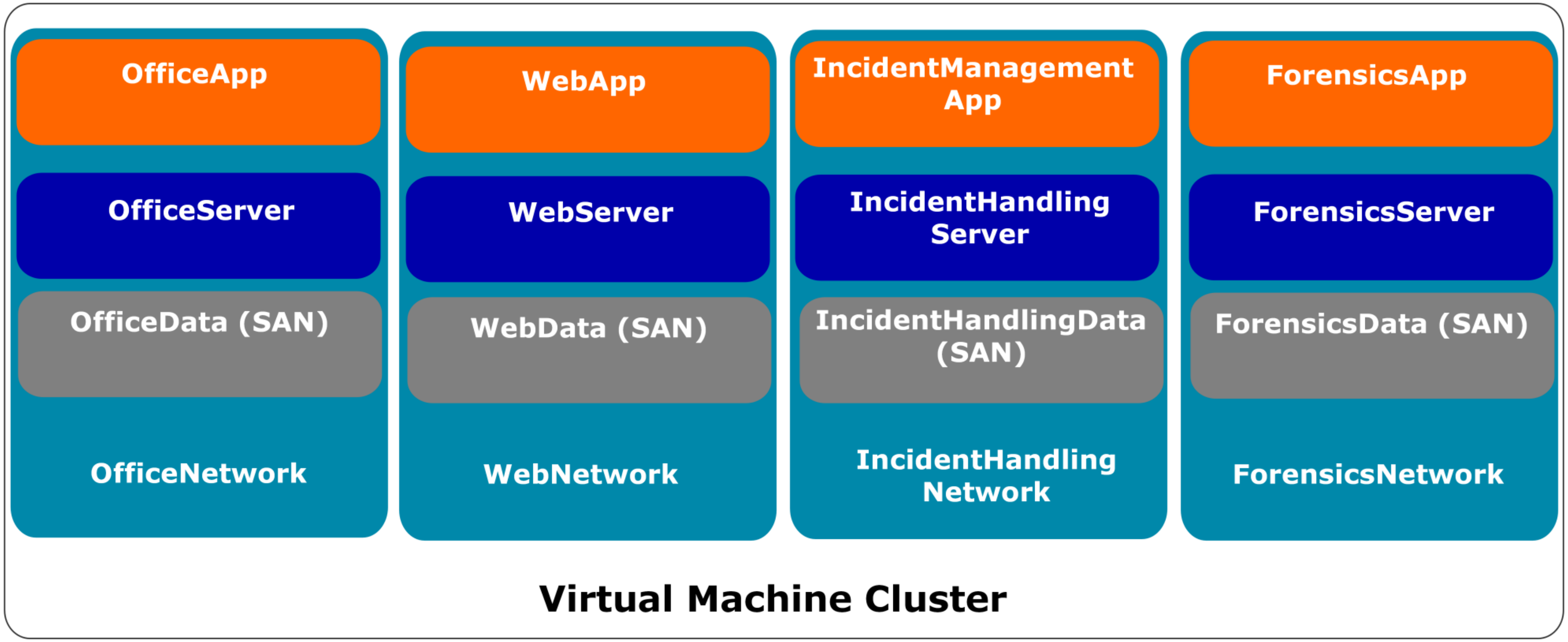
Simple (legacy) infrastructure



Updated CSIRT infrastructure



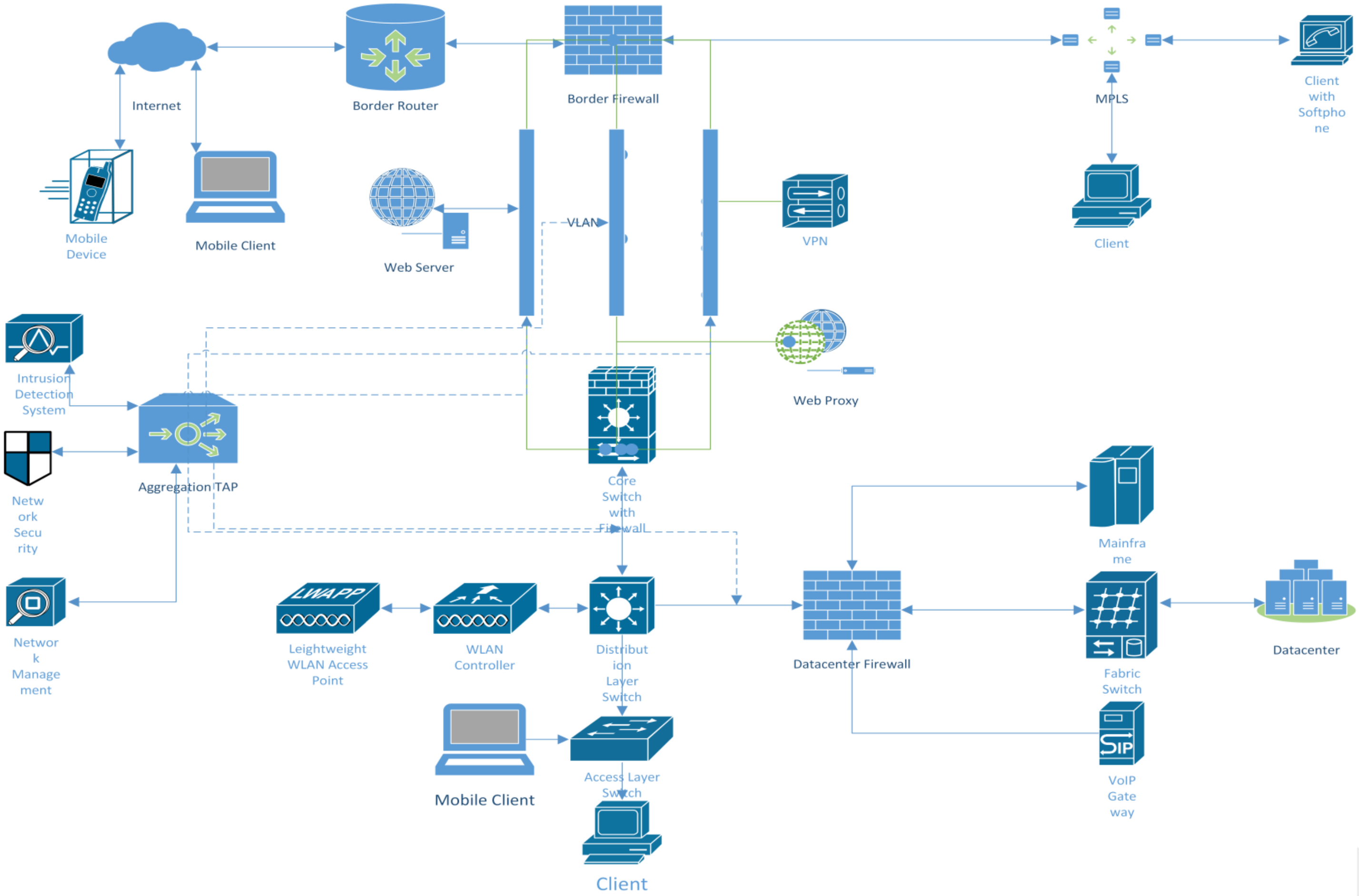
Virtualisation Layers



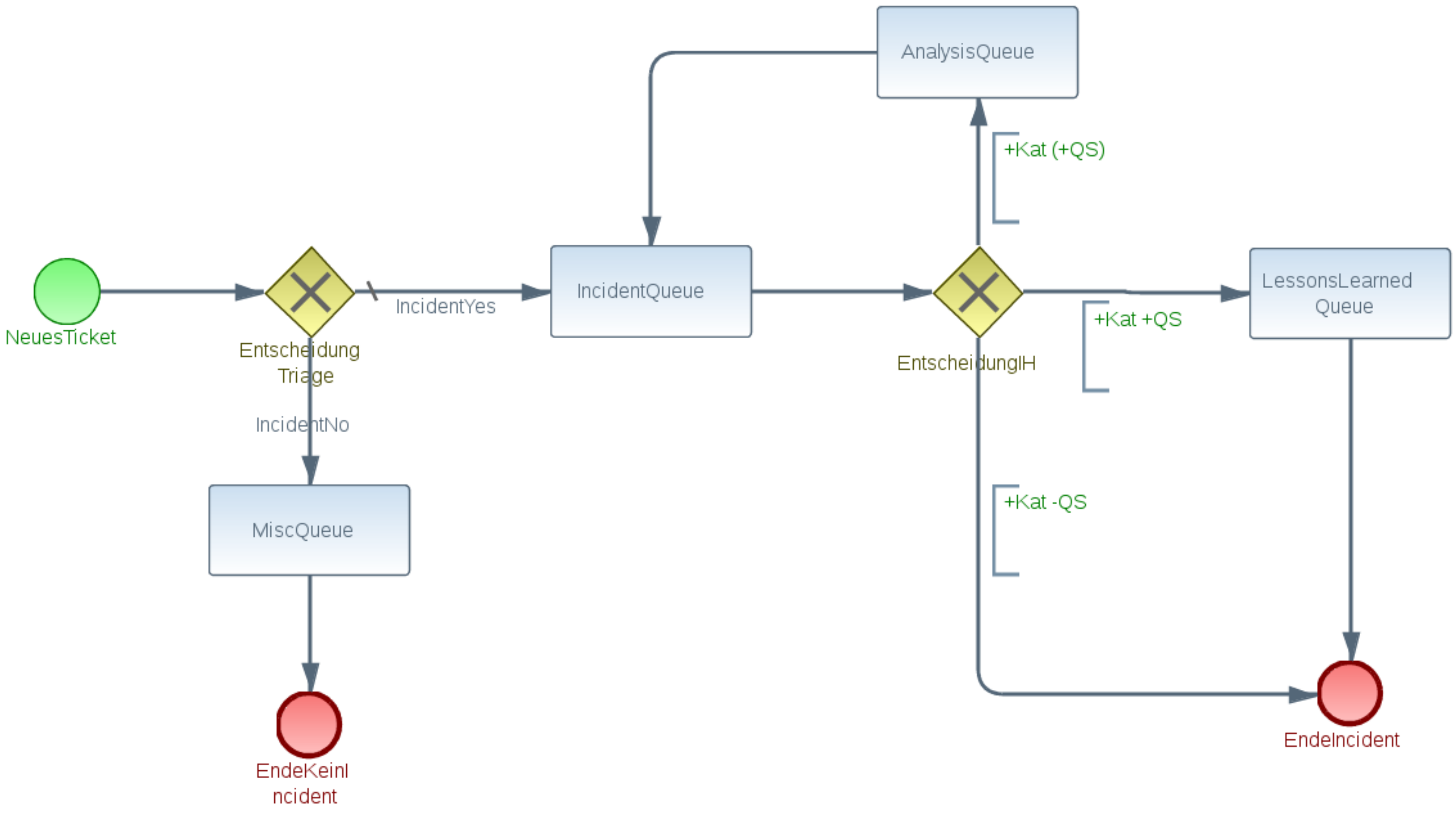
OfficeApp	WebApp	IncidentManagement App	ForensicsApp
OfficeServer	WebServer	IncidentHandling Server	ForensicsServer
OfficeData (SAN)	WebData (SAN)	IncidentHandlingData (SAN)	ForensicsData (SAN)
OfficeNetwork	WebNetwork	IncidentHandling Network	ForensicsNetwork

Virtual Machine Cluster

Enterprise-scale network architecture



Incident Handling workflow



Task 1: Questions

1. Discuss the proposed infrastructures for the incident handling – incident analysis service

Task 2: Questions

1. Discuss the proposed infrastructure for a further 3-5 services
2. The set of services chosen should include services from all main categories such as reactive services, proactive services and security quality management services (see the CSIRT services table by CERT/CC)

CSIRT services

Reactive Services	Proactive Services	Security Quality Management Services
- Alerts and Warnings - Incident Handling - Incident analysis - Incident response on site - Incident response support - Incident response coordination - Vulnerability Handling - Vulnerability analysis - Vulnerability response - Vulnerability response coordination - Artefact Handling - Artefact analysis - Artefact response - Artefact response coordination	- Announcements - Technology Watch - Security Audits or Assessments - Configuration and Maintenance of Security Tools, Applications, and Infrastructures - Development of Security Tools - Intrusion Detection Services - Security-Related Information Dissemination	- Risk Analysis - Business Continuity and Disaster Recovery Planning - Security Consulting - Awareness Building - Education/Training - Product Evaluation or Certification

Task 1/2: Questions and hints

1. Incidents could be reported several ways and via many channels. Which communications channels should be maintained by CSIRT teams at a minimum?
2. How would you organise the incident response handling process?
3. What tools can be used to better organize teamwork and information flow – especially for incidents reported via the Internet?

Task 1/2: Questions and hints

4. Where are incident reports stored and why is this so important?

5. How can we address a failure or outage of communication channels and servers?

6. How would you monitor your network for the failure or outage of servers, internet connections, etc.? How then would you respond to network failures?

7. How can CSIRTs secure their infrastructures?

Task 1/2: Questions and hints

8. Sometimes incident analysis requires going outside the network centre or lab. What tools are helpful in working remotely?

9. Some teams work as so-called “virtual teams”, these do not share a physical location or office but rely on the communication and collaboration capabilities of internet services.

Task 1/2: Questions and hints

10. Based on our answers for the last questions, what basic software should you have on hand for incident handling?

11. What basic software do you need to perform incident analysis?

- network forensics
- malware/binary analysis

Conclusion

Question No.	Topic	Answers	Comment
1.	Incident report channels		
2.	Workflow organisation		
3.	Workflow organisation tool requirements		
4.	Incident information storage		
5.	Infrastructure availability		
6.	Infrastructure monitoring / Failure response		
7.	Infrastructure security		
8.	On premises incident response tools		
9.	Virtual team requirements		
10.	Incident handling tools		
11.	Basic incident analysis tools		

Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu