

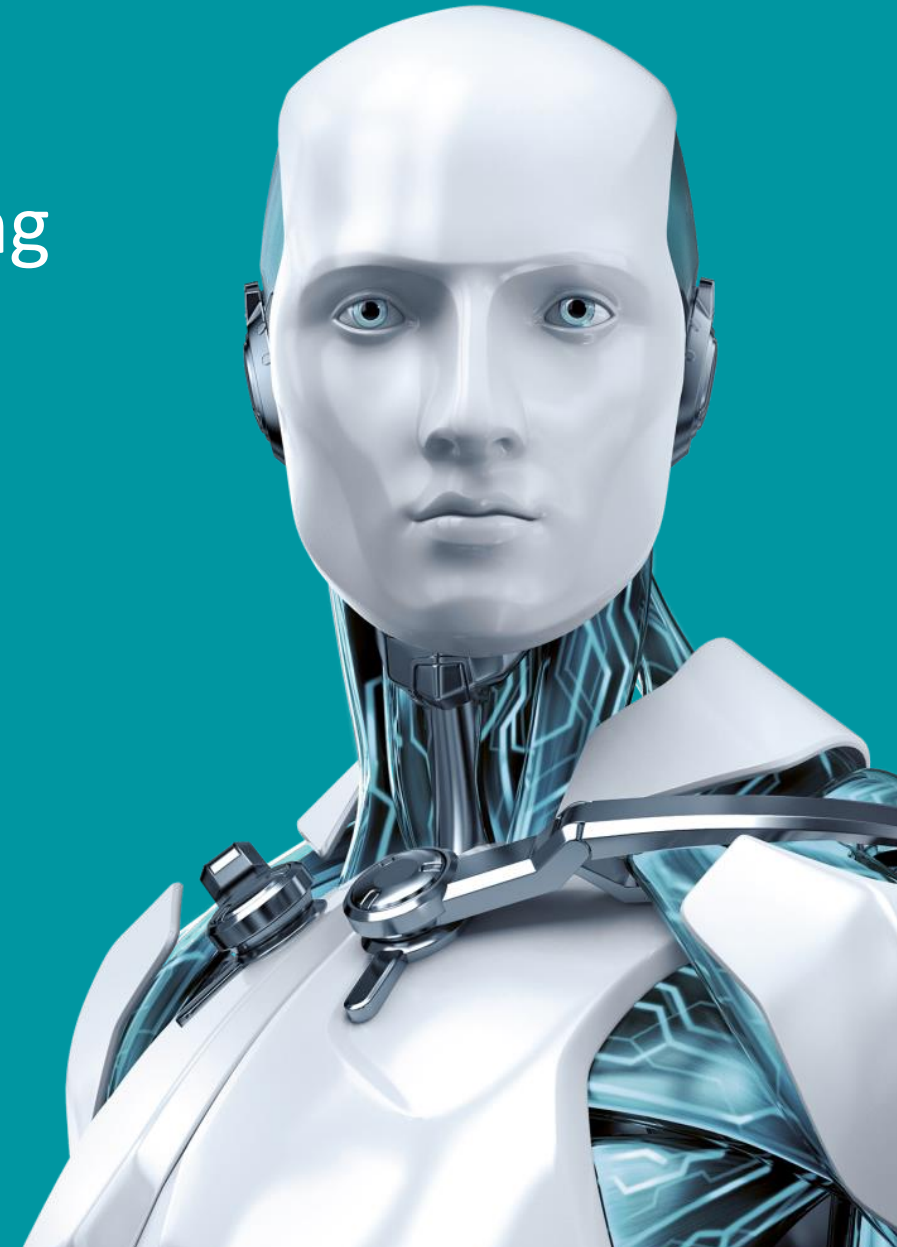
# Schutzziele der DSGVO

## Raketenwissenschaft vs. Risikominimierung

**Michael Schröder**

Business Development Manager

ESET Deutschland GmbH



# Was für ein Tag ist der 25. Mai 2018?



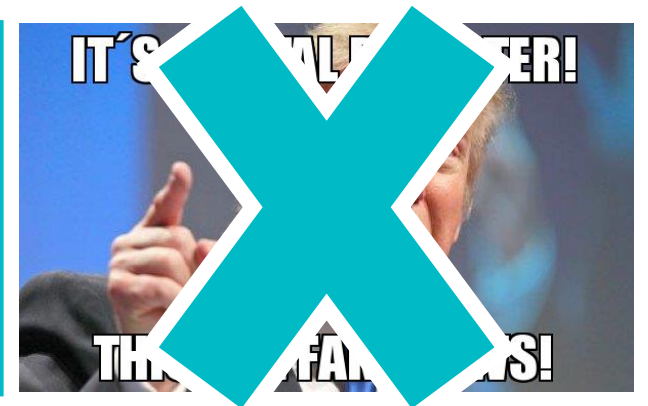
Richtig!: Am 25. Mai 2018 feiern wir zum 17. in Folge den „Towel-Day“ den intergalaktischen „Tag des Handtuchs“ in Gedenken an den Autor Douglas Adams „Per Anhalter durch die Galaxis“

# Short Facts zur DSGVO

Einstieg in die Welt der personenbezogenen Daten  
und warum quasi jeder betroffen ist.

# Short Facts zur DSGVO / Eckdaten

- Das bisherige DSG wird durch die neue Regelung ersetzt (DSG-August 2018)
  - Es gibt keine Übergangsfristen (Fallbeileffekt)
  - Branche / Betriebsgröße / behördliche Zuordnung spielt keine Rolle
  - Bußgeldstufe 1: bis 10 Mio. EUR oder 2% des weltweiten Jahresumsatzes
  - Bußgeldstufe 2: bis 20 Mio. EUR oder 4% des weltweiten Jahresumsatzes
- Die Bußgelder sollen wortwörtlich „abschreckend“ sein
  - Erhobene Bußgelder verbleiben bei der ausstellenden Aufsichtsbehörde
  - Unternehmen / Behörden werden „rechenschaftspflichtig“



# Short Facts zur DSGVO / Personenbezogene Daten



Schwarz= Offensichtlich  
Blau= weniger offensichtlich  
Orange= besondere Kategorien (Artikel 9) o. kritisch

# Short Facts zur DSGVO / Geltung und Anwendung

---

Es geht um die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von natürlichen Personen (außerhalb familiärer, behördlich präventiver und repressiver Zwecke) mit Wohnsitz in der EU oder „aufhältig“ in der EU (z.B. Urlaub).

Dies gilt grundsätzlich für alle Unternehmen/Behörden mit Sitz, Niederlassung oder einem Auftragsverarbeiter in der EU. Aber auch in allen Fällen, in denen Daten von EU-Bürgern durch außereuropäische Verarbeiter (Unternehmen) im Zusammenhang mit dem Absatz von Waren und Dienstleistungen verarbeitet werden.



# Short Facts zur DSGVO / Durchsetzung?

Fragebogen zur Umsetzung der DS-GVO zum 25. Mai 2018

Unternehmen/Verantwortliche Stelle	Eingangsstempel BayLDA
<b>I. Struktur und Verantwortlichkeit im Unternehmen</b>	
1.	<ul style="list-style-type: none"><li>Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch<ul style="list-style-type: none"><li>Vorhandensein einer Datenschutzleitlinie</li><li>Beschreibung der Datenschutzziele</li><li>Regelung der Verantwortlichkeiten</li><li>Bewusstsein über Datenschutzrisiken</li><li>Transparenz über Zielkonflikte (z.B. zwischen Marketing- und Rechtsabteilung)</li></ul></li></ul>
2.	<ul style="list-style-type: none"><li>Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten?<ul style="list-style-type: none"><li>Wenn nein, warum nicht?</li><li>Wenn ja, ist geklärt, wann er von wem einzubeziehen ist?</li><li>Wenn ja, ist er schon gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?</li></ul></li></ul>
<b>II. Übersicht über Verarbeitungen</b>	
1.	<ul style="list-style-type: none"><li>Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO?<ul style="list-style-type: none"><li>Wenn nein, warum nicht? Ist das dokumentiert?</li></ul></li><li>Wie haben Sie sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Prozesses in Ihrem Unternehmen Berücksichtigung finden (Privacy by Design –Art. 25 DS-GVO)?</li></ul>
<b>III. Einbindung Externer</b>	
1.	<ul style="list-style-type: none"><li>Haben Sie Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden?<ul style="list-style-type: none"><li>Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter?</li><li>Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?</li></ul></li></ul>
<b>IV. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte</b>	
1.	<ul style="list-style-type: none"><li>Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst?<ul style="list-style-type: none"><li>Wenn nein, warum nicht?</li></ul></li></ul>
2.	<ul style="list-style-type: none"><li>Haben Sie insbes. folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten:<ul style="list-style-type: none"><li>Kontaktdaten des Datenschutzbeauftragten</li><li>Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten</li><li>Falls Sie die Verarbeitung mit ihren berechtigten Interessen oder berechtigten Interessen eines Dritten</li></ul></li></ul>



- Mehr Personal für Aufsichtsbehörden
- Fragebögen zum Stand der Umsetzung
- Umfangreiche Auskunft- und Meldepflichten
- Faktische Beweislastumkehr bei Vorfällen/Anfragen
- Öffentliches Interesse zum Datenschutz steigt

# Short Facts zur DSGVO / Was wenn doch was passiert?

**SPIEGEL ONLINE** DER SPIEGEL SPIEGEL TV Suche Anmelden

Spionage, Sabotage, Datendiebstahl  
**Neuartige Angriffe kosten deutsche Wirtschaft 55 Milliarden Euro**

Ist die deutsche Wirtschaft vor digitalen Gefahren gut genug geschützt? Jede zweite Firma wurde schon angegriffen - meist verschweigen die Unternehmen die Attacken. Der Staatsschutz ist alarmiert.

Von  Fabian Reinbold



Notebook

[Teilen](#) [Twittern](#) [E-Mail](#) [+](#)

Freitag, 21.07.2017 10:30 Uhr [Drucken](#) [Nutzungsrechte](#) [Feedback](#) [Kommentieren](#)

Mehr als jedes zweite Unternehmen ist in den vergangenen zwei Jahren aus dem Internet angegriffen worden, 53 Prozent der deutschen Firmen wurden Opfer von [Wirtschaftsspionage](#), Sabotage oder Datendiebstahl. Der Schaden ist enorm: rund

- Reputationsverlust / Schlechte Presse
- Umsatzeinbrüche
- Bußgelder
- Prüfung durch Aufsichtsbehörden (Artikel 57 Abs. 1)
- Schadenersatzansprüche (Artikel 82)
- Schmerzensgeld (Artikel 82 / immaterielle Schäden)

## Haftung ist nicht delegierbar!



A man in a grey suit, blue shirt, and striped tie is smiling while talking on a mobile phone. He is also holding a tablet in his left hand. The background is a blurred office setting. The entire image has a teal overlay. A white rectangular box is centered over the image, containing the main title and subtitle in white text.

# Kontroll-Check: Schutzziele der DSGVO

Worum müssen wir uns kümmern?

# Schutzziele der DSGVO - Grundsätze

---



Orange= Schutzziele

Blau= Maßnahmen

(Art. 32 Abs. 1b oder § 64 BDSG/neu)

# Schutzziele der DSGVO – Fallbeispiele

---

- Gespeicherte Daten in der Organisation schützen (Daten in Ruhe)
- Daten bei der Übertragung schützen (Daten in Bewegung)
- Die Übermittlung zwischen zwei Speicherorten absichern

## **Verschlüsselung** von:

- Festplatten
- Mail-Kommunikation (teilweise)
- Dateien / Ordnern
- USB- und Wechselmedien

- Den Zugriff auf bestimmte Daten blockieren/einschränken
- Den sicheren Datenzugriff auf Anfrage/Genehmigung gestatten

## **Remote Management** für:

- Gruppen, Teams, Einzelnutzer
- alle Geräte (auch Offsite)

- Die Zugänge / Logins zu Geräten und Ressourcen absichern
- Ein angemessenes Schutzniveau gewährleisten

## **Regeln / Grundschutz** erzwingen:

- Gruppen, Geräte, Einzelnutzer
- Grundregeln / Devicecontrol

# Unser Engagement für Sie - [dsgvo.eset.ch](https://dsgvo.eset.ch)

Die neue EU-Datenschutzgrundverordnung (DSGVO)

Was ist die DSGVO? Wo stehen Sie? Jetzt testen! Drei Bausteine der IT-Sicherheit Wie ESET Sie unterstützt [COMPLIANCE CHECK MACHEN](#)

## Wie Sie Datenschutz am besten in die Praxis umsetzen – und wie ESET Sie unterstützt

[COMPLIANCE CHECK MACHEN](#) [KOSTENLOSE INFORMATIONEN](#)

Die neue EU-Datenschutzgrundverordnung (DSGVO)

Was ist die DSGVO? Wo stehen Sie? Jetzt testen! Drei Bausteine der IT-Sicherheit Wie ESET Sie unterstützt [COMPLIANCE CHECK MACHEN](#)

## Compliance Check

### Vorläufige Ergebnisse

Ihren Antworten zufolge bewerten wir Ihren derzeitigen Compliance-Status als:

**STATUS: INFORMIERT**

**Zusammenfassung:** Ihr allgemeines Bewusstsein für die gesetzlichen Änderungen beim Datenschutz beeinflusst Ihren Umgang mit der Datenverarbeitung. Allerdings haben Sie die Anforderungen noch nicht ganzheitlich analysiert, ausgearbeitet oder dokumentiert. Ihre bestehenden Strategien sind unter Umständen nicht vollständig.



### Vollständige Ergebnisse anfordern

Geben Sie Ihre Kontaktdaten ein und erhalten Sie umgehend einen **vollständigen, persönlichen Bericht** sowie eine detaillierte Beurteilung mit den empfohlenen nächsten Schritten.

## Ist Ihr Unternehmen für die DSGVO gewappnet?

Im Mai 2018 tritt die neue EU-Datenschutzgrundverordnung (DSGVO) in Kraft.

Die DSGVO wird die Datenschutzrichtlinie 95/46/EG ersetzen, mit dem Ziel, das europäische Datenschutzrecht zu vereinheitlichen. Die Regelungen betreffen alle europäischen Unternehmen und Behörden, die personenbezogene Daten jeglicher Art verarbeiten. Aber auch Organisationen ohne Niederlassung in Europa müssen sich an die Vorgaben halten, sofern sie Geschäfte in der EU tätigen. Die Regelungen sind sehr komplex und bei Nichteinhaltung drohen erhebliche Strafen.

Doch keine Sorge, wir machen Sie fit für die DSGVO. Auf dieser Webseite geben wir Ihnen das richtige Rüstzeug sowie hilfreiche Tipps und Tricks an die Hand, wie Sie die neuen An- und Herausforderungen sicher angehen.



## Schutzziele der DSGVO

### Raketwissenschaft vs. Risikominimierung

Michael Schröder  
Business Development Manager  
ESET Deutschland GmbH

30 30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

Sieht es mit dem Ton Klapp...  
Wie würde die Audio-Option "Call using my Computer" über einem die Einsatz über eine Telefonleitung.  
Es geht!

[COMPLIANCE CHECK MACHEN](#)

DESLOCK ENCRYPTION BY **eset**

## Quick Guide zur EU-Datenschutzgrundverordnung

ENJOY SAFER TECHNOLOGY™

**eset** ENJOY SAFER TECHNOLOGY™

## Leitfaden zur Umsetzung der Datenschutzgrundverordnung

Thomas Feil – Fachanwalt für IT-Recht und Arbeitsrecht und externer Datenschutzbeauftragter bei Unternehmen und Behörden



# IT-Sicherheit

Kollision von Anspruch und Realität

## Die Realität der IT-Sicherheit?:

---

**Welche IT-Security Lösungen haben Unternehmen heute vollständig ausgerollt und unternehmensweit im Einsatz?**

**Etwa 70% vertrauen letztlich noch immer allein auf bestehende AV-Lösungen und die interne Firewall (Hard-/Software)**

# Stand der Technik – Saubere Definition in der DSGVO?

---

„Unter Berücksichtigung **des Stands der Technik**, der **Implementierungskosten** und der Art, des Umfangs, der Umstände und der **Zwecke der Verarbeitung** sowie der unterschiedlichen **Eintrittswahrscheinlichkeit** und **Schwere des Risikos** für die Rechte und Freiheiten natürlicher Personen, treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem **Risiko angemessenes Schutzniveau** zu gewährleisten.“

(Art. 32 DSGVO)

**Es gibt also keine saubere Definition zum „Stand der Technik“.  
Verantwortliche sollen sich orientieren am...**

**IT-Grundschutz**



**IT-Sicherheitsgesetz**

# Stand der Technik – Die gute Nachricht

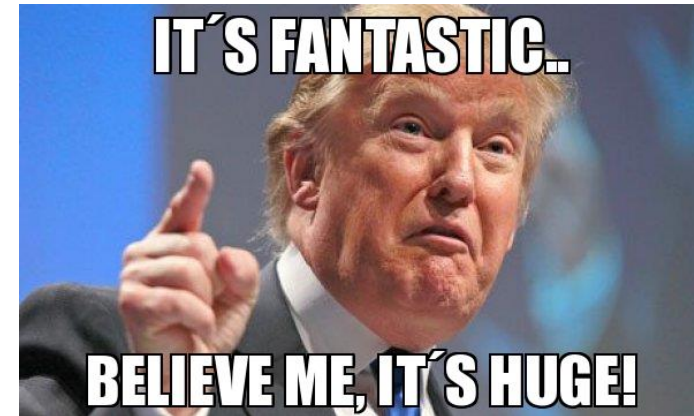
---

## Wir erinnern uns an die Definition?

- „Implementierungskosten“
- „Zwecke der Verarbeitung“
- „Eintrittswahrscheinlichkeit“
- „Schwere des Risikos“
- „Dem Risiko angemessenes Schutzniveau“

Vielmehr sollen technische Maßnahmen erhoben werden, die zur Verfügung stehen und die sich bereits in der Praxis bewährt haben. Gemeint sind also nicht Techniken, die gerade neu entwickelt wurden!

Unter Berücksichtigung Ihrer eigenen Risikobetrachtung/-beurteilung und unter Einbeziehung der obigen Punkte dürfen Sie die Anforderungen jederzeit „unterschreiten“ bzw. aufgrund Ihrer Kosten im Verhältnis zur Betriebsgröße als ungeeignet einstufen.

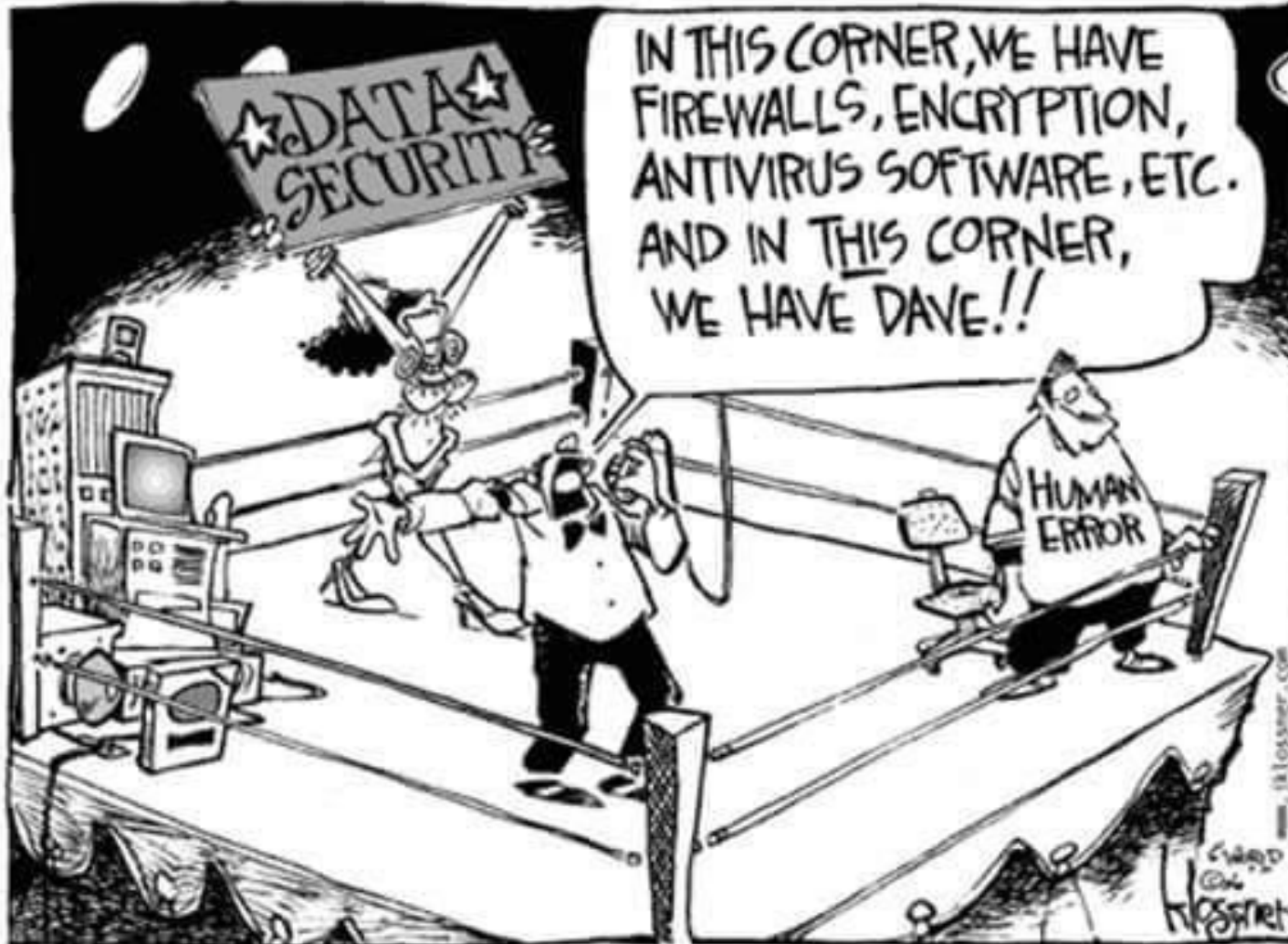






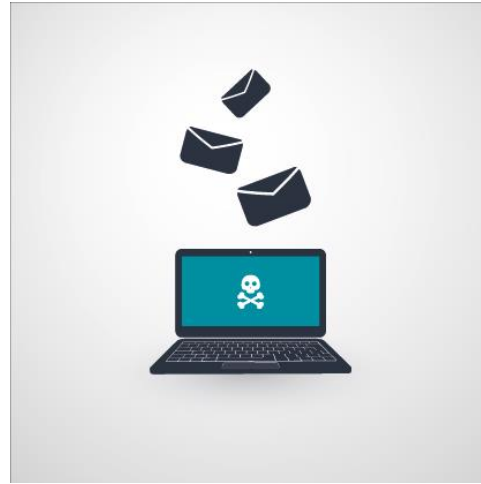
**Mit Risikominimierung um Lichtjahre voraus**  
Umsetzbare Szenarien für Organisationen und Mitarbeiter schaffen

# Problem Nummer 1: Der Faktor Mensch



# Problem Nummer 1: Der Faktor Mensch

---



Dateianhänge wie Bewerbungen, eingeschleuste Medien und Phishing-Mails sind noch immer Top aktuelle Angriffs-Vektoren für Cyberkriminelle.

Einfach / Effizient / Skalierbar

## Die digitale Sorglosigkeit

# Problem Nummer 2: Unsere „Passworthygiene“

Whitepaper Termine Partnerzone Anbieterkompass

Shop Zeitschriften Newsletter Media Kontakt



**funkschau**  
business.technology.strategy

SUCHEN

TELEKOMMUNIKATION | DATACENTER | MOBILE SOLUTIONS | MEHR +

channel port

HOME > TELEKOMMUNIKATION

Der Countdown läuft

## Wann wird Ihr Passwort gestohlen?

09.08.2017

Autor: Dr. Amir Alsibh / Redaktion: Axel Pomper

Erst kürzlich hat das Bundeskriminalamt (BKA) im Darknet eine Datenbank mit rund 500 Millionen Zugangsdaten aus Hacker-Attacken aufgespürt. Die Datensätze enthalten so sensible Informationen wie E-Mail-Adressen und Passwörter von Internetdiensten.

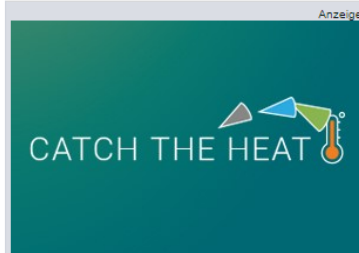


© Robert Mizerek - fotolia.com

Bis die Provider ihre Kunden über den Diebstahl informiert hatten, sind die Angreifer längst mit wertvollen persönlichen Informationen über alle Berge. Denn meistens verstreicht sehr viel wertvolle Zeit, bis die Unternehmen das Datenleck überhaupt erst einmal bemerkt haben: Laut Experten dauert das durchschnittlich mehr als vier Monate, im öffentlichen Sektor sogar bis zu einem Jahr und darüber hinaus.

### Passwörter wiegen Nutzer in falscher Sicherheit

Diese Zeitspannen kommen im Digitalzeitalter, das in Minuten und Sekunden denkt und handelt, geradezu Ewigkeiten gleich. Während die Kunden also noch ahnungslos sind, haben sich die Angreifer bei mehrfach genutzten Passwörtern bereits in diverse Webportale eingeloggt und dort möglicherweise weiteren Schaden für den Nutzer verursacht. Das kann von kostspieligen Bestellungen auf Amazon über Kontoabbuchungen bis hin zum umfangreichen Identitätsdiebstahl reichen. Die Geschichte eines US-



### PREMIUMANBIETER ZUM THEMA

ESET Deutschland GmbH



baramundi software AG



Axis Communications GmbH



Nexus Technology GmbH



### LESERWAHL ITK-PRODUKTE DES JAHRES 2017

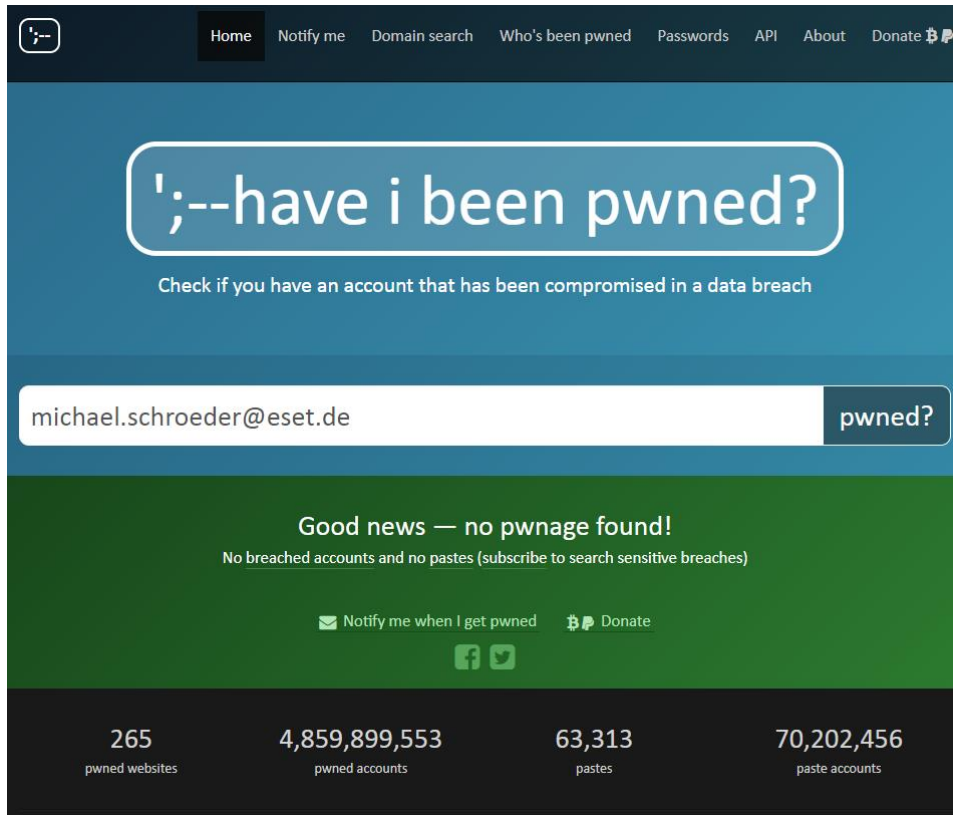


„... mittlerweile sind **gestohlene oder schwache Passwörter in 81 Prozent aller Fälle die Ursache für einen Hack**. 2016 waren es „nur“ knapp über 60 Prozent.“

„**Wann** Datenverluste Unternehmen, Mitarbeiter und Kunden betreffen, **ist inzwischen also nur eine Frage der Zeit** – wenn keine zusätzlichen Schutzmaßnahmen getroffen werden.“

„Dabei lässt sich Transaktionssicherheit **vergleichsweise schnell und einfach** durch eine risikobasierte Multi-Faktor-Authentifizierung (MFA) gewährleisten...“

# Problem Nummer 2: Unsere „Passworthygiene“



<http://www.haveibeenpwned.com>

Annähernd 5 Milliarden Accounts gehackt ...

Ihre Passwörter sind lang und komplex aufgebaut?

Zudem lassen Sie Ihre Nutzer die Passwörter alle 30/60/90 Tage wechseln ?

Gute Idee! - Oder ?

61%\* der Nutzer verwenden „besonderes sichere“ Passwörter mehrfach, auch im Internet oder für private Zwecke!

\*Verizon Data Breach Report 2011-13

## Problem Nummer 3: Mein Feind, das Gerät

---



- Keine ausreichenden Device-Regeln (Darf jeder „dropbox.com“ öffnen?)
- Lückenhaftes Patch-Risikomanagement (Sind aktuelle Sicherheitslücken des Systems geschlossen?)
- Offene Geräte-Schnittstellen (USB Ports, Speicherkarten, WebCams)
- Mobile Geräte als Risikofaktor (Diebstahl, keine sichere Verbindung, aufgeklebte/mitgeführte Passwörter)

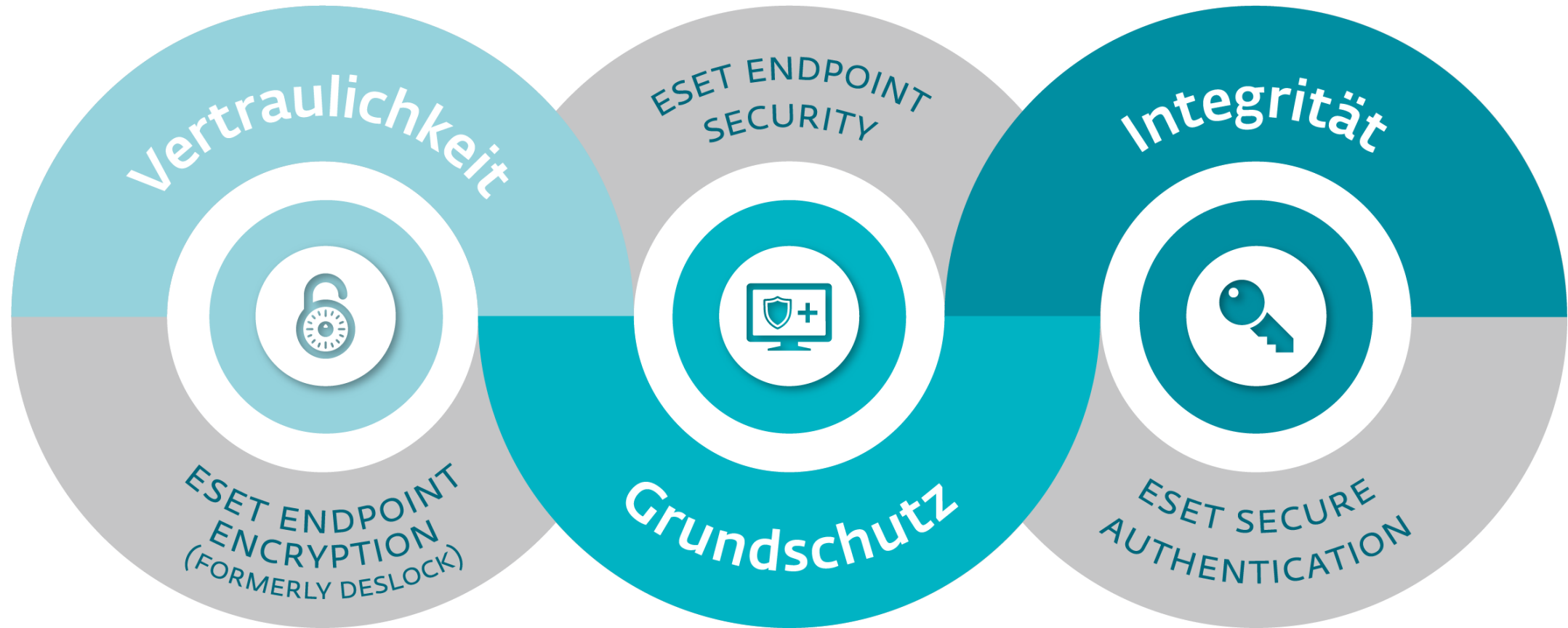


# Mehr Schubkraft durch technische Lösungen

Die 3 Bausteine der IT-Sicherheit

# Die 3 Bausteine der IT-Sicherheit

---





# Vertraulichkeit, Grundschutz, Integrität



Verhindert Datenschutzvorfälle durch Diebstahl, Verlust und „Fehlbedienung“ der Nutzer!

- Zertifiziert und Patentiert
- Sicherheit & Kontrolle, überall
- Ein Produkt, viele Lösungen

Perfekte Alltagstauglichkeit  
einzigartiges Remote Management!



Schützt vor aktuellen Bedrohungen und „unerwünschtem Verhalten“ Ihrer Mitarbeiter!

- Alles im Griff
- Sicher?, aber logisch!
- Darf hier eigentlich jeder alles?

Endpoint Security kann mehr als nur Anti-Virus!



Eliminiert das Risiko „unsicherer“ Passwörter für immer, ohne Ihre Mitarbeiter einzuschränken!

- Einfach und effektiv
- Effizient, auch bei den Kosten
- Flexibilität schafft Akzeptanz

2-Faktor-Authentifizierung sichert mehr als nur VPN-Zugänge!



Kommt ein Ochs in fremdes Land, er wird  
doch als Rind erkannt.

(Bernhard Freidank)

„Patentiert und Einzigartig“  
Was macht das Produkt so besonders?

# Vorgeschichte - Das „Problemkind“ Verschlüsselung

---

„...ein mangelndes Gleichgewicht zwischen Sicherheit und Produktivität!“

„...fehlendes Remote Management!“

„...zu komplex und sperrig für unsere Nutzer!“

„...leider NULL Flexibilität!“

**Schon mal gehört?**



ENJOY SAFER TECHNOLOGY™

# ESET ist nicht einfach eine weitere Black Box...

---



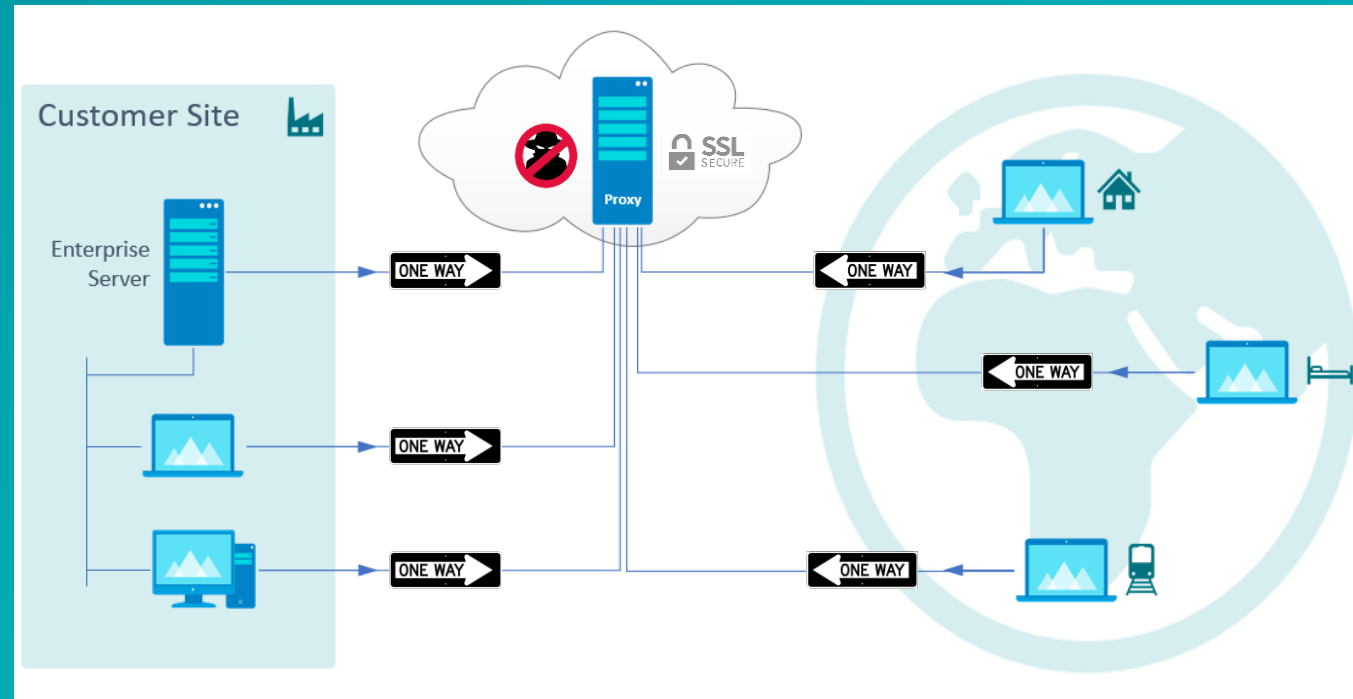
ENJOY SAFER TECHNOLOGY™

# Architektur – Wo verstecken sich unsere Patente?

Keine eingehenden Verbindungen, keine offenen Ports!

Einfache Installation, auch als VM oder auf eigenem SQL Server

Alle Daten liegen bei Ihnen, nicht in der Cloud!



Perfekt gesichert durch 256bit SSL Zertifikat von ESET

Pakete / Payload gesichert mit 256bit AES + 1024bit RSA

Jederzeit volle Kontrolle über alle Systeme!

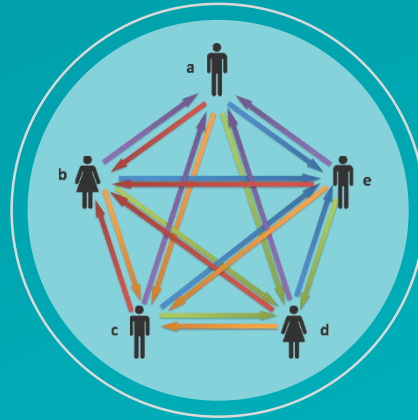
[AT341786](#) [CN1571949](#) [DE60215196](#) [EP1423765](#) [ES2274067](#) [GB2378539](#) [IL160709](#) [JP2005502240](#) [RU2273959](#) [WO03021400](#) [US7471796](#) ...

# Unsere „Schlüssel-Logik“



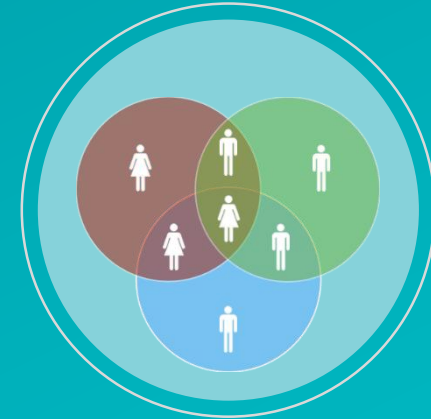
## Passwort = Schlüssel

- Veraltet
- Unsicher
- Ungeeignet im Alltag



## Public Key Infrastruktur

- Clever aber kompliziert
- Auf Dritte angewiesen
- Wo liegen Ihre Daten?



## ESET Schlüssel-Logik

- Kinderleicht zu verstehen
- Patentiert und logisch
- Hochdynamisch nutzbar

Policies und Keys können dadurch in Ihrer Organisationsstruktur granular angewendet und „vererbt“ werden!

# Funktionalität – Was bringt das Produkt mit?

---

## Festplattenverschlüsselung (256bit AES)



- Zentrale Management-Oberfläche
- Eigene, patentierte Technologie
- FIPS 140-2 Zertifizierung
- PreBoot Authentifizierung
- UEFI oder Legacy BIOS Modus
- Single-Sign-On für AD User
- TPM Unterstützung (optional)
- Multiuser-fähig
- Admin und Recovery Zugänge

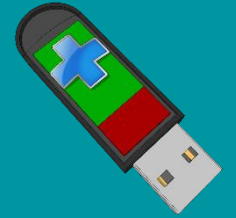


ENJOY SAFER TECHNOLOGY™

# Funktionalität – Was bringt das Produkt mit?

---

## Verschlüsselung von Wechselmedien (256bit AES)



- Zentrales Policy-Management
- Unterstützt alle Wechselmedien
- Voll- oder Teilverschlüsselung
- Trennt sichere und unsichere Daten
- Sperren von USB Funktionalitäten
- Nahtlose Integration in den Alltag
- Austausch mit Extern (Kurier etc.)



ENJOY SAFER TECHNOLOGY™



# Funktionalität – Was bringt das Produkt mit?

---

## Datei/Ordner/eMail Verschlüsselung (128bit AES)



- Sichere Datei/Ordner Verschlüsselung
- Keine Einschränkungen im Format
- Extrem transparente Schlüssellogik
- Umfangreiche Textverschlüsselung
- Mailverschlüsselung über PlugIn
- Mailversand an Extern (mit Passwort)



ENJOY SAFER TECHNOLOGY™

# Funktionalität – Was bringt das Produkt mit?

---

... „darf es noch etwas mehr sein?“



- Container Verschlüsselung
- Nutzung virtueller Disks
- Sichere Datenvernichtung
- Integration Ihrer AD-Struktur
- Auto-Enrolement (optional)
- Auto-Encryption (optional)
- Austauschbare Bootlogos (optional)



ENJOY SAFER TECHNOLOGY™

# Das Produkt ist am Markt daher kaum vergleichbar

---

- Wir haben ein „echtes“ Remote Management!
- Großer, alltagstauglicher Funktionsumfang
- Unsere Nutzer verstehen das Produkt
- Sie wissen wo Ihre Daten liegen
- Wir sind nicht auf „Dritte“ angewiesen



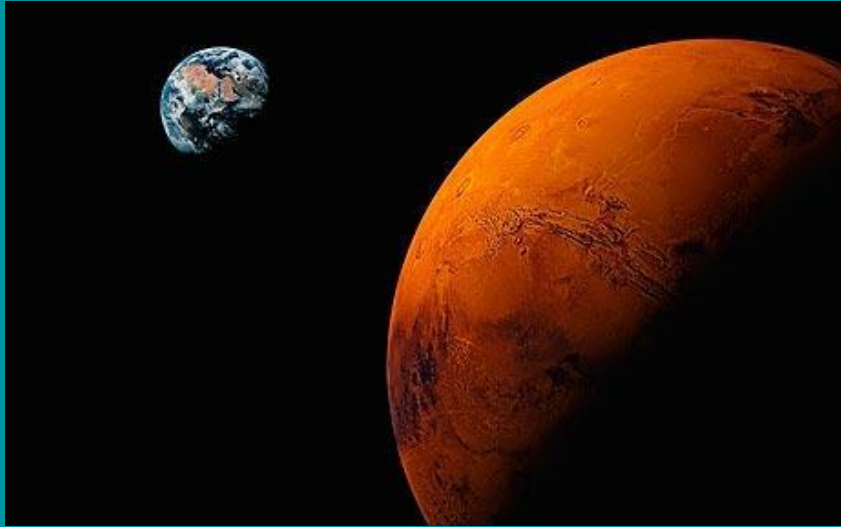
Ich hoffe wir verstehen uns?

---



ENJOY SAFER TECHNOLOGY™

# Mythbusters - Schlüsselstärke



**225.000.000 km  
(im Durchschnitt)**

**$2^{256}$  AES Keys**



**2.812.500.000.000  
(bei 8cm Länge)**

# Mythbusters - Schlüsselstärke

---

**Wenn jedes Nürnberger Würstchen nun einen AES Schlüssel symbolisiert...**

**... dann existieren genug Schlüssel um diese Würstchen-Kette zum Mars und wieder zurück zu legen ...**

20.585.260.308.856.200.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000

**Mal!**

(20 Nonilliarden)



ENJOY SAFER TECHNOLOGY™

# Mythbusters – Die Realität

---

**AES wurde niemals geknackt!**

**Ja, es gibt zwischenzeitlich Attacken die theoretisch 5 mal schneller sind als reines Brute-Forcing!**

**Selbst Quantencomputer bräuchten eine Ewigkeit um den passenden Key zu finden**

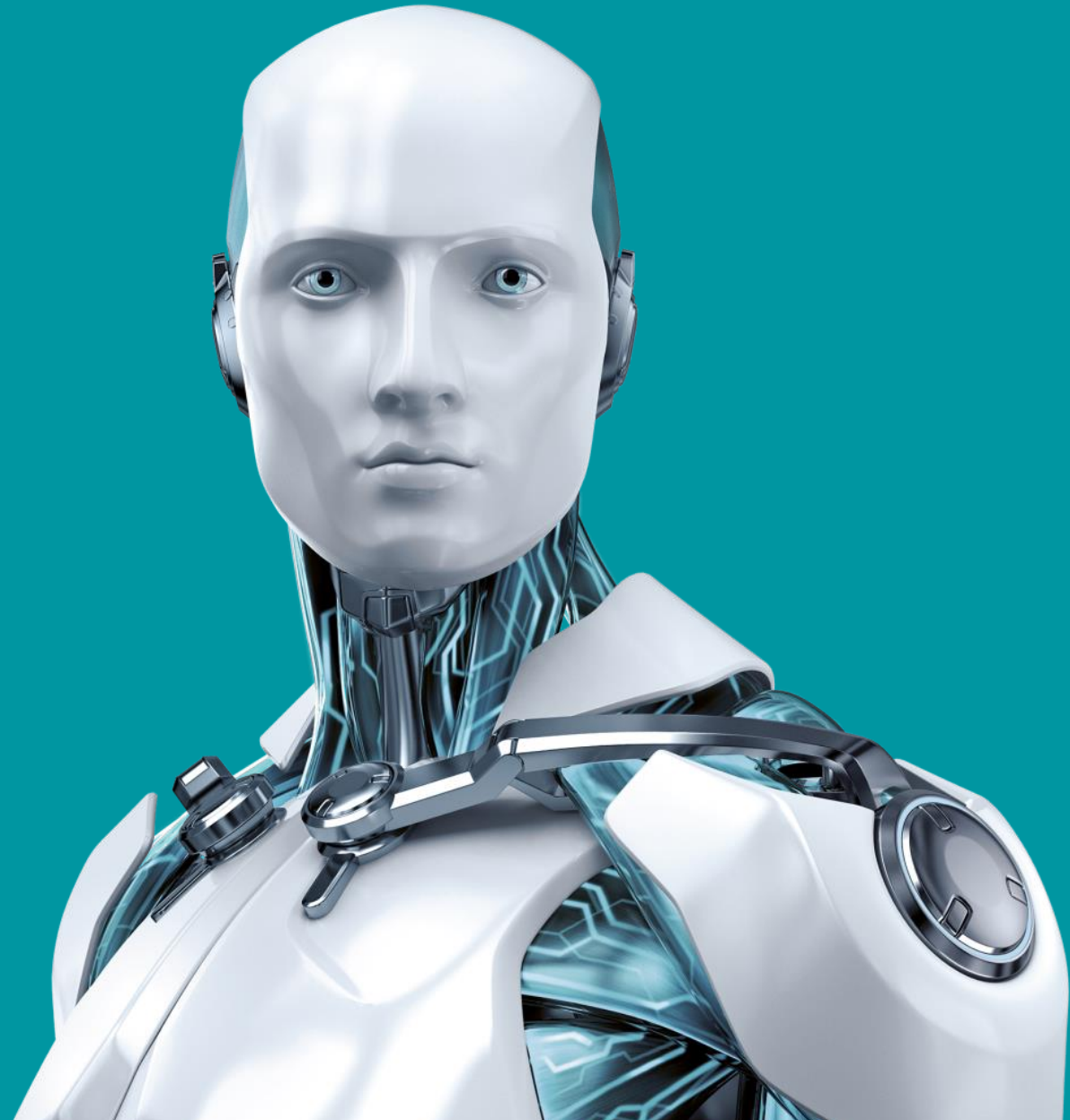


ENJOY SAFER TECHNOLOGY™



**Fragen?**







ENJOY SAFER  
TECHNOLOGY™

Michael Schröder

Business Development Manager  
New Technologies DACH

ESET Deutschland GmbH | [info@eset.de](mailto:info@eset.de) | [www.eset.de](http://www.eset.de)