Practical Security Awareness

Lessons Learnt and Best Practices

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

DeepSec 2019



About me



The Obstacles of a Training

- Motivation of your Workforce
- Instructional Design of a Security Awareness Campaign
- Dealing with Complexity
- Transferring the Training Outcomes to the Job



Motivation

Two Factor Theory by Herzberg

- satisfaction and discontent are *independent* dimensions
- discontent is raised by extrinsic factors
  status, fear of losing your job, relations between coworkers and superior
- satisfaction is raised by intrinsic factors
  sense of achievement, recognition, taking over responsibility
- you actually can only demotivate people



- Intrinsic motivation: behaviour that is driven by internal rewards
- Extrinsic motivation: behaviour to earn external rewards or avoid punishment



Motivation

- good communication means to motivate the other party
- motivation means the other party shows a behaviour I want them to show
- motivation means to drop an old behavioural pattern in favour of a new pattern
- motivation means to address an unfulfilled need and showing how to fulfill it
- the better someone can picture the fulfillment of the need, the better motivated they will get



Motivation

Don’t sell the steak – sell the sizzle



- Only current behaviour can be influenced at once!
- Every recurring behaviour has been trained through learning processes.
- Changing recurring behaviour requires new learning processes.
- Every learning process takes it's time.



Didactics / Instructional Design

- teaching methods
- theory and practice of teaching and learning
- the science that turns you into a teacher
- general didactics: general teaching methods, how learning and teaching works, how to structure teaching
- specific didactics: with regards to a specific learning field, eg. subjects in school
- learning outcomes might get obsolete
- teaching a click path isn't viable



- find roles: who does what and how
- professional fields of activity (according to a profession)
- learning situation and professional action



Complexity

- psychological regulation of work $\rightsquigarrow$ IO Psychology
- theory of action
- decomposition of a complex action into less complex actions
- taking away the act of making a decision by establishing rules
  eg password rules



Learning Transfer

- the workforce learnt something
- but doesn't transfer it on the job
- for several reasons
- this is a huge problem in trainings



- Identification of training needs and interests of the workforce
- Identification of roles the relevant learning outcomes
- Determination of learning contents and learning places
- instructional design and teaching methods
- Cost Control
- Success Control and Evaluation



Learning Transfer

- on the job
  - wrong selection of participants
  - learning outcomes are undefined or not clear enough
  - learning contents don't fit to the job
  - training is not accepted and carried by management and employees
  - no time for the training and transfer of the training outcomes
- by the learners
  - lack of insight into the applicability of the learning contents on the job
  - lack of practise of the new behaviour
  - lack of motivation on the job



Evaluation

1. the methodologically sound measurement
2. the science-based benchmarking of processes and outcomes
3. to better understand and design practical training measures through the evaluation of effectiveness, controlling and reflection

To achieve this, we have to methodise and document *processes* and `outcomes`



- the success of a completed training
- gather information for the instructional design of future trainings
- help reflect on a training
- to estimate and justify the costs of a training
  especially the costs of not doing the training
- management loves business indicators
- CFO: What happens if we spend money training our people and then they leave?
  CEO: What happens if we don't and they stay?



Storytelling



WHY?

- Motivation
- Show how easy it has become to start generic attacks with Kali, Metasploit etc.
- Show the consequences of a successfull hack
- Show that unfocused mass attacks happen all the time
- Storytelling



Storytelling

- lively storytelling motivates better than a dry list of facts
- has been used for centuries in all cultures of the world
- very good for the transportation of complex knowledge
- generates memories and supports learning mechanisms
- embed a Live-Hacking into a fitting story



- Hacker is a 15 year old pupil
- How long does he take to learn how to hack a Windows PC? (Youtube, 1h)
- What does he have to know and be able to do? (Almost nothing)
- Which Software does he need? (Kali, Metasploit)
- Where does he find those hacker tools? (Google)
- Examples: MafiaBoy/Stacheldraht, Operation PayBack
- the bottom line: Effort and Complexity



Sonstiges

- https://sicherheitstacho.eu Eye Candy
- https://cybermap.kaspersky.com/de
- https://threatmap.checkpoint.com/ThreatPortal/livemap.html
- Honeypots (SLAC2018)
- https://www.shodan.io/search?query=webcam



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- LinkedIn: Stefan Schumacher