secuvera

BSI-zertifizierter IT-Sicherheitsdienstleister und Prüfstelle

Wie Hacker arbeiten

KITZBÜHEL
COUNTRY CLUB

TeleTrusT
Pioneers in IT security.

Liebe KCC-Mitglieder,

Danke für Ihr Interesse an diesen Folien. Der Vortrag lebte vor Allem vom Erzählen. Die Folien sind daher bedingt selbstverklärend (und manchmal gar nicht). Wenn Sie Fragen haben, kontaktieren Sie mich gerne direkt:

tglemser@secuvera.de

+49 7032 9758-15

Ihr Tobias Glemser

secuvera

- Sitz der Gesellschaft: Stuttgart/Gäufelden
- Gründung: 1. Juli 1982
- Inhabergeführt
- Herstellerunabhängig
- Berater, keine „Consultants“
- IT-Sicherheit seit 1988
- reiner IT-Sicherheitsdienstleister

- Drei Beratungsfelder
  - Sicherheitsberatung (BSI-Grundschutz/ISO 27001)
  - Penetrationstests
  - BSI-Prüfstelle (Produktzertifizierungen) 62443 für Industrial Security (TÜV Nord)

- whoami
  - Tobias Glemser
  - 20 Jahre in der Branche
  - BSI-zertifizierter Penetrationstester
  - Autor
    - iX, c‘t, …
    - Whitepaper „Projektierung der Sicherheitsüberprüfung von Webanwendungen“
    - OWASP Top10 Übersetzung
  - Engagements: TeleTrusT Experte, OWASP German Chapter Lead, Botschafter casayoana

secuvera

Ausgangslage

Hunderte Coop-Supermärkte in Schweden

Pandemien und Hacker machen bayerischer Wirtschaft am meisten Angst

Welche Risiken machen bayerischen Firmen am meisten Sorgen? Pandemien sind nun auf dem ersten Platz. Doch damit geht nicht automatisch Vorsorge einher.

Die Folgen eines nicht näher besch

VERSICHERUNG

Asiatische Axa-Partner von Ra getroffen

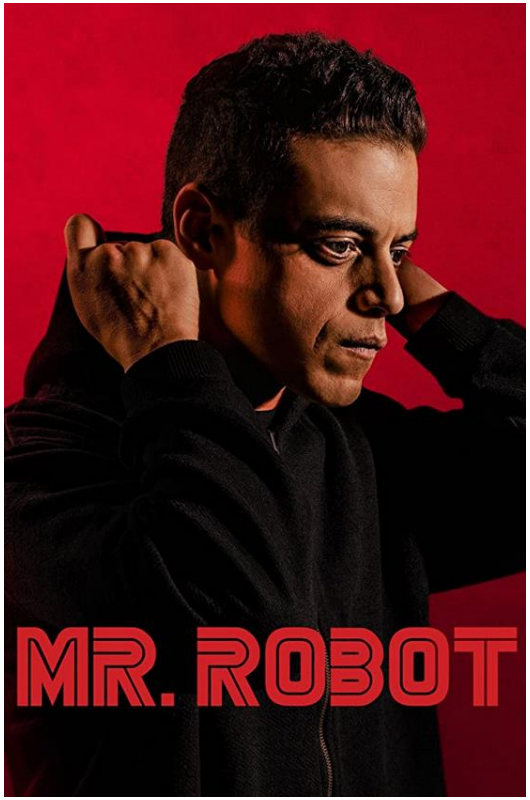
Teile des Versicherungskonzerns Axa in Asien wu
Angriff getroffen, es soll um 3 Terabyte Daten geh

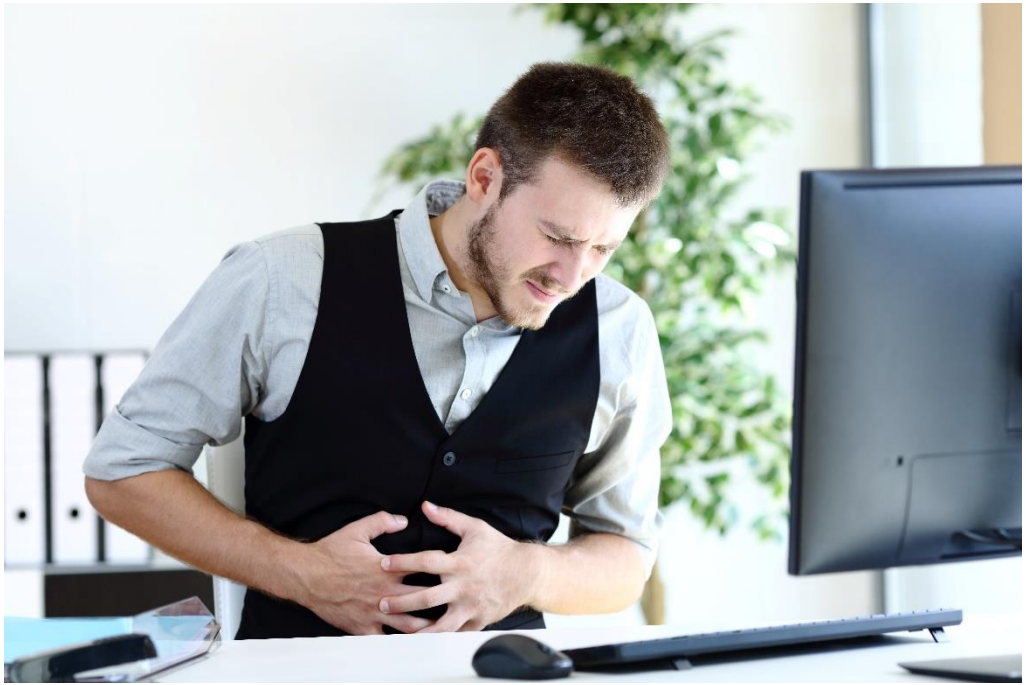
kenfm.de: Anonymous hackt Website des Aktivisten Ken Jebsen

Das Hackerkollektiv hat Zugriff auf kenfm.de erlangt und von dort nach eigenen Angaben 3 GByte Daten kopiert.

:attack
erangriff
ingestellt
ngriffs geworden. In
Ausmaß ist noch nicht

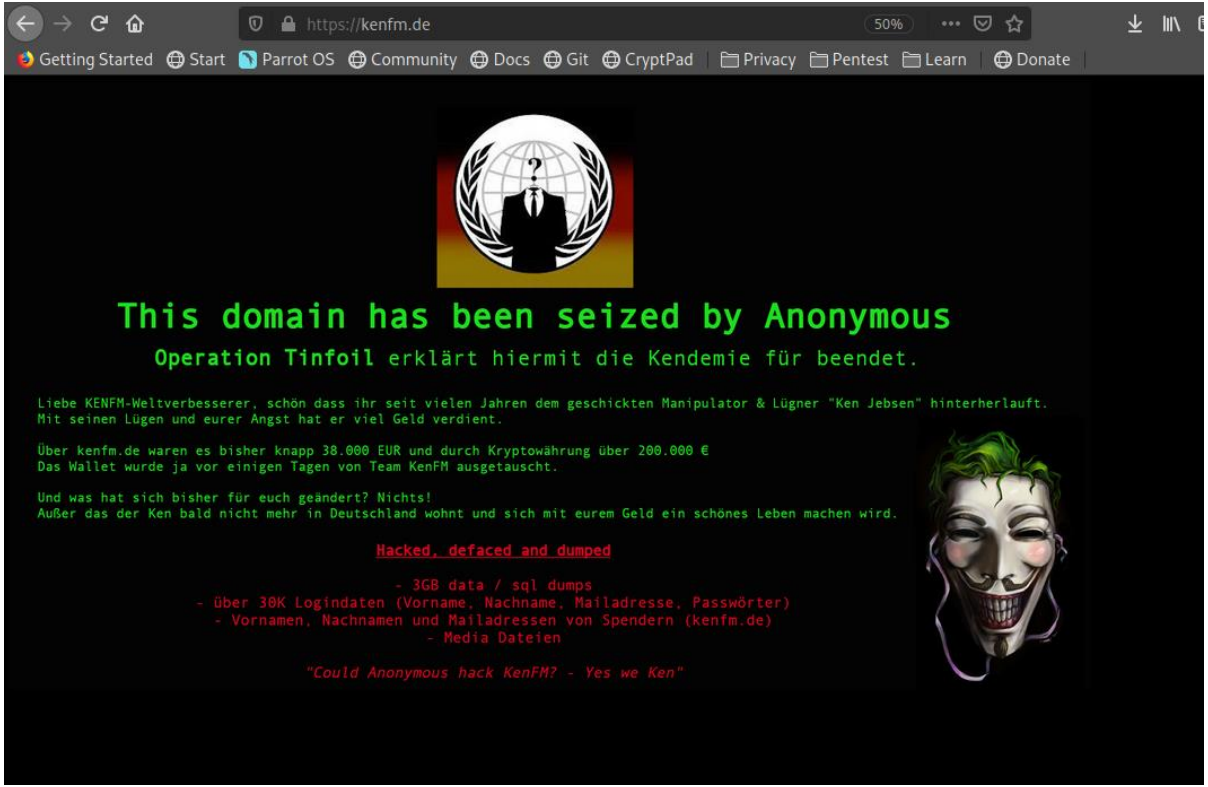
© olly - Fotolia.com


MR. ROBOT



© Antonioguillem - Adobe Stock

Angriff der Hacker



anonleaks.net

Kapitel I
Angriff der Profis

Your account is suspended

Your Google Ads account is temporarily suspended for Circumventing systems .

We want to help you regain control of your account as quickly as possible. p>

Here are some steps you can take to make your account secure:

1. Check your computer for malware and viruses with trusted anti-virus software, and remove any suspicious programs or applications.
2. log-in here to restore your account.

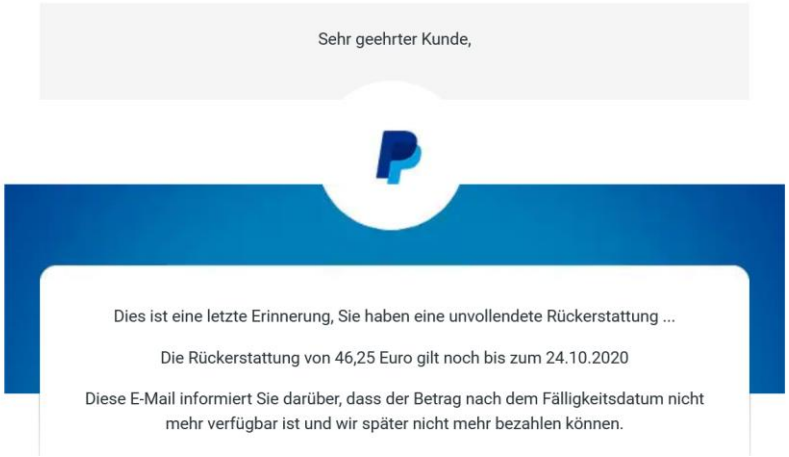
Learn more about suspended accounts.

The Google Ads Team

This email was sent to update you about your Google Ads account.

Google

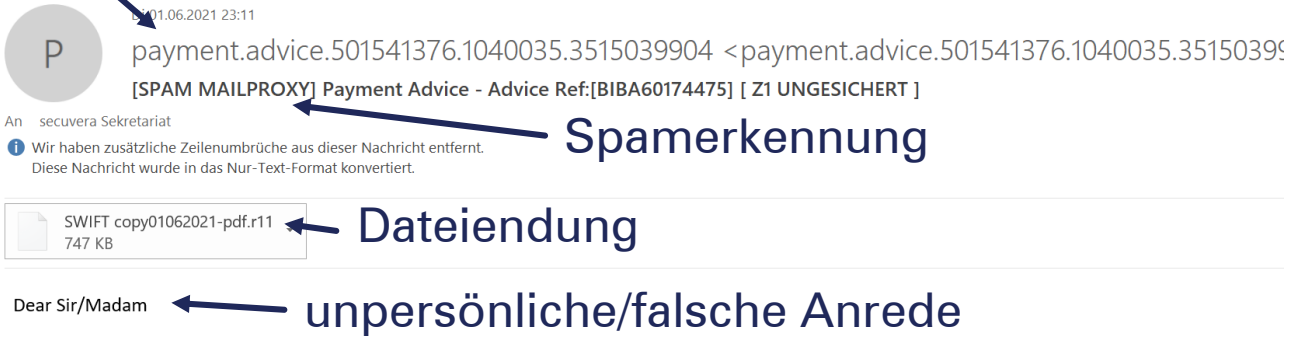
Google LLC
1600 Amphi theatre Parkway,
Mountain View, CA 94043



- Ziel: Einzelpersonen
- Methode: Phishing mit Link
- Zieldaten: Nutzernamen, Kennwörter

Kapitel II
Angriff der Profis

Absender



Spamerkennung

Dateiendung

unpersönliche/falsche Anrede

Absender zwar „OK“, aber irrelevant

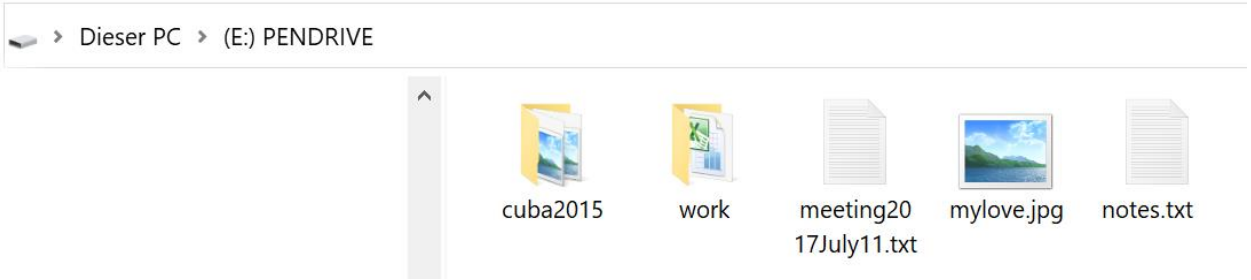
- Ziel: Firmen
- Methode: Phishing mit Anhang
- Zieldaten: Offen

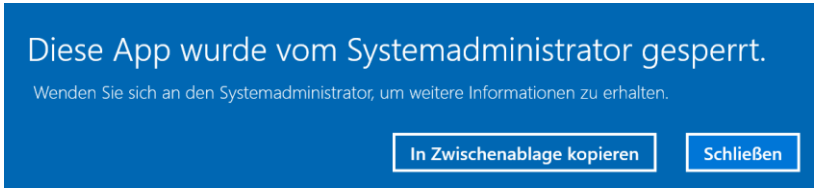
1. Infizieren
2. Auskundschaften
3. Kopieren und/oder verschlüsseln und/oder Daten verkaufen
4. Erpressen

Kapitel III
Angriff der Profis vor Ort

- Ziel: Firmen
- Methode: USB-Stick
- Zieldaten: Offen

1. Infizieren
2. Auskundschaften
3. Kopieren und/oder verschlüsseln und/oder Daten verkaufen
4. Erpressen


Dieser PC
(E:) PENDRIVE
cuba2015
work
meeting2017July11.txt
mylove.jpg
notes.txt


Diese App wurde vom Systemadministrator gesperrt.
Wenden Sie sich an den Systemadministrator, um weitere Informationen zu erhalten.
In Zwischenablage kopieren
Schließen

Abwehr


Arktischer Ozean
Atlantischer Ozean
Pazifischer Ozean
Indischer Ozean
Antarktischer Ozean
Risiko
Risiko
Risiko
Risiko
Risiko
Risiko

© HASBRO

- Organisation
  - Ist die Geschäftsleitung aufgeklärt?
  - Gibt es eine Cyberversicherung mit ausreichender Deckung?

- Technik
  - Können Nutzer Programme selbst starten?
  - Werden E-Mails mit eigener Domäne im Absender von außen blockiert/markiert?
  - Werden Nutzer regelmäßig sensibilisiert?
  - Lange Kennwörter und zwei-Faktor-Anmeldung?

- Strategisch
  - Stand der Dinge erheben lassen (z. B. TeleTrusT „Stand der Technik“ oder „Cyber-Sicherheits-Check“)
  - Maßnahmen technisch prüfen (z. B. Penetrationstest)
  - Managementsystem einführen (z. B. ISO 27001)

secuvera

Vielen Dank

KITZBÜHEL
COUNTRY CLUB

TeleTrusT
Pioneers in IT security.