Psychology of Security

Security as human behaviour and experience

Stefan Schumacher
www.sicherheitsforschung-magdeburg.de

Troopers14
Heidelberg, 2014-03-20

About me

- President of the Magdeburg Institute for Security Research
- Editor of the Magdeburg Journal of Security Research
- Freelance Security Consultant
- Hacker for 20 years, ex-NetBSD developer
- Educational Science and Psychology, Research on Social Engineering
- Focus on Social Engineering, Security Awareness, Organizational Security

ToC

Inhaltsverzeichnis

Psychology

- empirical and theoretical science
- describes, explains and predicts human behaviour and experiences
- human development and the internal and external causes and conditions
- Differential and Personality P., Social P., Industrial P., Organisational P., Pedagogical P.

Psychology and IT-Security?

Security is a latent social Construct and has to be treated as such. Psychological and sociological Methods and Tools are required. If the Security of a System should be enhanced, a Diagnosis, Prognosis and Intervention is required.

Security and Psychology

- Security is concluded by making Decisions
- Individuals make decisions based on their Biography, the Situation and how they perceive their Environment
  see: von Foerster, Luhmann, Spencer Brown, Baecker et.al.
- Psychology is the Science which researches these Topics.
- Therefore, Psychology is *required* to research Security.
- Psychology is the only Science able to research the basic fundamentals of Security.

Washing your Hands

- More pregnant Women died in the Vienna General Hospital than in a Monastery
- Ignaz Semmelweis discovered that Physicians transmit pathogenic agents
- He proposed that Physicians should wash their Hands
- His Idea was rejected and he was considered to be somewhat crazy
- This can only be explained by Psychology

Washing your Hands

- More pregnant Women died in the Vienna General Hospital than in a Monastery
- Ignaz Semmelweis discovered that Physicians transmit pathogenic agents
- He proposed that Physicians should wash their Hands
- His Idea was rejected and he was considered to be somewhat crazy
- This can only be explained by Psychology

1996: Ariane 5 Flight 501

320 000 000 Euro

Some Examples

- Users choose weak Passwords ...
- Users are not interested in Security ...
- Users don't understand Security ...
- Programmers create Buffer Overflows and forget safety Regulations ...
- Admins forget to patch ...
- Developers use MD5 as Password Hash ...
- Social Engineering
- Security Awareness

Research Programme

- Vienna Programme for Cyber-Peace
- introduced last year
- Psychology of Security is part of it
- 3 years estimated
- currently started

What do we need?

- Fundamental Research about the Perception of Security
- Fundamental Research about Personality / Attitudes and Security
- Organizational Development and Security
- Cultural Differences
- Didactics (Teaching Methodology) of Security
- What to teach?

Inhaltsverzeichnis

Perception of Security

- radical constructivistic approach
- each Individual perceives the World in one’s own Way
- shaped by one’s former experiences
- We have to explore this Worldview in depth
- by qualitative Research

Perception of Security

- different Tools and Methods exist
- several qualitative/semi-structured Interviews are lead with different interviewes
- eg. autobiographic-narrative Interviews with Hackers and Users
- Expertinterviews with Hackers and Researchers
- What shapes a Hacker's mind?
- How do Users perceive IT-Security?
- How can this Perception be changed?
- Are there Science based Security Awareness Tools?

Riskhomeostasis

- Risk behaviour is controlled by different Variables
- Self-perception, subjective Skills, objective Skills, Perception of Risk, Risk acceptance
- Researched in Industrial Psychology: Air Traffic Controller/Pilots, Workers in Nuclear Power Plants, Motor Vehicle Operator ...
- Study: East German Taxi Drivers switched from Wolga to Mercedes and had more accidents

Riskhomeostasis

- Risk behaviour is controlled by different Variables
- Self-perception, subjective Skills, objective Skills, Perception of Risk, Risk acceptance
- Researched in Industrial Psychology: Air Traffic Controller/Pilots, Workers in Nuclear Power Plants, Motor Vehicle Operator ...
- Study: East German Taxi Drivers switched from Wolga to Mercedes and had more accidents

Personality and Security

- Different Theories of Personality exist
- We use empirical sound Tools to examine Personality Traits and security relevant Behaviour
- Personality Traits are very stable over Lifetime
- quantitative research
- Big5: Neuroticism, Extraversion, Openness, Conscientiousness, Agreeableness
- Motives: Power, Achievement Orientation and others
- How do they correlate with security relevant behaviour?

Inhaltsverzeichnis

Organizational Development

- Security is a huge and hot Topic in Companies
- lots of Money is spend on Security Awareness and Training
- lots of different Methods exist eg. in Knowledge Management, Leadership, Organizational Development
- Which of them are useful for security relevant Behaviour?
- Strict Hierarchies can be easily attacked with Social Engineering ...

Inhaltsverzeichnis

Cultural Differences

- Culture influences Organisations and Individuals
- What are the differences? How can they influence Security?
- eg: How is the TVET system organizes? Is there a TVET System? On the job training? Only colleges?
- Lots of Tools and Methods exist, Research Results also
- Can they be transfered to our Problems?

Inhaltsverzeichnis

Didactics

- Didactics is the Science of Learning and Teaching
- Teaching Methodology
- very well researched in Germany due to the dual TVET System
- well funded and empirical sound
- several curriculums for IT skilled labour exist
- how can they be enhanced with IT security

How?

- How can we teach Security?
- Which Methods work best under which Circumstances?
- E-Learning? Blended Learning? Only Facts? Theory? Practical Approach?
- Culture is relevant
- well researched Model of Competencies/Capabilites is used in Germany
- not only facts are taught, but also studying and research methods
- independent learning is emphasized
- trainees learn *how* to keep their knowledge up to date
- trainees have to be able to know *what* to learn

How?

- How can we use this Model of Competencies/Capabilites?
- What are the best Methods to develop those Competencies?
- action oriented teaching? project work? masterpieces?

Who?

- Who has to learn about IT Security?
- Sysadmins, Developers, End Users
- create different roles
- determine what each role has to learn

What

- What to teach and learn?
- Who needs to understand Elliptic Curve Cryptography? Webmaster? Sysadmins? End Users?
- Who needs to understand what?
- How do we test that?
- When and How do those Curriculums and Tests need to be revised?

Web based teaching

- Part of the Programme
- modularized Curriculum
- adapted for different Roles
- different web based Methods including Mobile Learning
- including tests and certification

Inhaltsverzeichnis

Getting Knowledge

- Too much information is floating around
- too old information, which is obsolete and outdated
- false information
- find methods to identify correct knowledge
- create a knowledge base?
- who decides about the contents?
- empower users to identify correct/required knowledge?

What to do?

- Finish fundamental research
- Discuss what to teach
- Research cultural Differences
- Find adequate teaching Methods

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

- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher
- GnuPG: 9475 1687 4218 026F 6ACF 89EE 8B63 6058 D015 B8EF