Digitale Souveränität

>>NIS 2, Cybersicherheitsstandards und Cyberversicherungen in der Praxis<<

Thorsten Urbanski

Director of Marketing und
Leiter der TeleTrust Arbeitsgruppe IT Security made in EU

INTERNATIONAL CENTERS
BRATISLAVA (HQ)
SAN DIEGO
BUENOS AIRES
SINGAPORE

OFFICES
PRAGUE
JENA (DACH HQ)
MUNICH
BOURNEMOUTH
MILAN
TORONTO
MEXICO CITY
SAO PAULO
SYDNEY
MELBOURNE
TOKYO

RESEARCH AND DEVELOPMENT CENTERS
BRATISLAVA
KOSICE
ZILINA
PRAGUE
BRNO
JABLONEC NAD NISOU
KRAKOW
IAȘI
TAUNTON
MONTREAL
BUENOS AIRES
SINGAPORE

NR. 1 IN DER EU

35+ JAHRE CYBERSECURITY

MITARBEITENDE

2200+

NIEDERLASSUNGEN

23

FORSCHUNGS- & ENTWICKLUNGS- ZENTREN

12

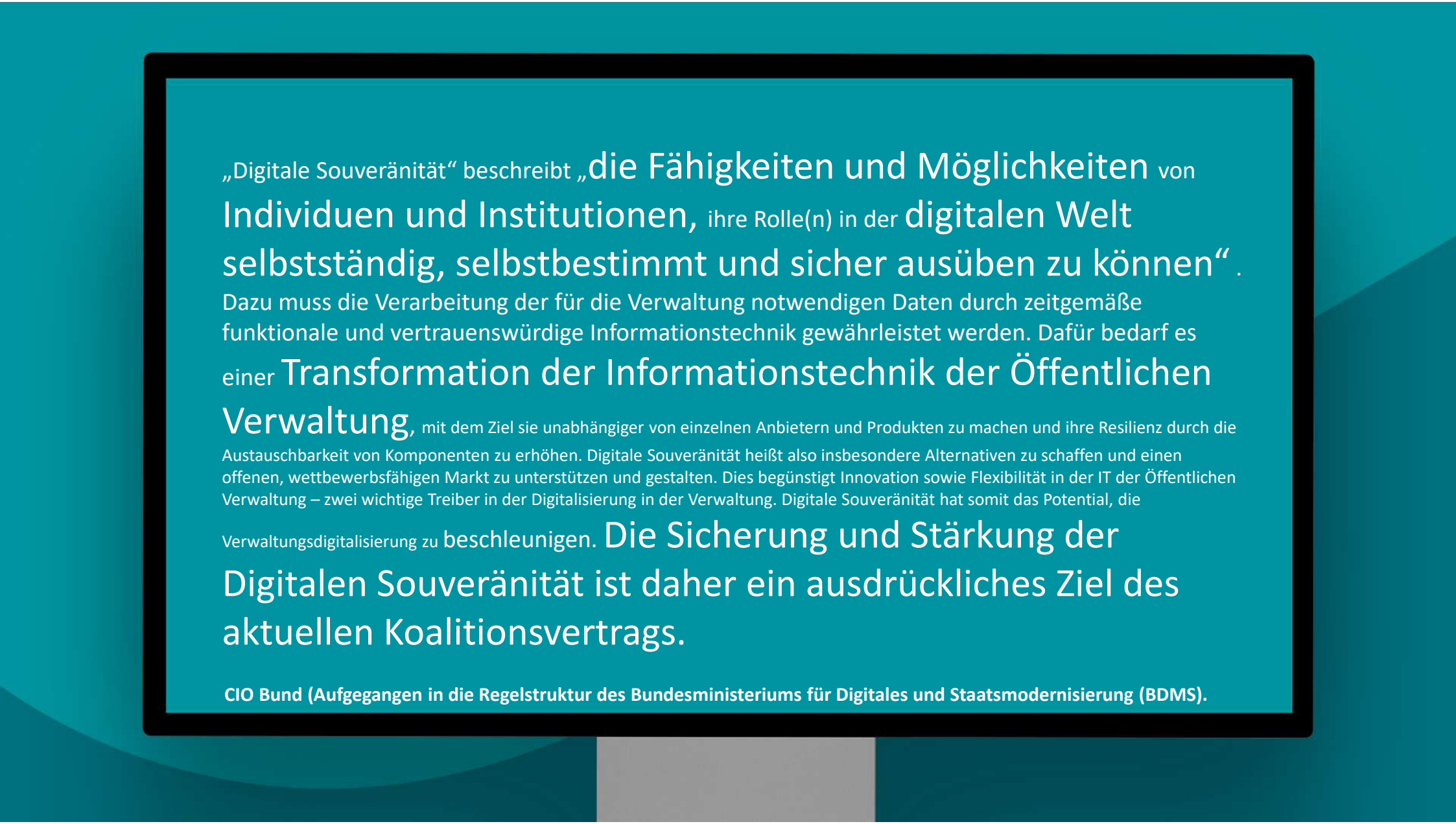
“

Deutschen Unternehmen ist durch Sabotage, Spionage und Datendiebstahl ein jährlicher Schaden von 267 Milliarden Euro entstanden

Bitkom-Wirtschaftsstudie 2024

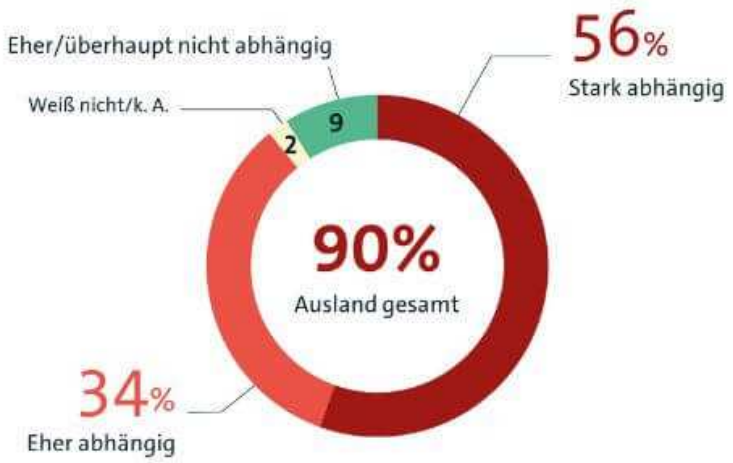
Digitale Souveränität?

Digital Security
Progress. Protected.


„Digitale Souveränität“ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“.
Dazu muss die Verarbeitung der für die Verwaltung notwendigen Daten durch zeitgemäße funktionale und vertrauenswürdige Informationstechnik gewährleistet werden. Dafür bedarf es einer Transformation der Informationstechnik der Öffentlichen Verwaltung, mit dem Ziel sie unabhängiger von einzelnen Anbietern und Produkten zu machen und ihre Resilienz durch die Austauschbarkeit von Komponenten zu erhöhen. Digitale Souveränität heißt also insbesondere Alternativen zu schaffen und einen offenen, wettbewerbsfähigen Markt zu unterstützen und gestalten. Dies begünstigt Innovation sowie Flexibilität in der IT der Öffentlichen Verwaltung – zwei wichtige Treiber in der Digitalisierung in der Verwaltung. Digitale Souveränität hat somit das Potential, die Verwaltungsdigitalisierung zu beschleunigen. Die Sicherung und Stärkung der Digitalen Souveränität ist daher ein ausdrückliches Ziel des aktuellen Koalitionsvertrags.
CIO Bund (Aufgegangen in die Regelstruktur des Bundesministeriums für Digitales und Staatsmodernisierung (BDMS).

Hohe Abhängigkeit von den USA und China

Wie stark ist Ihr Unternehmen abhängig vom Import digitaler Technologien und Leistungen aus anderen Ländern?



USA

41%
Stark abhängig

40%
Eher abhängig

China

44%
Stark abhängig

35%
Eher abhängig

Basis: Unternehmen, die digitale Technologien bzw. Leistungen aus dem Ausland beziehen (n=526) | Abweichungen von 100 Prozent sind rundungsbedingt |
Quelle: Bitkom Research 2025

bitkom

Quelle: Bitkom

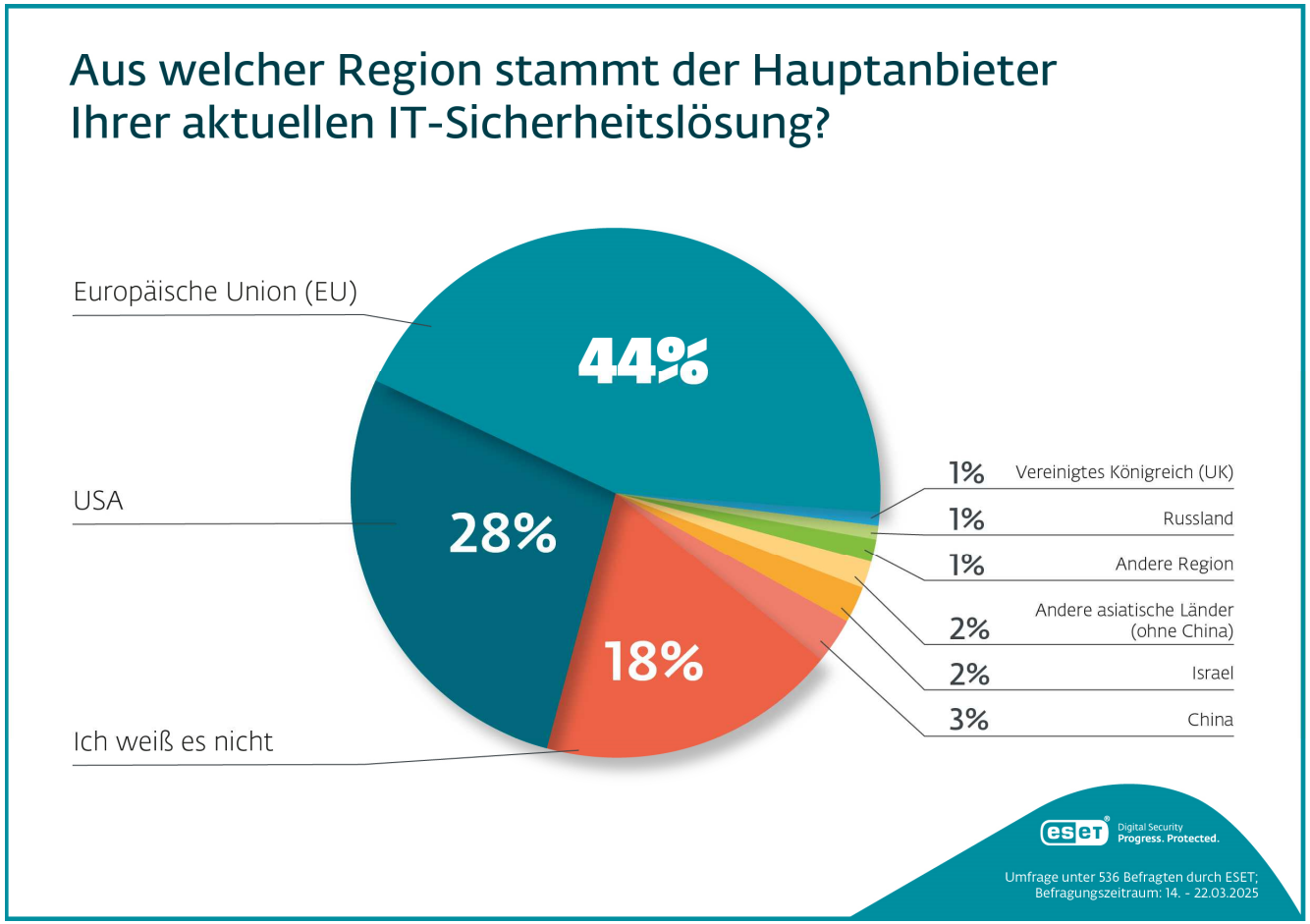
Digitale Zeitenwende?

Datenschutz „Made in EU“ ist Pflicht und keine Kür

ESET Digital Security
Progress. Protected.


IT-Security
„Made in EU“
Digital Security
Progress. Protected.

Herkunft des Herstellers

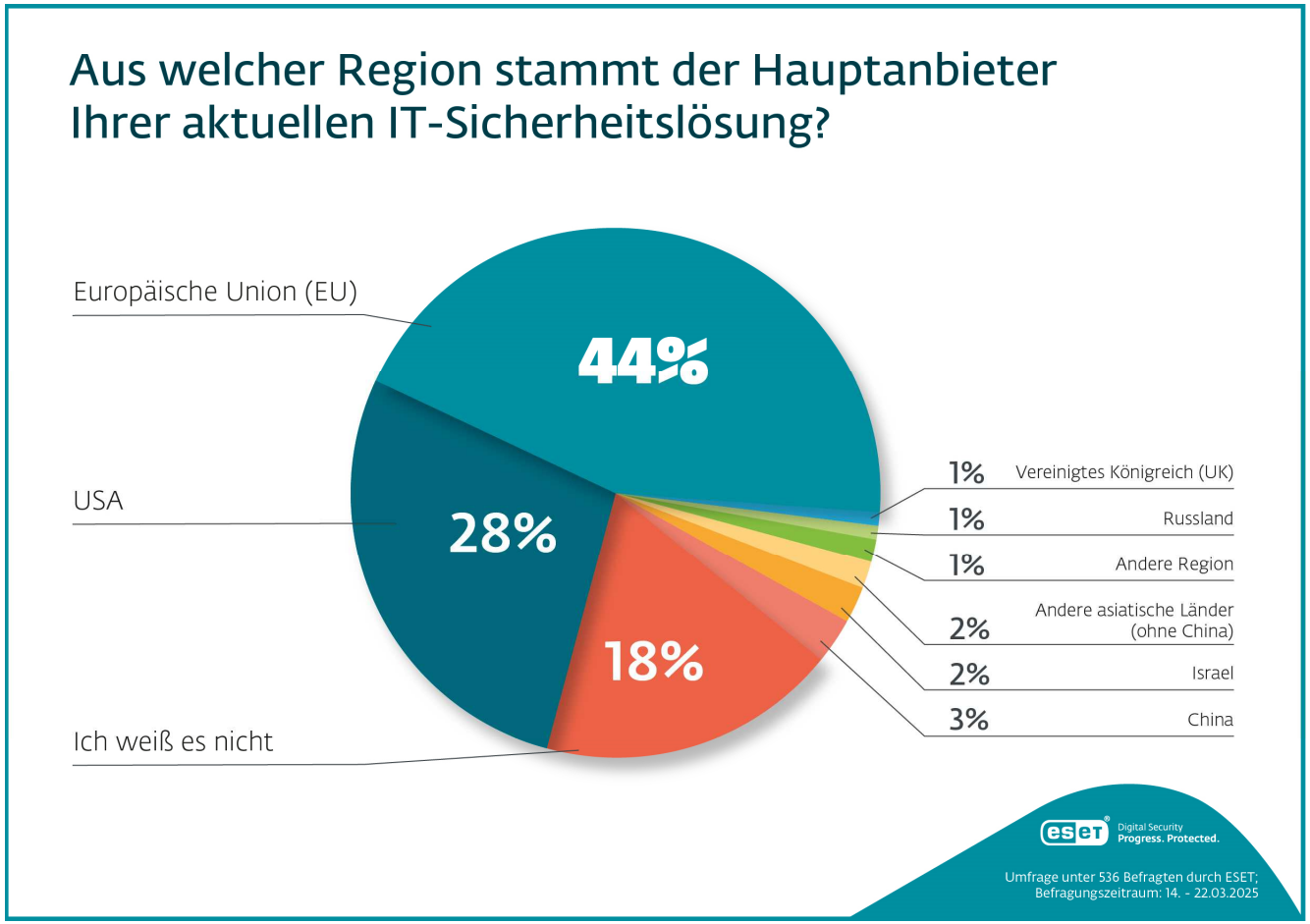


Bereits knapp

jeder Zweite

verwendet in seinem Unternehmen eine IT-Sicherheitslösung aus der europäischen Union, gefolgt von den USA mit 28 Prozent.

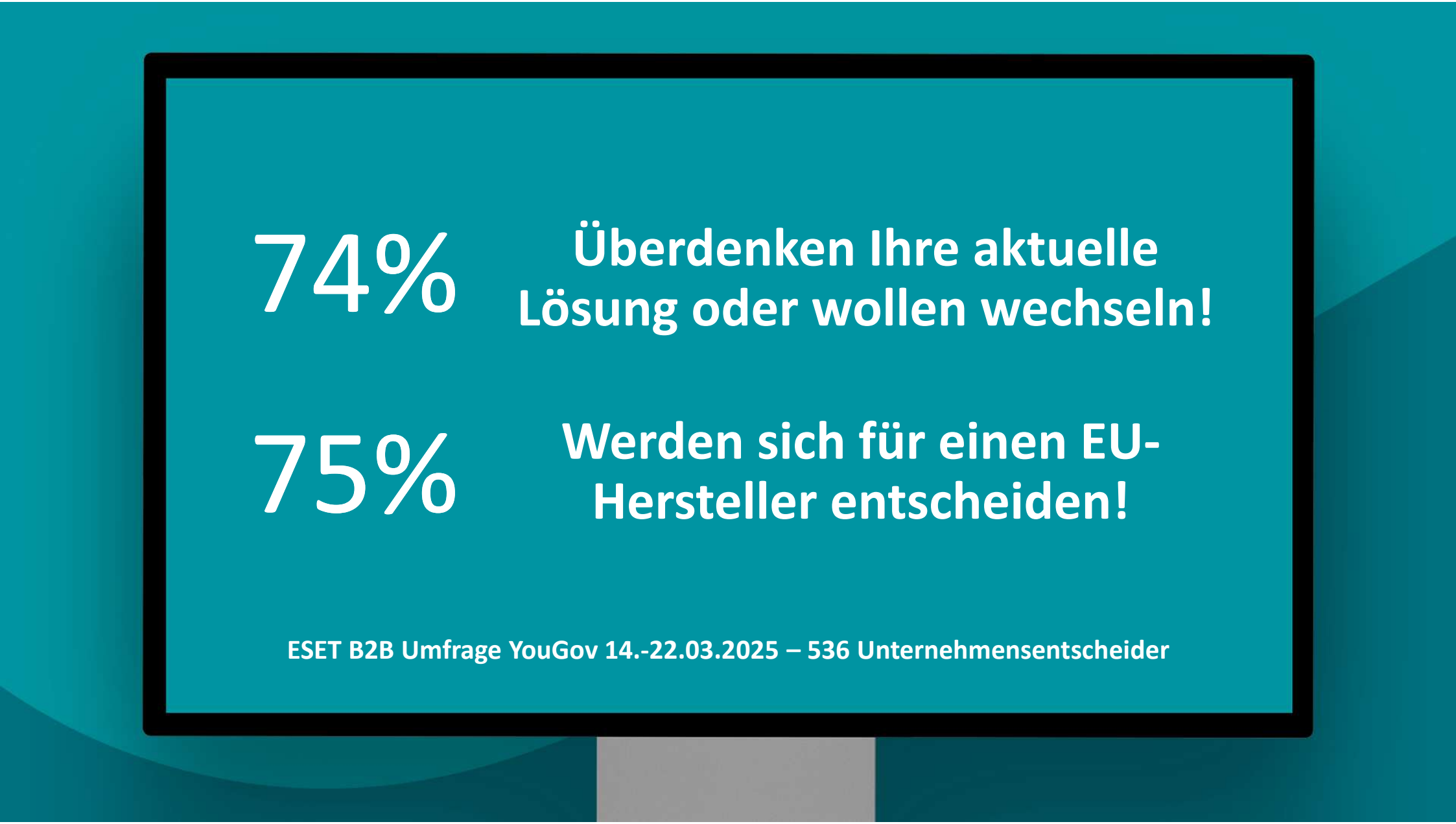
Herkunft des Herstellers



Bereits knapp

jeder Zweite

verwendet in seinem Unternehmen eine IT-Sicherheitslösung aus der europäischen Union, gefolgt von den USA mit 28 Prozent.


74%
Überdenken Ihre aktuelle Lösung oder wollen wechseln!
75%
Werden sich für einen EU-Hersteller entscheiden!
ESET B2B Umfrage YouGov 14.-22.03.2025 – 536 Unternehmensentscheider


IT-Security Made in EU
IT-Compliance
Einheitlicher Rechtsrahmen
Datenschutz und DSGVO-Komptabilität/ NIS 2


Vertrauen ist kein Add-On!

TeleTrust Kriterien:„IT Security made in EU“

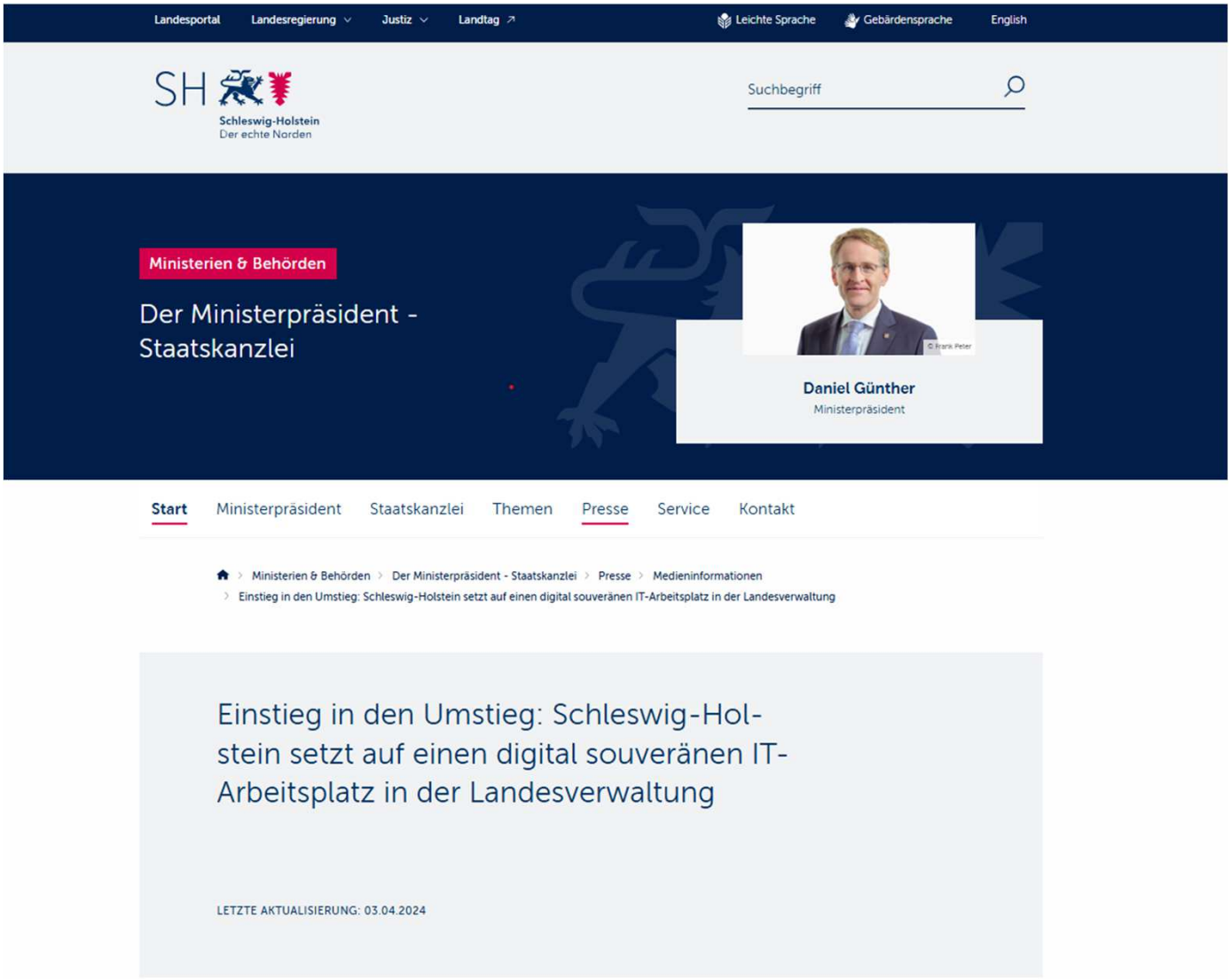
- ✓ Der Unternehmenshauptsitz ist in der EU
- ✓ Das Unternehmen bietet vertrauenswürdige IT-Sicherheitslösungen an
- ✓ „No Backdoor“-Garantie: Die angebotenen Produkte enthalten keine versteckten Zugänge
- ✓ Die IT-Sicherheitsforschung und -entwicklung findet in der Europäischen Union statt
- ✓ Das Unternehmen verpflichtet sich, den Anforderungen der EU-Datenschutz-Grundverordnung zu genügen

SecurITy made in EU
Trust Seal
www.teletrust.de/itsmie

https://www.teletrust.de/itsmie/

„Eine No-Backdoor-Garantie ist für uns selbstverständlich – denn: Als IT-Sicherheitshersteller aus der EU stehen wir zu 100 % hinter der demokratischen Grundordnung der europäischen Union“.

Holger Suhl, Country Manager DACH, ESET Deutschland.



„Der Weg der digitalen Souveränität folgt aber auch einem klaren industriepolitischen Kompass. […]Unsere Ziele beim Ausbau eines gemeinsamen digitalen Binnenmarktes sind digital souveräne Lösungen und Dienstleistungen, die wir miteinander vernetzen. […].“
Dirk Schrödter, Digitalisierungsminister Schleswig-Holstein

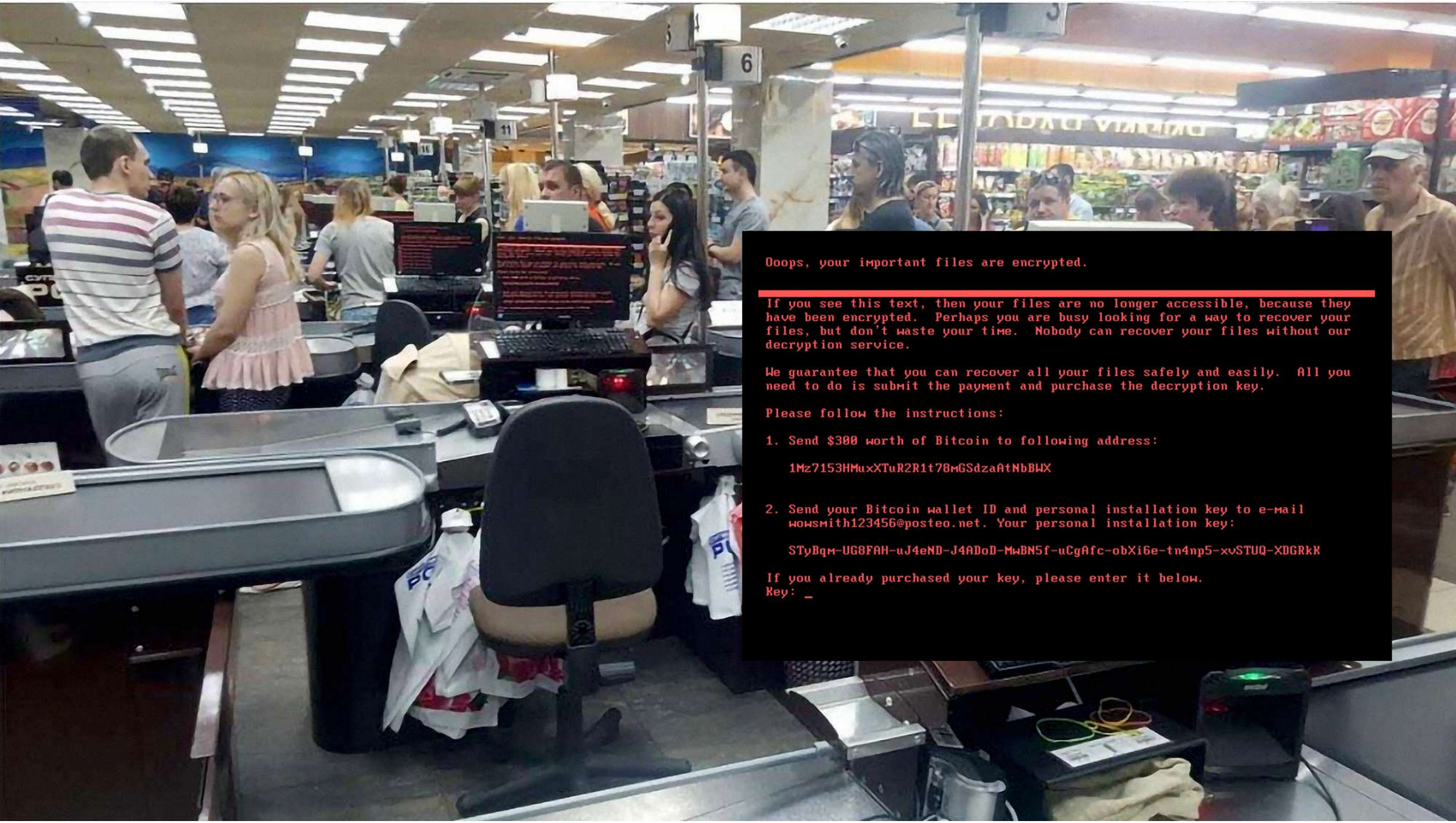
17. Dezember 2016

Angriffsziel:
KRITIS; Stromversorgung in Kiew

Auswirkungen:
Blackout

INDUSTROYER

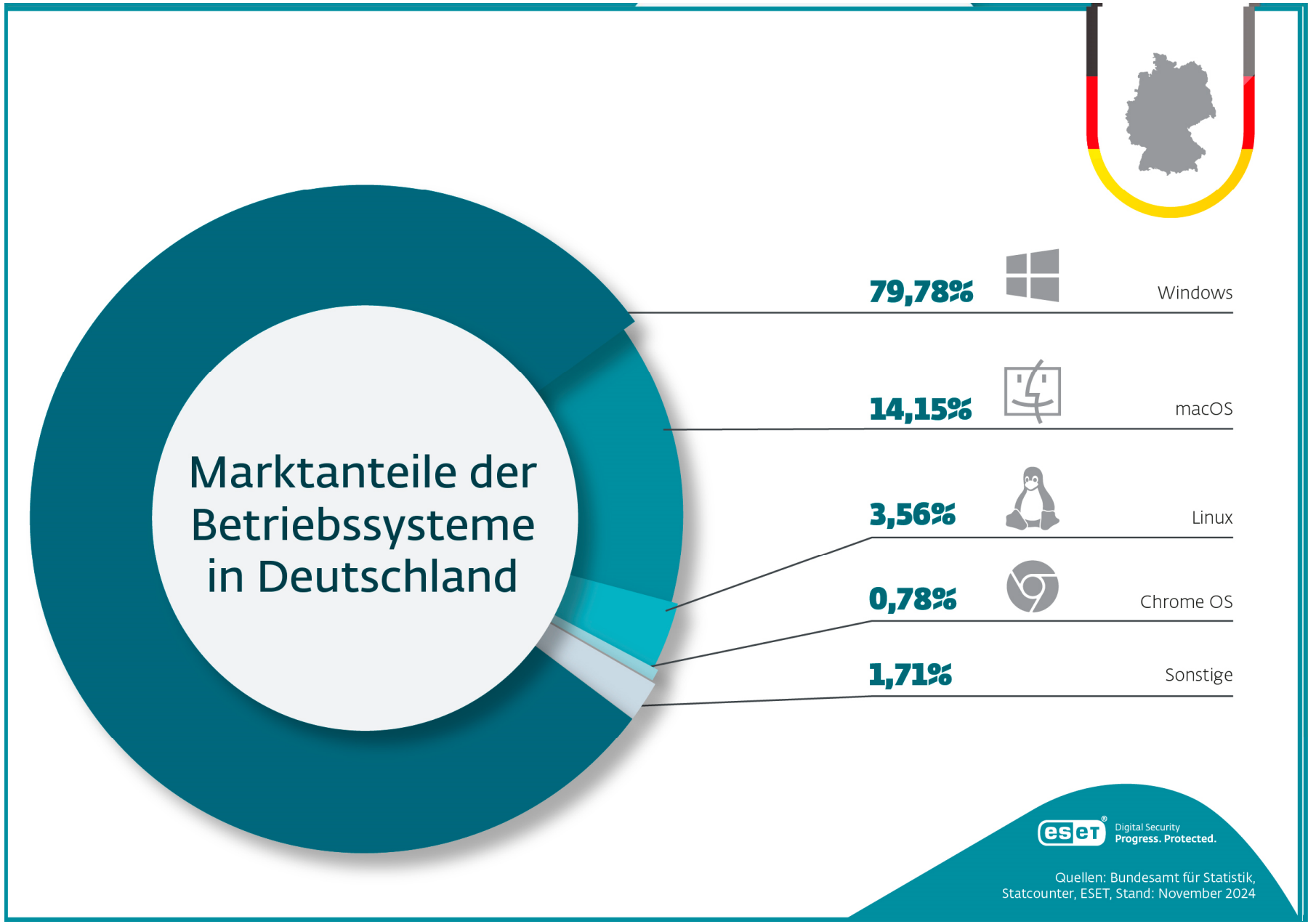
2017 NotPetya
(erste Kollateralschäden)


Ooops, your important files are encrypted.
If you see this text, then your files are no longer accessible, because they have been encrypted. Perhaps you are busy looking for a way to recover your files, but don't waste your time. Nobody can recover your files without our decryption service.
We guarantee that you can recover all your files safely and easily. All you need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-mail wowsmith123456@posteo.net. Your personal installation key:
STyBqm-UG8FAH-uJ4eND-J4ADoD-MwBN5f-uCgAfc-obXi6e-tn4np5-xvSTUQ-XDGRkK
If you already purchased your key, please enter it below.
Key: _

SCHADEN DURCH NOTPETYA

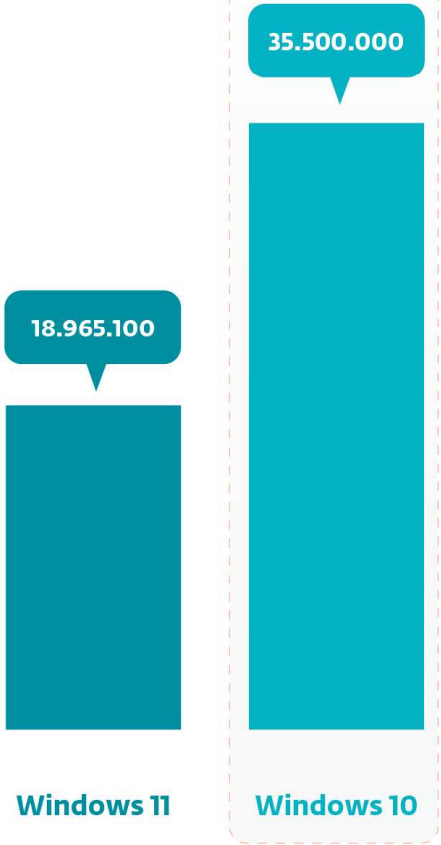
10 Milliarden USD

Software-Dinos


Marktanteile der Betriebssysteme in Deutschland
79,78%
Windows
14,15%
macOS
3,56%
Linux
0,78%
Chrome OS
1,71%
Sonstige
eset Digital Security
Progress. Protected.
Quellen: Bundesamt für Statistik,
Statcounter, ESET, Stand: November 2024

Verteilung der Windows Betriebssysteme in D-A-CH

Support läuft aus



1.26 Millionen Geräte sind unsicher

eset Digital Security
Progress. Protected.

Quellen: Bundesamt für Statistik, Statcounter, ESET, Stand: November 2024

Ich habe einen Virus!

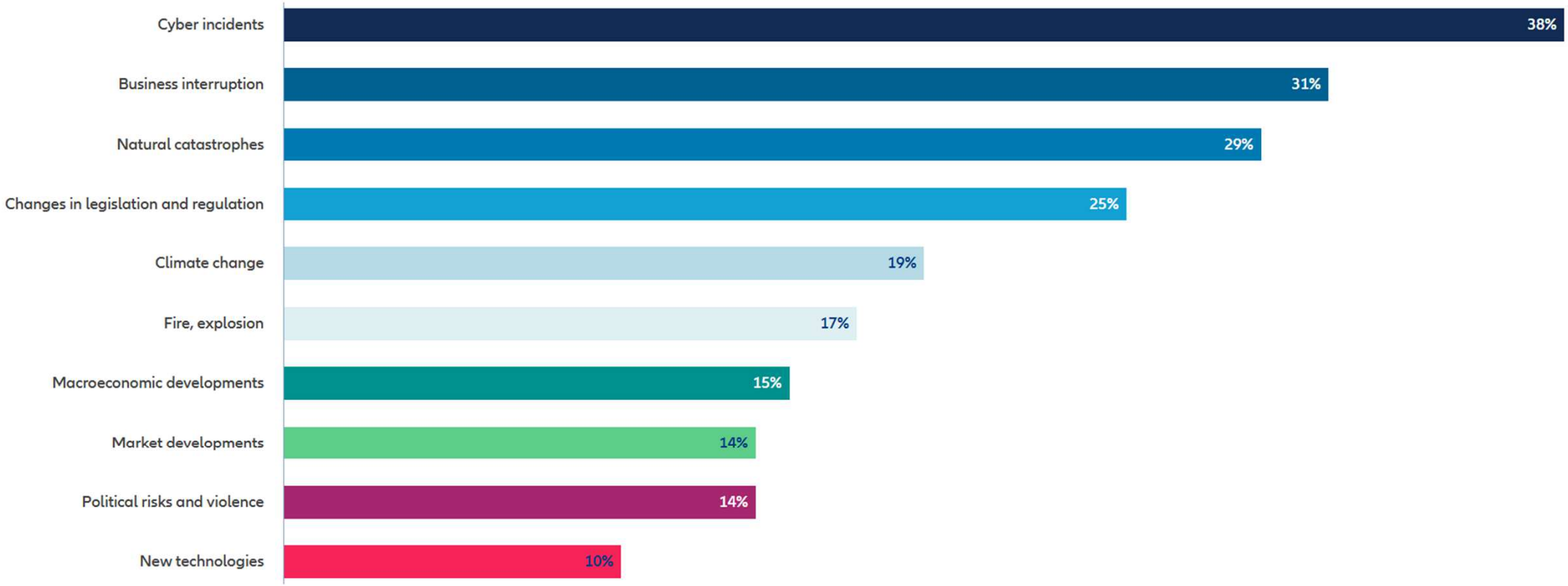
… sagt man heute nur noch beim Arzt

eset Digital Security
Progress. Protected.

The most important business risks in 2025: global

Allianz Risk Barometer 2025

Figures represent the number of risks selected as a percentage of all survey responses from 3,778 respondents. All respondents could select up to three risks per industry, which is why the figures do not add up to 100%.



Source: Allianz Commercial

Manche Dinge ändern sich nie, oder?

Top 5 Angriffsvektoren	Methodik	Relative Häufigkeit
1. Ransomware	Phishing, Remote Desktop	30%
2. Exploits & Schwachstellen	Sicherheitslücken, ZeroDays	25%
3. Phishing & Social Engineering	SpearPhishing, Mails, CEO-Fraud	20%
4. Supply-Chain-Angriffe	Software-Updates, kompromittierte Dienstleister	15%
5. Cloud-Sicherheitslücken & Fehlkonfigurationen	Fehlende MFA, Lücken in Konfiguration	10%

Quellen: BSI Lagebild, Enisa Threat Landscape, Deloite Cyber Threats, Swiss National Cyber Security Center, Microsoft Digital Defense Report

NIS 2: Auf einen Blick

Digital Security
Progress. Protected.

Der Zweck von NIS 2

Bedrohungslage

- hybride Bedrohungslage
- Lage ist kritisch
- Zeitenwende
- Cybercrime as a Service
- Staatliche Akteure
- Rekordschäden

Bestehende Mindeststandards (Regulierung)

- BSI-Gesetz / IT-SIG 2.0
- BSI-KritisV
- 10 Sektoren
- Hohe Schwellenwerte
- Ca. 3.000 Organisationen

Selbstregulierung des Marktes

- Unzureichend!
- Stand der Technik?
- IT-Security = Chefsache?
- …

Gesellschaftliche Stabilität und Versorgungssicherheit

Sektoren nach Anhang I
Energie
Verkehr und Transport
Bankwesen
Finanzmärkte
Gesundheitswesen
Trinkwasser
Abwasser
Digitale Infrastruktur
ICT* Service Management (Managed Service Provider - MSP)
Öffentliche Verwaltung
Weltraum

Sektoren nach Anhang II
Post- und Kurierdienste
Abfallwirtschaft
Produktion, Herstellung und Handel mit chemischen Stoffen
Produktion, Verarbeitung und Handel von Lebensmitteln
Verarbeitendes Gewerbe/Herstellung von Waren
Anbieter digitaler Dienste
Forschungseinrichtungen

A Besonders wichtige Einrichtungen

Große Betreiber aus 11 Sektoren (Anhang I) und Sonderfälle

B Wichtige Einrichtungen

Große/Mittlere Betreiber aus allen 18 Sektoren und Sonderfälle, soweit nicht von besonders wichtigen Einrichtungen erfasst

Mittlere Unternehmen

- Mindestens 50 Beschäftigte
- Jahresumsatz/Jahresbilanz > 10 Mio. EUR

Große Unternehmen

- Mindestens 250 Beschäftigte
- Umsatz > 50 Mio. EUR
- Bilanz > 43 Mio. EUR

Unabhängig von Unternehmensgröße

Qualifizierende Faktoren, z.B.:

- Kritische Tätigkeit
- Auswirkung auf öffentliche Ordnung
- Systemrisiken
- Grenzüberschreitende Auswirkungen

Neue Regeln, alte Strukturen?

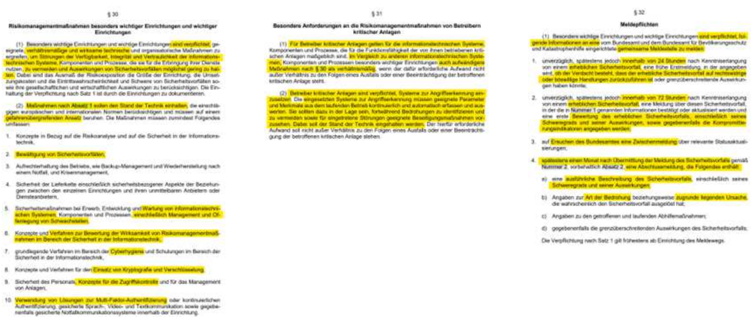

Cybersecurity = Fundament, nicht Fassade!

TOP Anforderungen der NIS2 (Referentenentwürfe)

Kapitel 2

Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten

§ 30	Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen
§ 31	Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen
§ 32	Meldepflichten
§ 33	Registrierungspflicht
§ 34	Besondere Registrierungspflicht für bestimmte Einrichtungsarten
§ 35	Unterrichtungspflichten
§ 36	Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen
§ 37	Ausnahmebescheid
§ 38	Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen
§ 39	Nachweispflichten für Betreiber kritischer Anlagen
§ 40	Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen
§ 41	Untersagung des Einsatzes kritischer Komponenten
§ 42	Auskunftsverlangen



Was es braucht:

- Robuste Cybersecurity-Lösung auf dem Stand der Technik
- Verschlüsselung als Absicherung vor Verluste und Datenabfluss
- Sicherung der Zugänge mittels MFA
- Absicherung von Cloud-Lösungen und Storage (Gefahrenübergreifend)

- Systeme zur Angriffserkennung (XDR/MDR)
- 24/7 Monitoring und vollständigen Überblick über Anomalien und Zusammenhänge (Meldewesen!)

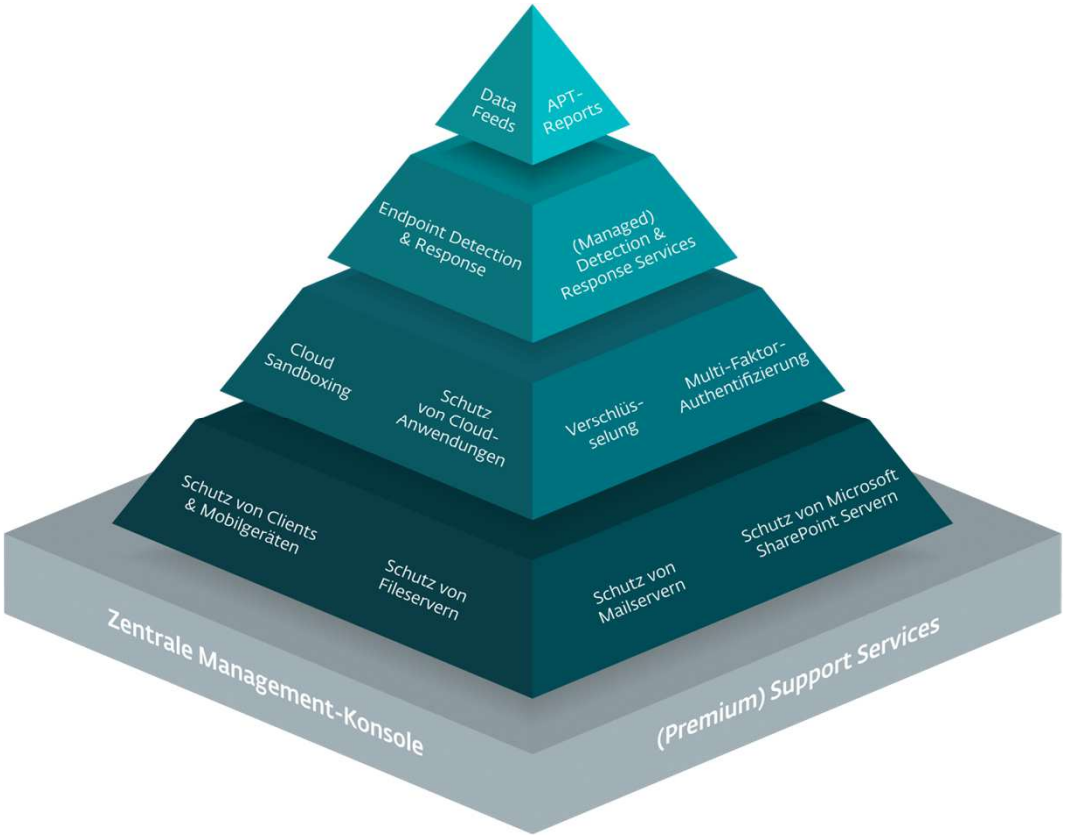
Digital Security
Progress. Protected.

Technologische Anforderungen

Must-Haves 2025

Digital Security
Progress. Protected.

Zero Trust-Pyramide



Der Zero Trust Security-Ansatz von ESET besteht aus einem mehrstufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer“.

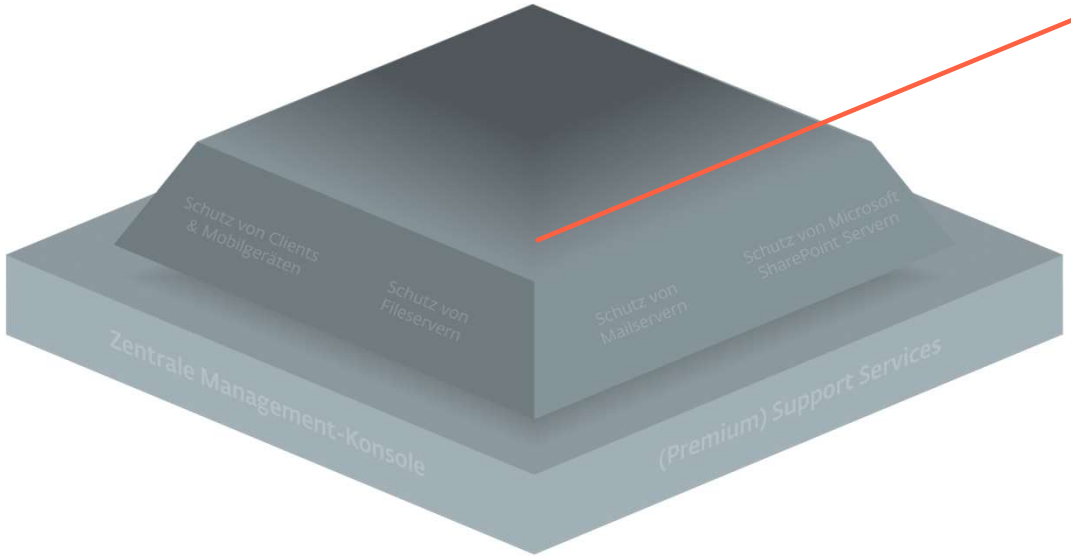
GRUNDSCHUTZ BASIS

Stufe 0:
Mindestabsicherung für Endgeräte und Server

Reifegrad der IT-Organisation:

- Zentrales Management (Cloud oder On-Prem)
- Policies und Regeln für die Geräte- und Internetnutzung

GRUNDSCHUTZ PLUS

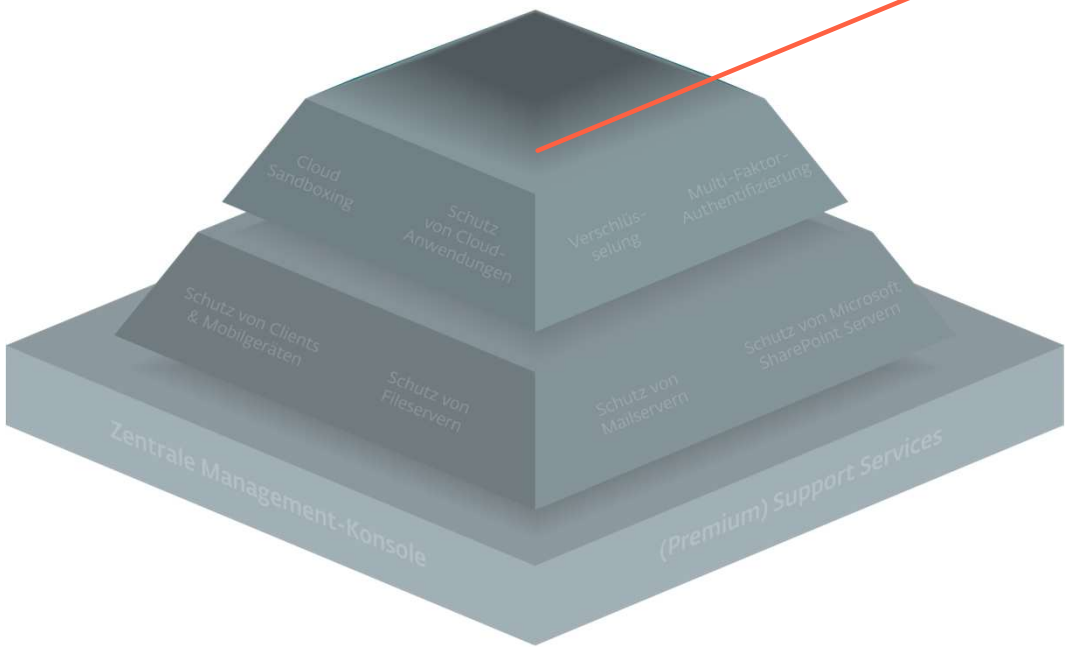


Stufe 1:
Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

Reifegrad der IT-Organisation:

- Zentrales Management (Cloud oder On-Prem)
- Adaptive und skalierbare Policies, die auf dem Output der jeweiligen Lösung basieren

GEFAHRENSUCHE UND ABWEHR - INNENSICHT

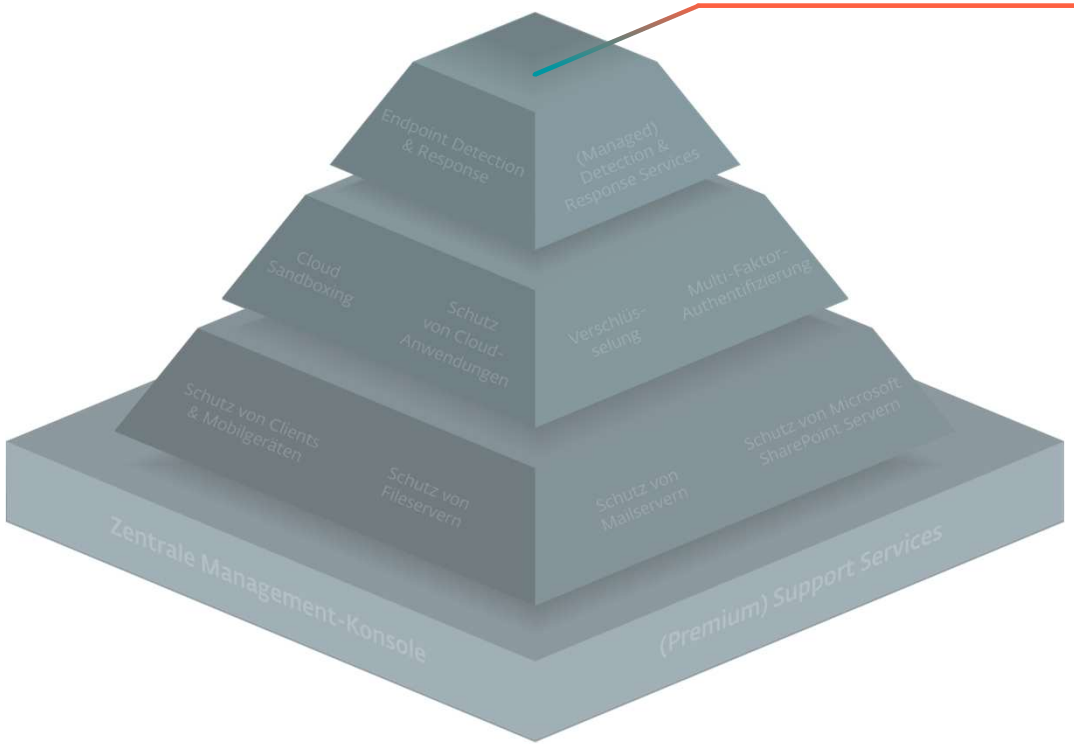


Stufe 2:
Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalieerkennung, Schwachstellen-analyse und Incident Management

Reifegrad der IT-Organisation:

- Automatisierte Incident Detection und Threat Monitoring inkl. Forensik
- Evolutionäre Policies und Regeln durch Erkenntnisse aus der XDR-Plattform

GANZHEITLICHES LAGEBILD - AUSSENSICHT



Stufe 3:
Bietet Einblicke in die globale Bedrohungsland-schaft als Grundlage für einen SOC-/SIEM-Betrieb

Reifegrad der IT-Organisation:

- Frühwarnsystem mittels SIEM-/SOC-Umgebung
- Umfangreiche präventive Sicherheitsmaßnahmen durch externes Lagebild

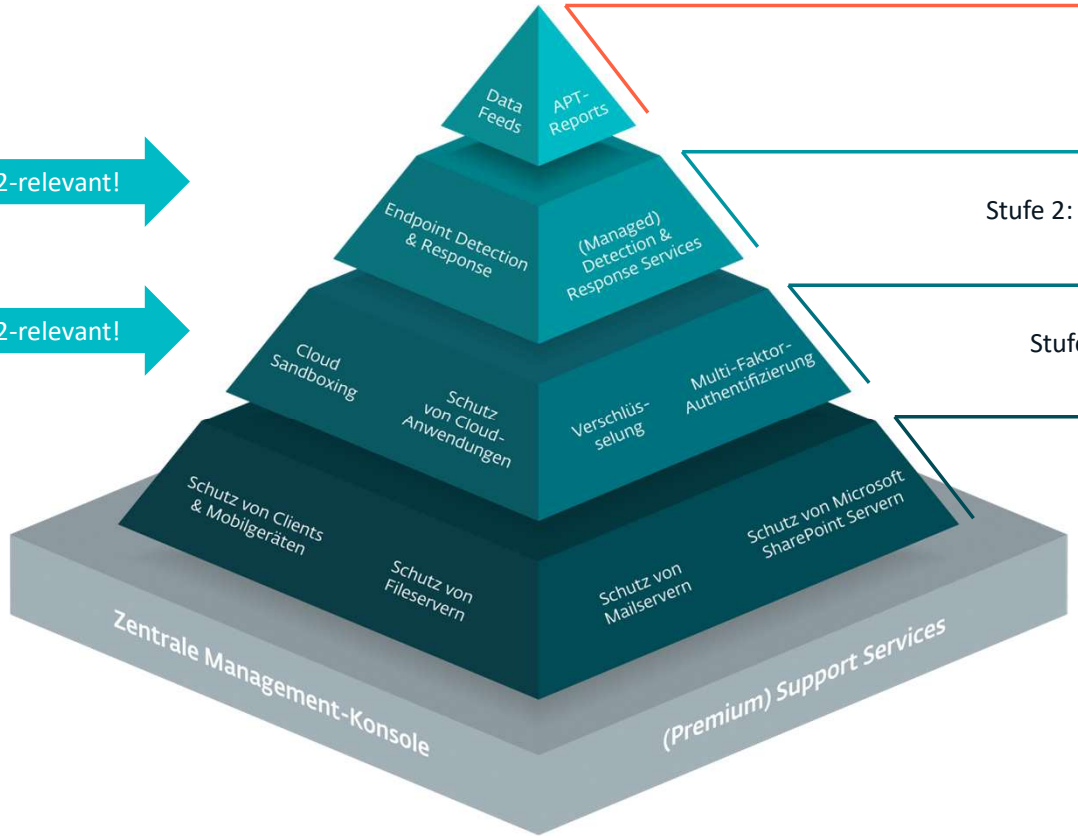
Technologien im Kontext von NIS 2

EINSATZBEREICH

SCHUTZLEVEL

NIS2-relevant!

NIS2-relevant!



Ganzheitliches Lagebild – Außensicht
Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaft als Grundlage für einen SOC-/SIEM-Betrieb

Gefahrensuche und Abwehr – Innensicht
Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalie-erkennung, Schwachstellenanalyse und Incident Management

Grundschutz Plus
Stufe 1: Empfohlene zusätzliche Absicherung für Cloud-Anwendungen, Daten und Zugänge sowie erweiterter Schutz vor Zero-Days

Grundschutz Basis
Stufe 0: Mindestabsicherung für Endgeräte und Server

eset Digital Security
Progress. Protected.

ESET PROTECT Bundle-Übersicht

Modul	MDR Ultimate	MDR	Elite	Enterprise	Complete	Advanced	Lösung	Kompatibilität
Zentrale Management-Konsole	●	●	●	●	●	●	ESET PROTECT	Konsole:
	●	●	●	●	●	●	ESET PROTECT On-Prem	Server:
Schutz von Clients, Mobilgeräten und Fileservern	●	●	●	●	●	●	ESET Endpoint Security* | Antivirus	
	●	●	●	●	●	●	Feature: Ransomware Remediation	
	●	●	●	●	●	●	ESET Server Security	
	●	●	●	●	●	●	Mobile Device Management*	iOS
Cloud Sandboxing	●	●	●	●	●	●	ESET LiveGuard® Advanced	
Verschlüsselung	●	●	●	●	●	●	ESET Full Disk Encryption	
Schutz von Mailservern	●	●	●		●		ESET Mail Security (inkl. ESET LiveGuard® Advanced für Exchange)	Exchange
Schutz von Cloud-Anwendungen	●	●	●		●		ESET Cloud Office Security (inkl. ESET LiveGuard® Advanced)	
Schwachstellen- & Patch-Management	●	●	●		●		ESET Vulnerability & Patch Management	
Multi-Faktor-Authentifizierung	●	●	●				ESET Secure Authentication	Konsole: Server: Apps: iOS
Endpoint Detection and Response	●	●	●	●			ESET Inspect**	
	●						Feature: ESET AI Advisor	Konsole:
	●	●	●	●			ESET Inspect On-Prem**	Server:
Premium Support Service	● Ultimate	●					ESET Premium Support	
MDR-Service	● Ultimate	●					ESET MDR	

● = nur im Cloud-Bundle enthalten

● = sowohl im Cloud- als auch On-Prem-Bundle enthalten

MSP = für MSP nur Cloud-Bundle buchbar (Ausnahme: ESET PROTECT Entry)

* ab ESET PROTECT Advanced (Cloud-Bundles) gibt es pro Seat eine zusätzliche Lizenz für ein weiteres Mobilgerät (Mobile Threat Defense)

** unterstützt Geräte mit Windows, Linux sowie macOS; ESET Inspect nur mit ESET PROTECT, ESET Inspect On-Prem nur mit ESET PROTECT On-Prem


eset
Digital Security
Progress. Protected.
www.eset.de
ESET
Made in EU
IT-Security