CyberSecurity

Securing Critical Business

Create IT- / OT-Security Awareness

… with the help of Gamification

Halle 6
Stand D04

Dr. Andreas Rieb

Cyber Security Specialist

AIRBUS

Dr. Andreas Rieb

Experience:

- 10 years experience in IT-Security Awareness
- PhD in IT-Security Awareness for IT-Security Professionals

Hobbies:

- Playing board games
- Photography

Create a new character:

- https://airbus-cyber-security.com/careers/

Trust us – we know IT and OT

Agenda

1 **Motivation and State of the Art**

2 **Gamified Approaches at Airbus**

Cyber Incident Game, Cyber Defence Game, CyberRange Trainings, Cyber Security Exercises

3 **Conclusion**

AIRBUS

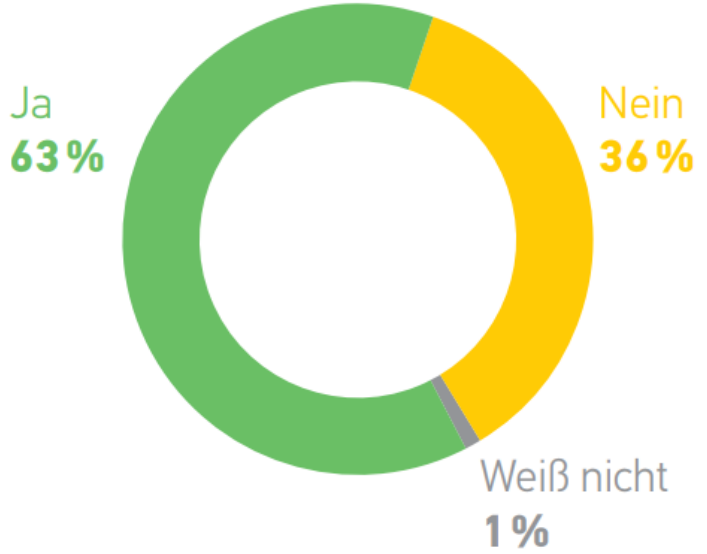
Motivation and State of the Art

CyberSecurity

Aktuelle Situation

- Zunahme an Cyberattacken im Bereich ICS / OT BSI (2019)
- Cyberattacken kombinieren häufig technische und menschliche Schwachstellen BSI (2019)
- IT- / OT-Security Awareness sind ausbaufähig

Werden in Ihrer Organisation regelmäßige Awareness-Schulungen für Ihre Mitarbeiter durchgeführt?



VeSiKi (2017)

Definition, Goals and Methods

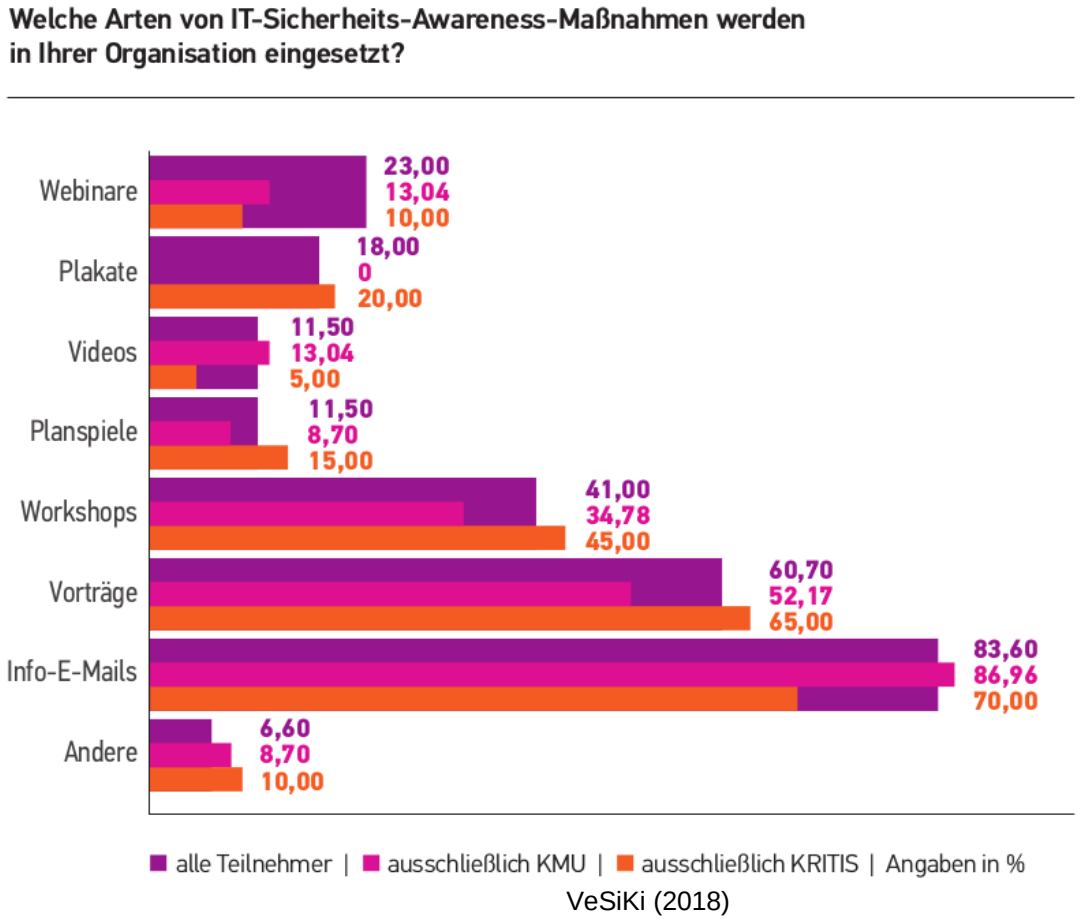
IT-Security Awareness:

“what does a person know (knowledge); how do they feel about the topic (attitude); and what do they do (behaviour)” Kruger / Kearney (2006)

Goals are improvements in the dimensions:

- Perception / to recognise threats
- Protection / to know solutions
- Behaviour / to act right

Hansch / Benenson (2014)



VeSiKi (2018)

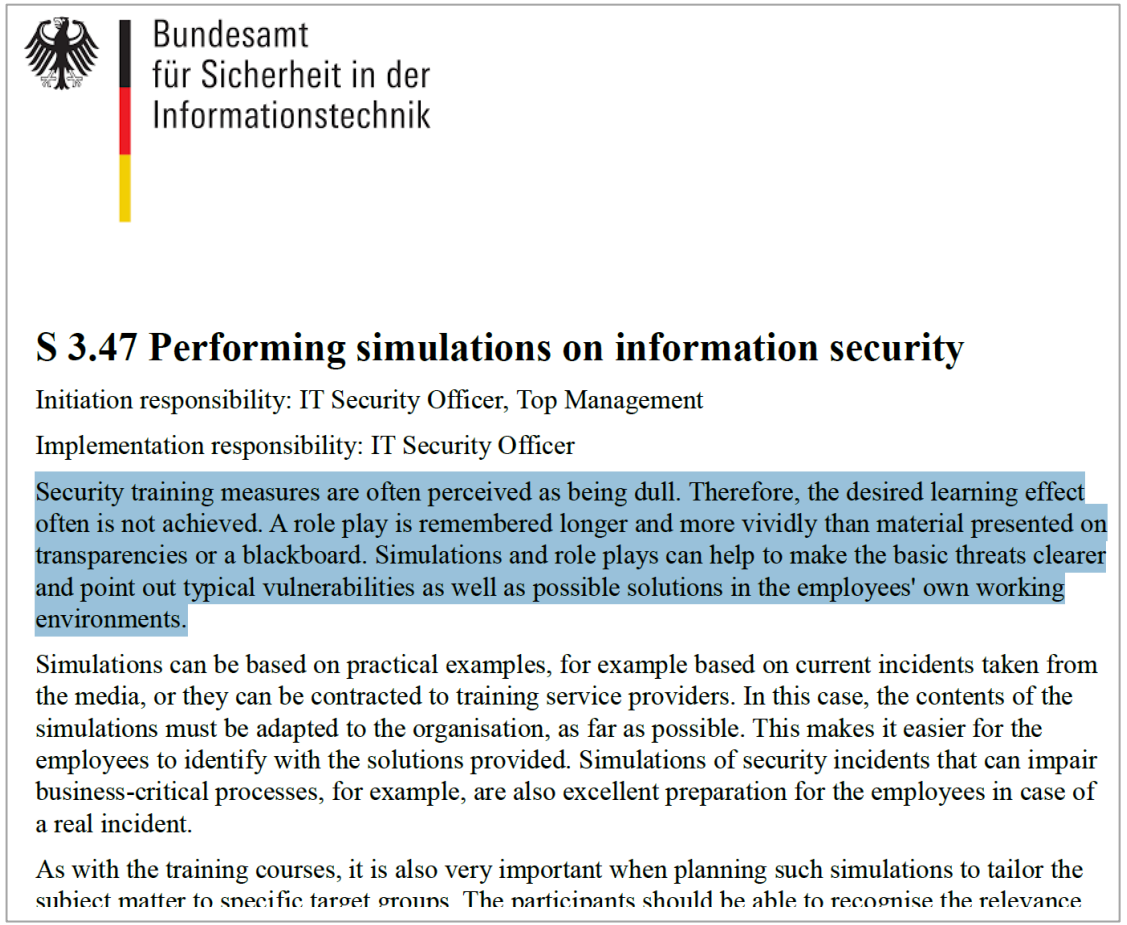
Gamified Approach

Confirmation in practice regarding conventional methods:

- Passive participation
- Less fun
- More single attack vectors than attack campaigns

Scientifically proven

(z.B. Rieb (2018), Nagarajan et al. (2012), Adams / Makramalla (2015))



Bundesamt
für Sicherheit in der
Informationstechnik

S 3.47 Performing simulations on information security

Initiation responsibility: IT Security Officer, Top Management

Implementation responsibility: IT Security Officer

Security training measures are often perceived as being dull. Therefore, the desired learning effect often is not achieved. A role play is remembered longer and more vividly than material presented on transparencies or a blackboard. Simulations and role plays can help to make the basic threats clearer and point out typical vulnerabilities as well as possible solutions in the employees' own working environments.

Simulations can be based on practical examples, for example based on current incidents taken from the media, or they can be contracted to training service providers. In this case, the contents of the simulations must be adapted to the organisation, as far as possible. This makes it easier for the employees to identify with the solutions provided. Simulations of security incidents that can impair business-critical processes, for example, are also excellent preparation for the employees in case of a real incident.

As with the training courses, it is also very important when planning such simulations to tailor the subject matter to specific target groups. The participants should be able to recognise the relevance

BSI (2016)

Serious Gaming and Gamification

Confirmation in practice regarding conventional methods:

Serious Gaming is an umbrella term for games that doesn´t solely focus on fun and entertainment.

e.g. Role Play, Red Teaming, Wargame, Business Wargame, Simulation Exercises, …

Blötz (2015)

Gamification is the use of

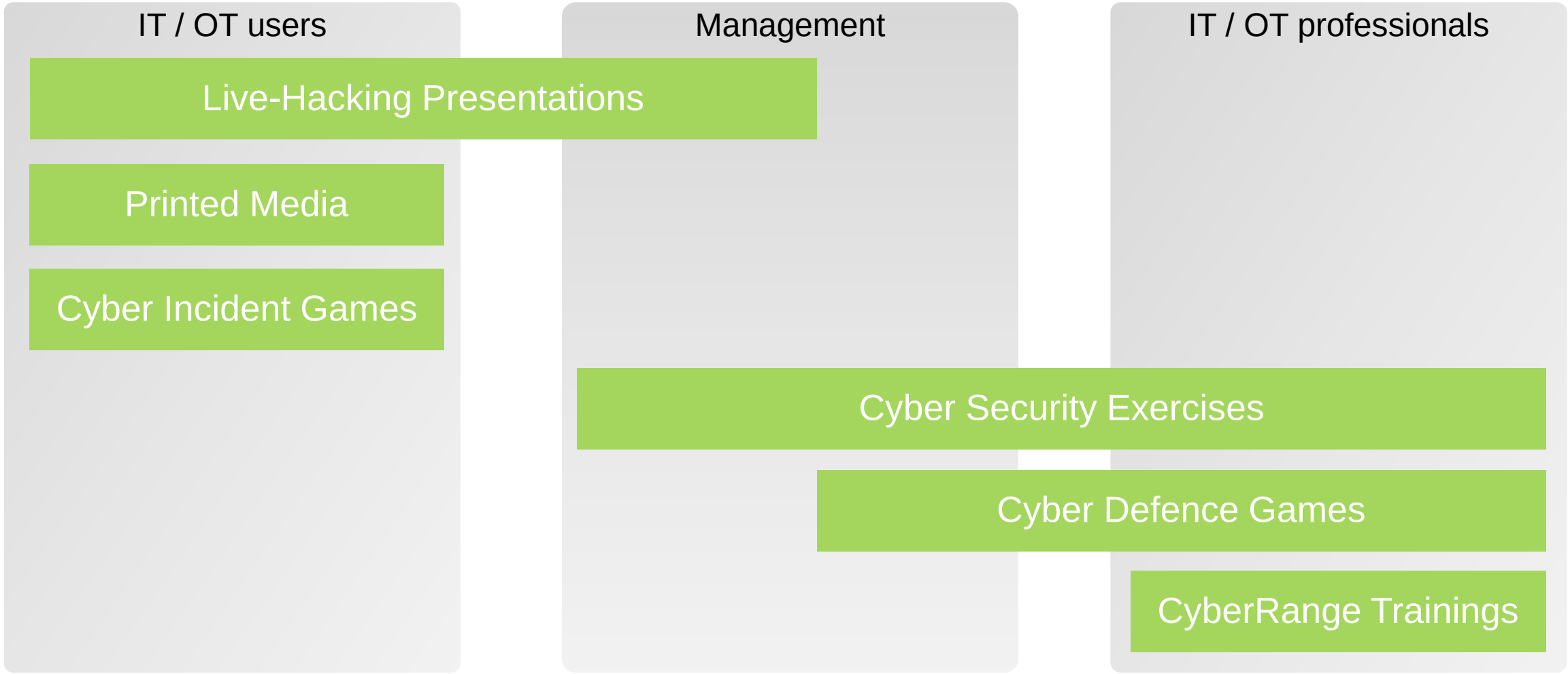
- design elements characteristic for games
- game thinking

in non-game situations

e.g. progress mechanics (such as points systems), player control (such as avatar use), rewards, collaborative problem solving, stories, and competition

Mackenzie / Maged (2015), McConigal (2011)

Airbus CyberSecurity Methods



Gamified Approaches
at Airbus

Cyber Incident Games

CyberSecurity

Cyber Incident Game

Story:

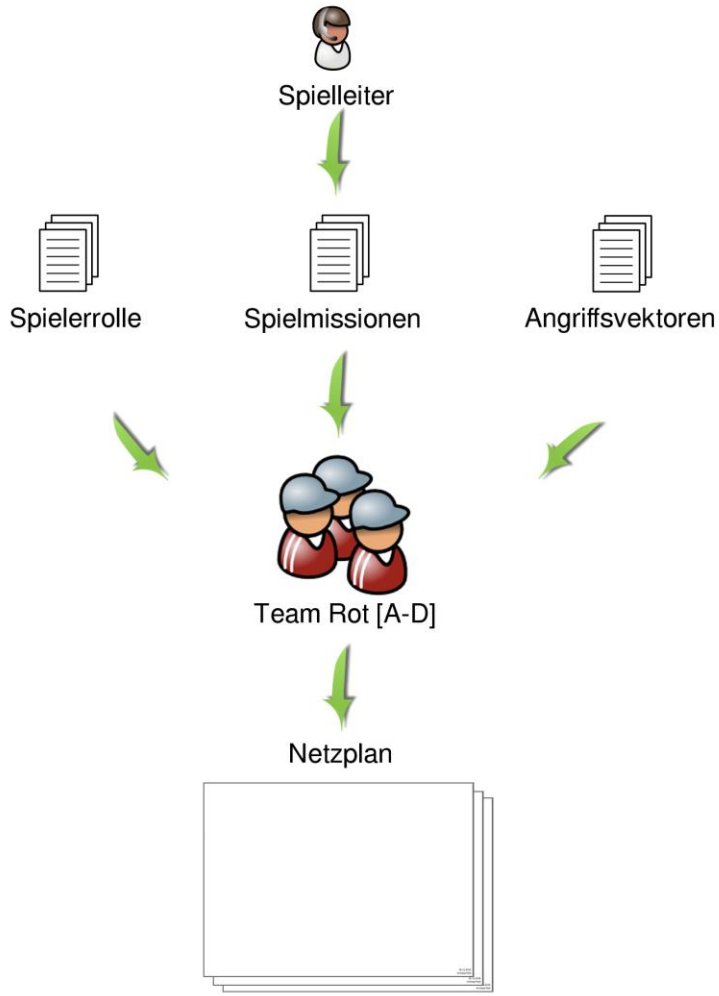
Eine Organisation (z.B. aus der Fertigungsindustrie) wird von 4 Teams angegriffen. Die Teams müssen unterschiedliche Missionen erfüllen und haben dafür unterschiedliche Angriffsvektoren zur Verfügung.

Das Team, das den hinterlistigsten Cyberangriff entwickelt, gewinnt.

Zielgruppe:

IT- / OT- Anwender aus

- HR
- Accounting
- Production
- Engineering
- …

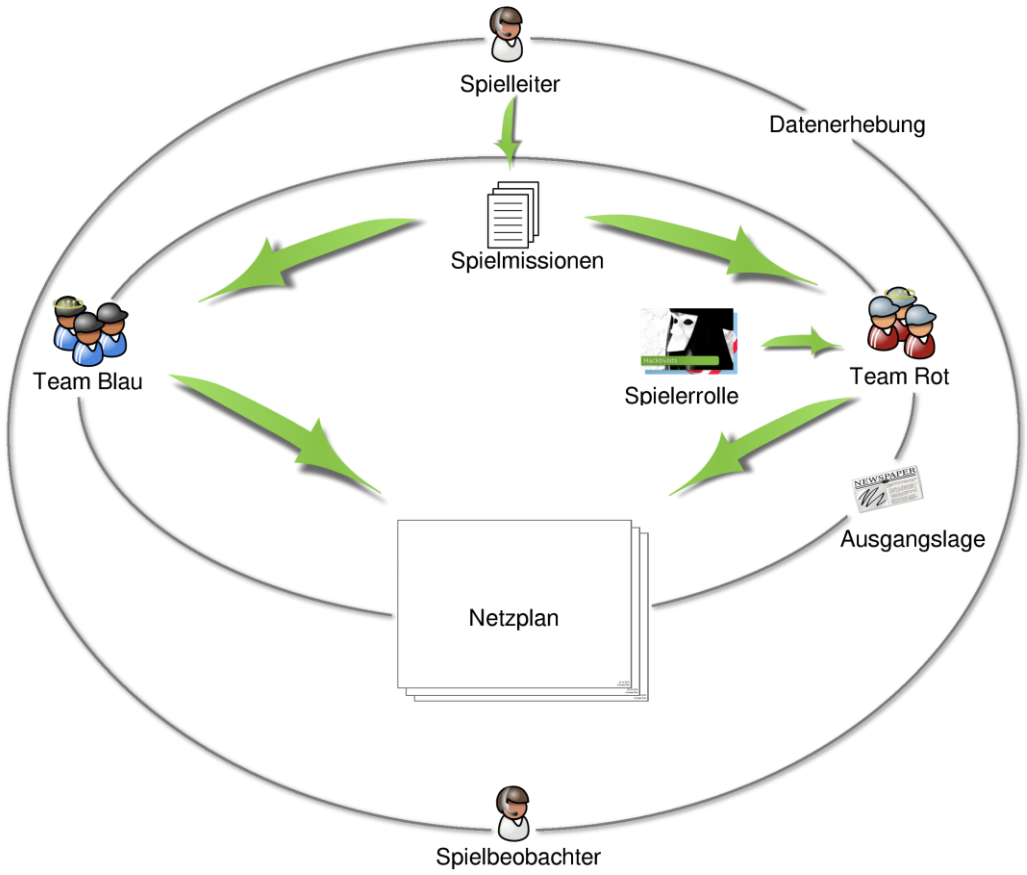


Gamified Approaches at Airbus

Cyber Defence Game

CyberSecurity

Cyber Defence Game



Target group:

IT professionals on a strategic, conceptual, and operative level; e.g.

- IT-Security Management
- Chief Risk Officers
- Business Continuity Management
- IT-Administrators
- SCADA-Operators

AIRBUS

CyberRange Trainings

CyberSecurity

CyberRange Trainings

CyberRange:

Simulation center to train your cyber team on critical incident response, risk analysis, forensic analysis, and other cyber topics.

Trainings:

- Ethical Hacking (Basic | Advanced)
- Advanced Persistent Threats and Targeted Attacks
- Capture the Flag
- ICS / OT Ethical Hacking (Basic | Advanced)

Topics covered:

- ICS / OT particularities / vulnerabilities / threats
- Cyber attacks (e.g. Asset discovery, MODBUS TCP Injection)
- ICS / OT-Security countermeasures (organizational, technical)

AIRBUS

Cyber Security Exercises

CyberSecurity

Cyber Security Exercises

> A plan that has not been tested is like improvising in emergency situations.

Benefits:

- Test and optimization of existing plans and processes
- Improvement of skillsets within incident handling (e.g. assessment of the situation, communication)
- Experienced emergency handling

AIRBUS

Conclusion

CyberSecurity

Conclusion

Gamified methods have a high rate of acceptance.

Gamified methods are powerful for raising IT-Security Awareness.

Gamified methods depend on participants´ motivation and social competency.


Wollen Sie mehr erfahren?
Halle 6, Stand D04
CyberSecurity
Securing Critical Business
AIRBUS

Bibliography

- Adams, M., & Makramalla, M. (2015); Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review, 5(January), 5–14.
- Blötz, U. (2015). *Planspiele und Serious Games in der beruflichen Bildung: Auswahl, Konzepte, Lernarrangements, Erfahrungen - Aktueller Katalog für Planspiele und Serious Games (Berichte zur beruflichen Bildung)* (5. Auflage). Bielefeld: W. Bertelsmann Verlag GmbH & Co. KG.
- BSI; 2016. IT-Grundschutz-Kataloge - 15. Ergänzungslieferung
- BSI; 2016: Industrial Control System Security - Top 10 Threats and Countermeasures 2016
- BSI; 2019: Industrial Control System Security - Top 10 Bedrohungen und Gegenmaßnahmen 2019
- Hansch, N., & Benenson, Z. (2014). Specifying IT security awareness. In *Proceedings - International Workshop on Database and Expert Systems Applications, DEXA* (pp. 326–330). München. https://doi.org/10.1109/DEXA.2014.71
- Kaspersky Labs; 2019: http://apt-securelist.com
- Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008
- McConigal, J. (2012). *Besser als die Wirklichkeit!: Warum wir von Computerspielen profitieren und wie sie die Welt verändern*. München: Heyne Verlag.
- Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). Exploring game design for cybersecurity training. *Proceedings - 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems, CYBER 2012*, 256–262. https://doi.org/10.1109/CYBER.2012.6392562
- VeSiKi; 2017: Monitor IT-Sicherheit Kritischer Infrastrukturen
- VeSiKi; 2018: Monitor 2.0 IT-Sicherheit Kritischer Infrastrukturen