Security

Manuel König | @kingbytewolf | #DVOC2019

Where do you think does Security start?

Security

Where does it start?

Security is a much broader field than just IT-Security!

- Security and Risk Management
- Asset Security
- Security Architecture and Engineering
- Communication and Network Security
- Identity and Access Management (IAM)
- Security Assessment and Testing
- Security Operations
- Software Development Security

Therefore it‘s broadened to **Information Systems** Security

Information Systems

Definition:

Information systems (IS) involve a variety of information technologies (IT) such as computers, software, databases, communication systems, the Internet, mobile devices and much more, to perform specific tasks, interact with and inform various actors in different organizational or social contexts.[1]

In short: In a sociotechnical perspective, information systems are composed by four components: task, people, structure (or roles), and technology.[2]

[1] What is an Information System? - 2015 48th Hawaii International Conference on SystemSciences (Sebastian K Boell, Dubravka Cecez-Kecmanovic)

[2] Information system - https://en.wikipedia.org/wiki/Information_system

Security

Start

CIA-Triad

Confidentiality

The goal is to prevent or minimize unauthorized access to data.

Integrity

Integrity protection prevents unauthorized alterations of data.

Availability

Authorized subjects are granted timely and uninterrupted access to objects.

Subject	Object
User, Device, Service	Device, Service, Data

Asset Security

Ensure appropriate asset retention

Record retention

Keep and maintain information as long as it is needed and destroy it when it is no longer needed.

Laws and regulations must be taken into account. Some laws and regulations dictate the length of time that the organization should retain data.

E.g.

HGB §257 Aufbewahrung von Unterlagen. Aufbewahrungsfristen[1]

1 Handelsgesetzbuch – dejure.org (https://dejure.org/gesetze/HGB/257.html)

Asset Security

Hardware retention

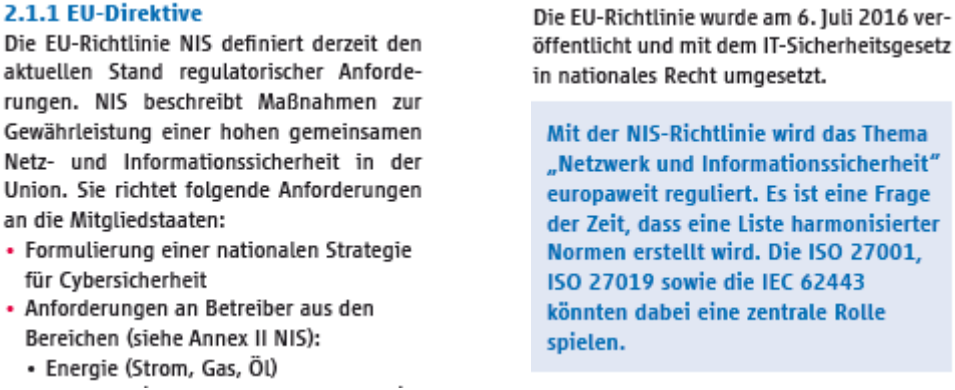
Refers to hardware that has a refresh cycle and/or is replaced regularly, such as computers.

The hardware must be retained until it is properly sanitized!

Security Architecture and Engineering

Depending on the industry different security controls must be applied to the product.

Credit Card Payment → Payment Card Industry Data Security Standard (PCI DSS)
Critical Infrastructure such as Energy → IT-Sicherheitsgesetz (ISO 27001, ISO 27019, IEC 62443)[1]



2.1.1 EU-Direktive

Die EU-Richtlinie NIS definiert derzeit den aktuellen Stand regulatorischer Anforderungen. NIS beschreibt Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union. Sie richtet folgende Anforderungen an die Mitgliedstaaten:

- Formulierung einer nationalen Strategie für Cybersicherheit
- Anforderungen an Betreiber aus den Bereichen (siehe Annex II NIS):
  - Energie (Strom, Gas, Öl)

Die EU-Richtlinie wurde am 6. Juli 2016 veröffentlicht und mit dem IT-Sicherheitsgesetz in nationales Recht umgesetzt.

Mit der NIS-Richtlinie wird das Thema „Netzwerk und Informationssicherheit" europaweit reguliert. Es ist eine Frage der Zeit, dass eine Liste harmonisierter Normen erstellt wird. Die ISO 27001, ISO 27019 sowie die IEC 62443 könnten dabei eine zentrale Rolle spielen.

[1]Orientierungsleitfaden für Hersteller zur IEC 62443 – ZVEI (S. 6) [Link]

Communication and Network Security

- Implement secure design principles in network architectures
- Secure network components
- Implement secure communication channels according to design

Identity and Access Management (IAM)

Manage the identity and access provisioning lifecycle

The provisioning lifecycle is subdivided in three steps.

- Creation
  User account(s) is/are created and the necessary access rights are provided
- Management
  Accounts are periodically reviewed to reduce the risk of “Creeping privileges”
- Deletion
  When employees leave the organization the account must be disabled and when it’s determined that the account is no longer needed, it should be deleted.

Security Assessment and Testing

- Design and validate assessment, test, and audit strategies
- Conduct security control testing
- Collect security process data
- Analyze test output and generate report
- Conduct or facilitate security audits

Security Operations

Implement recovery strategies

To be able to recover from a disaster you need a Disaster Recovery Plan (DRP).

There are two categories of Disasters:

Natural Disasters

- Earthquakes
- Floods
- Storms
- Fires

Man-Made Disasters

- Fires
- Acts of Terrorism
- Explosions
- Power Outages
- …

Software Development Security

- Understand and integrate security in the software development lifecycle (SDLC)
- Identify and apply security controls in development environments
- Assess the effectiveness of security
- Assess security impact of acquired software
- Define and apply secure coding guidelines and standards

Thanks!!

- Questions?