



Design by
iMedent GmbH

```
<!DOCTYPE html>  
<html><head>  
<title>
```

Datensicherheit in der Zahnarztpraxis - zu Risiken und Nebenwirkungen

```
</title> /head>  
<body> the content of the document  
</body>
```

Ein agiles und
Kundenorientiertes
Unternehmen, das
schnell auf die
wachsenden
Anforderung unserer
Kunden reagieren kann!

www.imedent.de

A portrait of Oliver Lubecki, a man with short brown hair and a light beard, wearing a dark blue patterned shirt under a dark jacket. He is looking directly at the camera with a slight smile.

Oliver Lubecki
Gründer von iMedent



Unsere Kernaufgaben
IT, Design & Marketing

Über Imedent

Das machen wir!

Praxi-IT,

Praxis-Design &

Marketing für Zahnärzte

www.imedent.de

Das machen wir nicht !

Wie sind kein Depot!

Wir verkaufen keine

Zahnarztsoftware

und keine sonstigen

Geräte.



*Wir machen, was wir
wirklich können!*

Qualifikation im Bereich IT und Datenschutz

- Studium der Informatik in Leipzig
- Gründung der iMedent GmbH 2015
- Zertifizierung zum Datenschutz-beauftragten
- Zertifizierung zum PED



Oliver Lubecki
Gründer von iMedent

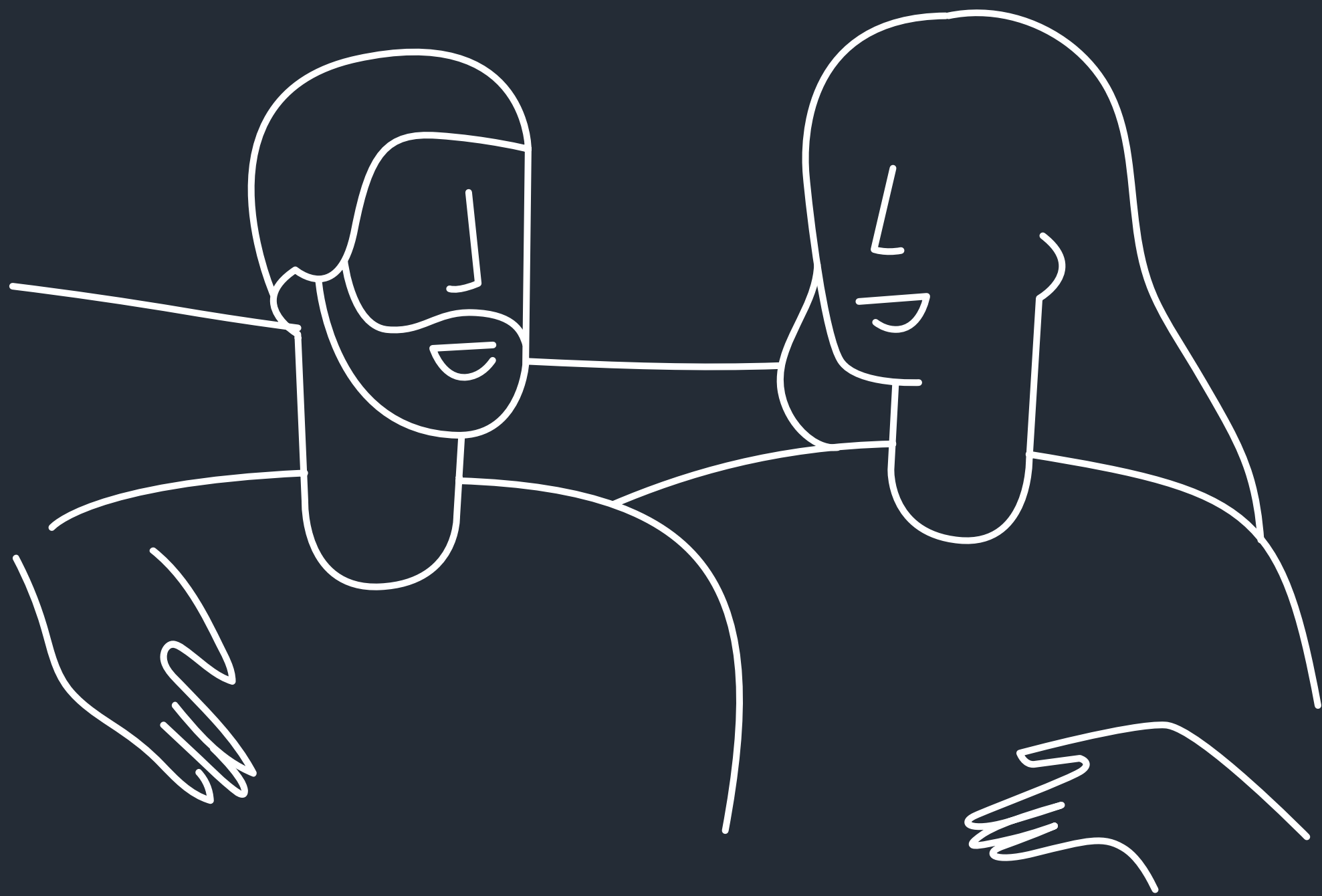
www.imedent.de

Aktuelle Meldung zum Thema IT, Zahnärzte & Sicherheit

- 01** Zurück zu Bleistift und Papier: Schadsoftware legt Klinikserver lahm. *Quelle Heise vom 15.08.2019*
- 02** Technische Probleme bei der Einführung der elektronischen Patientenakte. *Quelle: Spiegel vom 22.08.2019*
- 03** Schwachstelle in Intel-Prozessoren kann Passwörter preisgeben: *Quelle: Spiegel 07.08.2019*

Gliederung: "Datensicherheit in der Zahnarztpraxis"

- Theorieteil** Einführung in die Informatik - Grundlagen
und Begrifflichkeiten
- Pause** Hier gibt es reichlich Kaffee und Kuchen
- Praxisteil** Planung und Gedanken für eine sichere Zahnarztpraxis



Zitat der Landeszahnärztekammer sachsen

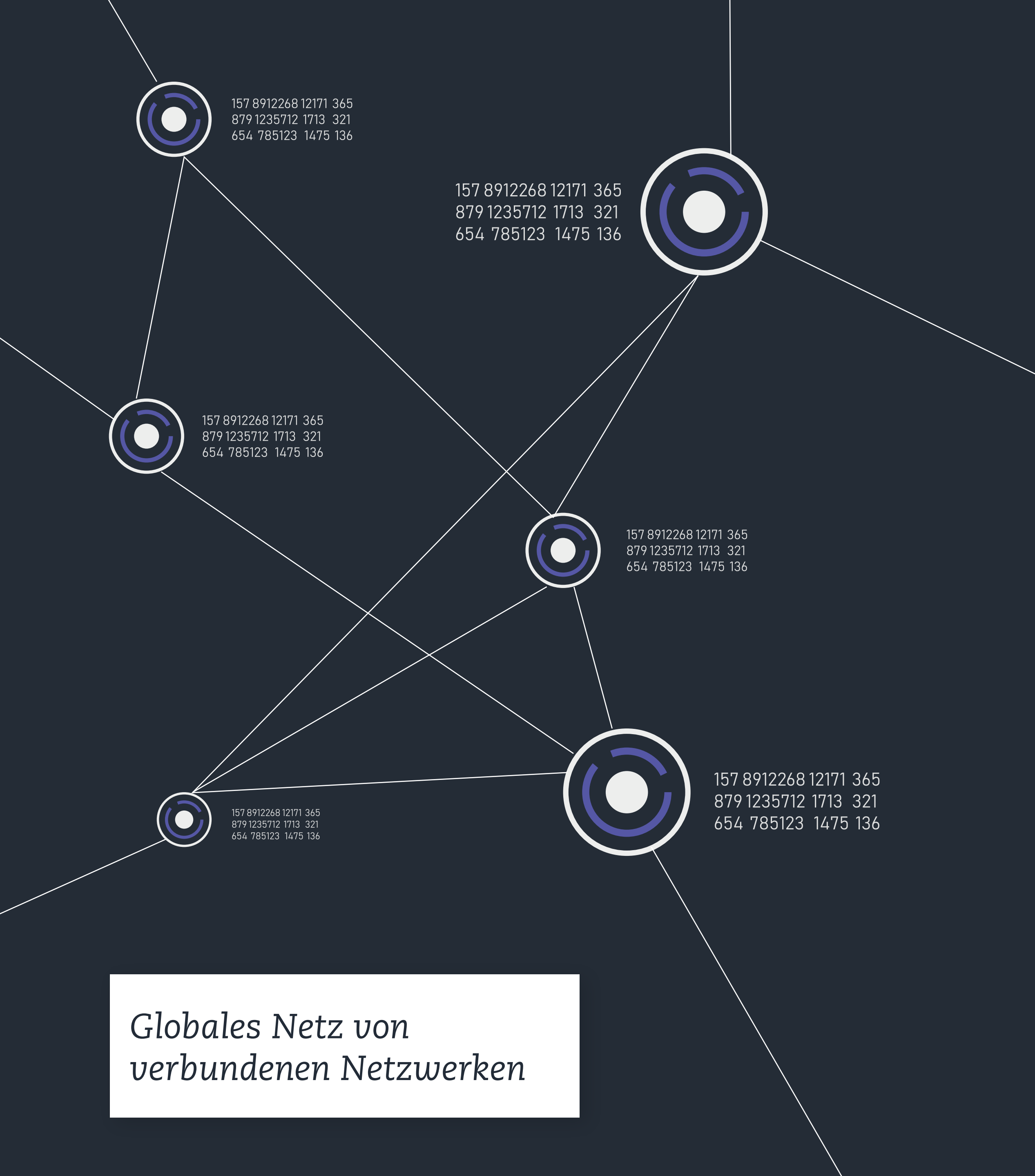
Mit „digitaler Zahnarztpraxis“ verbinden die Zahnärzte gleich digitale Abformung und alles weitere, was mit zahnärztlicher Tätigkeit und der damit verbundenen Technik zu tun hat.

Gliederung: Einführung in die Informatik – Grundlagen

Wer es selber weiß, der muß es anderen nicht glauben!

Ziele

Grundlagen schaffen für eigenständige Entscheidungen schaffen und Abhängigkeiten reduzieren und Selbstbewusstsein bei IT-Fragen stärken



*Das Internet –
Ein globales System
aus miteinander
verbundenen
Computer-netzwerken.*

*Globales Netz von
verbundenen Netzwerken*

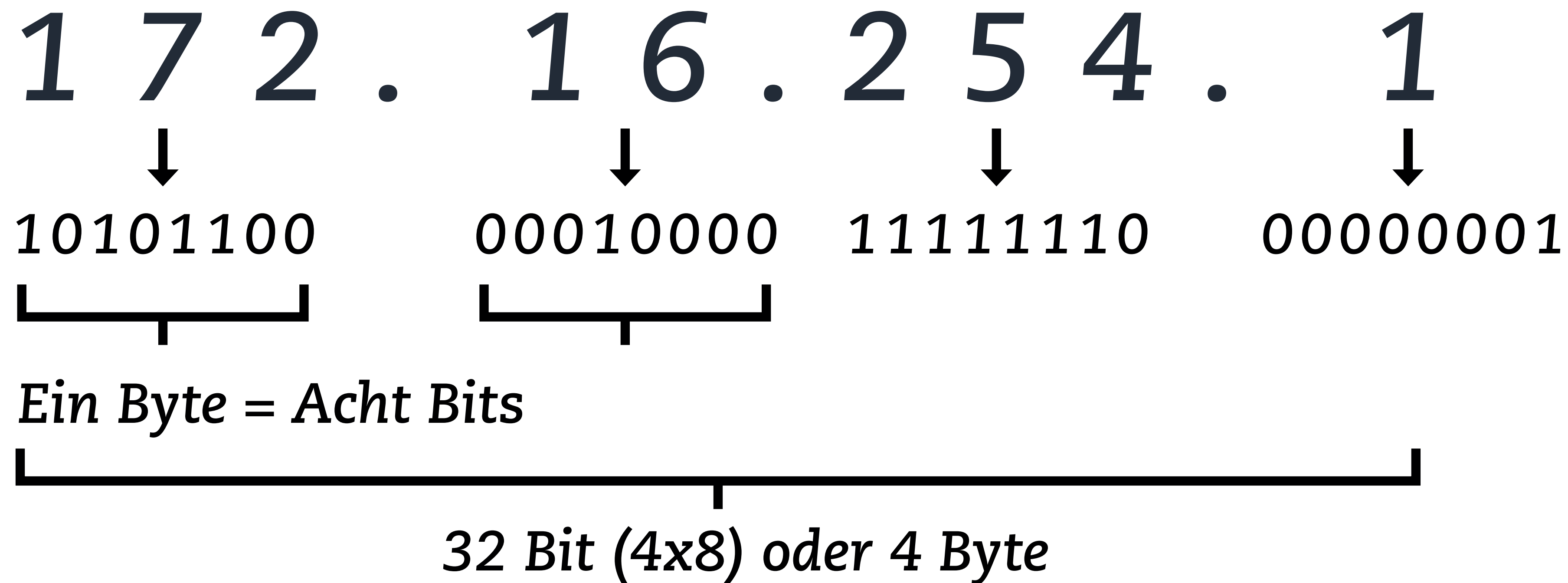
www.imedent.de

Zur Kommunikation wird eine einheitliche Sprache (Protokolle) benötigt.

IP und TCP - Die Superstars

IP ist das bekannteste und am meisten verbreitete Protokoll der Internet-schicht und bildet zusammen mit TCP die Grundlage des Internets. In einem IP-Netzwerk werden die Endgeräte im Netzwerk per IP-Adresse eindeutig adressiert (angesprochen).

Mit der IP-Adresse kann jemand eindeutig indentifiziert werden?



*Sie setzt sich zusammen aus
Netzteil, Hostteil*

IPv4 Adresse

1 7 2 . 1 6 . 2 5 4 . 1 / 1 6

Der *Netzanteil* identifiziert ein *Teilnetz*, der *Hostanteil* identifiziert ein Gerät (Host) innerhalb eines Teilnetzes.

1 7 2 . 1 6 . 2 5 4 . 1 / 1 6

00001010.00101011.00001000.01000000
= 10.43.8.64

$0 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3$
= 2 + 8 = 10

$1 \cdot 2^0 + 1 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3$
+ $0 \cdot 2^4 + 1 \cdot 2^5 = 1 + 2 + 8 + 32 = 43$

= 8

= 64

Die technische

Darstellung der

IP-Adressen ist binär ...

00001010.00101011.

00001000.01000000 =

10.43.8.64

Darstellung der IPv4
Adresse am Rechnerbeispiel



*... und damit ist (IPv4)
endlich. Die neue
Lösung ist IPv6.*

$2^{32} =$
4294967296 max. Anzahl

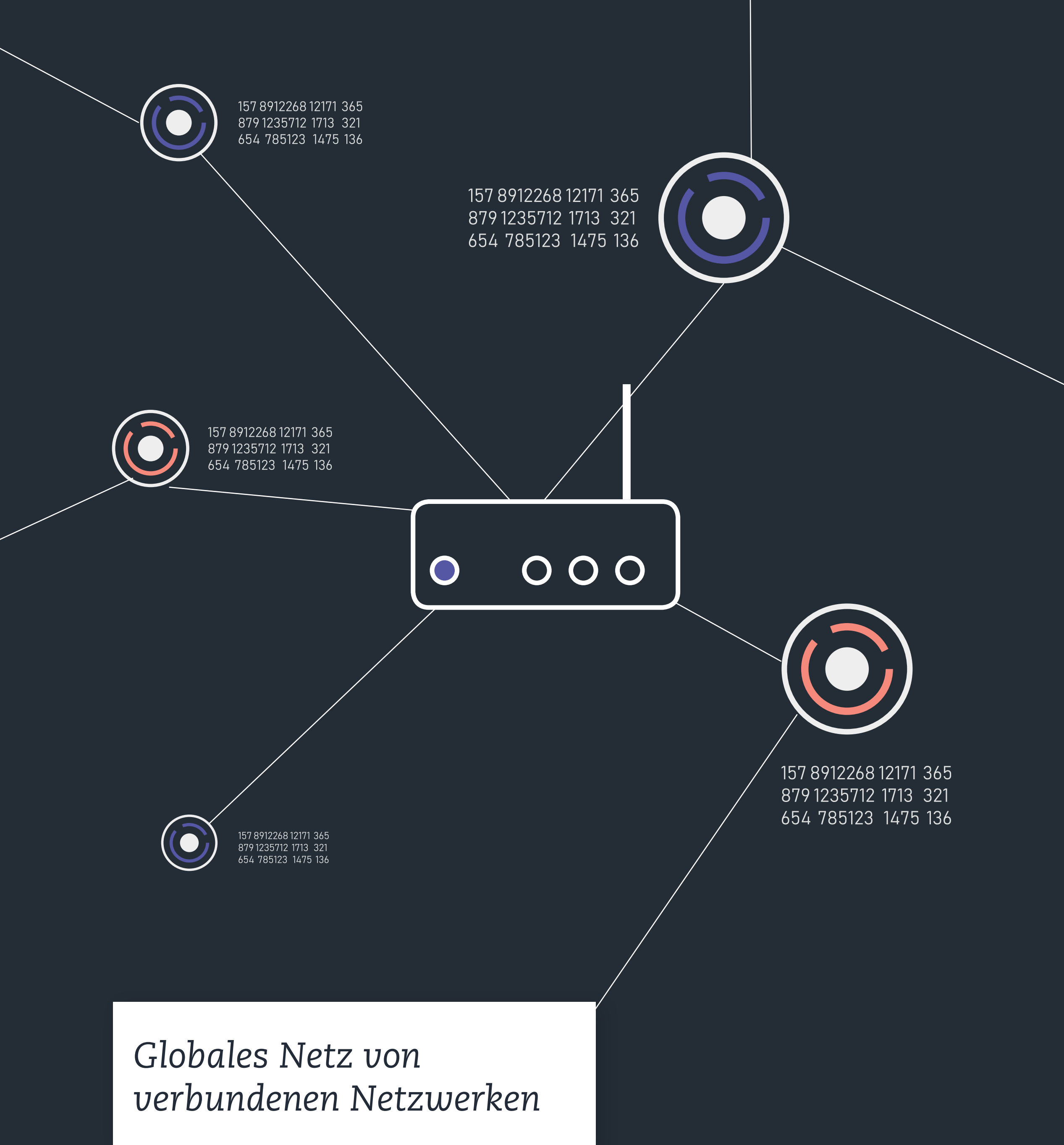
$2^{128} = \text{max. Anzahl}$
ipv6 $\approx$ 340 Sextillionen

*Die genaue Aufteilung zwischen
Netzanteil und Hostanteil wird
durch eine Subnetzmaske festgelegt*

1 7 2 . 1 6 . 2 5 4 . 1
2 5 5 . 2 5 5 . 2 5 5 . 0

IP-Adressen und Netze

Netzklasse	Adressbereich	Netzmaske	Netze / Adresse
Klasse A	10.0.0.0 bis 10.255.255.255	255.0.0.0. (/ 8)	1 / 16.777.216
Klasse B	172.16.0.0 bis 172.31.255.255	255.255.0.0. (/ 16)	16 / 65.536
Klasse C	192.168.0.0. bis 192.168.255.255	255.255.255.0. (/ 24)	256 / 256



*Soll eine Kommunikation
zwischen verschiedenen
Netzen oder
Subnetzen stattfinden,
wird ein Router benötigt.*

Router: Geräte die den Datenstrom transportieren

Für jedes teilnehmende Gerät vergibt der zuständige Administrator den Hostanteil eindeutig. Den Netzanteil vergibt der Besitzer oder Planer des Netzwerks.

Im Internet ist die *IANA (Internet Assigned Numbers Authority)* für die Vergabe der Netzanteile zuständig.

Routing

IPv4 unterscheidet nicht zwischen Endgeräten (Hosts) und Vermittlungsgeräten (Router). Jeder Computer und jedes Gerät kann gleichzeitig Endpunkt und Router sein. Ein Router verbindet dabei verschiedene Netzwerke. Die Gesamtheit aller über Router verbundenen Netzwerke bildet das Internet.

Routinggtabelle

IPv4-Routing-Tabelle								? X	
IP-Adresse	Netzmaske	Tag	Schaltzustand	Router	Distanz	Mask.	Kommentar	OK	
192.168.2.0	255.255.255.0	0	An, sticky für RIP	DENTIKA-1781VAW	0	Aus		Abbrechen	
192.168.3.0	255.255.255.0	0	An, sticky für RIP	ZAPRS-OST	0	Aus			
192.168.4.0	255.255.255.0	0	An, sticky für RIP	ZAPRS-WEST	0	Aus			
192.168.6.0	255.255.255.0	0	An, sticky für RIP	VISIODENT	0	Aus			
192.168.8.0	255.255.255.0	0	An, sticky für RIP	192.168.10.5	0	Aus			
192.168.15.0	255.255.255.0	0	An, sticky für RIP	ZAPRS-NORD	0	Aus			
192.168.100.0	255.255.255.0	0	An, sticky für RIP	192.168.10.5	0	Aus			
192.168.178.0	255.255.255.0	0	An, sticky für RIP	ZAPRS-DD-SUED	0	Aus			
192.168.200.0	255.255.255.0	0	An, sticky für RIP	ZAPRS-ZEITHAIN	0	Aus			
192.168.0.0	255.255.0.0	0	An, sticky für RIP	0.0.0.0	0	Aus	block private networks: 192.168.x.y		
172.16.0.0	255.240.0.0	0	An, sticky für RIP	0.0.0.0	0	Aus	block private networks: 172.16-31.x.y		
10.0.0.0	255.0.0.0	0	An, sticky für RIP	0.0.0.0	0	Aus	block private network: 10.x.y.z		
224.0.0.0	224.0.0.0	0	An, sticky für RIP	0.0.0.0	0	Aus	block multicasts: 224-255.x.y.z		
255.255.255.255	0.0.0.0	2	An, sticky für RIP	T-COMPCO	0	An	Voice		
255.255.255.255	0.0.0.0	1	Aus	HLKOM	0	An			
255.255.255.255	0.0.0.0	0	An, sticky für RIP	INTERNET	0	An			

QuickFinder

Default-Route

Hinzufügen...

Bearbeiten...

Kopieren...

Entfernen

Routing nur über IP

Beim Routing über IP können:

einzelne Pakete verlorengehen,
Pakete doppelt beim Empfänger ankommen,
Pakete verschiedene Wege nehmen,
Pakete fragmentiert beim Empfänger ankommen.

Wir benötigen **TCP**.

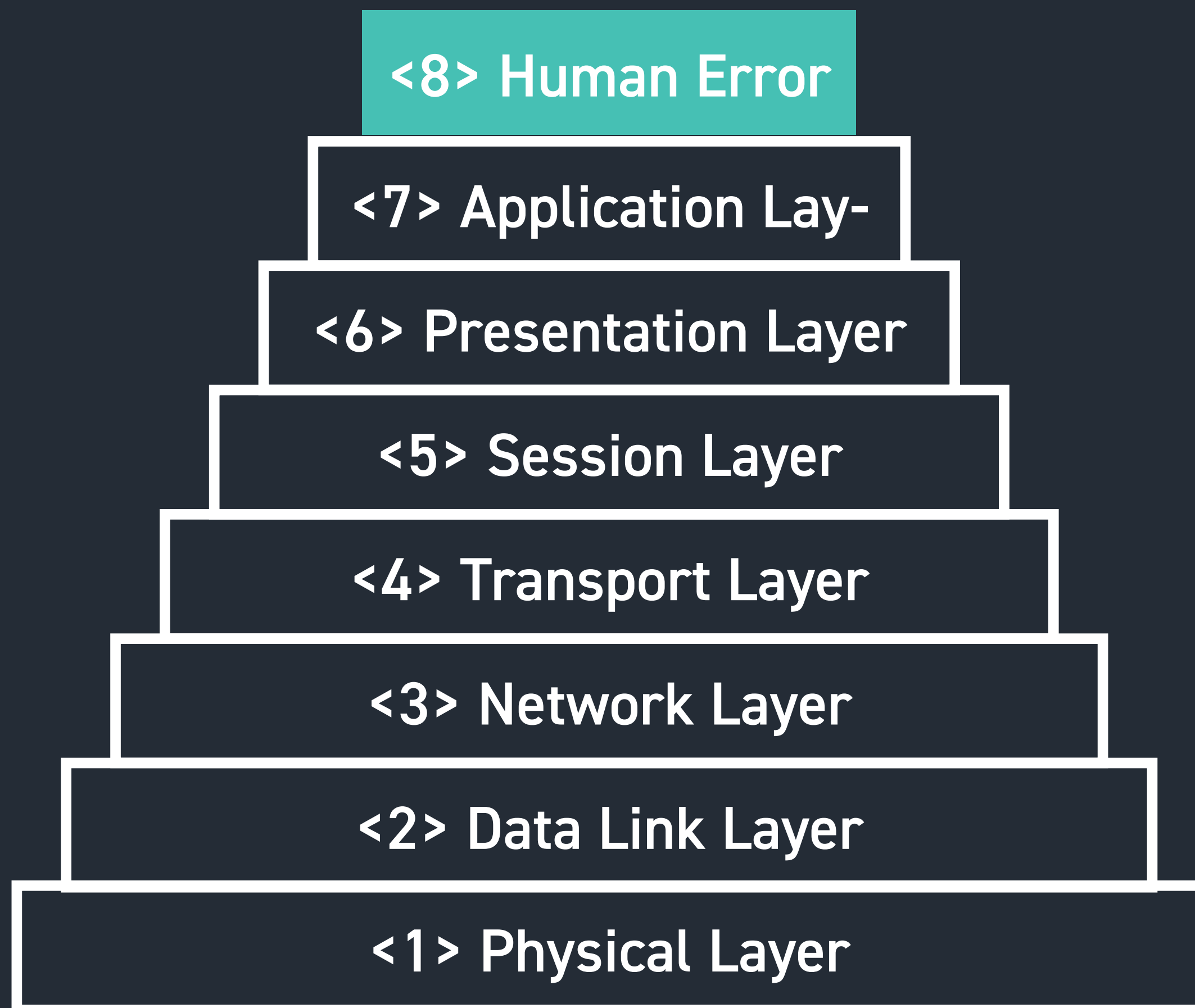
Zur Erinnerung: **TCP und IP Bilden ZUSAMMEN die Grundlage des Internets**

TCP / IP – Das Dreamteam

Wird TCP auf IP aufgesetzt (d. h. die Daten jedes IP-Pakets enthalten ein TCP-Paket, aufgeteilt in TCP-Header und Daten), so wird neben dem Aufheben der Längenbeschränkung auch der Paketverlust durch Wiederholung korrigiert.

Doppelte Pakete werden erkannt und verworfen.

Die Kombination TCP mit IP stellt dabei eine zuverlässige bidirektionale Verbindung eines Datenstroms dar.



Das OSI-Schichten-Modell
„Open System Interconnection“

Im OSI-Modell wird
beschrieben, welche
Voraussetzungen
gegeben sein müssen,
damit verschiedene Netz
werkkomponenten
miteinander
kommunizieren können.

Versand eines Datenpaketes von Leipzig in die USA

```
Routenverfolgung zu facebook.com [185.60.216.35]  
über maximal 30 Hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.100.254
2	<1 ms	<1 ms	<1 ms	192.168.10.2
3	1 ms	1 ms	<1 ms	217.6.134.81
4	1 ms	1 ms	<1 ms	87.190.86.189
5	7 ms	6 ms	7 ms	217.0.197.229
6	7 ms	7 ms	6 ms	62.157.251.102
7	5 ms	6 ms	5 ms	po161.asw02.fra5.tfbnw.net [204.15.21.28]
8	5 ms	6 ms	5 ms	po241.psw03.fra5.tfbnw.net [157.240.43.59]
9	7 ms	6 ms	6 ms	173.252.67.143
10	5 ms	5 ms	5 ms	edge-star-mini-shv-01-frx5.facebook.com [185.60.216.35]

```
Ablaufverfolgung beendet.
```

Intern oder Extern? Private Adressen werden im Internet nicht geroutet.

Wird ein Datenpaket von einem Host gesendet, prüft das IP Protokoll, ob das Datenpaket für den lokalen Host, für das eigene Netzwerk bestimmt ist oder ein für ein entferntes Ziel bestimmt ist.

Statistik: So viel Verkehr haben wir

Der Datendurchsatz hat im September 2012 erstmals die Marke von **2 Terabit pro Sek.** überschritten, im Dezember 2017 über **6 Terabit pro Sek.** Laut Website besitzt DE-CIX derzeit eine angeschlossene Kundenkapazität von über **22 Tbit/s**.

Name	Symbol	Anzahl Bytes
Kilobyte	kB[G 2]	1 000 = 10^3
Megabyte	MB	1 000 000 = 10^6
Gigabyte	GB	1 000 000 000 = 10^9

DNS: Domain Name System

Da IP-Adressen schwer zu merken sind und zudem wechseln können entstand die Idee anstelle von Zahlenblöcken Namen zu verwenden.

*194.15.233.249 =
zahnaerzte-in-sachsen.de*

Der Root-Server

Weltweit gibt es 13 Server, die DNS Einträge verwalten. Beim Besuch eines Dienstes im Internet wird noch eine DNS-Auflösung angefragt.

Kritik

- DNS ist unsicher
- Computer merken sich DNS Einträge im Cache
- bei Fehlern im Internet hilft häufig DNS-Cache leeren

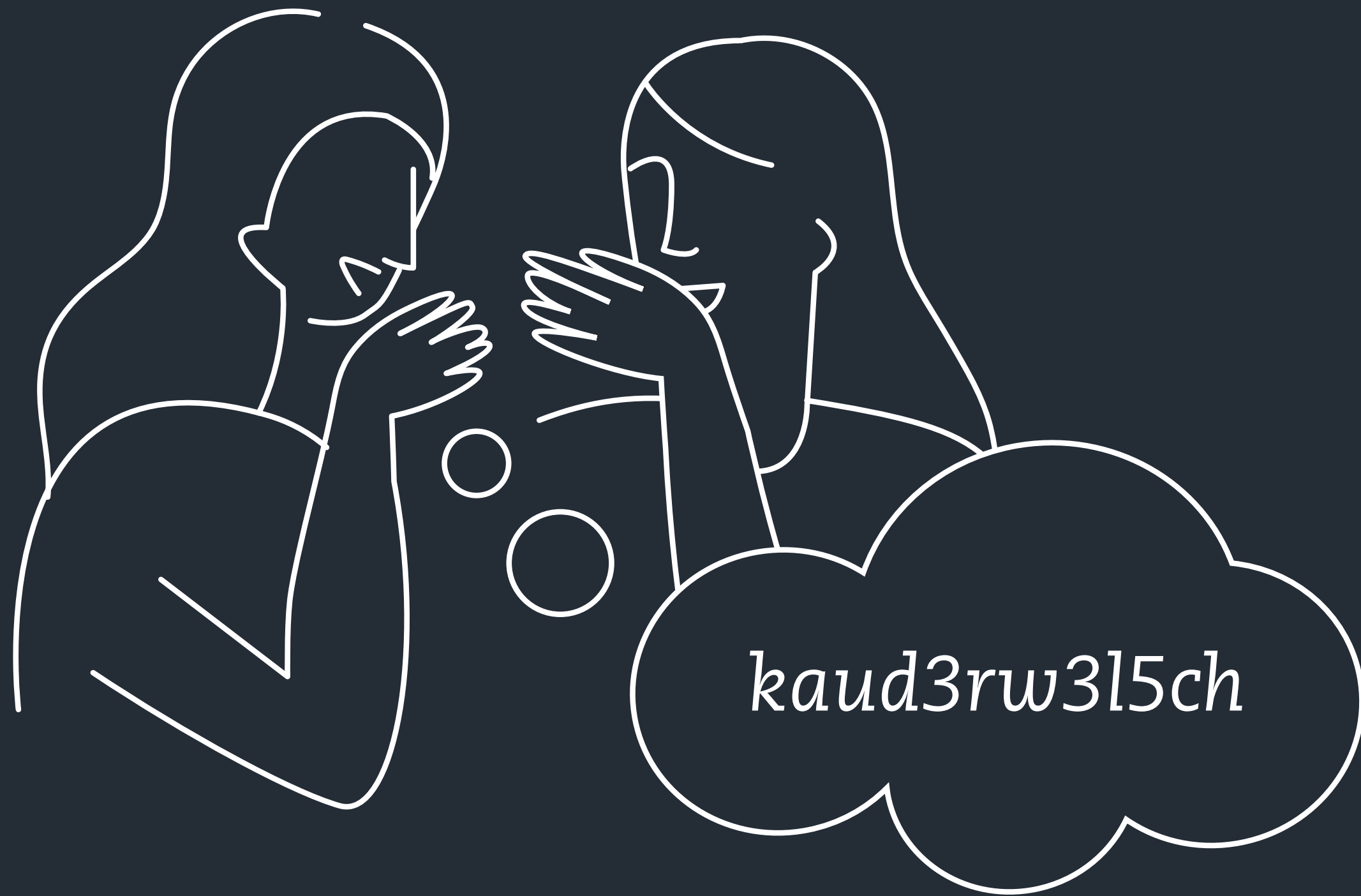
Die Verschlüsselung

Per se ist alles im Internet für jeden frei zugänglich und offen.

Soll eine sichere digitale Kommunikation zwischen Nutzern erfolgen ermöglicht dies eine Verschlüsselung. Die Verschlüsselung ist also nicht anders als ein Geheimnis zwischen zwei Nutzern.

Kritik

Verschlüsselung ist kein Allheilmittel und garantiert keine vollkommene Sicherheit.



Der Idealfall :

Zwischen Nutzer A und

Nutzer B wird ein

Geheimnis vereinbart.

Das "Geheimnis" wird

technisch übersetzt als

"Verschlüsselung".

Pretty Good Privacy (PGP; engl.
„ziemlich gute Privatsphäre“)

*Der öffentlicher Schlüssel dient
allen zum Verschlüsseln.
Der privater Schlüssel dient zum
Entschlüsseln.*

Nur der "Geheimnisträger" kann Entschlüsseln -> Solange der privater Schlüssel nicht gestohlen wird gilt er als eine eindeutige Identifikation.

Kommunikationsbeispiel:

01. Eine verschlüsselte Nachricht wird verschickt. Der Sender fordert eine Kopie des öffentlichen Schlüssels beim Empfänger der Nachricht an.
02. Eine geeignete Software verschlüsselt die Nachricht an den Empfänger mit dessen öffentlichem Schlüssel.
03. Die Nachricht wird verschickt und sieht für Außenstehende auf den ersten Blick aus wie „**kaud3rw3l5ch**“ „**kauderwelsch**“
04. Der Empfänger entschlüsselt die Nachricht mit einer Kombination aus öffentlichem und privatem Schlüssel.

Öffentlicher Schlüssel

```
0x861993459AC81DC8.asc - Editor
Datei Bearbeiten Format Ansicht Hilfe
|-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBE/5WgUBCAdoOH71oZ161TPC4w8PLhRo6Muo9CGIGIM6SSIIyYA5xM8H/jde1
5cKxeOUVp71XcWt06gUYw7ogtqaKrF9RdN3eUPtV08/kmHZ71BXyhtTF2SQB11Jo
W38e2sfa1xc9z63jk+Jn5U2er8721nrFS6Yt6jY+EBKOiEhH/xF66jLRBp84X+L2
fOyoSu137GFym+8+h3W0RgmR+fma7Uk0jqy2z60EW+ROqSf2s410TNmJzzTEZpxI
1fao9wf/oSbQNYH1u6hRFt02SFT4toNTdF0mEMYjCzzinGdSXkFhruE67Ia09z+S
GESqUYGccBXYRH9hrh06RGMe2Y7qZZUSCeQhABEBAAG0Jk9saXZ1ciBMdWJ1Y2tp
IDxvbG12ZXJfbHVhZWNraUBnbXguZGU+iQE+BBMBAgAoAhsjBgsJCACDAgYVCAIJ
CgsEFgIDAQIEAQIXgAUCWlt6kwUJDISHjgAKCRCGGZNFmsgdyOy+B/9Y18j484pz
PdZe/evWohh830uHKwQkxj4RAXFk9xNzBlmK4WnctYDTbMSjGuAwxdcdmy/uzr+
L/8xqqxf9K6XLb8xNAInEbkySvFXxMh+rCRMqQwiqVtoFavFMHKeU0dt3E/VgRk6
QTzapofhQZ12PfI12/Lo23FtDLuS/wzKJXHFCfDJvJfB+6S9k9n8XY8pQ4aaUKlu
9KwBViSe1wiEkkzInCt2PmF+WQT88d3CtrWQR1Eehd0bAy2agIqq/DpeH96q50nR
qK4Ka2rwAPHJ9bBqv5kCcgoiylCI9Ad1YOYDxid+PJt498/GGmcusgiXP7zzyUvB
wC1KLUBJoUOXuQENBE/5WgUBCACknm6CT55PALdwrFgyCIb1GQ5geWY27ylaX35v
YB2SdE2+Zi2vdz3YfPn+Nuy/WSV+3IiXPF7Lnn0gWkIRt1kmwkT1u6b0e0kzK/H
nv2GHhPmxQCtMff4x22REIsMwfn57zbDABuAbloTHPwurS11ToWvDX/7xcNAfcQY
TMjOwHMW51eBymxAlSy0u1RspvEmrPdSa2sd7gytibmodsbqk4YsJhtnCr00ipcw
gdoSvGJR3bZP+YOYP57Y456KYTVS1iW/7dsbNN9tJQY6g6gbUFmwAU7EPsQtzkSo
aOYNCivHtRKrcV7rLYUI+3a3jH+UkNECz8j6rcTTDidzJ62PABEBAAGJASUEGAEC
AA8CGwwFAlpbepMFCQ4kh44ACgkQhnmTRZrIHci5oQgAh4D1MwKKBibeWhQuXg3a
LBzgTMPuTmdI7u0HscjvQqfQREJHaK11NYggUnOj4PNKFcYfCPz0dzvtGp2Xe5E0
faoZhdplzIc6v7zNI/HW+sFBzZV+f9iKA9YqkP2JHw3MkPsz09uvsyDXLknbpXqk
4P7KhZmiraw5Ue/VnwFxI4nc+Zb7KuZQX1JctmE4pZg00e960459NkD3Q0scSKD
2wn97d1Kd2xSDEfeIJ42At9hnM3x0LYdRrKmkBkVHFAX0giK2eE1EUovOT560R31
7FM7I5g53uz5ie/uo8XdyGtIop7RUZj2n5zFwUuy71utaskEYUGU2Yf/ZLbBGhaw
4w==
=S/yn
-----END PGP PUBLIC KEY BLOCK-----
```


Verschlüsselung im Alltag

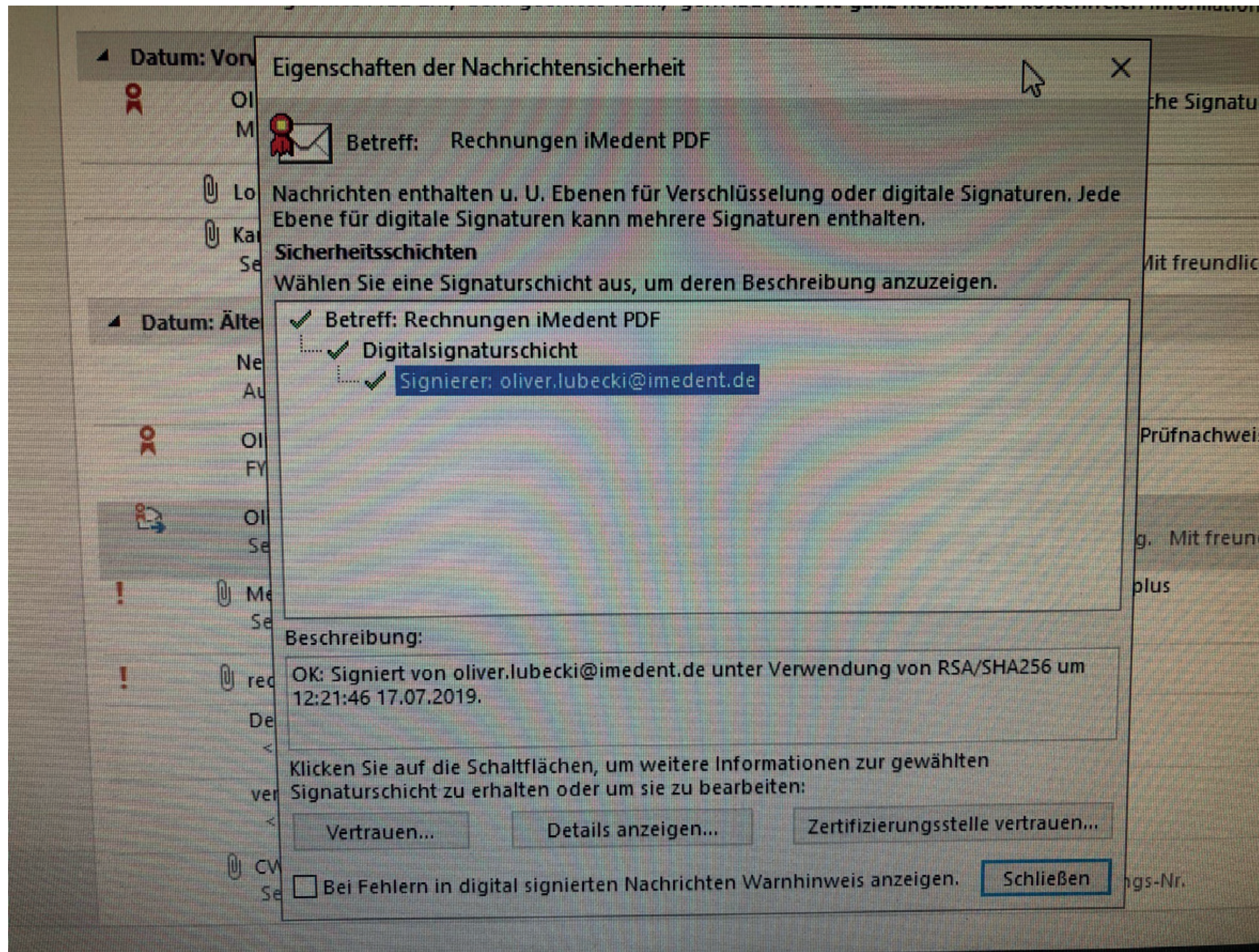
- Private und staatliche Unternehmen übernehmen die Hoheit über die privaten Schlüssel.
- Es gibt einen Aufbruch der Ende-zu-Ende Verschlüsselung
- In Deutschland gibt es ein staatliches Institut zum knacken von Verschlüsselung: ZITiS (Zentrale Stelle für Informationstechnik im Sicherheitsbereich)

Verschlüsselung im Alltag

Kritik

- Es wird zunehmend eine BackDoor für staatliche Behörden zum Aufbruch der Verschlüsselung gefordert.
- In anderen Staaten ist eine Backdoorf staatlich verordnet -
US Patriot Act - im Zuge des Krieges gegen den Terror - heute USA Freedom Act

Verschlüsselung im Alltag

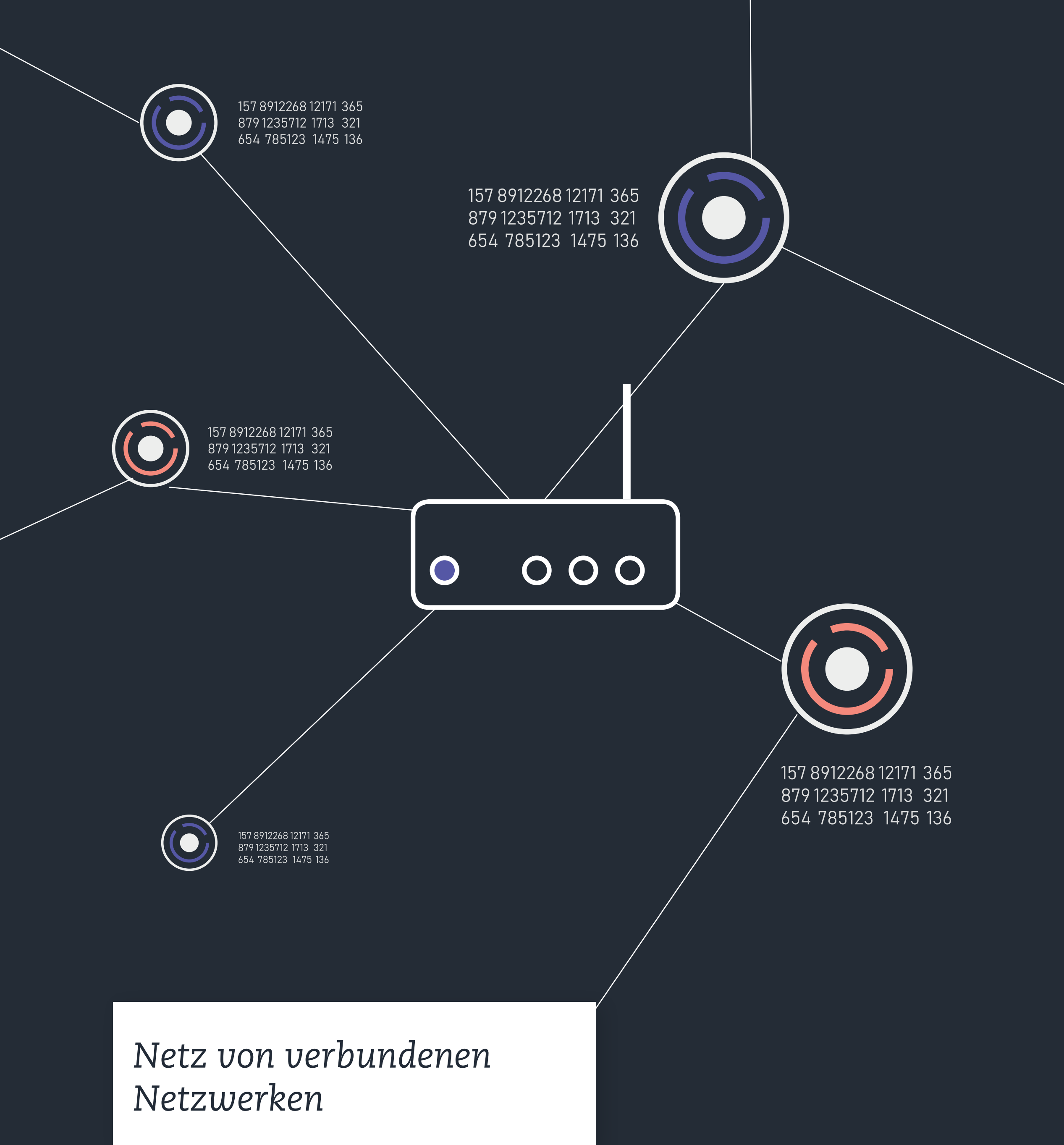


PAUSE!



Zusammenfassung: Wir wissen jetzt

- Was ist ein Netz und Was ist eine IP-Adresse
- Wie wird kommuniziert
- Es gibt unterschiedliche Protokolle
- wir sollten verschlüsseln



Wie baue ich ein sicheres Praxis-Netzwerk?

- Die Informatik dient nur als eine Art Hilfswissenschaft. Wir bilden mit ihr nur die organisatorische Gegebenheiten ab.
- Nehmen Sie sich Zeit für d Planung für ihre Praxis IT
- Organisation geht vor beliebiger Reaktion

Organisation - Netzwerkgröße

Wichtige Fragen

- Wie groß wird / ist meine Praxis?
- Hat meine Praxis mehrere Standorte?
- Arbeite ich von zu Hause aus?
- Ist meine Praxis dauerhaft am Internet angeschlossen?

Organisation - Netzwerkgröße

Client-IP-Adresse	Name	Leaseablaufdatum	Typ	Eindeutige ID
 192.168.8.111	S850A-GO.sachsen-praxen.local	13.09.2019 02:22:06	DHCP	7c2f80fcb53b
 192.168.8.159	server.sachsen-praxen.local	12.09.2019 03:19:56	DHCP	005056945ab3
 192.168.8.194	ZAPRS-Buro3.sachsen-praxen.local	13.09.2019 07:40:52	DHCP	704d7b270315
 192.168.8.186	ZAPRS-UKuls.sachsen-praxen.local	13.09.2019 13:34:29	DHCP	6c0b84b03930
 192.168.8.162	zaprsvm01.sachsen-praxen.local	09.09.2019 17:40:24	DHCP	005056946c7f
 192.168.8.163	zaprsvm02.sachsen-praxen.local	13.09.2019 04:10:08	DHCP	00505694801b
 192.168.8.164	zaprsvm03.sachsen-praxen.local	10.09.2019 04:11:07	DHCP	00505694550a
 192.168.8.165	zaprsvm04.sachsen-praxen.local	10.09.2019 04:01:59	DHCP	005056948a27
 192.168.8.166	zaprsvm05.sachsen-praxen.local	10.09.2019 04:03:48	DHCP	005056946509
 192.168.8.167	zaprsvm06.sachsen-praxen.local	13.09.2019 04:07:04	DHCP	00505694678c
 192.168.8.168	zaprsvm07.sachsen-praxen.local	13.09.2019 04:03:04	DHCP	005056942a82
 192.168.8.169	zaprsvm08.sachsen-praxen.local	12.09.2019 04:09:54	DHCP	00505694b19a
 192.168.8.170	zaprsvm09.sachsen-praxen.local	13.09.2019 04:13:45	DHCP	005056940f2b
 192.168.8.171	zaprsvm10.sachsen-praxen.local	10.09.2019 04:16:06	DHCP	005056941c02
 192.168.8.172	zaprsvm11.sachsen-praxen.local	13.09.2019 04:10:48	DHCP	005056942ee4
 192.168.8.173	zaprsvm12.sachsen-praxen.local	13.09.2019 10:56:07	DHCP	00505694b4e4
 192.168.8.174	zaprsvm13.sachsen-praxen.local	11.09.2019 17:26:17	DHCP	00505694bcb3
 192.168.8.175	zaprsvm14.sachsen-praxen.local	12.09.2019 14:32:16	DHCP	005056943556
 192.168.8.176	zaprsvm15.sachsen-praxen.local	12.09.2019 14:33:35	DHCP	00505694067d
 192.168.8.153	ZAPRS-VM16.sachsen-praxen.local	12.09.2019 14:33:52	DHCP	0050569f202f
 192.168.8.154	ZAPRS-VM17.sachsen-praxen.local	12.09.2019 14:34:08	DHCP	0050569fda96
 192.168.8.155	ZAPRS-VM18.sachsen-praxen.local	12.09.2019 14:34:11	DHCP	0050569f0a0a
 192.168.8.156	ZAPRS-VM19.sachsen-praxen.local	13.09.2019 04:01:56	DHCP	0050569f8a43
 192.168.8.157	ZAPRS-VM20.sachsen-praxen.local	10.09.2019 04:14:05	DHCP	0050569f5ea0
 192.168.8.158	ZAPRS-VM21.sachsen-praxen.local	13.09.2019 06:05:59	DHCP	0050569fd9dd
 192.168.8.160	ZAPRS-VM22.sachsen-praxen.local	09.09.2019 15:53:27	DHCP	0050569f5df4

Organisation - Netzwerkgröße

- jedes Gerät bekommt eine Adresse
- Drucker, Telefone, Tablets, EC, Telematik, Pads, Behandlungseinheiten, Röntgen, Sterilisation, Kameras, Computer, Telefone, Musik, TV-Geräte usw.
- Netzwerke werden schnell viel größer als ursprünglich gedacht -> THINK BIG

Organisation - Teilnehmer im Netzwerk

Wer sind die Eigentümer?

- Ärzte, Verwaltung und Office, Fachangestellte
- Azubis, Praktikanten ACHTUNG auch Minderjährige!
- externe (Steuerberater, Techniker, Depots, Administrator)

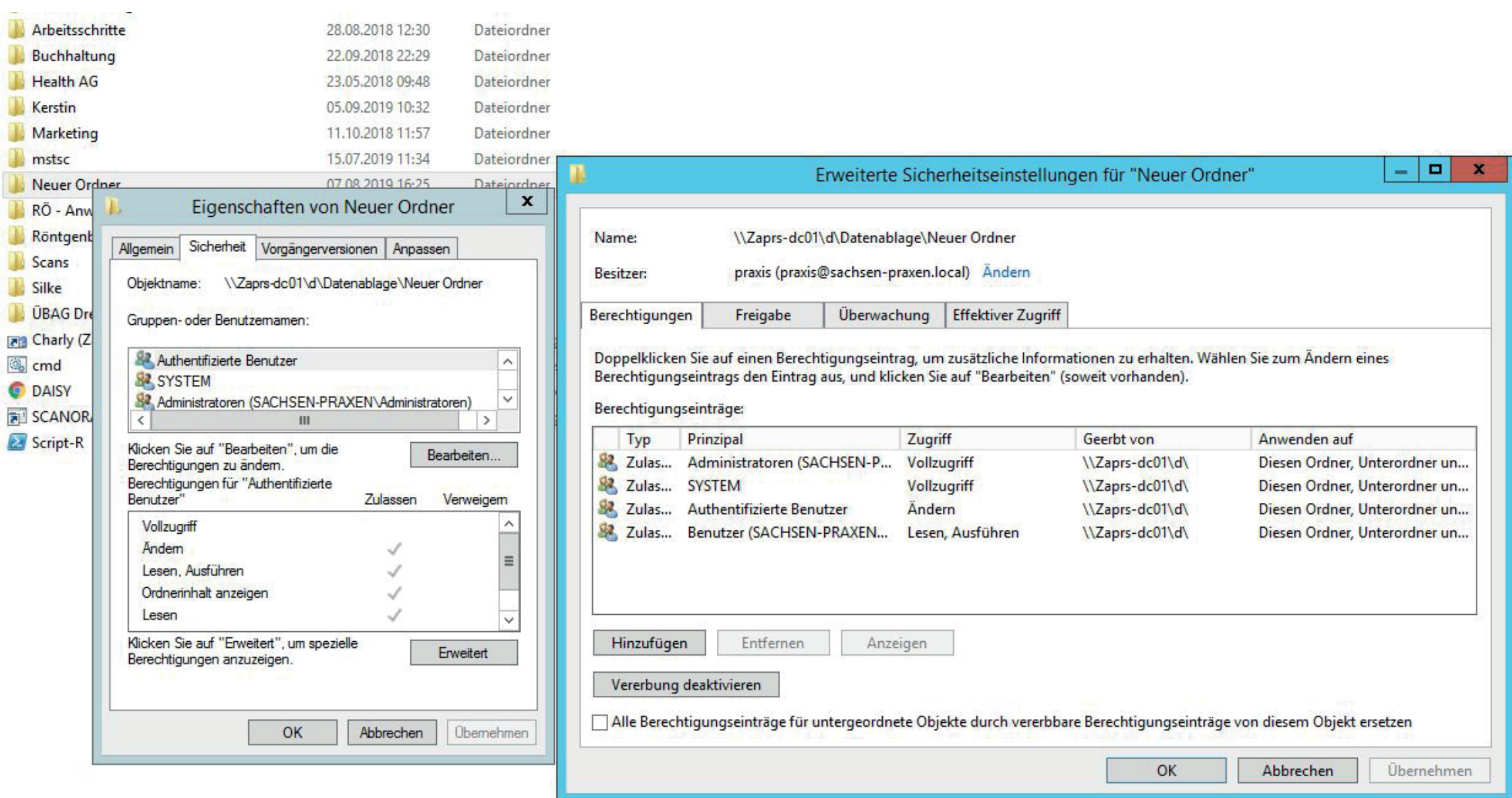
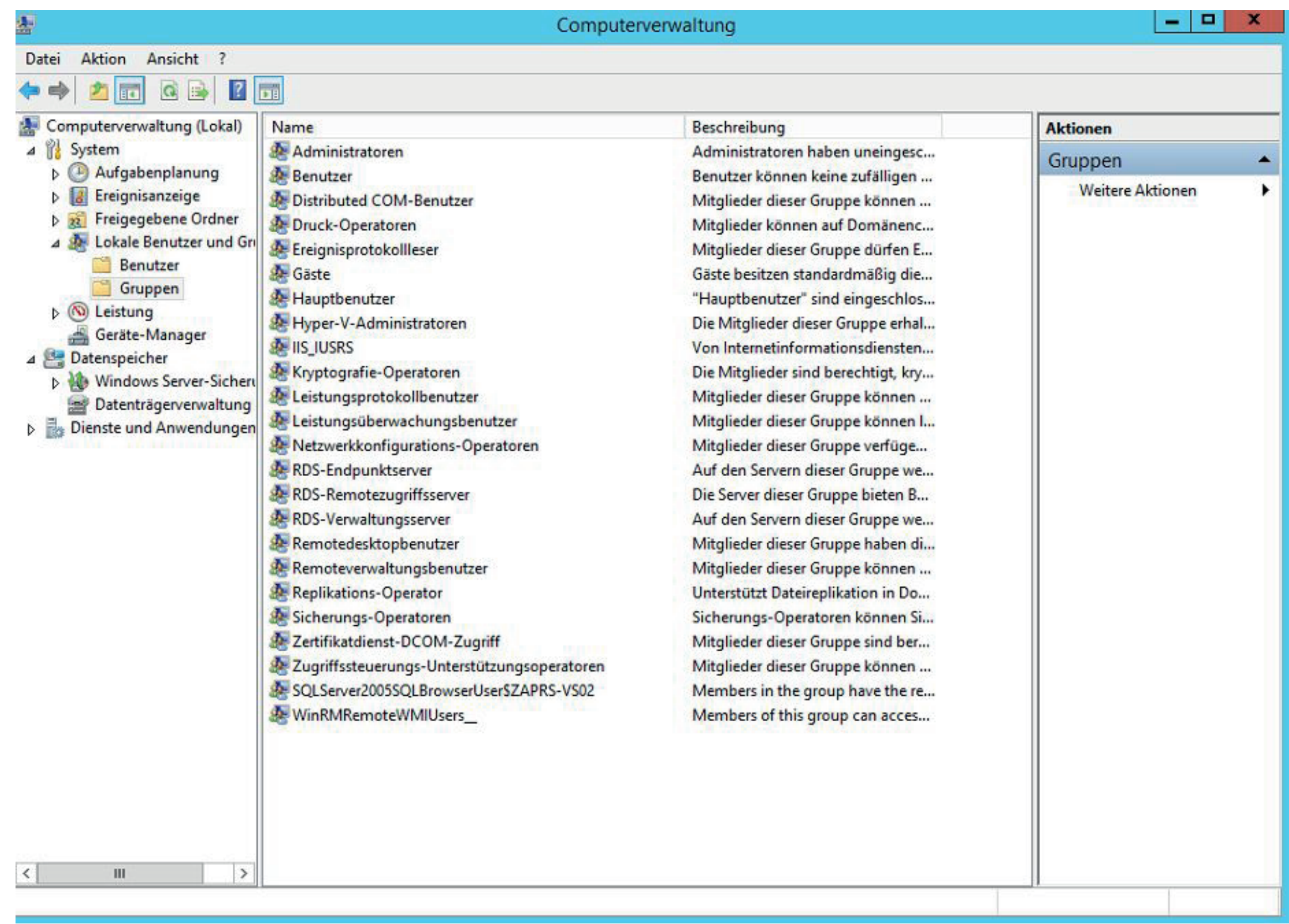
Organisation - Vom Allgemeinen ins Spezielle

- Gruppen anlegen!
- Nutzer werden Gruppen zugeordnet
- Gruppen erhalten im Netzwerk zukünftig Rechte etwas zu tun
- vom Allgemeinen ins Spezielle planen

Organisation - Gruppen & Nutzerrechte

- es wird nur das erlaubt was gebraucht wird
- es gibt keine JEDER darf alles Rechte
- alles wird verboten bis es ist etwas erlaubt
- größte Gefahr im Praxis Alltag!

Gruppen & Nutzerrechte



Organisation & Netzwerkplanung am Beispiel einer Mehrbehandlerp.

- Server / Netzwerkinfrastruktur / NAS samt WLAN
- Computer / Röntgen und dentale Komponenten / QM
- Peripherie / Drucker / Scanner / (Telematik) / Telefon / EC
- Homeoffice / Gäste und sonstige

Organisation & Netzwerkplanung am Beispiel einer Mehrbehandlung.

- kontrollierter Datenverkehr zwischen den Teilnetzen durch explizite Regeln (Protokolle)
- es wird nur das erlaubt, was benötigt wird der Rest ist verboten
- Zuarbeiten der Verantwortlichen mit in die Dokumentation aufnehmen

Organisation & Netzwerkplanung - Die Firewall



Die Firewall lässt sie nicht
im Regen stehen

Firewall - Lässt Sie nicht im Regen stehen

#	Quelle	Ziel	Dienst	NAT	Aktion	Aktiv	
7	 internal-network	 internet	 default-internet	 HN	ACCEPT		 
8	 internal-network	 internal-interface	 proxy		ACCEPT		 
22	 internal-network	 internet	 network-time	 HN	ACCEPT		 
37	 internal-network	 internet	 Alarmanalge	 HN	ACCEPT		 
19	 internal-network	 internet	 elster	 HN	ACCEPT		 
23	 internal-network	 internet	 ssh	 HN	ACCEPT		 
36	 internal-network	 internet	 Teamviewer	 HN	ACCEPT		 
38	 internal-network	 internet	 Dropbox	 HN	ACCEPT		 
44	 internal-network	 internet	 GlS_Smartclient_tcp	 HN	ACCEPT		 
45	 internal-network	 internet	 lancom	 HN	ACCEPT		 
46	 internal-network	 internet	 Testo_Datenlogger	 HN	ACCEPT		 

Organisation - Gruppen und Rechte

Windows Firewall schützt nicht ausreichend, zudem ist sie häufig deaktiviert

Kritik

- Alltag: bei einem Problem ist immer die Firewall schuld
- Alltag: alles muss erlaubt sein
- Benutzerkontensteuer ist häufig deaktiviert

Organisation - Gruppen und Rechte

- Abstufung zwischen: Administrator und Nutzer
- sonstige externe Dienstleister werden als solche angelegt und erhalten die Rolle Administrator
- strikt und streng, lieber zu wenig als zu viel
- mit Vererbungen arbeiten

Organisation - Internet

Der Router ist die Schnittstelle zwischen interne Praxis Netz und dem Internet, sparen Sie nicht an ihm. Denn, wenn am Router gespart wird müssen die Funktion auf andere Geräte ausgelagert werden. ***Ihre Praxis ist ein Unternehmen und kein Privatgebrauch, der Router sollte dem entsprechen!***

- im Idealfall wird am Router schon gefiltert
- klare Empfehlung: besser als Fritzbox!

Organisation - Internet-Protokolle

- welcher Datenverkehr muss aus welchem Netz in welches Netz
- Whiteliste oder Blacklist-Ansatz
- auf Spezial Dienste achten
- höchste Gefahr im Alltag geht von Mail-Protokollen aus

Organisation - Schutz vor unerwünschten Programmen

- eine Firewall kann die bewusste oder unbewusste Aktion eines Menschen nicht verhindern
- manipulierter und kompromittierter Internetverkehr
- Schutz durch ein Programm welches nach verdächtigen Code und/oder verdächtigen Verhalten sucht / Antivirenprogramm
- keine Ausnahmen akzeptieren (Softwarehersteller, Röntgen, Depot)

Technische Maßnahmen

- US Freedom Act und die sog. 5 Eyes
- Empfehlung deutsche Hersteller bevorzugen
- ein gutes Programm ist nutzlos bei schlechter Konfiguration
- saubere Planung schützt vor großer Nacharbeit

Der Server

- zentrales Organ in der Praxis
- spezielles Betriebssystem
- kein regulärer Arbeitsplatz
- ohne Server unseriöse Installation
- Server muss auch als Server konfiguriert werden

Der Server

- verwaltet Netzwerkdatenverkehr
- verwaltet Nutzer und Gruppen
- verwaltet Rechte und Freigaben
- verwalten Software und Geräte

Client- und Netzwerkschutz

- E-Mail ist der sensibelste Punkt
- Virens Scanner
- Mail-Filter
- Content-Filter

FILTERREGELN					URL-FILTER		EINSTELLUNGEN	
Pos.	Name	Filter	Aktiv					
2	Whitelist-Mails	Filterkriterien: Sender ist " ,...@bhmedical.com.cn,v _@gmx.d i@gmail.com,! @jizankj.com,! @geizdental.de, s @kicktipp.de,€ @omniaspa.eu,s @oral-care-c € @gmail.com" Ausführen: E-Mail annehmen	Ein					
3	URL_SMTP	Filterkriterien: Protokoll ist "SMTP" und wurde vom URL-Filter erfasst Ausführen: E-Mail in Quarantäne nehmen	Ein					
4	Virus_SMTP	Filterkriterien: Protokoll ist "SMTP" und enthält einen Virus Ausführen: E-Mail in Quarantäne nehmen	Ein					
5	Verdächtig_SMTP	Filterkriterien: Protokoll ist "SMTP" und ist als verdächtig eingestuft Ausführen: E-Mail in Quarantäne nehmen	Ein					
6	Spam_SMTP	Filterkriterien: Protokoll ist "SMTP" und ist als Spam klassifiziert Ausführen: E-Mail in Quarantäne nehmen	Ein					
7	Bulk_SMTP	Filterkriterien: Protokoll ist "SMTP" und ist eine Bulk E-Mail Ausführen: E-Mail in Quarantäne nehmen	Ein					
8	Spam_POP3-Proxy	Filterkriterien: Protokoll ist "POP3" und ist als Spam klassifiziert Ausführen: E-Mail im Betreff markieren mit "[Marked as spam]"	Ein					
9	Spam_Mail-Connector	Filterkriterien: Protokoll ist "MAIL-CONNECTOR" und ist als Spam klassifiziert Ausführen: E-Mail in Quarantäne nehmen	Ein					
10	Virus	Filterkriterien: enthält einen Virus Ausführen: zutreffenden Inhalt filtern	Ein					
					+ Regel hinzufügen			

Weitere Handlungsempfehlungen

- regelmäßige Wartung von IT-Systemen, Datensicherung
- Passwörter und Lizenzen zum Eigentümer nicht zum Dienstleister
- Dokumentation erstellen

Wichtigste Erkenntnis:

- Alle technischen Maßnahmen sind ohne besonnen Umgang wirkungslos
- Der Nutzer ist der entscheidende Faktor bei der Sicherheit
- IT ist nur eine Hilfestellung für die geplante Organisation

Fragen und Diskus- sion?



*Vielen Dank für Ihre
Aufmerksamkeit*

www.imedent.de

A portrait of a man with short brown hair and a light beard, wearing a dark blue jacket over a patterned shirt. He is looking directly at the camera with a slight smile.

Oliver Lubecki
Gründer von iMedent