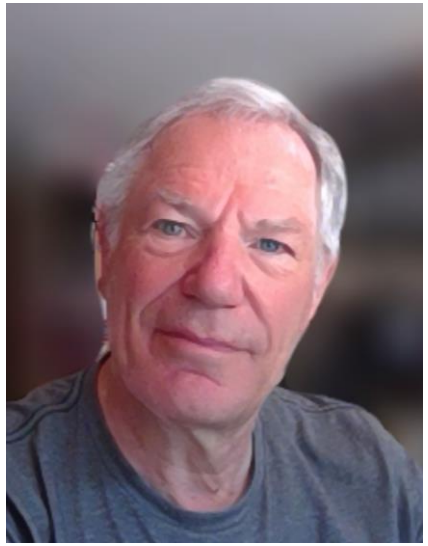
Sichererheit vs. Vertrauen

Berechtigungen, Angriffe, Datenschutz, Datensicherung

Udo Besenreuther, SIT-Heroldstatt

Februar 2023

Zur Person



Udo Besenreuther

- verheiratet, 3 Kinder
- Dipl. Ing. Fahrzeugbau
- Tätig als **IT-System-Architekt** und IT-Projektmanager eines weltweiten Internet-Datenportals (Business to Business, 24/7-Betrieb)
- **DSGVO-KnowHow** wegen der Tätigkeit als Datenschutzbeauftragter für Kirche und Jugendarbeit
- Tätig in der lokalen Seniorenarbeit SIT-Heroldstatt und engagiert in mehreren Vereinen.
- Im Vorstand des Netzwerk-sii-BW.

SIT

Programm

Netzwerk sii Baden-Württemberg

- Sicherheit vs. Vertrauen
- 4 Elemente der Datensicherheit
- Manipulation des Benutzers
- Verkürzte Links
- Virenschutz
- Angriffsvektoren auf das Smartphone
- Ransomware (Erpressungssoftware)
- Vertrauenswürdige Apps und App-Stores
- Katwarn – App
- NORA – Notruf-App

Sicherheit vs. Vertrauen

- **Sicherheit**

  Für Individuen und Gemeinschaften bezeichnet Sicherheit den **Zustand** des **Nicht-bedroht-Seins** der Freiheit ihrer **ungestörten Eigenentwicklung** in zweierlei Hinsicht:

  - im Sinne des **tatsächlichen (objektiven) Nichtvorhandenseins von Gefährdung** als Sicherheit im objektiven Sinne, sowie
  - im Sinne der **Abwesenheit von (subjektiver) Furcht vor Gefährdung** – als Sicherheit im subjektiven Sinne.

https://de.wikipedia.org/wiki/Sicherheit

SIT

Sicherheit vs. Vertrauen

Netzwerk sii Baden-Württemberg

- **Vertrauen**

  bezeichnet die **subjektive Überzeugung** (oder auch das Gefühl für oder Glaube an die) von der **Richtigkeit, Wahrheit von Handlungen, Einsichten und Aussagen** bzw. der **Redlichkeit von Personen**.

https://de.wikipedia.org/wiki/Vertrauen

SIT

Sicherheit vs. Vertrauen

Netzwerk sii Baden-Württemberg

- **Sicherheit oder Vertrauen in IT-Systemen**

  <u>These</u>:

  Die absolute Sicherheit in IT-Systemen ist nur mit immensen Aufwand zu erreichen und i.d.R. **nicht** vorhanden.

  Dennoch kann man den meisten Prozessen vertrauen, dass mit Daten und Informationen verantwortungsvoll umgegangen wird. Allerdings gilt es stets achtsam zu sein, welche Programme genutzt werden.

- **Auch in der analogen Welt haben wir Vertrauen** zu Bankangestellten, Postboten, Ärzten und Krankenschwestern, Lehrern, Polizisten, etc.

SIT

Netzwerk sii Baden-Württemberg

4 Elemente der IT-Datensicherheit

SIT

Datensicherheit
1. Verlust

Netzwerk sii Baden-Württemberg

Sicherheitsthemen in IT-Systemen

1. Sicherheit vor Datenverlust

Daten dürfen nicht verloren gehen.

Abhilfe:

Backup ist die Daten an mehreren Orten und/oder mehreren Systemen speichern. Sicherstellen, dass diese auch nicht unbewusst gelöscht werden können.

SIT

Datensicherheit
2. Manipulation

Netzwerk sii Baden-Württemberg

Sicherheitsthemen in IT-Systemen

2. Sicherheit vor Manipulation

Daten dürfen nicht verändert werden.

Abhilfe:

Beste Möglichkeit bietet die **Blockchain**. Dabei wird jede Änderung der Daten an möglichst vielen Orten gespeichert und mit Prüfsumme versehen. Wenn jemand versucht eine Änderung zu manipulieren, wird dies wieder korrigiert.

Spezielle Systeme für dokumentensichere Speicherung von Daten.

SIT

Datensicherheit
3. Ausspähung

Netzwerk sii Baden-Württemberg

Sicherheitsthemen in IT-Systemen

3. Sicherheit vor Ausspähung (Autorisierung)

Daten dürfen nicht von Unberechtigten gelesen werden.

Abhilfe:

Verschlüsselung der Daten soll best möglich erfolgen. Die Daten sind möglichst dicht an der Quelle und Nutzung ver- und entschlüsselt werden, ohne vorher gespeichert oder transportiert zu werden.

Spezieller Problemfall:

Wie gut die Verschlüsselung in Zukunft ist, ist nicht bekannt!

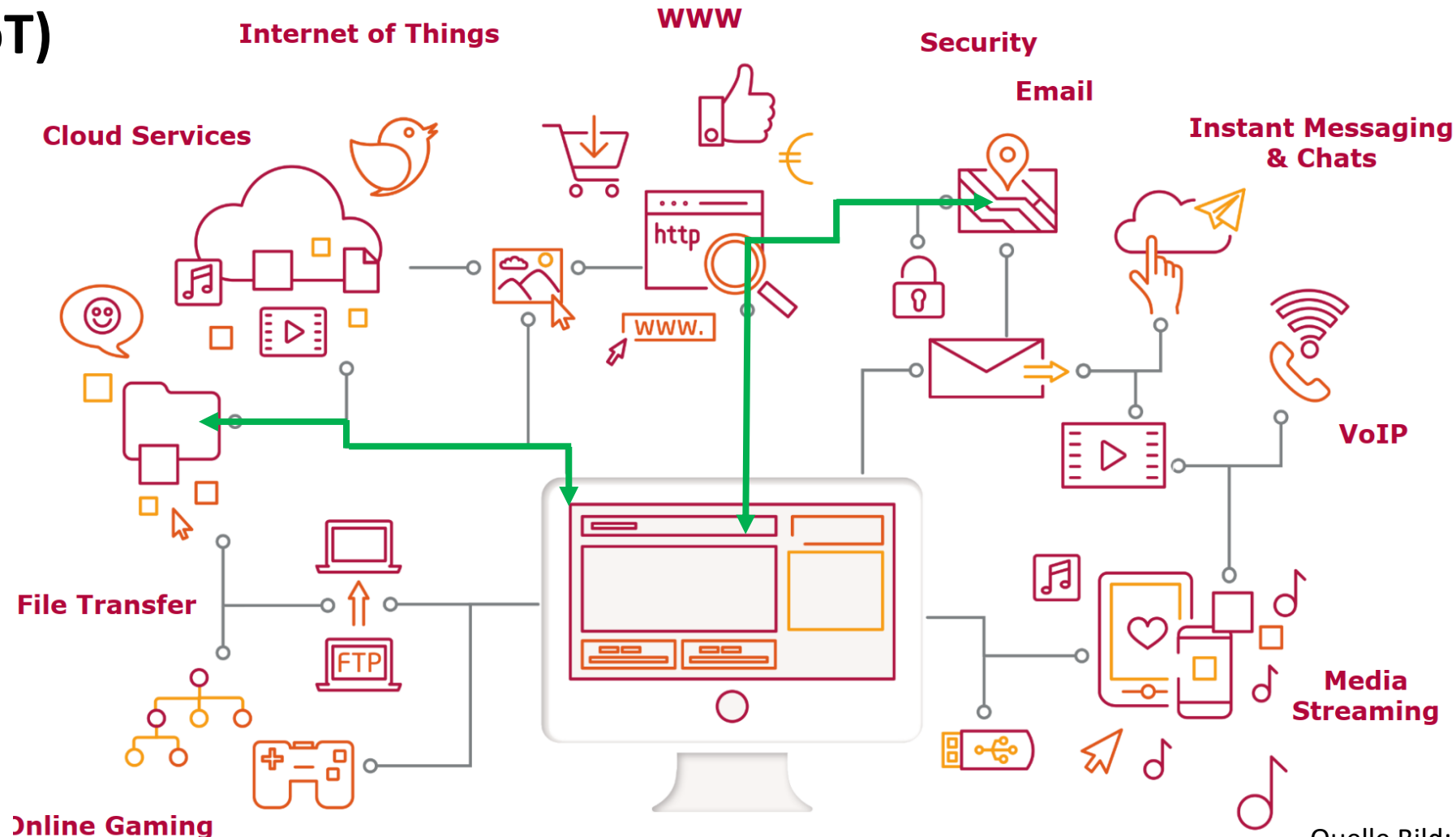
Datensicherheit
3. Ausspähung

Internet of Things (IoT)

Auf Grund der vielfältigen Geräte, Protokolle, Schnitt-stellen ist die Zahl der Schwachstellen nicht transparent und nur schwer überschaubar.

Deshalb:

End-to-End-Verschlüsselung



Quelle Bild: HPI

Datensicherheit
4. Nutzung

Haupt-
angriffsvektor

Sicherheitsthemen in IT-Systemen

4. Sicherheit vor unberechtigter Nutzung (Authentifizierung)

Daten und Apps dürfen nicht von Unberechtigten genutzt werden.

Abhilfe:

Der Zugang zu den Daten und Apps wird mit **persönlicher Authentifizierung** gesichert, die nur dem Nutzer bekannt ist und/oder durch eine Hardware, die nur der Benutzer besitzt (2-Faktor).

SIT

Datensicherheit
4. Nutzung

Netzwerk sii Baden-Württemberg

3 Komponenten der Authentifizierung:

- **Wissen**
  PIN, Passwort, ID-Nummer, etc.
- **Besitz**
  Schlüssel, Dongle, USB-Stick, Ausweis, Bankkarte, Smartphone, etc.
- **Biometrie**
  Fingerabdruck, Iris, Gesichtsgeometrie, etc.

Von **2-Faktor-Authentifizierung (2FA)** spricht man, wenn man 2 Elemente aus den Authentifizierungskomponenten benötigt.

Privatsphäre auf dem Smartphone

Wie schütze ich mein Smartphone/Laptop/PC:

- … vor Verlust der Daten:

  1. Regelmäßige Sicherungen und Backups an einem 2. Ort, in der Cloud oder auf lokalen Datenträgern (wie SD-Karte, SSD-Platte, USB-Stick, DVD)

- … vor Manipulation
- … vor Nutzung (Autorisierung)
- … vor Ausspähung (Authentifizierung)

  2. Vermeidung des Zugriffs von Unberechtigten.

SIT

Manipulation des Benutzers

Netzwerk sii Baden-Württemberg

Einige Beispiele für Betrugsmaschen

SIT

Netzwerk sii Baden-Württemberg

Betrogen um 15 000 Euro

Kriminalität Auf eine dreiste Telefon-Masche fällt ein 82-Jähriger herein.

Pfaffenhofen. Ein 82-Jähriger aus Pfaffenhofen ist Opfer eines Telefon-Betrugs geworden. Laut Polizei hatte er am Montag einen Anruf von einem angeblichen Microsoft-Mitarbeiter erhalten. Während des mehrstündigen Telefonats wurde er angeleitet, Software herunterzuladen und auf dem PC zu installieren, damit der Mitarbeiter „Hacker von seinem PC entfernen könne". Am Dienstag stellte der Mann fest, dass Unbekannte per Onlinebanking von seinem Konto vier Überweisungen auf deutsche und weitere europäische Konten in einer Gesamthöhe von beinahe 15 000 Euro vorgenommen hatten. Ein Konto ist aus vielen anderen Betrugsfällen bekannt. Nun wird versucht, die Überweisungen zu stoppen und rückgängig zu machen.

SIT

Manipulation des Benutzers

Netzwerk sii Baden-Württemberg

Betrogen um 15 000 Euro

Kriminalität Auf eine dreiste Telefon-Masche fällt ein 82-Jähriger herein.

Pfaffenhofen. Ein 82-Jähriger aus Pfaffenhofen ist Opfer eines Telefon-Betrugs geworden. Laut Polizei hatte er am Montag einen Anruf von einem angeblichen Microsoft-Mitarbeiter erhalten. Während des mehrstündigen Telefonats wurde er angeleitet, Software herunterzuladen und auf dem PC zu installieren, damit der Mitarbeiter „Hacker von seinem PC entfernen könne". Am Dienstag stellte der Mann fest, dass Unbekannte per Onlinebanking von seinem Konto vier Überweisungen auf deutsche und weitere europäische Konten in einer Gesamthöhe von beinahe 15 000 Euro vorgenommen hatten. Ein Konto ist aus vielen anderen Betrugsfällen bekannt. Nun wird versucht, die Überweisungen zu stoppen und rückgängig zu machen.

Südwest-Presse, 13.06.2022

- Betrüger nutzen das Vertrauen, welches die Menschen in große Unternehmen haben schamlos aus.
- Deshalb hilft nur, die Richtigkeit auf getrenntem Kanal zu überprüfen (Rückruf an bekannte Nummer, E-Mail an die bekannte Kontaktperson, etc.)

Fachbegriff: Social Engineering

SIT

Manipulation des Benutzers

Netzwerk sii Baden-Württemberg

FÜR IHRE DRINGENDE AUFMERKSAMKEIT Posteingang ×

Justin Shawn Wallace <shawnjustin25@gmail.com>
an

Hallo Freund,
Ich bin ein leitender Bankangestellter
Ich arbeite in einer der größten Banken Afrikas.
In unserem System befindet sich Geld, das wir auf ein ausländisches Konto überweisen möchten. Wir benötigen ein Bankkonto in Ihrem Land oder einem anderen europäischen Land. Wenn Sie antworten, gebe ich Ihnen meinen Banknamen und zeige Ihnen sogar das Geld in unserem Online-System.

Bitte kontaktieren Sie mich direkt per E-Mail. Weitere Informationen gebe ich per E-Mail.
Wir werden nach der Transaktion zufrieden sein. Wir benötigen ein Bankkonto von Ihnen. Neues oder altes Konto. Alles wird in Übereinstimmung mit den internationalen Geldtransfervorschriften durchgeführt.
Ich gebe Ihnen 30 % des Gesamtbetrags.
Ich warte auf deine Antwort.
Grüße
Herr Justin Shawn Wallace

Entweder wird eine Gebühr verlangt oder man macht sich wegen Geldwäsche strafbar.

SIT

Netzwerk sii Baden-Württemberg

Wir haben versucht Ihr Paket zuzustellen

H **Hermes <gold@jap.co.jp>**
17:31

An: Hermes

Sehr geehrte Kundin/Kunde,

Diese E-Mail soll Sie über der[illegible]ummer 02137160000699 informieren.
Dies ist darauf zurückzuführe[illegible]stiert oder in unserem System nicht gefunden werden kann.

H **Hermes**

E-Mail senden

gold@jap.co.jp

Was passiert als nächstes?
Ihr Paket wurde an unser lokales Lager zurückgesandt, wo es für die nächsten sieben Arbeitstage verbleiben wird.

> Von hier aus können Sie uns eine aktualisierte Adresse für dieses Paket mitteilen, indem Sie hier klicken.
Für die erneute Zustellung Ihres Pakets wird eine Gebühr erhoben.

Sie können Ihr Paket auch in unserem Lager in Belpstrasse 48, 3007 abholen.
Wenn Sie weitere Informationen zu diesem Zustellungsversuch benötigen, verwenden Sie bitte unser Kontaktformular.
Hermes

https://stitchingwires.com/paket

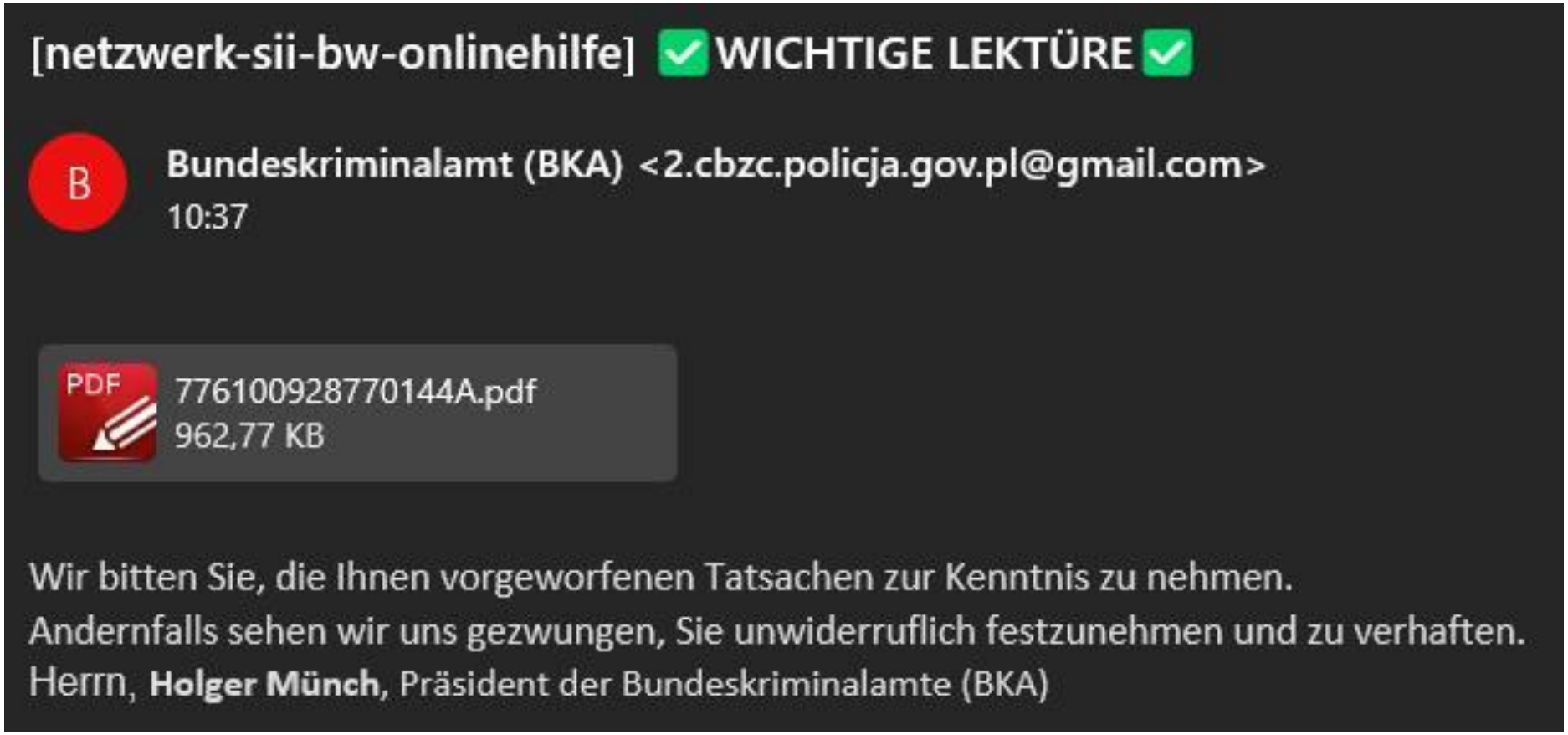
CONTACT US

MEHTA BROTHERS
8, Saifee Park,
Dr. Mascarenhas Road,
Mazgaon, Mumbai - 400 010
TEL : +91 22 2375 1012, 2371 6040
FAX : +91 22 2377 0254
EMAIL : stitchingwire@gmail.com

SIT

Manipulation des Benutzers

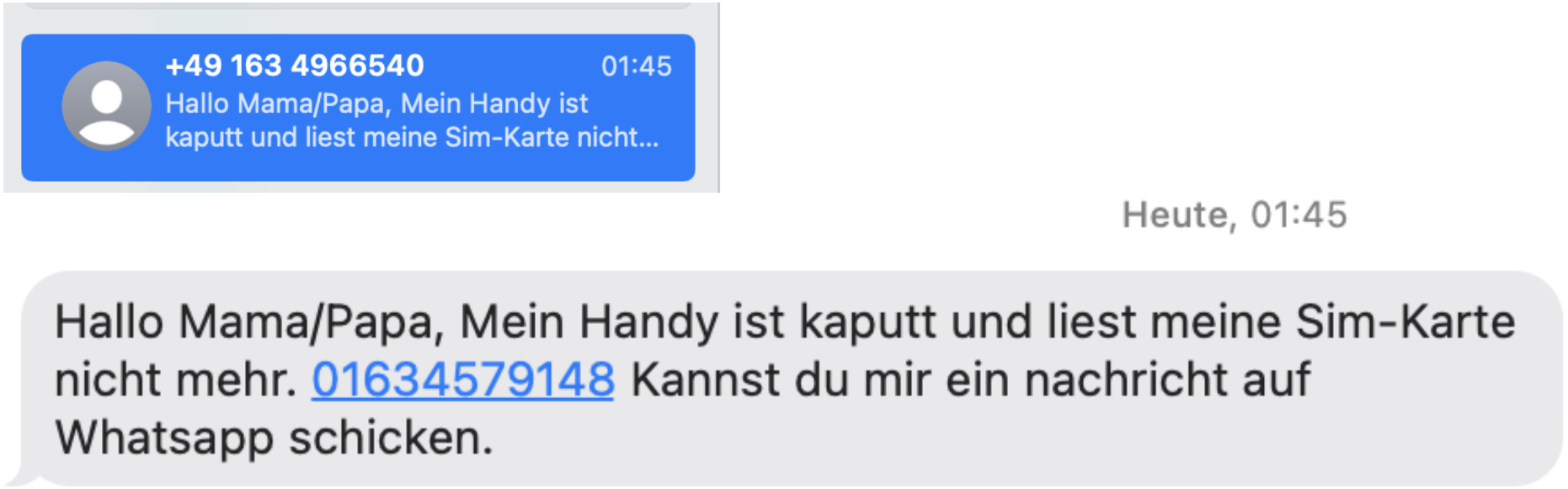
Netzwerk sii Baden-Württemberg



SIT

Manipulation des Benutzers

Netzwerk sii Baden-Württemberg



SIT

Manipulation des Benutzers

Netzwerk sii Baden-Württemberg

Banken versenden Infos zu Phishing zum Selbstschutz:

- Betrugsmaschen erkennen
  https://www.ing.de/wissen/sicherheit/?wt_mc=email.wwinfo..e-2301-ww-knd-info-s-0457.
- Wie kommen Phisher an meine Daten
  https://www.ing.de/wissen/phisher-daten/?wt_mc=email.wwinfo..e-2206-ww-knd-info-s-v1-0457
- Was ist Phishing genau?
  https://www.mobilcom-debitel.de/digitalrepublic/digital-lifestyle/was-ist-phishing-
- Wie kann ich mich vor Phishing schützen?
  https://www.ing.de/wissen/phishing-mails/
- Wie kann man Phishingmails erkennen?
  https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingmails-woran-sie-sie-erkennen-und-worauf-sie-achten-muessen-6073
- Checkliste: Phishing erkennen und damit umgehen:
  https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/so-lesen-sie-den-mailheader-6077
- Phishing-Radar
  https://www.verbraucherzentrale.de/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059
- Hoax-Datenbank
  https://hoax-info.tubit.tu-berlin.de/hoax/hoaxlist.shtml

Verkürzte Links

Vorsicht bei verkürzten Links

- Was tun mit: https://tinyurl.com/mrxhxye8
- Über verschiedene Portale können lange Links gekürzt werden, z.B.: Tiny-Url, Bitly, is.gd, T1p, Rebrandly
- Problem ist, dass man die richtige URL nicht mehr erkennt
- Um die richtige URL zu prüfen, gibt es ein Tool: https://checkshorturl.com/
- Ein Beispiel:
  https://tinyurl.com/mrxhxye8
  führt zu:
  https://sit-heroldstatt.de

SIT

Virenschutz fürs Handy

Netzwerk sii Baden-Württemberg

Benötigt man einen Virenschutz auf dem Handy?
Das Handy ist genau wie der Computer ständig mit dem Internet verbunden.

- Im Google-Playstore werden alle Apps gescannt und auf Viren geprüft
- Wer nur Apps aus dem Playstore läd, ist relativ sicher (?)
- Wer Apps aus alternativen Quellen installiert und gern alles ausprobiert, was so im Internet angeboten wird (Spiele, Angebote, Dating, etc.), sollte sich einen zusätzlichen Virenschutz installieren.

Android: https://www.chip.de/news/Virenscanner-fuer-Android-Schutz-wirklich-noetig_98607733.html

IKARUS App: https://www.ikarussecurity.com/privatkunden/ikarus-mobile-security/

iPhone: https://praxistipps.chip.de/virenschutz-fuers-iphone-sinnvoll-oder-unnoetig_1668

SIT

Schutzstrategien

Netzwerk sii Baden-Württemberg

Wie kommen Phisher auf mein Handy?

- Phishing Mails (Link)
- Betrügerische Apps
- Datenweitergabe eines betrügerischen Dienstleisters

Wie kann ich mich davor schützen?

- URLs prüfen
- Nicht alles installieren! Vorher informieren, wer der Anbieter ist. Impressum und Datenschutzerklärung liefern die nötigen Infos.
- Große Firmen möchten keinesfalls ihre Reputation verlieren. Gewinnorientierte Newcomer, sind auch schnell wieder weg vom Markt

SIT

Angriffe auf das Smartphone

Netzwerk sii Baden-Württemberg

Angriffsvektoren auf das Smartphone

Konponenten des Smartphones

Achtung vor Apps (auf Smartphones und PCs), diese können ggf. auf Komponenten zugreifen und deren Daten verwenden:

- Standort
- Anrufliste
- Kontakte
- Kalender
- Kamera
- Dateien und Medien
- Körpersensoren
- Körperliche Aktivität
- Mikrofon
- Telefon
- SMS
- Zusätzliche Berechtigungen
- Chatnachrichten lesen
- Chatnachrichten verfassen
- Fahrzeuginformationen

SIT

Berechtigungen verwalten

Netzwerk sii Baden-Württemberg

Begrenzung des Zugriffs von Apps auf das unbedingt Notwendige!

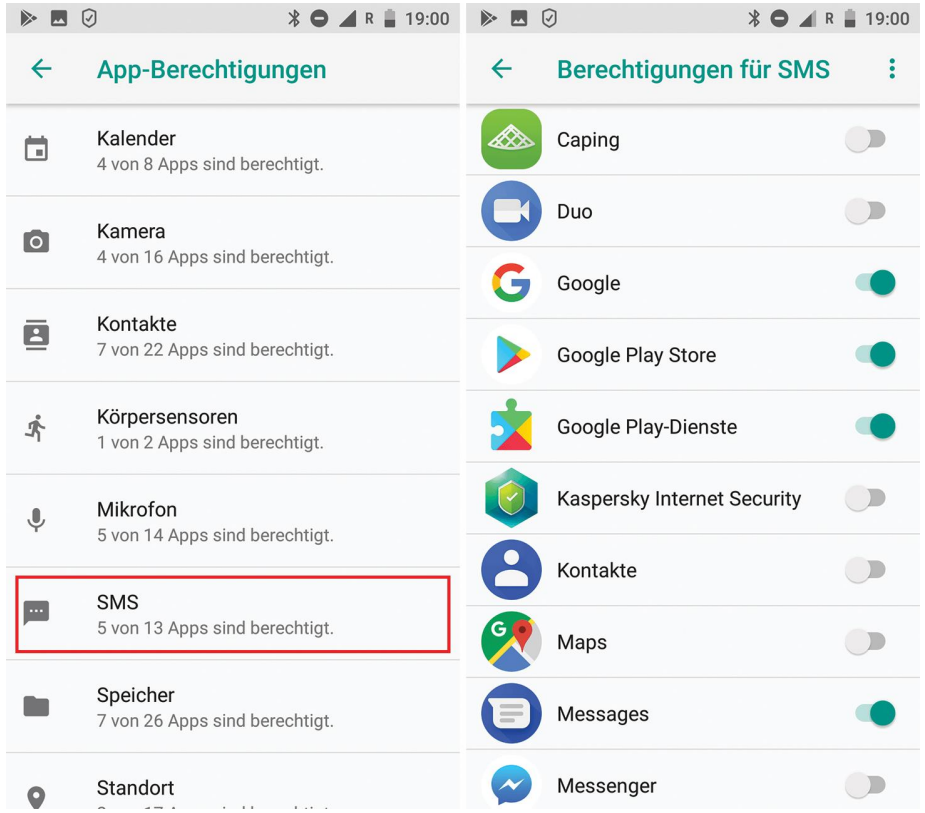
- Damit Apps auf dem Smartphone nur die Dinge tun, für die sie installiert sind, kann man ihre Berechtigungen einschränken.
- Für Smartphones ist Vorschrift , dass die Apps vor dem Zugriff um Genehmigung fragen.
- Auf PC/Laptops können Apps auf (fast) alles zugreifen. Können sich im Hintergrund installieren und dass Sie bei jedem Start aktiviert werden. Vieren und Trojaner nutzen diese Lücken aus. Vorsicht bei neuer Software!

Android: https://levato.de/wp-content/video/android/berechtigungen_android.mp4?_=1

Apple: https://levato.de/wp-content/video/iphone/berechtigungen_ios.mp4?_=2

Berechtigungen verwalten

Android – Berechtigungen verwalten

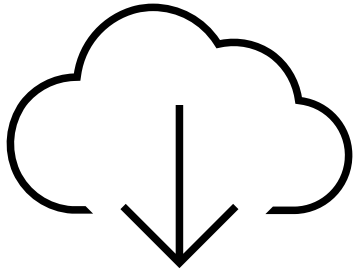


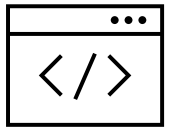
Apple – Datenschutz verwalten

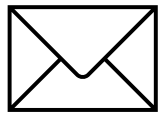
Ransomware (Lösegeld)

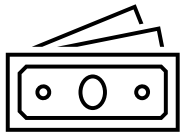
Mit Ransomware werden meist Firmen erpresst

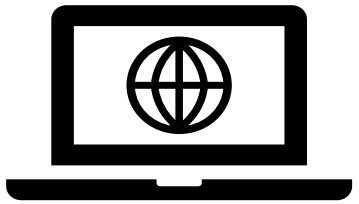
Ransomware (Lösegeld)









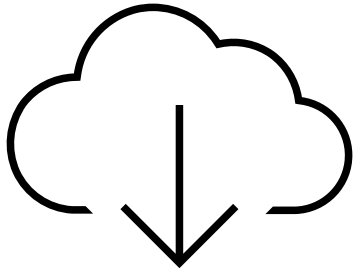


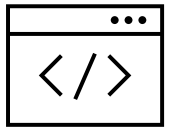
1. Ransomware kommt auf den PC

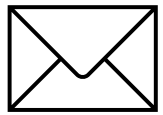
Mögliche Quellen:

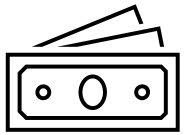
- Falsche Webseiten
- Spam Mails, mit Virus infiziert
- Phishing Mails

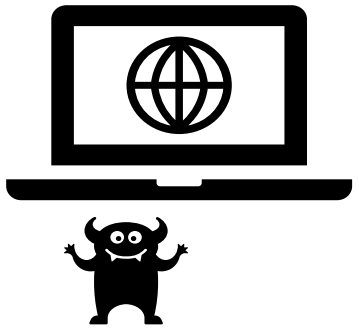
Ransomware (Lösegeld)









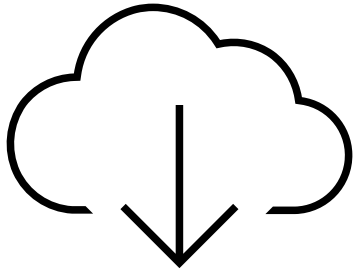


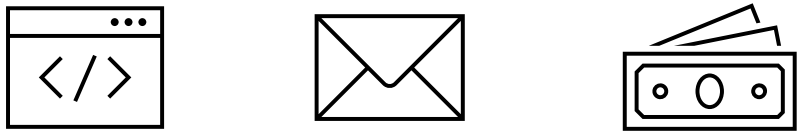
1. Ransomware kommt auf den PC

Mögliche Quellen:

- Falsche Webseiten
- Spam Mails, mit Virus infiziert
- Phishing Mails

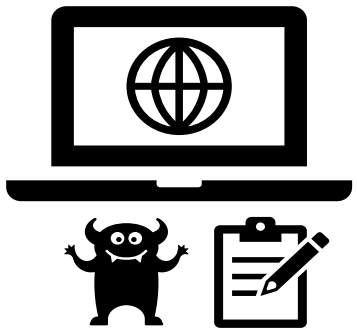
Ransomware (Lösegeld)

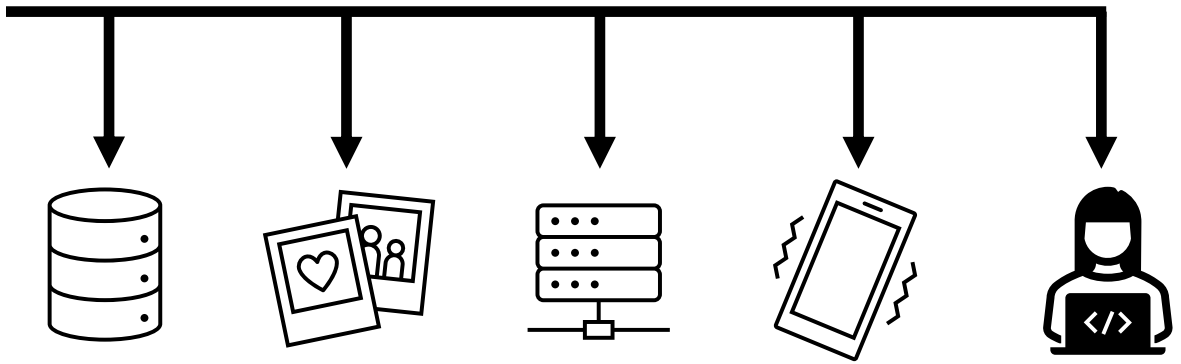




1. Ransomware kommt auf den PC

2. Ransomware beobachtet/protokolliert Verbindungen





Eigene Festplatten

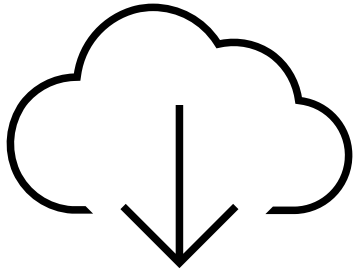
Bilder-Festplatten USB

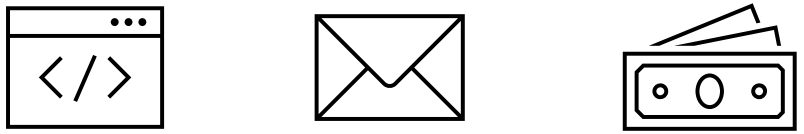
Netzwerk-Festplatten FTP / Cloud

Geräte Smartphone Kameras andere

Laptops von Familie, Freunden, Kollegen

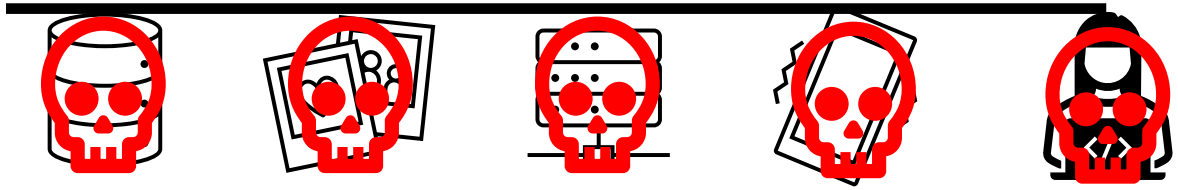
Ransomware (Lösegeld)





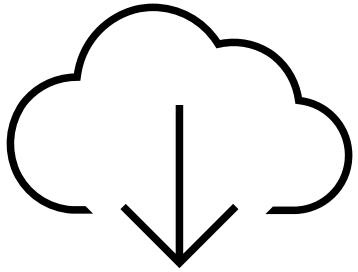
1. Ransomware kommt auf den PC

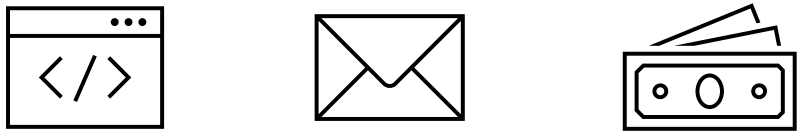
2. Ransomware beobachtet/protokolliert Verbindungen



3. Ransomware verschlüsselt alle Dateien der verbundenen Laufwerke und Geräte

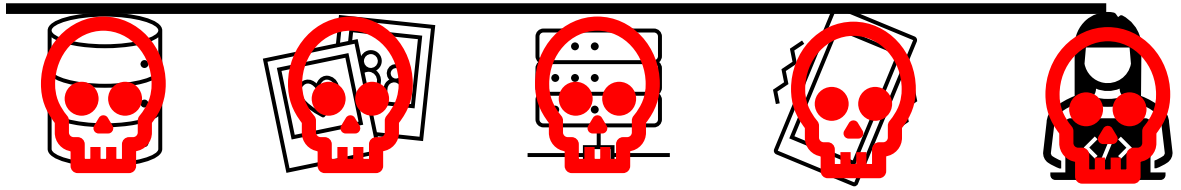
Ransomware (Lösegeld)



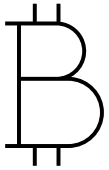


1. Ransomware kommt auf den PC

2. Ransomware beobachtet/protokolliert Verbindungen



3. Ransomware verschlüsselt irgendwann alle Dateien der verbundenen Laufwerke und Geräte



4. Erpresser verlangen BitCoins, haben eine sehr gute Hotline, um BitCoin-Konto einzurichten

SIT

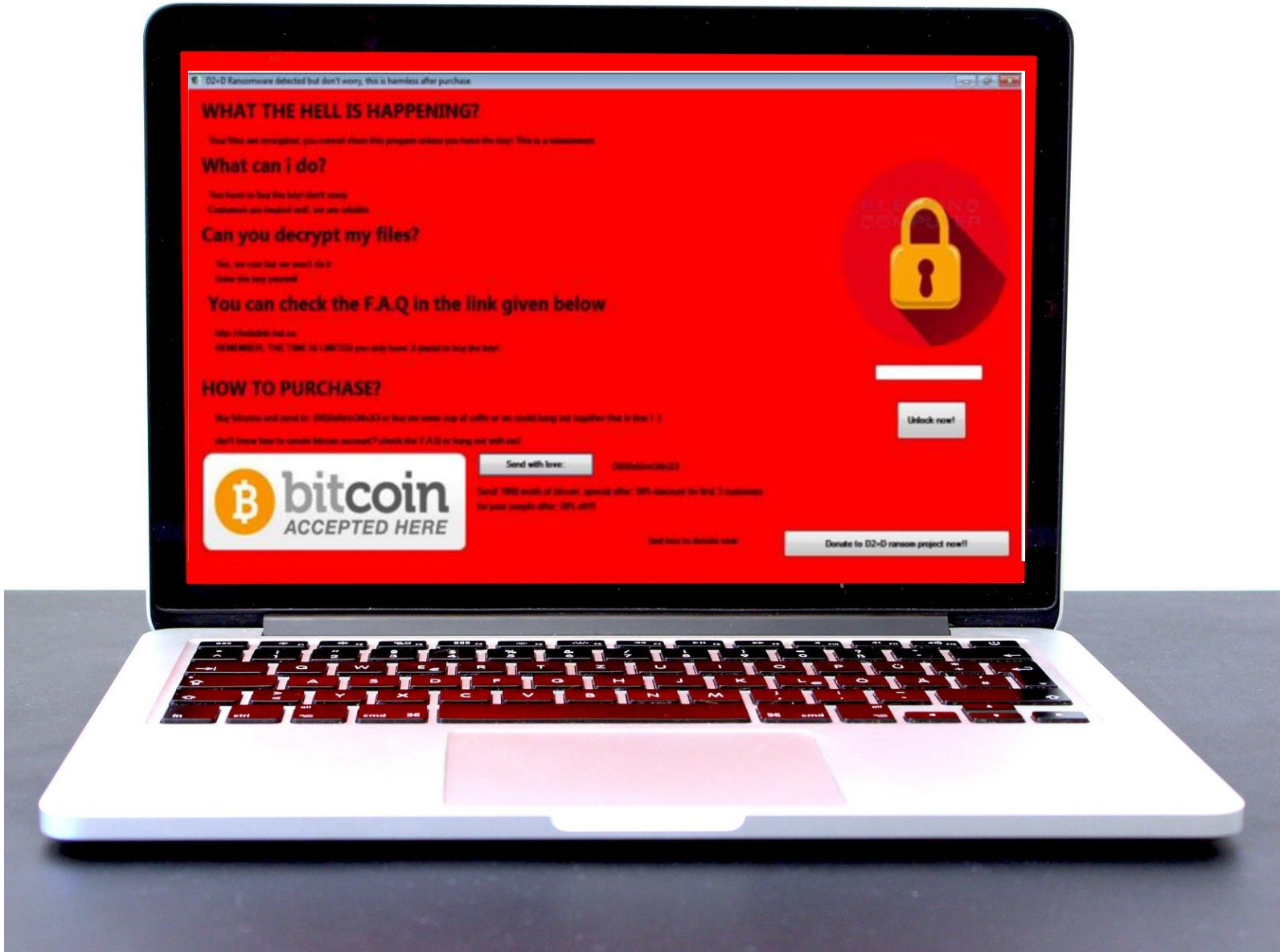
Ransomware (Lösegeld)

Netzwerk sii Baden-Württemberg

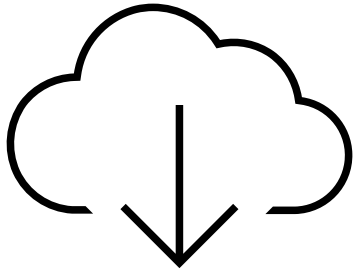
SIT

Ransomware (Lösegeld)

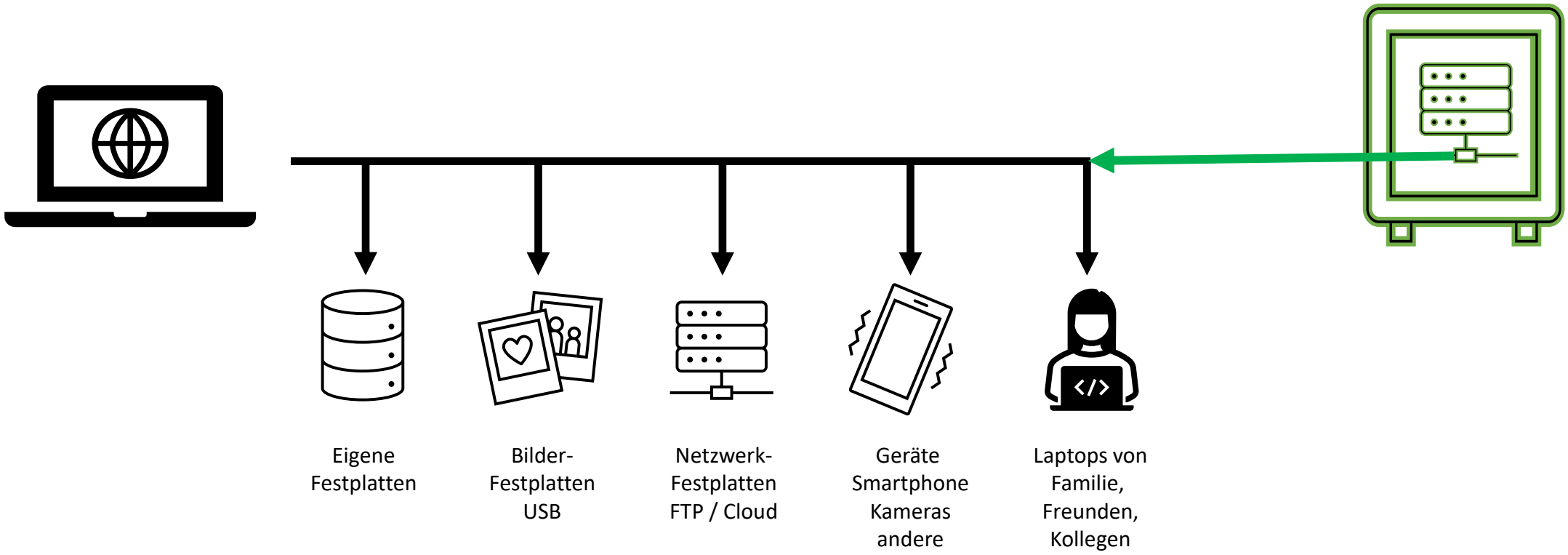
Netzwerk sii Baden-Württemberg



Ransomware (Lösegeld)



Schutz vor Ransomware ist ein Datenspeicher, der von sich die Verbindung auf freigegebene Speicherplätze aufbaut.



SIT. Alternative App und App-Store

Netzwerk sii Baden-Württemberg

Vertrauenswürdige Apps?

SIT

Privacy-Friendly-Apps

Netzwerk sii Baden-Württemberg

Forschungsgruppe SECUSO
entwickelte **Privacy Friendly Apps (PFA)** für Android-Geräte fordern nur die für die Funktionalität erforderlichen Berechtigungen an. Zudem enthalten sie keine Tracking-Mechanismen, so dass keinerlei (Nutzungs-) Daten gesammelt werden. Alle Applikationen der Privacy Friendly Apps-Gruppe können daher ohne Bedenken hinsichtlich Privatsphäre- Verletzungen installiert werden."

PRIVACY FRIENDLY APPS
Für das Android-Smartphone

NoPhishing-Quiz:
https://play.google.com/store/apps/details?id=de.tudarmstadt.informatik.secuso.phishedu2&hl=de

Die Forschungsgruppe:
https://secuso.aifb.kit.edu/

Die Apps:
https://secuso.aifb.kit.edu/105.php

https://simplemobiletools.com/

Privacy-Friendly-Apps

NoPhishing-Quiz installieren:
https://play.google.com/store/apps/details?id=de.tudarmstadt.informatik.secuso.phishedu2&hl=de

Whois & DNS-Lookup installieren:
https://play.google.com/store/apps/details?id=com.xsprice.nettools&hl=de

Suche nach IP-Adresse (Domain eingeben):

1. Ins Suchfeld Domain eingeben
2. Auf DNS klicken
   Infos zur IP werden angezeigt

Suche nach Domain (IP eingeben):

1. Ins Suchfeld IP-Adresse eingeben
2. Auf DNS klicken
   Wenn die IP eindeutig zugeordnet ist, wird die Domain angezeigt.

PRIVACY FRIENDLY APPS

Für das Android-Smartphone

Die Forschungsgruppe:
https://secuso.aifb.kit.edu/

Die Apps:
https://secuso.aifb.kit.edu/105.php

https://simplemobiletools.com/

SIT

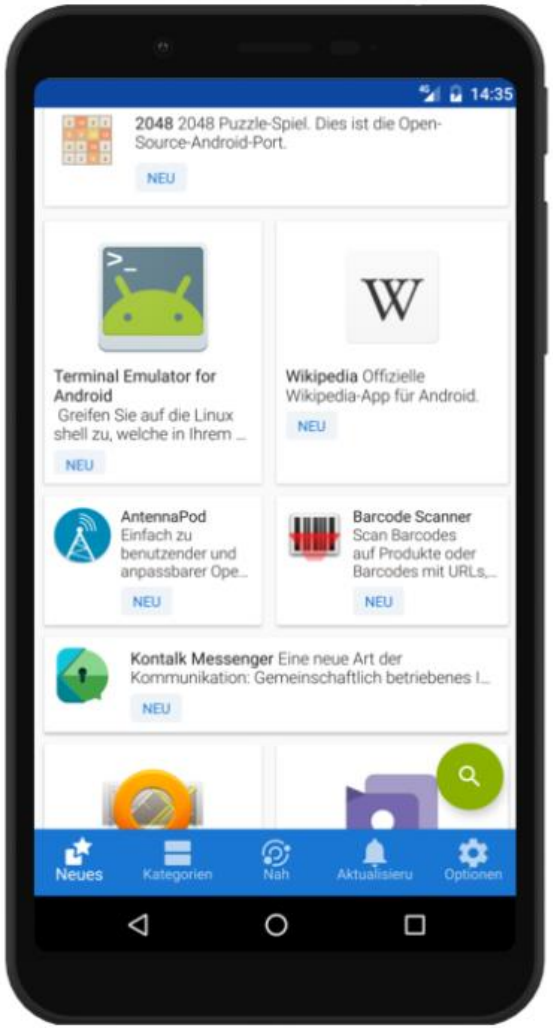
F-Droid

Netzwerk sii Baden-Württemberg

Was ist F-Droid?

F-Droid ist ein installierbarer Katalog mit FOSS-Apps (Free and Open Source Software) für Android. Der Client vereinfacht die Suche und Installation von Apps und behält den Überblick über Aktualisierungen.

F-DROID HERUNTERLADEN



Ist F-Droid sicher?

In den F-Droid-Katalog werden nur freie, quelloffene und zuvor von ehrenamtlichen Unterstützern geprüfte Apps aufgenommen. Das komplette Angebot ist kostenlos, eine Registrierung ist nicht erforderlich und es werden auch sonst keine Daten erhoben.

Mobilsicher.de - 07.03.2018

Alternativen zu Google-Playstore?

Neben Google-Playstore gibt es auch alternative App-Stores, bei welchen es z.T. App gibt, die im Google-Playstore kostenpflichtig zu erhalten sind. Aber Vorsicht, darunter könnten sich auch Malware-Apps befinden.

- Praxistipp von CHIP

SIT

Notfall-Katstrophen-App

Netzwerk sii Baden-Württemberg

Andere Gefahren für und Katastrophen

Nora-App

Notruf-App der Bundesländer

- Überall in Deutschland nutzbar
- Für alle Notfall- oder Unwetter-Meldungen
- Durch Registrierung erspart man sich die Nennung des Namens (Ersatz des Fax-Notrufs für Taubstumme).
- Stiller Notruf in Gefahrensituationen möglich
- Weitere Infos:
  https://www.nora-notruf.de/de-as/fragen/faq#236

Katwarn-App

- Öffentlichen Versicherer und Fraunhofer-Institut FOKUS
- Warnmeldungen von Bund und Ländern, Behörden- und Organisationen der angeschlossenen Landkreise und Städte, von Nutzern sowie von Betrieben kritischer Infrastrukturen. Dazu zählen auch Feuerwehr-Leitstellen, Polizei-Dienststellen, der Deutsche Wetterdienst, Hochwasser- und Erdbebenzentralen.
- Auch per SMS oder Email
  https://www.katwarn.de/anmeldung-mail-sms.php

NINA-App

NINA

Notfall-Informations- und Nachrichten-App

Warnungen fürs Smartphone

NINA-App kostenlos installieren

QR-Code scannen und direkt aus dem passenden Store herunterladen.

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
- Bevölkerungsschutzes, des Deutschen Wetterdienstes sowie lokale Hochwassermeldungen der Bundesländer.
- Karte mit bundesweiten Gefahren
- Verhaltenstipps für bestimmte Katastrophen-Szenarien.
- Derzeit Informationen zur Corona-Pandemie.

SIT

Netzwerk sii Baden-Württemberg

Herzlichen Dank!

Bleiben Sie sicher und engagiert!