Schutzziele der DSGVO

Raketenwissenschaft vs. Risikominimierung

Michael Schröder
Business Development Manager New Technologies
ESET Deutschland GmbH

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™

Vorab eine Frage zur Selbsteinschätzung:

Halten Sie die aktuellen (BDSG) und kommenden (DSGVO/BDSG-Neu) Datenschutzbestimmungen in Ihrer Organisation ein?

a.) Wir sind vollumfänglich konform zum aktuellen Datenschutz /BDSG

b.) Wir sind aktuell konform zum BDSG und arbeiten an der Umsetzung der EU-DSGVO

c.) Datenschutz ist bei uns teilweise ein Thema, spielte in der Vergangenheit aber eine untergeordnete Rolle

d.) Ehrlich gesagt, haben wir uns bisher mit dem Thema nicht aktiv auseinandergesetzt

Short Facts zur DSGVO

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

ENJOY SAFER TECHNOLOGY™

Short Facts zur DSGVO / Eckdaten

- Das bisherige BDSG wird durch die neue Regelung ersetzt (BDSG-Neu)
- 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

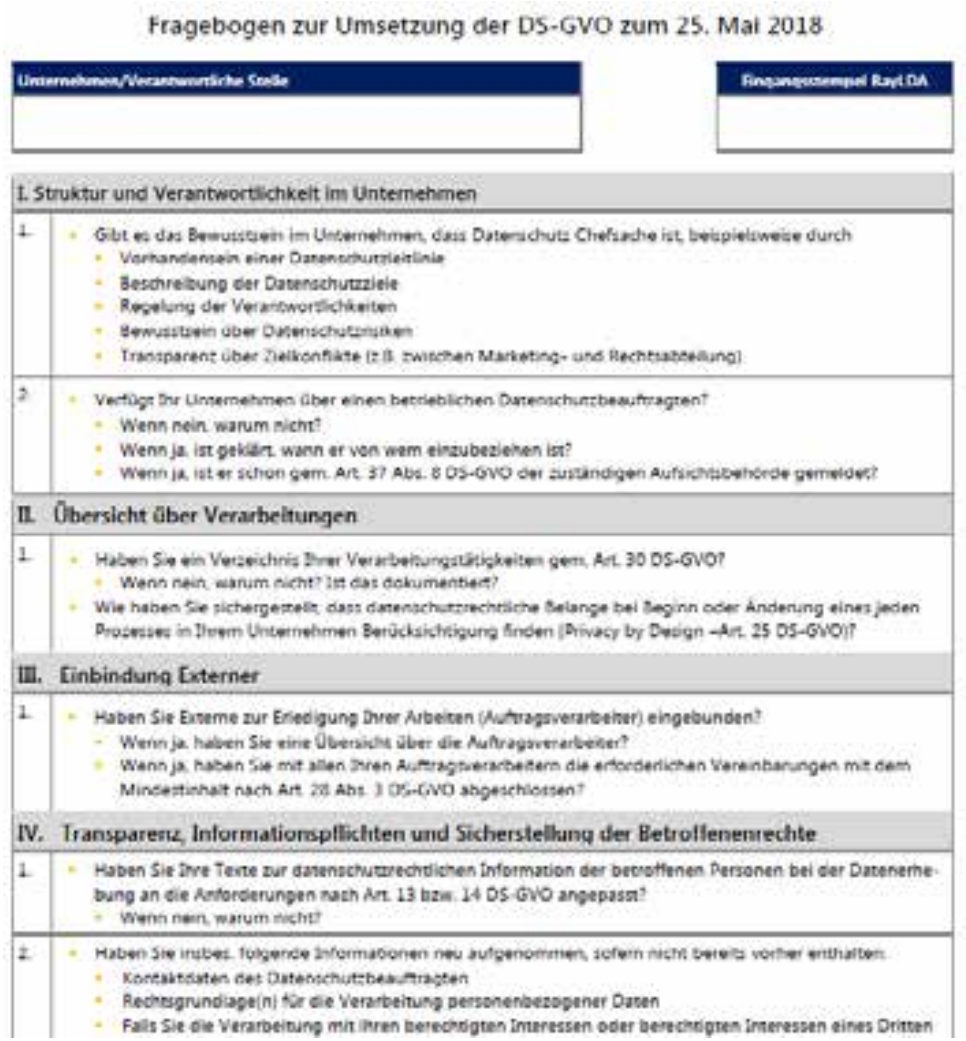
Schwarz= Offensichtlich
Blau= weniger offensichtlich
Orange= besondere Kategorien (Artikel9) o. kritisch

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

I. Struktur und Verantwortlichkeit im Unternehmen

1.
- Gibt es das Bewusstsein im Unternehmen, dass Datenschutz Chefsache ist, beispielsweise durch
  - Vorhandensein einer Datenschutzleitlinie
  - Beschreibung der Datenschutzziele
  - Regelung der Verantwortlichkeiten
  - Bewusstsein über Datenschutzrisiken
  - Transparenz über Zielkonflikte (z.B. zwischen Marketing- und Rechtsabteilung)

2.
- Verfügt Ihr Unternehmen über einen betrieblichen Datenschutzbeauftragten?
  - Wenn nein, warum nicht?
  - Wenn ja, ist geklärt, wann er von wem einzubeziehen ist?
  - Wenn ja, ist er schon gem. Art. 37 Abs. 8 DS-GVO der zuständigen Aufsichtsbehörde gemeldet?

II. Übersicht über Verarbeitungen

1.
- Haben Sie ein Verzeichnis Ihrer Verarbeitungstätigkeiten gem. Art. 30 DS-GVO?
  - Wenn nein, warum nicht? Ist das dokumentiert?
- 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)?

III. Einbindung Externer

1.
- Haben Sie Externe zur Erledigung Ihrer Arbeiten (Auftragsverarbeiter) eingebunden?
  - Wenn ja, haben Sie eine Übersicht über die Auftragsverarbeiter?
  - Wenn ja, haben Sie mit allen Ihren Auftragsverarbeitern die erforderlichen Vereinbarungen mit dem Mindestinhalt nach Art. 28 Abs. 3 DS-GVO abgeschlossen?

IV. Transparenz, Informationspflichten und Sicherstellung der Betroffenenrechte

1.
- Haben Sie Ihre Texte zur datenschutzrechtlichen Information der betroffenen Personen bei der Datenerhebung an die Anforderungen nach Art. 13 bzw. 14 DS-GVO angepasst?
  - Wenn nein, warum nicht?

2.
- Haben Sie insbes. folgende Informationen neu aufgenommen, sofern nicht bereits vorher enthalten:
  - Kontaktdaten des Datenschutzbeauftragten
  - Rechtsgrundlage(n) für die Verarbeitung personenbezogener Daten
  - Falls Sie die Verarbeitung mit Ihren berechtigten Interessen oder berechtigten Interessen eines Dritten

BayLDA

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

Short Facts zur DSGVO / Hindernisse und Blockaden

Was hält Unternehmen davon ab, die DSGVO direkt umzusetzen?	Allgemein vorhandene Ängste und Meinungen
Die Initialkosten (TOM Technische & Organisatorische Maßnahmen)	Die Umsetzung der DSGVO verschlingt große Teile des aktuellen Cash-Flow.
Interne Aufwände / Personal (Verfahrensverzeichnisse, Datenschutzbeauftragter, Meldewesen)	Die geforderten Maßnahmen sind einfach nicht umsetzbar.
Neue Abläufe im Unternehmen (Datenschutzrelevante Umstellungen, Notfallpläne)	Bestimmte Geschäftsbereiche, Auftragsverarbeiter, Prozesse müssen auf den Prüfstand .
Die eigene Risikoeinschätzung (vorhandene Bedrohungen / Selbstreflektion)	„Wir sind zu klein um aufzufallen“ „Was gibt es bei uns schon zu holen“ „Bei uns passiert schon nichts“

Short Facts zur DSGVO / Was wenn doch was passiert?

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV

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

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!

(§ 42 BDSG neu)

eset ENJOY SAFER TECHNOLOGY™

Short Facts zur DSGVO / Kosten eines Datenschutzvorfalls

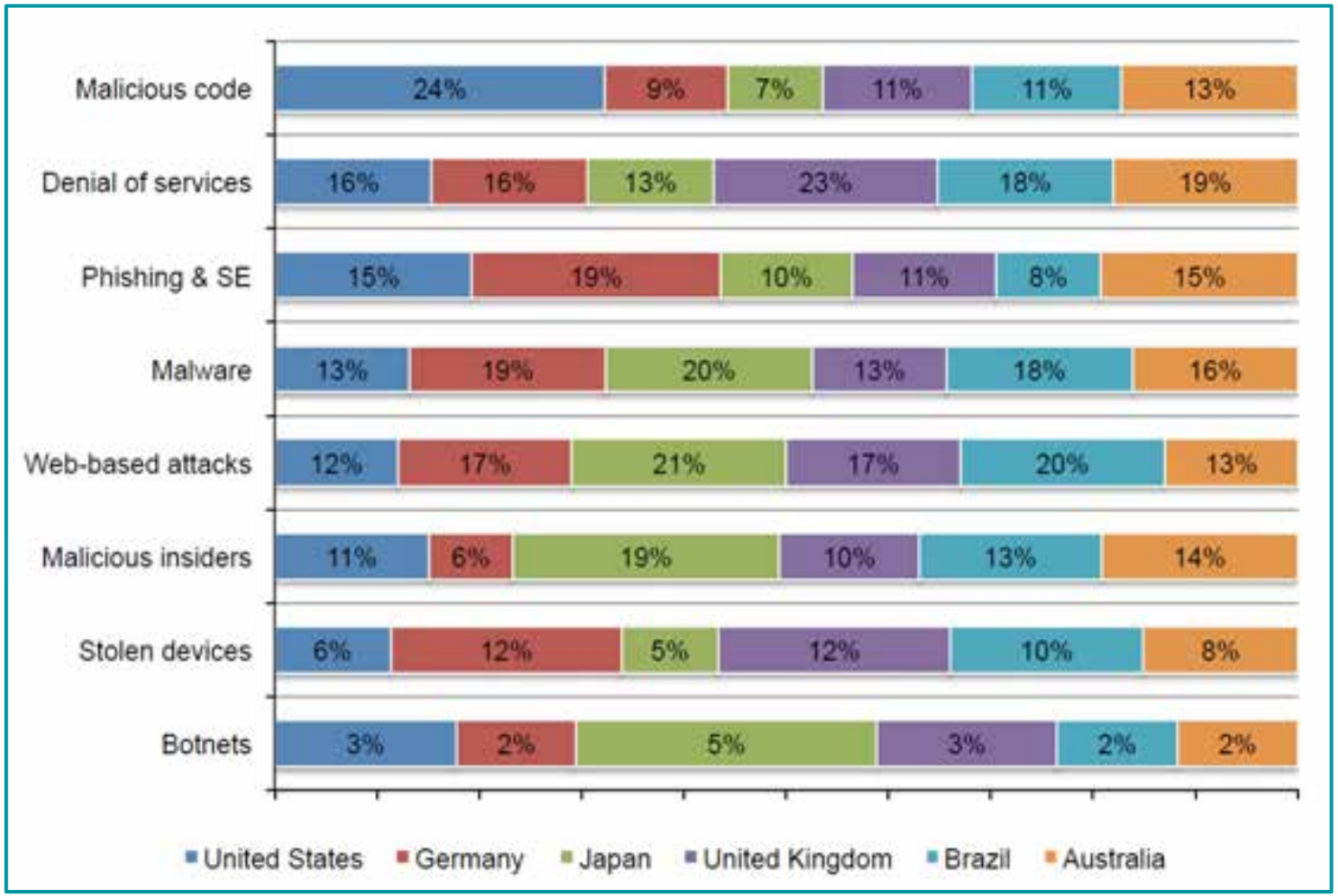
z.B. Aufwände für:

- Wiederherstellung der Systeme
- Wiederbeschaffung der Daten
- Erstellen einer Analyse
- Krisenmanagement intern
- PR Aufwand / Benachrichtigung
- ohne Bußgelder !

Ø Kosten pro Datensatz: 178,- EUR
(Ponemon's 2015 Cost of a Data Breach Study Germany $211)

Beispiele:

500 Kunden	= 89.000,- EUR
2.500 Kunden	= 445.000,- EUR
12.500 Kunden	= 2.225.000,- EUR



Percentage annualized cyber crime cost by attack type 2016 Cost of Cyber Crime Study & the Risk of Business Innovation, Ponemon Institute (October 2016)

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.de

IT-Sicherheit

Kollision von Anspruch und Realität

Die Realität der IT-Sicherheit?:

Welche IT-Security Lösungen haben Sie vollständig ausgerollt und unternehmensweit im Einsatz?

a.) Wir nutzten ein etabliertes AV/Malware-Produkt

b.) Wir nutzen neben einem AV/Malware-Produkt eine Firewall (Hardware- / Software)

c.) Wir haben neben den genannten weitere Lösungen im Einsatz (2FA/Encryption/Layer2 etc.)

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

Bundesamt für Sicherheit in der Informationstechnik

IT-Sicherheitsgesetz

eset ENJOY SAFER TECHNOLOGY™

Stand der Technik – Auszug aus dem IT-Sicherheitsgesetz

…aus der Handreichung „Stand der Technik im Sinne des IT-Sicherheitsgesetz“ TeleTrust Verband

3.2.1.5 Layer2-Encryption

Layer2-Verschlüsselung ist eine Sicherheitslösung, welche in bestimmten Anwendungsszenarien als Alternative zu Layer3-VPNs existiert. Sie wird statt auf IP-Pakete auf die Payload von Ethernet-Frames angewandt. Die IP-Header müssen nicht verarbeitet werden (Zeitgewinn) und es entsteht kein Verschlüsselungs-Overhead (Leitungsbandbreite steht voll zur Verfügung). Voraussetzung für den Einsatz ist ein Ethernet-basiertes Netzwerk (Punkt-zu-Punkt, Hub-Spoke oder vollvermascht) über eigene Kabel (Kupfer/Glasfaser) und sowie bei vermaschten Netzen WAN-Switches, oder von Netzwerkprovidern bereitgestellte Layer 2 Services (z.B. Carrier Ethernet-Dienste). Beim Einsatz dieser Netzwerk-Verschlüsselungstechnologie ist eine Änderung an der bestehenden Infrastruktur, insbesondere der IP-Routing-Konfiguration, nicht notwendig. Diese Art der Verschlüsselung ist für praktisch alle Netzwerk-Dienste und Anwendungen der OSI Schichten 3 und höher transparent und bringt keine Auswirkungen auf die Performance des Netzwerkes mit sich.

3.2.4.6 E-Mail-Verschlüsselung

Im E Mail-Verkehr sollte zur Transportverschlüsselung TLS (Transport Layer Security) in der aktuellen Version 1.2 (definiert in RFC 5246 [1]) oder alternativ ein verschlüsseltes VPN eingesetzt werden. Zum Einsatz kommen müssen sichere Verschlüsselungsverfahren (aktuell z.B. AES-256), die Verwendung unsicherer Verschlüsselungsverfahren (z.B. RC4) muss ausgeschlossen werden. Forward Secrecy sollte generell aktiviert werden. Zusätzlich ist es sinnvoll, die bei TLS genutzten Zertifikate der jeweiligen Gegenseite auf Authentizität und Gültigkeit zu überprüfen, z.B. mittels DANE (RFC 7671 [2]). Umfassende Empfehlungen zu TLS liefert die Technische Richtlinie TR-02102-2, Teil 2 des BSI [3].

Stand der Technik – Das IT-Sicherheitsgesetz

Das IT-Sicherheitsgesetz (ITSiG) dient als Orientierung für Betreiber kritischer Infrastrukturen (KRITIS Verordnung)

Versorgungsgröße >= 500.000 Personen, aus den Sektoren:

- Energie
- Informationstechnik
- Ernährung und Wasser

sowie kommende Sektoren:

- Gesundheit
- Finanz- und Versicherungswesen
- Transport und Verkehr

Lässt sich das für jeden adaptieren ?

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

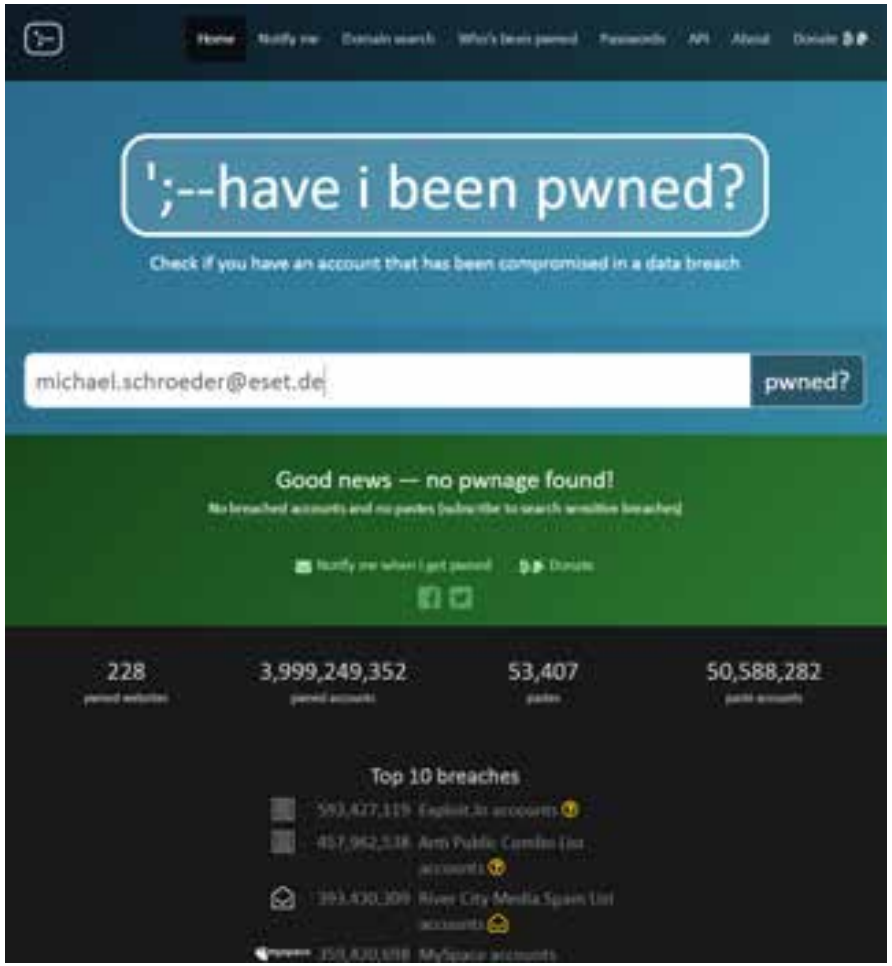
Problem Nummer 2: Unsere „Passworthygiene“

„… 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 4 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

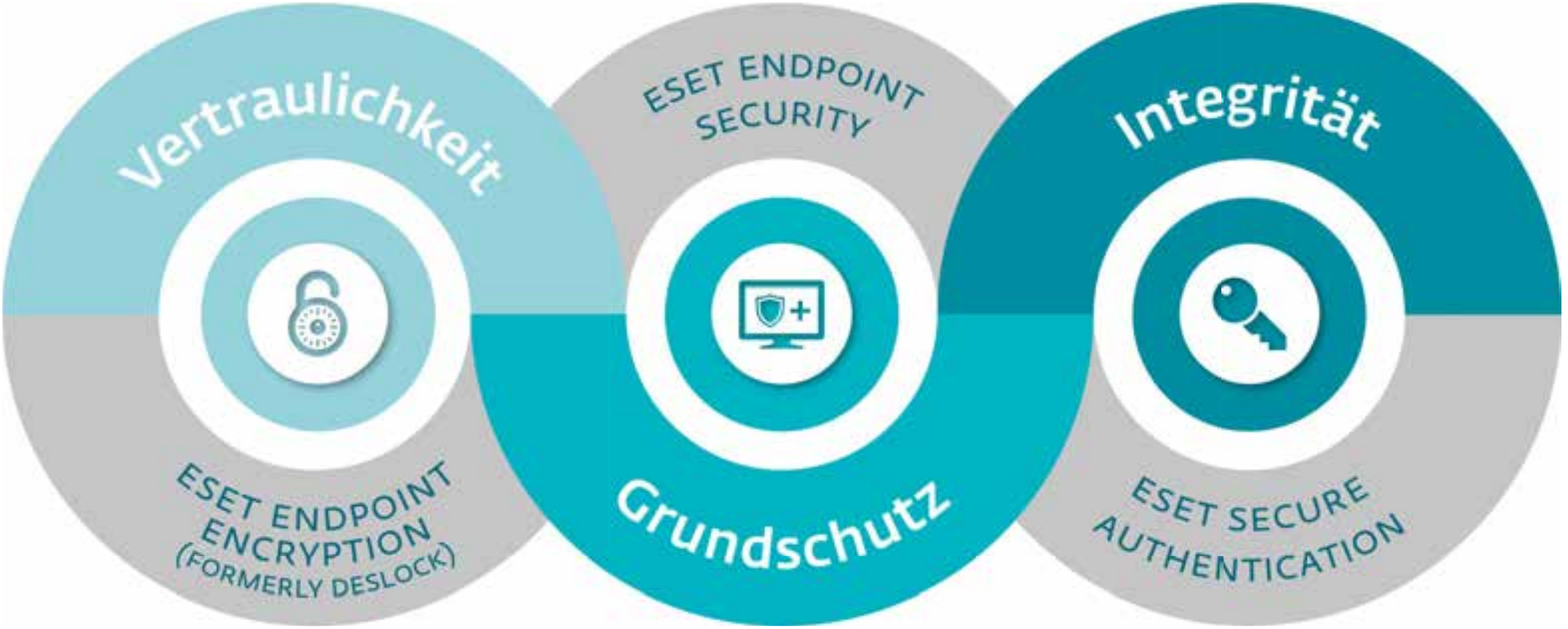
Problem Nummer 3: Mein Feind, das Gerät

- 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!

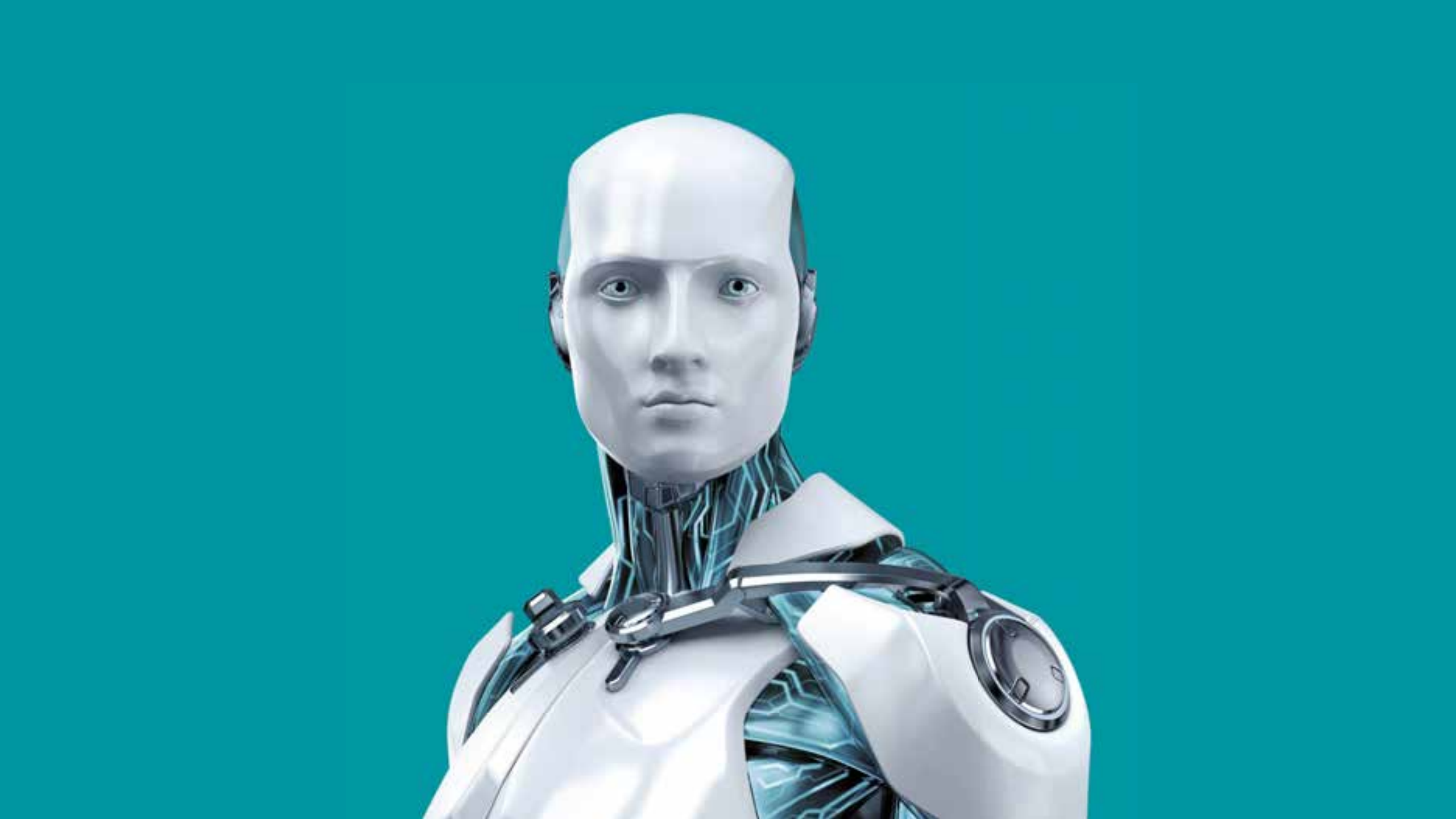
Eliminiert das Risiko „unsicherer“ Passwörter für immer, ohne Ihre Mitarbeiter einzuschränken!

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

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

eset ENJOY SAFER TECHNOLOGY™

Fragen?



Michael Schröder

Business Development Manager
New Technologies

ESET Deutschland GmbH | info@eset.de | www.eset.de