Charity Organisation - “SikreNorge”

Abdisalan Mohamed Hussein
Job Nestor Bahner
Johannes Borgen
Thomas Løkkeborg

Non-profit charity organisation that provides information security services to businesses and institutions in Norway. The organisation seeks to secure Norway by helping those who would not otherwise have the means to prioritize security.

Agenda

- Business case
- ISMS
- ICT and Network Infrastructure
- Questions

Business Case

Background

Reliant on local volunteers and hired professionals. Operates through donations, government subsidies and income from webshop.

Locations

18 “Learning Centres”, one in each county:

- 1 Headquarter. Hosts internal services.
- 17 Branch sites. Connected to HQ for services.

Services

- Consultation on-site and at learning centre
- Teaching at Learning Centre
- Network security laboratory
- Public website
  - Webshop
  - Learning resources
  - Info
- Management website

ISMS

To be discussed:

- Security Policy
- Risk assessment

Security Policy

EISP with ISSP elements as defined in *Principles of Information Security 4th ed.* - M.Whitman

- Statement of policy
- Responsibilities
- Authorized access
- Prohibited usage of equipment
- Systems management
- Violation of policy
- Policy review and modification
- Limitations of liability

Statement of policy

- Our organization

  “Every member is expected to know the content of our policy and comply. Ignorance is equal to non compliance.”

Security Policy Key Points

Responsibility

- CO’s
- CISO

Awareness rising

- Briefing

Classification

- Official
- Confidential
- Restricted
- Secret

Passwords

- NIST recommendations

Emails

Storage and transfer of data

- Restricted access, AAA
- Encryption
- Disposal

Risk Assessment

- Unauthorized access to confidential data
- Branch losing connection to HQ
- Leakage of confidential information by employee or volunteer
- DDoS on our website
- Failure due to natural disaster at the HQ
- Failure due to power outage at HQ

Other risks handled in *Methods for hardening*

ICT and Network Infrastructure

Focus in design is cost reduction.

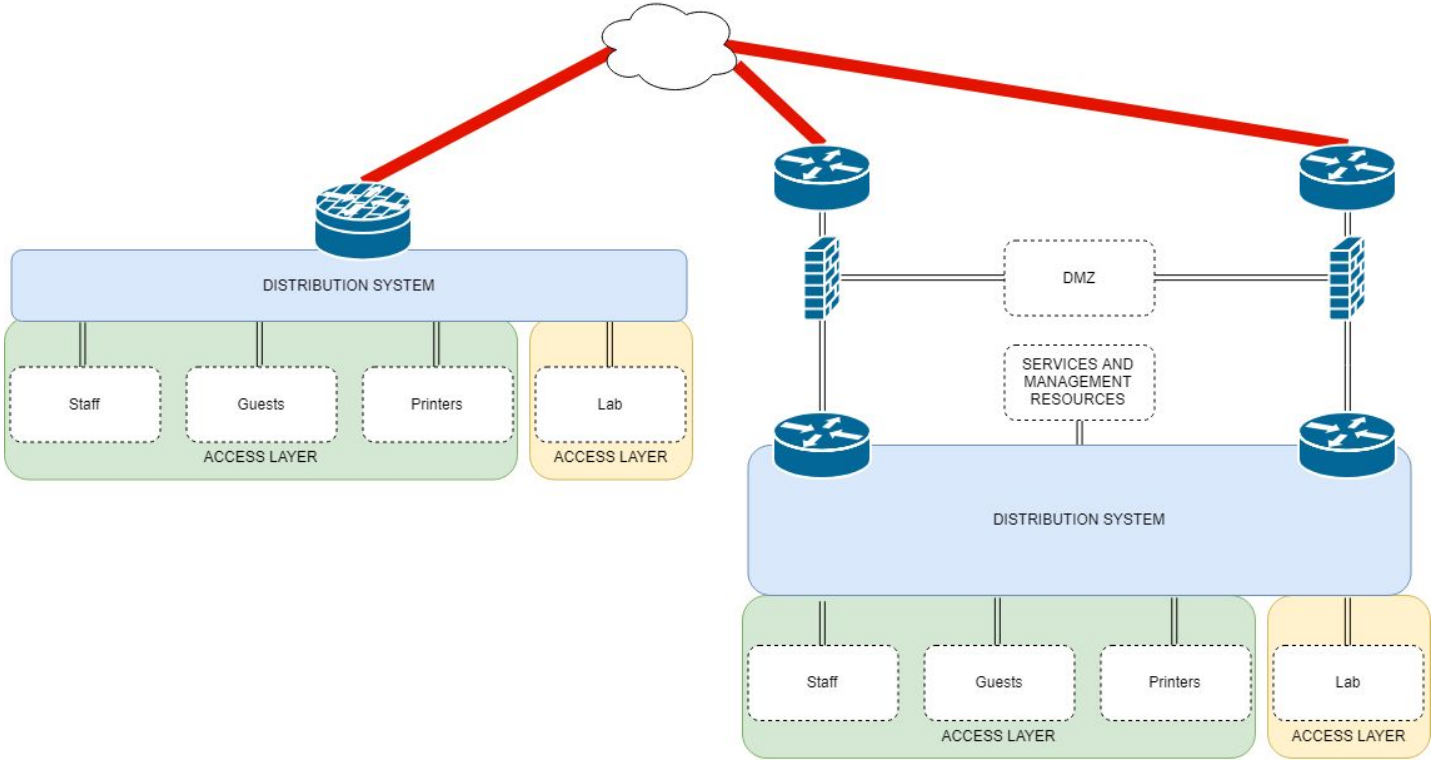
To be discussed:

- Architecture
- WAN
- Methods for hardening
  - Physical
  - LAN
  - Network infrastructure
  - Endpoint security

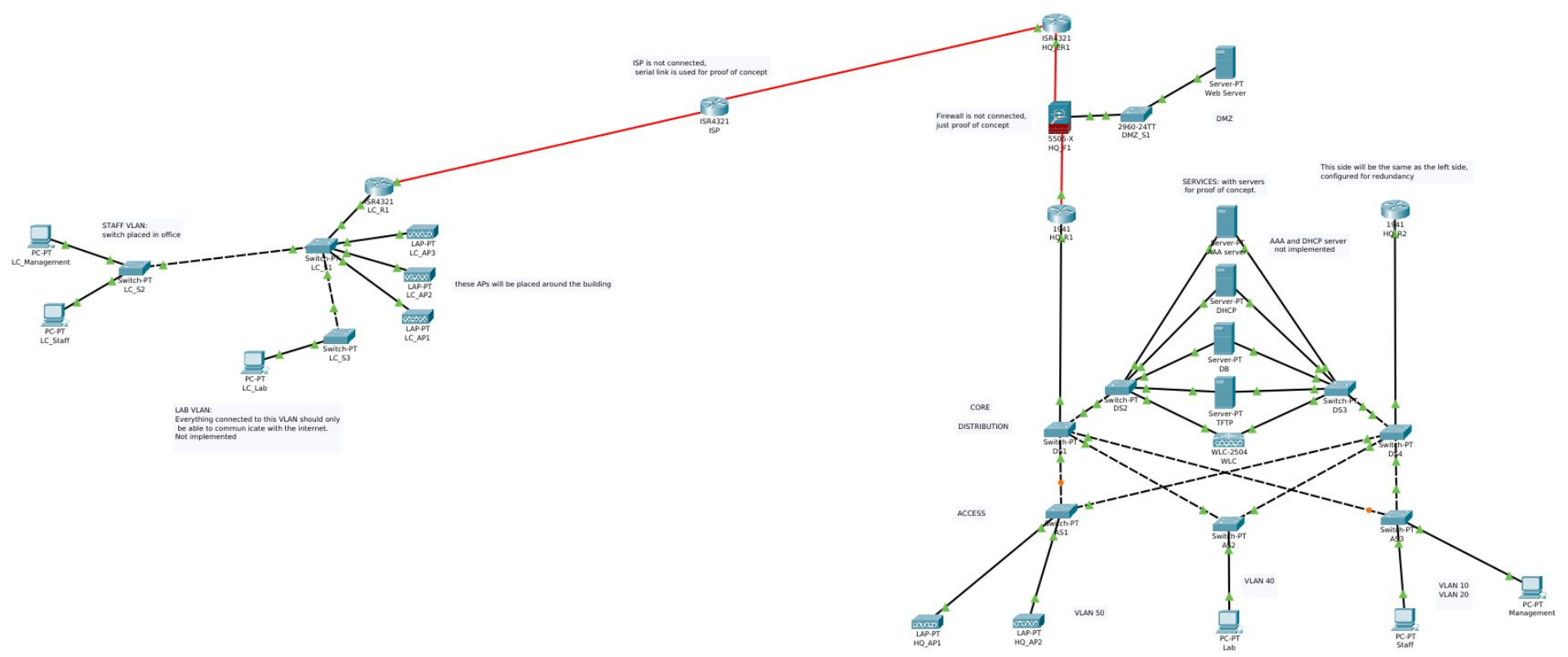
Architecture

- Collapsed-core
  - Chosen over 3-tier for simplicity and cost savings.
  - Provides performance and redundancy to services.
- GLBP for First Hop Redundancy at HQ
- Lightweight Access points with Wireless LAN Controllers

Logical Design



Physical View / Demo Implementation



WAN

- WAN through VPN
- IPsec site to site
- Encryption and key sharing
- AES 256
- Diffie-Hellman PSK group 5 (..oops)

Methods for Hardening

Physical:

- Premise access:
  - Restricted staff and management premises
  - Restricted server room
  - Surveillance + mantrap
  - ID-cards
- Device access:
  - Physical ports secured
    - Passwords
    - Not in use - disabled

LAN:

- Separate switches
- Access ports
  - Port-security
  - STP security
  - Disabled DTP
- Trunks
  - Native blackhole VLAN
- DHCP Snooping
- DAI
- IPSG

Methods for Hardening

Network infrastructure:

- Router and switch access
  - SSH
- Firewalls
  - Next-gen
- AAA
  - TACACS+ server
  - 802.1x
  - NTP
- ACL’s
  - Lab and guests
  - Management

Endpoint security:

- Anti-Malware Protection
- Email Security Appliances
- Web Security Appliances
- Network Admission Control

Questions?