Security Officer:
An NREN Secondee Perspective

Jan Kohlrausch, DANTE

TF-CSIRT Meeting
18/19 September 2014
Rome

connect • communicate • collaborate

Background

- About me:
  - Senior Incident Handler and Researcher with DFN-CERT
  - Currently member of ACDC project (Fighting Botnets)

- NREN Security Officer / Secondee at DANTE
  - Position from 14th July to 23rd December
  - Motivation: Win-Win situation

- Content:
  - Overview of the Security Officer Role
  - Preliminary Results
  - Benefits for the constituency and other security teams

Motivation

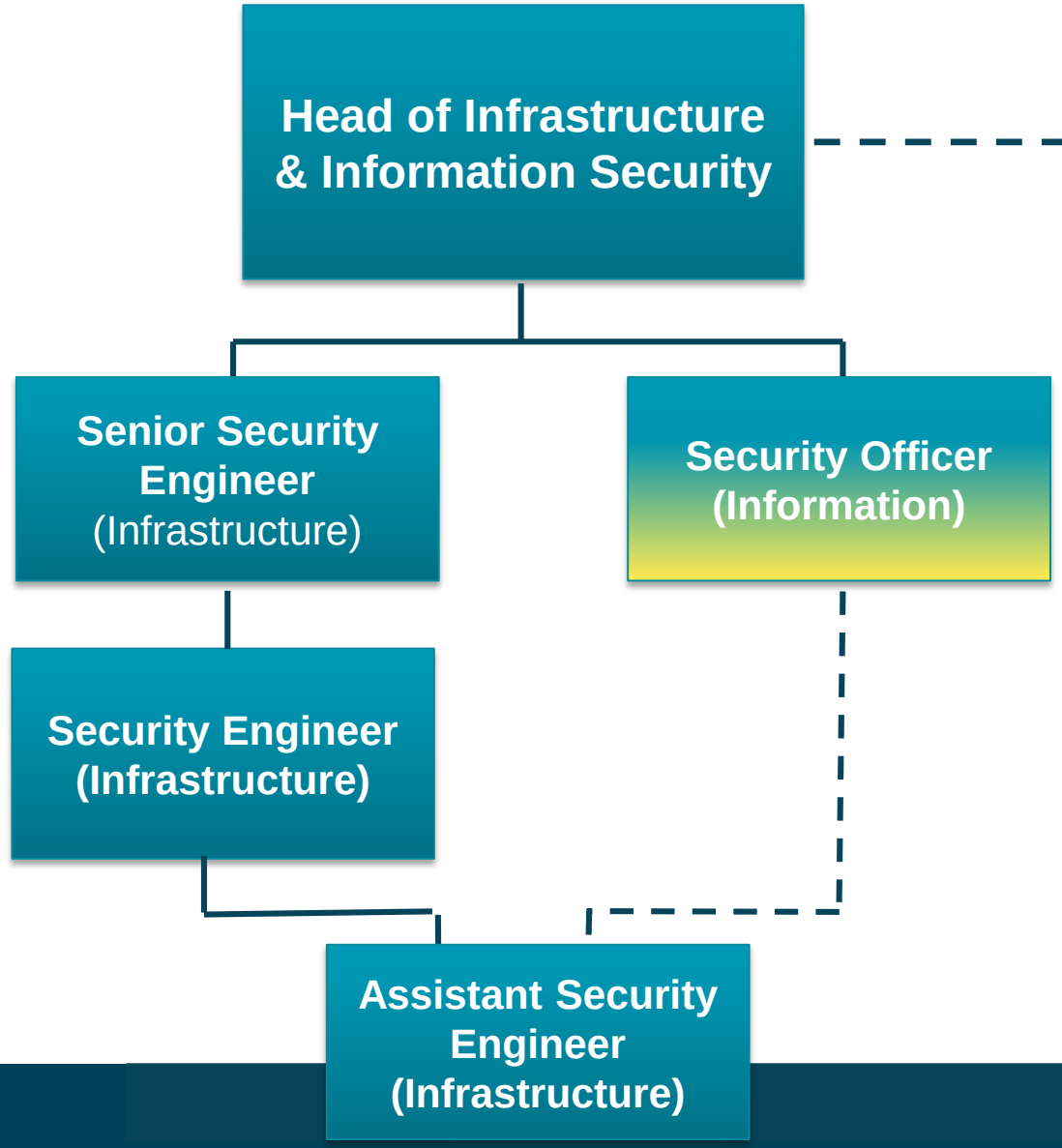
- New Chances and Threats:
  - Cloud Computing
  - Mobile Devices

- New Challenges:
  - Targeted Attacks (APT)
  - Large-scale DDoS (Reflector attacks)
  - Large increase of number of malware samples and attacks

- Increased collaboration among security teams:
  - Incident Data Exchange
  - IOC
  - Trust becomes more and more important

Security Officer

Security Team - Proposed New Structure



Security Officer Role

- Recommendation of the NREN & ISP Security Working Group
- Separation into
  - *Information Security*
  - *Operational Security (Infrastructure Security)*

Security Officer Objectives

- Security Policies and Guidelines
  - Cloud Computing
  - BYOD
  - AUP
- Review of Incident Handling Processes
- Prepare for TI Certification
- Initiate project for ISO 27001 certification

→ Important for building trust in the CSIRT community

Building Trust

- **Following Best Practice**
  - Security Controls to protect the GÈANT Network
  - Enforcing and Auditing Security Polices
  - Data Protection and Security
  - Incident Handling
- **Code of Conduct**
  - Collaboration with constituency and security teams
  - Demonstrating responsibility
  - Providing help and information
- **Security Audit**
  - Following Standards (ISO 27001 Series)
  - Trusted Introducer Accreditation/Certification
  - NREN Security Working Group Review

Cloud and BYOD Policy

- **Challenges:**
  - Benefit from Cloud Services and Mobile Devices omitting specific Risks
  - Coping with the loss of governance
  - Selecting the appropriate scope:
    - *Cloud Models (SaaS, PaaS, and IaaS)*
    - *Eligible Mobile Devices and Operating Systems*
- **Preliminary Results:**
  - Survey of Best Practices
  - Requirement collection for both polices
    - *Current and future requirements*

ISO 27001 Certification

- **Overview:**
  - Information Security Standard
  - Used to specify a Information Security Management System
  - 14 Groups of controls, e.g.:
    - *Information Security Policies*
    - *Human Resources*
    - *Information Security Incident Handling*
    - *Compliance*
- **Approach:**
  - Threat Analysis
  - Definition of scope: e.g. Focus on DANTE CSIRT
  - Implementation of controls
  - Further improvement

TI Certification

- **Trusted Introducer:**
  - Clearing House for CSIRTs
    - *Directory of CSIRTs*
    - *Supporting data exchange*
  - Levels of Trust
    - *Registration*
    - *Accreditation*
    - *Certification*
- **TI Certification uses the "SIM3 Model" to assess CSIRTs maturity**
- **Gap Analysis of required documents and TI certification process**

Conclusion and Outlook

- **Conclusion**
  - Separation of operational and information security as advised by the NREN & ISP Security Working Group
  - NREN Secondee position to define Security Officer role
  - First preliminary results on security polices and TI/ISO 27001 certification
- **Outlook**
  - Further work on policy creation and enforcement
  - Continuing with the ISO 27001 certification process
  - Further involvement of the NREN community:
    - *Continuation of the Security Officer role as NREN Secondee?*
    - *Collaboration with NREN CSIRTs pertaining new security services*

Thank you

Any questions?