Recommended ICT Security Architecture In the Higher Education Sector

Best Practice Document

Produced by UNINETT led working group on security
(UFS122)

Authors: Gunnar Bøe, Per Arne Enstad, Øyvind Eilertsen
March 2011

Document No: GN3-NA3-T4-UFS122
Version / date: March 2011
Original language: Norwegian
Original title: “Anbefalt IKT-sikkerhetsarkitektur i UH-sektoren”
Original version / date: 2009-08-28
Contact: campus@uninett.no

UNINETT bears responsibility for the content of this document. The work has been carried out by an UNINETT led working group on security as part of a joint-venture project within the HE sector in Norway.

The review and translation of this report has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 23 8875, relating to the project 'Multi-Gigabit European Research and Education Network and Associated Services (GN3)'.

Table of Contents

Executive Summary

The goal of this document is to serve as a guide for the implementation of ICT security architecture in the Norwegian higher education (HE) sector. The recommendations are based on “best practice”, risk assessments, regulatory and commercial requirements, and directives issued by the Norwegian Data Inspectorate (*Datatilsynet*), with a major emphasis on existing practices.

The target group comprises ICT and network managers at HE institutions.

The project group has been made up of the following personnel: Gunnar Bøe, Per Arne Enstad, Øyvind Eilertsen, Vidar Faltinsen, Kenneth Høstland, Morten Knutsen, Torgrim Lauritsen, Rune Sydskjør (all from UNINETT), Stig-Henning Verpe, and Arild Nybraaten (NTNU).

1 Document Goal

The goal of this document is to define an overall architecture that will enable HE organisations to appropriately protect their information and information systems. Key requirements for information security include:

- **Confidentiality** (information is not made available or disclosed to unauthorized individuals, entities, or processes).
- **Integrity** (information is accurate and complete).
- **Accessibility** (information is accessible and usable upon demand by an authorized entity).

It is a prerequisite that the organisation in question has prepared an information security policy that specifies its overall security objectives, decisions, and priorities.

2 Overall requirements

An ICT security architecture for the HE sector must meet the following overall requirements:

- Institutions must provide adequate protection for their information assets. Security and risk levels must be *well-established at the management level* and based on risk assessments.
- The ICT systems must comply with the institution's *information security policy*.
- Consideration must be given to relevant regulatory requirements and directives, such as the EU directive on privacy and electronic communication (2002/58/EC) and local legislation.
- The security architecture must comply with the institution's objectives as stipulated in [appropriate local legislation], and with any agreements the institution may have with third parties.
- The ICT systems must be equipped with appropriate capacity and adequate robustness in the event of failure (*resilience*).
- The ICT systems must have sufficient quality.

3 The security architecture

The security architecture is based on the following principles:

- The network must be subdivided into z*ones* and *security classes.*
- There should be a clear separation between *servers* and *clients.*
- Servers and clients must be placed in relevant security classes based on risk assessments.
- Access to services must be controlled by appropriate *security barriers*.
- Virtual servers and clients must be handled according to the same principles as other units.

3.1 Subdivision into zones, security classes and segments

- The subdivision into zones and classes must be based on *risk assessments*.
- The *system owner* is responsible for the classification and placement of the system.
- The subdivision into z*ones* is an underlying principle for the security architecture. A zone defines a minimum level of security. It is recommended to employ three zones: *Open, Internal,* and *Secure* zone. HE institutions may choose to implement additional zones according to requirements and risk assessments.
- A zone at a given security level should have no access to a zone at a higher security level, unless specific permission has been granted.
- A zone at a given security level does not necessarily have access to a zone at a lower security level.
- Each zone contains one or more *network segments,* cf. Figure 1.
- Network segments within a specific zone may operate under different security criteria. Segments within a specific zone operating under common security criteria may be grouped together in a *security class.*
- Network segments in the same zone or security class are not necessarily mutually accessible.

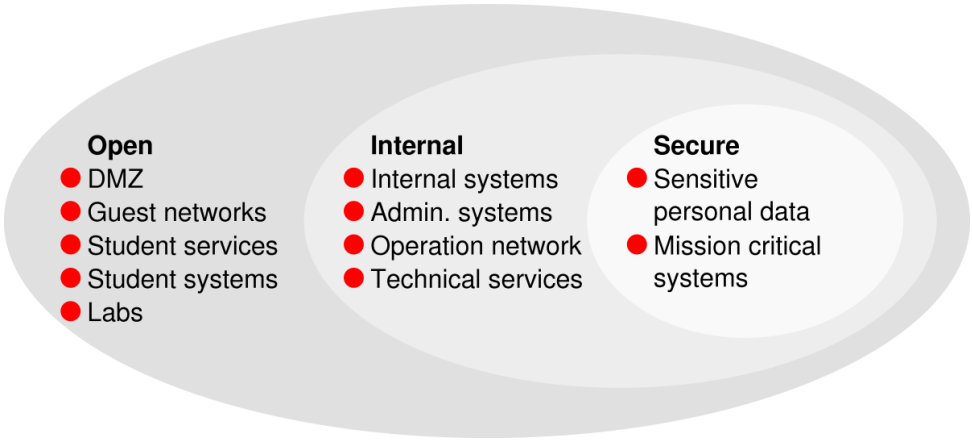

Figure 1: An example of a subdivision into zones and network segments.

3.2 Security barriers

A *security barrier* represents a set of conditions that must be met in order to gain access to resources located in a given zone or security class. The security barrier may consist of one or more of the following elements (the list is not exhaustive):

- firewall/firewall functionality in a router
- packet filter
- application gateways, such as proxies and terminal servers
- authentication and access control
- VPN systems/SSL Gateways
- client requirements
- server requirements

In addition, users must be made aware of their responsibilities by administrative initiatives, including policies, procedures, and training.

3.3 Zone assignment

It is recommended to organise the zones as follows:

Secure zone	Critical systems, i.e. systems that handle sensitive personal data or mission-critical information.
Internal zone	The institution's internal network segments used by employees and others associated with the institution. It should not be possible to access the institution's internal segments directly from machines located outside the institution.
Open zone	Everything else, such as student zones, guest networks, DMZ, and personal equipment.

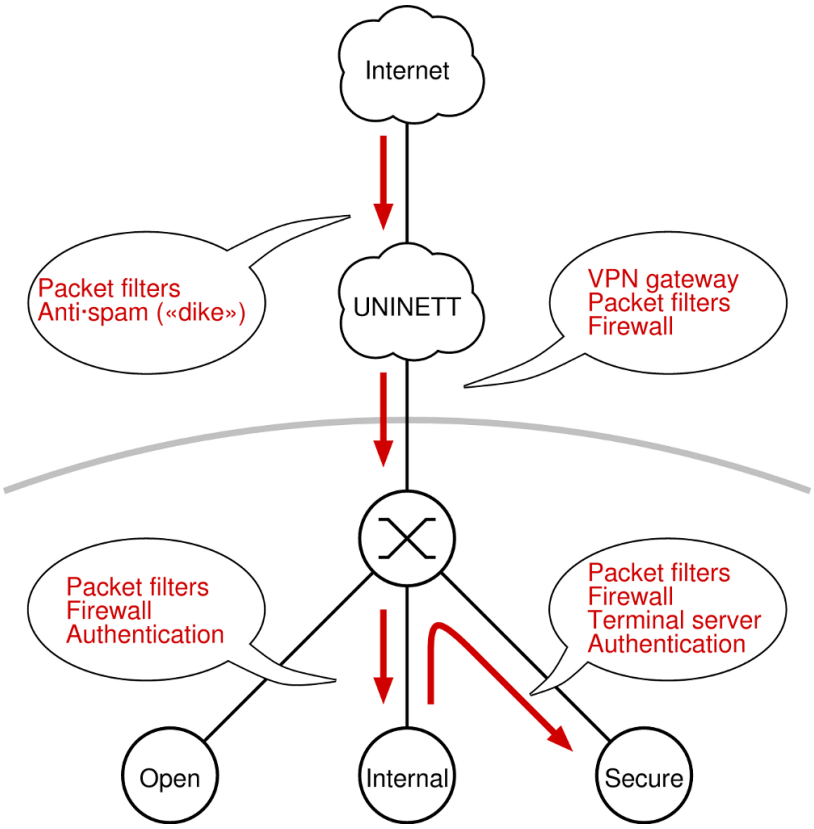

Figure 2: Implementation of zones and security barriers

3.4 Requirements for dedicated servers

Open zone:
Requirements related to good system administration, such as patching and the disabling of unnecessary services. Services located in a demilitarised zone (DMZ) should satisfy additional requirements for servers, such as security hardening and central logging. As a general rule, central logging is recommended for all dedicated servers.

Internal zone:
The same requirements as for the Open zone

Secure zone:
In addition to the requirements employed for the Internal zone, additional measures should be considered, such as integrity checks, host-based intrusion detection, data encryption, security hardening, and central logging.

3.5 Requirements for clients

In all zones, clients should be separated from dedicated servers. In other words, clients and servers should be located in different network segments.

Open zone:

- The institution will determine the client requirements.

Internal zone:

- Clients must be administered centrally, i.e. only system managers have administrator privileges. Administrator privileges will not be given to standard users.
- Clients must comply with the institution's standards for operating systems.
- Client protection measures, such as antivirus software, must be updated to the latest version.
- Private clients, i.e. clients that are not owned nor administered by the institution, must not be located in the Internal zone.

Secure zone:

- Clients should not be placed in the Secure zone.
- Clients requiring access to services in a Secure zone must be located in the Internal zone. These clients must be centrally administered and have updated client protection software. Private clients shall not have such access.
- Special care must be taken if remote access is permitted.

4 Authentication and access control

The term *access control* describes a security barrier that a client must pass in order to gain access to resources hosted in a specific zone and security class.

The following general principles apply:

- Access shall be granted on a “need-to-have” basis only
- Adequate mechanisms must be in place to enable logging and traceability.

In the case of the administration of personal data, local legislation may stipulate logging of historical records for some minimum period. The same applies to other events or incidents that may be significant in terms of ICT security.

Open zone:

- Access control for wireless networks should be implemented using eduroam or equivalent implementations of IEEE 802.1X.
- A separate arrangement must be put in place for guests who are not participants in eduroam.
- Eduroam or equivalent authentication procedures must also be employed in a wired Open zone, such as in auditoria and meeting rooms.

Internal zone:

- All equipment connected to the network must be authenticated, e.g. using IEEE 802.1X.
- All users should be authenticated against a central user database.
- Systems that do not support central authentication must be given special protection.

Secure zone:

- Users wishing to gain access to the Secure zone from the Internal zone must be re-authenticated or re-challenged, e.g. using an application gateway.
- Special care must be taken if remote access is permitted to a Secure zone, such as from an office at home.

5 The services and systems in the zoned network

The system owner of a given service is responsible for determining the zone in which the service will be located and the type of protection it will be allocated. For example, it is not the job of the IT department to decide if a system should be located in the Secure zone. The system owner and IT department must work together to determine both the location and the extent of protection measures.

5.1 Open Zone

The Open zone hosts services that are intended for external access. These include the network segments DMZ (demilitarised zone), guest networks, and labs, as well as the students' network segments. The following subdivision is recommended for individual segments in the Open zone:

5.1.1 DMZ

A DMZ (demilitarised zone) is a network segment that is used to isolate services that are exposed to external access, and which require special protection. Services located in a DMZ may include the following:

- External websites and portals
- Reception of incoming e-mail from external networks
- Webmail servers
- External name servers (DNS, also known as an authoritative or publishing name server)
- VPN services for employees.

5.1.2 Guest networks

A guest network is a network segment intended for guests such as customers, suppliers, and employees at other educational institutions. The institution's own employees may also use the guest network to gain easy access to the internet. In order to maintain traceability, all guest network users should be authenticated.

From a security point of view, the guest network should be considered equivalent to the internet.
The institution may choose to provide wireless or wired guest networks, for example in its meeting rooms and auditoria. Guest users requesting connection must accept the institution's terms and conditions of use. Institutions may choose to stipulate additional requirements, e.g. regarding the type of equipment or software utilised by the user.

5.1.3 Student services

This network segment hosts services that the institution offers to students for use in their studies. Examples of such services include:

- Internal student e-mail services
- file server(s) for home directories and web applications used by students
- print servers.

5.1.4 Labs

This network segment contains laboratory equipment, provided that such equipment does *not* contain personal data or other mission-critical systems or information.

5.1.5 Student client services

This network segment contains clients for users registered as students at the institution. Typically, these clients only have access to the segment that hosts student service systems.

5.2 Internal zone

The Internal zone hosts systems such as the technical services, administrative systems, and the management network, as well as clients who are entitled to access the services located in a Secure zone. If remote access to the Internal zone is permitted, appropriate access control mechanisms must be implemented.

The institution's internal services that do *not* contain sensitive personal data should be placed in this zone. A recommendation for the placement of some relevant services is provided below. The list is not exhaustive.

5.2.1 Basic services

System administrative services such as:

- system services including DHCP, NTP, SIP, and recursive DNS
- user databases, active directory domain controllers (AD)
- student services
- internal e-mail servers
- file servers for home directories used by employees
- the institution's internal websites
- calendar systems
- client administration systems such as SMS, SUS, antivirus, and licences

- print servers.

5.2.2 Technical services

Services such as technical operations that the institution depends on, such as:

- Building management systems (BMS).
- Administration systems for AV equipment
- Video surveillance equipment

5.2.3 Adminstrative services

Remote desktop systems that facilitate access to services in the Secure zone and systems that are used primarily for administrative tasks, including:

- Archiving systems
- Administrative systems
- Administrative servers that are not located in the Secure zone, such as the institution's financial management system. Risk assessments determine whether such servers should be located in the Internal or the Secure zone.

5.2.4 Management network

This segment hosts network and service monitoring servers, as well as network electronics, such as switches and access points.

5.3 Secure zone

All services and systems that contain sensitive personal data, and all mission-critical systems, must be located in the Secure zone.

5.3.1 Sensitive personal data

All services and systems that host sensitive personal data, such as:

- various patient record systems
- administrative systems that contain sensitive personal data
- video surveillance recordings.

5.3.2 Mission-critical systems

All services that are mission-critical or which contain mission-critical data such as:

- locking systems
- access control
- research materials/contract research data
- back-up data
- other information relevant for information security, as determined by risk assessments.

6 Definitions

System owner
The person within in the institution that has overall responsibility for ensuring that the system is used in accordance with prevailing agreements, legislation and regulations. The system owner is responsible for defining and regulating access to data within the system, and for ensuring that the organisation has adequate user support, written procedures, and auditing routines for use of the system.

Personal data
Information and appraisals that can be linked to a named individual.

Sensitive personal data
Information regarding:

- racial or ethnic origin; political opinions, religious or philosophical beliefs.
- criminal record,
- health-related matters,
- sex life or sexual orientation,
- trade union membership.

7 References

(1) The Norwegian Personal Data Act (*personopplysningsloven*). *http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/Engelsk%20lov%20ny%20utg%C3%A5ve%20til%20publisering.pdf*

(2) Regulations governing the processing of personal data *(personopplysningsforskriften)*. http://www.datatilsynet.no/upload/Dokumenter/regelverk/lov_forskrift/Engelsk%20forskrift%20ny%20utg%C3%A5ve%20til%20publisering.pdf

(3) The Norwegian Data Inspectorate: Guidance on information security for municipal and county administrations *(Veiledning i informasjonssikkerhet for kommuner og fylker,* also known as *"Kommuneveilederen"),* in Norwegian. http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/tv202_2005_1.pdf

(4) ISO/IEC 27001:2005 Information security – Security techniques – Information security management systems – Requirements.

(5) ISO/IEC 27002:2005 Information security – Security techniques – Code of practice for information security management.

(6) The Norwegian Data Inspectorate: Guidance in the use of thin clients *(Veileder for bruk av tynne klienter),* in Norwegian. http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Veileder_tynneklienter.pdf