IT-Sicherheit für Ihr Unternehmen ohne großen Aufwand!

Markus Koscielny – G DATA

15.05.2019

Markus Koscielny

G DATA Sales Engineer

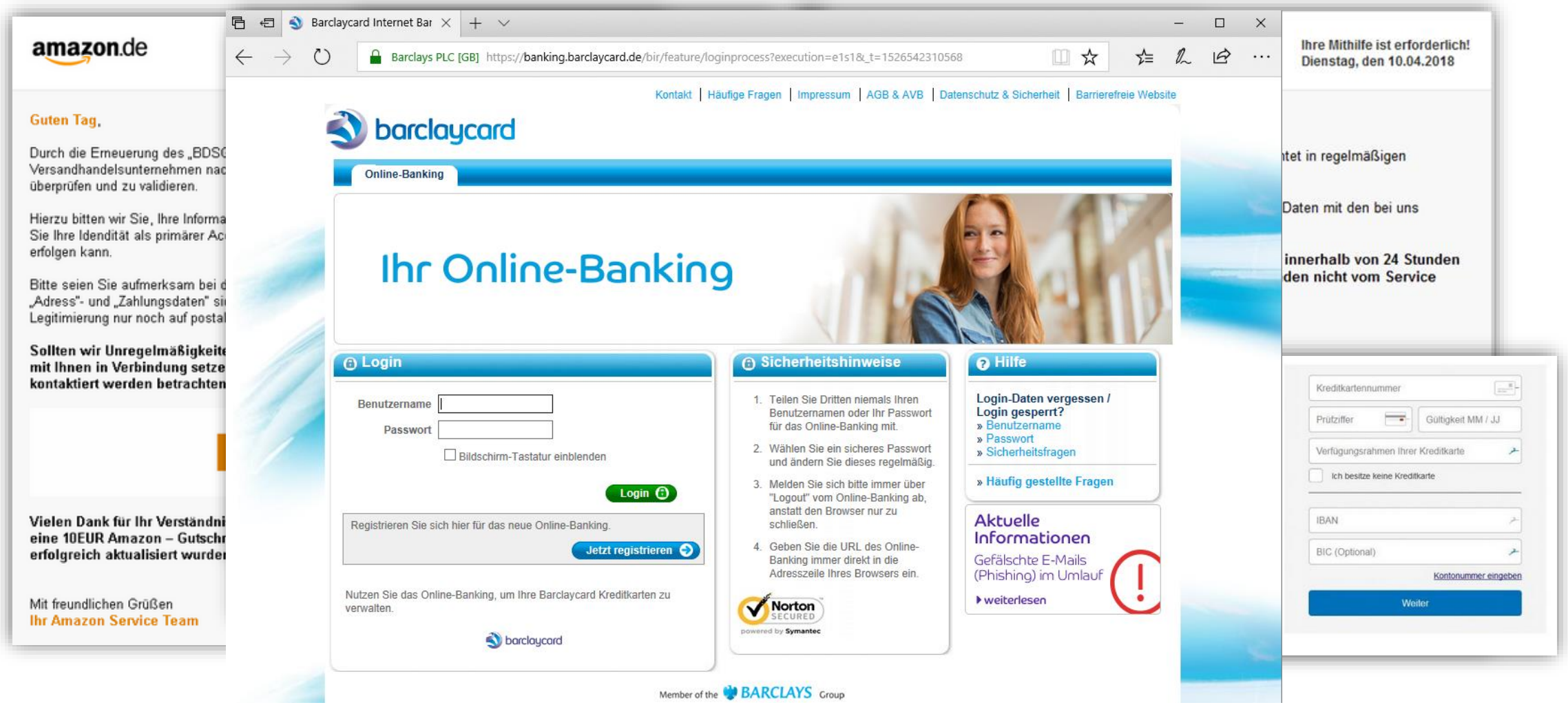
- „Markus Koscielny ist Sales Engineer bei der G DATA Software AG und unterstützt seit über zehn Jahren erfolgreich das Bochumer Security-Team. In seiner langjährigen Funktion als Quality Assurance Engineer betreute er die Entwicklung und Einführung neuer Funktionen und war so maßgeblich am Erfolg der Security-Lösungen beteiligt.
- Seit 2018 vertritt er die G DATA Software AG zudem als Berater auf Kongressen und Konferenzen zum Thema IT-Sicherheit und betreut mittelständische und große Unternehmen bei allen Fragen rund um G DATA Sicherheitslösungen.

Agenda

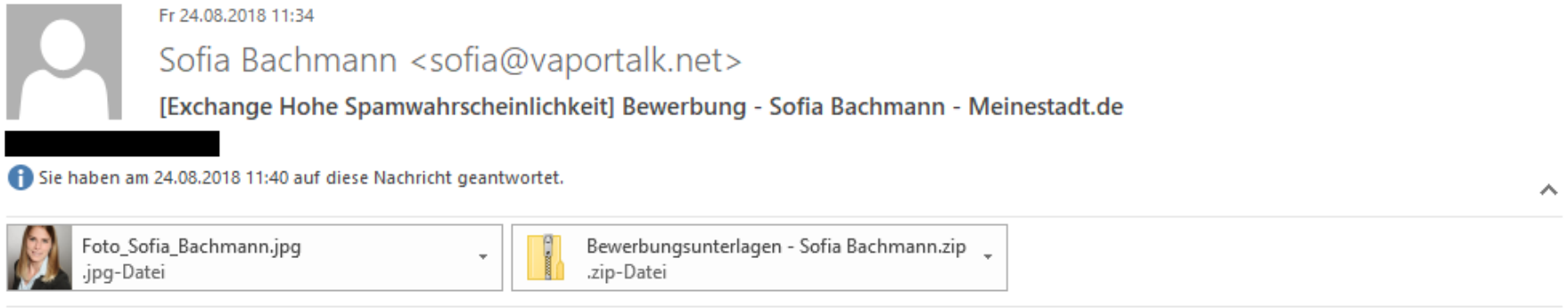
1. Aktuelle Angriffsszenarien
2. Was ist eigentlich Ransomware wie ‚Emotet‘?
3. Tipps und Tricks für den IT-Admin
4. Ganzheitliches Sicherheitskonzept Layered Security
5. Allgemeine Fragerunde

1. Aktuelle Angriffsszenarien

Bitte aktualisieren Sie Ihre Daten…



Eine ganz normale Bewerbung (?)



Fr 24.08.2018 11:34

Sofia Bachmann <sofia@vaportalk.net>

[Exchange Hohe Spamwahrscheinlichkeit] Bewerbung - Sofia Bachmann - Meinestadt.de

[redacted]

Sie haben am 24.08.2018 11:40 auf diese Nachricht geantwortet.

Foto_Sofia_Bachmann.jpg
.jpg-Datei

Bewerbungsunterlagen - Sofia Bachmann.zip
.zip-Datei

G DATA MAILSECURITY: Diese Mail steht unter Spamverdacht. Sollte diese Mail einen Anhang haben bitte nicht ohne vorherige Prüfung öffnen!
Sehr geehrte Damen und Herren,

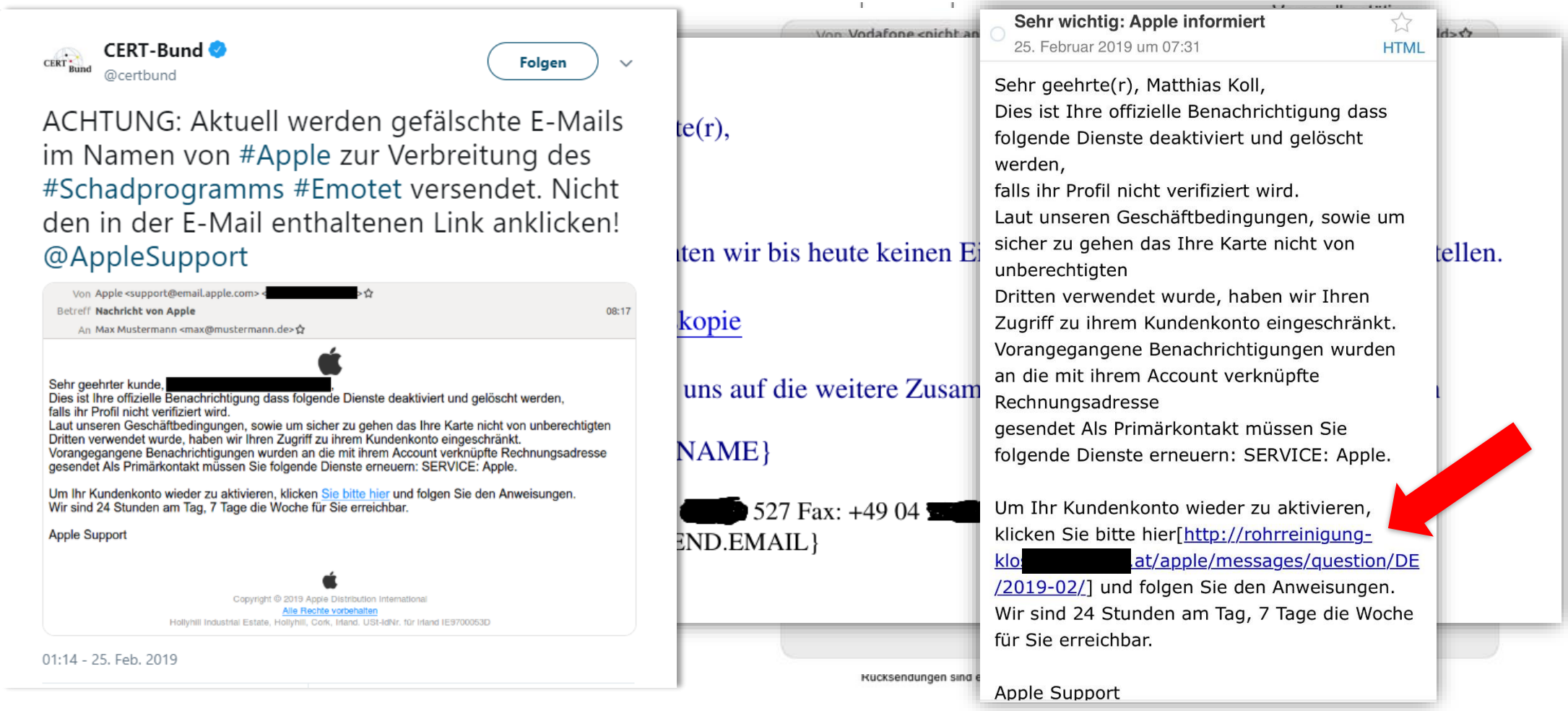
anbei erhalten Sie meine Bewerbung für Ihre ausgeschriebene Stelle bei meinestadt.de. Warum ich die Stelle optimal ausfüllen kann und Ihrem Unternehmen durch meine Erfahrung im Vertrieb und der Kundenbetreuung zahlreiche Vorteile biete, entnehmen Sie bitte meinen ausführlichen und angehängten Bewerbungsunterlagen.

Ich freue mich auf ein persönliches Vorstellungsgespräch.

Mit besten Grüßen

Sofia Bachmann

Geschäftsbeziehungen



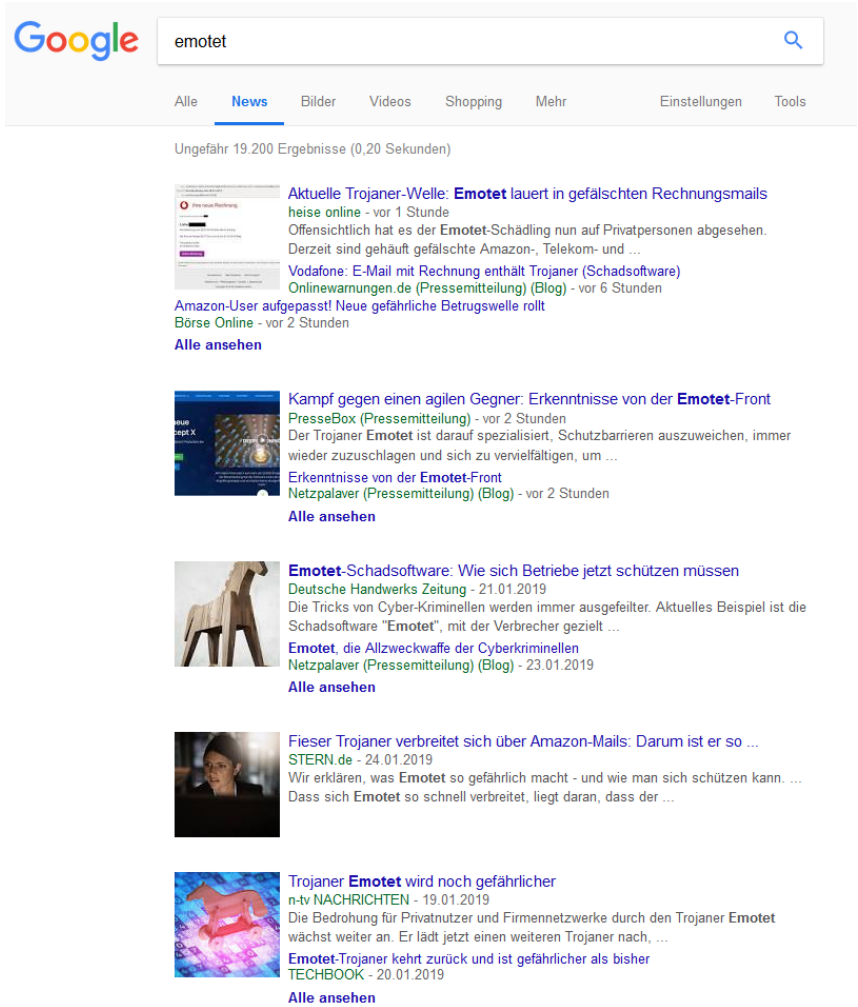
2. Was ist eigentlich Ransomware?

Eine Definition

- Ransom (engl.) = *Lösegeld*
- Erpresser-Trojaner
- Daten werden „gekapert“
- höchste geforderte Lösegeldsumme in 2018:

500.000€

Emotet – In aller Munde

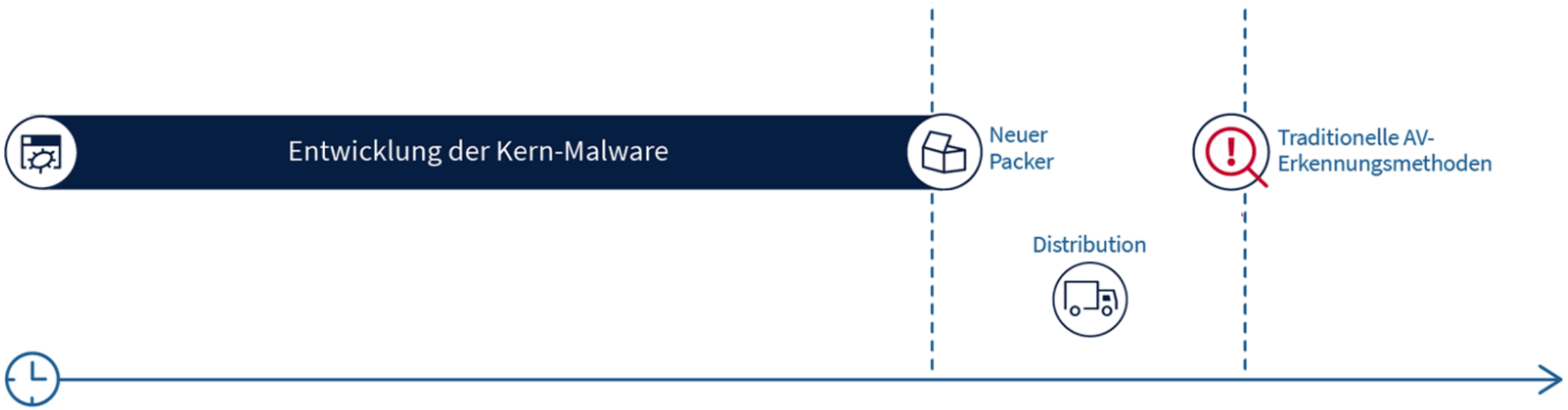


Nach Weihnachtspause zurück

Onlinebanking-Trojaner Emotet ist jetzt noch gefährlicher

Emotet – In aller Munde

Malware - Entwicklung



Das Multitool für Cyberkriminelle

Auswirkungen von Cybercrime

- Diebstahl von Daten / Datenträgern
- Abhören der Kommunikation
- Ausfall der IT / Produktion / Dienstleistung
- Rechtsstreitigkeiten / Reputationsschäden
- Social Engineering

Der wirtschaftliche Schaden

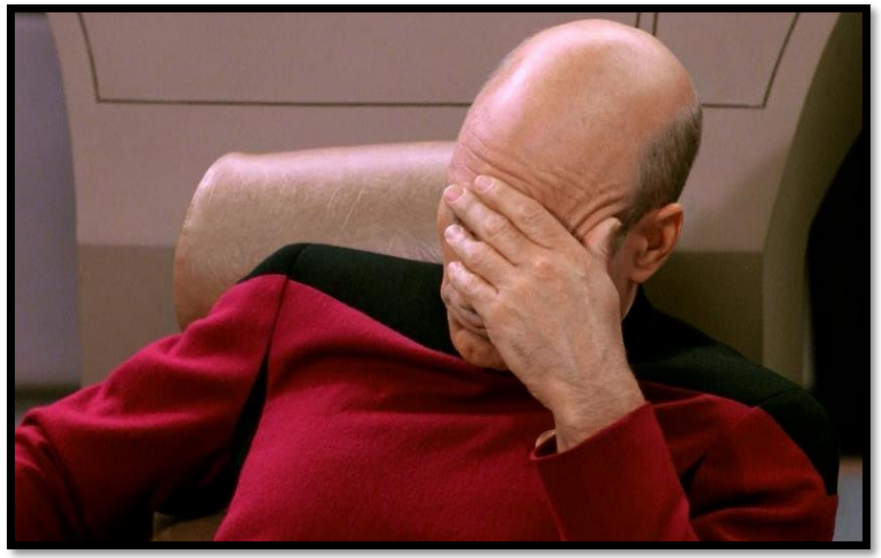
3. Tipps und Tricks für den IT-Admin

Sicherheitstipps

- Patchen Sie zeitnah
- Erstellen Sie regelmäßig Backups
- Benutzerkonten für E-Mail und Surfen
- Deaktivieren Sie die Ausführung von Makros
- Achten Sie auf Aktualität Ihrer Antiviren-Software

Passwörter

0 0 0 0



WTF 30.03.2019 17:10 Uhr

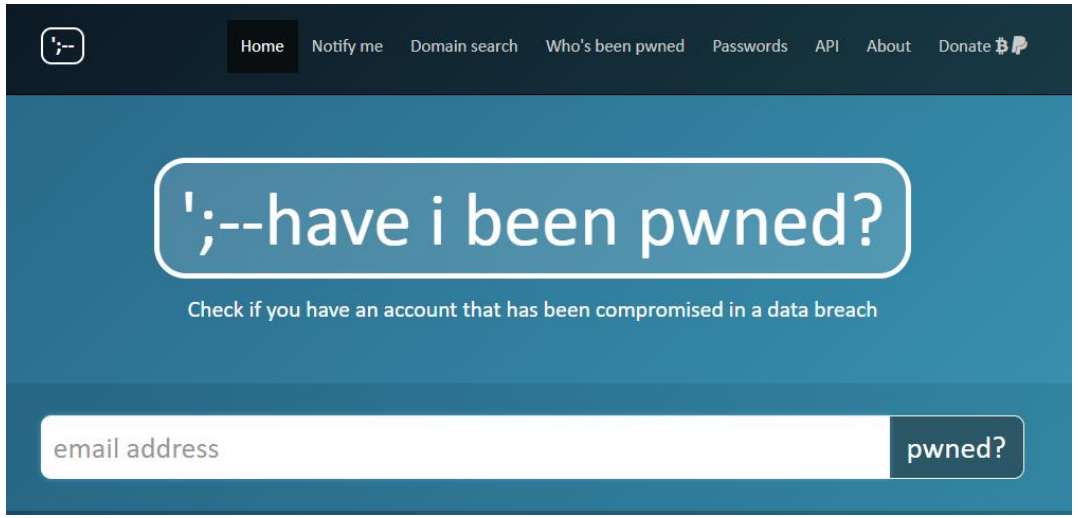
Viermal die Null: Kostenloser Sprit dank Default-Passwort an Zapfsäule

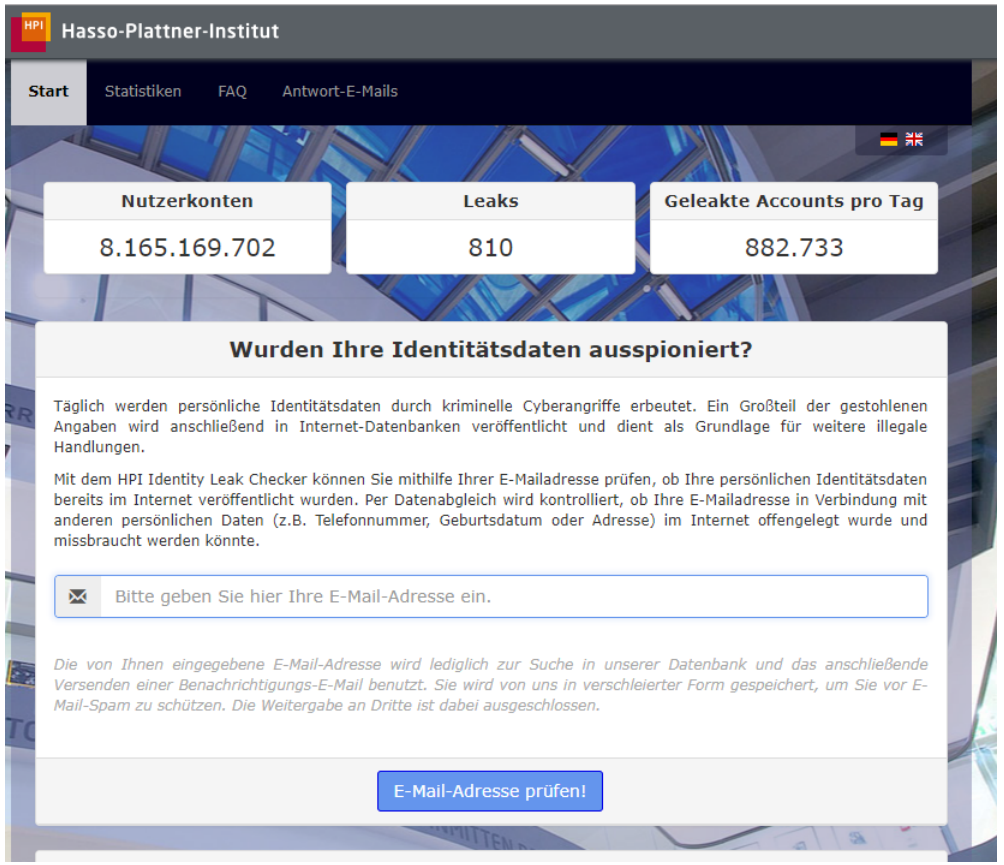
In Frankreich haben sich Kriminelle kostenlos an Tankstellen bedient. Sie manipulierten die Zapfsäulen – weil deren Default-Passwort nicht geändert worden war.

Von **Tilman Wittenhorst** 205

(Bild: pixabay.com)

Bin ich betroffen?





4. Ganzheitliches Sicherheitskonzept Layered Security

Technologische Maßnahmen - Gefühlt

Technologische Maßnahmen - Wunsch

Quelle: Victorinox, Swiss Champ XAVT

Technologische Maßnahmen - Realität

Quelle: Victorinox, Swiss Champ XAVT

Technologische Maßnahmen - Realität

- AntiVirus? *… nach 3 Jahren im Auslieferungszustand*
- Firewall? *… Default-Zustand, Logs ungelesen*
- Assetmanagement? *… Schatten IT, Free-/Shareware*
- Anwendungs- & Gerätekontrolle? *… stillgelegt*
- Backup-Strategie? *… nie getestet*
- SIEM, SOC, IDS/IPS *… Logfiles ungenutzt*

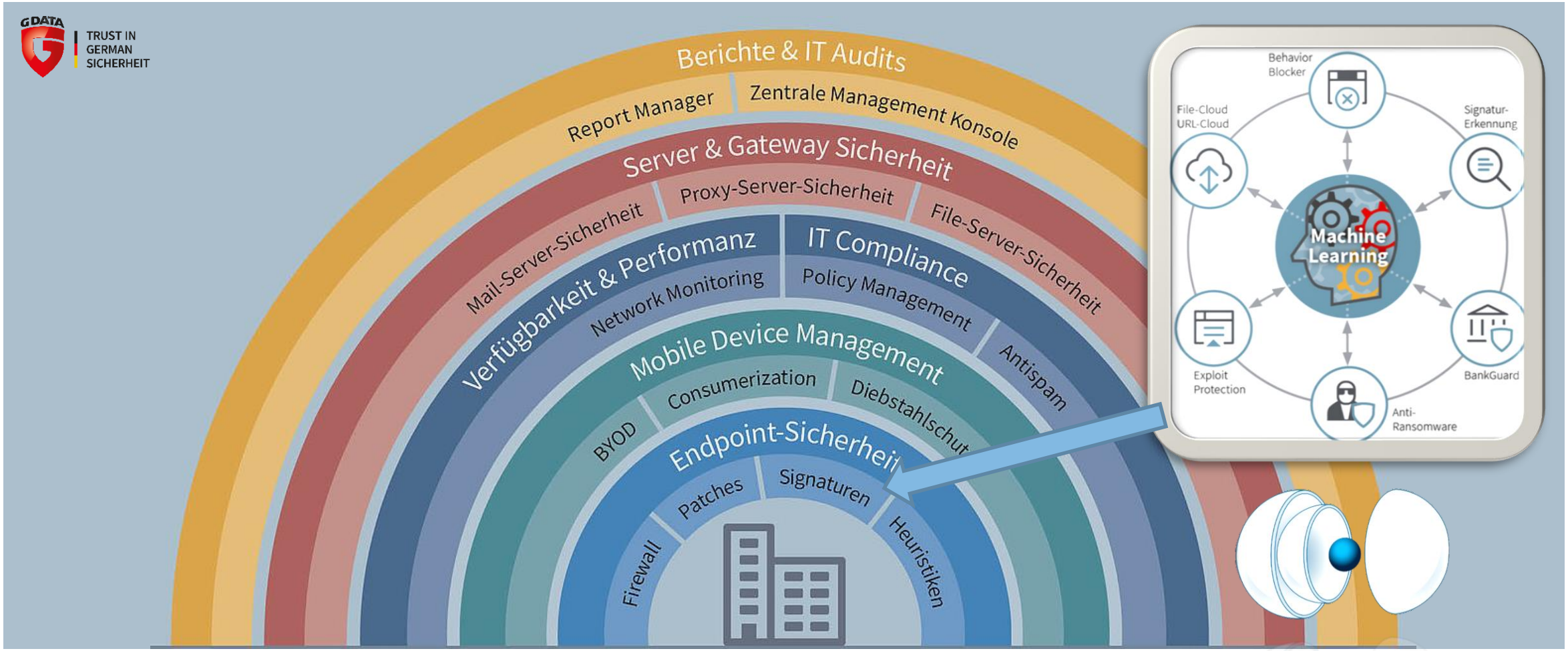
Quelle: Victorinox, Swiss Champ XAVT

Sicherheitskonzept

- Awareness / Zugriffsrechte
- Management von Anwendungen und externen Geräte (USB-Sticks…)
- Patch-/Update-Konzept & Mobile Device Management
- Backup- & Restore-Strategie
- Ganzheitliche Endpoint-Sicherheitslösung mit intelligenten Erkennungsmechanismen

Quelle: Victorinox, Swiss Champ XAVT

G DATA Layered Security



Wenn es bereits passiert ist…

Im Fall der Fälle…

… der **Notfall-Plan!**

Die „Richtung“ stimmt, wenn:

- ✓ … ein Sicherheitskonzept implementiert wurde!
- ✓ … IT-Sicherheit zur Chefsache wird!
- ✓ … IT-Sicherheit als Prozess verstanden wird!