POSITIONSPAPIER

Made in EU
IT-Sicherheit und Digitale Souveränität

Cybersecurity
Progress. Protected.

Inhaltsverzeichnis

Autor: Michael Klatte, ESET Deutschland GmbH

Stand: Juni 2025

Cybersecurity
Progress. Protected.

Digitale Souveränität ist kein abstraktes politisches Ziel.

Sie ist eine Grundvoraussetzung für Sicherheit, Wettbewerbsfähigkeit und Innovation in Europa. Wer diese Kontrolle nicht hat, riskiert nicht nur Datenverlust, sondern auch den Verlust seiner technologischen Selbstbestimmung.

Executive Summary

Positionspapier IT-Sicherheit & Digitale Souveränität

Europa steht an einem Wendepunkt: Wer die Kontrolle über Daten und digitale Infrastrukturen verliert, gibt ein Stück seiner wirtschaftlichen und politischen Unabhängigkeit preis. Globale Spannungen und gezielte Cyberangriffe zeigen täglich, wie verwundbar selbst große Unternehmen und Institutionen sind.

Stellen Sie sich vor: Ihre Sicherheitssoftware schützt nicht nur Ihre Systeme, sondern liefert Informationen an Behörden im Ausland. Oder ein Update verändert plötzlich Funktionen, weil politische Interessen im Spiel sind. Genau hier beginnt digitale Souveränität.

Unser Positionspapier erklärt, warum IT-Sicherheitslösungen „Made in EU“ weit mehr bedeuten als Datenschutz. Sie sind der Schlüssel zu Resilienz und Unabhängigkeit. Es beschreibt, welche Gesetze wie NIS2, DORA, der Cyber Resilience Act oder der CLOUD Act die Spielregeln bestimmen und welche Risiken entstehen, wenn Unternehmen auf außereuropäische Anbieter setzen.

Am Beispiel des europäischen Sicherheitsanbieters ESET wird aufgezeigt, wie europäische Sicherheitslösungen Vertrauen schaffen: durch klare Herkunft, transparente Technologien, eigene Forschung in der EU und Dienstleistungen wie Prävention („Prevention First“), Managed Detection and Response oder Threat Intelligence.

Entscheider in Politik, Verwaltung und Wirtschaft erhalten damit einen strategischen Überblick über aktuelle Herausforderungen, regulatorische Anforderungen und praktikable Wege zur Stärkung der europäischen IT-Sicherheit.

Unser Appell: Prüfen Sie, wem Sie in Sachen IT-Sicherheit vertrauen. Denn digitale Souveränität bedeutet: selbst entscheiden anstatt fremdbestimmt handeln zu müssen.

1. Digitale Souveränität

Kontrollverlust oder Selbstbestimmung in der vernetzten Welt?

Stellen Sie sich vor, eine Behörde muss im Ernstfall schnell handeln. Doch plötzlich erscheint auf ihrem Bildschirm eine Fehlermeldung: „Service unavailable – vendor policy restrictions apply." Dann wird klar: Jemand anders kontrolliert das System. Das ist kein Science-Fiction-Szenario. In modernen Hightech-Systemen gibt es sogenannte „Kill Switches", mit denen Hersteller Geräte aus der Ferne abschalten können. Wer Technik nutzt, über die er keine volle Kontrolle hat, gibt damit auch ein Stück seiner Handlungsfähigkeit ab.

Digitale Souveränität bedeutet, diese Kontrolle zu behalten. Es geht nicht nur um Datenschutz, sondern um die Freiheit, im Ernstfall selbst Entscheidungen zu treffen. Ob in der Verteidigung, bei kritischen Infrastrukturen oder in der Verwaltung sensibler Daten. Überall stellt sich dieselbe Frage: Wer hat letztendlich die Kontrolle?

Nehmen wir ein Beispiel: Wer in Deutschland online seinen Personalausweis beantragt, kann davon ausgehen, dass seine Daten nach europäischen Datenschutzvorgaben sicher verarbeitet werden. Doch steckt hinter der Software ein außereuropäischer Anbieter oder liegen die Server außerhalb der EU, wird es kompliziert. Dann greifen oft Gesetze wie der US Cloud Act. Das heißt: Behörden könnten verpflichtet werden, Zugriff auf diese Daten zu gewähren. Und das ohne deutsche Gerichtsbeschlüsse.

Dazu kommt: Wer auf ausländische Anbieter setzt, ist auch bei Updates und Sicherheitslücken abhängig. Wenn der Hersteller nicht liefert, kann die Verwaltung oft nichts tun. Und im schlimmsten Fall weiß niemand, ob es versteckte Hintertüren im Code gibt. Manipulation, Spionage oder Erpressung sind reale Risiken, die oft unbemerkt bleiben.

Genau deshalb heißt digitale Souveränität, eigene Gestaltungsspielräume rechtlich, organisatorisch und technisch zu schaffen. Systeme müssen nachvollziehbar sein, überprüfbar und frei von ungewollten Zugriffen. Sicherheitslösungen sollten europäischen Werten entsprechen. Nur so lassen sich Datenschutz, Transparenz und Unabhängigkeit wirklich umsetzen.

IT-Sicherheit ist keine technische Nebensache. Sie ist der Schlüssel zur digitalen Selbstbestimmung. Wer seine Systeme schützt, behält die Kontrolle über seine digitale Zukunft.

IT-Sicherheit bildet das Rückgrat dieser Souveränität. Staaten, Unternehmen und öffentliche Einrichtungen müssen wissen, wer hinter der eingesetzten Technologie steht. Nur dann lässt sich Vertrauen aufbauen. Europäische Sicherheitslösungen bieten diese Transparenz. Im Unterschied zu Blackbox-Systemen aus Drittstaaten zeigen sie offen, wie ihre Technologie funktioniert.

ESET bringt es auf den Punkt. In einem Blogartikel von 2022 heißt es: „Wir entwickeln alle Kerntechnologien zu 100 Prozent in der EU. Ohne Backdoors, ohne Datenabfluss, ohne Kompromisse." Damit zeigt ESET, worauf es wirklich ankommt: modernste Sicherheitslosungen, die europaische Werte wie Datenschutz, Transparenz und Unabhangigkeit in der Praxis umsetzen. Dazu gehört auch das Prinzip „Prevention First". Es erkennt Angriffe frühzeitig und stoppt sie, bevor sie Schaden anrichten können. In Verbindung mit Diensten wie Managed Detection and Response entsteht so ein praxisnahes Modell für digitale Souveränität, das in Europa entwickelt, betrieben und verantwortet wird.

2. IT-Sicherheit „Made in EU“
Warum dies mehr als ein Gütesiegel ist

Das Gütesiegel „Made in EU“ genießt weltweit und natürlich auch in Deutschland einen hohen Stellenwert. Dies bestätigt eine ↗neue repräsentative Umfrage von ESET. Darin wurde untersucht, welchen IT-Herstellern deutsche Unternehmen noch vertrauen. Denn die aktuelle geopolitische Lage lässt diese Frage zu Recht aufkommen. Viele Organisationen sorgen sich, dass die technologische Abhängigkeit in nicht funktionierendem Schutz resultiert.

Was hilft die beste Security-Lösung, wenn der Hersteller beispielsweise Updates verzögert, bewusst Malware übersieht oder ganz einfach den Dienst einstellt. Es zeigt sich: 75 Prozent der deutschen Unternehmen wollen bei der Auswahl ihrer Schutzlösung auf einen Hersteller aus der Europäischen Union setzen. Und sogar knapp die Hälfte zieht einen Wechsel ihrer IT-Sicherheitslösung schon in Betracht.

Die Studie zeigt, dass sich Unternehmen längst mit der Herkunft ihrer IT-Sicherheitslösung beschäftigen. Mehr denn je müssen Organisationen in Deutschland entscheiden, ob sie ihre wertvollen Daten in die Hände außereuropäischer Anbieter geben wollen. Die IT-Sicherheit ist einer der wichtigsten Bereiche eines Unternehmens und sollte deswegen in die Hände von Anbietern gelegt werden, die dem europäischen Wertekanon und dem hiesigen strengen Datenschutz folgen.

Der Status quo in Deutschland

Befragt nach der Herkunft ihrer IT-Sicherheitslösung gab knapp die Hälfte (44 Prozent) an, auf einen Anbieter aus der EU zu vertrauen. Gut ein Viertel (28 Prozent) nutzt Hersteller aus den USA. Andere Länder und Regionen wie beispielsweise Israel, das Vereinigte Königreich und Asien sind kaum vertreten. Auf die einzelnen Branchen heruntergebrochen zeigt sich: Insbesondere die deutsche Industrie (51 Prozent) setzt auf EU-Produkte. Eine mögliche Erklärung hierfür: Die deutsche Industrie verfügt über große Mengen kritischer Daten. Europäische IT-Sicherheitslösungen bieten für diese Informationen einen ausgezeichneten Datenschutz.

Herkunft ist wichtig: Unternehmen sind wechselbereiter

Generell geben zwei Drittel (67 Prozent) der Befragten an, ihnen sei die Herkunft ihrer IT-Sicherheitslösung wichtig. Fast die Hälfte (44 Prozent) ziehen nach den jüngsten Spannungen zwischen den USA und Europa einen Herstellerwechsel in Betracht. Größere Unternehmen ab 250 Mitarbeitern wollen eher umsteigen als kleinere Organisationen.

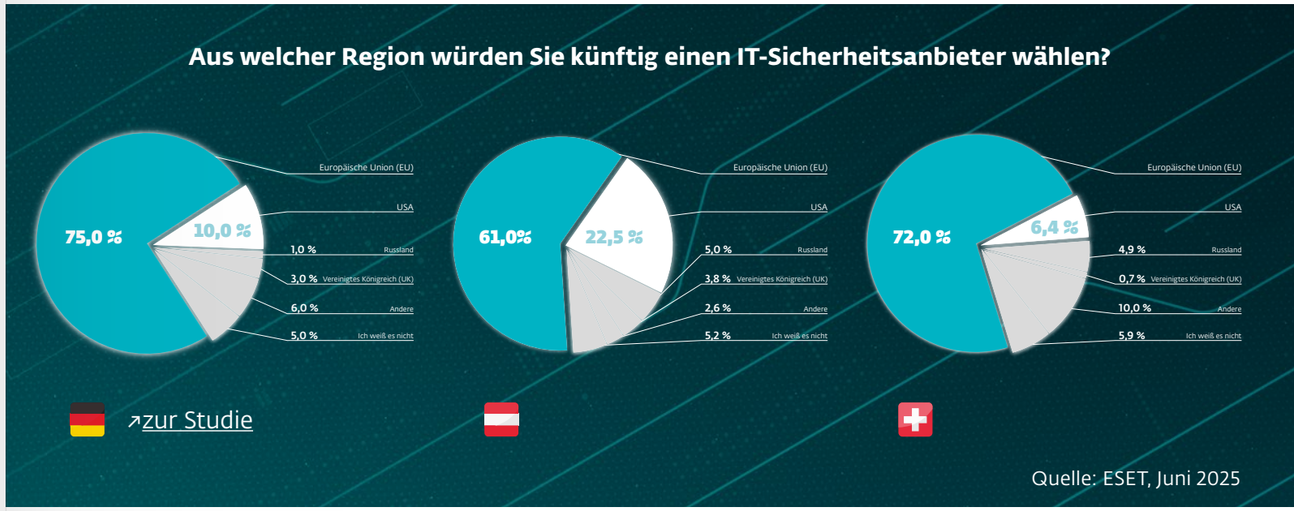
Besonders Großunternehmen achten darauf, ob der Hersteller von IT-Sicherheitslösungen unter dem gleichen Rechtsrahmen wie sie handelt. Lösungen, die datenschutzkonform und zuverlässig funktionieren, sind hier eindeutig im Vorteil. Denn je größer die Organisation ist, desto schwerer wiegt jeder Sicherheits- oder Datenschutzvorfall.

Steigende Nachfrage bei europäischen IT-Sicherheitsherstellern

Diejenigen, die wechseln wollen, kennen dabei nur eine Richtung: Zurück nach Europa. Drei Viertel (75 Prozent) der Wechselwilligen zieht es branchenübergreifend hin zu EU-Anbietern. Datenschutzstandards spielen dabei eine entscheidende Rolle. Der Aussage, dass Unternehmen europäische Anbieter von IT-Sicherheitslösungen bevorzugen sollten, um hiesigen Datenschutzstandards zu genügen, stimmten vier von fünf Befragten zu.

„Hersteller aus der Europäischen Union können besseren Datenschutz gewährleisten als ihre außereuropäischen Mitbewerber. Cybersicherheitsanbieter aus der EU verbindet nicht nur ihre geografische Herkunft. Sie fühlen sich den europäischen Werten stärker verpflichtet als Anbieter aus anderen Regionen.“

— so Thorsten Urbanski, Director of Marketing bei ESET Deutschland.



Datenschutz „Made in EU“ ist Pflicht und keine Kür

Angesichts dieser sich rasant verändernden globalen Gemengelage wird insbesondere im Bereich der IT-Sicherheit der Ruf nach mehr europaischer Eigenstandigkeit lauter.

Die EU verfügt auf diesem Gebiet über starke Technologieführer. Deren Potenzial sollte nun gezielt genutzt und weiter ausgebaut werden.

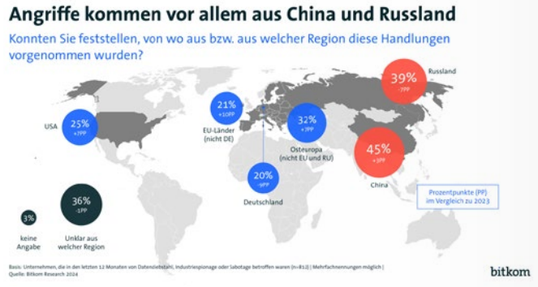
In Zeiten wachsender Bedrohungen im Cyberraum ist digitale Souveränität ein zentraler Pfeiler der Verteidigungsfähigkeit. Die ersten Schritte auf diesem Weg wurden bereits gemacht: Das EU-Programm „↗ReArm Europe“ setzt genau hier an, indem es die Verteidigung der Region stärken soll. Dazu gehört explizit auch die Cybersicherheit als integraler Bestandteil.

3. Aktuelle Bedrohungslage
Daten und Statistiken zu Cyberangriffen in Europa

Die Bedrohungslage im Cyberraum ist alarmierend. Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) bleibt die ↗IT-Sicherheitslage in Deutschland angesichts zunehmender Bedrohungen weiterhin besorgniserregend. Ähnliche Tendenzen zeigen sich europaweit: Cyberangriffe auf Unternehmen und öffentliche Einrichtungen nehmen kontinuierlich zu und werden immer ausgefeilter. Laut dem aktuellen ↗ENISA Threat Landscape Report 2024 haben sich gezielte Ransomware-Kampagnen, Advanced Persistent Threats (APT)-Aktivitäten und Lieferkettenangriffe weiter intensiviert. Besonders europäische KRITIS-Betreiber stehen im Fokus staatlich unterstützter Hacker-Gruppen.

Neben klassischen Cybercrime-Gruppen treten zunehmend staatlich unterstützte APT-Akteure in den Vordergrund. Diese kombinieren Industriespionage, Sabotage und psychologische Operationen gegen öffentliche Einrichtungen, kritische Infrastrukturen und Unternehmen in der EU – mit dem Ziel, Vertrauen zu untergraben und wirtschaftliche Schäden zu verursachen.

Eine Studie des ↗Digitalverbands Bitkom verdeutlicht das Ausmaß: In den vergangenen 12 Monaten waren 81 Prozent der deutschen Unternehmen Opfer von Datendiebstahl, Spionage oder Sabotage. Das ist ein neuer Höchstwert (2013 waren es 72 Prozent). Die dadurch entstandenen Schäden summierten sich 2024 auf rund 266,6 Milliarden Euro, ein Anstieg um 29 Prozent gegenüber dem Vorjahr. Besonders auffällig ist, dass viele Angriffe auf ausländische Urheber zurückzuführen sind: 45 Prozent der betroffenen Unternehmen konnten mindestens einen Angriff nach China zurückverfolgen, 39 Prozent nach Russland. Solche Attacken führen häufig nicht nur zu erheblichen finanziellen Verlusten, sondern können auch die nationale Sicherheit gefährden. Dies ist besonders schwerwiegend, wenn kritische Infrastrukturen betroffen sind oder sensible Regierungsdaten ins Visier geraten.



Zudem sind Cyberangriffe zunehmend politisch motiviert. So zeigt ein Bericht von ↗Orange Cyberdefense, dass eine pro-russische Hacktivistengruppe seit März 2022 über 6.600 Cyberattacken verübt hat, von denen 96 Prozent gezielt europäische Länder trafen. Diese Welle an Hacktivismus im Zuge geopolitischer Spannungen (etwa infolge des Ukraine-Krieges) beweist, dass europäische Staaten im Fadenkreuz digitaler Angriffe stehen, die über reine Kriminalität hinausgehen. Für europäische Unternehmen und Behörden ergibt sich daraus die dringende Notwendigkeit, ihre Abwehrbereitschaft zu erhöhen und vertrauenswürdige IT-Sicherheitslösungen einzusetzen, die gezielt auf diese Bedrohungen reagieren können.

4. Wirtschaftliche Bedeutung von Made in EU
Unabhängigkeit, Innovationskraft und Sicherheit

Angesichts dieser Bedrohungslage wird ersichtlich, wie wichtig Unabhängigkeit von außereuropäischen Anbietern ist. Europas Strategie der digitalen Souveränität zielt explizit darauf ab, die ↗Abhängigkeit von nicht-europäischer Technologie zu reduzieren. Der Einsatz von IT-Sicherheitslösungen Made in EU ermöglicht es Unternehmen, ihre Kerninfrastruktur mit vertrauenswürdigen Produkten zu schützen, ohne sich auf außereuropäische Technologiekonzerne verlassen zu müssen. Dies verringert Risiken, die aus externer Einflussnahme entstehen könnten. Darunter fallen unter anderem Zugriffe fremder Staaten auf Daten durch extraterritoriale Gesetze.

Darüber hinaus leistet Made in EU einen wirkungsvollen Beitrag zur Wirtschafts- und Innovationskraft Europas. Investitionen in europäische Cybersecurity-Anbieter stärken die heimische Industrie, schaffen hochwertige Arbeitsplätze und fördern technologisches Know-how innerhalb der EU. Die ↗Europäische Kommission stellt im Rahmen des Programms „Digitales Europa" allein für den Zeitraum 2025 bis 2027 rund 1,3 Milliarden Euro für kritische Technologien wie Künstliche Intelligenz, Cloud, Datenbanken und Cybersicherheit bereit. Institutionen in der EU investieren gezielt in digitale Infrastruktur, um die technologische Autonomie zu fördern. Initiativen wie GAIA-X oder die European Cloud Initiative werden mit einer Milliarde Euro gefördert, um eine europäische Cloud-Infrastruktur zu entwickeln.

Unternehmen, die auf europäische Sicherheitslösungen setzen, stärken einen heimischen Markt für Cybersecurity. So wird gewährleistet, dass kritische Sicherheitskompetenzen und -kapazitäten langfristig auf unserem Kontinent erhalten bleiben und ausgebaut werden.

Schließlich bedeutet wirtschaftliche Unabhängigkeit auch Resilienz: Europa kann sich in Krisenzeiten – sei es geopolitisch oder pandemiebedingt – auf eigene Technologien stützen, Lieferketten in der IT-Sicherheit besser kontrollieren und schneller auf Störungen reagieren. Die Fähigkeit, in Krisenzeiten auf eigene Technologien und Lieferketten zurückzugreifen, erhöht die wirtschaftliche Resilienz und Handlungsfähigkeit Europas erheblich. IT-Sicherheit wird somit zur Managementaufgabe und zum strategischen Erfolgsfaktor: Unternehmen, die frühzeitig in Compliance und Sicherheit investieren, verschaffen sich nachhaltige Wettbewerbsvorteile und schützen sich vor finanziellen Schäden, Reputationsverlust und Marktbarrieren.

5. Rechtliche und regulatorische Entwicklungen in der EU
Aktueller Überblick

NIS2-Richtlinie

Die Europäische Union hat in den letzten Jahren eine Reihe an gesetzlichen Rahmenwerken auf den Weg gebracht, um Cybersecurity und digitale Souveränität zu stärken. Ein Meilenstein ist die ↗NIS2-Richtlinie (EU 2022/2555 - network and information systems), welche die alte NIS-Richtlinie erweitert. NIS2 verpflichtet deutlich mehr Unternehmen und Organisationen strenge IT-Sicherheitsmaßnahmen umzusetzen. Dazu zählen auch mittelgroße Einrichtungen aus kritischen Sektoren. Die Richtlinie musste bis zum 17. Oktober 2024 in nationales Recht übertragen werden, was in ↗Deutschland allerdings noch nicht geschehen ist. Ab diesem Zeitpunkt gelten höhere Mindeststandards: Unternehmen müssen z. B. Risikoanalysen durchführen, Vorfälle melden und ihre Lieferketten absichern. Letztlich soll durch NIS2 gesamtwirtschaftliche Resilienz erhöht werden.

Cybersecurity Act

Ein weiterer wichtiger Baustein ist der ↗EU Cybersecurity Act, der bereits seit Juni 2019 gilt. Dieses Gesetz etablierte ein dauerhaftes Mandat für die ↗EU-Agentur für Cybersicherheit (ENISA) und schuf einen einheitlichen europäischen Zertifizierungsrahmen für ICT-Produkte, -Dienstleistungen und -Prozesse. Dadurch können Hersteller ihre Produkte nach EU-weit anerkannten Sicherheitsstandards zertifizieren lassen („low", „substantial" oder „high"), was einen europäischen Vertrauensnachweis darstellt. Die Mitgliedstaaten arbeiten in diesem Rahmen eng zusammen, um die Zertifizierung kritischer Produkte (z. B. in kritischen Infrastrukturen) weiterhin souverän zu gestalten. Der Cybersecurity Act stärkt damit Europas Rolle als vertrauenswürdiger Akteur im globalen Cyberraum und fördert die Zusammenarbeit der EU-Staaten bei Zertifizierung und Incident Response.

Cyber Resilience Act

Aktuell befindet sich auch der ↗Cyber Resilience Act (CRA) in der Umsetzung. Der CRA ist die erste EU-Verordnung, die ein Mindestmaß an Cybersicherheit für alle Produkte mit digitalen Elementen vorschreibt, die im EU-Binnenmarkt verkauft werden. Vom IoT-Gerät über Business-Software bis zur Industrieanlage müssen alle künftig grundlegende Sicherheitsanforderungen erfüllen, um Schwachstellen zu minimieren. Diese Vorgaben gelten unmittelbar in allen Mitgliedstaaten und werden bis 2027 schrittweise verpflichtend. Für Unternehmen bedeutet dies: Sicherheitsupdates, sichere Voreinstellungen und Verantwortung der Hersteller für die IT-Sicherheit ihrer Produkte werden zur Pflicht. Dies ist ein wichtiger Schritt, um Verbraucher und Unternehmen besser zu schützen.

Datenschutz-Grundverordnung

Schließlich ist die ↗Datenschutz-Grundverordnung (DSGVO) eine tragende Säule europäischer digitaler Souveränität. Seit 2018 verpflichtet sie Unternehmen und Organisationen, personenbezogene Daten nur auf rechtmäßige, transparente und sichere Weise zu verarbeiten. Sie stärkt Betroffenenrechte, schafft klare Regeln für Datenübermittlungen ins Ausland und verlangt von Unternehmen strikte Sicherheitsmaßnahmen inklusive Meldepflichten bei Datenschutzverletzungen. Die DSGVO zeigt: Digitale Souveränität in Europa bedeutet nicht nur Schutz vor technischen Angriffen, sondern auch die Selbstbestimmung der Bürger über ihre Daten. Für Unternehmen ist sie ein maßgeblicher Faktor, der Technologieeinsatz und Anbieterauswahl beeinflusst.

Digital Operational Resilience Act

Eine weitere zentrale EU-Verordnung ist der ↗Digital Operational Resilience Act (DORA), der seit Januar 2025 verbindlich für den gesamten Finanzsektor gilt. DORA schreibt eine robuste digitale Resilienz vor, um IT-Systeme und Daten gegen Störungen, Angriffe und Ausfälle abzusichern. Betroffen sind Banken, Versicherungen, Wertpapierfirmen, Börsenplätze sowie auch kritische IT-Dienstleister in diesem Umfeld. Die Verordnung gilt unmittelbar in allen Mitgliedstaaten ohne nationale Umsetzungsakte und verdeutlicht: Digitale Resilienz ist längst ein integraler Bestandteil wirtschaftlicher Stabilität und EU-weiter Sicherheitspolitik geworden.

All diese Regelungen unterstreichen, dass digitale Souveränität mittlerweile Chefsache in Europa ist. So betonte ↗EU-Kommissionspräsidentin Ursula von der Leyen in ihrer Rede am 21. Januar 2025 auf dem Weltwirtschaftsforum in Davos:

Europa müsse „sicherstellen, dass [es] die Kontrolle über die Technologien behält, die unser tägliches Leben bestimmen. Cybersicherheit und digitale Souveränität sind eine Frage der europäischen Unabhängigkeit."

Solche Stimmen zeigen die Spannungsfelder: Einerseits der Ruf nach europäischer Eigenständigkeit und Schutz kritischer Technologien, andererseits der Ruf nach effektiveren Werkzeugen im Inneren. Unternehmen und Organisationen bleibt nichts anderes übrig, als den Überblick über die EU-Regularien zu behalten und proaktiv Compliance-Maßnahmen umzusetzen, um rechtlich wie sicherheitstechnisch auf der Höhe zu sein. Aber auch der Blick ins Ausland darf nicht fehlen. Denn Anbieter mit Sitz außerhalb der EU können durch Gesetze verpflichtet werden, Daten auch ohne Wissen des betroffenen Unternehmens oder Nutzers an Behörden weiterzugeben. Dies widerspricht europäischen Datenschutzstandards fundamental. Die ↗EU-Kommission betont in ihren Strategiepapieren zur digitalen Souveränität, dass technologische Abhängigkeiten zu einem Sicherheitsrisiko werden. Nur durch eigene, kontrollierbare Systeme ließe sich langfristige Resilienz sicherstellen.

6. Technologische Aspekte
Datenschutz, Compliance, Transparenz und Innovationsfähigkeit

Europäische IT-Sicherheitslösungen bieten spezifische technologische Vorteile, die für Unternehmen in puncto Datenschutz und Compliance anderen überlegen sind. Ein zentrales Plus ist die strikte Einhaltung der Datenschutz-Grundverordnung. Lösungen, die in der EU entwickelt wurden, sind von vornherein darauf ausgerichtet, den hohen Anforderungen der Datenschutz-Grundverordnung zu genügen. Für Anwender bedeutet das: Datenschutz by Design ist integriert, das Risiko von Datenschutzverletzungen sinkt und Bußgelder wegen Compliance-Verstößen werden unwahrscheinlicher. EU-Anbieter unterliegen der Aufsicht europäischer Datenschutzbehörden und müssen sich an die Entscheidungen des Europäischen Datenschutzausschusses halten. Ein Rahmen, der Vertrauen schafft.

Ein weiterer Vorteil ist die Transparenz und Nähe zum regulatorischen Umfeld. Europäische Hersteller arbeiten räumlich und kulturell näher an den europäischen Gesetzgebern und Standards. Dadurch können sie neue regulatorische Vorgaben von NIS2, dem Cyber Resilience Act oder weiteren EU-Initiativen schnell in ihre Produkte einfließen lassen. Unternehmen, die auf solche Lösungen setzen, profitieren von maßgeschneiderten Sicherheitskonzepten, die aktuelle EU-Regularien berücksichtigen und an lokale Bedürfnisse angepasst sind. Zudem sind europäische Anbieter weniger anfällig für ausländische, staatliche Eingriffe. Dies steht im Gegensatz zu Firmen, die Gesetzen außerhalb der EU unterliegen. So wird das Risiko minimiert, dass versteckte Hintertüren oder Sicherheitslücken aufgrund externer Geheimdiensteinflüsse entstehen.

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, zum Beispiel der DSGVO, dem zukünftigen BSI-Gesetz oder der NIS2-Richtlinie. Das schafft Vertrauen, rechtliche Klarheit und Verlässlichkeit, insbesondere im Haftungsfall. Zum einen vermeiden sie zusätzliche Hürden wie Drittland-Transfers nach DSGVO oder unklare Zugriffsbefugnisse ausländischer Behörden, die nicht durch den EU-Rechtsrahmen gebunden sind. Zum anderen bewegen sich Anbieter und Anwender 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. Unternehmen profitieren von Rechtssicherheit, Nachvollziehbarkeit und politischen Stabilitätsvorteilen.

Auch in Bezug auf technische Innovationsfähigkeit brauchen sich europäische Produkte nicht zu verstecken. Europas Forschung ist weltweit führend in Bereichen wie Kryptographie, Datenschutztechnologien und sichere Softwareentwicklung. Europäische Anbieter wie ESET setzen mit Diensten wie dem AI Advisor auf erklärbare, datenschutzkonforme KI-Modelle. Diese helfen Unternehmen dabei, Vorfälle automatisiert zu analysieren, Bedrohungsmuster schneller zu erkennen und sicherheitsrelevante Entscheidungen nachvollziehbar zu treffen. Dies geschieht ohne Cloud-Abhängigkeiten von Drittländern.

Europäische Sicherheitslösungen setzen oft auf Open-Source-Komponenten oder offene Standards, was die Überprüfbarkeit des Quellcodes ermöglicht und einen sogenannten Vendor-Lock-in vermeidet. Dies erhöht die Transparenz und ermöglicht unabhängigen Stellen, die Sicherheit zu auditieren. Gleichzeitig fördern Programme der EU wie Horizon Europe oder Digital Europe Programme kontinuierlich Innovation in Cybersecurity, von KI-gestützter Threat Intelligence bis zu Quantenkryptographie. Die Nähe zu diesem Innovationsökosystem fließt in EU-Produkte ein. Moderne europäische Anbieter wie ESET setzen dabei auf KI-unterstützte, verhaltensbasierte Analysemodelle, die auch mithilfe von Machine Learning Bedrohungen erkennen, bevor sie signaturbasiert erfasst werden können. Diese „early detection"-Mechanismen ergänzen klassische Schutzmechanismen um eine proaktive Komponente.

Kurz gesagt: Made in EU steht für

datenschutzkonforme, transparente und hochinnovative IT-Sicherheit, die mit den dynamischen Bedrohungen Schritt hält.

7. Die Rolle des Verbands TeleTrusT
für die digitale Souveränität

Ein zentraler Akteur bei der Stärkung der digitalen Souveränität in Europa ist der ↗Bundesverband IT-Sicherheit e. V. (TeleTrusT). Der Verband vertritt als neutrale und unabhängige Instanz die Interessen von über 400 Unternehmen, Forschungseinrichtungen und öffentlichen Institutionen im Bereich IT-Sicherheit. TeleTrusT hat sich in den letzten Jahren als eine der wichtigsten Stimmen für europäische Sicherheitsstandards, Transparenz und Unabhängigkeit etabliert.

Eine der wichtigsten Initiativen des Verbands ist das Gütesiegel ↗„IT Security made in EU", das als Antwort auf die wachsende Abhängigkeit von nicht-europäischen Anbietern geschaffen wurde. Dieses Label setzt klare Kriterien voraus: Der Hauptsitz des Unternehmens muss sich in der EU befinden, Forschung und Entwicklung dürfen ausschließlich innerhalb der EU erfolgen, die Produkte müssen nachweislich DSGVO-konform sein und es dürfen keine Backdoors vorhanden sein. Damit schafft TeleTrusT einen klar definierten Maßstab für europäische IT-Sicherheit, der Unternehmen und Behörden Orientierung bietet.

Darüber hinaus positioniert sich TeleTrusT auch politisch. Der Verband fordert eine gezielte Stärkung der europäischen Cybersecurity-Branche, um digitale Souveränität langfristig zu sichern. In seinen Stellungnahmen warnt TeleTrusT vor der unreflektierten Nutzung von Cloud-Diensten aus Drittstaaten, insbesondere im öffentlichen Sektor. Er spricht sich konsequent für eine technologische Selbstbestimmung Europas aus und fordert von der Politik verbindliche Rahmenbedingungen, die faire Wettbewerbsbedingungen für europäische Anbieter schaffen.

Die Einbindung von TeleTrusT in strategische Überlegungen zur IT-Sicherheit Made in EU ist deshalb nicht nur eine Ergänzung, sondern ein zentraler Baustein. Der Verband zeigt, wie sektorübergreifende Zusammenarbeit und transparente Standards einen nachhaltigen Beitrag zur digitalen Unabhängigkeit Europas leisten können.

„IT-Sicherheit ‚Made in EU' ist nicht nur ein Label, sondern vielmehr ein Bekenntnis."

— Thorsten Urbanski, Leiter der Initiative „IT Security made in EU" des größten deutschen IT-Security-Verbandes ↗TeleTrusT

Trust Seal
www.teletrust.de/itsmie

8. ESETs Beitrag zur IT-Sicherheit in Europa
Europäische Kompetenz in der Praxis

ESET ist nicht nur ein europäischer IT-Sicherheitsanbieter, sondern hat seinen Hauptsitz in der EU, über 30 Jahre Erfahrung, mehrere Forschungszentren auf dem Kontinent und engagiert sich als aktiver Mitgestalter hiesiger Cybersicherheitsstandards. Das Unternehmen trägt sowohl das ↗„Cybersecurity Made in Europe"-Label der European Cyber Security Organisation (ECSO) als auch das zuvor erwähnte TeleTrusT-Siegel „IT Security made in EU". Das Unternehmen engagiert sich aktiv im politischen und wirtschaftlichen Dialog der EU, u. a. als Mitglied der ↗Business Advisory Group der EU Global Gateway Initiative, in ↗EU Cyber Dialogues und als Teilnehmer des ↗Pall Mall Process zur Verhinderung der Proliferation von Cyberwaffen.

ESET orientiert sich konsequent an europäischen Zertifizierungsstandards wie ↗ISO/IEC 27001 und ↗Common Criteria (ISO/IEC 15408) und unterstützt deren Verbreitung aktiv. Dies ist ein wichtiges Signal fur Compliance und Vertrauensbildung.

Forschung, Regulierung und gesellschaftliche Verantwortung

ESET ist in europäischen Fach- und Standardisierungsgremien aktiv, unter anderem bei ENISA, im ↗ECSO-Vorstand und im Advisory Board von Europol EC3. Die Experten des Unternehmens begleiten regulatorische Entwicklungen wie die NIS2-Richtlinie, den Cyber Resilience Act oder DORA nicht nur fachlich, sondern unterstützen Kunden auch aktiv bei deren Umsetzung.

Darüber hinaus leistet ESET erhebliche ↗Beiträge zu Bildung und Wissenschaft: Das Unternehmen unterstützt Hochschulen in der Slowakei, Polen, Tschechien und der Ukraine mit Lehraufträgen, Forschungspartnerschaften und technischer Expertise in Bereichen wie Machine Learning und statistischer Analyse. Auch Programme zur Nachwuchsförderung und Diversität, etwa Women in Cybersecurity, werden aktiv vorangetrieben.

ESET bietet über seine Büros in Europa auch ↗lokalen NGOs Unterstützung, die beispielsweise im Bereich Jugendhilfe oder psychische Gesundheit tätig sind. Zudem engagieren sich viele Mitarbeitende in freiwilligen Projekten, etwa in Deutschland oder der Slowakei.

Als ↗inhabergeführtes Unternehmen mit europäischem Hauptsitz verfolgt ESET eine langfristige, werteorientierte Strategie jenseits von Investorenlogik. Das zeigt sich auch in der Unternehmenskultur. Diversität, Weiterbildung und faire Arbeitsbedingungen sind fest verankert.

Eine No-Backdoor-Garantie ist für uns selbstverständlich – denn: Als europäischer IT-Sicherheitshersteller stehen wir zu 100% hinter den demokratischen Werten Europas.

— Holger Suhl, Country Manager, ESET Deutschland GmbH

↗ESETs Sicherheitsplattformen beruhen auf Echtzeit-Telemetrie von Millionen europäischer und globaler Endpunkte. Die Kombination aus KI-gestützter Analyse, ↗Threat Intelligence, forensischer Forschung und mehrstufigem Schutz ermöglicht eine vorausschauende Erkennung von Bedrohungen. Dazu zählen auch staatlich gesteuerte Cyberkampagnen, die zunehmend europäische Unternehmen und kritische Infrastrukturen ins Visier nehmen.

Mit Angeboten wie ↗ESET MDR und dem AI Advisor unterstützt ESET Kunden dabei, komplexe Bedrohungen schnell zu erkennen, einzuordnen und abzuwehren. Über den AI Advisor stellt ESET zusätzlich eine KI-gestützte Entscheidungshilfe bereit, die sicherheitsrelevante Vorfälle bewertet, priorisiert und mit Erklärungen versieht. Die Lösung wurde vollständig in Europa entwickelt und erfüllt höchste Ansprüche an Transparenz, Verlässlichkeit und Datenschutz.

Ergänzt wird dies durch ESETs umfassende Threat Intelligence Feeds, die unter anderem Informationen zu APT-Gruppen, Botnets, Zero-Day-Aktivitäten und Ransomware-Taktiken liefern. Behörden, CERTs und Unternehmen nutzen diese strategischen Frühwarnsysteme, um ihre Sicherheitsstrategie gezielt anzupassen.

Technologischer Schutz mit europäischen Werten

Besonders hervorzuheben ist: Die gesamte Datenverarbeitung erfolgt konform zur DSGVO und innerhalb der EU. Zusätzlich betreibt ESET unter anderem ↗ein eigenes Rechenzentrum in Frankfurt sowie ein ↗Security Operations Center (SOC) in Jena.

ESETs KI-basierte Bedrohungsanalyse verarbeitet Daten aus unterschiedlichsten Quellen von Honeypots und OSINT über Web Crawling bis hin zu Botnet-Tracking. Die Daten werden mithilfe von Machine Learning analysiert und durch ein Analystenteam in handlungsrelevante Informationen überführt. Sie bieten Behörden, Unternehmen und kritischen Infrastrukturen somit wichtige Entscheidungsgrundlagen.

Die Forschungsteams von ESET analysieren global relevante Cyberkampagnen und betreiben mit dem Threat Intelligence Hub eine zentrale Plattform für Frühwarnung, IOC-Feeds und Analysen von APT-Operationen. Diese werden vielfach von CERTs, Regierungen und KRITIS-Betreibern genutzt..

Sicherheit in Krisenzeiten: Das Beispiel Ukraine

Der Krieg in der Ukraine macht deutlich, wie eng physische Konflikte und digitale Angriffe heute verknüpft sind. Cyberangriffe zählen längst zum festen Repertoire staatlich unterstützter Kampagnen, insbesondere gegen kritische Infrastrukturen. ESET übernimmt in diesem Kontext nicht nur eine technologische Schlüsselrolle, sondern agiert auch als verlässlicher Partner mit konkreter Hilfe vor Ort.

Bereits seit 2014 unterstützt ESET ukrainische Organisationen, insbesondere im Energiesektor, bei der Abwehr gezielter ↗Cyberattacken. Die Entdeckung und Analyse hochentwickelter Malware wie BlackEnergy, Industroyer, NotPetya, CaddyWiper, ↗HermeticWiper und AcidRain stammen aus den Forschungslaboren von ESET. Diese Erkenntnisse werden weltweit mit Sicherheitsbehörden, CERTs und Partnern geteilt und helfen so, auch über die Ukraine hinaus, Cyberabwehrstrategien zu stärken.

Nach Beginn des russischen Angriffskriegs im Februar 2022 intensivierte ESET seine Unterstützung auf mehreren Ebenen:

Technisch: Kritische ukrainische Einrichtungen erhielten kostenfreie Lizenzen und Upgrades auf höchste Schutzklassen. Zudem wurde das ukrainische Partnerteam vorübergehend an den ESET Hauptsitz in Bratislava umgesiedelt, um dort sicher weiterarbeiten zu können.

Humanitär: ESET stellte Generatoren für Krankenhäuser, Schulen und andere systemrelevante Einrichtungen zur Verfügung. Mitarbeiter engagierten sich in Freiwilligenprogrammen für Geflüchtete. Das Unternehmen richtete zudem ein Stipendienprogramm ein, um Kindern geflüchteter Familien digitale Bildung zu ermöglichen. Insgesamt hat die ESET Foundation mehr als 1,2 Millionen Euro für Hilfsprojekte in der Region bereitgestellt.

Wer Vertrauen, Kontrolle und Sicherheit in der digitalen Welt stärken will, sollte Sicherheitslösungen einsetzen, die genau diese Werte glaubhaft verkörpern – oder wie ESET sagt: „Trust is the currency of cybersecurity.

— Richard Marko, CEO ESET

9. Prevention First
ESETs Sicherheitsansatz im Zeichen der digitalen Souveränität

Von reaktiver Verteidigung zur vorausschauenden Abwehr

Angriffe auf IT-Systeme sind heute keine Ausnahme mehr, sondern Alltag. Oft bleiben sie über Wochen oder Monate unentdeckt – mit gravierenden Folgen für Unternehmen, Behörden und kritische Infrastrukturen. Wer dann erst reagiert, ist zu spät dran. Klassische Verteidigungsstrategien, die auf Vorfälle warten, um Gegenmaßnahmen einzuleiten, greifen deshalb zu kurz. Die Realität erfordert ein anderes Denken.

Die klassische IT-Sicherheitsarchitektur, die vor allem auf reaktive Verteidigung setzt, stößt zunehmend an ihre Grenzen. Angesichts von Zero-Day-Exploits, Lieferkettenangriffen und hoch entwickelten APT-Kampagnen braucht es einen Paradigmenwechsel: weg von Incident Response, hin zu frühzeitiger Erkennung und Verhinderung von Angriffen.

Genau hier setzt der von ↗ESET entwickelte Ansatz Prevention First an. Er versteht IT-Sicherheit als strategische Daueraufgabe, die schon in der Architektur beginnt: durch sichere Voreinstellungen (Secure Defaults), kontinuierliche Systemhärtung, automatisierte Angriffserkennung und eine ständige Bewertung der Bedrohungslage. Das Ziel ist es, Risiken möglichst frühzeitig zu identifizieren, bevor sie Schaden anrichten und idealerweise bevor ein Angreifer überhaupt Zugang zum System erhält. Prevention First ist damit nicht nur ein technischer Ansatz, sondern auch Ausdruck einer sicherheitsbewussten Organisationskultur.

Prevention First als europäischer Wert

Dieser Sicherheitsansatz steht in enger Verbindung zu den Werten, für die die Europäische Union eintritt: Datenschutz, Transparenz, Kontrolle über eigene Daten und Unabhängigkeit von außereuropäischen Einflussnahmen. Anbieter, die sich zu Prevention First verpflichten, setzen auf Sicherheitsmechanismen, die nicht auf tiefgreifende Überwachung oder umfassende Datensammlung angewiesen sind. Stattdessen liegt der Fokus auf der technologischen Abwehr von Bedrohungen, z. B. durch signaturlose Erkennung, verhaltensbasierte Analysen und Sandboxing.

ESET hat Prävention zum Leitprinzip seiner Produktentwicklung gemacht. Die ↗Schutzmechanismen der Lösungen kombinieren mehrere Layer: unter anderem Netzwerkmonitoring, Heuristik, Machine Learning, UEFI-Scanner, cloudbasierte Sandbox-Analysen und Threat Intelligence. Sie sollen Angriffe frühzeitig blockieren, ohne den Datenschutz zu kompromittieren. Dabei entstehen keine unnötigen Abhängigkeiten oder intransparente Prozesse. Dies ist ein wesentlicher Unterschied zu vielen außereuropäischen Anbietern. Gleichzeitig unterstützt Prevention First Organisationen dabei, zentrale Anforderungen der EU-Gesetzgebung zu erfüllen. Dazu zählen insbesondere die in Kapitel 5 erwähnten Vorgaben wie Datenschutz-Grundverordnung, NIS2 und CRA.

Doch Prävention endet nicht bei der Architektur. Sie muss im operativen Alltag durch kontinuierliche Überwachung ergänzt werden. Genau hier setzt Managed Detection and Response an und verbindet vorausschauende Sicherheitskonzepte mit reaktiver Handlungsfähigkeit.

Managed Detection and Response als verlängerter Arm der Prävention

Insbesondere kleine und mittlere Unternehmen stehen vor der Herausforderung, ihre IT-Sicherheit mit begrenzten Ressourcen auf professionelles Niveau zu heben. ↗Managed Detection and Response (MDR) wird hier zum entscheidenden Hebel. Als Dienstleistung kombiniert MDR die kontinuierliche Überwachung von IT-Systemen mit aktiver Bedrohungsanalyse und -beseitigung. Das Prinzip bleibt auch hier: Angriffe möglichst frühzeitig erkennen und blockieren.

Ein Beispiel dafür ist ESET MDR (und Ultimate), das auf dem Prevention First-Prinzip aufbaut. Der Dienst wird in Europa betrieben, von europäischen Analystenteams ausgeführt und unterliegt ausschließlich EU-Recht. ↗Im Security Operation Center (SOC) in Jena kümmern sich Spezialisten um Kunden aus Deutschland, Österreich und der Schweiz. Damit bietet MDR Ultimate nicht nur hohen technischen Schutz, sondern auch maximale rechtliche Transparenz und Datenschutzkonformität. Kunden profitieren von:

- 24/7 Überwachung durch ein europäisches SOC
- Aktiver Bedrohungssuche (Threat Hunting)
- Schneller Reaktion im Eskalationsfall
- Klarer Kommunikation ohne Fachjargon
- Integration mit vorhandenen ESET- oder Drittanbieter-Systemen

Die Kombination aus technologischem Know-how, regulatorischer Nähe und echter Präventionskultur macht MDR-Dienste wie ESET MDR Ultimate zu einem zentralen Baustein für souveräne IT-Sicherheit Made in EU.

Prevention First als Fundament europäischer Resilienz

Digitale Souveränität bedeutet, Kontrolle zu behalten: über Daten, Systeme, Entscheidungen und Risiken. Der Prevention First-Ansatz liefert dafür das passende Fundament. Er verbindet technologische Exzellenz mit europäischen Werten und schafft eine Sicherheitsstrategie, die nicht auf Abschreckung, sondern auf Verhinderung beruht. Anbieter wie ESET zeigen, dass präventive Cybersicherheit und europäische Selbstbestimmung kein Widerspruch sind, sondern sich ideal ergänzen. Wer Made in EU ernst meint, sollte auch beim Sicherheitskonzept auf Früherkennung, Transparenz und Rechtskonformität setzen.

10. Fazit

Die vorangegangenen Ausführungen machen deutlich, dass IT-Sicherheit Made in EU kein Selbstzweck ist, sondern ein strategischer Schlüsselfaktor für Unternehmen, Organisationen und Verwaltungen in Europa. Angesichts immer neuer Cyberbedrohungen und geopolitischer Unsicherheiten können europäische Lösungen einen wichtigen Beitrag leisten, um die Resilienz zu erhöhen, Compliance sicherzustellen und Unabhängigkeit zu wahren. Durch den Einsatz von Sicherheitsprodukten, die hohe europäische Standards erfüllen, stärken Organisationen ihre Abwehrkraft und gewinnen zugleich das Vertrauen von Kunden, Partnern und Bürgern zurück. Digitale Souveränität wird so vom Schlagwort zur gelebten Praxis.

Indem Verantwortliche diese Maßnahmen beherzigen, machen sie einen wichtigen Schritt, um die IT-Sicherheit in ihrem Wirkungsbereich zu erhöhen und gleichzeitig die digitale Souveränität Europas zu stärken. Die Wahl von Sicherheitslösungen Made in EU ist mehr als nur eine politische oder wirtschaftliche Entscheidung. Sie ist vielmehr ein pragmatischer Weg, Vertrauen, Kontrolle und Sicherheit in der digitalen Zukunft zu verankern. Europas Unternehmen, Organisationen und Verwaltungen werden dadurch widerstandsfähiger gegen Cyberbedrohungen und können die Chancen der Digitalisierung selbstbestimmt und sicher nutzen.

IT-Entscheider sollten daher prüfen, ob ihre eingesetzten Sicherheitslösungen sowohl technologisch als auch regulatorisch der digitalen Souveränität Europas entsprechen. Und wenn nicht: handeln.

ESET Experten geben Handlungsempfehlungen

über die Verantwortliche nachdenken oder in den Alltag umsetzen sollten:

Bevorzugung europäischer IT-Sicherheitslösungen

Prüfen Sie bei der Beschaffung von Security-Software und -Services, ob europäische Alternativen verfügbar sind. Lösungen mit Labels wie IT Security Made in Europe garantieren z. B. ↗keine versteckten Zugänge und EU-basierte Datenverarbeitung. Durch den Einsatz solcher Produkte reduzieren Sie Abhängigkeiten und erfüllen leichter europäische Datenschutz- und Sicherheitsstandards.

Compliance mit EU-Regulierungen sicherstellen

Machen Sie Ihr Unternehmen frühzeitig mit relevanten EU-Vorschriften vertraut (NIS2, Cybersecurity Act, DSGVO, Cyber Resilience Act usw.). Implementieren Sie interne Richtlinien und technische Maßnahmen, um diese Anforderungen zu erfüllen. So vermeiden Sie nicht nur Strafen, sondern verbessern auch ganz praktisch Ihr Sicherheitsniveau. Orientieren Sie sich an Zertifizierungen oder Siegeln, die auf EU-Standards basieren, um Vertrauen bei Kunden und Auditoren zu schaffen.

Mitarbeiter sensibilisieren und weiterbilden

Technische Maßnahmen greifen nur, wenn Mitarbeiter entsprechend handeln. Schulen Sie Ihr Personal regelmäßig in IT-Sicherheit, Datenschutz und im Umgang mit Phishing & Co. Laut BSI-Lagebericht ist die kontinuierliche Weiterbildung von IT-Fachkräften unerlässlich, um wachsenden Cyberbedrohungen zu begegnen. Fördern Sie eine Sicherheitskultur, in der Vorfälle sofort gemeldet und bewährte Praktiken im Alltag gelebt werden.

Zusammenarbeit und Austausch nutzen

Nutzen Sie europäische Netzwerke und Plattformen zum Informationsaustausch über Cybergefahren (z. B. CERTs, ISACs branchenbezogen oder Initiativen im Rahmen des EU Cybersecurity Strategy). Die Kooperation zwischen Staat und Wirtschaft sowie zwischen EU-Mitgliedsländern ist entscheidend, um ↗breite Angriffswellen abzuwehren. Teilen Sie Erfahrungen und Best Practices.

Strategische Risikoanalyse und Notfallplanung

Bauen Sie eine robuste Cyber-Resilienz auf, indem Sie Risiken regelmäßig analysieren und Notfallpläne erarbeiten. Europäische Normen wie ISO 27001 oder der BSI-Grundschutz bieten Rahmenwerke, die mit EU-Regularien kompatibel sind. Ein durchdachtes Business-Continuity-Management und Übungen für den Ernstfall stellen sicher, dass Ihr Betrieb auch bei einem Sicherheitsvorfall handlungsfähig bleibt. Planen Sie außerdem für den Fall von Cloud-Ausfällen oder Lieferkettenproblemen Alternativen ein. Dies geschieht idealerweise unter Einbeziehung europäischer Dienstleister, um im Krisenfall Unterstützung vor Ort zu haben.

3 VON ÜBER 500.000 ZUFRIEDENEN KUNDEN

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

Unsere Lösungen sind nach den Qualitäts- und Informations-sicherheitsstandards ISO 9001:2015 und ISO/IEC 27001:2022 zertifiziert

ESET IN ZAHLEN

110.000.000+
Geschützte Nutzer weltweit

178
Länder & Regionen

500.000+
Geschützte Unternehmen

11
Forschungs- und Entwicklungs-zentren weltweit

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.

welivesecurity by ESET

ESET Digital Security Guide

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

ESET.DE | ESET.AT | ESET.CH