

IT-Sicherheit für Ihr Unternehmen ohne großen Aufwand!

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...

The screenshot shows a web browser window displaying the Barclays online banking login page. The browser's address bar shows the URL: <https://banking.barclaycard.de/bir/feature/loginprocess?execution=e1s1&t=1526542310568>. The page features the Barclays logo and a navigation menu with links for 'Kontakt', 'Häufige Fragen', 'Impressum', 'AGB & AVB', 'Datenschutz & Sicherheit', and 'Barrierefreie Website'. The main heading is 'Ihr Online-Banking'. Below this, there are three sections: 'Login' with input fields for 'Benutzername' and 'Passwort', a 'Login' button, and a 'Jetzt registrieren' button; 'Sicherheitshinweise' with a list of four security tips and a Norton Secured logo; and 'Hilfe' with links for 'Login-Daten vergessen / Login gesperrt?' and 'Häufig gestellte Fragen'. A red warning box on the right side of the page reads: 'Ihre Mithilfe ist erforderlich! Dienstag, den 10.04.2018' and 'Ihre Daten werden innerhalb von 24 Stunden nicht vom Service entfernt'. Below this warning is a form with fields for 'Kreditkartennummer', 'Prütziffer', 'Gültigkeit MM / JJ', 'Verfügungsrahmen Ihrer Kreditkarte', 'IBAN', and 'BIC (Optional)', with a 'Weiter' button. The footer of the page includes 'Member of the BARCLAYS Group' and 'IT-Sicherheit für Ihr Unternehmen'.

Eine ganz normale Bewerbung (?)



Fr 24.08.2018 11:34

Sofia Bachmann <sofia@vaportalk.net>

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

 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

CERT-Bund @certbund

ACHTUNG: Aktuell werden gefälschte E-Mails im Namen von #Apple zur Verbreitung des #Schadprogramms #Emotet versendet. Nicht den in der E-Mail enthaltenen Link anklicken! @AppleSupport

Von Apple <support@email.apple.com> - [REDACTED] - ☆
Betreff: Nachricht von Apple 08:17
An: Max Mustermann <max@mustermann.de> - ☆

Sehr geehrter Kunde, [REDACTED]
Dies ist Ihre offizielle Benachrichtigung dass folgende Dienste deaktiviert und gelöscht werden, falls ihr Profil nicht verifiziert wird.
Laut unseren Geschäftsbedingungen, sowie um sicher zu gehen das Ihre Karte nicht von unberechtigten Dritten verwendet wurde, haben wir Ihren Zugriff zu ihrem Kundenkonto eingeschränkt.
Vorangegangene Benachrichtigungen wurden an die mit ihrem Account verknüpfte Rechnungsadresse gesendet Als Primärkontakt müssen Sie folgende Dienste erneuern: SERVICE: Apple.

Um Ihr Kundenkonto wieder zu aktivieren, klicken Sie bitte hier und folgen Sie den Anweisungen. Wir sind 24 Stunden am Tag, 7 Tage die Woche für Sie erreichbar.

Apple Support

Copyright © 2019 Apple Distribution International
Alle Rechte vorbehalten
Hollyhill Industrial Estate, Hollyhill, Cork, Irland. USt-IdNr. für Irland IE9700053D

01:14 - 25. Feb. 2019

Von Vodafone spricht an

Sehr wichtig: Apple informiert ☆ HTML
25. Februar 2019 um 07:31

Sehr geehrte(r), Matthias Koll,
Dies ist Ihre offizielle Benachrichtigung dass folgende Dienste deaktiviert und gelöscht werden, falls ihr Profil nicht verifiziert wird.
Laut unseren Geschäftsbedingungen, sowie um sicher zu gehen das Ihre Karte nicht von unberechtigten Dritten verwendet wurde, haben wir Ihren Zugriff zu ihrem Kundenkonto eingeschränkt.
Vorangegangene Benachrichtigungen wurden an die mit ihrem Account verknüpfte Rechnungsadresse gesendet Als Primärkontakt müssen Sie folgende Dienste erneuern: SERVICE: Apple.

Um Ihr Kundenkonto wieder zu aktivieren, klicken Sie bitte hier [http://rohrreinigung-klo[REDACTED].at/apple/messages/question/DE/2019-02/] und folgen Sie den Anweisungen. Wir sind 24 Stunden am Tag, 7 Tage die Woche für Sie erreichbar.

Apple Support



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

Google 

Alle **News** Bilder Videos Shopping Mehr Einstellungen Tools

Ungefähr 19.200 Ergebnisse (0,20 Sekunden)


Aktuelle Trojaner-Welle: Emotet lauert in gefälschten Rechnungsmails
 heise online - vor 1 Stunde
 Offensichtlich hat es der **Emotet**-Schädling nun auf Privatpersonen abgesehen. Derzeit sind gehäuft gefälschte Amazon-, Telekom- und ...
[Vodafone: E-Mail mit Rechnung enthält Trojaner \(Schadsoftware\)](#)
[Onlinewarnungen.de \(Pressemitteilung\) \(Blog\)](#) - vor 6 Stunden
 Amazon-User aufgepasst! Neue gefährliche Betrugswelle rollt
 Börse Online - vor 2 Stunden
[Alle ansehen](#)


Kampf gegen einen agilen Gegner: Erkenntnisse von der Emotet-Front
 PresseBox (Pressemitteilung) - vor 2 Stunden
 Der Trojaner Emotet ist darauf spezialisiert, Schutzbarrieren auszuweichen, immer wieder zuzuschlagen und sich zu vervielfältigen, um ...
[Erkenntnisse von der Emotet-Front](#)
[Netzpalaver \(Pressemitteilung\) \(Blog\)](#) - vor 2 Stunden
[Alle ansehen](#)


Emotet-Schadsoftware: Wie sich Betriebe jetzt schützen müssen
 Deutsche Handwerks Zeitung - 21.01.2019
 Die Tricks von Cyber-Kriminellen werden immer ausgefeilter. Aktuelles Beispiel ist die Schadsoftware "Emotet", mit der Verbrecher gezielt ...
[Emotet, die Allzweckwaffe der Cyberkriminellen](#)
[Netzpalaver \(Pressemitteilung\) \(Blog\)](#) - 23.01.2019
[Alle ansehen](#)


Fieser Trojaner verbreitet sich über Amazon-Mails: Darum ist er so ...
 STERN.de - 24.01.2019
 Wir erklären, was **Emotet** so gefährlich macht - und wie man sich schützen kann. ...
 Dass sich **Emotet** so schnell verbreitet, liegt daran, dass der ...

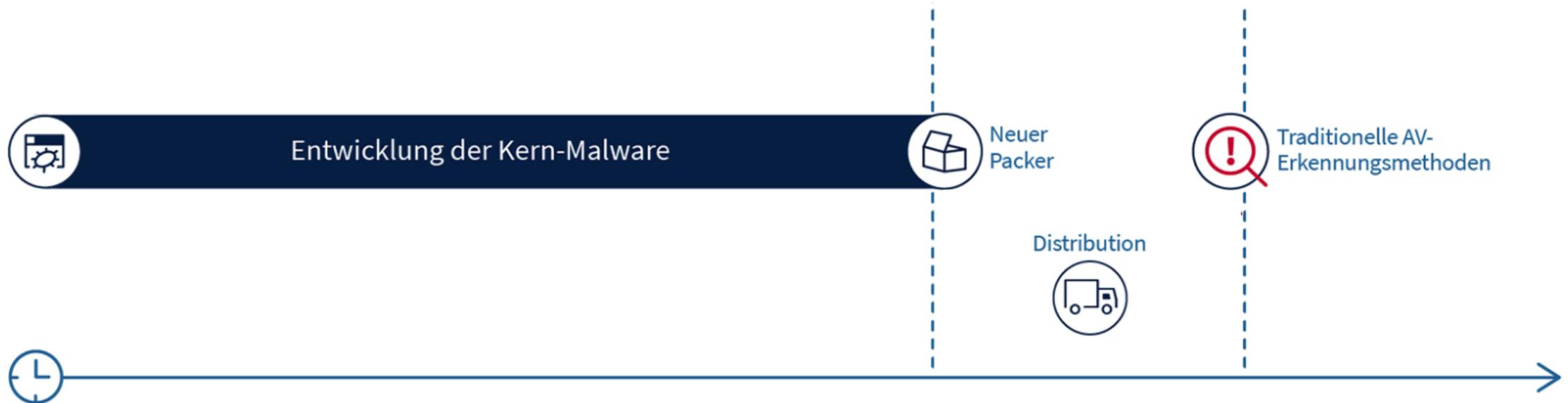

Trojaner Emotet wird noch gefährlicher
 n-tv NACHRICHTEN - 19.01.2019
 Die Bedrohung für Privatanutzer und Firmennetzwerke durch den Trojaner **Emotet** wächst weiter an. Er lädt jetzt einen weiteren Trojaner nach, ...
[Emotet-Trojaner kehrt zurück und ist gefährlicher als bisher](#)
 TECHBOOK - 20.01.2019
[Alle ansehen](#)

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



Schäden durch
Cyber-Spionage p.a.

50-100 Mrd €*

*(BDI / VDI)

3.

Tipps und Tricks für den IT-Admin

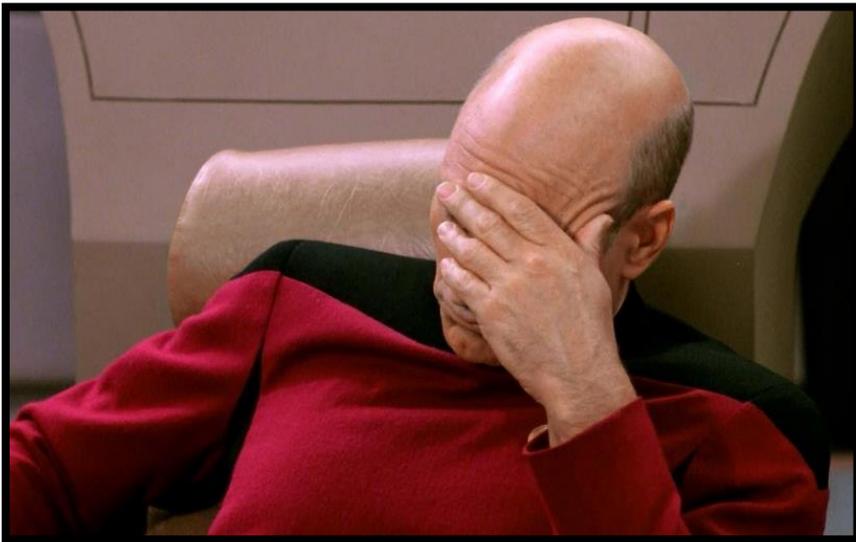
Sicherheitstipps

- 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.

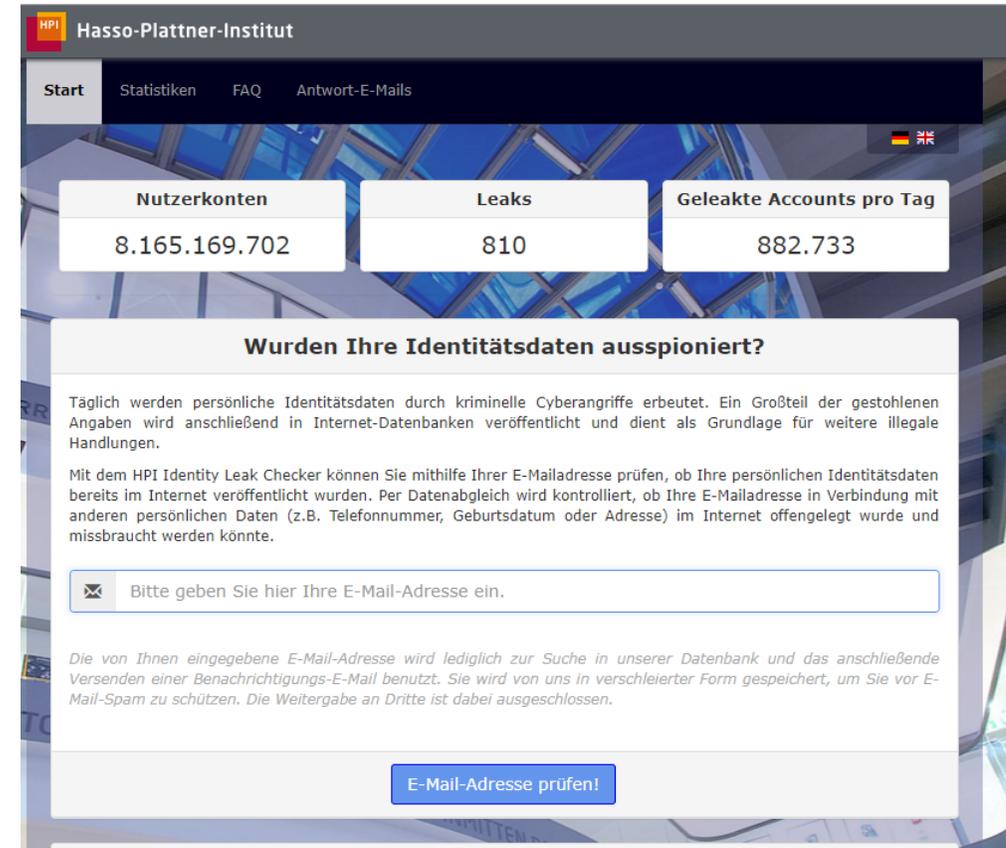
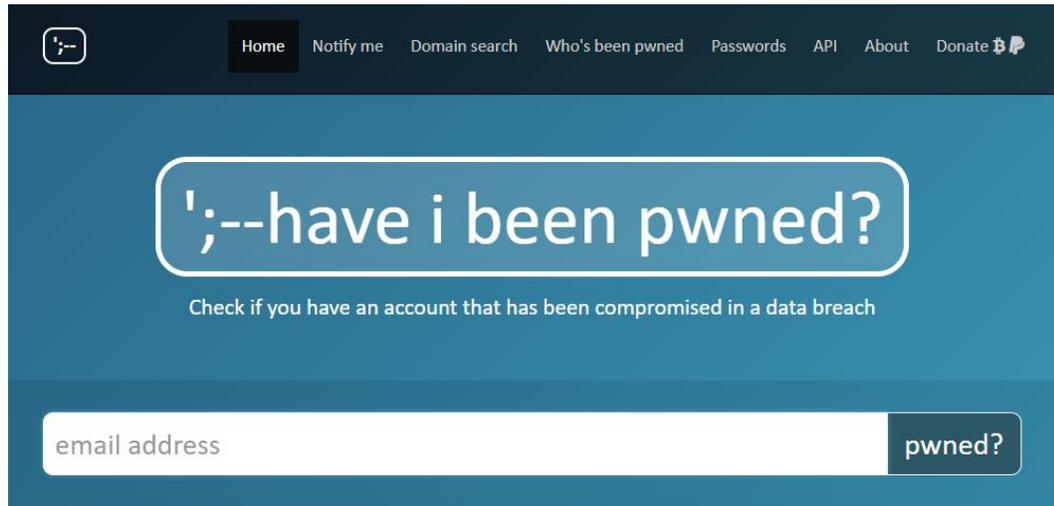
Von Tilman Wittenhorst

🔊 | 🖨️ | 💬 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

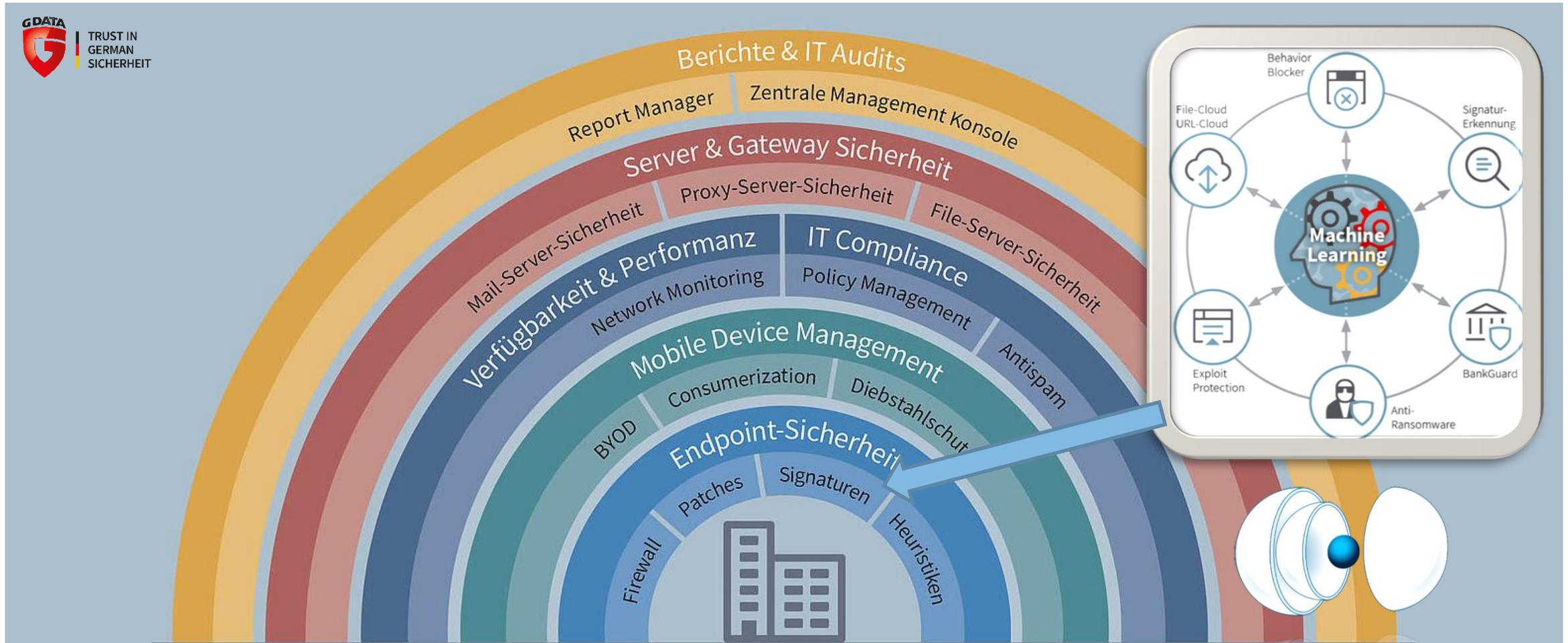
Technologische Maßnahmen - Realität

- 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

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!