MUNI
FI

Basic Principles of System Hardening

PA211 Advanced Topics of Cyber Security

November 8, 2022

Daniela Belajová, Pavel Čeleda, Jan Vykopal

Agenda

- Response to the Exit Ticket from Last Week
- Introduction to This Part of the Course
- Introduction to System Hardening
- Introducing Our Case Study – Web Application
- Hardening Best Practices
- Hardening Guidelines and Helpers Based on Their Reliability

Exit Tickets From Last Week – I

Do you have any feedback on Homework 2 (report and presentation)?

A: Overall, you were positive and asked for more guidance, such as:

> *I didnt know how to perform the pentesting. It would be better to have a dedicated class for the testing and then perform the hw2.*

Exit Tickets From Last Week – II

Ask one question about today's content.

Q: *How were we supposed to know other webpages than the main one exist ?*

A: If you inspect the SSL certificate, you may notice it was issued to other Cursio websites.

Q: *Should have we approached the environment we tested as an isolated testing environment or*

A: The end of the question is missing.

Anyway, we have to clarify the scope of the test next time.

Exit Tickets From Last Week – III

Do you have any suggestions for how today's class could have been improved?

A: I have liked it. I think we were not aware of the 7 minute time limit for presentations, so please mention it the week before next time.

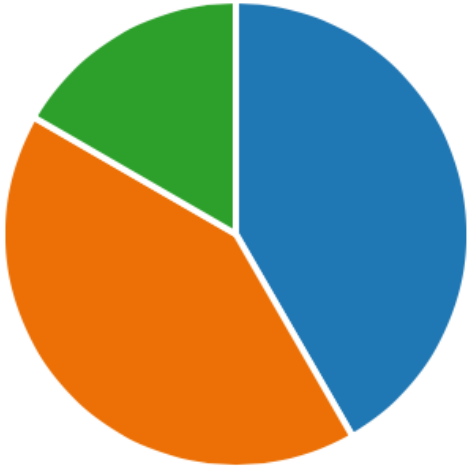
A: Let everybody do presentation. There were few important things we planned to talk about on our presentation, but do not have thenIm specifically written in presentation, so I'm afraid we might loose a point if only the presentation file will be evaluated, because we thought we will be evaluated by what we will say during the presentation.

Thanks for your feedback!

Exit Tickets From Last Week – IV

Which course part do you like more?

Part I - asset, vulnerability, and t...	5
Part II - penetration testing prac...	5
I have no preference	2



MUNI FI

Week	Date	Class Topic
1	13.09.2022	Course organization and motivation
2	20.09.2022	Asset management
3	27.09.2022	Vulnerability management
4	04.10.2022	Threat management
5	11.10.2022	Penetration testing – introduction
6	18.10.2022	Penetration testing – process
7	25.10.2022	Penetration testing – report
8	01.11.2022	Penetration testing – exemplary report and presentations
9	08.11.2022	Introduction to web application hardening (Daniela Belajová)
10	15.11.2022	Access control mechanisms (Peter Velan)
11	22.11.2022	OS-level, virtualization and containerization (Daniela Belajová)
12	29.11.2022	Web server and application hardening (Adam Chovanec)
13	06.12.2022	Course feedback session

Part III – Hardening of OS and Applications

- **Syllabus:** Web application stack hardening
- **Objectives:**
  - Introduce basic principles and best practice of system hardening
  - **Selected case study:** web application service
- **Learning outcomes:**
  - **Hands-on experience** with tools for monitoring, system configuration (e.g., Pakiti, Ansible)
  - Knowledge and practical usage of selected **access control mechanisms**
  - Knowledge of web-based attacks countermeasures, hardening of web app and servers
- **Assessment:** 2 homework(s)

Agenda

- Response to the Exit Ticket from Last Week
- Introduction to This Part of the Course
- Introduction to System Hardening
- Introducing Our Case Study – Web Application
- Hardening Best Practices
- Hardening Guidelines and Helpers Based on Their Reliability

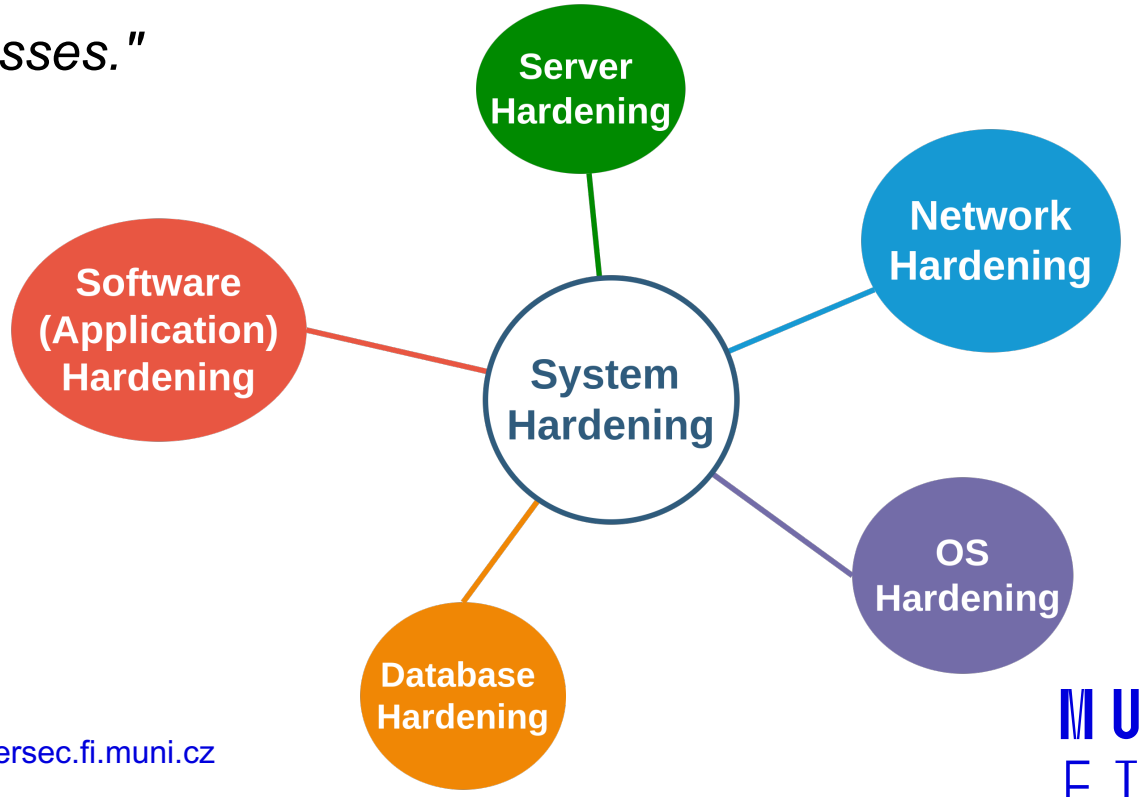
System Hardening

- *"With system hardening, IT administrators **take action to reduce the potential attack surface**, leaving fewer opportunities for hackers to exploit your systems...System hardening means doing everything possible to find and fix security vulnerabilities, whether in hardware, firmware, software, applications, passwords, or processes."*

Intel Corporation

- *"A process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services."*

NIST Special Publication 800-152



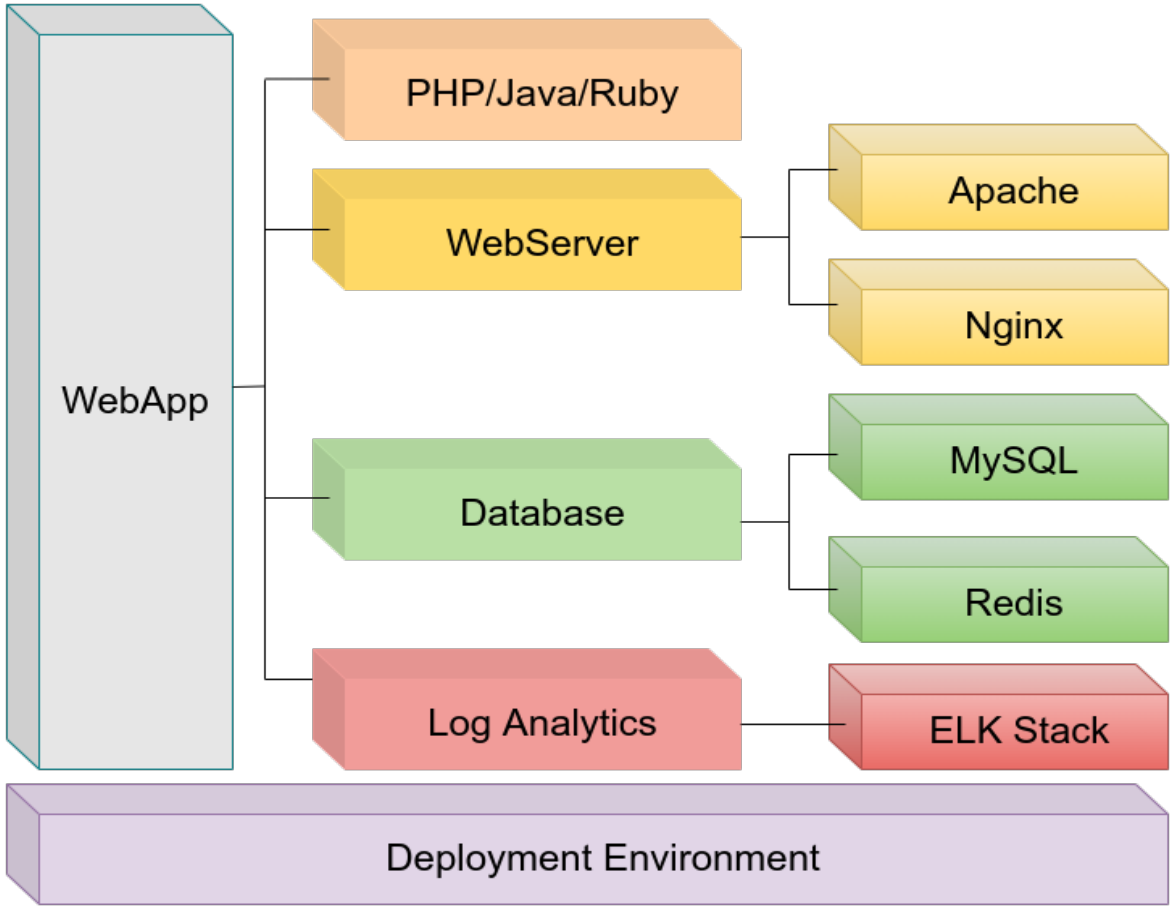
MUNI FI

Case Study for Part III

Web Application Service

Web Application Stack

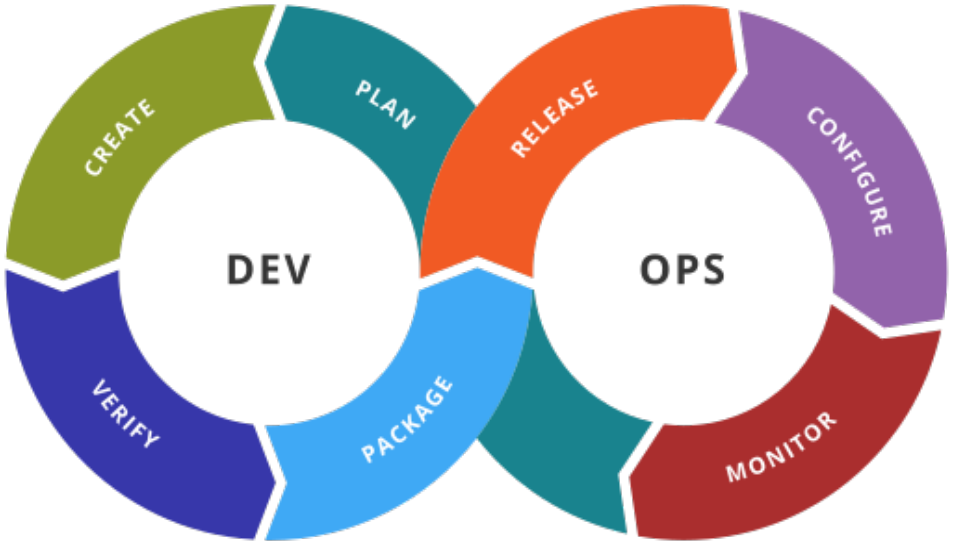
Vertical vs. Horizontal Approach



MUNI FI

Week	Date	Class Topic
1	13.09.2022	Course organization and motivation
2	20.09.2022	Asset management
3	27.09.2022	Vulnerability management
4	04.10.2022	Threat management
5	11.10.2022	Penetration testing – introduction
6	18.10.2022	Penetration testing – process
7	25.10.2022	Penetration testing – report
8	01.11.2022	Penetration testing – exemplary report and presentations
9	08.11.2022	Introduction to web application hardening (Daniela Belajová)
10	15.11.2022	Access control mechanisms (Peter Velan)
11	22.11.2022	OS-level, virtualization and containerization (Daniela Belajová)
12	29.11.2022	Web server and application hardening (Adam Chovanec)
13	06.12.2022	Course feedback session

Your Role: DevSecOps



- More **SecOps** than **Dev**
  - We do **not** focus on *secure coding*[1]**,** *however ...*
  - **Verizon Data Breach Investigation Report, 2021**: *"The majority of successful organizational breaches (90%) and incidents (50%) happen on the web application layer."*
    - 33.3% in SQL Injection Vulnerabilities
    - 30% in Remote Execution Vulnerabilities
    - 57% in XSS Vulnerabilities
- Anyway, don't underestimate the global security and other layers of web application stack!

[1] PV286 Secure coding principles and practices

MUNI FI

Deployment Environment

Two things you must think about

1. Development vs. production environment
   - Nowadays, significantly differ for most of software development
   - Security requirements vary, or rather, are inherently different
     - Developer's local machine vs. production cloud
2. Applications run in various *production environments*
   - Containerized applications, e.g., Kubernetes
   - Running on virtual machines, e.g., cloud platforms
   - Broken into both, containers and VMs

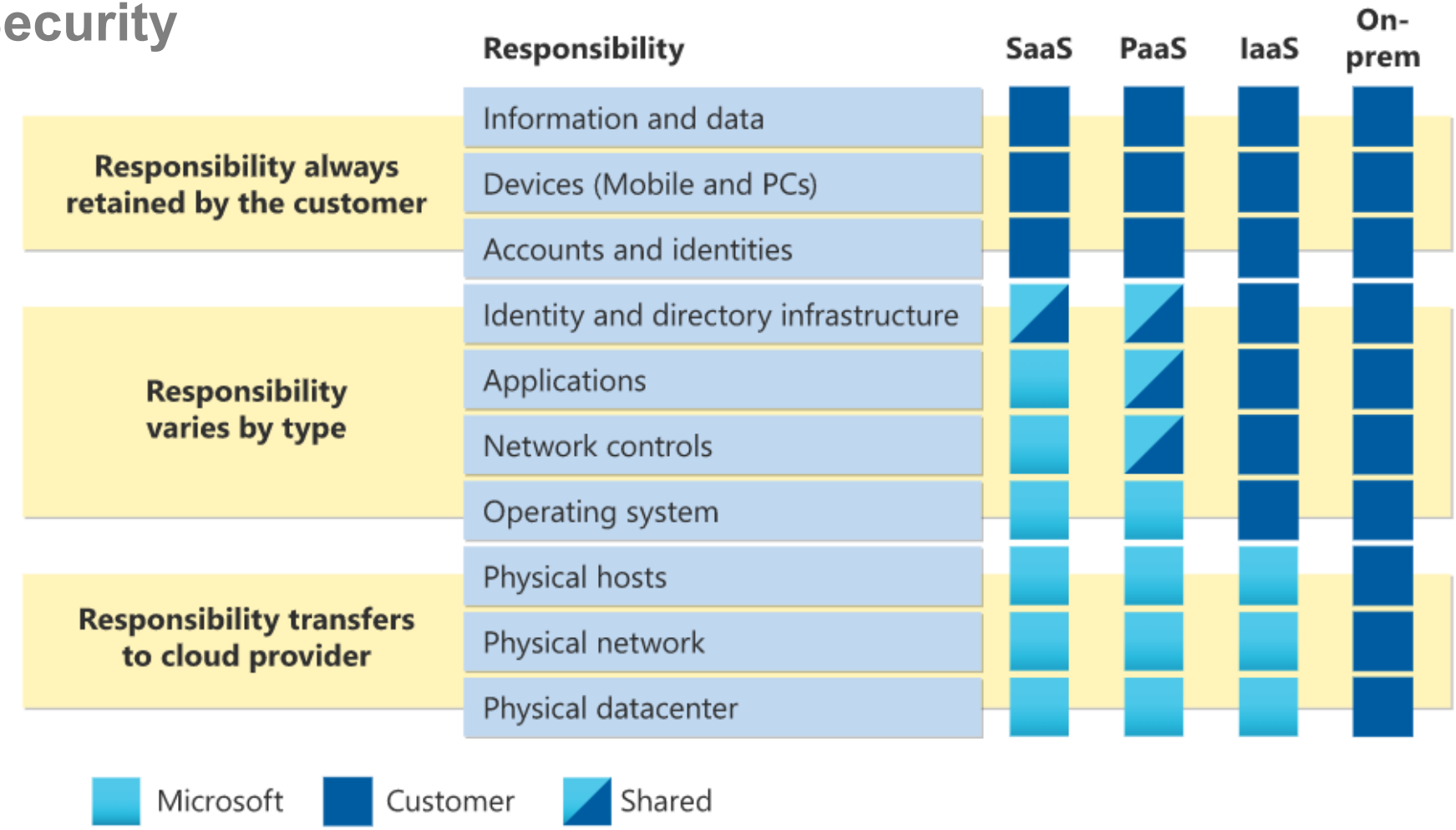
Note: Virtualization is a vast topic, mainly the focus on containerization (Week 11)

Cloud Service Models

1. Software as a Service (SaaS)
   - Applications running in cloud (Dropbox or Microsoft Office 365)
   - Accessible to users via, e.g., internet browsers
   - Software updates, bug fixes, maintenance are taken care of for the user
2. Platform as a Service (PaaS)
   - Hardware, application-software platform provided and managed by cloud provider
   - Users handle apps running on top of the platform and the data the app relies on
   - Microsoft Azure
3. Infrastructure as a Service (IaaS)
   - Provider manages the infrastructure (actual servers, network, virtualization, data storage)
   - User manages things like the operating system, apps, and middleware
   - e.g. virtual machines hosted in the cloud

Shared Responsibility Model

Cloud Security



https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

MUNI FI

Agenda

- Response to the Exit Ticket from Last Week
- Introduction to This Part of the Course
- Introduction to System Hardening
- Introducing Our Case Study – Web Application
- Hardening Best Practices
- Hardening Guidelines and Helpers Based on Their Reliability

Best Practices

"Ten commandments" of (system) hardening

- Recommendations applicable through all layers
- Which ones come to your mind?

"Ten commandments"[1]

1) Maintain Up-To-Date Software and Operating Systems
2) Configure AAA and Access Control Mechanisms (ACM)
3) Apply the Principle of Least Privilege
4) Password Management (i.e., strong, unique, not default)
5) Implement Encryption and Data Backup Policies
6) Enable malware defense – endpoint vs. on perimeter vs. app firewalls, IDS/IPS/ADS
7) Disable Unused Ports/Services/Protocols/Accounts/Applications
8) Enable Log Management
9) Continuous Monitoring and Vulnerability Management
10) Perform Security Audits Regularly

[1] Based sed on intersection of **CIS Controls**, **NIST 800-123**, **NSA Network Infrastructure Security Guide**

"Ten commandments" of (system) hardening

- Recommendations applicable for all layers
- Which ones come to your mind?
- **Ten commandments are simplified view on hardening**
  - In general, you need to follow specific rules for specific components of the system to provide security at sufficient level.

Hardening Guidelines

or where to start?

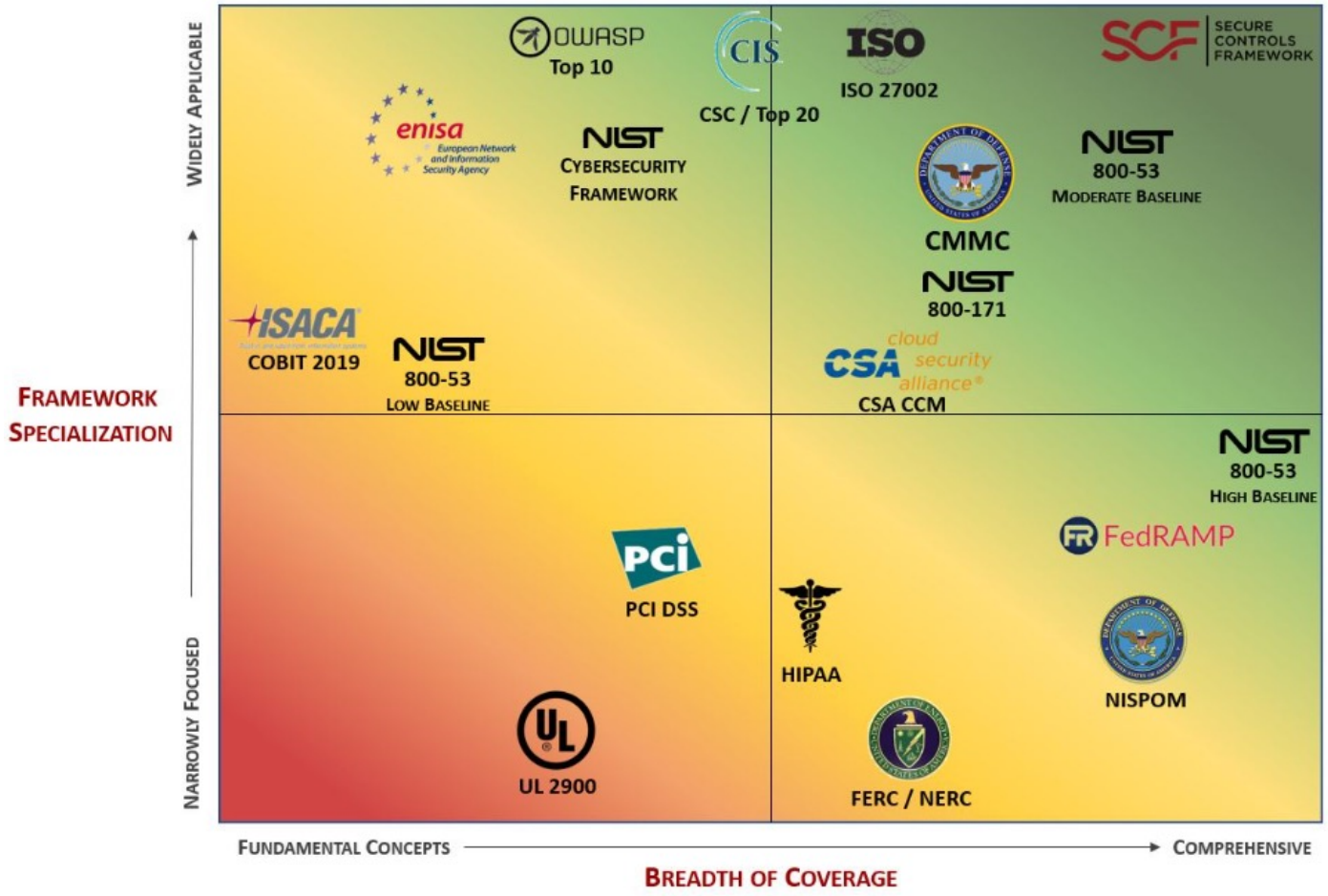
Types of sources

- **Industry Standards and Best Practices**
  - Guides published by CIS, NIST, ISO27k, NSA, NÚKIB, ...
- **Vendors' Guidelines**
  - Popular products have the best practices provided directly by their vendors
  - e.g., Security baselines by Microsoft, AWS Best Practices
- **Best Practices (other approaches, see seminar)**
  - **Proactive (reduces attack surface):** Secure system configuration, ideally automatically, e.g., *security templates*
  - **Reactive (detects threats):** Regular monitoring/scanning of the system to detect vulnerabilities and their *ASAP* fix (based on standards, best practices in organization, your knowledge and skills, etc.)

Standardization Authorities

Survey

Have you ever heard of any of these standards?



MUNI FI

NÚKIB (NCISA)

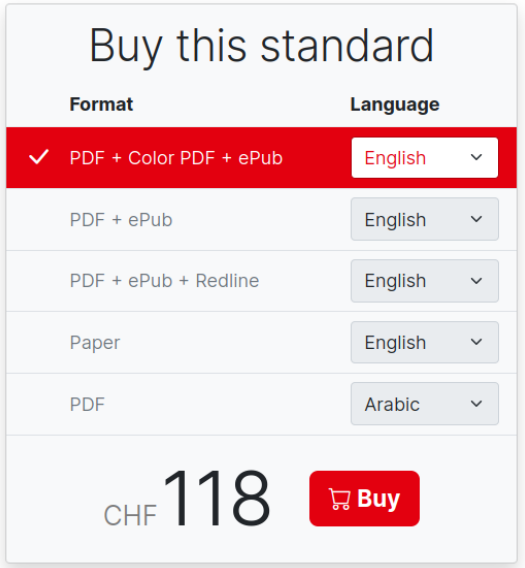
National Cyber and Information Security Agency

- The central administrative body for cyber security in the Czech Rep.
- Besides news/warnings, it publishes:
  - Reports about cyber security incidents
  - Legislation documents
  - Analysis and summary reports
  - **Good Practice Guides**
  - Other supportive materials
- To follow these documents is **compulsory for some subjects**
  - e.g., admins of an *important information system* (MUNI), admins of *critical information infrastructure information system* (hospitals), etc.
  - **Recommended for the rest,** see
    - Act No 181/2014 Coll. on Cyber Security
    - Cybersecurity Decree No 82/2018

MUNI FI

ISO

International Organization for Standardization



- Non-governmental organization
- International standards
  - ISO 27k – set of standards to improve organization's information security systems
  - Besides 27000 (Overview), not free (around 3000 Kč per standard) as involve audits and certification
- Intended for auditors, head of IT departments, security managers, etc.
  - **Internationally recognized** requirements for establishing, implementing, maintaining, and continually improving an **information security management system (ISMS)**

MUNI FI

NIST

National Institute of Standards and Technology

- Develops cybersecurity standards, guidelines, best practices, etc.
- **U.S. private-sector** owners and operators of critical infrastructure **primary**, but have **global impact**

NIST Publications

https://csrc.nist.gov/publications

FIPS	**Federal Information Processing Standards:** Security standards. *Learn more*
SP	**NIST Special Publications** Guidelines, technical specifications, recommendations and reference materials, comprising multiple sub-series: **SP 800** **Computer security** *Learn more* **SP 1800** **Cybersecurity practice guides** *Learn more* **SP 500** **Information technology (relevant documents)**
IR (NISTIR)	**NIST Internal or Interagency Reports** Reports of research findings, including background information for FIPS and SPs.
CSWP	**NIST Cybersecurity White Papers** General white papers, thought pieces, and official cybersecurity- and privacy-related papers not published as a FIPS, SP, or IR.
ITL Bulletin	**NIST Information Technology Laboratory (ITL) Bulletins (1990-2020)** Monthly overviews of NIST's security and privacy publications, programs and projects.

NIST

National Institute of Standards and Technology

- Most popular publications:
  - **NIST SP 800-Series Compliance**
  - **NIST Cybersecurity Framework (CSF)**

NIST CSF vs. NIST SP

- **NIST Cybersecurity Framework (NIST CSF)**
  - Industry standards and best practices to help organizations manage their cybersecurity risks
  - NIST 800-53 and NIST 800-171 provide security controls for implementing NIST CSF
  - Current version from 2014, **version 2.0** should be released at the 2023/2024

- **NIST Special Publications (NIST SP)**
  - NIST has produced more than 200 special publications
  - A deeper dive into specific areas
  - Covering many aspects of cybersecurity risk management: identity access control, managing protective technology, responding to a cybersecurity event or incident, ...

ISO 27001 vs. NIST CSF

- ISO 27001 involves auditors & certifying bodies (not-free), NIST CSF is voluntary (free)
- ISO 27001 – good for maturity organizations
- NIST CSF may be best suited for organizations in the initial stages developing a cybers ecurity risk program
- ISO is less technical
- **Both:** Standards that help businesses, large or small, develop stronger information sec urity system and protect data. **Complementary frameworks:**

"You've completed 50% of the NIST CSF when you've finished your ISO 27001!
What's even better is that if you implemented NIST CSFs,
you're already 80% of the way to achieving ISO 27001."

https://www.trustnetinc.com/nist-vs-iso-27001/

MUNI FI

Task

1. Log in and open your browser with Google.
2. Look for a special publication (SP) from NIST with guidelines to **harden server** (in general).
3. In NIST SP 800-123, look at **Server Security Principles**. Can you recognize some we have already talked about?
4. What does it say about **user authentication**?

CIS

Center for Internet Security

- CIS is a non-profit organization
  - Cyber-security professionals from academia, industry, government, and business
- **CIS Benchmarks**
  - **Guidelines for hardening** specific OS, middleware, applications, and network devices, etc.
  - Regarded as **industry standard** by compliance standards (HIPAA, PCI DSS, NIST)
  - a.k.a. CIS Benchmarks present "how everybody does it"
- **CIS Critical Security Controls (CSC)**
  - a general set of recommended practices for securing a wide range of systems and devices
- Both (Controls and Benchmark) are free to download and use

CIS Security Levels

- CIS Benchmarks include *configuration profiles*:
  - *Profile* describes the configurations assigned to benchmark recommendations
    - **Level 1**
      - Proposes necessary basic security criteria (**intent is to lower attack surface**)
      - Can be implemented by system administrators with any level of technical skills
      - Settings that are not likely to interfere with system or application function
    - **Level 2**
      - **"defense in depth"**
      - security settings are recommended for areas needing increased security
      - may result in some restricted functionality
    - **STIG (replaced Level 3)**
      - Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs)
      - Requirements defined by the U.S. Department of Defense
      - Overlaps recommendations of other profiles

NIST vs. CIS

- Again, **they are complementary**
- Neither NIST CSF or CIS CSC guidelines are mandatory
  - Business can adhere to and reference without any limitations
- CIS CSC standards directly map to other standards
  - PCI DSS, HIPAA, ISO, GDPR,…
  - To follow CIS CSC guidelines, you meet NIST CSF standards
- **CIS Controls are much more specific** than NIST CSF
  - CIS is more prescriptive, whereas NIST CSF provides more security objectives that you can reach at your own

Conclusion

1. There's **no one-size-fits-all set of cybersecurity guidelines** that every company should follow... **but better some than none**.
2. For individual products, primarily **follow recommendations given by their vendors** (if exist).

Bonus: NSA/CSS

National Security Agency/Central Security Service

- A federal government intelligence agency of the U.S. Department of Defense
- **NSA Cybersecurity**
  - prevents and eradicates threats to U.S. national security systems
  - publishes -- with Cybersecurity and Infrastructure Security Agency (CISA) -- various Cybersecurity Technical Report, Cybersecurity Advisories & Guidance, etc.
    - Network Infrastructure Security Guide
    - Kubernetes Hardening Guidance
    - Hardening SIEM Solutions
    - Security Guidance for 5G Cloud Infrastructures

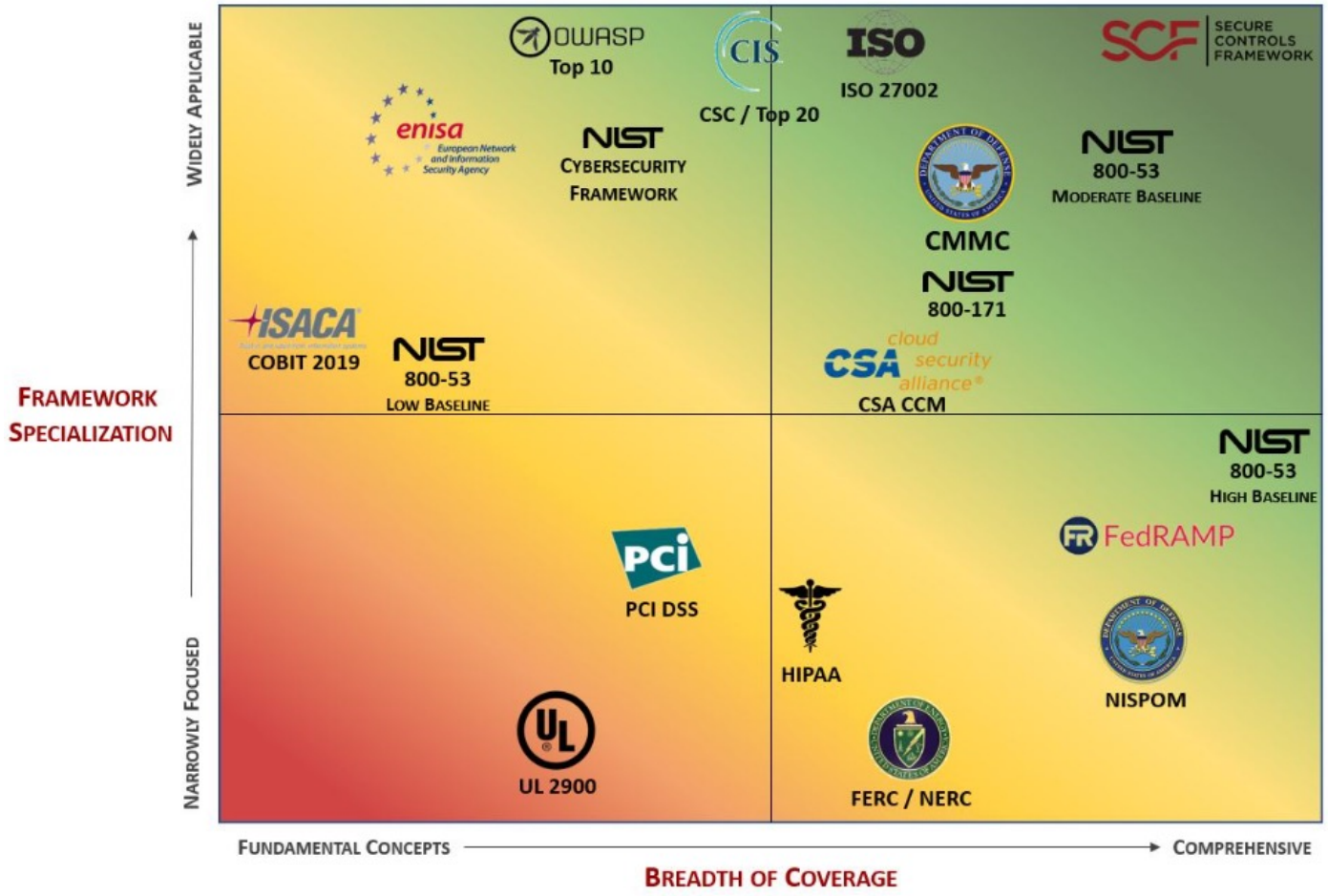
- It's not relevant to us, but can be an interesting security perspective

Bonus: Maybe you have heard about...

- PCI SSC (PCI Security Standards Council)
  - global forum that brings together payments industry stakeholders to develop and drive adoption of data security standards and resources for safe payments worldwide
  - **PCI DSS (Payment Card Industry Data Security Standard) -** rules to control "world of credit cards"
- HIPAA (The Health Insurance Portability and Accountability Act of 1996)
  - Federal law to protect sensitive patient health information
  - HIPAA Privacy Rule implements HIPAA, issued by the US Department of Health and Human Services
- **SOC2**
  - An auditing procedure that ensures service providers securely manage data to protect the interests of the organization and the privacy of its clients
  - Developed by the American Institute of CPAs (AICPA)

Summary

– Comparing NIST CSF vs. ISO 27001/27002 vs NIST 800-53



MUNI FI

Supplementary materials

- Act No 181/2014 Coll. on Cyber Security vs. ISO 27001 (in Czech)
  - The ISO/IEC 27k series is basis for the Cybersecurity Act/Decree
  - If you must follow the Cybersecurity Act (or Decree) **compliance with ISO or certification does not exempt** entities from the obligation

MUNI

FI