

Cybercrime ... und die Mühle steht



FRIESSNIK Erhard

Bundesministerium für Inneres
Bundeskriminalamt – Büro 5.2

Agenda

- Technische Entwicklung und Digitalisierung
- Entwicklung Cybercrime
- Aktuelle Phänomene und Herausforderungen
- Präventive und reaktive Maßnahmen



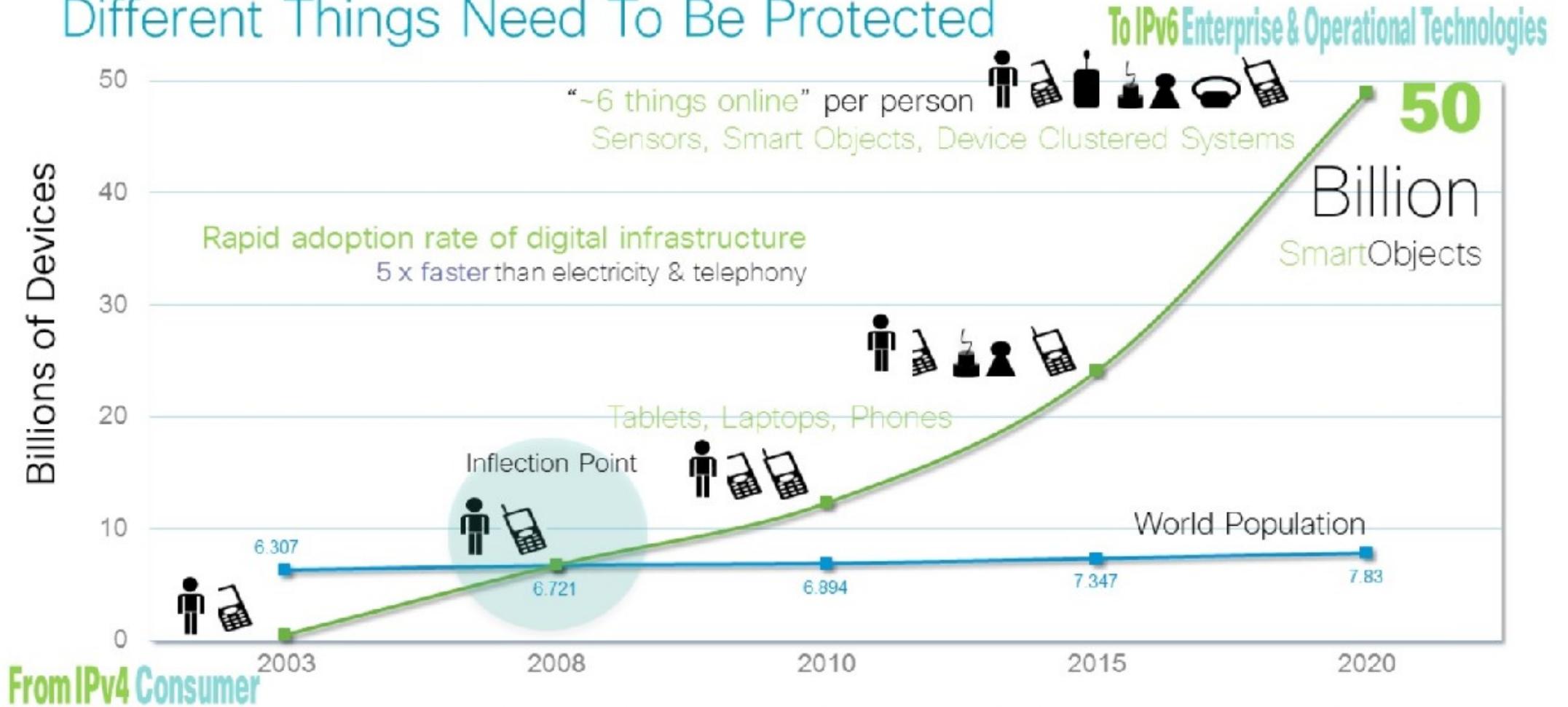
- **Landwirtschaft 4.0**
 - Einsatz von Robotern / Drohnen
 - Selbstfahrende Arbeitsmaschinen
 - Sensorik
- **Precision Farming**
 - Gezielte Aussaat
 - Bewässerung
 - Düngung
- **Digital Farming**
 - Feuchtigkeit
 - Temperatur
 - Stickstoff



- OT – Steuerungen
- Direkter Datenaustausch
- Agrarmanagementsoftware
- Mobile Endgeräte – Smartphones
- Tablets



Different Things Need To Be Protected



Source: Cisco IBSG projections, UN Economic & Social Affairs <http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf>

Cybersecurity



Cybercrime





 [Digital Life](#)

Hacker wollen 5 Millionen Euro von Land Kärnten

25.05.2022

Hackergruppe behauptet, Daten abgesaugt zu haben.
Beweise dafür gibt es nicht.

**futurezone
Newsletter**

Email*

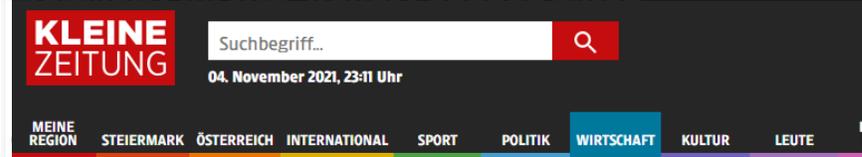
max.mustermann@gr



Foto: thinkstockphotos.de

McAfee-Studie 22.02.2018 10:34

Weltweit 600 Mrd. Dollar Schaden durch



KLEINE ZEITUNG
Suchbegriff...
04. November 2021, 23:11 Uhr
MEINE REGION STEIERMARK ÖSTERREICH INTERNATIONAL SPORT POLITIK WIRTSCHAFT KULTUR LEUTE

Startseite > Wirtschaft

Cyberangriffe nehmen zu | Einfallspunkt Cybercrime als "Acht-Stunden-Job"

Kriminelle Krisengewinner: Inmitten der globalen Pandemie wuchs das Geschäft sich und bietet Schadsoftware immer häufiger zum Mieten an. Was Unternehmen

Von Roman Vilgut, Markus Zottler | 05.30 Uhr, 31. August 2021

Quelle der Cl



Dass die weltumspannende Pandemie einen Digitalisierungsschub auslöste, gilt längst als



ZDNet CLOUD STORAGE IOT MOBILE SICHERHEIT NETZWERKE KMU



Unified Communications & Collaboration
silicon.de Kundenbeziehungen verbessern

ZDNet / Sicherheit / Cyberkriminalität

Ransomware: Webhoster zahlt 1 Million Dollar

DIGITAL LIFE

08.02.2018

430 Millionen Schaden: Cybercrime-Ring aufgeflogen



© APA

US-Behörden haben einen groß angelegten Betrug eines internationalen Rings von Cyberkriminellen aufgedeckt.

WELS

Haberfellner-Mühle im Visier von Cyberkriminellen

Von Michaela Krenn-Aichinger 05. Oktober 2017 00:04 Uhr



Vermutlich von Indien aus hackten sich Internetkriminelle in den Adressverteiler des Grieskirchner Betriebes.
Bild: GRIESKIRCHEN. Unternehmen warnt vor Fake-E-Mails mit Geldforderungen

Cyberangriff legt Produktion beim Traktorenhersteller Fendt lahm

Am Fendt-Stammsitz in Marktoberdorf stehen die Bänder nach einer Cyberattacke still. Details sind noch unklar, die Konzernmutter spricht von Erpressung.



Christof Kerkmann



Anja Müller

09.05.2022 • Update: 09.05.2022 - 14:54 Uhr • [Kommentieren](#) • [1 x geteilt](#)

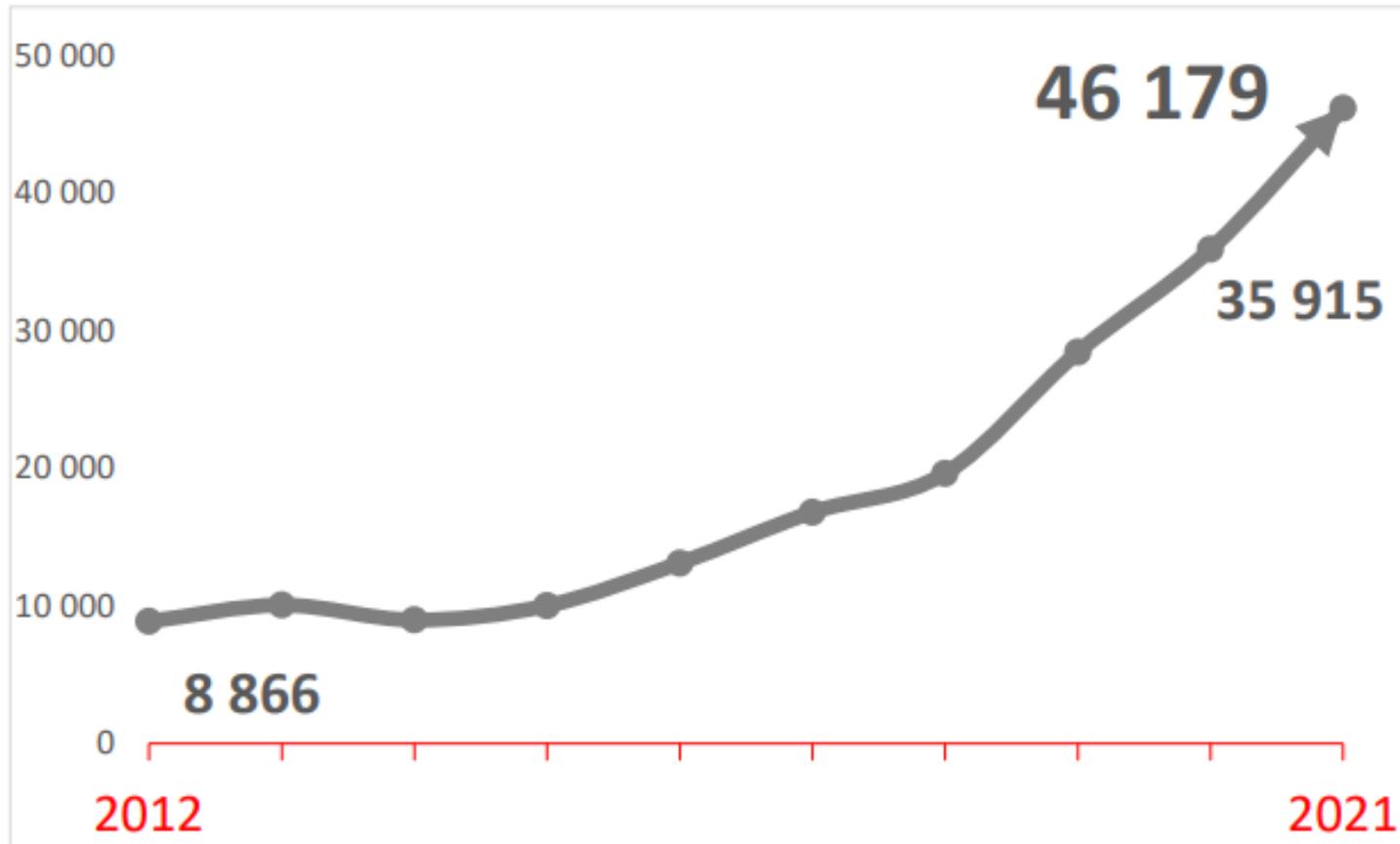


Cybercrime damages are predicted to cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015.



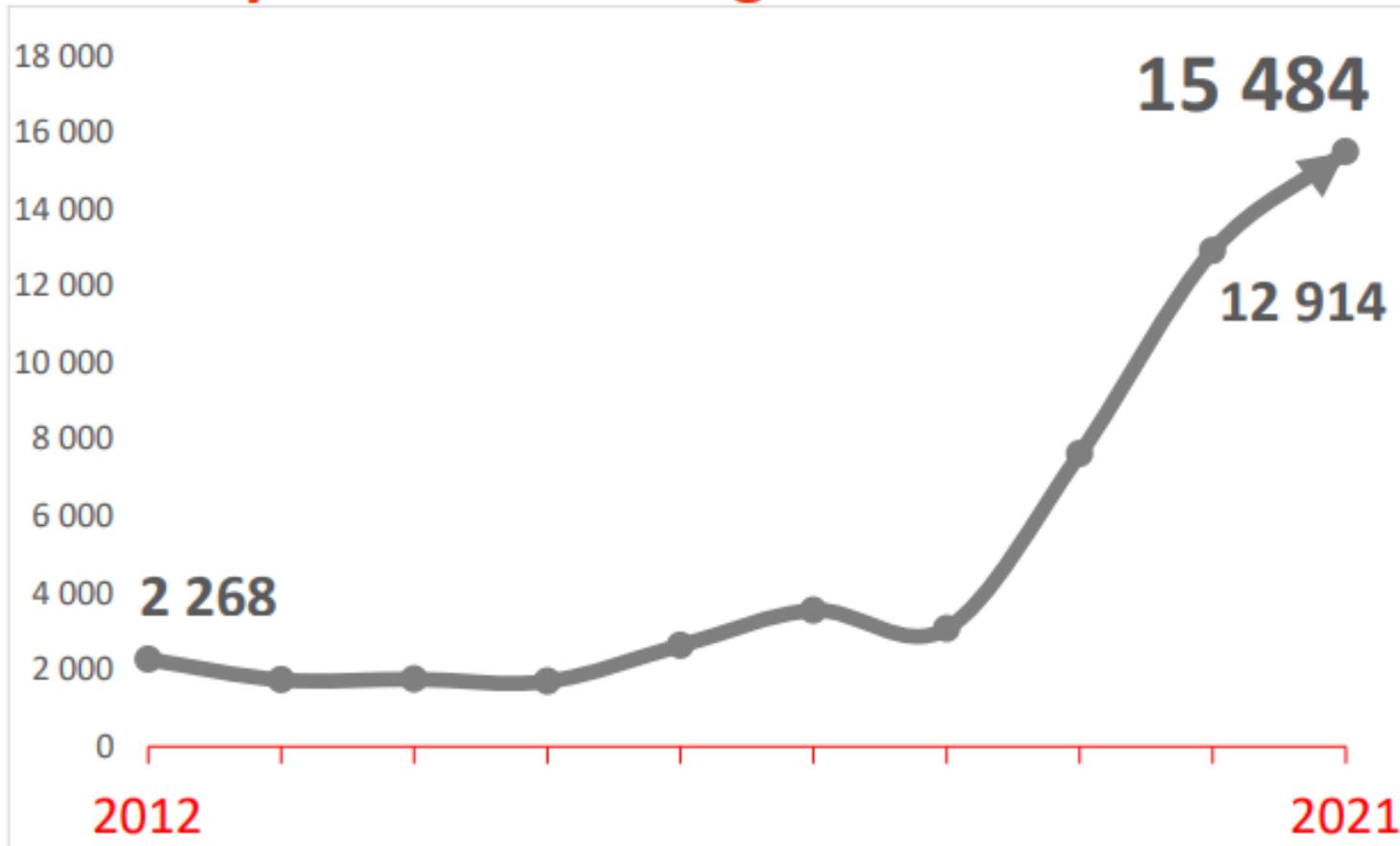
Trillion = 1.000.000.000.000 = 10^{12}

Kriminalität im Internet



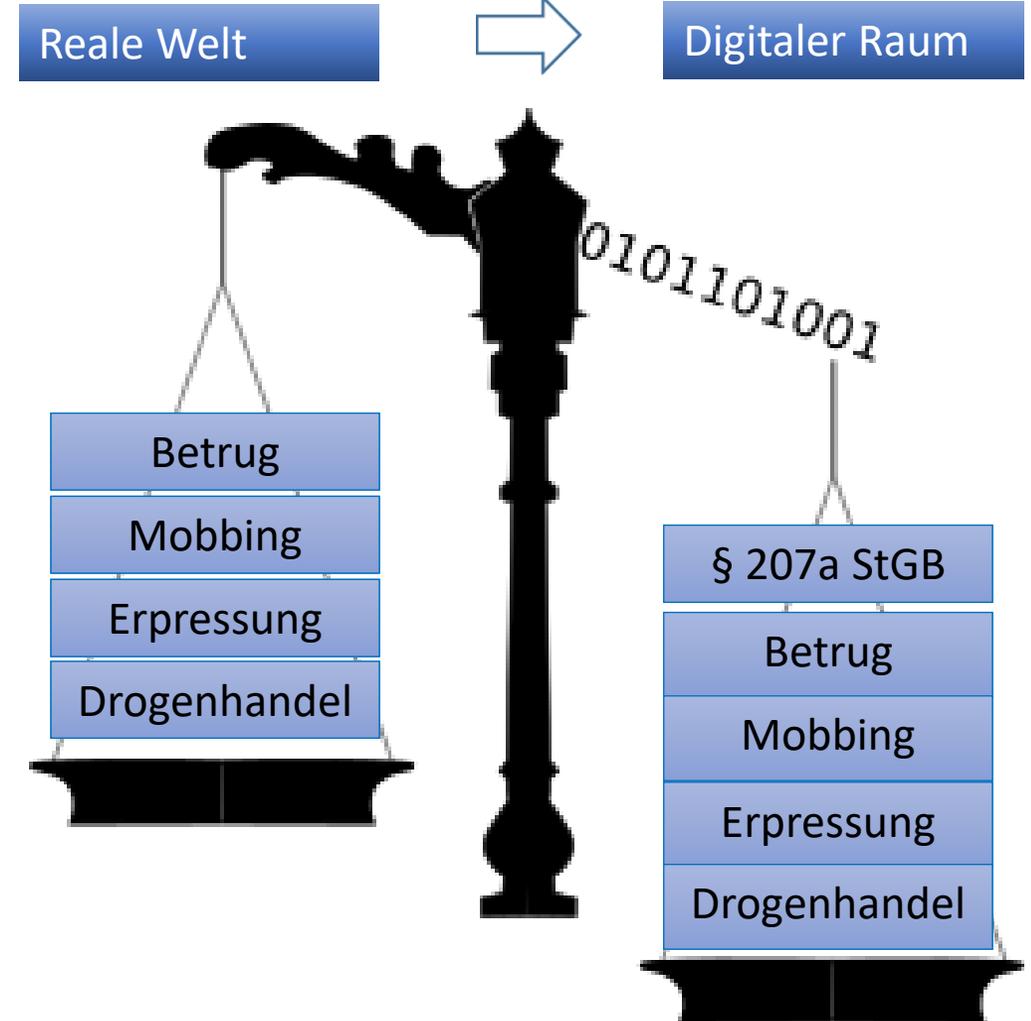
+28,6 %

Angriff auf IT

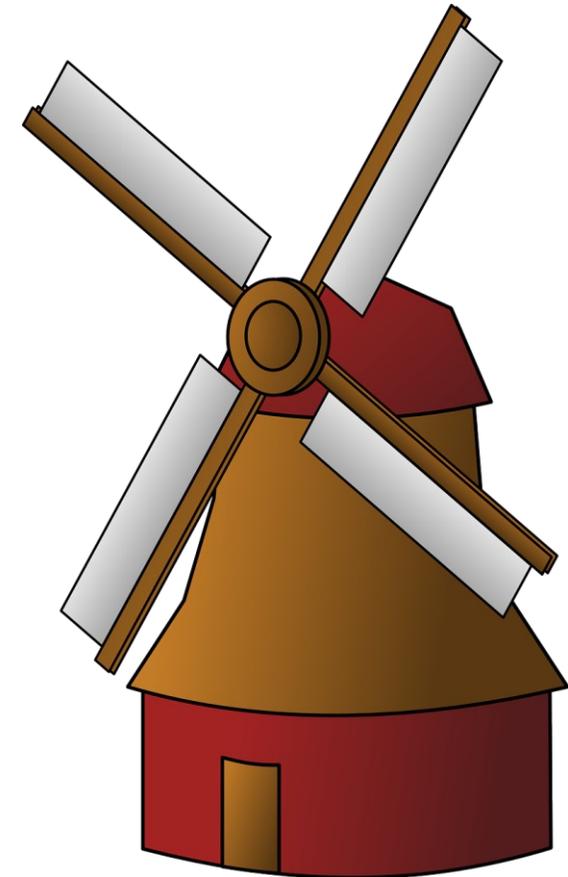


+19,9 %

Verlagerung der Kriminalität



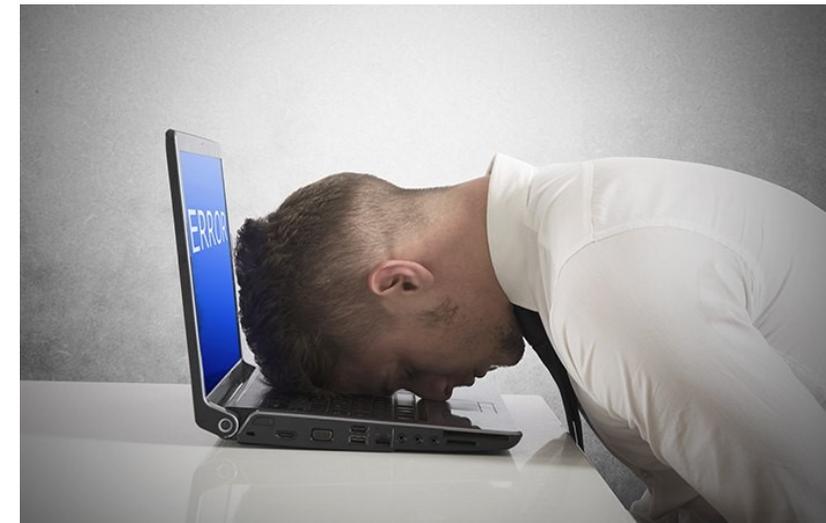
Bedrohungen und Angriffsvektoren



- Daten unzugänglich machen - Ransomware
- Information stehlen – Spyware
- Daten zerstören / Schaden zufügen – Virus
- Ressourcen nutzen
- Backdoor einrichten



- Passwort-Hacking
- Phishing
- Öffentliche Netzwerke
- Datenträger



Bewerbung via AMS

Julian Heyne

Gesendet: Dienstag, 30. August 2016 um 08:39

An:

  Julian Heyne.jpg (48,2 KB);  Bewerbung - Julian Heyne.zip (3,7 KB) [Vorschau für alle](#)

Sehr geehrte Damen und Herren,

anbei erhalten Sie meine Bewerbung für Ihre bei der AMS ausgeschriebene Stelle. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

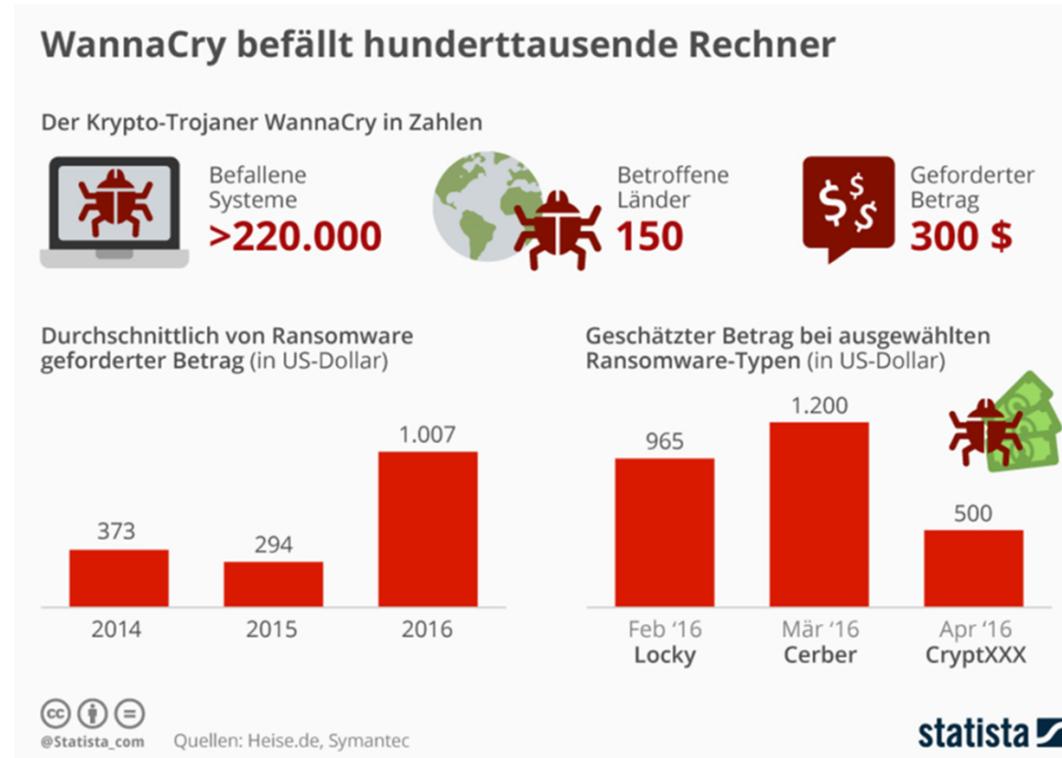
Ich freue mich, wenn ich mich Ihnen noch einmal persönlich vorstellen kann.

Mit freundlichen Grüßen,

Julian Heyne



- Lösegeldforderung durch Verschlüsseln des Datenbestandes
- Einbringung:
 - drive by download
 - Email
 - Sicherheitslücken
- Mehrere betroffene Großunternehmen
- Lösegeldforderungen im 6stelligen Bereich
- Weitere Erpressung mit Datenverkauf



Angestellte überwies fast 150.000 Euro an Betrüger

Die unbekanntes Täter konnten die Frau mit gefälschten Email-Aufträgen ihres Chefs dazu bringen, ihnen fast 150.000 Euro an ausländische Konten zu überweisen.

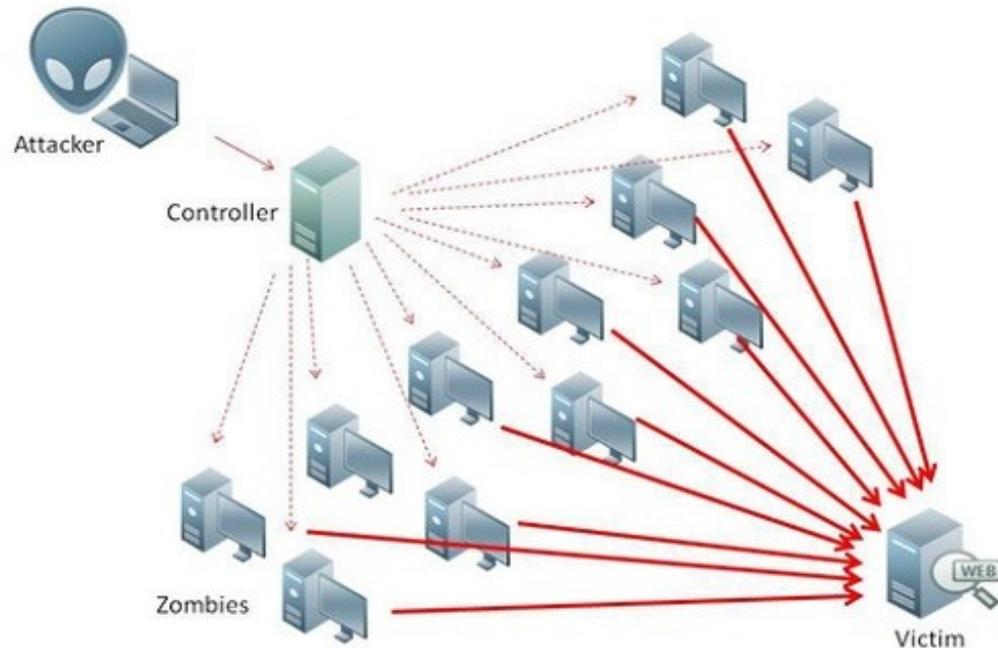


Die unbekanntes Täter gaben vor der Chef des Unternehmens zu sein. Symbolfoto (Bild: iStock)

In Deutschland
40 Prozent von 500 Unternehmen

Beispiele:

Oberöster. Unternehmen	50 Mio. Euro
Schmuckhändler Graz:	146.000 Euro
Vorarlberg Techn.Untern.:	150.000 Euro



MIRAI-IOT-BOTNET

IP-Kamera nach 98 Sekunden mit Malware infiziert

Droht die Netzwerkapokalypse, sobald ein unsicheres IoT-Gerät im Heimnetzwerk angeschlossen wurde? Der Sicherheitsforscher Rob Graham hat es ausprobiert - und sich innerhalb von 98 Sekunden die erste Infektion abgeholt.

Der Sicherheitsforscher Rob Graham wollte selbst ausprobieren, wie es um die Sicherheit eines IoT-Gerätes bestellt ist. Dazu kaufte er sich eine IP-Kamera für rund 55 US-Dollar, schloss sie an sein Heimnetzwerk an [und twitterte über das Ergebnis](#) . Bis zu ersten Infektion dauerte es seine Angaben zufolge nur 98 Sekunden.



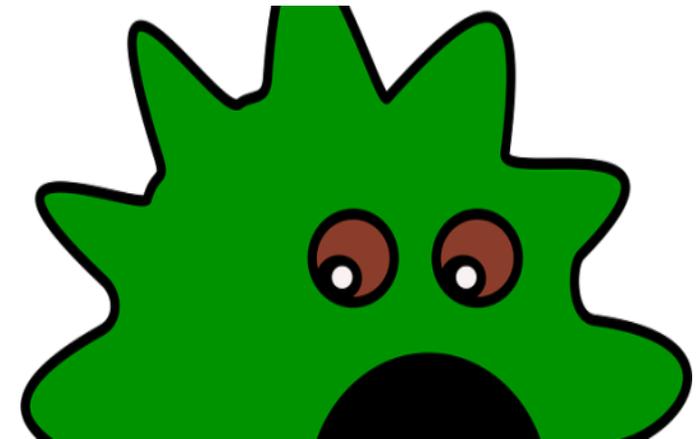
Quelle: <https://www.golem.de>

- Zahlungsmittel im kriminellen Umfeld
 - Schwer zu Verfolgen (Mixer-Technologien)
- Angriff auf IT um virtuelle Zahlungsmittel zu vermehren



Angriffsvektoren

- Angriffsvektor - Mensch
- Sicherheitslücken
 - Quasi in jeden Betriebssystem/Applikation
 - Schadcode wird immer intelligenter / passt sich an
 - Anzahl der Geräte nimmt enorm zu



Präventive und reaktive Maßnahmen

- Ausbau der Bezirks-IT-Ermittler
- Ausbau der Spezialisten für digitale Forensik und Ermittlung in den LKA und BK
- Neue Abteilung für Cybercrime im BK
- Aufbau eines universitären/hochschulischen Ausbildungscampus

Zusammenarbeit

Verstärkung der nationalen und internationalen Zusammenarbeit



INTERPOL



Kooperationen



Regelmäßiges Backup/Updates

Antivirensoftware und Firewall aktuell halten

Sensibilisierung der Mitarbeiter

Awarenessbildung

Schulungen

Notfallpläne

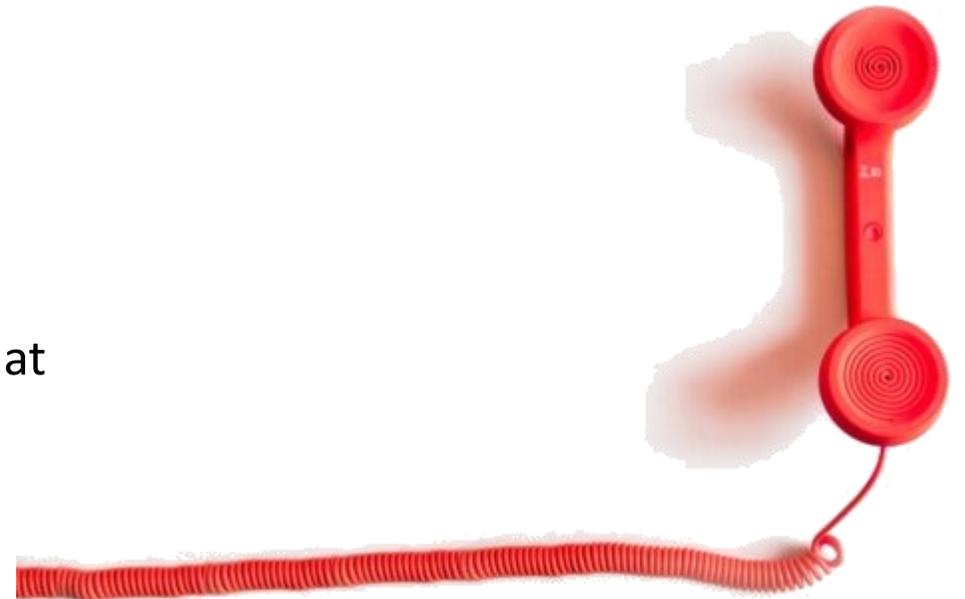


Was tun wenn ..

- Professionelle Hilfe in Anspruch nehmen
- Angriffsvektor identifizieren
- Mögliche Beweise sichern
- Anzeige erstatten
- Ggf. Meldung Datenschutz



- Wirtschaftskammer Österreich
 - Cyber-Security-Hotline: 0800 888 133
 - Bietet einfache Erstmaßnahmen
 - Koordiniert zu spezialisierten Unternehmen
- Bundesministerium f. Inneres:
 - Meldestellen im Bundeskriminalamt: ccu@bmi.gv.at



NO MORE RANSOM!

Besuchen Sie die Webseite
<http://www.NoMoreRansom.org>
um weitere Informationen über Ransomware
und bereits verfügbare Entschlüsselungstools
zu erhalten!

Herzlichen Dank für die Aufmerksamkeit

Fragen?

FRIESSNIK Erhard

Bundesministerium f. Inneres
Bundeskriminalamt - C4

Erhard.Friessnik@bmi.gv.at



Cybercrime Ermittlungen

