Schutzziele der DSGVO.

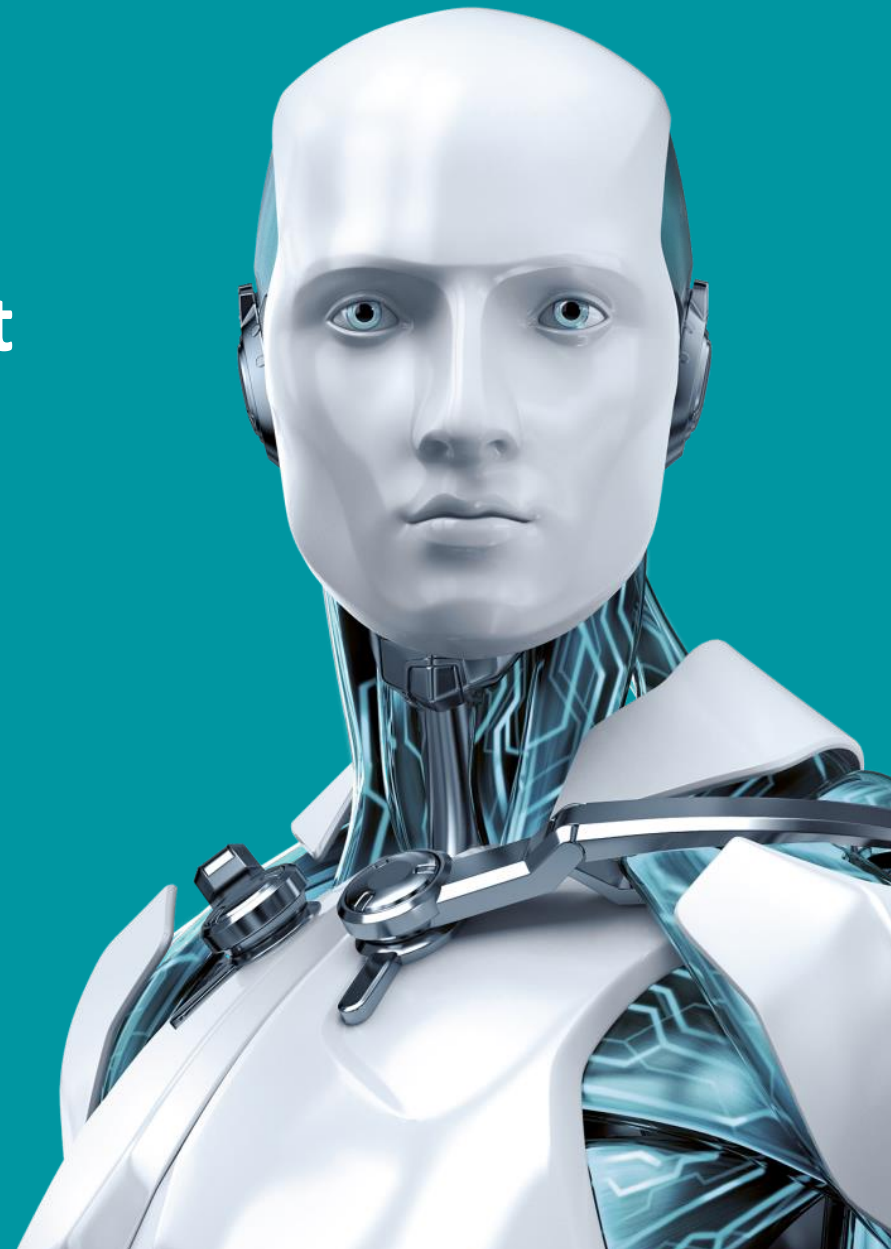
Datenschutz ist keine Raketenwissenschaft

Alexander Schulz

Territory Market Manager

30 YEARS OF CONTINUOUS IT SECURITY INNOVATION

ENJOY SAFER TECHNOLOGY™



Die EU-Datenschutzgrundverordnung ist keine Raketenwissenschaft

Sie bringt aber IT- und Datenschutz in neue Sphären

Schutzziele der DSGVO

Agenda

- Fakten zur DSGVO
  Einstieg in die Welt der personenbezogenen Daten
- Schutzziele der DSGVO
  Schutzziele, Schutzmaßnahmen und Fallbeispiele
- IT-Sicherheit
  Kollision von Anspruch und Realität - Von der Anforderung zum Lösungsansatz „Risikominimierung“
- Risikominimierung
  Umsetzbare Szenarien, Lückenschluss zwischen realen Problemen und den technischen Lösungen
- Technische Lösungen
  Die 3 Bausteine der IT-Sicherheit

Eine Frage der Selbsteinschätzung

Werden die aktuellen (BDSG) und kommenden (DSGVO/BDSG (neu) 2017) Datenschutzbestimmungen in Ihrer Organisation eingehalten?

a.) Wir sind vollumfänglich konform zum aktuellen 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, wir haben uns vor dieser Veranstaltung mit dem Thema nicht aktiv auseinandergesetzt.

Fakten zur DSGVO

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

ENJOY SAFER TECHNOLOGY™

Fakten zur DSGVO - Eckdaten

- Das bisherige BDSG wird durch die neue Regelung ersetzt (BDSG (neu) 2017)
- Es gibt keine Übergangsfristen (Fallbeileffekt)
- Branche / Betriebsgröße / behördliche Zuordnung spielt keine Rolle
- Bußgeldstufe 1: bis 10 Mio. Euro oder 2% des weltweiten Jahresumsatzes
- Bußgeldstufe 2: bis 20 Mio. Euro oder 4% des weltweiten Jahresumsatzes

- Die Bußgelder sollen wortwörtlich „abschreckend“ sein
- Erhobene Bußgelder verbleiben bei der ausstellenden Aufsichtsbehörde
- Unternehmen / Behörden werden „rechenschaftspflichtig“

Fakten zur DSGVO - Personenbezogene Daten

Schwarz = Offensichtlich

Blau = weniger offensichtlich

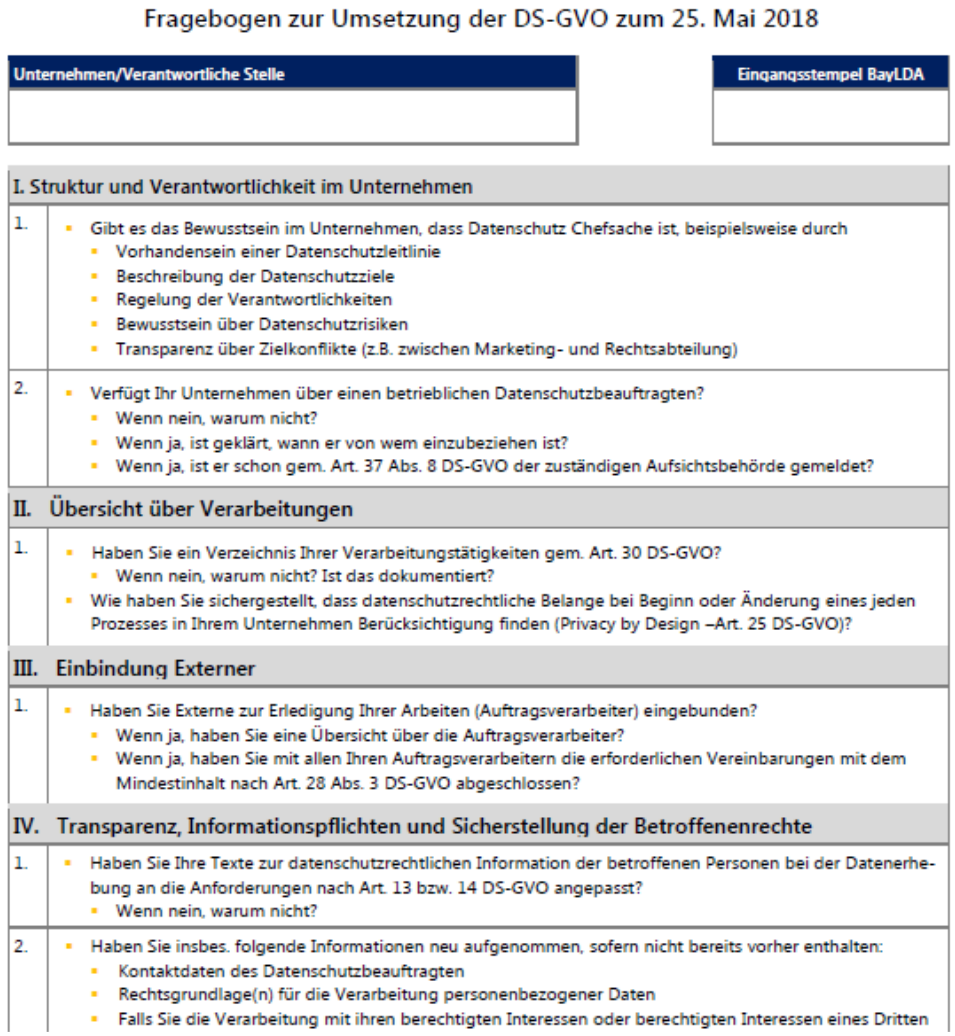
Orange = besondere Kategorien (Artikel 9) oder kritisch

Fakten 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.

Fakten 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

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

Fakten 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“.

Fakten zur DSGVO - Wenn doch etwas passiert?

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV 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

DPA

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 und 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) 2017)

Fakten zur DSGVO - Datenschutzvorfall-Kosten

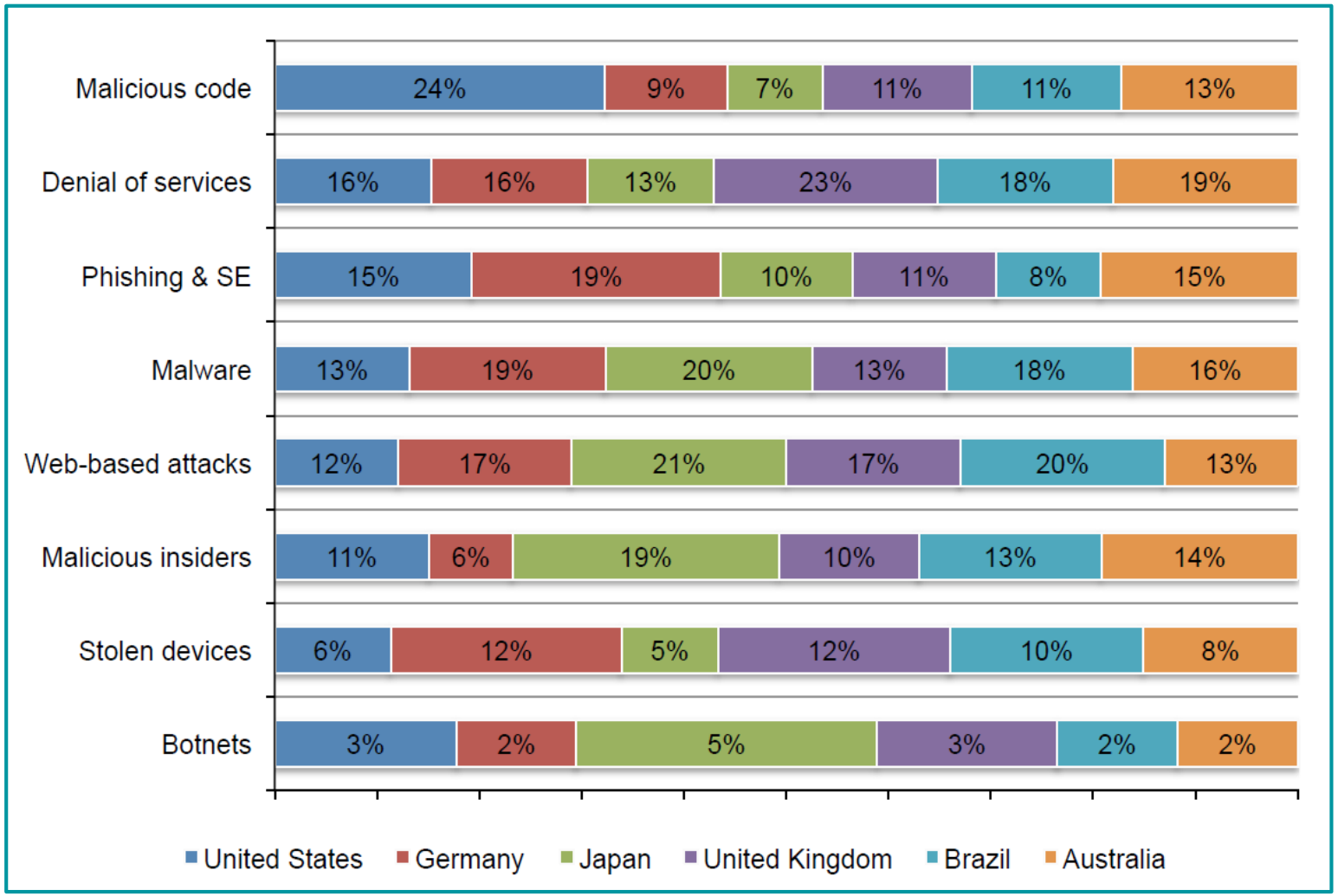
Aufwände für:

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

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

Beispiele:

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



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
(Artikel 32 Absatz 1b oder § 64 BDSG (neu) 2017)

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 und 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 / Device-Control

IT-Sicherheit

Kollision von Anspruch und Realität

Die Realität der IT-Sicherheit?

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

a.) Wir nutzten ein etabliertes Anti-Virus/Anti-Malware-Produkt.

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

c.) Wir haben neben den genannten auch weitere Lösungen im Einsatz (Verschlüsselung/2FA/Layer 2/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."

(Artikel 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

Stand der Technik - Auszug aus dem IT-Sicherheitsgesetz

… aus der Handreichung „Stand der Technik im Sinne des IT-Sicherheitsgesetzes“ (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 dies 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“

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.

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!

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 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 +

channelXport

HOME > TELEKOMMUNIKATION

Der Countdown läuft

Wann wird Ihr Passwort gestohlen?

09.08.2017 Autor: Dr. Amir Alsbih / 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 Geschickte eines US-

Anzeige

CATCH THE HEAT

PREMIUMANBIETER ZUM THEMA

ESET Deutschland GmbH

baramundi software AG

Axis Communications GmbH

Nexus Technology GmbH

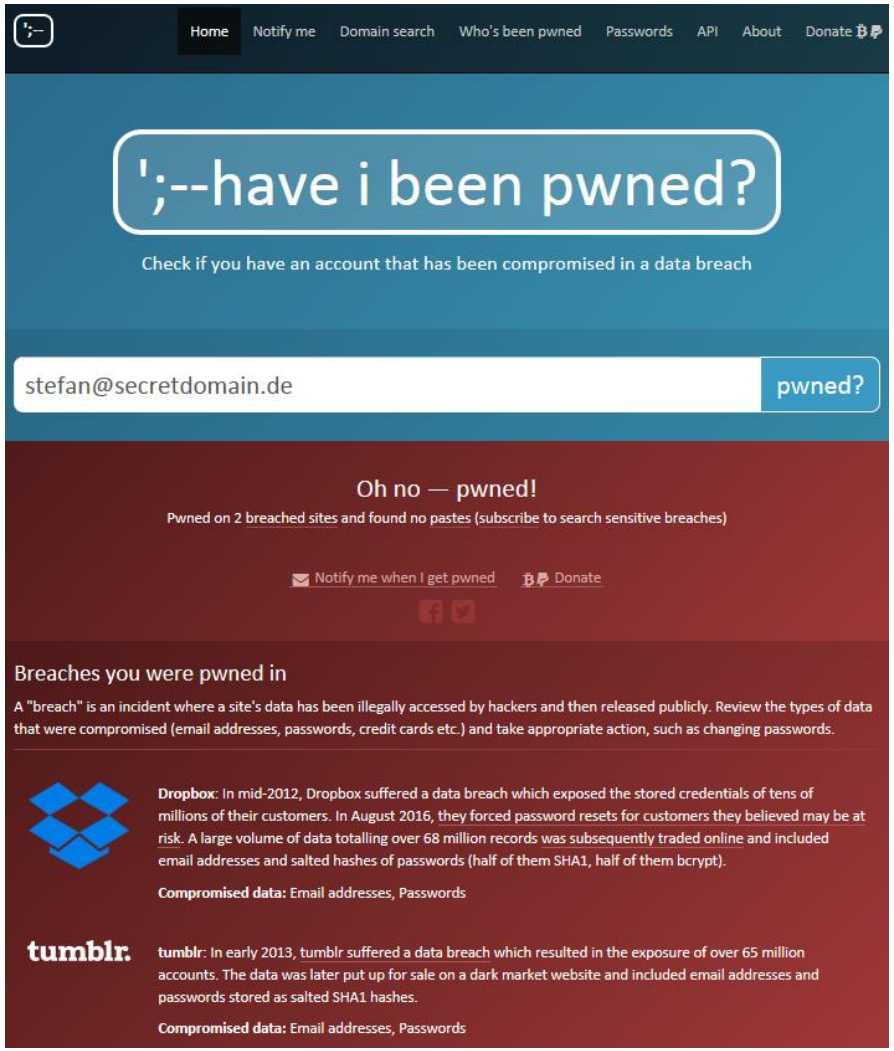
LESERWAHL ITK-PRODUKTE DES JAHRES 2017

„… 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.“

„Transaktionssicherheit lässt sich vergleichsweise schnell und einfach durch eine risikobasierte Zwei-Faktor-Authentifizierung (2FA) 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

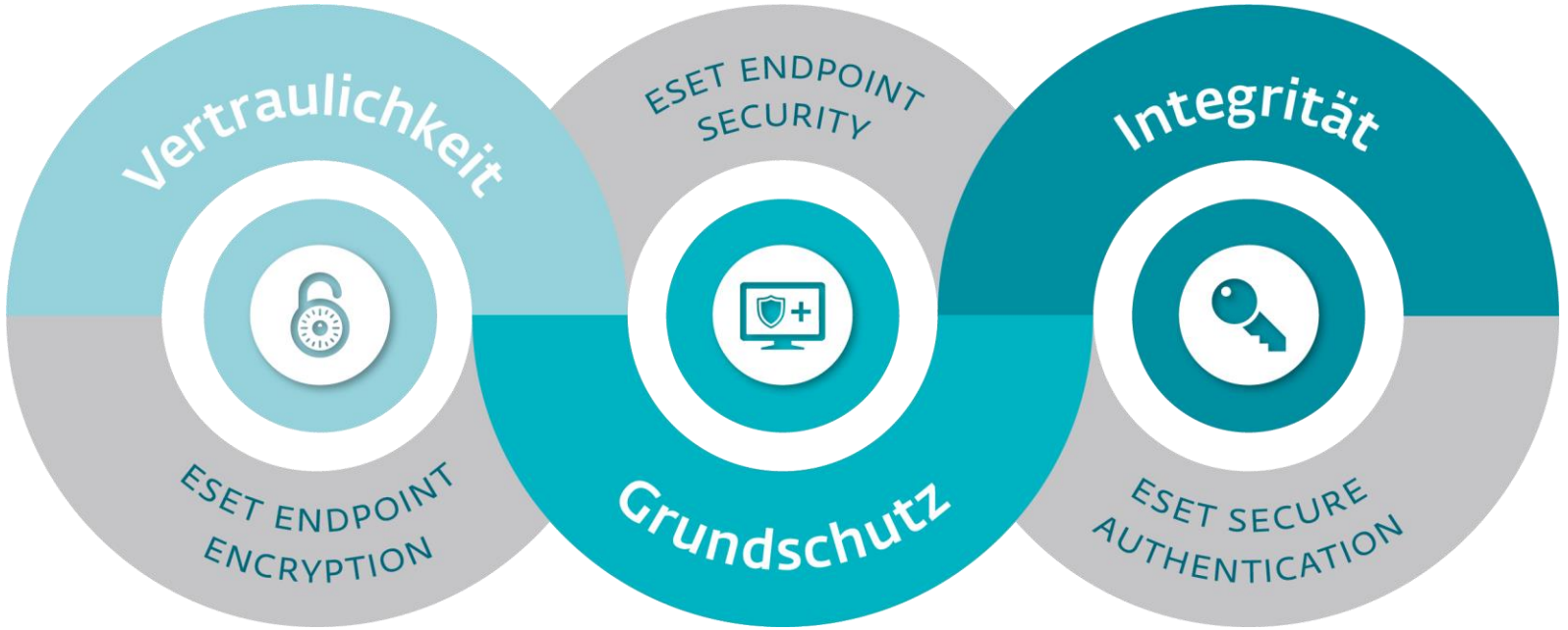
Problem Nummer 3 - Mein Feind, das Gerät

- 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



1.
Ohne Grundschutz keine Sicherheit

2.
Vertraulichkeit durch Verschlüsselung

3.
Integrität durch sicheren Systemzugriff

Ohne Grundschutz keine Sicherheit

ESET Endpoint Security kann mehr als nur Anti-Virus!

Alles im Griff!

Zentrales Management (ERA) für ESET Produkte auf Enterprise Level inkl. Lizenzmanagement. Einfacher Rollout. Auch über MS Azure oder aus der Cloud.

Sicher? Aber logisch!

Analysiert Datenverkehr im Netzwerk, erkennt verdeckte und unbekannte Ransom- und Malware, findet verdächtige Prozesse im Speicher und überwacht permanent Systemdateien (HIPS).

Darf hier eigentlich jeder alles?

Schützt z.B. USB Schnittstellen über Device-Regeln. Benutzer-Schutz durch Steuerung, welche Webseiten/Services genutzt werden dürfen (White-/Black-Listing).

Vertraulichkeit durch Verschlüsselung

ESET Endpoint Encryption (bisher DESlock+) bietet perfekte Alltagstauglichkeit und einzigartiges Remote Management

Zertifiziert und Patentiert!

Durchdachte Schlüssel-Logik und weltweit einzigartiges Remote-Management. Mehrfach patentiert und unabhängig zertifiziert (z.B. FIPS 140-2).

Sicherheit & Kontrolle - überall!

Der Enterprise Server benötigt keine Zertifikate, keine offenen Ports und keine eingehenden Verbindungen. Externe Geräte bleiben jederzeit unter Kontrolle - auch über 3G oder öffentliches WLAN. Regeln sind jederzeit und überall aktiv.

Ein Produkt, viele Lösungen!

Festplattenverschlüsselung, Verschlüsselung von Ordnern, Dateien, Mails, Dokumenten oder externer Medien (USB). Multi-User-Szenarien (Geräte und Daten) und die Kommunikation mit „Externen“ jederzeit möglich!

Integrität beginnt mit dem Systemzugriff

ESET Secure Authentication sichert mehr als nur VPN-Zugänge ab!

Einfach und effektiv!

ESA lässt sich in nur 10 Minuten installieren und integriert sich in vorhandene AD-Strukturen. Das zentrale Management erlaubt die Provisionierung der Geräte innerhalb kürzester Zeit.

Effizienz, auch bei den Kosten!

Keine teuren Hardware-Tokens notwendig. Nutzung vorhandener mobiler Infrastruktur. Vom Smartphone bis zum SMS-fähigen Mobilgerät - die ESA App unterstützt eine Vielzahl von Geräten - auch private Geräte der Benutzer.

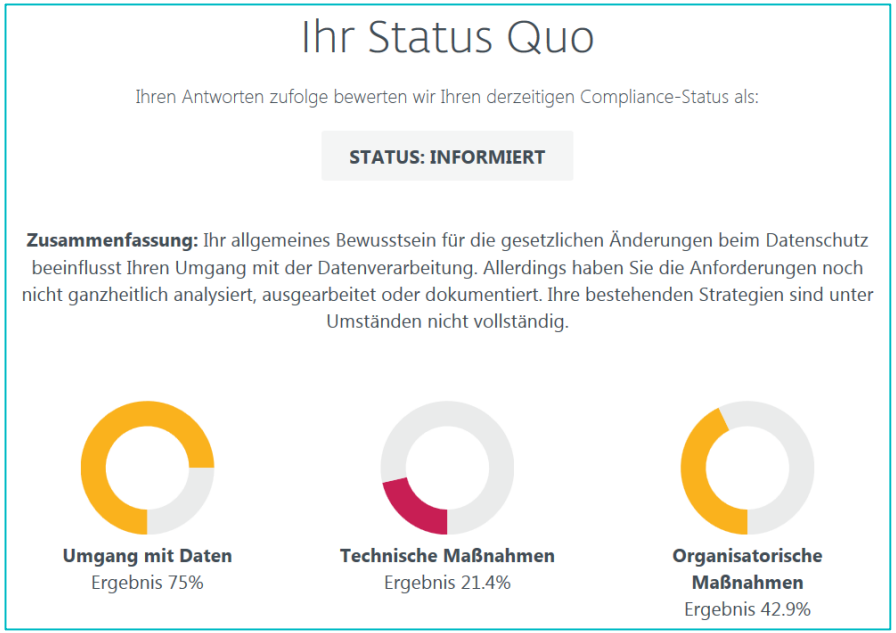
Flexibilität schafft Akzeptanz!

Schützt neben Desktop-Logins auch Cloud-Dienste (ADFS 3.0) und alle externen Zugänge (Radius).
Auswahl der gewünschten Methode z.B. „Push-Authentification“ und 2FA-Nutzung auch „offline“ (z.B. im Flugzeug).

DSGVO - Unser Engagement für Sie

Das ESET-DSGVO-Portal: https://dsgvo.eset.de

- Compliance-Check



- Quick Guide und Leitfaden

ENJOY SAFER TECHNOLOGY™

Q&A!?