

# IT Security

## Information & Network Security

by Bjoern Kimminich

# Bjoern Kimminich

- [Nordakademie](#) Graduate (199a)
- Product Group Lead Architecture Governance + Application Security at [Kuehne + Nagel](#)
- Lecturer at [Nordakademie](#) since 2009
- Volunteer in the [Open Web Application Security Project](#)
- Board Member of the [German OWASP Chapter](#)
- Project Lead of the [OWASP Juice Shop](#)



# Contact Information

## Email

- [bjoern.kimminich@nordakademie.de](mailto:bjoern.kimminich@nordakademie.de)
  - PGP: 062A 85A8 CBFB DCDA

## Miscellaneous

- <https://keybase.io/bkimminich>
- <https://twitter.com/bkimminich>

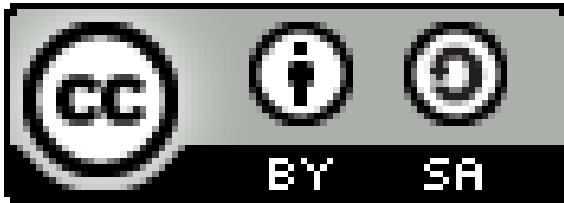
## Exercise 0.1 ()

1. Write the industry you work in on a post-it and place it on the board. Cluster identical industries.
2. In the following table self-assess your own **IT security awareness** by ticking one of the columns

 Gold	 Silver	 Bronze	 Wood

# Course Material

<https://github.com/bkimminich/it-security-lecture>



# Course Material

- All slides and references are in  language
- The lecture can be held in  or  language
- Latest course material is available only on GitHub
- Content exists as `Markdown` files for use with [Marp](#)
- Slides can be [downloaded as PDF](#) from GitHub
- All slides are published as [OER](#) under [CC BY-SA 4.0](#) license

*You can help save a  by not  all slides for the entire course in advance as content might change during the course!*

# Rules

- Presence at lectures is mandatory and will be logged
- Exercises are mandatory (unless explicitly marked as *optional*)
- Exercises marked with
  - "👉" are done in small work groups
  - "📌" are usually done as a group using whiteboard, flipcharts or brown-paper or a dedicated [Spitfire](#) virtual whiteboard
  - "📝" have a (digitally) written outcome per student or work group
  - "🏠" are homework and must be completed until the next lecture
- Active participation and questions are encouraged at all times
- If you are done early with the last exercise of the day, you may leave

# Curriculum 1st Semester



1. Motivation
2. Security Goals
3. Malware
4. Network Security
5. Encryption
6. Security Management & Organization
7. Threat Modeling
8. Penetration Testing




# Curriculum 2nd Semester

1. Open Web Application Security Project (OWASP)
2. XSS
3. Injection
4. Authentication Flaws
5. Authorization Flaws
6. Sensitive Data
7. Insecure Dependencies & Configuration
8. XXE & Deserialization
9. Secure Development Lifecycle

# Schedule

- Tuesdays, 9:15 - 11:45
- 10 lectures (13.10. - 15.12.20)
-  Tue, 13.10. has been moved to  Wed, 21.10. (13:15 - 15:45)

## Test Exam

- At the end of 2nd semester (90min)
-  Covers topics from both semesters

# Recommended Resources

- [Berkley Information Security and Policy - Best Practices & How-To Articles](#)

## Optional Literature Recommendations

- Andress: The Basics of Information Security (2nd Edition), 2014
- Shostack: Threat Modeling: Designing for Security, 2014
- Paar/Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners, 2010
  - [Introduction to Cryptography by Christof Paar](#) (24 recorded lectures)

## Prerequisites @ Angewandte Informatik (B.Sc.)

Information & Network Security	S5	Application Security & SDLC	S6
Diskrete Mathematik 2	S2	Datenbanksysteme	S2+3
Technische Grundlagen der Informatik 2	S3+4	Praxis der Softwareentwicklung	S3+4
Gestaltung von Informationssystemen	S3+4	Softwarequalitaet	S4
IT-Organisation und Projektmanagement	S3+4	Software Engineering	S5+6
Informatik und Gesellschaft	S1	Internet Anwendungsarchitekturen	S5+6