UMFRAGE

ESET Studie

Digitale Souveränität auf dem Prüfstand

Was deutsche Unternehmen wirklich von IT-Security „Made in EU“ halten

ESET Made in EU IT-Security

Cybersecurity
Progress. Protected.

ESET.DE | ESET.AT | ESET.CH

Inhaltsverzeichnis

Cybersecurity
Progress. Protected.

Digitale Souveränität auf dem Prüfstand: **Was Unternehmen wirklich von IT-Security „Made in EU“ halten**

Ob Ukrainekrieg, angespannte transatlantische Beziehungen oder Cyberbedrohungsszenarien aus Fernost: Die geopolitische Lage hat sich in kürzester Zeit verändert. Insbesondere das transatlantische Verhältnis hat durch verschiedene politische Entscheidungen eine andere Dynamik angenommen.

In diesem Kontext stellt sich die Frage: Wie reagieren wir in Europa und in Deutschland auf diese Veränderungen? Genau in diesen Zeiten ist es sinnvoll, sich auf das zu konzentrieren, was die Europäische Union groß gemacht hat: Technologische Raffinesse, kombiniert mit einem starken Wertekodex.

Gleichzeitig ist die Europäische Union eines der Hauptziele von Cyberattacken: Nach aktuellen Zahlen des Bitkom fühlen sich sieben von zehn Unternehmen in Deutschland durch analoge und digitale Angriffe stark bedroht. Die Zahl der betroffenen Organisationen ist in den letzten Jahren kontinuierlich gestiegen: 2024 hatten 81 Prozent der Unternehmen mit Diebstahl, Wirtschaftsspionage oder Sabotage zu kämpfen oder vermuteten einen Vorfall - ein deutlicher Anstieg gegenüber den Vorjahren. Der jährliche Gesamtschaden durch Cyber-Angriffe und verwandte Delikte beläuft sich mittlerweile auf rund 266,6 Milliarden Euro, wobei allein Hackerattacken für rund zwei Drittel dieses Schadens verantwortlich sind. Der gleiche Anteil an Unternehmen sieht sich durch Cyber-Angriffe in ihrer Existenz bedroht[1].

„Die Gefährdungslage ist und bleibt besorgniserregend, aber es liegt in unserer Hand, sie zu verbessern“, sagt Claudia Plattner, Präsidentin des Bundesamts für Sicherheit in der Informationstechnik.

Diese Bedrohungen kommen dabei aus unterschiedlichen Regionen mit verschiedenen Zielen: Vor allem zu China und Russland gehörende Hackergruppen haben es auf Organisationen in Europa abgesehen. Sie nehmen insbesondere Regierungsorganisationen sowie Transport- und Verteidigungsunternehmen ins Visier[2].

Aufgrund dieser beiden Faktoren – schwindendes Vertrauen in außereuropäische Partner und die Bedrohung durch Cyberangriffe – gewinnt das Thema IT-Sicherheit „Made in EU“ zunehmend an Bedeutung.

„Die aktuelle Lage hat Unternehmen wachgerüttelt: Während viele zurzeit auf außereuropäische IT-Sicherheitshersteller vertrauen, will der Großteil in Zukunft auf Hersteller aus der EU setzen. Und diese Entscheidung ist genau richtig, schließlich bieten EU-Hersteller gegenüber ihren außereuropäischen Pendants viele Vorteile, nicht nur was den Datenschutz betrifft“,

— Thorsten Urbanski, Leiter der TeleTrust Initiative „IT Security made in EU“ und Director of Marketing bei ESET Deutschland GmbH.

1 Quelle: www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

2 ESET APT Activity Report Q4 2024 – Q1 2025

Was bedeutet „Made in EU“ überhaupt?

Doch wie nehmen Unternehmen die Vorteile und Herausforderungen von IT-Sicherheit „Made in EU“ konkret wahr? Wem vertrauen deutsche IT-Entscheider noch und welche Rolle spielen europäische Werte? „Made in EU“ steht für Qualität, Sicherheit und Nachhaltigkeit. Das Gütesiegel signalisiert, dass ein Produkt unter fairen Arbeitsbedingungen, mit hohen Umweltstandards und nach europäischen Qualitätsrichtlinien gefertigt wurde. Besonders in Zeiten wachsender Sensibilität für ethische Produktion und kurze Lieferketten schafft „Made in EU“ Vertrauen und dient als starkes Kaufargument – vor allem im Vergleich zu Produkten aus Regionen mit weniger transparenten Standards.

536
Teilnehmer

Laufzeit von
14. bis 22. März 2025

Umfrage-ergebnisse

Über die **Umfrage**

Die Daten dieser Befragung basieren auf Online-Interviews mit Mitgliedern des YouGov Panels, die der Teilnahme vorab zugestimmt haben. Für diese Befragung wurden im Zeitraum vom 14. bis zum 22.03.2025 insgesamt 536 Unternehmensentscheider befragt. Die Erhebung wurde quotiert und die Ergebnisse gewichtet. Die Befragten setzen sich repräsentativ nach Beschäftigtenanteil pro Unternehmensgröße, nach Geschlecht und Altersgruppen von Unternehmensentscheidern, nach sechs NACE-Wirtschaftszweigen sowie nach Nielsen-Regionsverteilung von Unternehmen zusammen.

Kern**fragen**

- Angesichts der aktuellen geopolitischen Entwicklungen – wie beurteilen Sie die Wahrscheinlichkeit, dass Sie die Herkunft Ihrer IT-Sicherheitslösungen überdenken oder diese sogar wechseln?
- Aus welcher Region würden Sie bevorzugt einen neuen Anbieter für Ihre zukünftige IT-Sicherheitslösung wählen?
- Wie wichtig bzw. unwichtig ist die Herkunft des Herstellers bei der Auswahl von IT-Sicherheitslösungen für Ihr Unternehmen?
- Aus welcher Region stammt der Hauptanbieter Ihrer aktuellen IT-Sicherheitslösung?

44%

der Unternehmen überdenken die Herkunft seiner IT-Sicherheitslösung.

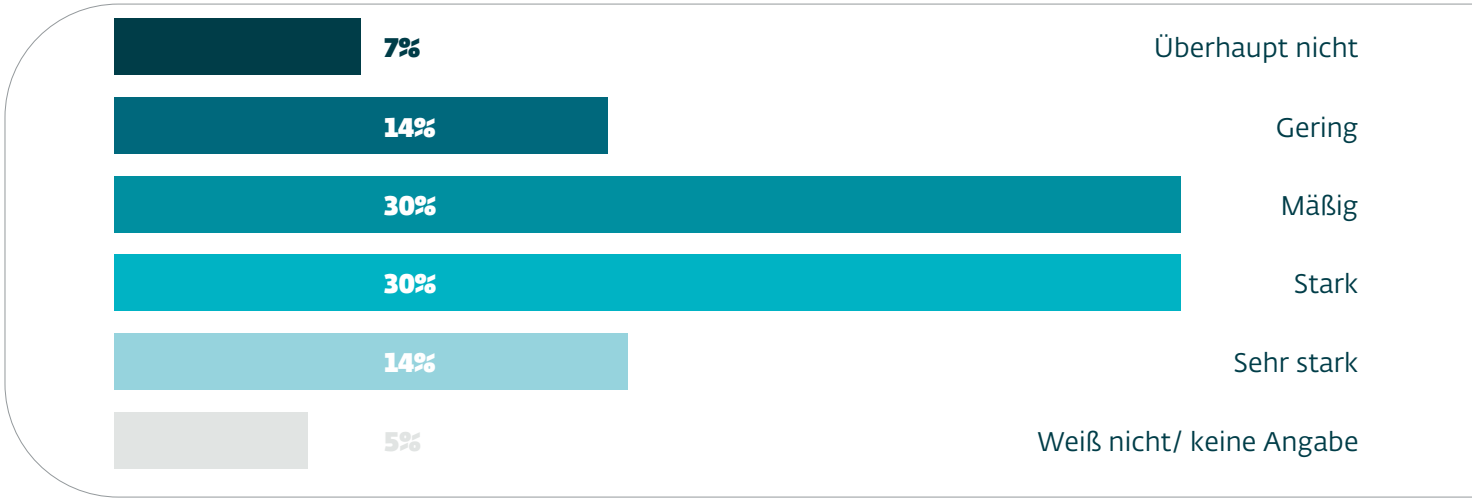
Frage 1: Angesichts der aktuellen geopolitischen Entwicklungen – wie beurteilen Sie die Wahrscheinlichkeit, dass Sie die Herkunft Ihrer IT-Sicherheitslösungen überdenken oder diese sogar wechseln?

Hypothese: Aufgrund der aktuellen Lage sind viele einem Wechsel der IT-Sicherheitslösung zugeneigt.

Ergebnis: Bestätigt

Die derzeit unruhige geopolitische Lage verunsichert viele Befragte. Viele Unternehmen befürchten offenbar, dass ihre IT Security-Lösung leicht aus der Ferne abgeschaltet werden könnte. Das macht EU-Anbieter beliebter: Fast jedes zweite Unternehmen (44 %) überdenkt die Herkunft seiner Cybersicherheitslösung oder erwägt einen Wechsel.

Auch hier sind es Produktions- und Dienstleistungsunternehmen, die einen Umstieg häufiger in Betracht ziehen (57 %) als andere Branchen. Am geringsten ist die Wechselbereitschaft im Groß- und Einzelhandel: Nur knapp jeder Dritte überdenkt in der aktuellen Situation die Ursprungsregion seiner IT-Sicherheitslösung.



Nur

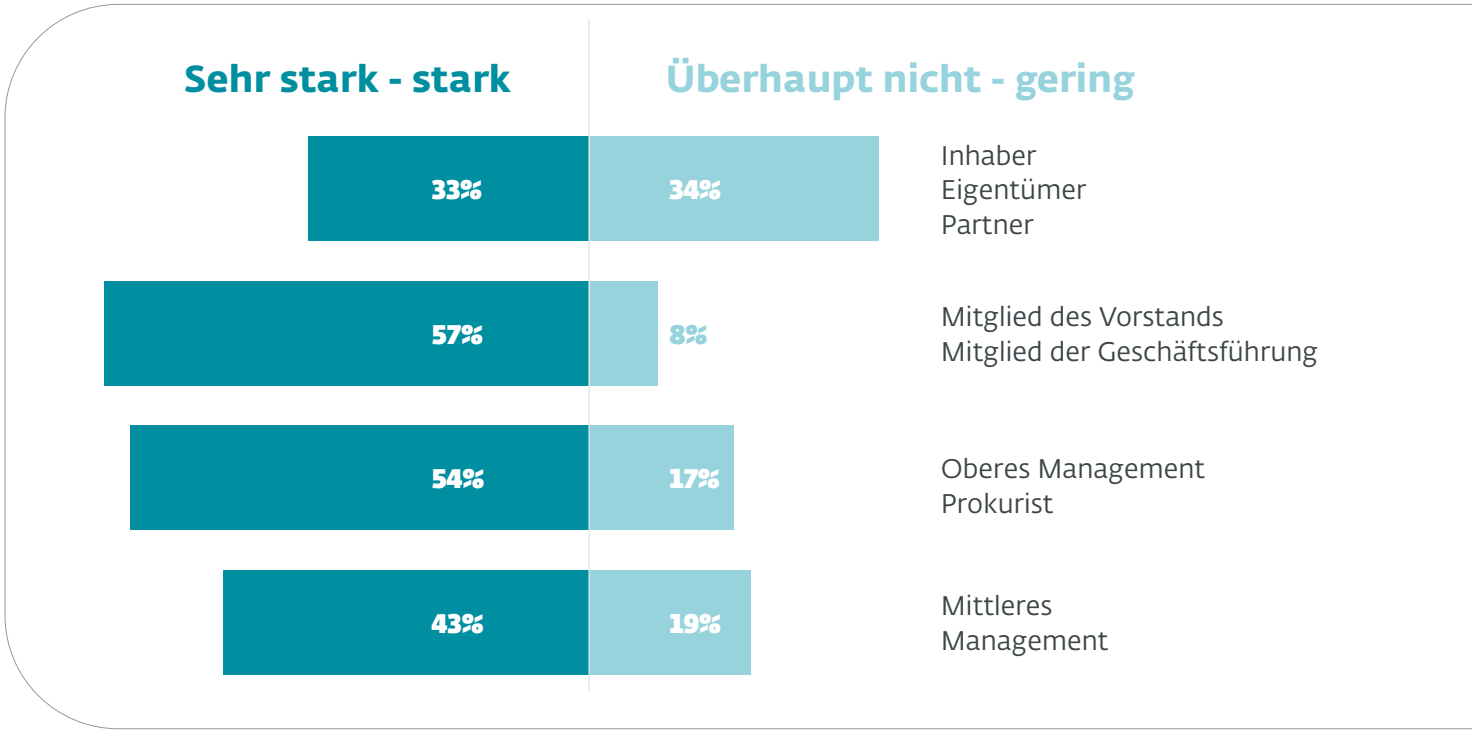
33%

der Inhaber eines Unternehmens ziehen einen Wechsel in Betracht

Vorstände (57 %) sowie das obere (54 %) und mittlere Management (43 %) sind eher zu einem Wechsel bereit. Ein Grund hierfür könnte sein, dass Inhaber sich sorgen könnten, ein Umstieg würde Produktionseinbußen oder Ausfälle in der IT zur Folge haben. Andere Führungsebenen im Unternehmen wissen, dass ein Wechsel – den richtigen Anbieter vorausgesetzt – schnell und problemlos vonstattengeht.

Wie abhängig Deutschland im Technologiebereich von anderen Ländern ist, zeigt eine weitere Bitkom-Umfrage[3]: Darin gaben 90 Prozent der Befragten an, auf den Import digitaler Technologien und Dienstleistungen aus anderen Ländern angewiesen zu sein. Zumindest im Bereich der IT-Sicherheit, so zeigt die aktuelle ESET Umfrage, haben die Unternehmen erkannt, dass diese Abhängigkeit riskant ist und suchen einen Ausweg. Die Wechselwilligen unter den Befragten kennen dabei nur eine Richtung: zurück in die EU. Drei Viertel geben an, bei der Wahl eines IT-Sicherheitsherstellers künftig auf europäische Anbieter zu setzen.

3 Quelle: www.bitkom.org/Presse/Presseinformation/Deutschlands-digitale-Abhaengigkeit-steigt



75%

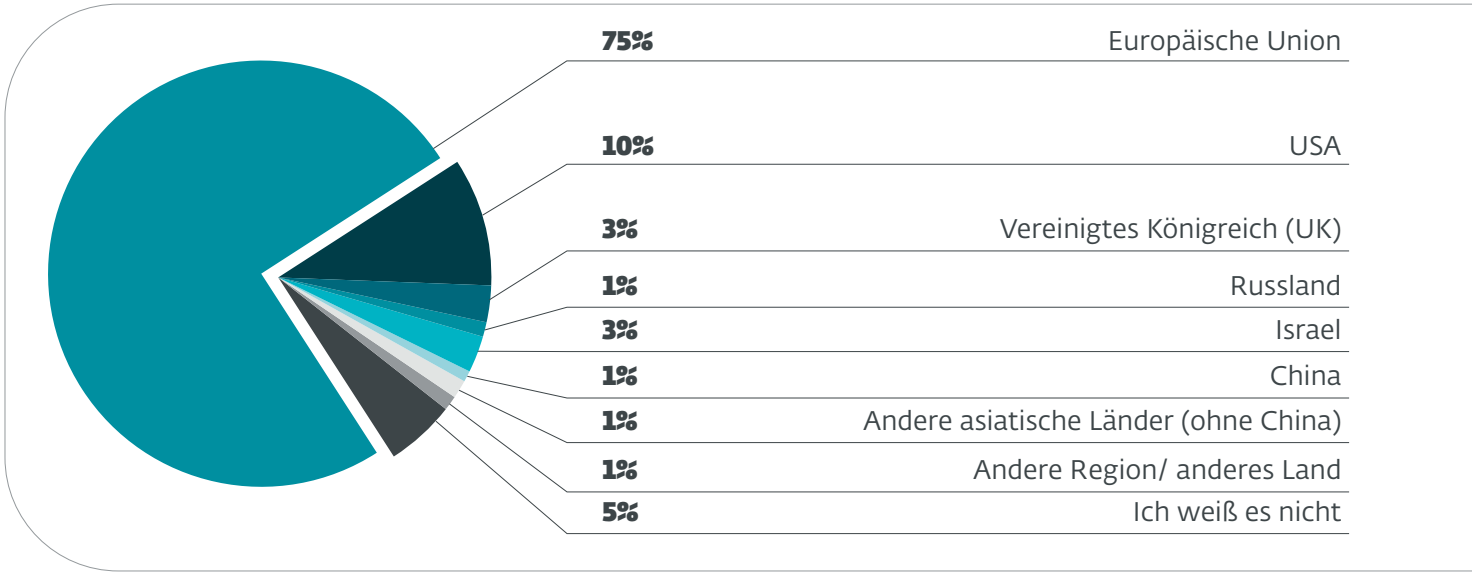
der befragten Wechselwilligen wollen zukünftig einen europäischen Anbieter beschäftigen.

Frage 2: Aus welcher Region würden Sie bevorzugt einen neuen Anbieter für Ihre zukünftige IT-Sicherheitslösung wählen?

Hypothese: Europäische Lösungen sind erste Wahl bei Entscheidern.

Ergebnis: Bestätigt

Diejenigen Befragten, die wechselwillig sind, wollen mit großer Mehrheit einen IT-Sicherheitsanbieter aus der EU: Ganze drei Viertel (75 %) geben an, zukünftig einen europäischen Anbieter beschäftigen zu wollen. Nur jeder Zehnte würde bei einem Wechsel einen US-amerikanischen Hersteller wählen. Diese Antworten zeigen: Europäische Lösungen genießen einen hervorragenden Ruf bei deutschen Unternehmensentscheidern, wohingegen andere Regionen hintenanstehen. Eine Erklärung hierfür ist, dass Entscheider europäischen Lösungen eher vertrauen. Darüber hinaus fühlen sich hiesige Hersteller stärker der Region verbunden, während außereuropäische Anbieter ihrer Heimatregion loyal gegenüber sind.



42%

im Gesundheits- und Rechtswesen nutzen bereits europäische Anbieter.

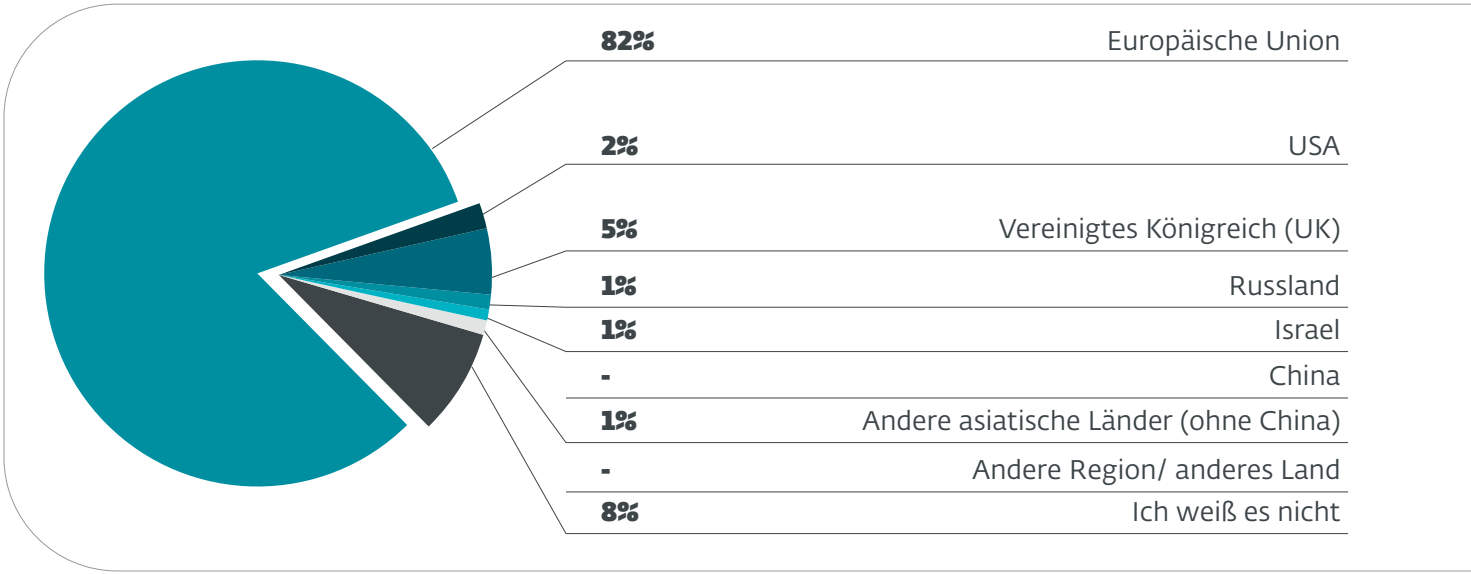
82%

geben an, demnächst zu einem EU-Anbieter wechseln zu wollen.

Besonders interessant: Im Gesundheits- und Rechtswesen nutzen zwar nur 42 Prozent bereits europäische Anbieter, aber ganze 82 Prozent geben an, demnächst zu einem EU-Anbieter wechseln zu wollen. Eine Erklärung hierfür ist, dass gerade die aktuelle politische Situation viele Organisationen in dem Bereich zu europäischen Lösungen bringt. Darüber hinaus hat ein vom Hersteller induzierter Ausfall einer Cybersicherheitslösung für einen Healthcare-Betrieb katastrophale Folgen.

Krankenhäuser gehören zu den beliebtesten Zielen von Hackern und ein erfolgreicher Angriff kann Leben von Patienten gefährden.[4] Hier könnte die Befürchtung von Seiten der Krankenhäuser bestehen, dass nicht-europäische Anbieter unzuverlässiger sind – sei es durch unverschuldete Ausfälle oder bewusste Abschaltungen durch Kill Switches.

4 Quelle: www1.wdr.de/nachrichten/cyberangriffe-auf-krankenhaeuser-100.html



75%

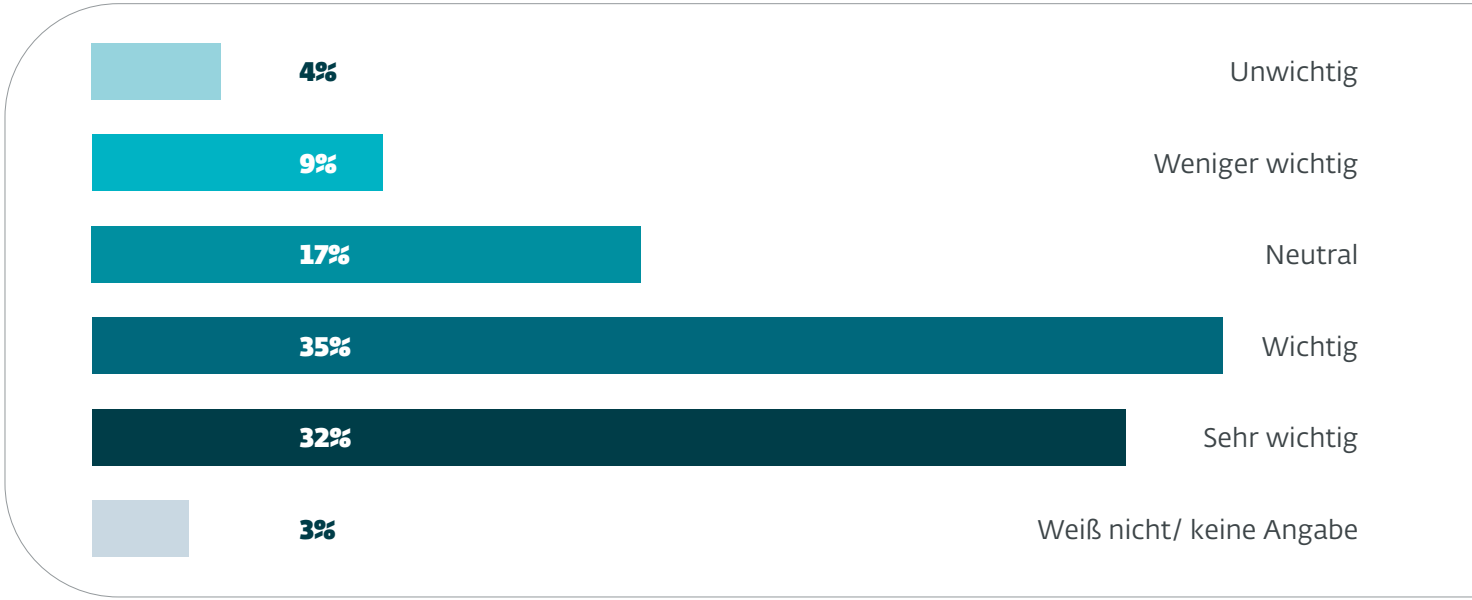
der befragten Wechselwilligen wollen zukünftig einen europäischen Anbieter beschäftigen.

Frage 3: Wie wichtig bzw. unwichtig ist die Herkunft des Herstellers bei der Auswahl von IT-Sicherheitslösungen für Ihr Unternehmen?

Hypothese: Die Herkunft ist ein ausschlaggebendes Kriterium bei der Wahl einer IT-Sicherheitslösung.

Ergebnis: Bestätigt

Generell achten deutsche Unternehmen auf die Regionalität ihrer IT-Sicherheit. Insgesamt 67 Prozent geben an, dass ihnen die Herkunft wichtig oder sehr wichtig ist. Besonders große Unternehmen mit mehr als 250 Mitarbeitern legen großen Wert darauf: Hier geben drei von vier Befragten an, auf den Ursprung ihrer Lösungen zu achten.



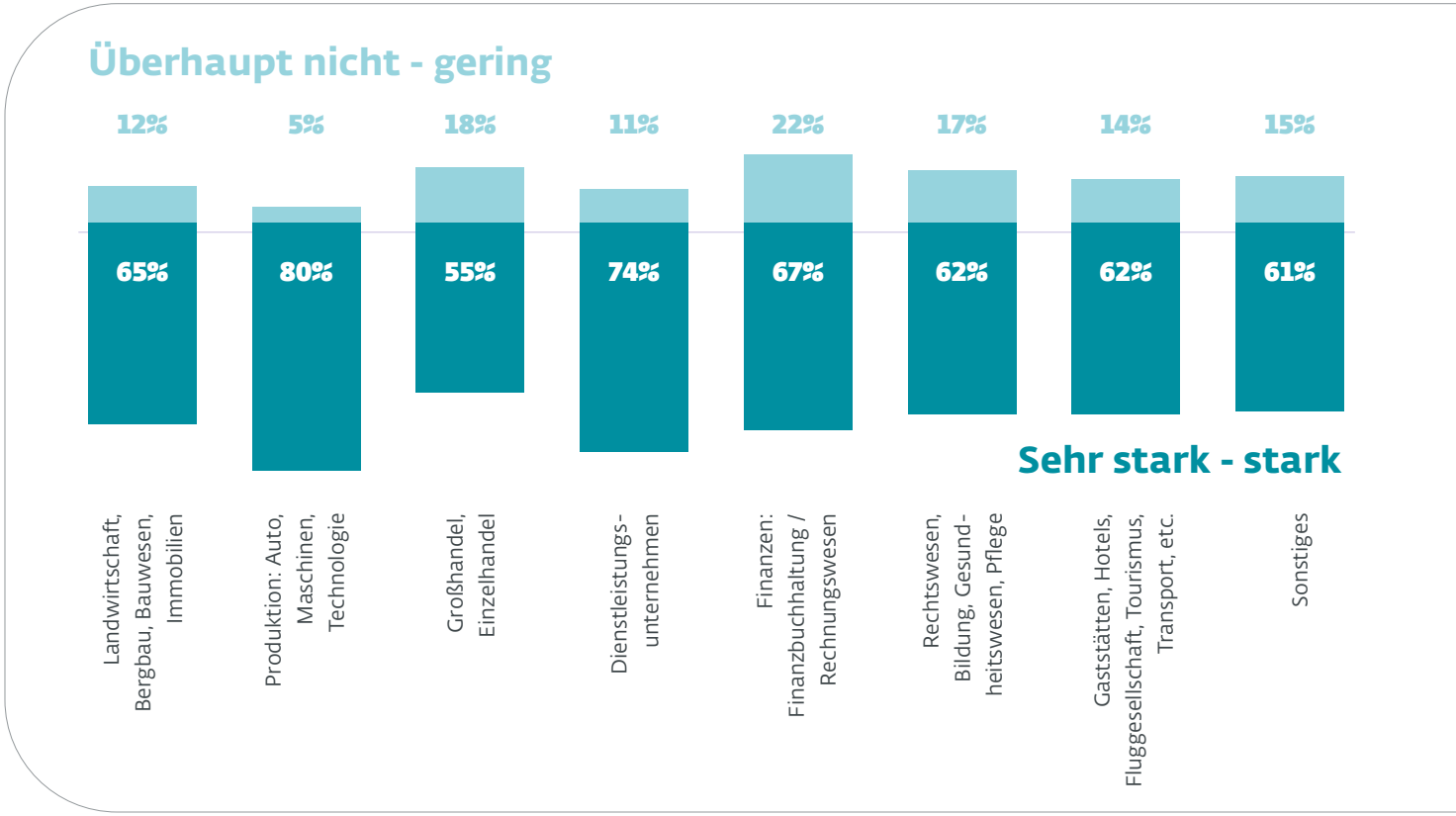
79%

der Entscheidungsträger mit mehr als 300 Mitarbeiter geben an, darauf großen Wert zu legen.

Bei den Branchen ist es wiederum das verarbeitende Gewerbe, das am stärksten auf die Region achtet (80 %) – Finanzunternehmen geben am häufigsten an, weniger Wert darauf zu legen (22 %). Ein Grund dafür könnte sein, dass viele Organisationen im Finance-Bereich international aufgestellt sind. Das heißt, eine europäische Lösung nimmt deshalb in diesem Sektor keinen so hohen Stellenwert ein wie bei anderen Branchen.

Es zeigt sich auch: Je höher die Position der Befragten, desto mehr wird auf die Herkunft geachtet. Fast vier von fünf Entscheidungsträgern (79 %) mit mehr als 300 Mitarbeitern geben an, darauf großen Wert zu legen.

Dass die meisten Unternehmen der Ursprungsregion ihrer IT-Sicherheitslösung viel Bedeutung beimessen, liegt sicherlich auch an den hohen Datenschutzstandards, die hiesige Hersteller vorweisen können. Bei einem europäischen Anbieter müssen sie sich um Datenschutz und Compliance keine Sorgen machen.



44%

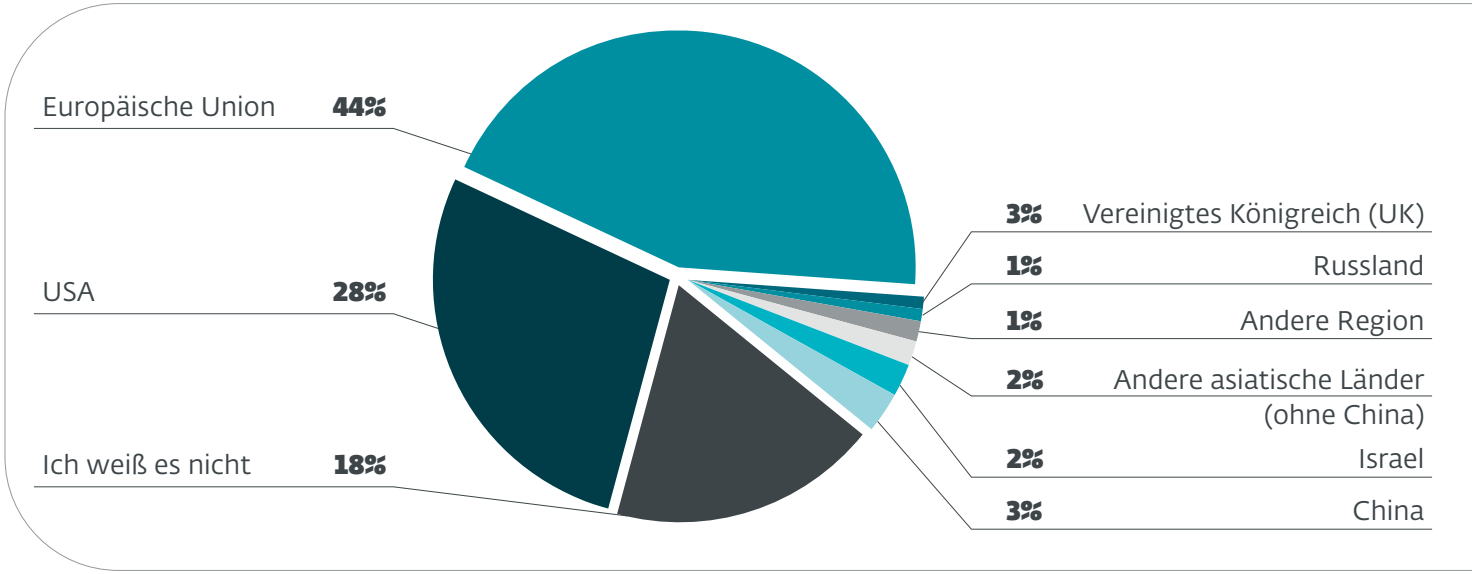
der Befragten nutzen bereits IT-Sicherheitsanbieter aus der EU

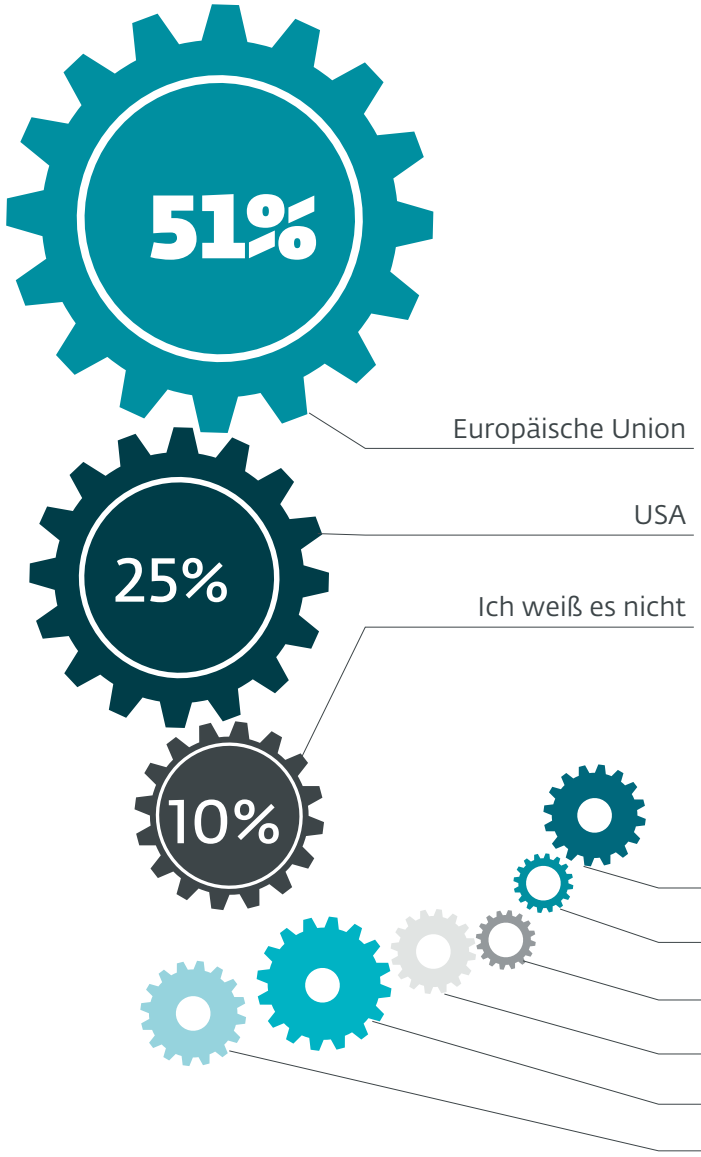
Frage 4: Aus welcher Region stammt der Hauptanbieter Ihrer aktuellen IT-Sicherheitslösung?

Hypothese: Wenn vielen Unternehmen die Herkunft wichtig ist, ist eine europäische Lösung bereits bei den meisten in Verwendung.

Ergebnis: Teilweise widerlegt

Die Wurzeln bei der IT-Sicherheit spielt für die meisten Organisationen eine entscheidende Rolle. Das zeigt die aktuelle Verteilung auf dem deutschen Markt: Befragt nach der Herkunft ihrer aktuellen IT-Sicherheitslösung gab knapp die Hälfte (44 %) an, auf EU-Hersteller zu setzen. An zweiter Stelle folgen die USA mit 28 Prozent. Andere Länder und Regionen wie Großbritannien, Asien und Russland spielen eine untergeordnete Rolle. Knapp jedes fünfte Unternehmen (18 %) konnte nicht sagen, woher es seine Lösung bezieht. Vor allem Einzelhandelsunternehmen und Großhändler wissen seltener, wo sie herkommt. Das könnte daran liegen, dass diese Unternehmen bei der Auswahl ihrer Lösung





eher auf die Spezifikationen der Lösung als auf ihre Herkunft achten. Allerdings ist das Ergebnis hier nicht eindeutig: Da 18 Prozent der Befragten nicht sagen konnten, woher ihre Lösung stammte, könnten mehr Unternehmen über eine europäische Lösung verfügen, ohne es zu wissen.

Kleine Unternehmen mit weniger als zehn Mitarbeitern verfahren bei der Auswahl ihrer Sicherheitslösungen nach dem Motto: Egal woher, Hauptsache es funktioniert. Hier wusste gut jeder dritte Befragte (34 %) nicht auf Anhieb, wo der Hersteller seiner Lösung beheimatet ist.

Der Grund hierfür ist offensichtlich: Besonders Großunternehmen achten darauf, ob der Hersteller von IT-Sicherheitslösungen unter dem gleichen Rechtsrahmen wie sie handelt. Lösungen, die datenschutzkonform und zuverlässig funktionieren, sind hier eindeutig im Vorteil. Denn je größer die Organisation ist, desto schwerer wiegt jeder Sicherheits- oder Datenschutzvorfall. Das zeigt sich auch in den Umfrageergebnissen: Fast die Hälfte der großen Organisationen (45 %) verlassen sich auf europäische Anbieter, bei kleineren Unternehmen bis 9 Mitarbeiter ist es nur ein knappes Drittel (31 %).

Am ehesten wissen Beschäftigte aus den Bereichen IT (50 %) sowie Produktion und Service (49 %), woher ihre IT Security stammt – unabhängig davon, wie groß ihr Unternehmen ist.

Branchenspezifisch zeigt sich, dass produzierende Unternehmen wie Automobil- und Maschinenbauer besonders häufig, und zwar gut jeder Zweite (51 %) auf IT-Sicherheitslösungen aus der EU setzen. Nur jeder Vierte (25 %) nutzt US-amerikanische Anbieter, andere Länder und Regionen sind marginal vertreten. Die Unternehmen dieser Branchen verfügen über viele wertvolle Informationen wie Produktions- und Forschungsdaten. Und Wirtschaftsspionage ist in diesem Bereich eine existenzbedrohende Gefahr, die in der Vergangenheit immer wieder vorgekommen ist – zum Teil sogar von offizieller Seite[5]. Für die produzierende Industrie ist es daher nur folgerichtig, bei einer so tief in die Systeme eingreifenden IT-Lösung auf europäische Anbieter zu setzen.

Darüber hinaus können Hersteller aus der Europäischen Union einen besseren Datenschutz gewährleisten als ihre außereuropäischen Konkurrenten. Es verbindet sie nicht nur ihre geografische Herkunft. Sie fühlen sich auch europäischen Werten stärker verpflichtet als Anbieter aus anderen Regionen.

5 www.fr.de/wirtschaft/betreiben-wirtschaftsspionage-11278668.html

Interview

Welchen Sinn ergibt es, **europäische Lösungen einzusetzen?**

Dr. Jens Eckhardt ist Fachanwalt für Informationstechnologierecht, Datenschutzauditor (TÜV) sowie IT-Compliance-Manager (TÜV) bei der Düsseldorfer Kanzlei pitc Legal Eckhardt Rechtsanwälte PartmbB. Im Gespräch mit Thorsten Urbanski, Director of Marketing bei ESET Deutschland GmbH erklärt er, warum es in der IT-Sicherheit Sinn ergibt, auf „Made in EU" zu setzen.

Thorsten Urbanski: **Warum ist der Begriff „Made in EU" im Cybersecurity-Kontext mehr als nur eine geografische Angabe?**

Dr. Jens Eckhardt: In der Cybersicherheit geht es nicht nur darum, woher eine Lösung stammt – sondern vor allem darum, welchem Rechtsrahmen sie originär unterliegt. Ein Anbieter mit Sitz in der EU unterliegt denselben Gesetzen wie seine Kunden – etwa der DSGVO, dem zukünftigen BSI-Gesetz oder der NIS2-Richtlinie. Das schafft Vertrauen, rechtliche Klarheit und Verlässlichkeit, insbesondere im Haftungsfall.

Thorsten Urbanski: **Gibt es aus juristischer Sicht konkrete Vorteile für Unternehmen, wenn sie auf europäische Anbieter setzen?**

Dr. Jens Eckhardt: Ja. Zum einen vermeiden sie zusätzliche Hürden wie Drittland-Transfers nach DSGVO oder unklare Zugriffsbefugnisse ausländischer Behörden, die nicht durch den EU-Rechtsrahmen gebunden sind. Anbieter und Anwender bewegen sich im gleichen Rechtsrahmen. Das bedeutet: Ein möglicher Rechtsstreit endet im Zweifel beim Europäischen Gerichtshof, dessen Entscheidungen beide Seiten unmittelbar binden. Das ist ein großer Vorteil gegenüber Anbietern aus außereuropäischen Rechtsordnungen.

Thorsten Urbanski: **Was ändert sich durch die neue EU-Security-Regulation für die Unternehmensverantwortung – gerade mit Blick auf aktuelle Regulierungen wie NIS2?**

Dr. Jens Eckhardt: Die Verantwortung der Geschäftsführung für IT-Sicherheit nimmt deutlich zu. Die NIS-2-Richtlinie verpflichtet das Leitungsorgan explizit zur Billigung und Überwachung von „Cybersicherheitsmaßnahmen". Gleichzeitig wird auch eine Schulungspflicht verankert. Das heißt: IT-Sicherheit ist kein technisches Randthema mehr, sondern eine zentrale Compliance- und Haftungsfrage auf Führungsebene.

Thorsten Urbanski: **Wie lautet Ihr Fazit in Bezug auf die Frage, ob „Made in EU" ein valides Auswahlkriterium für Cybersicherheitslösungen ist?**

Dr. Jens Eckhardt: Absolut. Unternehmen profitieren von Rechtssicherheit, Nachvollziehbarkeit und politischen Stabilitätsvorteilen. In einer Welt zunehmender geopolitischer Spannungen bietet „Made in EU" ein Maß an Vertrauen und Verlässlichkeit, das über technische Aspekte hinausgeht. Es ist eine strategische Entscheidung – sowohl für die Sicherheit als auch für die Unternehmensführung.

„Made in EU“ **schafft Vertrauen**

Den Ergebnissen dieser Studie zufolge genießt IT-Sicherheit „Made in EU“ bei deutschen Unternehmen einen hervorragenden Ruf und wird durchweg positiv bewertet. Auf die Frage, ob Unternehmen europäische Anbieter von Sicherheitslösungen bevorzugen sollten, um die Einhaltung der EU-Datenschutzstandards zu gewährleisten, bejahten sogar 80 Prozent. Die Zustimmung ist in allen Branchen und Tätigkeitsbereichen hoch.

Dies zeigt, dass „Made in EU“ im Zusammenhang mit IT-Sicherheit mehr bedeutet als Ortsverbundenheit. Es signalisiert zwar, dass IT-Sicherheitslösungen von Unternehmen stammen, die ihren Sitz haben, doch auch ein Großteil ihrer Wertschöpfung in der Europäischen Union liegt, die den strengen europäischen Datenschutz- und Sicherheitsstandards wie der DSGVO unterliegen.

> *„‚Made in EU‘ bedeutet nicht nur geografische Herkunft – es steht für gemeinsamen Rechtsrahmen, verbindliche Standards und digitale Souveränität“,*
>
> — Dr. Jens Eckhardt, Fachanwalt für IT-Recht.

Die wachsende Beliebtheit europäischer Produkte und Dienstleistungen ist nicht ausschließlich auf Datenschutz und Lokalpatriotismus zurückzuführen. Vielmehr sind es Anbieter aus der EU, die mit ihrer Technologie weltweit führend sind. Es wäre wünschenswert und wird durch die europäische Politik stärker forciert, dass regionale Hersteller bevorzugt eingesetzt werden. Denn nur mit einer digitalen Strategie, die „Made in EU“ priorisiert, ist wirkliche digitale Souveränität möglich.

Digitale Souveränität ist **ohne IT-Sicherheit „Made in EU“ unmöglich**

Digitale Souveränität bedeutet die Fähigkeit Europas zur selbstbestimmten Nutzung, Entwicklung und Kontrolle digitaler Technologien und Infrastrukturen auf Basis europäischer Werte, Gesetze und Sicherheitsstandards. Sie setzt voraus, dass Staaten, Unternehmen und Institutionen unabhängig von außereuropäischen Anbietern agieren können, insbesondere im Bereich der IT-Sicherheit. Digitale Souveränität kann nur durch starke, vertrauenswürdige IT-Sicherheitslösungen „Made in EU“ gewährleistet werden. Der Ukraine-Konflikt zeigt eines deutlich: Eine staatliche Autonomie ist die Voraussetzung dafür, dass Wirtschaft, Gesundheitswesen und unsere Gesellschaft handlungsfähig sind und bleiben. Was einfach klingt, ist heute keinesfalls selbstverständlich. Denn überall dort, wo die IT-Security nicht auf höchstem Niveau und frei von politischen Restriktionen agiert, gerät die digitale Souveränität ins Straucheln.

Das spricht für „Made in EU“

Mit der fortschreitenden Digitalisierung steigt der Komplexitätsgrad von IT-Systemen und IT-Infrastrukturen. Dadurch wird es für Unternehmen und Privatanwender immer schwieriger, einzelne IT-Sicherheitslösungen und deren Hintergründe zu verstehen und zu bewerten. Diese Entwicklung führt zu einer Verunsicherung der Menschen. Die Experten von ESET sensibilisieren unter dem Motto „IT-Sicherheit ist Vertrauenssache“ Organisationen wie Privatanwender zum Thema IT-Schutz Made in EU und engagieren sich für die Förderung der digitalen Souveränität. Seit über drei Jahrzehnten steht das Unternehmen für professionelle Schutztechnologien, die höchsten technischen, rechtlichen und ethischen Standards entsprechen.

Für diese Werte steht ESET als europäischer IT-Sicherheitshersteller:

- **Datenschutz und Compliance:** Als Unternehmen mit Hauptsitz in der EU ist ESET verpflichtet, die strengen Datenschutzstandards der Europäischen Union, einschließlich der DSGVO, zu erfüllen. Ihre Daten sind bei uns in sicheren Händen – das ist mehr als nur eine gesetzliche Regelung, der wir folgen, es ist eine Garantie, die wir allen Nutzern geben.
- **Vertrauenswürdigkeit und Transparenz:** Angesichts immer ausgeklügelter Angriffe müssen Sie genau wissen, wem Sie Ihre Sicherheit anvertrauen. ESET steht für Transparenz, offene Kommunikation und eine klare Haltung gegen Backdoors und versteckte Zugänge. Ihre Sicherheit ist bei uns keine Frage des Vertrauens – es ist eine Frage der Überzeugung.
- **Geopolitische Stabilität:** In unserer vernetzten Welt kann die Wahl eines europäischen Anbieters den Unterschied ausmachen. ESET trägt zur digitalen Souveränität Europas bei und schützt kritische Infrastrukturen vor ungewollten externen Einflüssen. Sie stärken nicht nur Ihr Unternehmen, sondern auch die digitale Sicherheit Europas.

ESET war 2020 eines der ersten Unternehmen, das sich der TeleTrusT-Initiative „IT Security Made in EU“ anschloss. Mit der Unterzeichnung der freiwilligen Konformitätserklärung setzen wir ein klares Zeichen für unser Engagement im Bereich Datenschutz und vertrauenswürdiger IT-Sicherheitstechnologien.

✓ Als Mitglied der Initiative erfüllt ESET die fünf Kriterien, um das Siegel führen zu dürfen:

✓ 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

Trust Seal
www.teletrust.de/itsmie

So hilft ESET
Unternehmen bei der IT-Sicherheit

IT Security Made in EU: Mehr als nur ein Label

Als europäischer Cybersicherheitsanbieter steht ESET seit über drei Jahrzehnten für professionelle Schutztechnologien, die höchsten technischen, rechtlichen und ethischen Standards entsprechen.

Datenschutz, Transparenz, offene Kommunikation und eine klare Haltung gegen Backdoors und versteckte Zugänge – wir von ESET entwickeln Schutz ohne Kompromisse.

Sicherheit ohne geopolitisches Risiko
Unsere Technologien entstehen in Europa. So trägt ESET zur digitalen Souveränität bei und schützt Wirtschaft, Behörden und Privatanwender vor ungewollten externen Einflüssen.

In Europa verwurzelt, weltweit im Einsatz
5 europäische Standorte mit starkem Netzwerk aus Partnern, Managed Service Providern und Distributoren, 8 Forschungs- & Entwicklungszentren in der EU und 100 % unabhängig.

Eigenes Rechenzentrum und Security Operations Center in Deutschland
Wer höchste Anforderungen an Datenschutz stellt, setzt auf unsere Rechenzentren und SOCs in Deutschland und der EU – mit Kerntechnologien, die lokal betrieben werden.

Ihre Daten bleiben in der EU
Wir von ESET kennen den gesetzlichen Rahmen, in denen sich unsere Kunden bewegen (müssen). Alle Daten werden innerhalb der EU gespeichert und verarbeitet, nach deutschem Datenschutzrecht und ohne Umwege über Drittstaaten.

Wir l(i)eben ein hohes Sicherheitsniveau
NIS2 und DSGVO: Als europäisches Unternehmen verstehen wir die EU-Regularien nicht nur, wir leben sie. Unser Team unterstützt unsere Kunden bei deren Umsetzung.

Eine No-Backdoor-Garantie ist für uns selbstverständlich – denn: Als IT-Sicherheitshersteller aus der EU stehen wir zu 100 % hinter den demokratischen Werten der europäischen Union.
— Holger Suhl, Country Manager DACH, ESET Deutschland GmbH

IT-Sicherheit auf dem Stand der Technik, **„Made in EU“**

Im Zuge der Umsetzung dieser Anforderungen an Unternehmen gewinnt auch das Qualitätssiegel „Made in EU“ zunehmend an Bedeutung: IT-Sicherheitslösungen aus der Europäischen Union stehen nicht nur für hohe technische Standards, sondern erfüllen in der Regel auch strenge Datenschutz- und Compliance-Vorgaben. Die Kombination aus technologischem Fortschritt und europäischen Werten stärkt das Vertrauen in die IT-Sicherheit und macht den „Stand der Technik“ zu einem strategischen Erfolgsfaktor für Unternehmen innerhalb der EU.

Darüber hinaus werden mit Inkrafttreten der NIS2-Richtlinie viele Unternehmen strengere Auflagen in ihrer IT-Sicherheit erfüllen müssen. Wie eingangs bereits erwähnt, ein Begriff, der in diesem Zusammenhang immer wieder fällt, ist der „Stand der Technik“. Dabei handelt es sich um einen unbestimmten Rechtsbegriff: Der Gesetzgeber umgeht hiermit die Notwendigkeit, die Regelung ständig neu überarbeiten zu müssen, z. B. wenn sich ein Sachverhalt geändert oder die Technik weiterentwickelt hat. Die Sicherheit von Unternehmen muss sich dabei an zwei weiteren unbestimmten Rechtsbegriffen orientieren: dem Stand der Wissenschaft und Forschung sowie allgemein anerkannten Regeln der Technik.

Der Stand der Technik bezeichnet keine optionale Empfehlung, sondern eine verbindliche Anforderung, die sich aus Gesetzen wie der DSGVO oder der NIS-2-Richtlinie ableitet. Für die IT-Sicherheit bedeutet das konkret: Organisationen müssen angemessene organisatorische und technische Maßnahmen treffen, um dem Stand der Technik zu entsprechen.

Mehr Informationen zum Thema „Stand der Technik“ lesen sie in diesem Whitepaper. ↗Jetzt herunterladen.

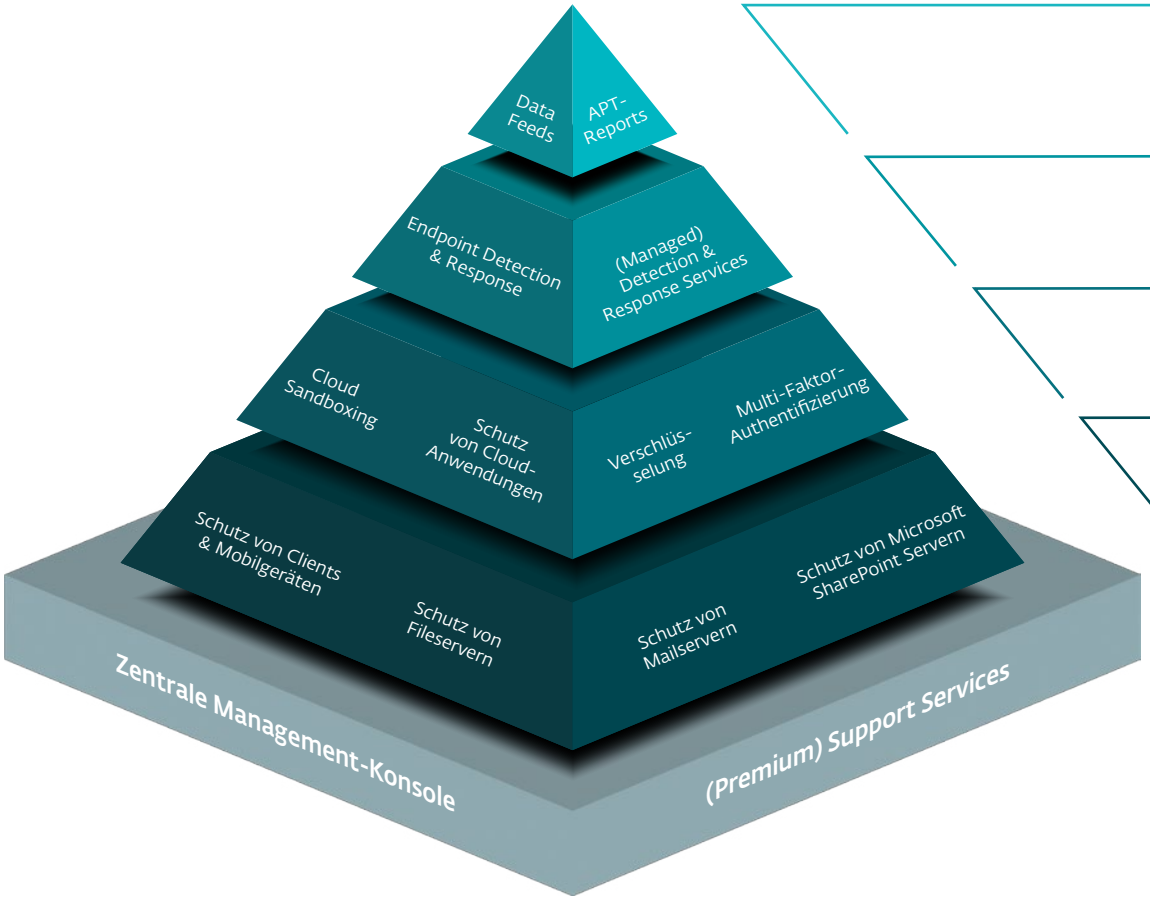
Konkrete Handelsempfehlungen

- **Vorbereitet sein:** Unternehmen für den Worst Case einen Notfallplan in der Hinterhand haben, um den Betrieb aufrechtzuerhalten. Dazu gehört auch ein umfassendes Backup-Management, Wiederherstellungsmaßnahmen nach einem Notfall sowie eine passende Cyberversicherung.
- **Up-to-date sein:** Eine zentrale Management-Konsole hilft IT-Teams dabei, den Überblick zu den aktuellen (Versions-)Status von Clients, Servern und Mobilgeräten zu behalten. Außerdem können Updates hiermit automatisiert ausgerollt werden. Ein Patch & Vulnerability-Management rundet das Paket ab.
- **Datenhoheit behalten:** Datacenter sollten ausschließlich lokal oder in der EU liegen, um den höchstmöglichen Sicherheitsstandards zu entsprechen. So behalten Unternehmen die Kontrolle über ihre Daten.
- **Ausreichenden Datenschutz realisieren:** Personenbezogene Daten genießen seit Inkrafttreten der DSGVO einen besonderen Schutz. Unternehmen, die sie verarbeiten, müssen deshalb entsprechende Maßnahmen treffen, um sie vor unberechtigtem Zugriff zu bewahren. Dazu gehört beispielsweise eine sichere Verschlüsselung auf Endgeräten.
- **Budget einplanen:** Entscheider sollten für ihre Sicherheitslösungen Kosten einplanen. Auf diese Weise sinkt die Wahrscheinlichkeit für Produktionsausfälle und damit einhergehende Folgeschäden.
- **Vertrauen? Zero.** Mitarbeiter sollten nur Zugriff auf die Daten erhalten, die sie wirklich für ihre tägliche Arbeit benötigen. Solche Zero-Trust-Konzepte bieten zudem eine Orientierungshilfe, wie man das eigene Netzwerk unter Berücksichtigung individueller Anforderungen optimal schützen kann.

Besonders der letzte Punkt ist für die IT-Sicherheit von Organisationen sehr wichtig. Das Zero Trust-Konzept von ESET besteht aus einem dreistufigen, aufeinander aufbauenden Reifegradmodell. Je höher die Stufe ist, desto sicherer ist die Schutzwirkung – also „reifer“. Ob als Standardlösung oder Managed Service – die Kombination aus Endpoint Security, Verschlüsselung, Multi-Faktor-Authentifizierung, Cloud Sandboxing und Schutz für Cloud-Anwendungen bildet dabei das richtige Fundament für Zero Trust – nicht nur, um dem Stand der Technik zu entsprechen, sondern auch, um so gut wie möglich vor Cyberbedrohungen geschützt zu sein.

Eine aktuelle Umfrage von ESET bestätigt, wie wichtig das Zero-Trust-Konzept von ESET zur Verbesserung des Stands der Technik in Organisationen ist: Fast 95 Prozent geben an, dass das Modell ihnen beim Erreichen des Stands der Technik hilft. Allerdings ist laut eigener Aussage nur knapp jeder Dritte (31 %) finanziell und personell gut aufgestellt – bei knapp 29 Prozent mangelt es trotz passender Finanzen und vorhandenem Personal an Qualifizierung bzw. Weiterbildungen. Hier besteht für die Zukunft noch Handlungsbedarf.

EINSATZBEREICH



SCHUTZLEVEL

GANZHEITLICHES LAGEBILD – AUSSENSICHT

Stufe 3: Bietet tiefe Einblicke in die globale Bedrohungslandschaftals Grundlage für einen SOC-/SIEM-Betrieb

GEFAHRENSUCHE UND ABWEHR – INNENSICHT

Stufe 2: Gewährleistet die Wirksamkeit der IT-Sicherheit mittels Anomalieerkennung, 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 bietet Informationssicherheit **für Unternehmen jeder Größe**

Qualitätsmanagement – Made in EU:

- Überall verfügbar – vollautomatischer Schutz der gesamten Organisation
- Volle Kontrolle über Ihre Daten dank transparenter (Sample-)Analysen innerhalb der EU
- Einzigartige Geschwindigkeit bei der Analyse von eingehenden Warnmeldungen
- Zuverlässig und sicher – alle Anforderungen von Datenschutzbestimmungen (bspw. DSGVO) bequem erfüllen
- Große Flexibilität in puncto Lizenzform, Hardwareeinsatz und Anforderungen an die Infrastruktur

Vorteile für Unternehmen:

- Passgenaue IT-Sicherheit für alle Unternehmensgrößen und -anforderungen
- Mitarbeiter entlasten und (Hardware-) Ressourcen schonen
- Compliance und Sicherheitsstandards erweitern
- Verwaltung der Schutzlösungen für alle gängigen Betriebssysteme via ESET PROTECT (Cloud oder On-Premises)
- Lizenzvielfalt – Kombination beliebiger Betriebssysteme (Windows, macOS, Linux) und Geräte (Clients, Server, Mobilgeräte) entsprechend der Bedürfnisse

„Als Security-Hersteller bieten wir moderne Lösungen, Dienstleistungen und Konzepte an, mit denen Unternehmen und Verwaltungen eine Cyber-Resilienz auf höchstem Niveau gestalten können."

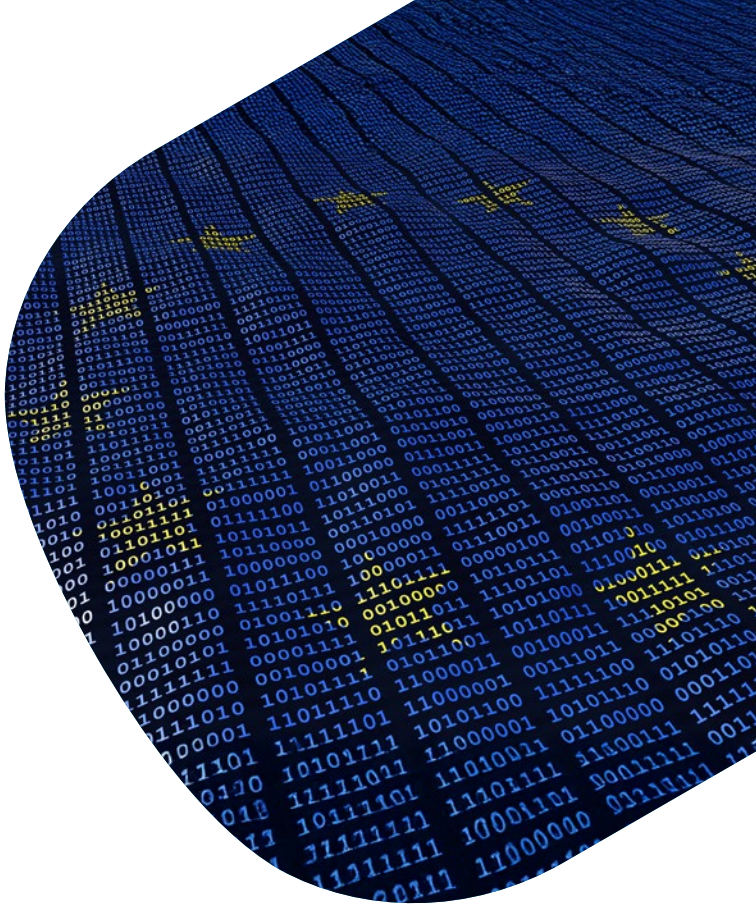
— Holger Suhl, Country Manager DACH,
ESET Deutschland GmbH

Fazit

Die aktuelle Studie beleuchtet eindrucksvoll, wie sich Sicherheitsbewusstsein und Vertrauen von Unternehmen in Europa angesichts geopolitischer Umbrüche, wachsender Cyberbedrohungen und regulatorischer Anforderungen wandeln. Im Zentrum steht dabei die Frage: Wer schützt unsere digitalen Werte – und unter wessen Rechtsrahmen?

Die Ergebnisse zeigen eine eindeutige Tendenz: Immer mehr deutsche Unternehmen ziehen IT-Sicherheitslösungen „Made in EU" in Betracht – und das nicht nur aus patriotischen Motiven, sondern aus handfesten Gründen. Rund 75 Prozent der wechselwilligen Unternehmen bevorzugen europäische Anbieter. Auch die Herkunft des Anbieters spielt für zwei Drittel aller Befragten eine wichtige oder sehr wichtige Rolle.

Diese Entwicklung ist Ausdruck eines grundlegenden Wandels. Unternehmen erkennen zunehmend, dass digitale Souveränität nicht allein technologische, sondern auch rechtliche und ethische Dimensionen hat. Europäische IT-Sicherheitsanbieter bieten gegenüber außereuropäischen Lösungen den Vorteil eines einheitlichen und strengen Datenschutzrechts (insbesondere der DSGVO), klarer Haftungsregeln und einer transparenten Unternehmenspraxis – inklusive „No Backdoor"-Garantie. Gerade im Lichte der Erfahrungen mit kritischen Infrastrukturen in Kriegs- und Krisensituationen wird deutlich, wie schnell technische Systeme zu geopolitischen Spielbällen werden können. Die wachsende Verunsicherung gegenüber außereuropäischen Herstellern, insbesondere aus den USA oder Asien, beruht auf realen Risiken: Fernwartungsmöglichkeiten, politische Einflussnahme oder intransparente Datenverarbeitung stehen zunehmend im Widerspruch zu den Sicherheits- und Compliance-Zielen europäischer Unternehmen. Die Befürchtung, dass auch IT-Sicherheitslösungen „ferngesteuert" deaktiviert oder kompromittiert werden könnten, ist längst kein abstraktes Szenario mehr – sie ist für viele Entscheider eine reale Bedrohungslage.



IT-Sicherheitslösungen „Made in EU“ sind weit mehr als eine geografische Herkunftsbezeichnung – sie stehen für Rechtsklarheit, Compliance-Sicherheit und digitale Souveränität. Europäische Anbieter wie ESET unterliegen denselben Datenschutz- und Sicherheitsstandards wie ihre Kunden und vermeiden dadurch juristische Unsicherheiten, die etwa durch Drittland-Transfers oder fremde Zugriffsbefugnisse entstehen könnten. Die steigenden regulatorischen Anforderungen, insbesondere durch die NIS2-Richtlinie, verlangen eine Orientierung am „Stand der Technik“. Europäische Lösungen bieten hier nicht nur technische Exzellenz, sondern auch rechtliche Verlässlichkeit und politische Stabilität – ein entscheidender Vorteil in Zeiten geopolitischer Spannungen. Das Zero-Trust-Modell von ESET hilft Unternehmen, ihre IT-Sicherheit auf den Stand der Technik zu bringen.

Das Vertrauen in IT-Sicherheit „Made in EU“ fußt nicht zuletzt auf Transparenz, Datenschutzverpflichtung und der konsequenten Ablehnung versteckter Zugänge. Für Unternehmen bedeutet dies: Wer in europäische Sicherheitslösungen investiert, stärkt nicht nur die eigene IT-Abwehr, sondern auch den Schutz kritischer Infrastrukturen und die Handlungsfähigkeit der gesamten Gesellschaft.

Über ESET

Als europäischer Hersteller mit mehr als 30 Jahren Erfahrung bietet ESET ein breites Portfolio an Sicherheitslösungen für jede Organisationsgröße. Wir schützen betriebssystemübergreifend sämtliche Endpoints und Server mit einer vielfach ausgezeichneten mehrschichtigen Technologie und halten Ihre Infrastruktur mithilfe von Cloud Sandboxing frei von Zero-Day-Bedrohungen. Mittels Multi-Faktor-Authentifizierung und zertifizierter Verschlüsselungslösungen unterstützen wir Sie bei der Umsetzung von Datenschutzbestimmungen sowie Compliance-Maßnahmen.

Unsere Endpoint Detection and Response-Lösung, dedizierte Services wie z.B. Managed Detection and Response und Frühwarnsysteme in Form von Threat Intelligence ergänzen das Angebot im Hinblick auf Incident Management sowie den Schutz vor gezielter Cyberkriminalität und APTs. Dabei setzt ESET nicht allein auf modernste KI-Technologie, sondern kombiniert Erkenntnisse aus der cloudbasierten Reputationsdatenbank ESET LiveGrid® mit Machine Learning und menschlicher Expertise, um Ihnen den besten Schutz zu gewährleisten.

ESET Deutschland GmbH
Spitzweidenweg 32
07743 Jena
Tel.:+49 3641 3114 200

3 VON ÜBER 500.00 ZUFRIEDENEN KUNDEN

BVB 09 CHAMPION PARTNER

Seit 2019 ein starkes Team
auf dem Platz und digital

Allianz Suisse

Seit 2016 durch ESET geschützt
Mehr als 4.000 Postfächer

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur|Ty made in EU
Trust Seal
www.teletrust.de/itsmie

ESET wurde das Vertrauenssiegel
„IT Security made in EU" verliehen

SYSTEM CERTIFICATION ISO 9001 SGS
SYSTEM CERTIFICATION ISO/IEC 27001 SGS

Unsere Lösungen sind nach den Qualitäts- und
Informationssicherheitsstandards ISO 9001:2015
und ISO/IEC 27001:2013 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

500.000+
Geschützte Unternehmen

178
Länder & Regionen

11
Forschungs- und Entwicklungszentren weltweit