

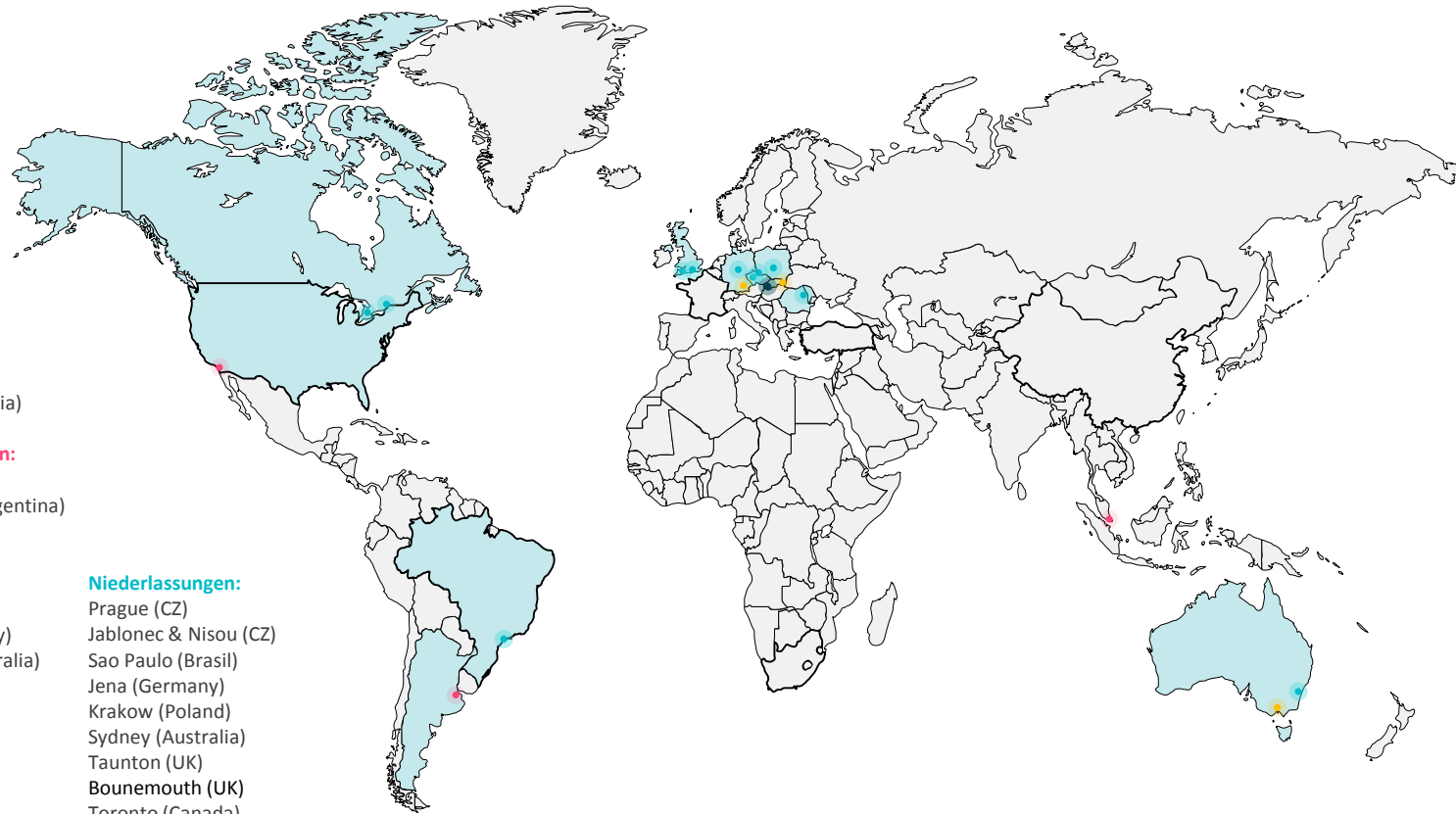


ENJOY SAFER
TECHNOLOGY™

**Die neue EU DSGVO
als Motor für Ihr Geschäft!**



ESET – Weltweit für Sie da, seit 1987!



HQ :
Bratislava (Slovakia)

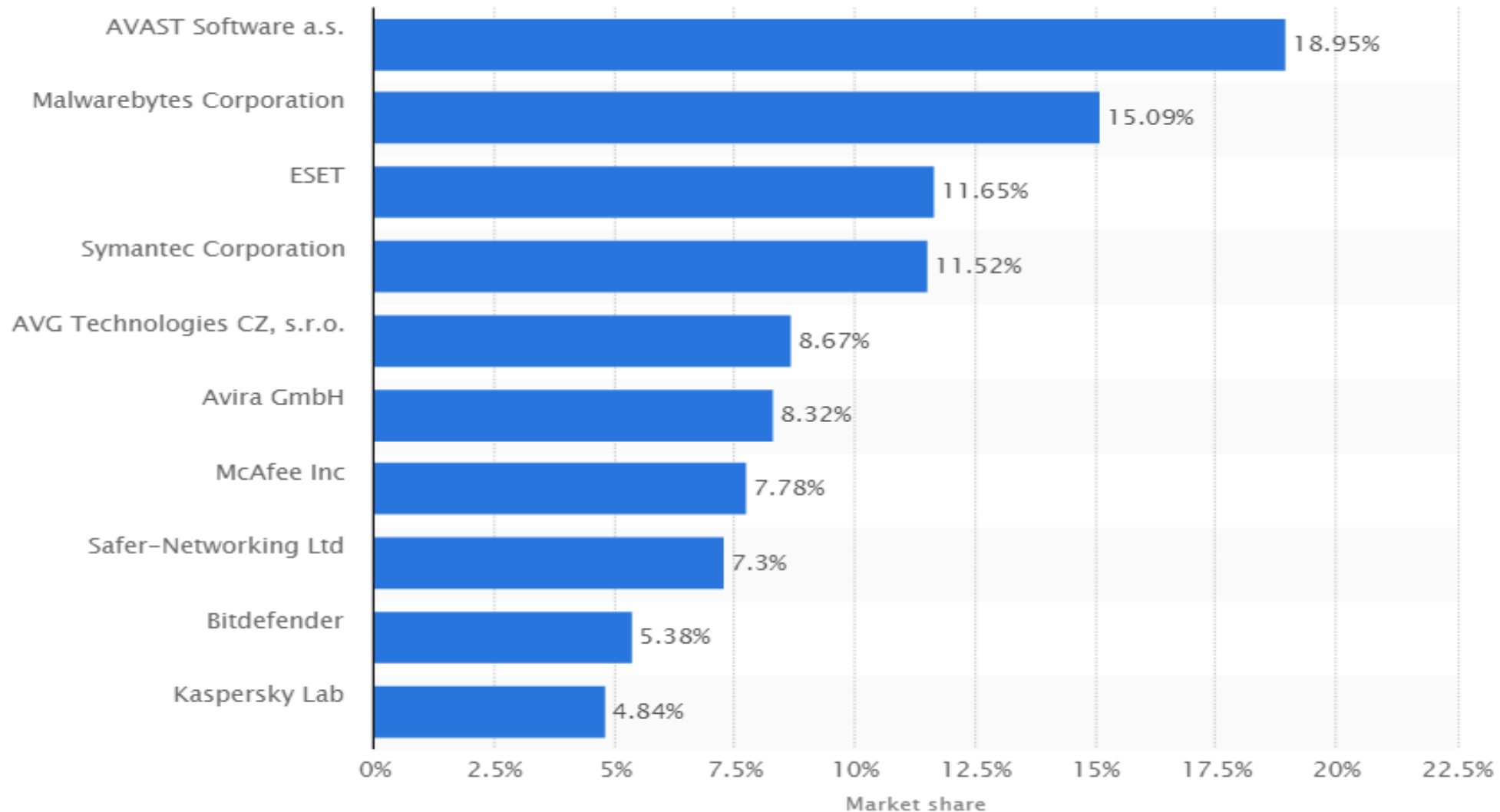
Regionale Zentren:
San Diego (US)
Buenos Aires (Argentina)
Singapore

Lokale Büros:
Kosice (Slovakia)
Munich (Germany)
Melbourne (Australia)

Niederlassungen:
Prague (CZ)
Jablonec & Nisou (CZ)
Sao Paulo (Brasil)
Jena (Germany)
Krakow (Poland)
Sydney (Australia)
Taunton (UK)
Bournemouth (UK)
Toronto (Canada)
Montreal (Canada)
Iasi (Romania)

- 14 Niederlassungen
- 24/7 Cyber Intelligence
- 25 Produkte
- 201 Länder
- 234 Distributoren
- über 120 Millionen Anwender
- **Made in Europe**
- VB100 Test- Rekord
11 Jahre in Folge

Global Market Share (Windows OS)



ESET Kunden weltweit



DSGVO – Short Facts / Was Sie wissen müssen!

EU-DSGVO (eng. GDPR) – Deadline 25.05.2018!

Eine Richtlinie (EU 1995) wird zur Verordnung!



28 Interpretations of the Data Protection **Directive**



One Data Protection **Regulation**
Harmonized across all EU member states

Etwa **4,4 Millionen** Unternehmen allein in **D/A/CH** müssen sich mit diesem Thema befassen!

DSGVO – Short Facts / Eckdaten und Fakten

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

- Es gibt **RECHENSCHAFTSPFLICHT: Art. 5 Abs.**

- Ihre B **2 DSGVO**

- Bußg Unternehmen müssen dokumentieren, was sie zur Einhaltung der Vorgaben der DSGVO tun. Und dies müssen sie auch beweisen können.
- Bußg
- Die B
- Erhok
- Unter

05.2018



DSGVO – Short Facts / Geltungs- und Anwendungsbereich?

Es geht also um **die Erhebung, Verarbeitung und Nutzung personenbezogener Daten** von **natürlichen Personen** (außerhalb familiären-, behördlich präventiven- und repressiven Zwecken) **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....

25.05.2018



DSGVO – die wesentlichen Änderungen

- Recht auf **mehr Transparenz** (Proaktive Kommunikation mit dem Kunden bei Erhebung und Änderung - WAS, WOZU, WIE LANGE?)
 - Recht auf
 - Recht auf
 - Recht auf
 - Recht auf
 - **Schutz vor**
 - **Meldepflicht**
 - Umfangre
 - Und erst
- In der neuen DSGVO wird Unternehmen künftig in Art. 30 DSGVO das Führen eines **Verzeichnisses aller Verarbeitungstätigkeiten** vorgeschrieben. Es müssen weiter die wesentlichen Informationen der Datenverarbeitung zusammengefasst werden, also Angaben zu Zweck der Verarbeitung, Löschfristen und Empfänger.



DSGVO – die Anforderungen

Technische und Organisatorische Maßnahmen, ein Auszug (Artikel 32):

- „..Verschlüsselung personenbezogener Daten“
- „..Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste... auf Dauer sicherzustellen.“
- „..die Verfügbarkeit .. von Daten und Zugang .. bei einem physischen und technischem Zwischenfall rasch wiederherzustellen.“

Kurz, **Sie benötigen** in jedem Fall ein **validiertes Verschlüsselungsprodukt**, dass Sie auch im Falle von Diebstahl oder Verlust von Daten schützt ... aber es gibt noch einige Hausaufgaben..



DSGVO – sind Sie vorbereitet?

Womit Sie jetzt beginnen sollten:

- Ihre Systeme analysieren
- Ihre Prozesse und Strategien überarbeiten
- Mitarbeiter schulen/sensibilisieren (Handbücher umschreiben)
- Ihre Systemlandschaft aktualisieren
- Sofern nicht vorhanden, eine Verschlüsselungstechnologie einführen!

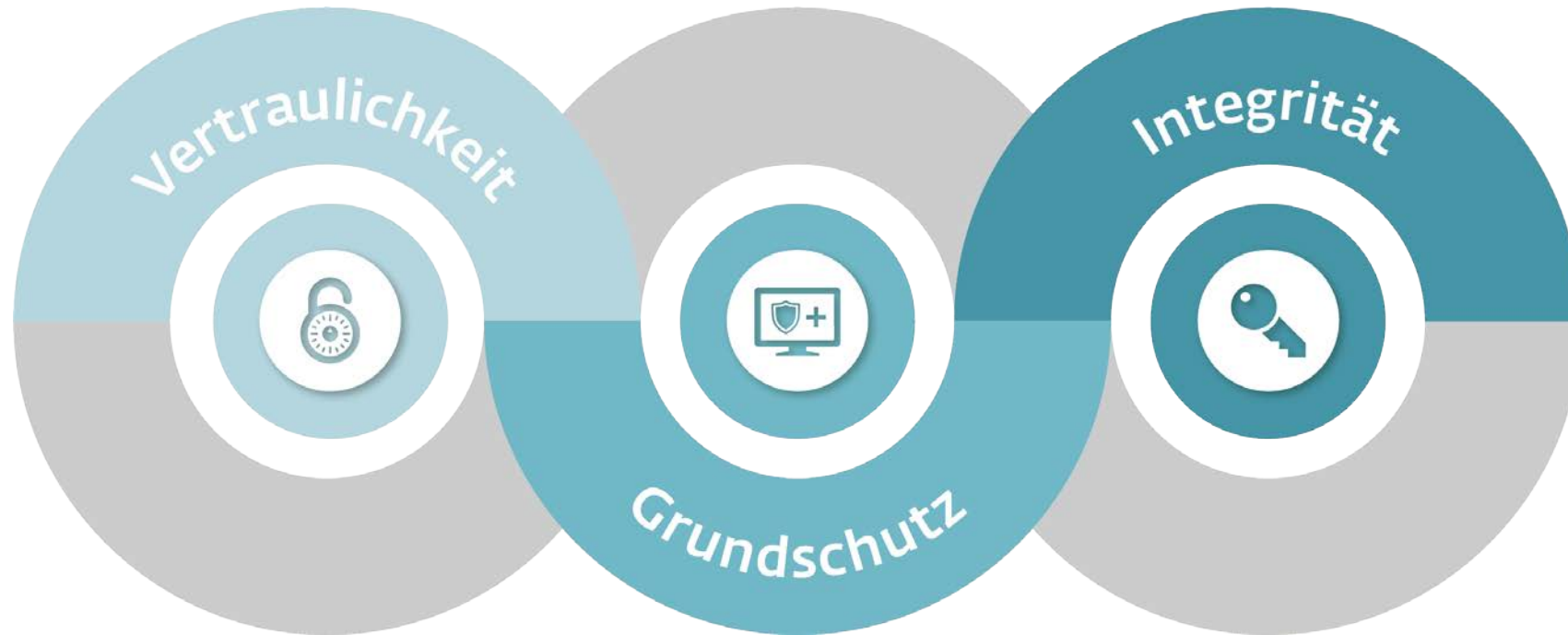
Neben guter Organisation ist aber auch eine überlegte Beschaffungspolitik angebracht...



Datensicherheit, Integrität, Vertraulichkeit (Artikel 5, Abs 1f)

Die 3 Bausteine der IT Sicherheit

Die 3 Bausteine der IT Sicherheit



1.
Vertraulichkeit
durch Verschlüsselung!

2.
Ohne Grundschutz
keine Sicherheit

3.
Integrität durch
sicheren Systemzugriff

1. Vertraulichkeit durch Verschlüsselung!



DESlock bietet perfekte Alltagstauglichkeit und einzigartiges Remote Management

Zertifiziert und Patentiert!

Sowohl unsere kinderleichte Schlüssel-Logik als auch unser weltweit einzigartiges Remote Management sind mehrfach patentiert und unabhängig zertifiziert (z.B. FIPS 140-2).

Sicherheit & Kontrolle, überall!

Unser Enterprise Server benötigt kein Zertifikate, keine offenen Ports und keine eingehenden Verbindungen. Dennoch bleiben Ihre externen Geräte jederzeit unter Kontrolle, auch über 3G oder öffentliches W-LAN. Ihre Regeln jederzeit aktiv, überall.

Ein Produkt, viele Lösungen!

Ob Festplattenverschlüsselung, Verschlüsselung von Ordnern, Dateien, Mails, Dokumenten oder externer Medien (USB), alles ist mit DESlock möglich. Dabei bleiben Ihre Multi-User-Szenarien (Geräte und Daten) aber auch die Kommunikation mit „Externen“ möglich!

2. Ohne Grundschutz keine Sicherheit!



Unsere Endpoint Security kann mehr als nur Anti-Virus!

Alles im Griff!

Ein zentrales Management (ERA) für ESET Produkte auf Enterprise Level inkl. Lizenzmanagement. Einfacher Rollout, vielfältige RMM Plugins. Gern auch über MS Azure oder aus der Cloud.

Sicher?, aber logisch!

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

Darf hier eigentlich jeder alles?

Schützt z.B. Ihre USB Schnittstellen über Device-Regeln. Steuern Sie aktiv welche Webseiten/Services genutzt werden dürfen (beides über White-/Black-Listing) und schützen Sie sich und Ihre User.



3. Integrität beginnt mit dem Systemzugriff!

„Unsere Logins sind durch komplexe und ausreichend lange Passwörter geschützt“

„Außerdem muss das Passwort alle 90 Tage geändert werden!“

... aber macht das Ihre Passwörter wirklich sicherer?

61%* der Nutzer verwenden identische Passwörter mehrfach, auch im Netz!

76%* aller Einbrüche basieren auf schwachen oder gestohlenen Passwörtern!

... und JA, 50%* der Nutzer tauschen Ihr Passwort gegen Schokolade!

3. Integrität beginnt mit dem Systemzugriff!



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

Einfach und effektiv!

ESA lässt sich in nur 10 Minuten installieren und integriert sich nahtlos in Ihre vorhandene AD Struktur. Die zentrale Management Console (MMC snap-in) erlaubt die Provisionierung Ihrer Geräte innerhalb kürzester Zeit.

Effizienz, auch bei den Kosten!

Wir benötigen keine teuren Hardware-Tokens, sondern nutzen vorhandene mobile Infrastruktur. Vom Smartphone bis zum SMS-fähigen Mobilgerät, unsere APP unterstützt jedes Ihnen bekannte Betriebssystem, auch private Geräte der Nutzer.

Flexibilität schafft Akzeptanz!

Schützen Sie neben Desktop Logins auch Ihre Cloud-Dienste (ADFS 3.0) und alle externen Zugänge (Radius). Sie wählen die gewünschte Methode z.B. „Push-Authentication“ und können mit uns 2FA auch dann nutzen, wenn Sie „Offline“ sind (z.B. im Flugzeug)

Fragen?

Besuchen Sie uns an unserem Stand



ENJOY SAFER TECHNOLOGY™