Organizational and Technical Data Security in the Context of European Data Protection Law

An Overview

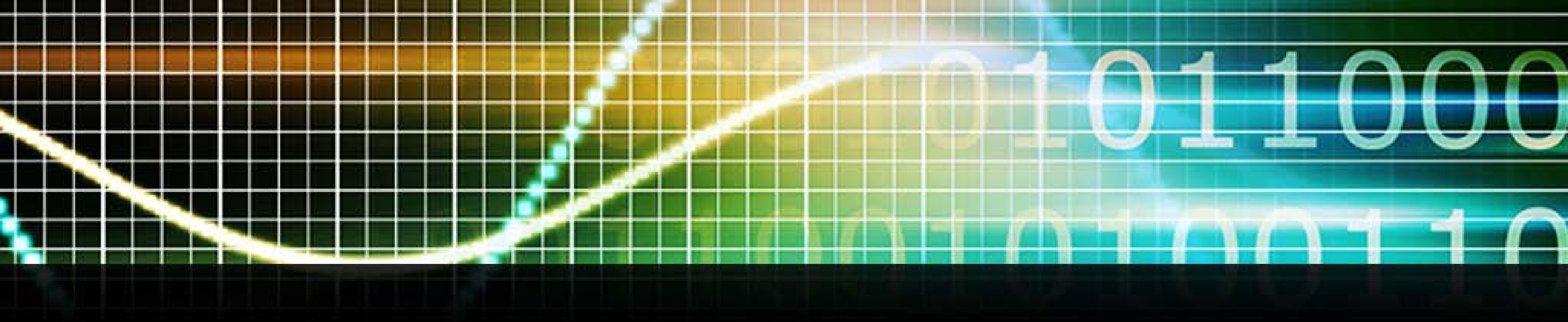
The Speaker

PhDr. M.A. Dipl.-Betriebswirt (FH) Thomas H. Lenhard, PhD.

- Government-accredited expert for IT and data protection
- Accredited expert for the European Privacy Seal
- CEO of the medi-ip data protect UG, Bonn
- President of the German Association of Consultants and Experts in Health and Social Services (VBSG e.V.) and Chairman of its section “IT and Data Protection”

www.it-planung.com www.medi-ip-dataprotect.com

EuroPriSe European Privacy Seal TECHNICAL EXPERT



Structure of the Presentation

- Why do we care about Data Protection/Privacy?
- The link between Data Protection and Data Security
- Data Protection in international environments
- Worse things happen at … the computer center
- Categories of an data protection audit
- Some considerations about „Hacking“

Why do we Care About Data Protection/Privacy?

CHARTER OF **FUNDAMENTAL RIGHTS** OF THE EUROPEAN UNION

(2000/C 364/01) Article 8 (Protection of personal data):

(1) **Everyone** has the right to the protection of personal data concerning him or her.

Why do we Care About Data Protection/Privacy?

Article 8 Paragraph 2 of the Charter of fundamental rights of the EU gives a complete definition of the requirements that have to be fullfilled for processing personal data:

1. For Processing Personal Data it needs
   - a. The consent of the person concerned or
   - b. a legal basis
2. The use of Personal Data is limited to the purpose for which this data were collected

Why do we Care About Data Protection/Privacy?

Unanimously, on the 18th Dec. 2013, the UN General Assembly has adopted the resolution about

„The right to privacy in the digital age“:

Member states confirmed to respect and protect data privacy

Why do we Care About Data Protection/Privacy?

The aim of Data Protection is not limited to the prevention of unauthorized access to personal data:

Personal data has to be prevented from

- any kind of unauthorized manipulation
- loss and destruction
- unauthorized access
- any lack of availibility and operational safety

The Link Between Data Protection and Data Security

The most important regulations about data protection in the EU are:

Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the „protection of individuals with regards to the proecssing of personal data and on the free movement of such data“

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning “the processing of personal data and the protection of privacy in the electronic communications sector” (Directive on privacy and electronic communications)

The Link Between Data Protection and Data Security

Technical and organisational measures

Article 4 Paragr. 1 of the Directive 2002/58/EC:

“The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security” …

The Link Between Data Protection and Data Security

Technical and Organisational measures

Article 4 Paragr. 1 of the Directive 2002/58/EC:

- … “Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.“

The Link Between Data Protection and Data Security

Technical and Organisational measures

Item #25 of the Directive 95/46/EC:

Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security …

The Link Between Data Protection and Data Security

Technical and Organisational measures

Item #46 of the Directive 95/46/EC:

Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, …

The Link Between Data Protection and Data Security

Technical and Organisational measures

Article 17 Paragr. 1 (Security of Processing) of the Directive 95/46/EC:

Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

The link between Data Protection and Data Security

European Law does not only define that personal data have to be protected

European Law does also define that there must be technical and organisational measures to protect personal data

The Link Between Data Protection and Data Security

The technical and organisational measures for protecting data can be summarized under the term

DATA SECURITY

It is an essential part of Data Protection/Privacy

The Link Between Data Protection and Data Security

Since technical and organisational measures envolve, the European Law speaks about

- appropriate technical and organisational meassures
- **the state of the art**

The Link Between Data Protection and Data Security

The state of the art …

… in the context of data security is found in standards like the ISO 27001 (one of the most important standards in IT)

Even if standards do not constitute a legal obligation, special acts demand for the “state of the art”

Data Protection in International Environments

Using an external data center (sic!) or an external provider for processing or storing personal data means in general

processing data as a service

As long as a service provider is located in the European Community and data is not transmitted into a third country, it is assumed that the required level of data protection is ensured

Data Protection in International Environments

Safe countries for data processing:

- States of the European Economic Area (EEA)
  = EU Member States, Norway, Liechtenstein, Iceland
- Switzerland (special bilateral agreements)

Data Protection in International Environments

Unsafe countries for data processing:

All countries that are not defined as being a safe country …

e.g. Togo, Bangladesh, India, Russia, Taiwan, Nigeria, North Korea, …and also the USA

Data Protection in International Environments

Directive 95/46/EC prohibits in principle the transfer of personal data from EU Member States in countries that do not have a comparable level of data protection.

Since the United States of America are the biggest trading partner of the European Union a special solution has been launched by the EU:

The Safe Harbor System

Data Protection in International Environments

If an US-Company is member of the Safe Harbor System, it is assumed that the required level of data protection is ensured.

Members of the Safe Harbor System are e.g.

- Hewlett-Packard
- IBM
- Microsoft

Data Protection in International Environments

Three methods are available to ensure the nescessary level of data protection in third countries:

- The Safe Harbor System
- Binding Corporate Rules
- EU-Standard-Clauses (in contracts)

Worse Things Happen at … the Computer Center

Worse Things Happen at … the Computer Center

Data Security does not only mean using a Firewall

Worse Things Happen at … the Computer Center

Some disciplines that belong to Data Security:

Electricity and high-frequency technology

Fire protection

Water protection

Lightning protection

Protection against burglary, theft and sabotage

…

Worse Things Happen at … the Computer Center

Some disciplines that belong to Data Security:

…

Protection against espionage

Prevention against Human errors and technical failures

High-availability of systems (and data)

Protection against a loss of data

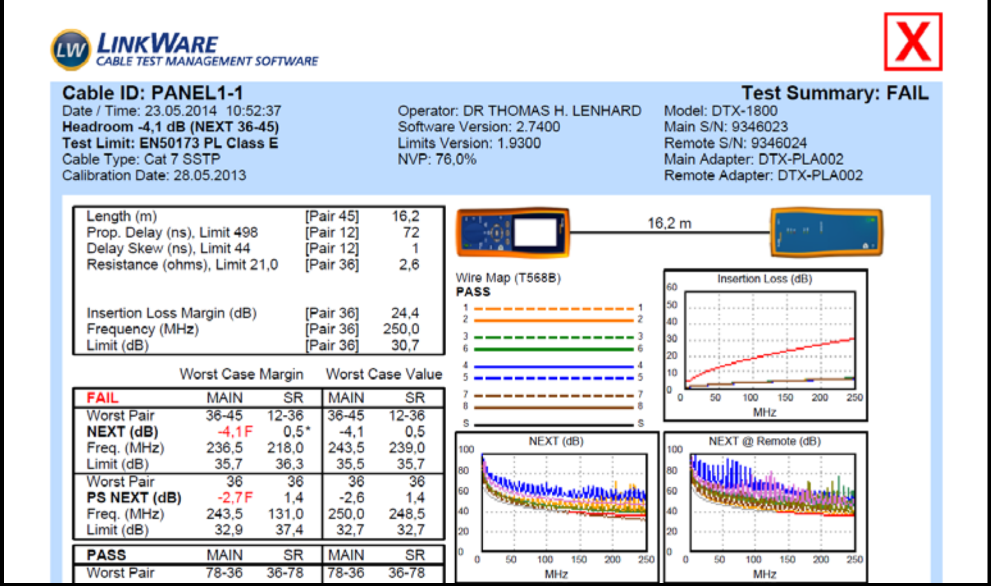
Reliability of Systems

Worse Things Happen at … the Computer Center

Impressions of IT installations

Worse Things Happen at … the Computer Center

Impressions of IT installations



LINKWARE
CABLE TEST MANAGEMENT SOFTWARE

X

Cable ID: PANEL1-1 | **Test Summary: FAIL**

Date / Time: 23.05.2014 10:52:37
Headroom -4,1 dB (NEXT 36-45)
Test Limit: EN50173 PL Class E
Cable Type: Cat 7 SSTP
Calibration Date: 28.05.2013

Operator: DR THOMAS H. LENHARD
Software Version: 2.7400
Limits Version: 1.9300
NVP: 76,0%

Model: DTX-1800
Main S/N: 9346023
Remote S/N: 9346024
Main Adapter: DTX-PLA002
Remote Adapter: DTX-PLA002

Length (m)	[Pair 45]	16,2
Prop. Delay (ns), Limit 498	[Pair 12]	72
Delay Skew (ns), Limit 44	[Pair 12]	1
Resistance (ohms), Limit 21,0	[Pair 36]	2,6
Insertion Loss Margin (dB)	[Pair 36]	24,4
Frequency (MHz)	[Pair 36]	250,0
Limit (dB)	[Pair 36]	30,7

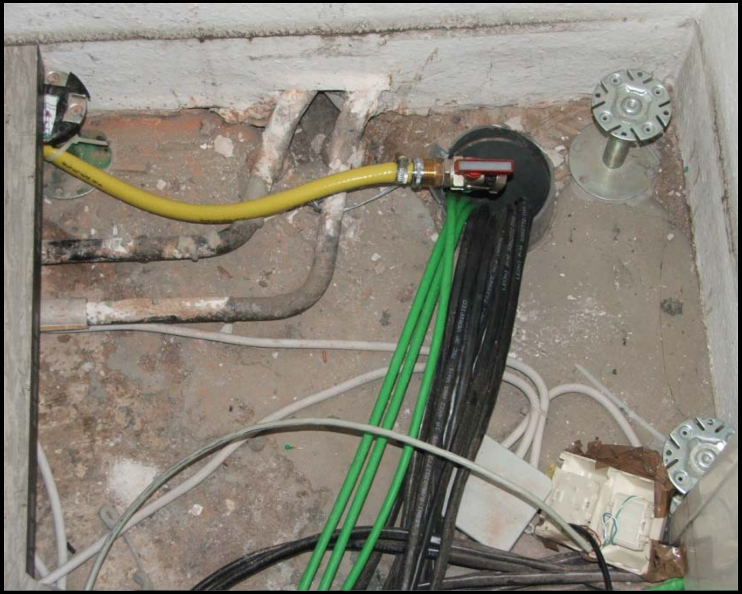
	Worst Case Margin		Worst Case Value	
FAIL	MAIN	SR	MAIN	SR
Worst Pair	36-45	12-36	36-45	12-36
NEXT (dB)	-4,1F	0,5*	-4,1	0,5
Freq. (MHz)	236,5	218,0	243,5	239,0
Limit (dB)	35,7	36,3	35,5	35,7
Worst Pair	36	36	36	36
PS NEXT (dB)	-2,7F	1,4	-2,6	1,4
Freq. (MHz)	243,5	131,0	250,0	248,5
Limit (dB)	32,9	37,4	32,7	32,7

PASS	MAIN	SR	MAIN	SR
Worst Pair	78-36	36-78	78-36	36-78

Wire Map (T568B)
PASS

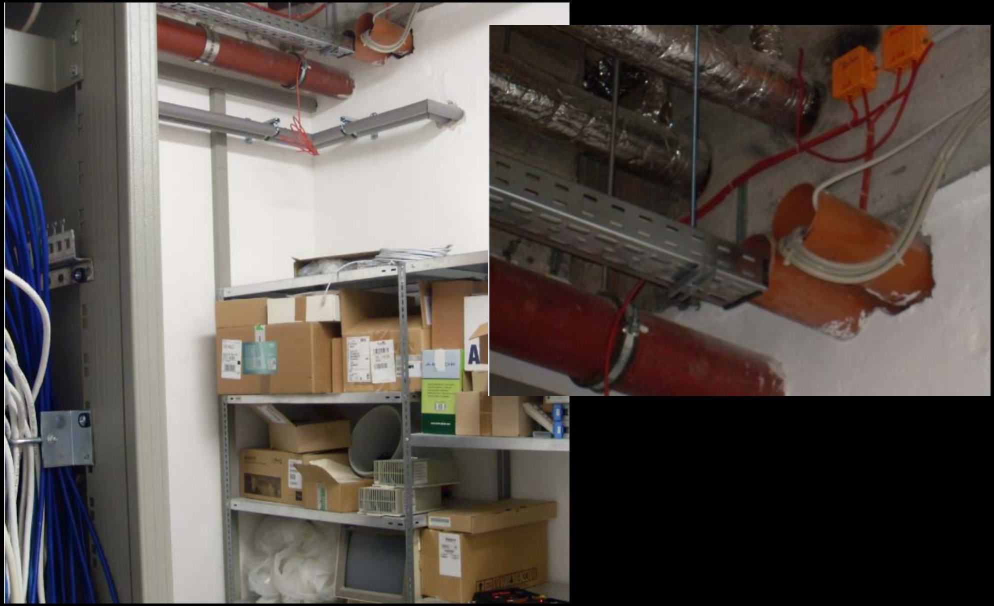
Worse Things Happen at … the Computer Center

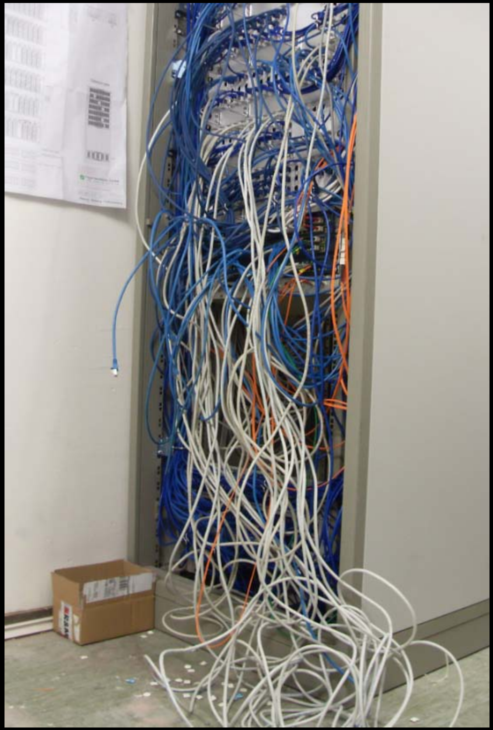
Impressions of IT installations



Worse Things Happen at … the Computer Center

Impressions of IT installations





Worse Things Happen at … the Computer Center

Impressions of IT installations

Worse Things Happen at … the Computer Center

Sometimes the administrator is the biggest threat to IT security …

Categories of an Data Protection Audit

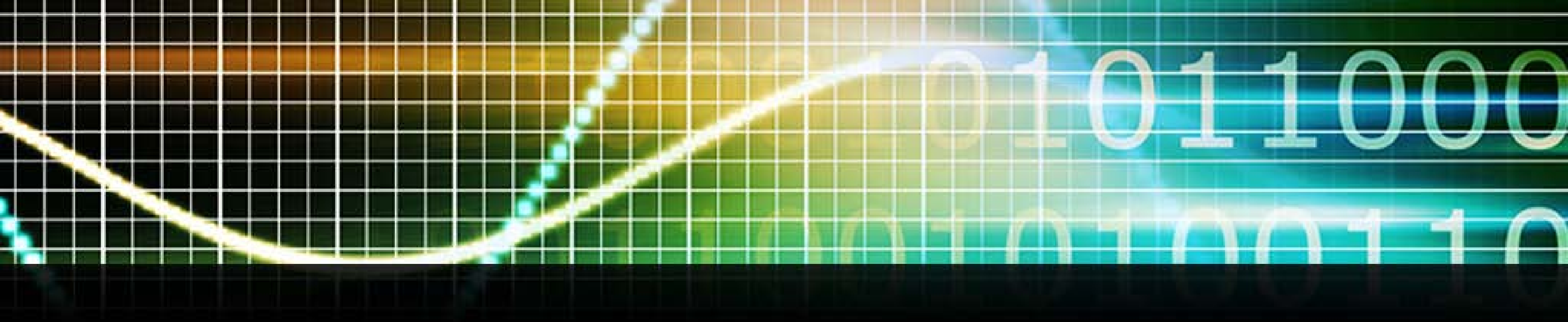
- Entry Control (datacenter, server room, building)
- Admission Control
- Control of Access Permissions
- Transfer Control
- Input Control (Validation)
- Control of Order
- Availability Control

Categories of an Data Protection Audit

Basic Questions:

Which kinds of personal data are processed?

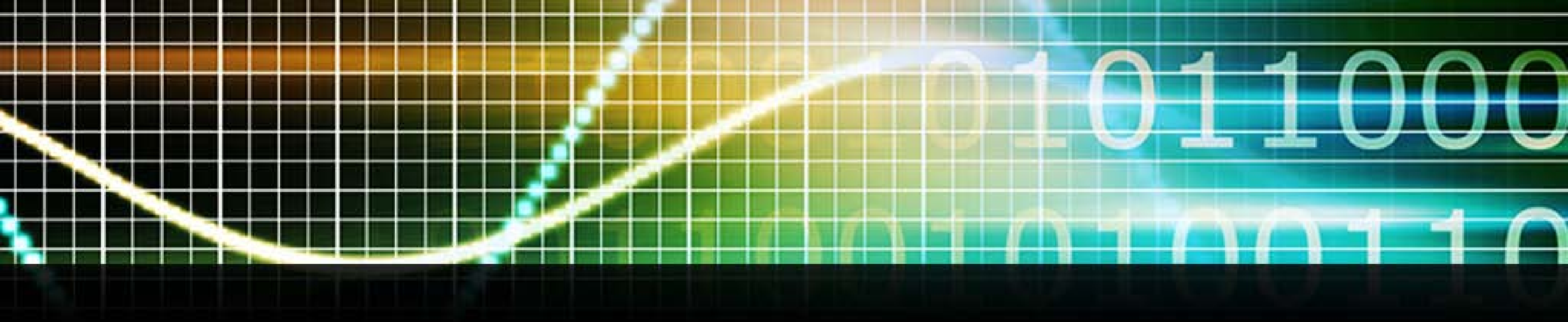
Which level of data protection/security is needed/nescessary?



Categories of an Data Protection Audit

Entry Control (datacenter, serverroom, building)

- camera surveillance
- Intrusion detection (physical)
- Secure locking system / RFID-Tokens / Using Codes
- List of visitors
- Regulations about the permission to enter a server room
- Measures against unauthorized entry into the computer center or into office rooms
- …



Categories of an Data Protection Audit

Admission Control

- Firewalls
- Intrusion Detection System (Software)
- Monitoring
- Standard procedures for locking unused network socket (e.g. RJ45)
- Data Encryption

Categories of an Data Protection Audit

Control of Access Permissions

- Regulations about the complexity of passwords
- Procedures to set up, lock or delete user accounts
- Concept about user group and user rights
- Logging of activities and access to personal data
- Regulations about handling passwords (employee training)
- Password protected screen saver
- Directions, e.g. locking out when leaving the office

Categories of an Data Protection Audit

Availability Control

- Backup concept
- Emergency manual
- Anti-Virus concept
- Concept about availability (e.g. Clustering)
- Risk management
- …

Categories of an Data Protection Audit

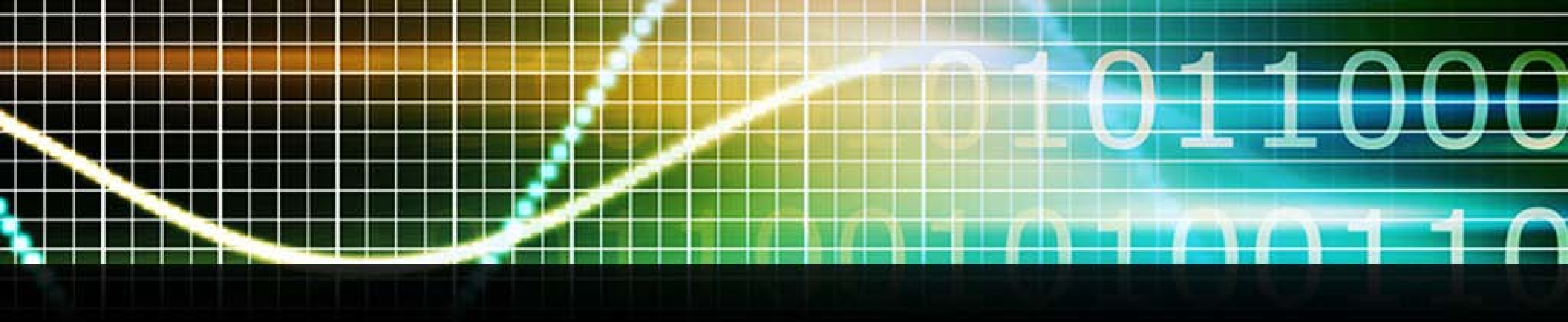
It is nescessary for any data security/protection concept that the employees are trained regularly about …

- Handling hard- and software
- Handling personal data
- Confidentiality obligation
- Risks, when using IT
- Dangers of viruses, trojan and other malware
- Dangers of hacking

Some Considerations About „Hacking“

The danger of an privacy incident can be lowered significant or minimized by realizing consequently organisational and technicals measures.

Hacking is only the second largest treath, because hackers use organisational and technical vulnerabilities (in many cases, this is the result of insufficient planning and bad administration)



Some Considerations About „Hacking“

Some simple examples:

Criminals use „hacked“ Wlans in order to deseive people. Sometimes WLans are not encrypted!

It needs less than 10 Minutes to hack an WLan-Access-Point that uses the obsolete encryption WEP (Tool: Backtrack, Kali-Linux)

Some Considerations About „Hacking“

Some simple examples:

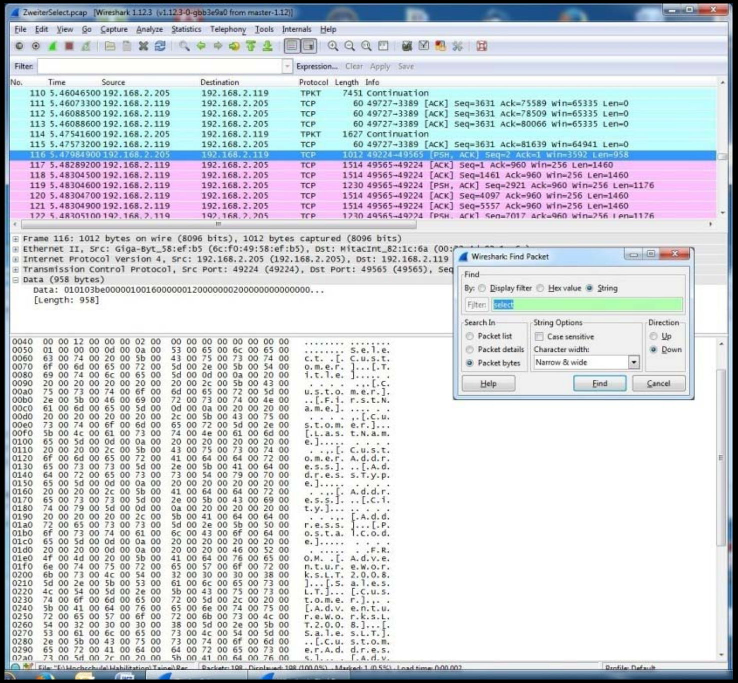
A defence company was hacked out from a computer room of European University in the 90‘s. Internet connection was available without authentication.

A vunerability of former unix/linux distribution was used for this hack. The passwords where decrypted using dictionaries.

Some Considerations About „Hacking“

Some simple examples:

If data is not encrypted in the network, TCP-packages can be logged very easy. Message can be read. (Tool: Wireshark) or VoIP-Calls can be replicated (Tool: Backtrack)


ZweiterSelect.pcap [Wireshark 1.12.3 (v1.12.3-0-gbb3e9a0 from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
Wireshark: Find Packet
Help Find Cancel

```
No.  Time       Source         Destination    Protocol Length Info
 110 5.46046500 192.168.2.205  192.168.2.119  TPKT     7451 Continuation
 111 5.46073300 192.168.2.119  192.168.2.205  TCP        60 49727→3389 [ACK] Seq=3631 Ack=75589 Win=65335 Len=0
 112 5.46088500 192.168.2.119  192.168.2.205  TCP        60 49727→3389 [ACK] Seq=3631 Ack=78509 Win=65335 Len=0
 113 5.46088600 192.168.2.119  192.168.2.205  TCP        60 49727→3389 [ACK] Seq=3631 Ack=80066 Win=65335 Len=0
 114 5.47541600 192.168.2.205  192.168.2.119  TPKT     1627 Continuation
 115 5.47573200 192.168.2.119  192.168.2.205  TCP        60 49727→3389 [ACK] Seq=3631 Ack=81639 Win=64941 Len=0
 116 5.47984900 192.168.2.205  192.168.2.119  TCP      1012 49224→49565 [PSH, ACK] Seq=2 Ack=1 Win=3592 Len=958
 117 5.48289200 192.168.2.119  192.168.2.205  TCP      1514 49565→49224 [ACK] Seq=1 Ack=960 Win=256 Len=1460
 118 5.48304500 192.168.2.119  192.168.2.205  TCP      1514 49565→49224 [ACK] Seq=1461 Ack=960 Win=256 Len=1460
 119 5.48304600 192.168.2.119  192.168.2.205  TCP      1230 49565→49224 [PSH, ACK] Seq=2921 Ack=960 Win=256 Len=1176
 120 5.48304700 192.168.2.119  192.168.2.205  TCP      1514 49565→49224 [ACK] Seq=4097 Ack=960 Win=256 Len=1460
 121 5.48304900 192.168.2.119  192.168.2.205  TCP      1514 49565→49224 [ACK] Seq=5557 Ack=960 Win=256 Len=1460
 122 5.48305100 192.168.2.119  192.168.2.205  TCP      1230 49565→49224 [PSH, ACK] Seq=7017 Ack=960 Win=256 Len=1176
```

```
⊞ Frame 116: 1012 bytes on wire (8096 bits), 1012 bytes captured (8096 bits)
⊞ Ethernet II, Src: Giga-Byt_58:ef:b5 (6c:f0:49:58:ef:b5), Dst: MitacInt_82:1c:6a (00:
⊞ Internet Protocol Version 4, Src: 192.168.2.205 (192.168.2.205), Dst: 192.168.2.119
⊞ Transmission Control Protocol, Src Port: 49224 (49224), Dst Port: 49565 (49565), Seq
⊟ Data (958 bytes)
    Data: 010103be000001001600000012000000020000000000000...
    [Length: 958]
```

Find

By: ○ Display filter ○ Hex value ● String

Filter: select

Search In: ○ Packet list ○ Packet details ● Packet bytes

String Options: □ Case sensitive

Character width: Narrow & wide

Direction: ○ Up ● Down

```
0040  00 00 12 00 00 00 02 00  00 00 00 00 00 00 00 00   ........ ........
0050  01 00 00 00 0d 00 0a 00  53 00 65 00 6c 00 65 00   ........ S.e.l.e.
0060  63 00 74 00 20 00 5b 00  43 00 75 00 73 00 74 00   c.t. .[. C.u.s.t.
0070  6f 00 6d 00 65 00 72 00  5d 00 2e 00 5b 00 54 00   o.m.e.r. ]...[.T.
0080  69 00 74 00 6c 00 65 00  5d 00 0d 00 0a 00 20 00   i.t.l.e. ]..... .
0090  20 00 20 00 20 00 20 00  20 00 2c 00 5b 00 43 00    . . . .  .,.[.C.
00a0  75 00 73 00 74 00 6f 00  6d 00 65 00 72 00 5d 00   u.s.t.o. m.e.r.].
00b0  2e 00 5b 00 46 00 69 00  72 00 73 00 74 00 4e 00   ..[.F.i. r.s.t.N.
00c0  61 00 6d 00 65 00 5d 00  0d 00 0a 00 20 00 20 00   a.m.e.]. .... . .
00d0  20 00 20 00 20 00 20 00  2c 00 5b 00 43 00 75 00    . . . . ,.[.C.u.
00e0  73 00 74 00 6f 00 6d 00  65 00 72 00 5d 00 2e 00   s.t.o.m. e.r.]...
00f0  5b 00 4c 00 61 00 73 00  74 00 4e 00 61 00 6d 00   [.L.a.s. t.N.a.m.
0100  65 00 5d 00 0d 00 0a 00  20 00 20 00 20 00 20 00   e.]..... . . . .
0110  20 00 20 00 2c 00 5b 00  43 00 75 00 73 00 74 00    . .,.[. C.u.s.t.
0120  6f 00 6d 00 65 00 72 00  41 00 64 00 64 00 72 00   o.m.e.r. A.d.d.r.
0130  65 00 73 00 73 00 5d 00  2e 00 5b 00 41 00 64 00   e.s.s.]. ..[.A.d.
0140  64 00 72 00 65 00 73 00  73 00 54 00 79 00 70 00   d.r.e.s. s.T.y.p.
0150  65 00 5d 00 0d 00 0a 00  20 00 20 00 20 00 20 00   e.]..... . . . .
0160  20 00 20 00 2c 00 5b 00  41 00 64 00 64 00 72 00    . .,.[. A.d.d.r.
0170  65 00 73 00 73 00 5d 00  2e 00 5b 00 43 00 69 00   e.s.s.]. ..[.C.i.
0180  74 00 79 00 5d 00 0d 00  0a 00 20 00 20 00 20 00   t.y.]... .. . . .
0190  20 00 20 00 20 00 2c 00  5b 00 41 00 64 00 64 00    . . .,. [.A.d.d.
01a0  72 00 65 00 73 00 73 00  5d 00 2e 00 5b 00 50 00   r.e.s.s. ]...[.P.
01b0  6f 00 73 00 74 00 61 00  6c 00 43 00 6f 00 64 00   o.s.t.a. l.C.o.d.
01c0  65 00 5d 00 0d 00 0a 00  20 00 20 00 20 00 20 00   e.]..... . . . .
01d0  20 00 20 00 0d 00 0a 00  20 00 20 00 46 00 52 00    . ..... . .F.R.
01e0  4f 00 4d 00 20 00 5b 00  41 00 64 00 76 00 65 00   O.M. .[. A.d.v.e.
01f0  6e 00 74 00 75 00 72 00  65 00 57 00 6f 00 72 00   n.t.u.r. e.W.o.r.
0200  6b 00 73 00 4c 00 54 00  32 00 30 00 30 00 38 00   k.s.L.T. 2.0.0.8.
0210  5d 00 2e 00 5b 00 53 00  61 00 6c 00 65 00 73 00   ]...[.S. a.l.e.s.
0220  4c 00 54 00 5d 00 2e 00  5b 00 43 00 75 00 73 00   L.T.]... [.C.u.s.
0230  74 00 6f 00 6d 00 65 00  72 00 5d 00 2c 00 20 00   t.o.m.e. r.].,. .
0240  5b 00 41 00 64 00 76 00  65 00 6e 00 74 00 75 00   [.A.d.v. e.n.t.u.
0250  72 00 65 00 57 00 6f 00  72 00 6b 00 73 00 4c 00   r.e.W.o. r.k.s.L.
0260  54 00 32 00 30 00 30 00  38 00 5d 00 2e 00 5b 00   T.2.0.0. 8.]...[.
0270  53 00 61 00 6c 00 65 00  73 00 4c 00 54 00 5d 00   S.a.l.e. s.L.T.].
0280  2e 00 5b 00 43 00 75 00  73 00 74 00 6f 00 6d 00   ..[.C.u. s.t.o.m.
0290  65 00 72 00 41 00 64 00  64 00 72 00 65 00 73 00   e.r.A.d. d.r.e.s.
02a0  73 00 5d 00 2c 00 20 00  5b 00 41 00 64 00 76 00   s.]... . [.A.d.v.
```

A SQL-Message is „sniffed“

Some Considerations About „Hacking“

Some simple examples:

A very popular method to infect a companies network is to leave some USB-Sticks with some malware at the parking area of this company.

If a screen is not secured/locked while employees go to lunch, it needs less than one minute to install any malware or even to decrypt a passwords (e.g. in MS-Outlook)

Conclusion

Data Security is an important item of data protection/privacy

European data protection law defines a frame to protect our personal data by pointing to the state of the art

European data protection law facilitates the cooperation of European and international companies

Most cases of hacking and many privacy incidents could be avoided, if companies would scrupulously and consequent act according to the existing regulations and standards

But data protection/privacy can only be succesful if you remember one thing:

Keep your eyes open!

Thank you for your attention!