



## Ransomware auf Tablet und Smartphone

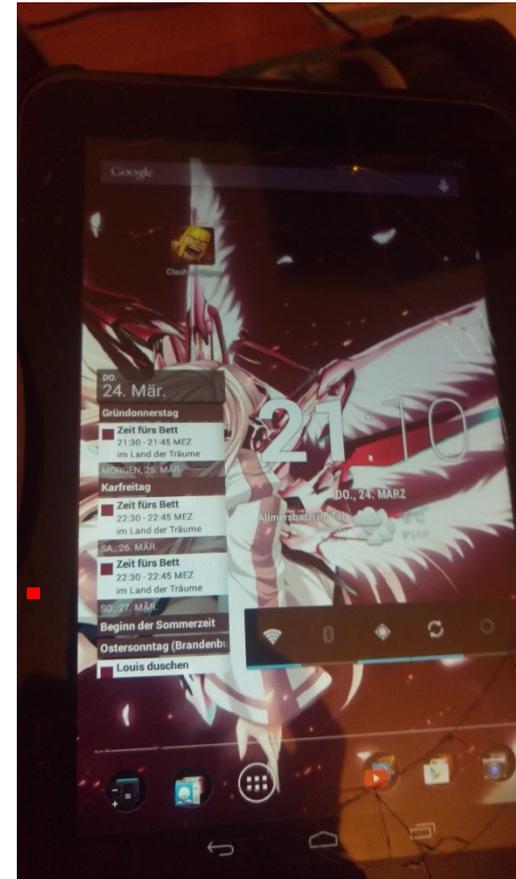
## Referent



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.

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

Wikipedia

## RECHTLICHER HINTERGRUND

### Tatbestände Erpressung und Computersabotage

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

#### Strafgesetzbuch

Besonderer Teil (§§ 80 - 358)

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

#### Strafgesetzbuch

Besonderer Teil (§§ 80 - 358)

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

#### § 303b

#### Computersabotage

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

(2) Rechtswid  
angestrebten

(3) Der Versuch

(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.

## RECHTLICHER HINTERGRUND

### Die Realität

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**

#### Strafgesetzbuch

Besonderer Teil (§§ 80 - 358)

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

#### Strafgesetzbuch

Besonderer Teil (§§ 80 - 358)

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

#### § 303b

#### Computersabotage

(1) Wer einen zu einer Handlung oder eines anderen Freiheitsstrafe

(2) Rechtswidrig angestrebten

(3) Der Versuch

(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.

## 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



**Mehrere Millionen von Menschen waren auf der ganzen Welt betroffen...**

**...dass es Cyberkriminelle auf ihr Geld abgesehen haben und sich das Geld durch Lösegeldzahlungen von den Opfern zahlen lassen.**

Die Hälfte der Betroffenen ist bereit, Geld zu zahlen – auch wenn die Daten niemals zur Verfügung gestellt werden.

LAND	BETROFFENE, DIE WIEDERHERSTELLUNG DER DATEN GEZAHLT HABEN
USA	50%
Deutschland	33%
Rumänien	48%
Frankreich	N/A
Großbritannien	44%
Dänemark	30%

**>\$1 Mio**

beträgt der monatliche Schaden, den CryptoWall und andere Varianten der neuesten und bedeutendsten Ransomware verursacht haben.

**\$3000**

ist der Preis für das Cryptolocker / Cryptowall 3.1 Ransomware Kit, das sogar den Quellcode zusammen mit einem Handbuch und kostenlosem Support beinhalten soll.



## 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.

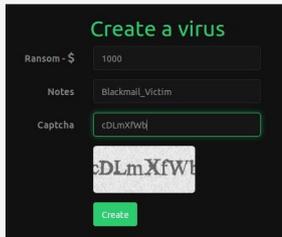


Image: Screenshot from the Tox site

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

## Die Realität

Es ist ein Businessmodell – auf beiden Seiten!

Ist **KOSTENLOSE** Antivirus-Software die richtige Lösung für Sie?

Kostenlose Antivirus-Software **NIEDRIG**

SCHUTZSTUFE **Antivirus Antispyware**

**Norton™ Security Standard Abonnement\* 1 Gerät**

SCHUTZSTUFE **Antivirus Antispyware Identitätsdiebstahl Virenentfernungsversprechen SPAM Ant**

1 Jahr/1 Gerät

39,99€  
24,99€ **Jetzt abonnieren** Kostenlose Testversion

**38% RABATT** Angezeigter Preis gilt für die ersten drei Monate\*

### Beseitigt Bedrohungen, Ihren PC und Mac gefährden

Virenschutzversprechen: Viren entfernt oder Geld zurück

Antivirus/AntiSpyware/AntiMalware

Schutz vor Identitätsdiebstahl

Wirkt sich nicht auf die Geschwindigkeit Ihres Geräts aus

Erkennt bösartige Dateien

### Schützt Ihre Mobilgeräte

Schützt Ihr Android- oder iOS-Smartphone oder -Tablet

Scannt nach gefährlichen Apps und entfernt sie

Scannt nach Apps, die Datenschutzrisiken bergen und einen hohen Akku-/Datenverbrauch aufweisen

Zeigt Ihnen den genauen Standort Ihres verlorenen oder gestohlenen Telefons/Tablets an

### Wahrt Ihre Privatsphäre

Speichern Sie Ihre Benutzernamen und Kennwörter sicher und bequem

Scannt Facebook und andere Websites nach verdächtigen Links

2-Wege-Firewall

Blockieren von Spam-E-Mails

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

# Hilfe!

## **AKTUELLE SITUATION**

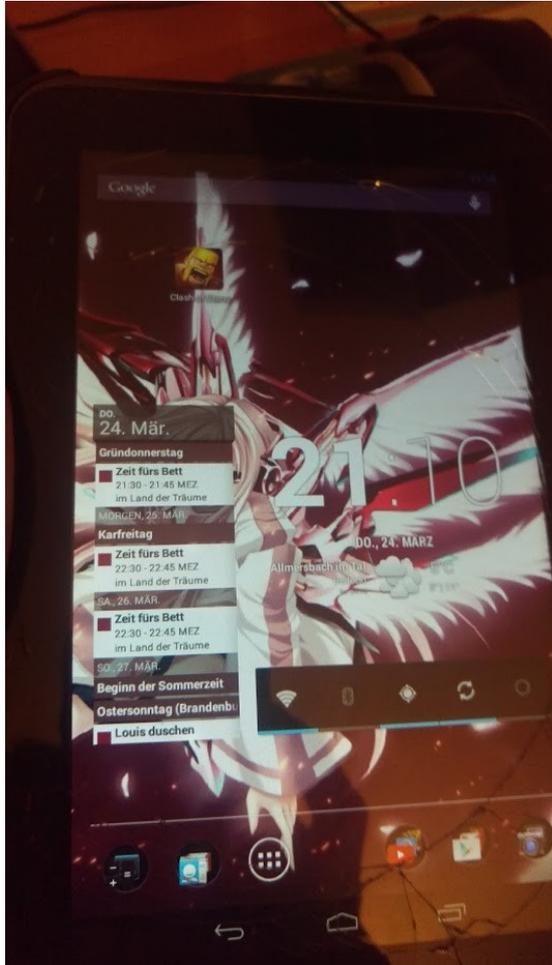
Haben Sie ein Handtuch?  
Wo ist ihr Babelfish?



**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:

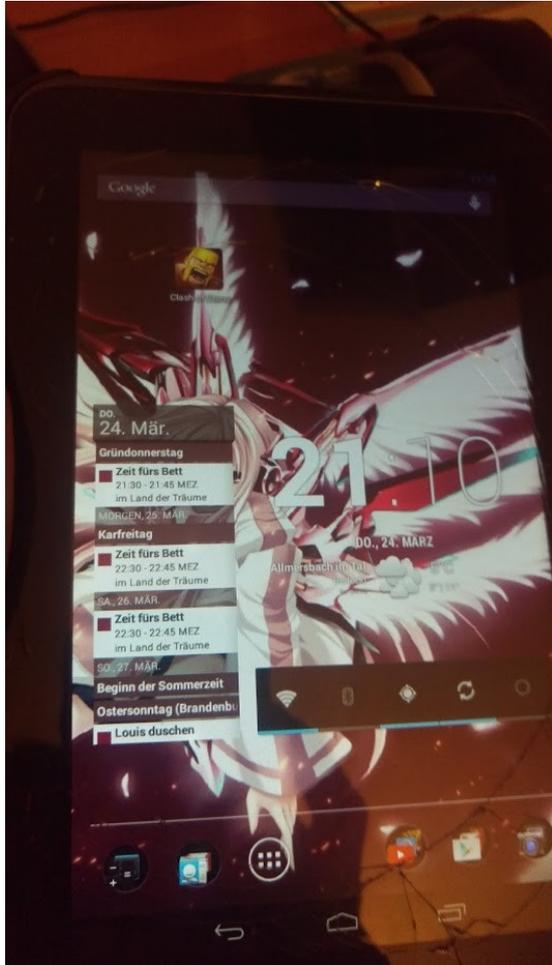
„warum man nicht einfach was installieren sollte...“

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

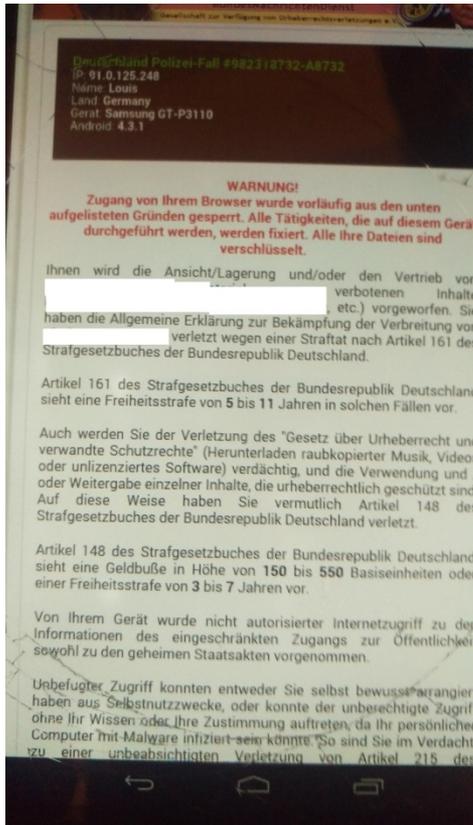


### Minecraft:

- 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



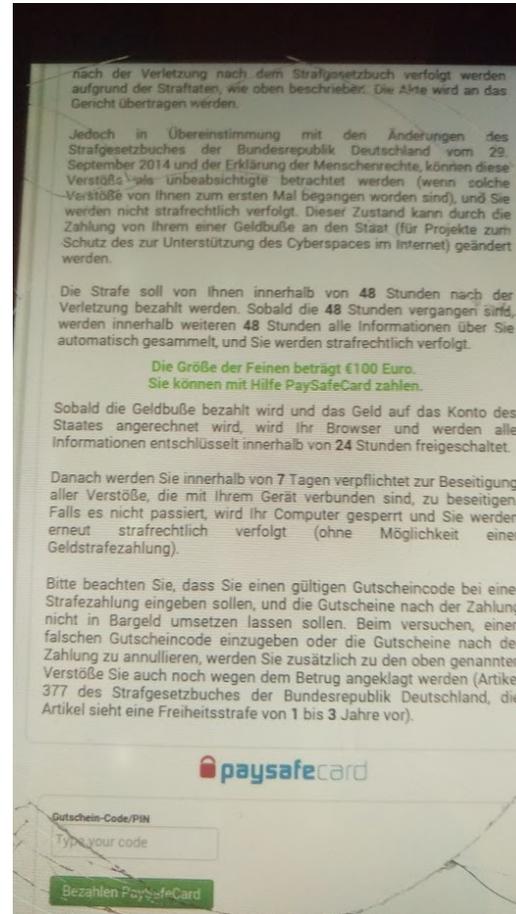
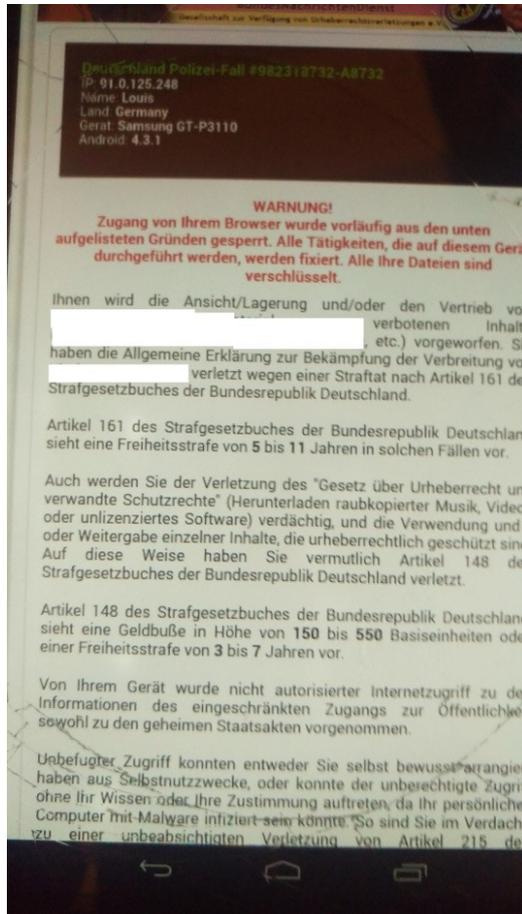
### Und schon ist's passiert:

- Anzeige einer Lösegeldforderung
- Sperrung des Zugriffs auf das Gerät

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

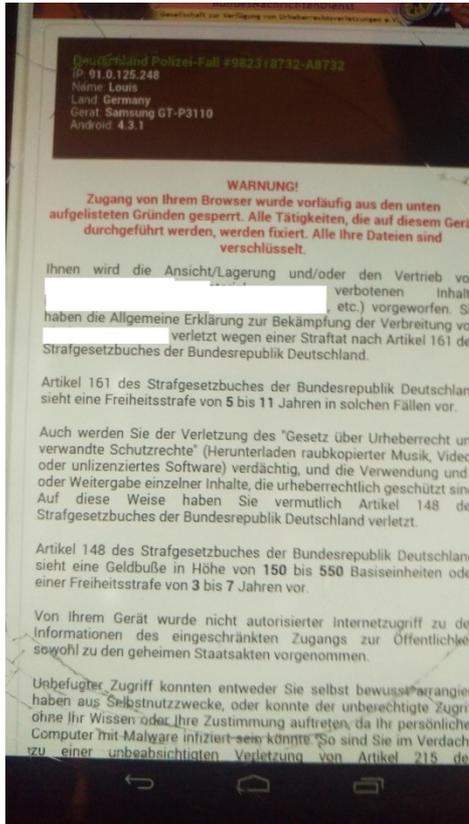


## EIN BEISPIEL



**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

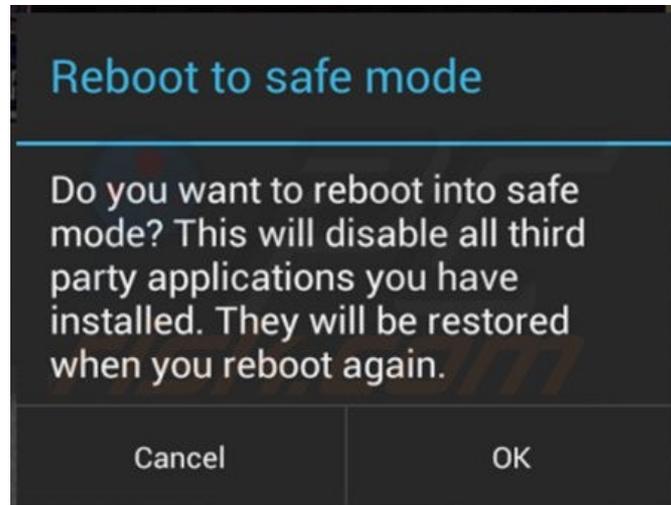
**Agenda**  
**Aktuelle**  
**Situation**  
**Rechtlicher**  
**Hintergrund**  
**Ein Beispiel**  
**Was ist zu**  
**tun?**  
**Erste Hilfe**  
**Schutz und**  
**Vorbeugung**

## WAS IST ZU TUN?

### „Safe“ Modus

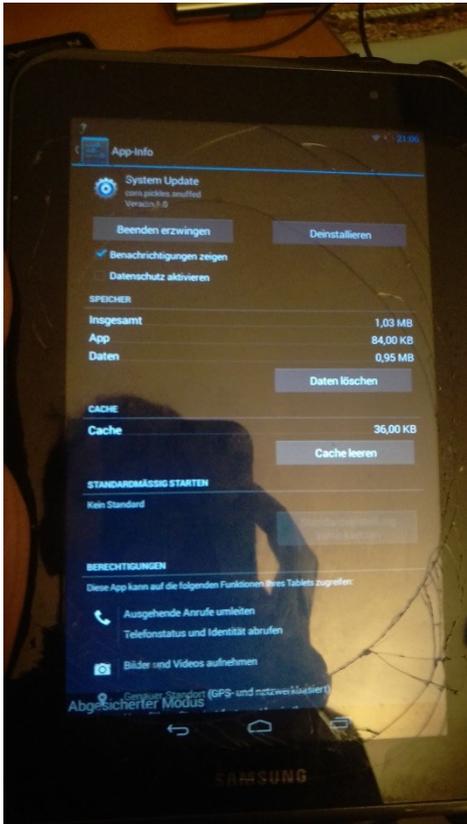
POWER und LAUTSTÄRKE LEISER bzw LAUTSTÄRKE LEISER und LAUTSTÄRKE LAUTER zeitgleich drücken und halten, bis das Tablet bootet.

Android startet OHNE die automatisch gestarteten Dienste und Apps



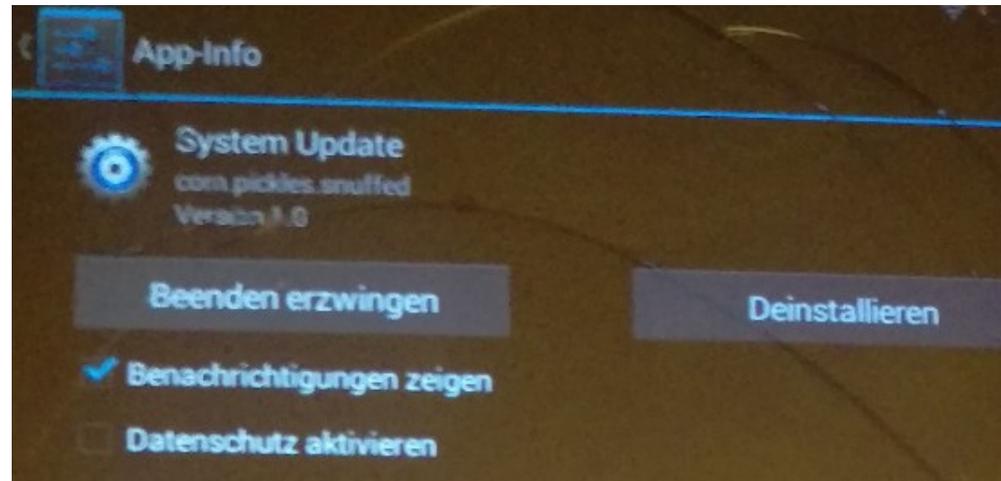
**Agenda**  
**Aktuelle**  
**Situation**  
**Rechtlicher**  
**Hintergrund**  
**Ein Beispiel**  
**Was ist zu**  
**tun?**  
**Erste Hilfe**  
**Schutz und**  
**Vorbeugung**

## 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**



# Google play

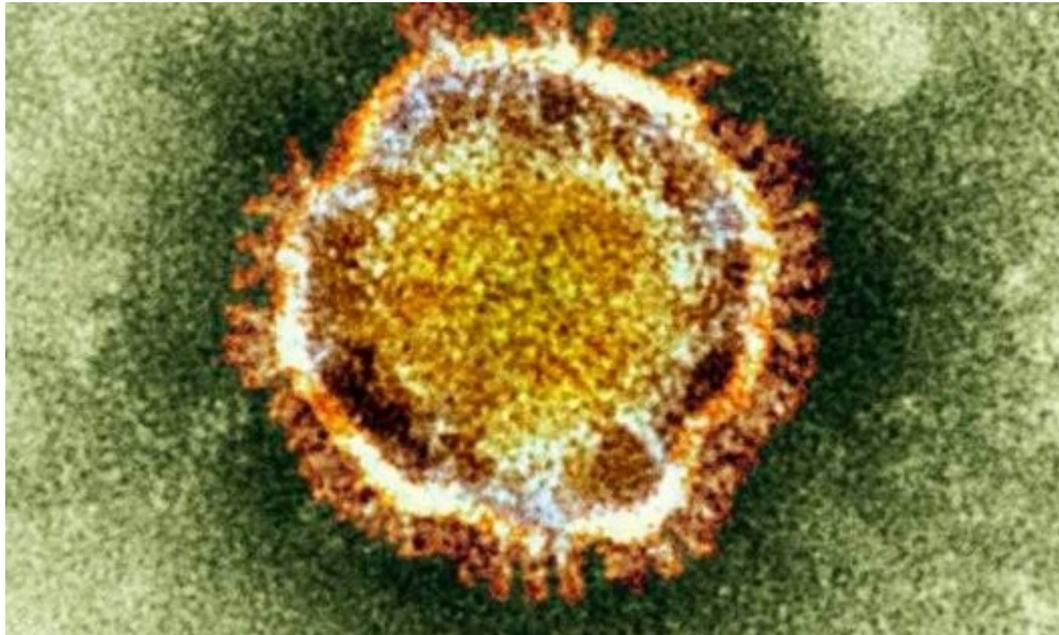
**Agenda**  
**Aktuelle**  
**Situation**  
**Rechtlicher**  
**Hintergrund**  
**Ein Beispiel**  
**Was ist zu**  
**tun?**  
**Erste Hilfe**  
**Schutz und**  
**Vorbeugung**

## **SCHUTZ & VORBEUGUNG**



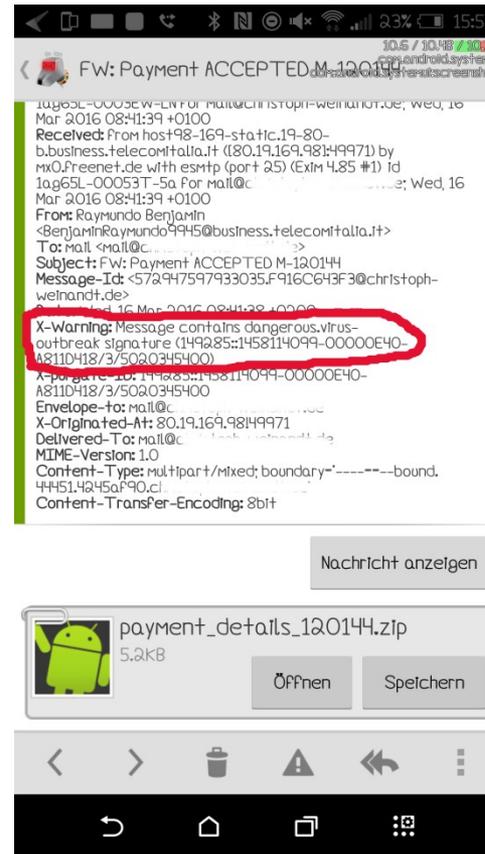
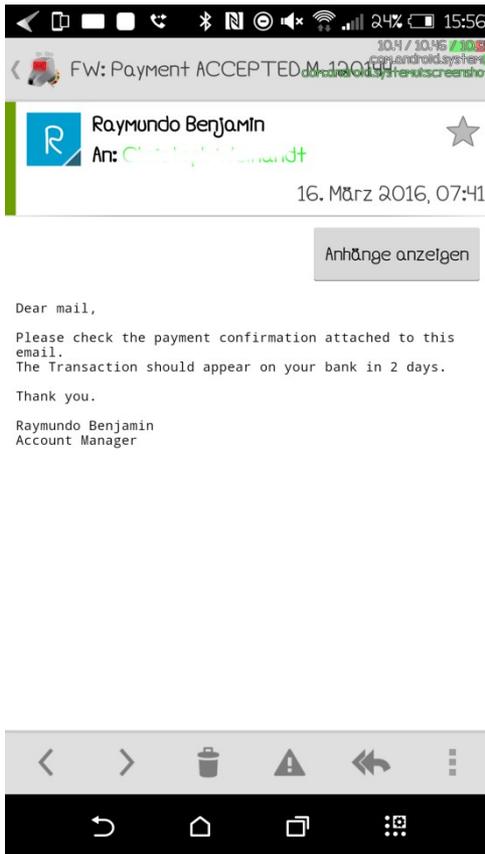
**Agenda**  
**Aktuelle**  
**Situation**  
**Rechtlicher**  
**Hintergrund**  
**Ein Beispiel**  
**Was ist zu**  
**tun?**  
**Erste Hilfe**  
**Schutz und**  
**Vorbeugung**

## **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**

### **Merklste**

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 Trojaner und Virus

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

