secuvera

Cybersicherheit. Nachhaltig.

Ransomware effektiv verhindern

29. März 2023

itsa 365

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

- Drei Beratungsfelder
  - Sicherheitsberatung
    - BSI-Grundschutz/ISO 27001
    - Ciso as a Service (CaaS)
  - Penetrationstests
  - BSI-Prüfstelle (Produktzertifizierungen) Industrial Security (63442)

- whoami
  - Tobias Glemser
  - +20 Jahre in der Branche
  - BSI-zertifizierter Penetrationstester
  - Autor
    - iX, c‘t, …
    - OWASP Top10 Übersetzung
  - Referent
    - secIT, devSec(), DWX, JCon, Java Days
  - Engagements: TeleTrusT Experte, OWASP German Chapter Lead, Botschafter casayohana

ziener

Ausgangslage

secuvera

Salatknappheit: Produktionsausfall in den

Der nächste Hackerangriff

Bei Häfele in Baden-Württemberg war einige Wochen niemand mehr erreichbar, die meisten Mitarbeiter wurden nach Hause geschickt. Wie sich zeigte, war ein Cyberangriff schuld.

eingestellt.

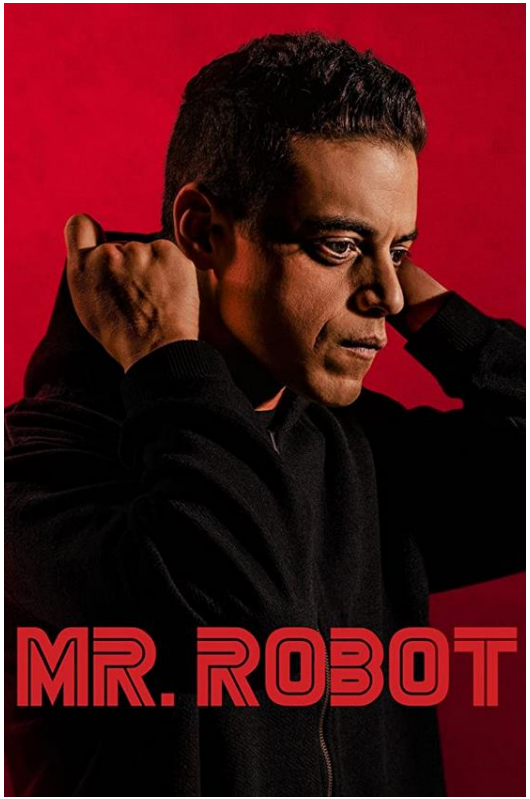
Attacken müssen jetzt zahlen

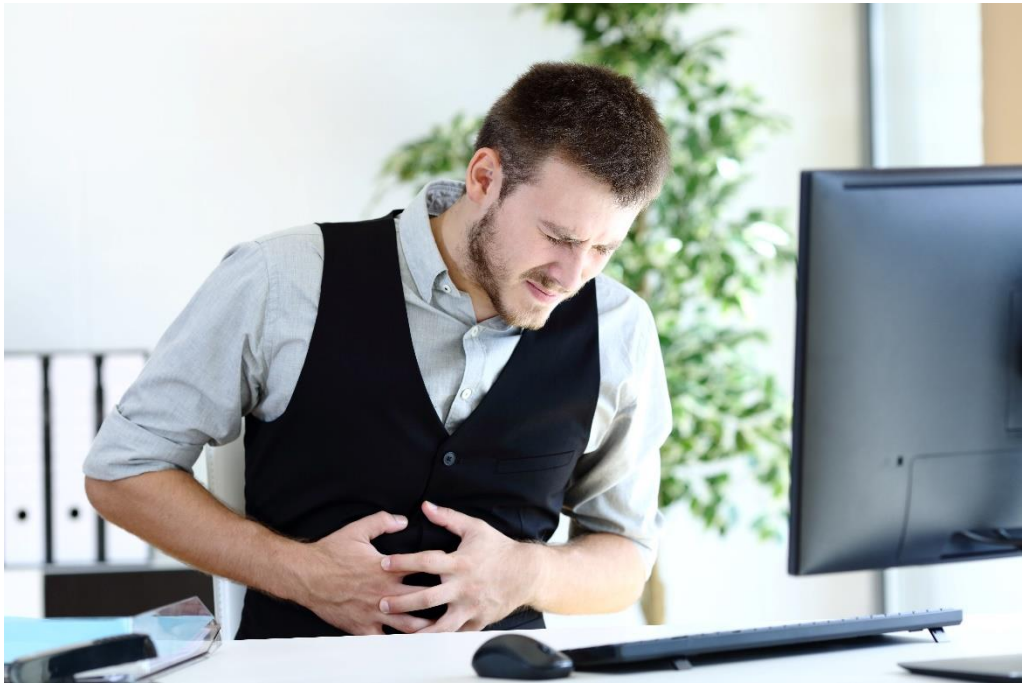
Cyberversicherer machen erstmals Verluste – Markt legt weiter zu

Hackerangriffe sind eine wachsende Gefahr für die Wirtschaft, zeigen neue Zahlen der Cyberversicherer. 2021 mussten sie deutlich mehr Schäden regulieren, die Aufwendungen überstiegen gar erstmals die Einnahmen. Der Markt wächst indes weiter.

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

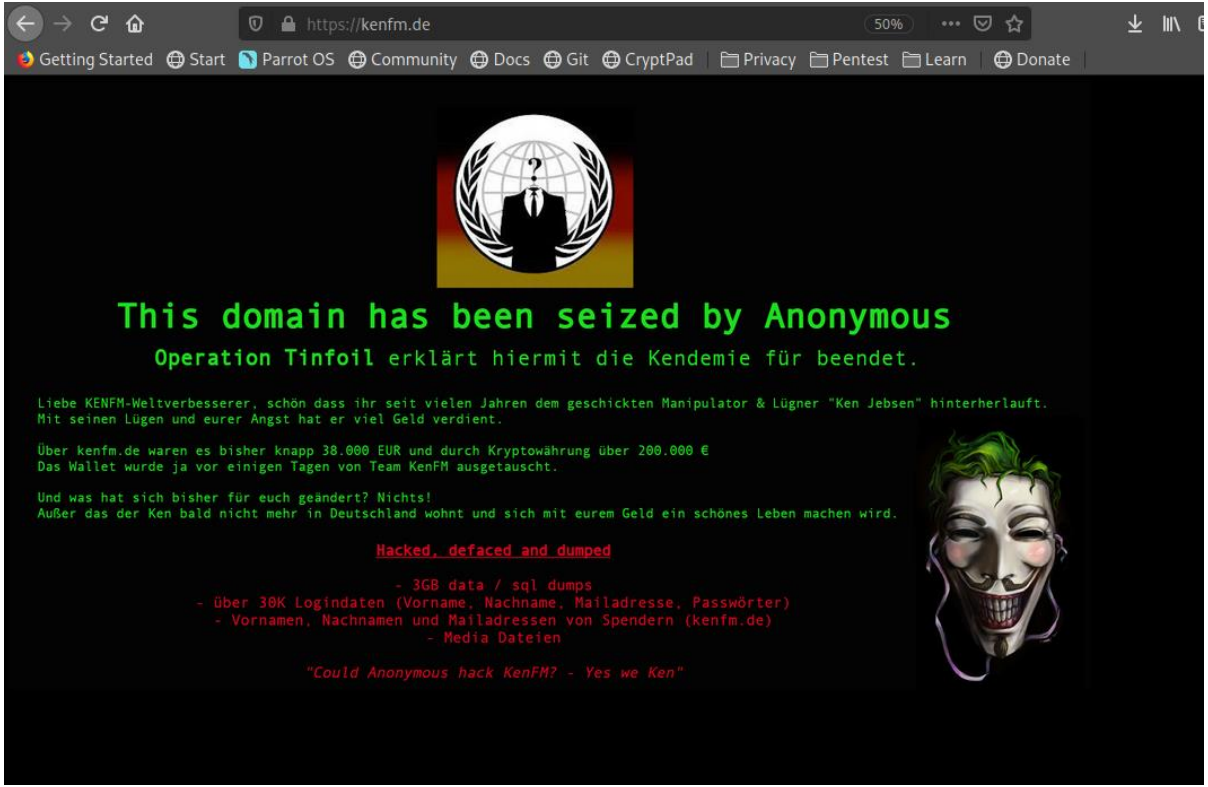
© olly - Fotolia.com


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.

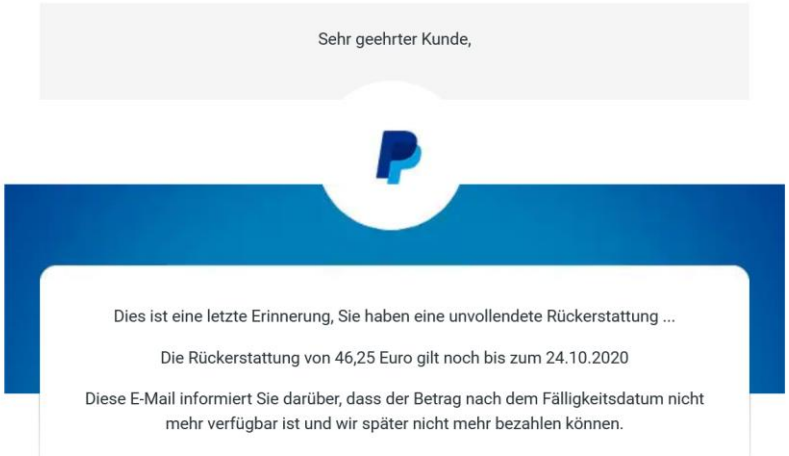
Learn more about suspended accounts.

The Google Ads Team

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

Google

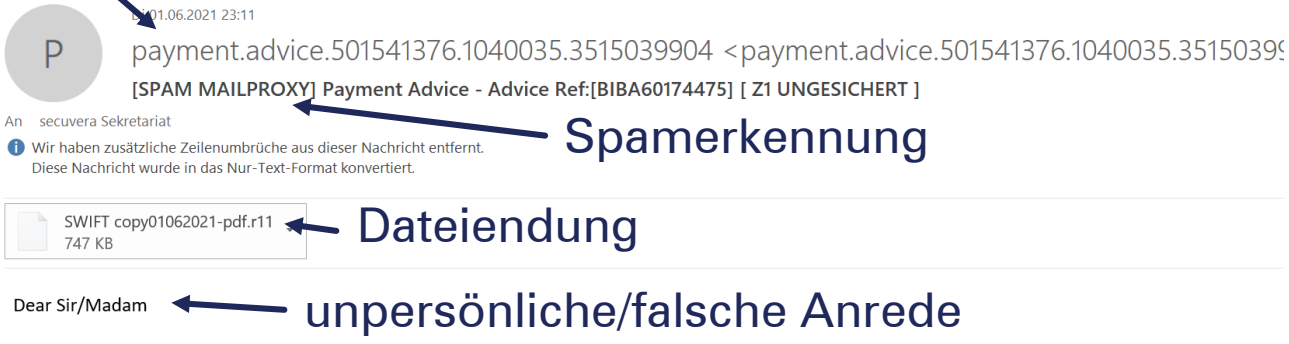
Google LLC
1600 Amphi theatre Parkway,
Mountain View, CA 94043



- Ziel: Einzelpersonen
- Methode: Phishing mit Link
- Zieldaten: Nutzernamen, Kennwörter
- Ziel: Wiederverwendung für VPN/Webmail/…

Kapitel II
Angriff der Profis

Absender

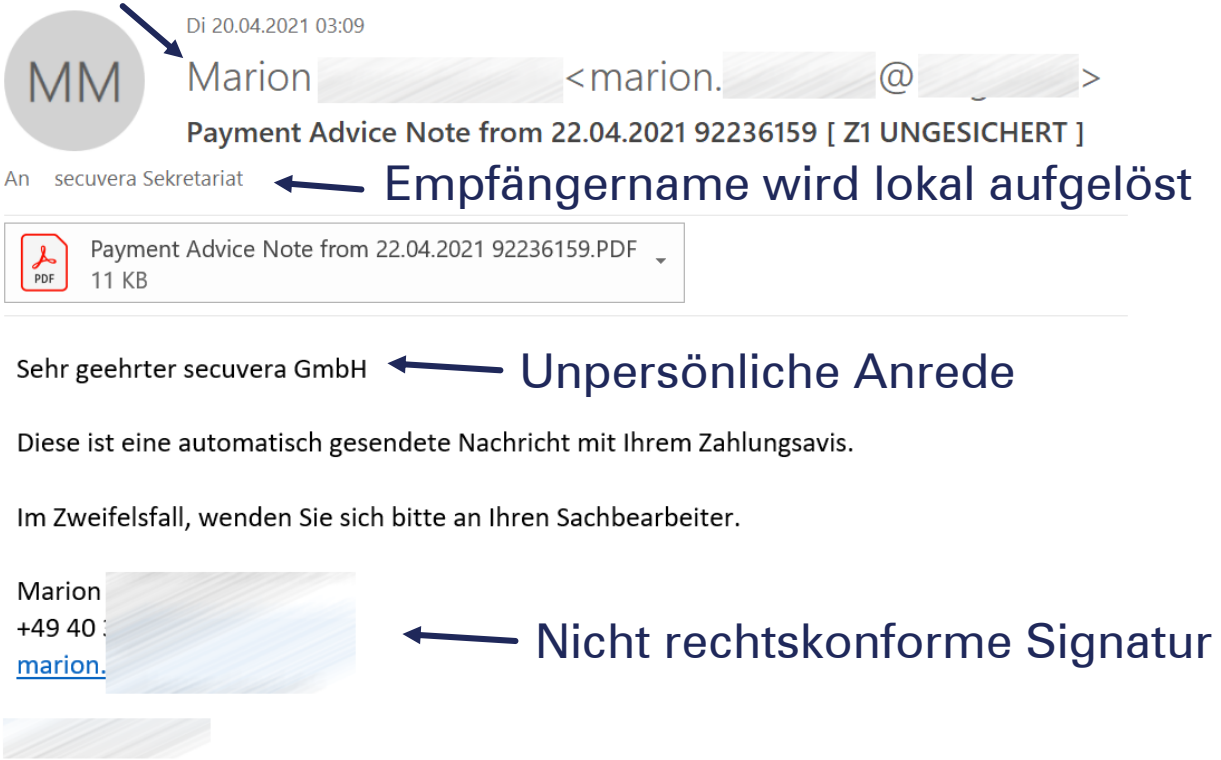


Spamerkennung

Dateiendung

unpersönliche/falsche Anrede

Absender zwar „OK“, aber irrelevant



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

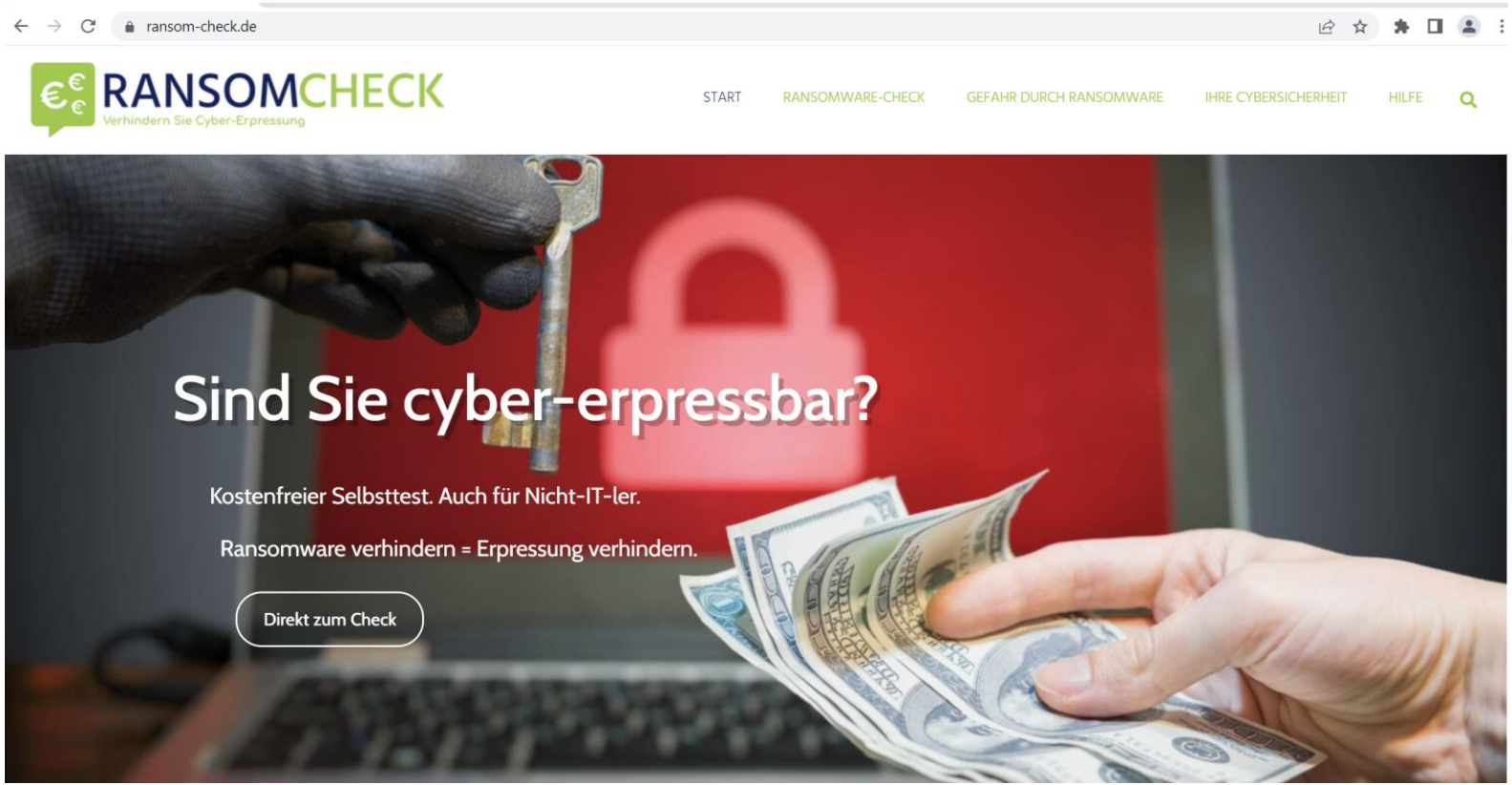
1. Infizieren
2. Auskundschaften
3. Kopieren und/oder verschlüsseln und/oder Daten verkaufen
4. Erpressen

Kapitel III
Angriff der Profis vor Ort

© secuvera GmbH

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

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


ransom-check.de
RANSOMCHECK
Verhindern Sie Cyber-Erpressung
START
RANSOMWARE-CHECK
GEFAHR DURCH RANSOMWARE
IHRE CYBERSICHERHEIT
HILFE
Sind Sie cyber-erpressbar?
Kostenfreier Selbsttest. Auch für Nicht-IT-ler.
Ransomware verhindern = Erpressung verhindern.
Direkt zum Check

Abwehr

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

© HASBRO

- Universelle Maßnahmen für Alle
  - Lange Kennwörter (+16 Zeichen)
  - Individuelle Kennwörter je System/Anwendung
  - Passwortspeicher wie KeePass
  - Zweiten Faktor aktivieren (!)
  - Biometrie ist sicherer als ihr Ruf
  - Updates
  - Backups
  - Einheitlichkeit der Umgebung
  - Microsoft ruft nicht an

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

- Technik
  - Können Nutzer Programme selbst starten (ransom-check.de)?
  - Werden E-Mails mit eigener Domäne im Absender von außen blockiert/markiert?
  - Werden Nutzer regelmäßig, positiv und einfach sensibilisiert?
  - Unsignierte Markos möglich (ransom-check.de)?

- Strategisch
  - Stand der Dinge erheben lassen (z. B. „Cyber-Sicherheits-Check“, siehe ACS)
  - Maßnahmen technisch prüfen (z. B. Penetrationstest)
  - Managementsystem einführen (z. B. ISO 27001)
  - Hilfe holen (z. B. Ciso as a Service)

ziener

secuvera

Cybersicherheit. Nachhaltig.

Vielen Dank

itsa 365