

Daten – Zugriff auf das Gold der Zukunft

28.09. 2017 – Arnd Winter

Inhaltsverzeichnis

Daten

Zugriff

Zugriffskonzepte

Rechte

Mobile Daten



Was sind Daten?

Daten

The screenshot shows the Wireshark interface with the following components:

- Menu:** Datei, Bearbeiten, Ansicht, Navigation, Aufzeichnen, Analyse, Statistiken, Telephonie, Wireless, Tools, Hilfe
- Toolbar:** Includes icons for file operations, search, and display settings.
- Filter:** Anzeigefilter anwenden ... <Ctrl-/>
- Packets List:** A table with columns: No., Time, Source, Destination, Protocol, Length, Info.

No.	Time	Source	Destination	Protocol	Length	Info
130	9.151509	192.168.11.8	192.168.11.106	IPv4	1514	Fragmented IP protocol (proto=UDP 17, off=0, ID=078e) [Reassembled in #131]
131	9.151511	192.168.11.8	192.168.11.106	SIP/XML	365	Request: NOTIFY sip:%7BB2D4251A-8F84-44DF-954A-36423A5362A1%7D@192.168.11.106:5070
132	9.165111	192.168.11.106	192.168.11.8	SIP	690	Status: 200 OK
133	9.201898	ZyxelCom_fb:53:20	Broadcast	0x8899	60	Realtek Layer 2 Protocols
134	9.245652	62.202.27.158	192.168.11.106	UDP	60	53591 → 57907 Len=16
135	9.324528	192.168.11.9	192.168.11.106	TCP	155	3389 → 59682 [PSH, ACK] Seq=708 Ack=1 Win=62687 Len=101
136	9.361643	192.168.11.12	192.168.11.106	TLSv1.2	203	Application Data
137	9.361644	192.168.11.12	192.168.11.106	TLSv1.2	203	Application Data
138	9.361645	192.168.11.12	192.168.11.106	TLSv1.2	203	Application Data
139	9.361645	192.168.11.12	192.168.11.106	TLSv1.2	203	Application Data
140	9.361647	192.168.11.12	192.168.11.106	TLSv1.2	203	Application Data
141	9.361647	192.168.11.12	192.168.11.106	TLSv1.2	203	Application Data
142	9.362052	192.168.11.106	192.168.11.12	TCP	54	59376 → 443 [ACK] Seq=1 Ack=299 Win=2053 Len=0
143	9.362052	192.168.11.106	192.168.11.12	TLSv1.2	155	Application Data
- Packet Details:** Frame 137: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on interface 0. Ethernet II, Src: Microsof_0b:79:6b (00:15:5d:0b:79:6b), Dst: HewlettP_fc:c7:a9 (68:b5:99:fc:c7:a9). Internet Protocol Version 4, Src: 192.168.11.12, Dst: 192.168.11.106. Transmission Control Protocol, Src Port: 443, Dst Port: 59416, Seq: 1, Ack: 1, Len: 149. Secure Sockets Layer.
- Packet Bytes:** Hex and ASCII view of the selected packet. The ASCII view shows the beginning of a TLS record: h.....].y...E...x.@...l.....j...z...&.P.....8...{yTL+... (...).}Gq.b 4...9B.....] e.LN...F...N;...;...Z...ys. k"...vX...ua.2..Nl...X..8. (IW. .U: {...:2...yK.....0...],. J78

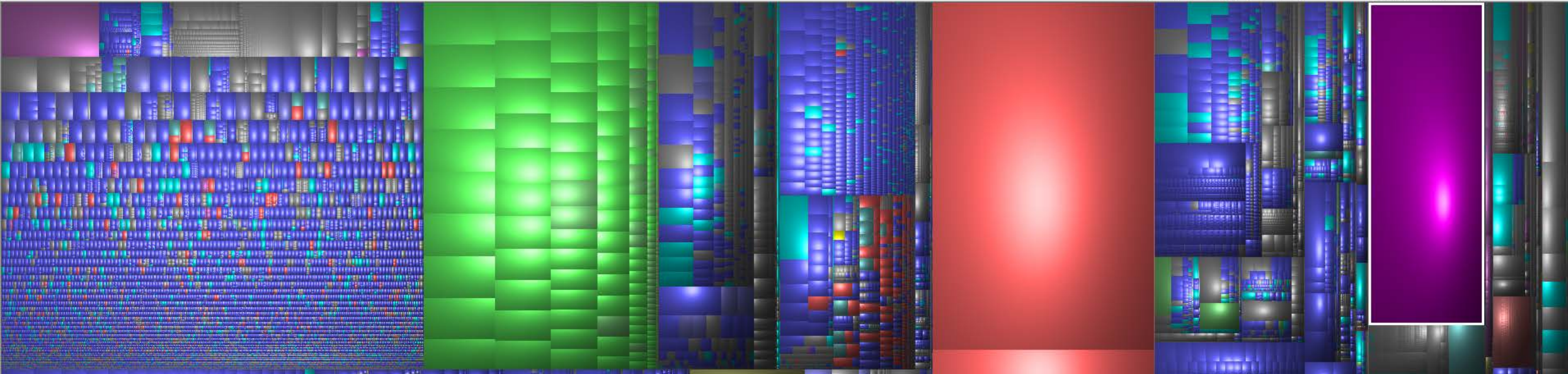
Ihre Daten



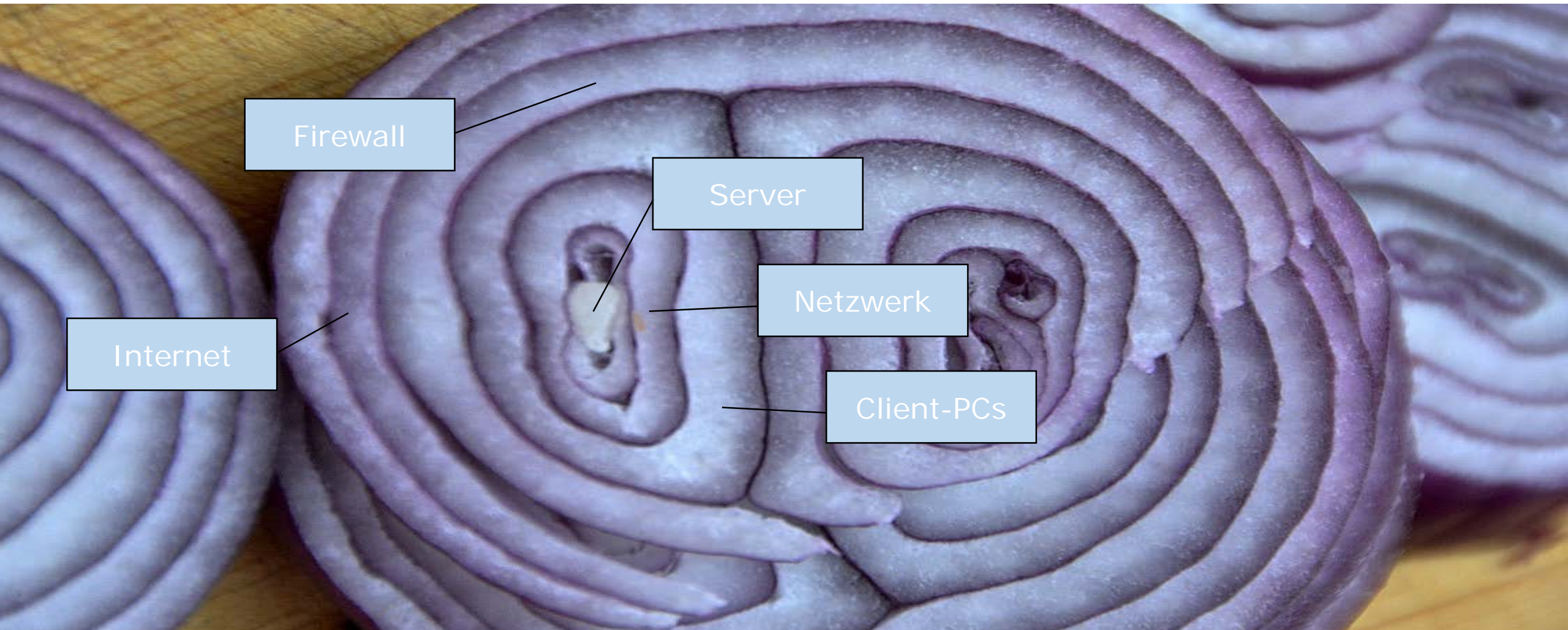
Ihre Daten

<Dateien>	13.2%	4.4 GB	5	5	0	21.09.2017	05:25:11	
Program Files (x86)	12.7%	4.3 GB	17'816	15'464	2'352	21.09.2017	13:50:15	R
Users	12.0%	4.0 GB	27'347	24'714	2'633	21.09.2017	13:50:23	R
Program Files	2.9%	996.5 MB	2'595	2'334	261	15.09.2017	15:22:11	R
ProgramData	2.7%	910.1 MB	1'139	759	380	21.09.2017	13:49:39	H
WEIT.install	0.5%	156.1 MB	524	476	48	15.06.2017	08:04:51	
SWSetup	0.5%	154.4 MB	293	274	19	15.06.2017	08:22:19	
SRecycle.Bin	0.1%	27.6 MB	77	71	6	11.08.2017	08:43:24	HS
SAVG	0.0%	32.0 KB	3	1	2	07.08.2017	05:55:23	H
WEIT.RUN	0.0%	3.4 KB	2	2	0	18.08.2017	12:43:27	
AVG_SysInfo	0.0%	0	2	0	2	25.08.2017	12:26:52	
Config.Msi	0.0%	0	0	0	0	18.09.2017	05:31:04	HS
Dokumente und Einstellun...	0.0%	0	0	0	0	15.06.2017	07:20:18	HS
MSOCache	0.0%	0	0	0	0	15.06.2017	07:55:55	RH
PerfLogs	0.0%	0	0	0	0	16.07.2016	11:47:47	
Programme	0.0%	0	0	0	0	15.06.2017	07:20:18	HS
Recovery	0.0%	0	0	0	0	15.06.2017	07:20:18	HS
System Volume Information	0.0%	0	0	0	0	19.07.2017	11:40:58	HS

.msp	Windows Installer-Patch	3.3 GB	9.7%	105
.exe	Anwendung	2.2 GB	6.7%	3'216
.ost	Outlook-Datendatei	1.6 GB	4.7%	1
.cab	CAB-Datei	664.8 MB	1.9%	97
.ttc	TrueType-Schriftartensamm...	580.3 MB	1.7%	48
.	Lokaler Datenträger	519.0 MB	1.5%	9'583
.msi	Windows Installer-Paket	470.6 MB	1.4%	177
.dat	DAT-Datei	403.4 MB	1.2%	797
.bin	BIN-Datei	386.4 MB	1.1%	752
.edb	EDB-Datei	330.8 MB	1.0%	9
.log	Textdokument	330.3 MB	1.0%	271
.cat	Sicherheitskatalog	302.7 MB	0.9%	16'526
.ttf	TrueType-Schriftartendatei	262.8 MB	0.8%	539
.zip	ZIP-komprimierter Ordner	236.9 MB	0.7%	23
.mui	MUI-Datei	236.7 MB	0.7%	9'171
.avm	AVM-Datei	226.3 MB	0.7%	3
.07...	07275332_82E4_4820_9FDD_...	190.6 MB	0.6%	393
.imd	IMD-Datei	153.6 MB	0.4%	34
.b4...	B4988E63_555A_4DEB_A5F4_...	150.1 MB	0.4%	203



Zugang zu Ihren digitalen Daten



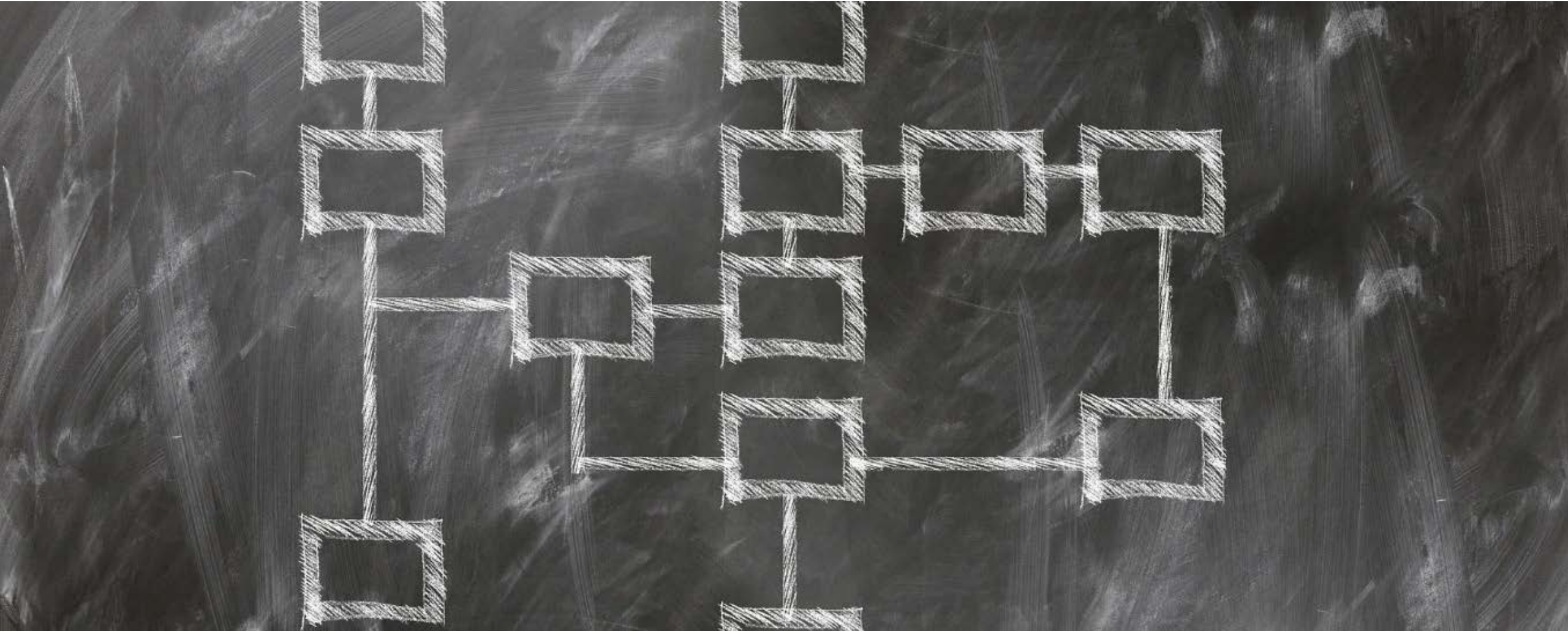
Zugang zu Ihren digitalen Daten



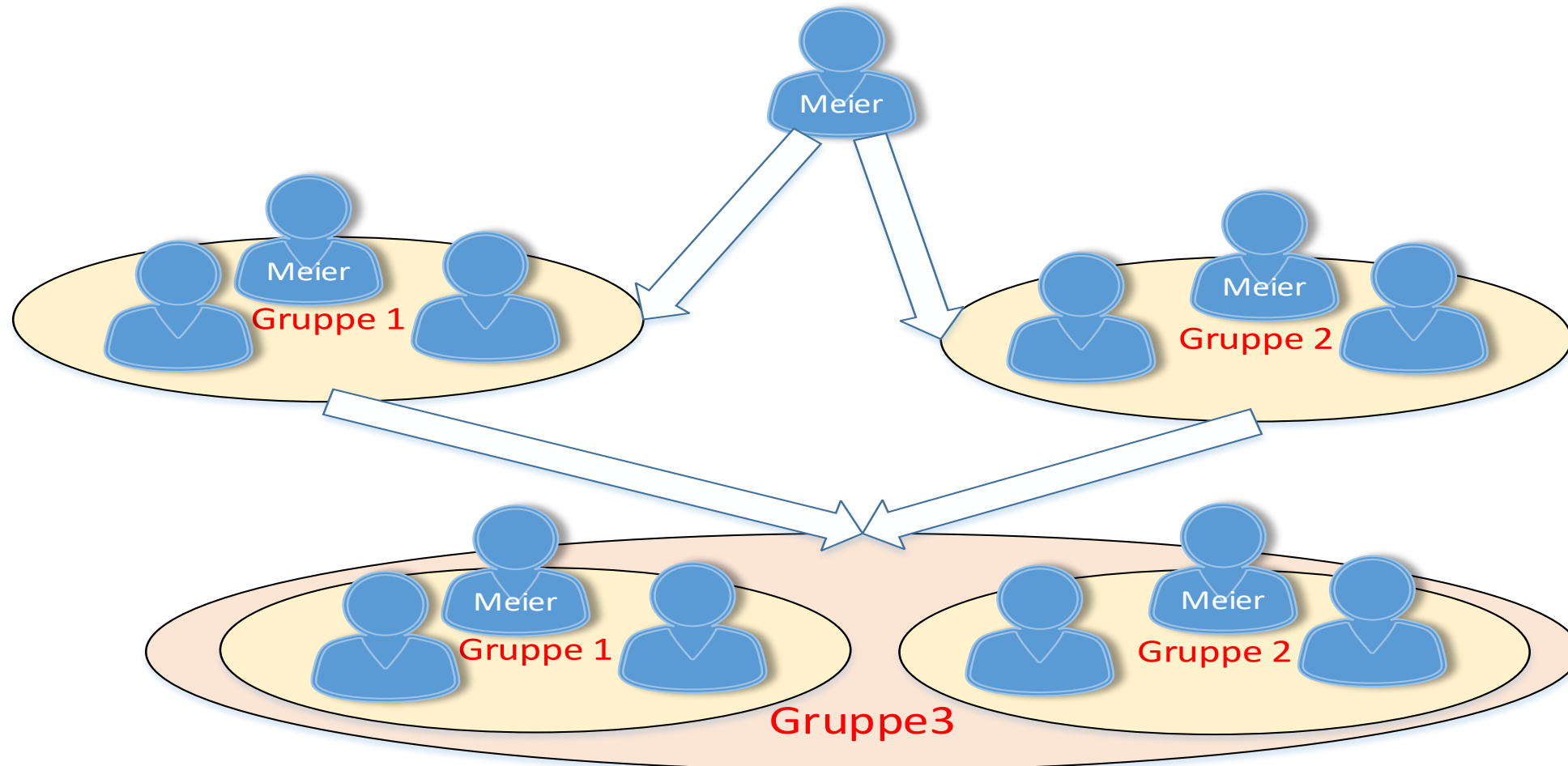




Benutzer, Gruppen, Rechte



Benutzer, Gruppen, Rechte





Rechte

```
DO-WEIT\Domänen-Admins:(I)(F)
F:\Coordination\_Führung KAM\samuel-zeller-360588.jpg DO-WEIT\SG_MANAGEMENT_RW:(I)(M)
DO-WEIT\WI:(I)(F)
NT-AUTORITÄT\SYSTEM:(I)(F)
DO-WEIT\Domänen-Admins:(I)(F)
F:\Coordination\_Führung KAM\sand-2616055_1920.jpg DO-WEIT\SG_MANAGEMENT_RW:(I)(M)
DO-WEIT\WI:(I)(F)
NT-AUTORITÄT\SYSTEM:(I)(F)
DO-WEIT\Domänen-Admins:(I)(F)
F:\Coordination\_Führung KAM\sure-1435364_1920.jpg DO-WEIT\SG_MANAGEMENT_RW:(I)(M)
DO-WEIT\WI:(I)(F)
NT-AUTORITÄT\SYSTEM:(I)(F)
DO-WEIT\Domänen-Admins:(I)(F)
F:\Coordination\_Führung KAM\Thumbs.db DO-WEIT\SG_MANAGEMENT_RW:(I)(M)
DO-WEIT\WI:(I)(F)
NT-AUTORITÄT\SYSTEM:(I)(F)
DO-WEIT\Domänen-Admins:(I)(F)
F:\Coordination\_Führung KAM\WEIT_Wissensgipfel V.pptx DO-WEIT\SG_MANAGEMENT_RW:(I)(M)
DO-WEIT\WI:(I)(F)
NT-AUTORITÄT\SYSTEM:(I)(F)
DO-WEIT\Domänen-Admins:(I)(F)
```




Mobile Daten







mERCI

Wehrich Informatik GmbH
Allestrasse 20
8280 Kreuzlingen

info@wehrich.ch
www.wehrich.ch