Security in a Post NSA age

Stefan Schumacher
www.sicherheitsforschung-magdeburg.de

AusCERT 2014
Gold Coast, Australia,
2014-05-15



ToC

1. Intro
2. Social Science
3. Psychology



ToC

1. Intro
2. Social Science
3. Psychology



About me

- Head 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, Security Awareness, Organizational Security
- psychological profiling for social engineering
- my PoV is more a psychological PoV



ToC

1 Intro

2 Social Science

3 Psychology



Security in a Post NSA age?

- Can there be »security« in a Post NSA age?
- If so, why and how?
- If not, shouldn't we just surrender?
- Of course there can and will be security post NSA.
- Let's discuss some problems and ideas.
- And have a holistic view (read: not just technical)
- use sociological system theory and 2nd order cybernetics
- use psychology to discuss human behaviour and experience



Security in a Post NSA age?

- Can there be »security« in a Post NSA age?
- If so, why and how?
- If not, shouldn't we just surrender?
- Of course there can and will be security post NSA.
- Let's discuss some problems and ideas.
- And have a holistic view (read: not just technical)
- use sociological system theory and 2nd order cybernetics
- use psychology to discuss human behaviour and experience



After Snowden

- NSA leaks had differents effects on society
- sociological system theory (Niklas Luhmann et.al.): societies differentiate into functional specialised subsystems
- each subsystem focuses on different aspects of it's environment/society
- Legal System vs. Religious Systems vs. Political System
- Science: Philosophy vs. Humanities vs. Engineering vs. Natural Science



After Snowden

- Hacker: those conspiracy theorists with their tin foil hats were right ...
- IT-Sec: Paranoids: we expected the worst case scenario and prepared for it
- IT-Sec: not so paranoid: well, they have a lot to do
- Business: often helpless against industrial espionage, resigned
- Politicians: follow the party programme ..., Piratenpartei failed
- End User: either uninterested or resigned, Twitter activism does not really help
- Media: circlejerking according to their agenda



Consequences for us?

- What do the Snowden Leaks mean for us as security researchers?
- Let's assume there is an adversary with almost unlimited resources.
- How do we have to change how security works?
- What research has to be done?



2nd Order Cybernetics

break the circlejerk

- Cybernetics: transdisciplinary approach for exploring regulatory systems, their structures, constraints, and possibilities.
- Anything said, is said by an observer (Maturana/Varela)
- add the observer to the regulatory system: 2nd order cybernetics
- An observer acting in his field: 1st order cybernetics
- An observer discussing how he constructs his perception of the field he works in: 2nd order cybernetics



Trust

- Trust is one of the buzzwords here
- needs to be defined or explicated
- and operationalized (make it measurable)
- Niklas Luhmann explicated Trust in his 1968 Book *Vertrauen*
- as a »mechanism to reduce social complexity«
- social complexity is reduced with functional specialised subsystems
- Lawyers a experts for Laws, Hackers for IT-Sec, Physicians for Medicine etc. pp.



Trust

- every user has to trust the sysadmin
- every sysadmin has to trust the OS developers
- every os developer has to trust the compiler
- every compiler has to trust the OS it's running on
- there is no way to have an ontological access to the surrounding world
- you have to trust your own perception
- can you?



Trust

- every user has to trust the sysadmin
- every sysadmin has to trust the OS developers
- every os developer has to trust the compiler
- every compiler has to trust the OS it's running on
- there is no way to have an ontological access to the surrounding world
- you have to trust your own perception
- can you?



something to read/watch

- Niklas Luhmann: Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität
- Niklas Luhmann: Trust and Power
- Daniel F. Galouye: Simulacron-3/Counterfeit World
- Rainer Werner Fassbinder: Welt am Draht / World on a Wire
- Ryunosuke Akutagawa: Rashomon and Akira Kurosawa: Rashomon
- Wachowski Brothers: The Matrix



Consequences

- IT Security needs to professionalize beyond technical problems
- discussing the 31337th Buffer Overflow of the week won't fix fundamental problems
- human factors have to be analysed
- extend IT Security to Information Security
- create a new scientific field of Information Security
- include Psychology, Sociology, Educational Science, Didactics and others
- operationalize Information Security to make it measurable
- create a new vocational field of Information Security



ToC

1 Intro

2 Social Science

3 Psychology



Why 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?

My Operationalisation of InfoSec

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

- two maternity clinics in Vienna, the 1st with MDs the second with midwifes only
- more pregnant Women died in the 1st one
- pregnant women would rather give birth in the streets than be sent to the 1st clinic
- Ignaz Semmelweis discovered that Physicians transmit pathogenic agents (cadaverous poisoning)
- He proposed that Physicians should wash their Hands
- the death rate dropped 90%
- His Idea was rejected and he was considered to be crazy
- psychiatrised by force in Vienna



Washing your Hands

- two maternity clinics in Vienna, the 1st with MDs the second with midwifes only
- more pregnant Women died in the 1st one
- pregnant women would rather give birth in the streets than be sent to the 1st clinic
- Ignaz Semmelweis discovered that Physicians transmit pathogenic agents (cadaverous poisoning)
- He proposed that Physicians should wash their Hands
- the death rate dropped 90%
- His Idea was rejected and he was considered to be crazy
- psychiatrised by force in Vienna
- This can only be explained by Psychology



Washing your Hands

- two maternity clinics in Vienna, the 1st with MDs the second with midwifes only
- more pregnant Women died in the 1st one
- pregnant women would rather give birth in the streets than be sent to the 1st clinic
- Ignaz Semmelweis discovered that Physicians transmit pathogenic agents (cadaverous poisoning)
- He proposed that Physicians should wash their Hands
- the death rate dropped 90%
- His Idea was rejected and he was considered to be crazy
- psychiatrised by force in Vienna
- This can only be explained by Psychology



1996: Ariane 5 Flight 501



320 000 000 Euro

Ministerium für Staatssicherheit



1 official agent per 180 citizens

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



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?



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?



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 ...



Cultural Differences

- Culture influences Organisations and Individuals
- What are the differences? How can they influence Security?
- Death by Fan?
- The Protestant Ethic and the Spirit of Capitalism by Max Weber
- 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?



Didactics

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



- 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