The German Data Privacy Law and IT Security

Stefan Schumacher

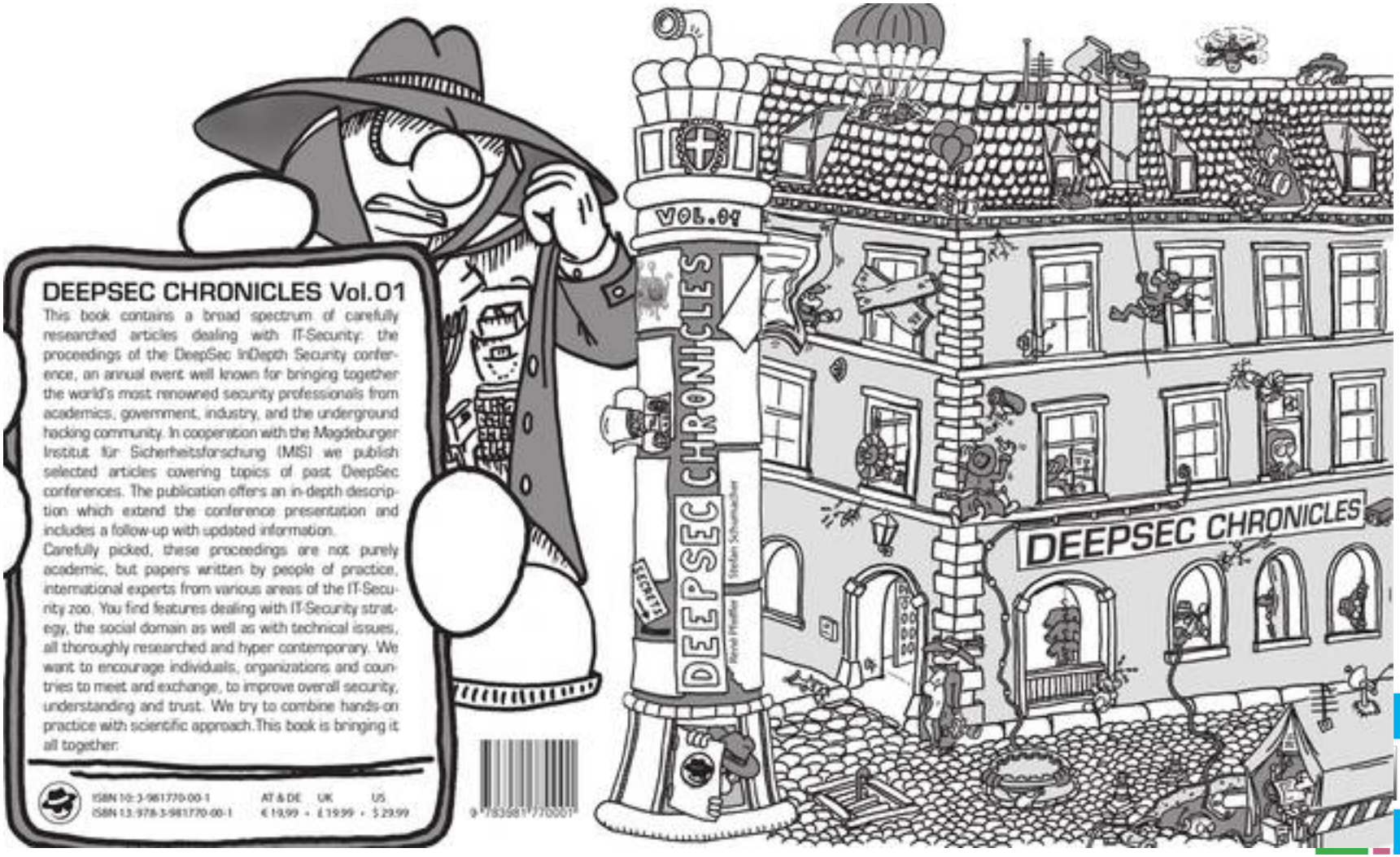
sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

DeepSec In Depth Security Conference



About Me




DEEPSEC CHRONICLES Vol.01
This book contains a broad spectrum of carefully researched articles dealing with IT-Security: the proceedings of the DeepSec InDepth Security conference, an annual event well known for bringing together the world's most renowned security professionals from academics, government, industry, and the underground hacking community. In cooperation with the Magdeburger Institut für Sicherheitsforschung (MIS) we publish selected articles covering topics of past DeepSec conferences. The publication offers an in-depth description which extend the conference presentation and includes a follow-up with updated information.
Carefully picked, these proceedings are not purely academic, but papers written by people of practice, international experts from various areas of the IT-Security zoo. You find features dealing with IT-Security strategy, the social domain as well as with technical issues, all thoroughly researched and hyper contemporary. We want to encourage individuals, organizations and countries to meet and exchange, to improve overall security, understanding and trust. We try to combine hands-on practice with scientific approach.This book is bringing it all together.
ISBN 10: 3-981770-00-1
ISBN 13: 978-3-981770-00-1
AT & DE UK US
€ 19,99 £ 19,99 $ 29,99
vol.01
DEEPSEC CHRONICLES
DEEPSEC CHRONICLES

Research Programmes

- Social Engineering / Security Awareness
- Psychology of Security
- Didactics of Security/Cryptography
- Construction of Security in Individuals (qualitative research)
- IT security in (very) small enterprises



ToC

1 Data Privacy Laws

2 Directory of Procedures

3 small and medium-sized enterprises



History

- debates about privacy and data processing in the 1960s
- computers became powerful and affordable
- governments wanted to collect and analyse data
- data, information and knowledge is power
- population was not happy with this
- scientific and political debate begun
- leading to data privacy laws



Data Privacy Laws

- first law introduced in 1970 in Hesse
- federal law in West Germany since 1977
- 1981 introduced in all West German federal states
- based on the concept of informational self-determination



informational self-determination

... in the context of modern data processing, the protection of the individual against unlimited collection, storage, use and disclosure of his/her personal data is encompassed by the general personal rights of the German constitution.

This basic right warrants in this respect the capacity of the individual to determine in principle the disclosure and use of his/her personal data.

Limitations to this informational self-determination are allowed only in case of overriding public interest.



informational self-determination

- administration/companies are not allowed to gather data about me
- administration/companies are not allowed to process data about me
- administration/companies are not allowed to share data about me
- unless you are legally allowed to
- or I agreed to it (written, with certain limitations)



main concepts of data protection

- prohibition with reservation of authorisation (by law or the person affected)
- data reduction and data economy
- necessity
- appropriation: data is only allowed to be processed for the purpose it was collected.
  eg. a mail order company cannot use address and banking data for marketing purposes



main concepts of data protection

- prohibition with reservation of authorisation (by law or the person affected)
- data reduction and data economy
- necessity
- appropriation: data is only allowed to be processed for the purpose it was collected.
  eg. a mail order company cannot use address and banking data for marketing purposes



Thomas Hobbes

Leviathan

And Covenants, without the Sword, are but Words, and of no strength to secure a man at all.



supervision

- federal data protection officer for federal agencies
- federal states data protection officers for agencies of federal states
- who also supervise companies
- companies have to have an internal data protection officer depending on the number of employees and/or type of data processed



supervision

- shut down and confiscate the IT system
- supervisors can give out monetary penalties
- companies can get the money back from the board/executives
- but also help with IT security methods
- Lidl had to pay 1.46m Euro



supervision

- shut down and confiscate the IT system
- supervisors can give out monetary penalties
- companies can get the money back from the board/executives
- but also help with IT security methods
- Lidl had to pay 1.46m Euro



in company data privacy officer

- checks the data privacy measures of the company
- reports directly to the board/executive
- has no power to direct
- cannot be fired
- has to be reliable and skilled
- typically an external consultant



ToC

1 Data Privacy Laws

2 Directory of Procedures

3 small and medium-sized enterprises



Directory of Procedures

- required if personal data is processed
- directory or list of all procedures that process personal data
- e.g. application process, personal records, email, disciplinary warning letters
- public part has to be handed out to anyone who wants one
- internal part describing security measures only for supervisors



Directory of Procedures

- describes the process
- the involved staff
- source of personal data
- object of data processing
- people/organisations that receive personal data



Directory of Procedures

- What data is there?
- Where does it come from?
- Is it illegal gathered data?
- Is the data correct?
- Who entered illegal/incorrect data?
- Where and how is it processed?
- Who has access to the data?
- Are there external companies involved?



Technical Organisational Measures

- required in the internal version, not to be published
- describes all technical and organisational measures to secure data
- different terminology than used in IT sec (unfortunately)
- developed by government officials and lawyers, so it's *legalese*



Technical Organisational Measures

- physical access control (server room is locked, document files are locked away)
- access control (user/password, 2FA)
- user access control/role-based access control (ACLs, roles/groups, categories for data)
- disclosure/transfer control (external backups are encrypted and stored in a vault)



Technical Organisational Measures

- input control (who entered data? who is responsible for mistakes)
- commission control (external data processor have to follow your orders and conform to the BDSG)
- availability control (backups, redundant systems, hot standby, UPS)
- segregation control (data collected for different purposes has to be stored and processed segragated, eg. clients ./. potential clients)



Data Privacy ./. IT Sec

- they are not the same
- they do not cover the same field
- they are interconnected
- IT Sec is required when you want to do data privacy
- eg. using GnuPG to encrypt data to protect it



ToC

1 Data Privacy Laws

2 Directory of Procedures

3 small and medium-sized enterprises



small and medium-sized enterprises

- EU definition of SME:
- staff headcount: less than 250
- turnover: less than 50m
- balance sheet total: less than 43m
- ca. 60% of the German workforce work in SME



SME and IT Sec

- there often is no IT sec at SMEs
- there often even is no IT at all at SMEs
- IT sec awareness non existing
- data privacy law is a lever to get SMEs to do something about IT sec
- could be a model for an IT sec law ...



SME and IT Sec

- SME are not interested in IT sec
- They are often not aware of their role in IT sec
- they are often overwhelmed by IT sec - and sometimes even IT
- lack of skilled labour in very small SME
- no strategy about IT (and IT Sec)
- we cannot motivate them to do something
- consequences of security incidents are too far away



SME and IT Sec

how they rationalize IT sec

- we are not important ...
- no one will attack us ...
- we haven't been attacked in the last 30 years ...
- we don't know what to do ...
- that topic is too complex ...
- They know nothing about botnets, skript kiddies and Metasploit



SME and IT Sec

how the rationalize not doing IT sec

- We show them `Sicherheitstacho.eu`, Kippo logs and password cracker
- Live-Hacking with Kali/Metasploit and how easy it is
- show them security incidents that happened in DE
- they get afraid
- and give up (fatalistic approach: ... there is nothing we can do anyways ...)
- paternalistic approach: I won't let politicians tell me what to do! I built this company!



SME and IT Sec

how the rationalize not doing IT sec

- We show them `Sicherheitstacho.eu`, Kippo logs and password cracker
- Live-Hacking with Kali/Metasploit and how easy it is
- show them security incidents that happened in DE
- they get afraid
- and give up (fatalistic approach: ... there is nothing we can do anyways ...)
- paternalistic approach: I won't let politicians tell me what to do! I built this company!



countermeasures

- offer trainings *suited for very small enterprises*
- offer standards and procedures *suited for very small enterprises*
- we developed a 25 pages guideline for very small enterprises via the E-Businesslotsen in Germany
- use the data privacy law as a lever for IT sec



countermeasures

- if they don't want to do IT sec, force them to do so
- at least at a basic level
- with the help of the data privacy law
- they are forced to create the Directory of Procedures
- including the Technical Organisational Measures
- which leads to an analysis of their procedures
- so they have to think about IT sec!



countermeasures

- it is really hard to motivate people to do IT Sec
- or data privacy
- psychologically: we would have to find their demands (regarding IT sec)
- and show them how to fulfill them
- intrinsic motivation is much better than extrinsic motivation
- punishments suck, because we have to constantly punish them
- but how do we get them to do IT Sec?



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



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