How IT Security Awareness Should be Tested

Arnold Sykosch: sykosch@cs.uni-bonn.de
Matthias Wübbeling: wueb@cs.uni-bonn.de

Friedrich-Wilhelms-Universität Bonn: Working Group IT Security
Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE: Cyber Security Department
The Idea
IT Security Awareness
Quantification
The Idea

- There are a lot of training efforts. Goals include, but are not limited to:
  - Increase of incident reports by users.
  - Decrease of incidents.
  - *Change human behavior*.
  - ...

- Evaluation is recommended ...
  - ... but instructions are (usually) missing.
THE IDEA

ITS.APT: IT SECURITY AWARENESS PENETRATION TESTING

ITS.APT: THE PROJECT

- 6 Partners:
  - Security Researchers
  - Security service provider
  - Privacy officer
  - Psychologists
  - Lawyers
  - Operator of a critical infrastructure

- Start: 1. January 2015
- End: 31. December 2017
- https://itsec.cs.uni-bonn.de/itsapt
ITS.APT: The Project

Project Goals:
- A tool to measure IT security awareness (tech)
- Recommendation for action (law)
- Privacy concept (privacy officers)
- Concept to derive awareness from behavior (psychology)
- Training concept (security service)
- Evaluation (operator)
“information security awareness [is] used to refer to a state where users in an organization are aware of [...] their security mission (often expressed in end-user security guidelines).”¹

“Awareness is the degree or extent to which every member of staff understands: the importance of information security, the levels of information security appropriate to the organisation, their individual security responsibilities and acts accordingly.”²

“Awareness is not training.”³

¹Siponen, M. T.: A Conceptual Foundation for Organizational Information Security Awareness.
²Stevens, T.; Creasey, J.; Kwok, A.; Maule, J.: Effective Security Awareness
³NIST 800-50: Building an Information Technology Security Awareness and Training Program
“Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future.”

---

SITUATION AWARENESS

IT security awareness is situation awareness (acc. Endsley) limited to elements directly or indirectly related to IT security.
**IT security awareness is**
*situation awareness (acc. Endsley)*
*limited to elements directly or indirectly related to IT security.*

- **Level 1:** The first step in achieving SA is to perceive the status, attributes, and dynamics of relevant elements in the environment.

- **Level 2:** Based on the knowledge of Level 1 elements, particularly when put together to form patterns with other elements (gestalt), the decision maker forms a holistic picture of the environment, comprehending the significance of objects and events.

- **Level 3:** The ability to project the future actions of the elements in the environment [... ] is achieved through knowledge of the status and dynamics of the elements and comprehension of the situation [... ].
IT Security Related Elements

- Natural Elements
  - Your password.
  - The monthly password change notification.
  - Legitimate emails.
  - The “green lock” (valid certificate).
  - Files (trustworthiness)
    - Known file ending
    - Known source

- Everything that is aligned to given protection objectives.
Natural Elements
- Your password.
- The monthly password change notification.
- Legitimate emails.
- The “green lock” (valid certificate).
- Files (trustworthiness)
  - Known file ending
  - Known source

Artifacts
- The password request form that can’t be made to belong a specific authentication request.
- The phishing mail (body, sender, link, attachment, ...)
- Residual SQL syntax elements.
- Constant resource utilization (fan noise / LED blink)

Everything that is aligned to given protection objectives.

Everything that is brought to the situation artificially.
ARTIFACTS ORIGINATE FROM ATTACKS

- Footprinting
- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Command and Control (C2)
- Installation
- Actions on Objectives
- Lateral Movement

Potential Damage

Optional
Non-Optional
ARTIFACTS ORIGINATE FROM ATTACKS

Optional

Non-Optional

Optional

Footprinting

Reconnaissance

Weaponization

Delivery

Exploitation

Command and Control (C2)

Installation

Actions on Objectives

Lateral Movement

Potential Damage

MEASURING SITUATION AWARENESS

- Direct measurement:
  - Allows direct assessment of the item of interest.
  - Allows retrieval of SA about specific elements.

- Indirect measurement:
  - Does not measure the item of interest, but an effect that is assumed to be correlated.
  - May introduce bias and inaccuracies.

SA Assessment Methods

  Direct

  Indirect
During a simulation (e.g. flight simulation)...

- ... the simulation in paused and the test operator asks questions about elements within the situation (outline).
- ... the test operator pretends to be ground control and requests specific information of the individual (inline).

Requirements:
- High interaction
- Control over the environment
Indirect Self Assessment

- After a situation the individual is interviewed / fills out a questionnaire
  - Questions about elements are criticized to test memory function rather then awareness.
  - Questions about the individuals own assessment of his/hers situation awareness rather test confidence then SA itself.

- Requirements:
  - High interaction
  - No control over the environment
The hypothesis is, that better SA leads to better performance. Performance indicators are taken as measurement.

- Performance indicators and results of direct SA assessment do not correlate.
- There is too much bias.
- Unknown effects for sub-situations.

Requirements:
- High interaction
- No control over the environment
PASSIVE RESPONSE MEASUREMENT

- The Individual shows psychophysical reaction to element exposure
  - This may include eye movement, brain activity, stress level reactions, ...
  - This shows whether or not an individual understands its situation (lvl1, lvl2)

- Requirements:
  - No interaction with the individual.
  - Limited control to the environment (monitoring).
  - Costly sensor equipment.
Active Response Measurement

- Experts anticipate and rate possible responses to an element
  - Which response shows *good* and *bad* SA.
  - Individuals actions are then rated against expert opinion.
  - Biased. *This is where further research has to be done.*

- Requirements:
  - No interaction with the individual.
  - Limited control to the environment (monitoring).
  - No costly equipment.
HOW IT SECURITY AWARENESS SHOULD BE TESTED

- Use the method that is applicable for your setting:
  - Direct measurement method:
    - This can not be done during daily business.
  - Active response measurement:
    - Too much bias to be fully expressive.

- Recommendation (for now):
  - Rate a test by level (1, 2, 3).
    - Level 1: Is the element recognized?
    - Level 2: Can the individual distinguish between natural element and artifact?
    - Level 3: Can the individual anticipate possible consequences of his/her actions?
  - Take bias into account.
THANK YOU FOR YOUR KIND ATTENTION

its.apt@uni-bonn.de