Cybersecurity Made in EU

Mehr als eine Herkunftsangabe

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

Digitale Zeitenwende 2.0

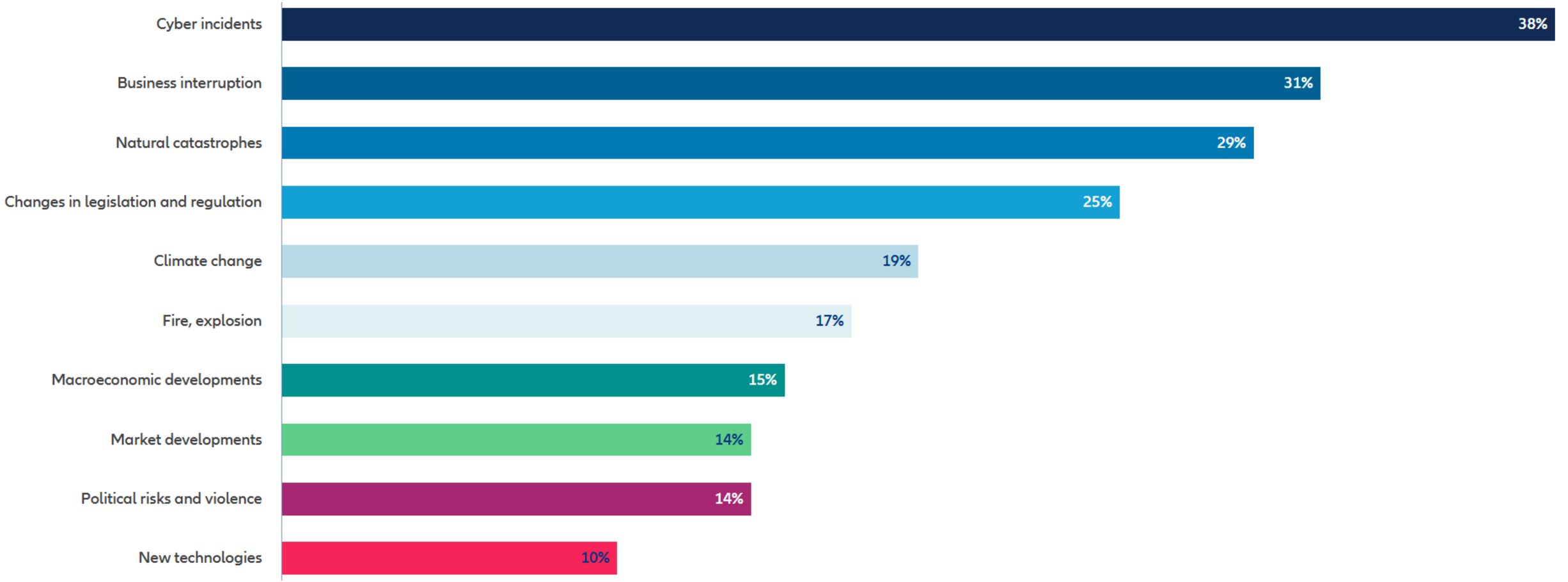
Datenschutz „Made in EU“ ist Pflicht und keine Kür

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

“

1.2 Milliarden Euro Schaden durch Cybercrime bei österreichischen Unternehmen pro Jahr.

EY Studie zu Cyberangriffen 2024

17. Dezember 2016

Angriffsziel:
KRITIS; Stromversorgung in Kiew

Auswirkungen:
Blackout

INDUSTROYER

Angriffsvektoren

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

Relation Cyber-Incidents zu KRITIS-Meldungen

DE

136.865

BKA/BSI Daten

davon KRITIS
200+ (0,15 %)

AT

17.000

CERT.at

davon KRITIS
85-170 (5-10%)

CH

34.000

Swiss NCSC

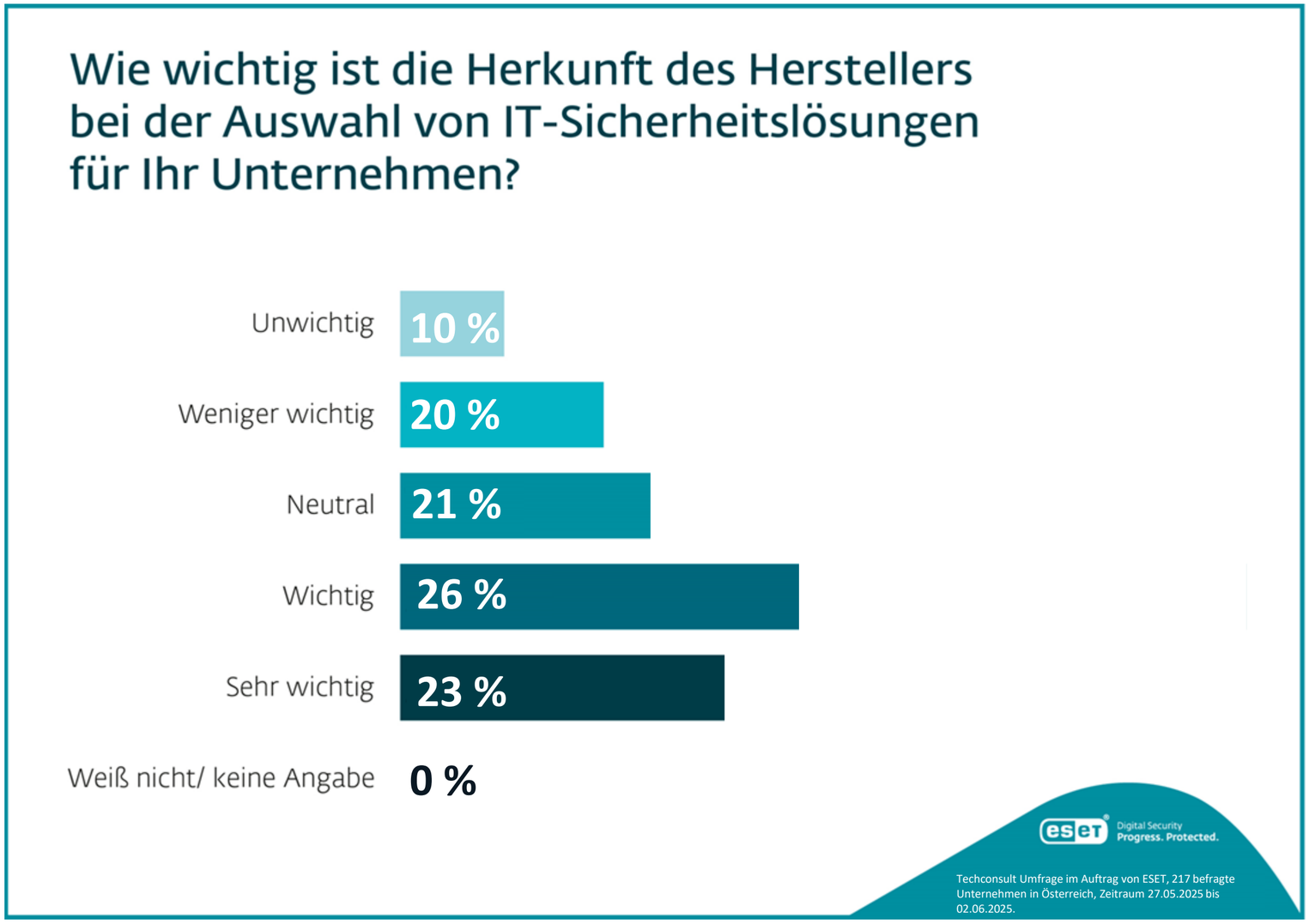
davon KRITIS
340-510 (10-15%)


Die Russland-Affäre im
Schweizer Geheimdienst
«Das ist Spionage»

ESET Umfrage „Made in EU“

Digital Security
Progress. Protected.

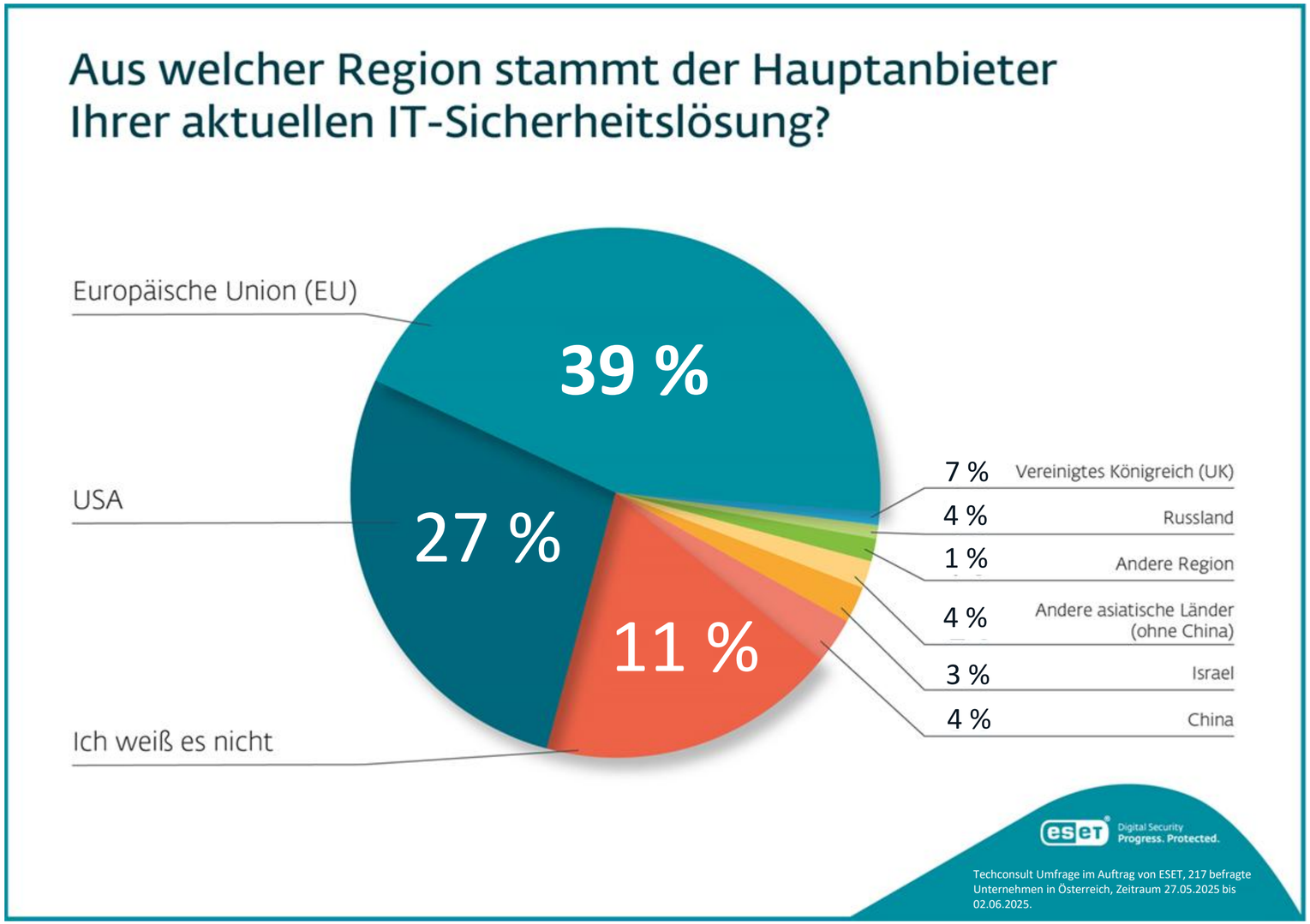
Herkunft des Herstellers



49 %

der Unternehmen in Österreich bewerten die Herkunft als wichtig oder sehr wichtig.

Herkunft des Herstellers

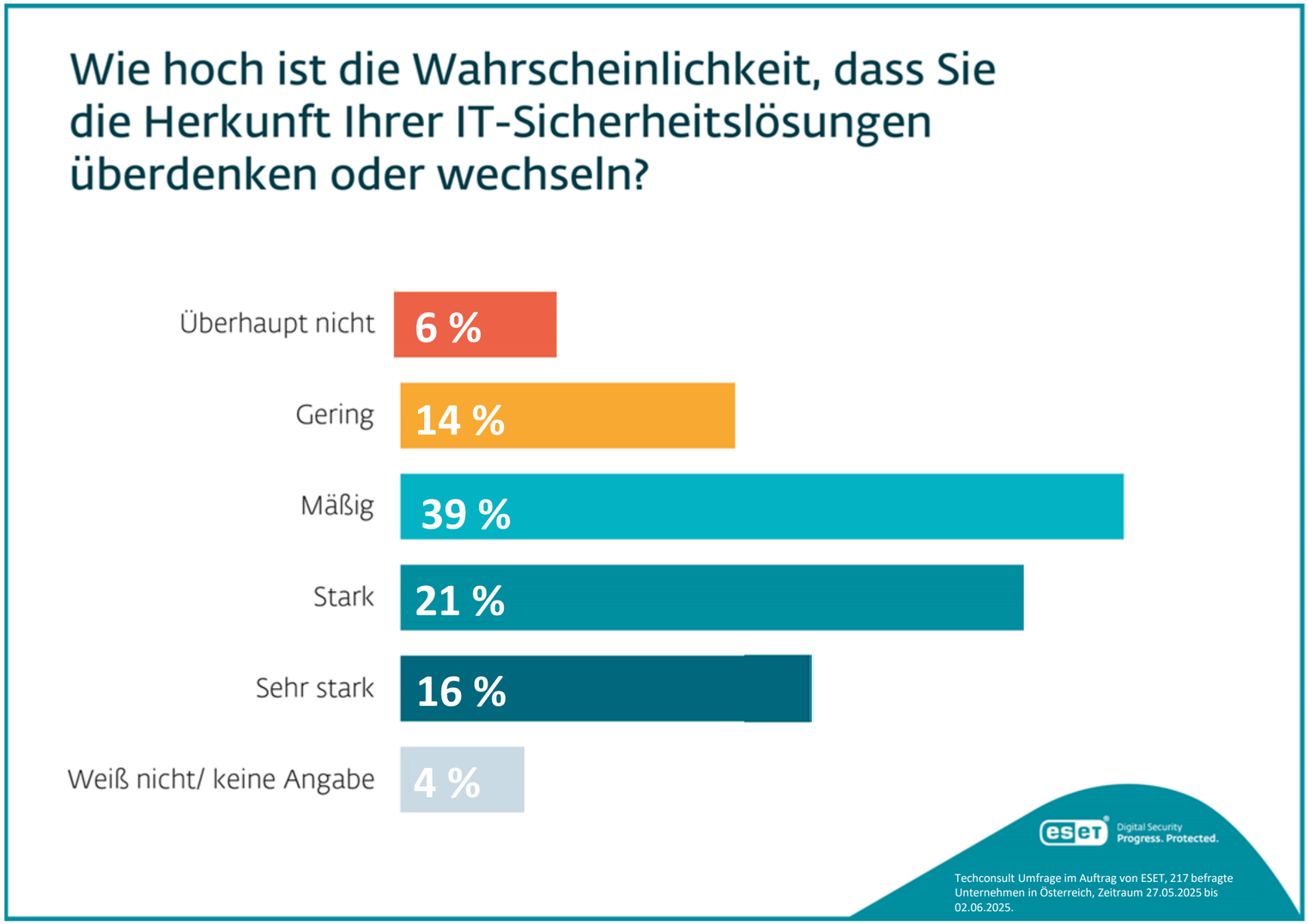


knapp

vier von 10

verwenden in ihren Unternehmen eine IT-Sicherheitslösung aus der europäischen Union, gefolgt von den USA mit 27 Prozent.

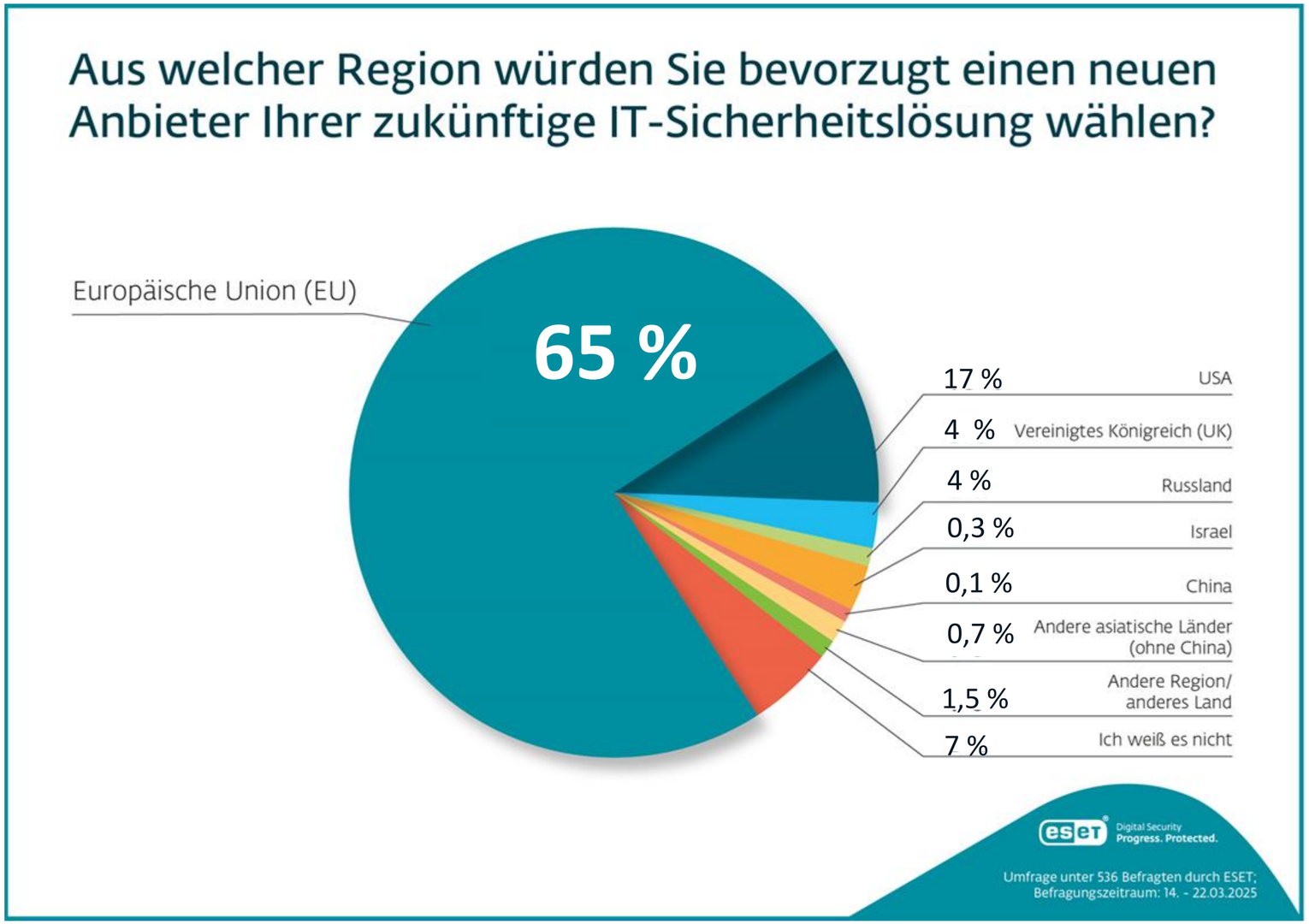
Herkunft des Herstellers



37%

der Befragten überdenken oder ziehen einen Wechsel Ihrer IT-Sicherheitslösung in Betracht.

Wechselbereitschaft



Bei Befragten, die eine neue IT-Sicherheitslösung auswählen wollen, dominiert deutlich die EU mit

65 Prozent

37% Überdenken Ihre aktuelle Lösung oder wollen wechseln!

65% Werden sich für einen EU-Hersteller entscheiden!

ESET B2B Umfrage techconsult 27.05.-02.06.2025 – 217 Unternehmen

Vertrauen & Integrität

Digital Security
Progress. Protected.

IT-Security Made in EU

IT-Compliance

Einheitlicher Rechtsrahmen

Datenschutz und DSGVO-Komptabilität/ NIS 2

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

Secur|Ty
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“.

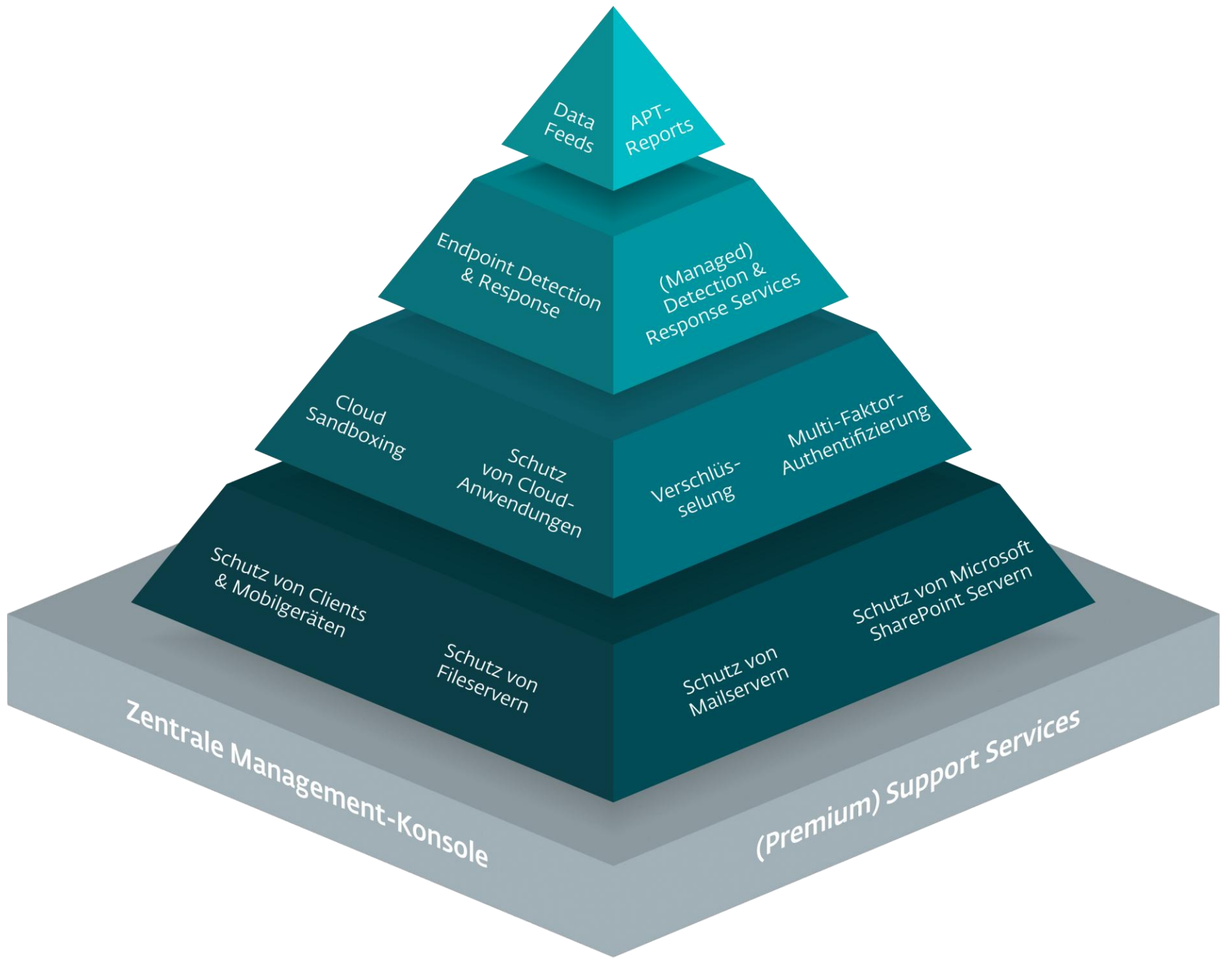
Holger Suhl, Country Manager DACH, ESET Deutschland.

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“.

Digital Security
Progress. Protected.

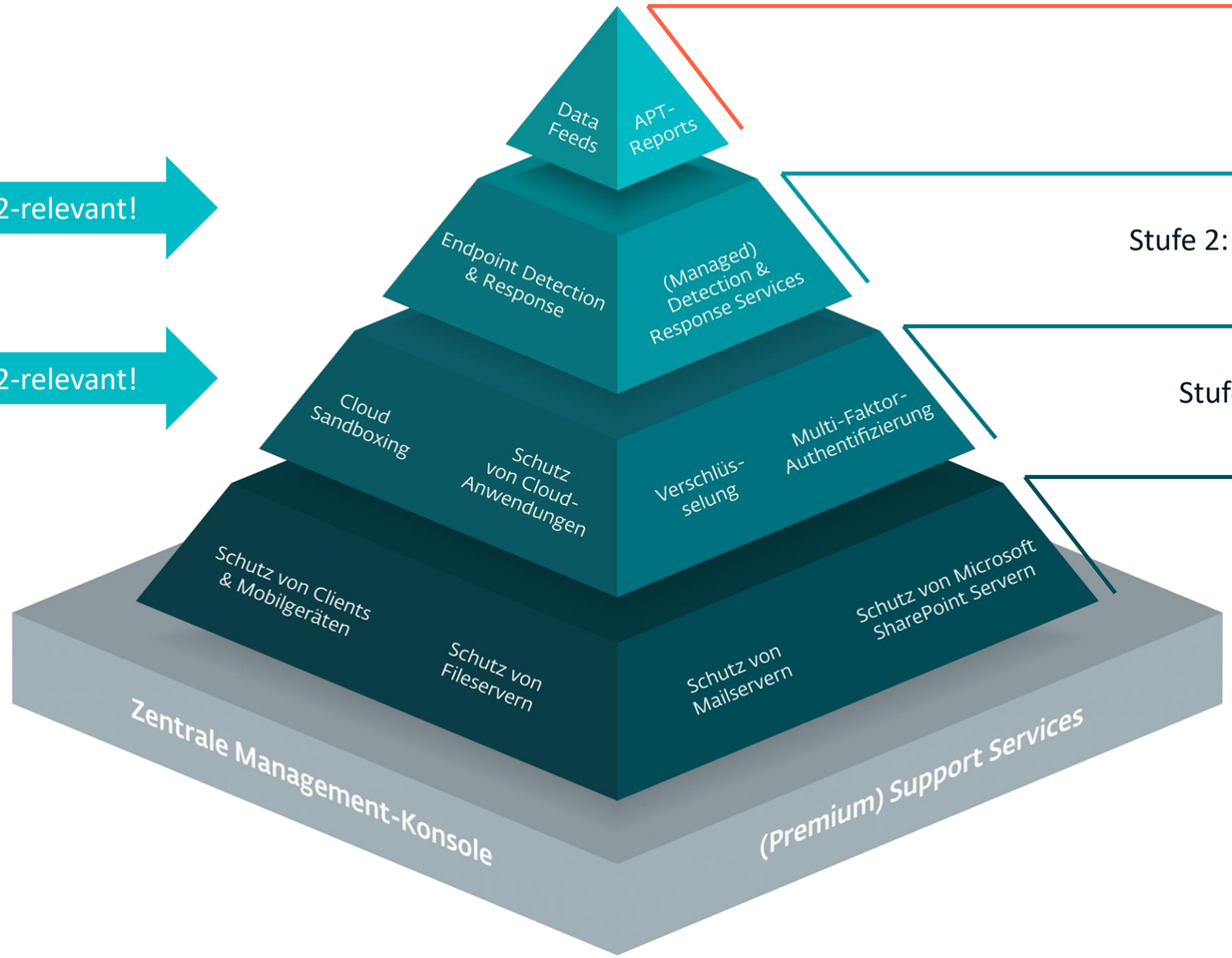
Technologien im Kontext von NIS 2

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