Ransomware

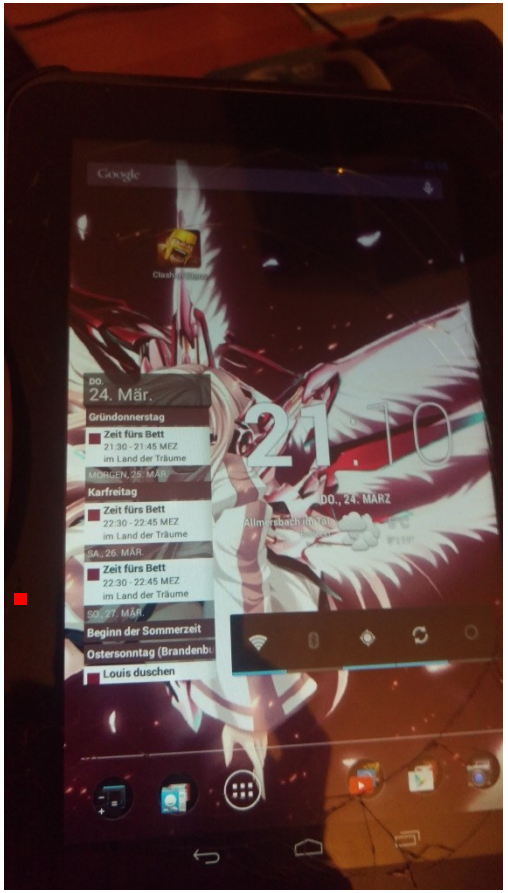
auf Tablet und Smartphone

Referent

Netzwerkadministration
IT-Sicherheit
Firewall- und IDS Infrastruktur

Agenda

- Ransomware
  - Aktuelle Situation
  - Rechtlicher Hintergrund
  - Ein Beispiel
    - Was ist zu tun?
    - Erste Hilfe
  - Schutz und Vorbeugung
- Workshop



AKTUELLE SITUATION

Ransomware,

auch Erpressungstrojaner, Kryptotrojaner oder Verschlüsselungstrojaner, sind Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Dabei werden private Daten auf einem fremden Computer verschlüsselt oder der Zugriff auf sie wird verhindert, um für die Entschlüsselung oder Freigabe ein „Lösegeld“ zu fordern.

Wikipedia

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

RECHTLICHER HINTERGRUND

Tatbestände

Erpressung und Computersabotage

Strafgesetzbuch

Besonderer Teil (§§ 80 - 358)

20. Abschnitt - Raub und Erpressung (§§ 249 - 256)

Strafgesetzbuch

Besonderer Teil (§§ 80 - 358)

27. Abschnitt - Sachbeschädigung (§§ 303 - 305a)

(1) Wer einen
zu einer Handl
oder eines an
Freiheitsstrafe

(2) Rechtswid
angestrebten

(3) Der Versuc

§ 303b
Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

RECHTLICHER HINTERGRUND

Die Realität

Strafgesetzbuch

Besonderer Teil (§§ 80 - 358)

20. Abschnitt - Raub und Erpressung (§§ 249 - 256)

Strafgesetzbuch

Besonderer Teil (§§ 80 - 358)

27. Abschnitt - Sachbeschädigung (§§ 303 - 305a)

(1) Wer einen
zu einer Handl
oder eines an
Freiheitsstrafe

(2) Rechtswid
angestrebten

(3) Der Versuc

§ 303b
Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

WER ist der Täter und WO ist er?
WIE sichern Sie Beweise?
WAS machen Sie jetzt?

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

RECHTLICHER HINTERGRUND

Die Realität

Es ist ein Businessmodell – auf beiden Seiten!

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

RECHTLICHER HINTERGRUND

A Dark Web Hacker Is Offering Ransomware for Free

May 28, 2015 // 06:40 AM EST

Ransomware is a real pain. It's a type of virus that infects a target's computer, encrypts their files, and keeps them locked out until the victim pays a hefty lump sum, often in bitcoin.

For this, a blackmailer would usually either make their own ransomware program, or buy one ready-made from a forum or marketplace. Now, one dark web hacker has taken a crowdsourced approach to generating income: 'Tox' has released their own free ransomware for anyone to download and distribute. Users just have to cut the creator in on any profits.

It takes only a few seconds to set up an account on the host site (also called Tox), and you don't need to provide an email or any other identifying information. A user then types in the ransom amount they want to ask for, an additional note such as the name of the target, and clicks "Create". The custom ransomware—which is designed to work on Windows systems—is then available to download and spread.

Image: Screenshot from the Tox site

"Once you have downloaded your virus, you have to infect people," writes Tox, who

Die Realität

Es ist ein Businessmodell – auf beiden Seiten!

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

Hilfe!

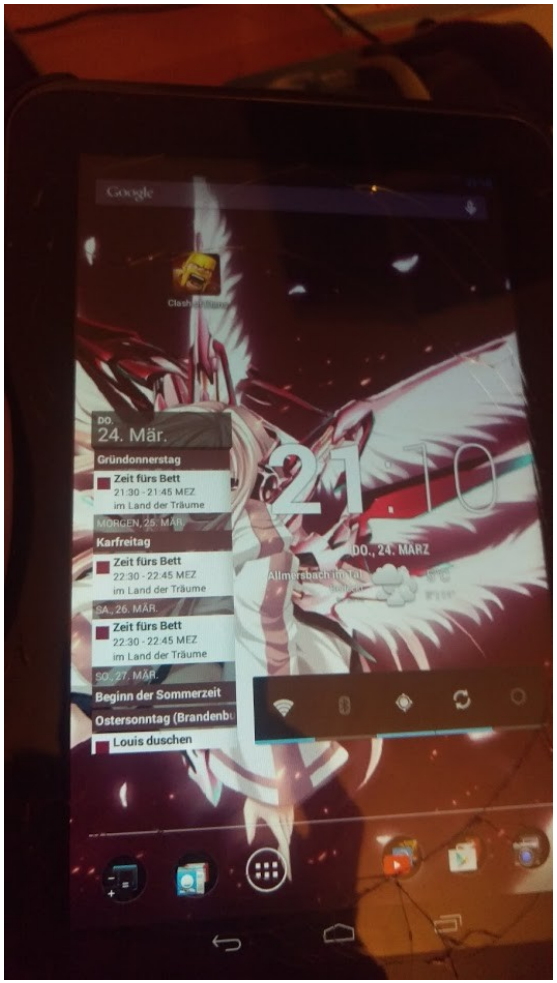
AKTUELLE SITUATION

Haben Sie ein Handtuch?
Wo ist ihr Babelfish?

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

Don´t panic !

EIN BEISPIEL



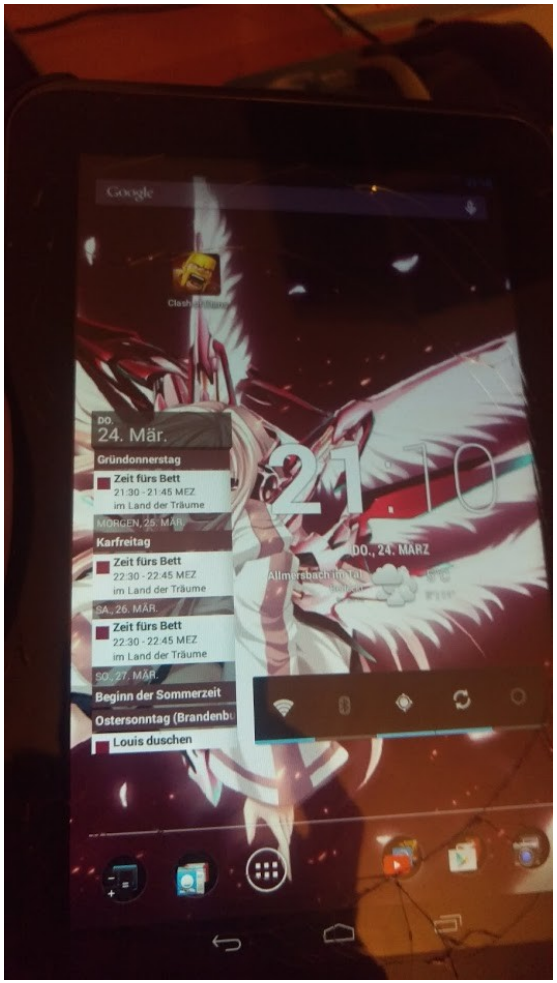
Eine persönliche Erfahrung

Im Kino: 24.03.2016
Starring: mein Sohn
sein Galaxy Tab 2
Android 4
Minecraft
Minecraft Mods
Das Internet

Oder:
„warum man nicht einfach was installieren sollte...“
Und:
„warum Papa´s Paranoia doch wenigstens manchmal ganz gut ist“

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

EIN BEISPIEL

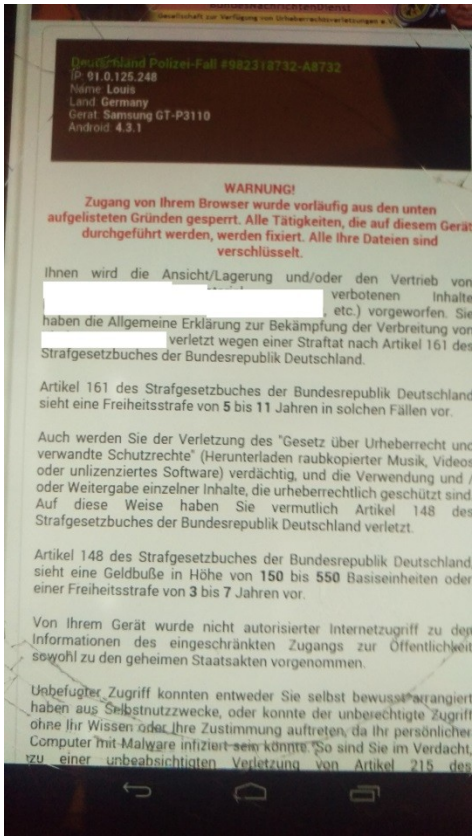


Minecraft:

- Installation einer App, um zu „modden“ – Sideload!
- Internet Link zum Download
- Anfrage von „Geräteadministrator“-Berechtigung

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

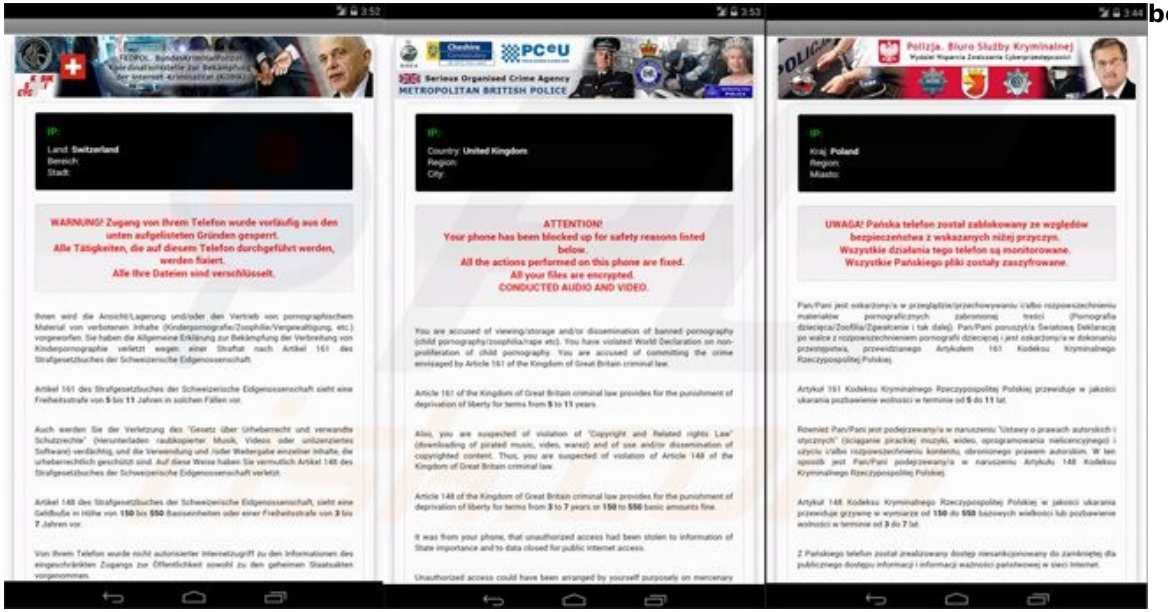
EIN BEISPIEL



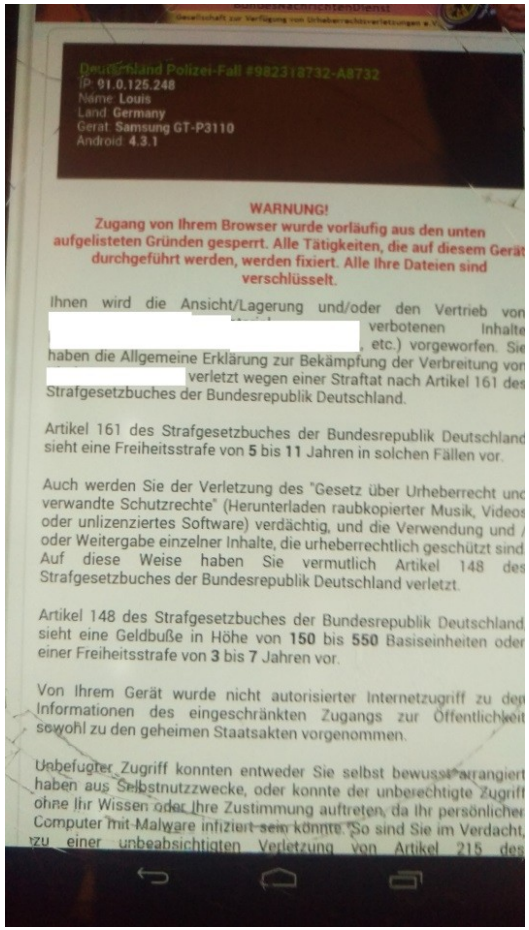
Und schon ist´s passiert:

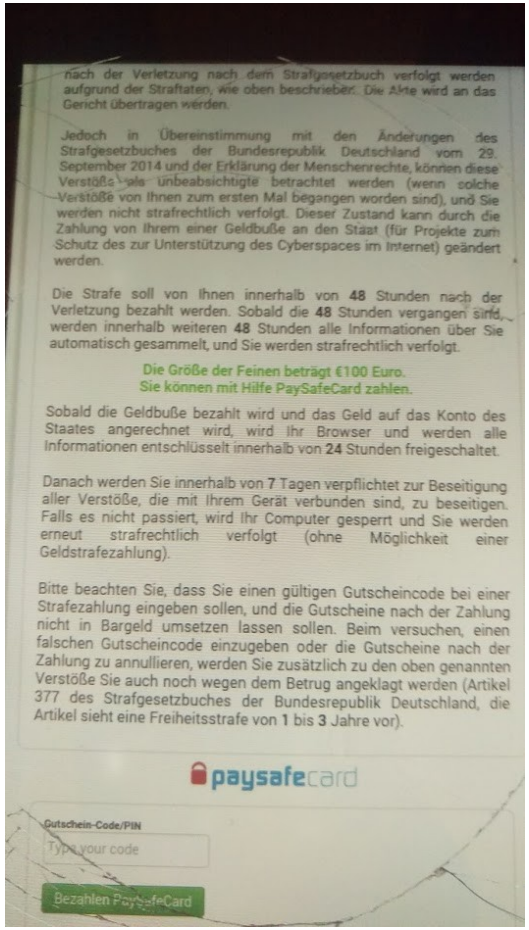
- Anzeige einer Lösegeldforderung
- Sperrung des Zugriffs auf das Gerät

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und beugung



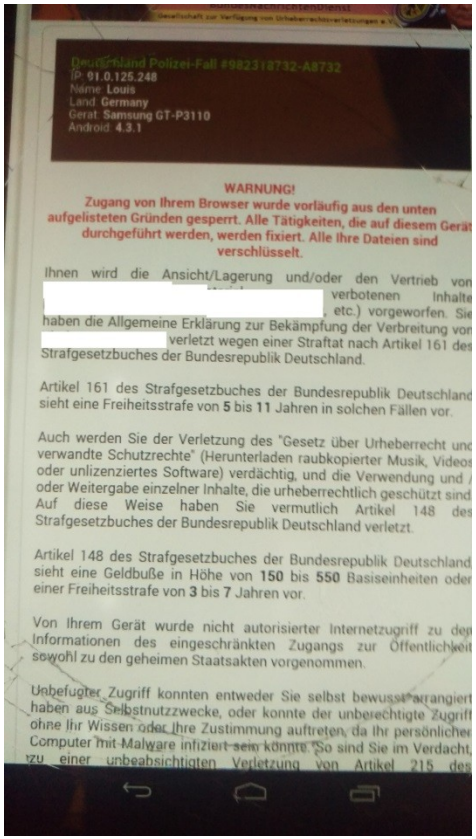
EIN BEISPIEL





Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

WAS IST ZU TUN?



Don´t panic

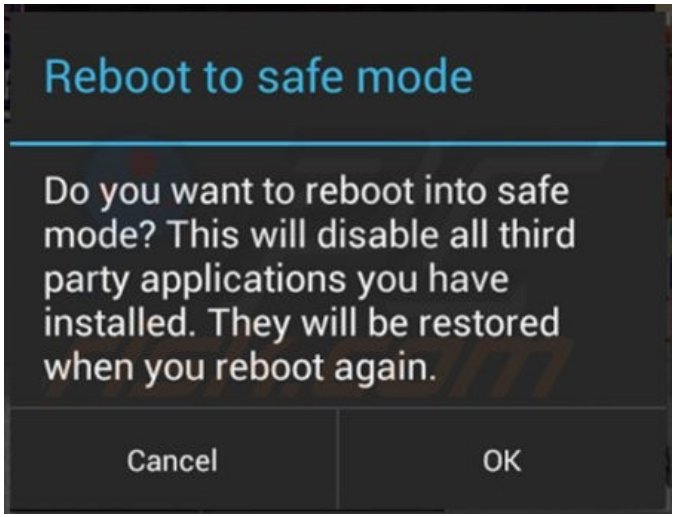
1) Fotos machen !!!
2) Don´t panic !!!
3) Backup vorhanden?
4) Tablet herunterfahren
5) Tablet I‘m RECOVERY Modus neu starten

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

WAS IST ZU TUN?

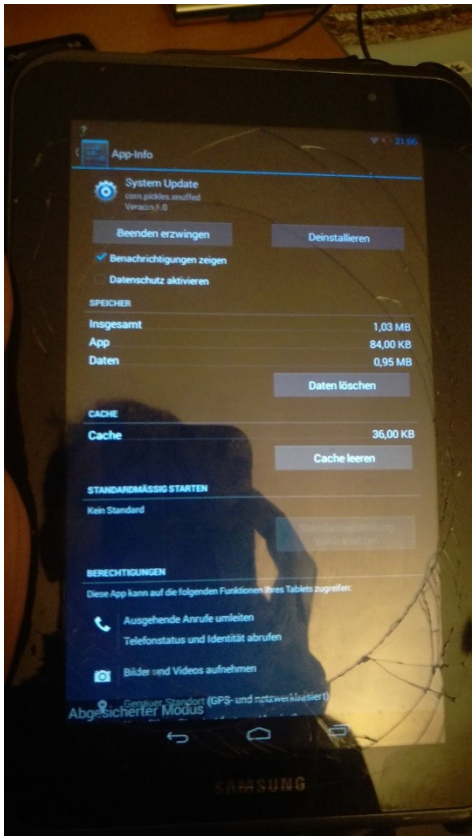
„Safe“ Modus
POWER und LAUTSTÄRKE LEISER bzw LAUTSTÄRKE LEISER und LAUTSTÄRKE LAUTER zeitgleich drücken und halten, bis das Tablet bootet.

Android startet OHNE die automatisch gestarteten Dienste und Apps

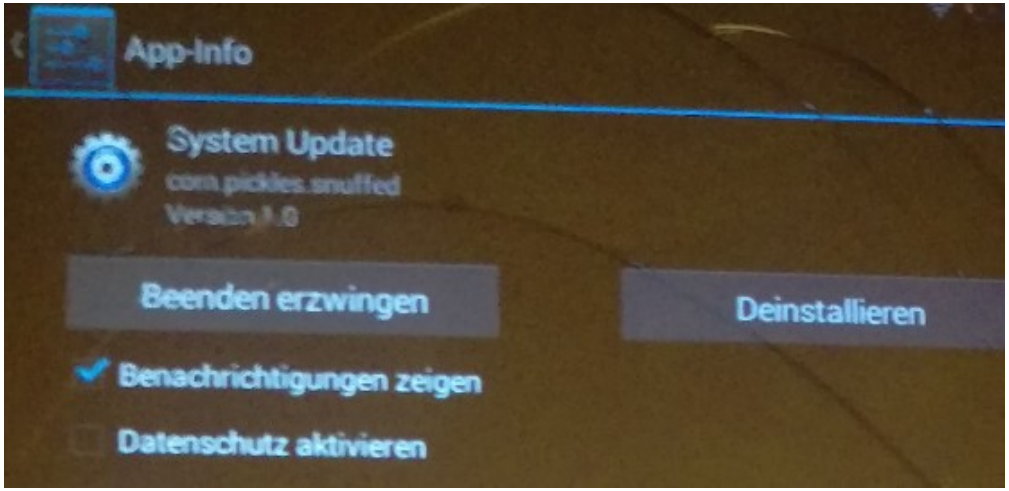


Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

WAS IST ZU TUN?



„Safe“ Modus
Wir suchen in der Liste der installierten Apps nach Auffälligkeiten und finden dies hier
APPS-APPLICATION MANAGER – SYSTEM UPDATE



Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

ERSTE HILFE

Checkliste

1. Reboot im SAFE MODE
2. Entfernen der App
   1) FAIL? -> Continue
   2) Reboot im RECOVERY MODE
   3) Reset auf „Factory default“
      - Reboot
      - FAIL? -> Continue

   Flash STOCK ROM oder CUSTOM ROM

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

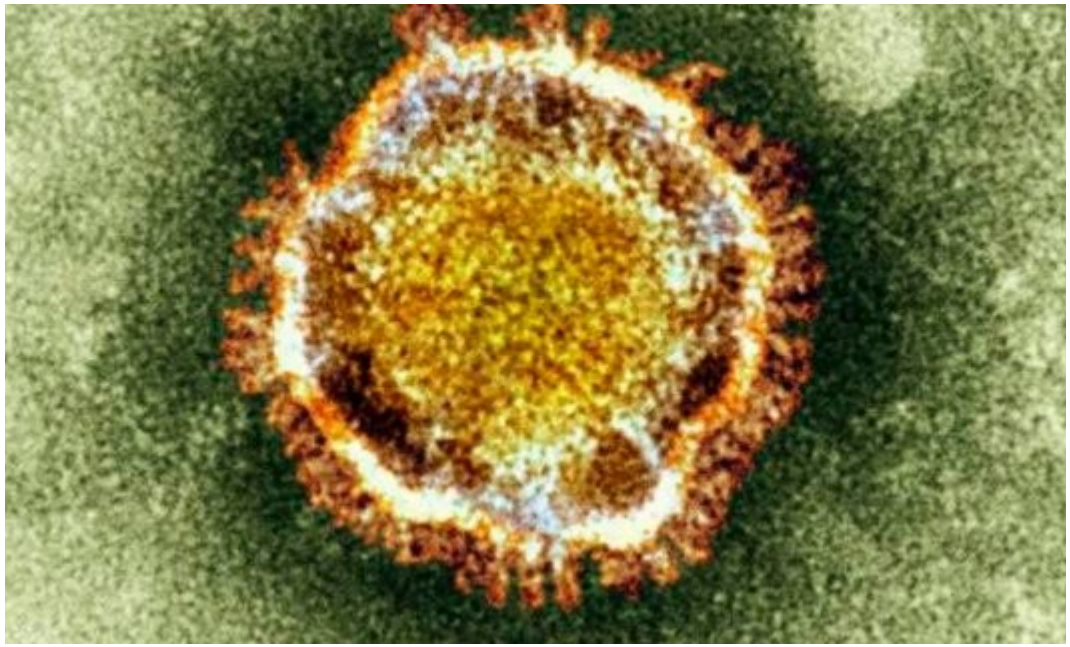
SCHUTZ & VORBEUGUNG

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

SCHUTZ & VORBEUGUNG

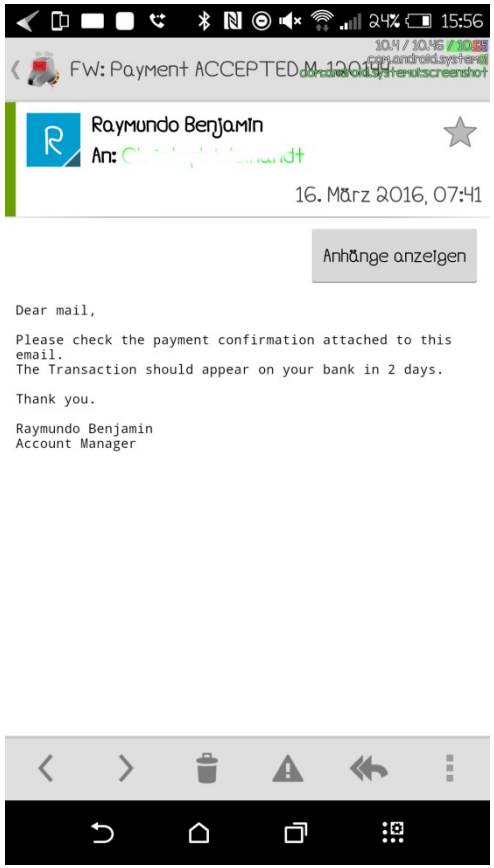
Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

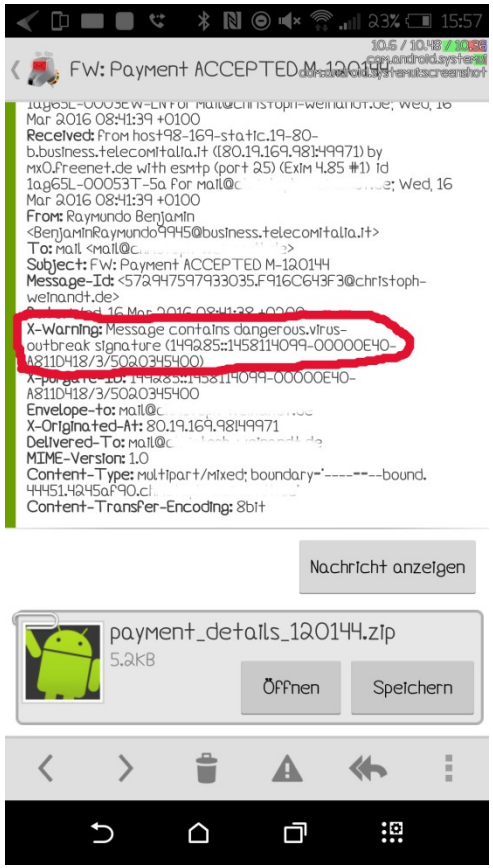
SCHUTZ & VORBEUGUNG



Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

SCHUTZ & VORBEUGUNG





Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

SCHUTZ & VORBEUGUNG

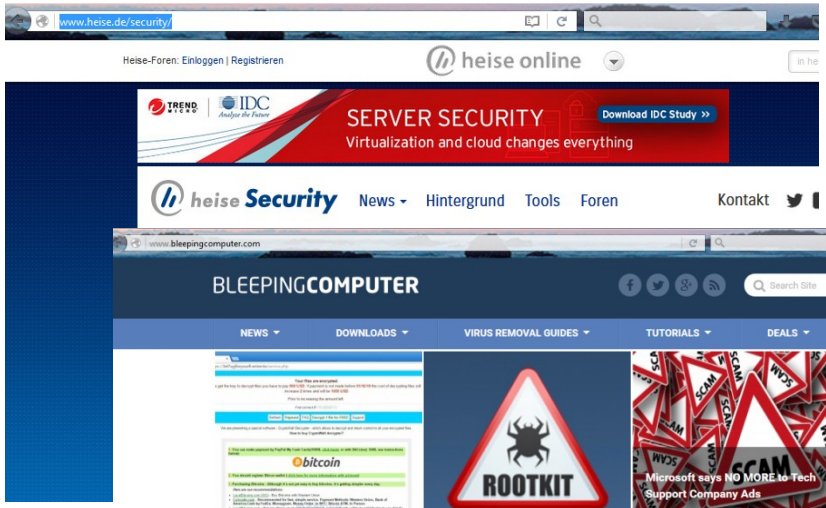
Merkliste

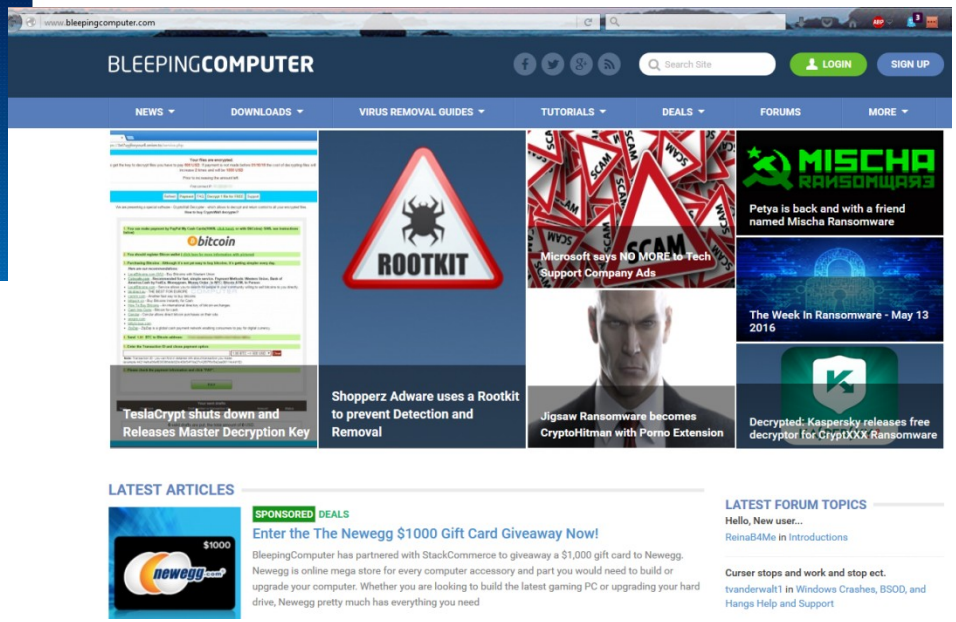
1. Kein SIDELOAD – NUR Google Play oder Amazc App Shop
2. Backup!
3. Kontrolle der Berechtigungen
4. Fotos und möglichst alles auf Speicherkart ablegen
5. Cloud Sync (Google Fotos, Dropbox usw)

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung

Danke für Ihre Aufmerksamkeit!

WEITERFÜHRENDE LINKS





Sites

1. Heise Security -
2. Bleeping Computer – Ransomware und Trojane und Virus

Agenda
Aktuelle Situation
Rechtlicher Hintergrund
Ein Beispiel
Was ist zu tun?
Erste Hilfe
Schutz und Vorbeugung