WHITEPAPER

Ethik als Fundament digitaler Sicherheit

Ein transatlantischer Wertevergleich

ESET Made in EU IT-Security

Cybersecurity
Progress. Protected.

Inhaltsverzeichnis

Autor: Stephanie Wündsch, ESET Deutschland GmbH

Stand: Oktober 2025

Cybersecurity
Progress. Protected.

0 WARUM ETHIK in der heutigen Unternehmenswelt entscheidend ist

„Die Frage nach den ethischen Werten, die ein Unternehmen leiten, ist keine Nebensache. Insbesondere in der Cybersicherheit ist sie entscheidend."

— Stephanie Wündsch, Product Marketing Manager mit M.A. in Angewandter Ethik, ESET Deutschland GmbH

Einleitung

Als Facebook 2004 die digitale Bühne betrat, war es zunächst nur ein Netzwerk für Studierende der Harvard Universität. Doch was als Campus-Projekt begann, sollte sich schnell zu einem globalen Tech-Giganten entwickeln und die Art, wie wir miteinander interagieren, nachhaltig ändern. Dabei stand das frühe Motto „Move fast and break things" sinnbildlich für eine Unternehmenskultur, die geprägt war von Innovationsgeist, Geschwindigkeit und Risikobereitschaft. Während diese Haltung rasche Produktentwicklungen und wirtschaftliche Erfolge ermöglichte, ging sie gleichzeitig mit einer gewissen Sorglosigkeit gegenüber den Folgen einher. So hatte insbesondere die Privatsphäre der Nutzer gelegentlich zu leiden. Eines der brisantesten Beispiele ist der ↗Cambridge-Analytica-Skandal aus dem Jahr 2018[1], bei dem Daten von mehreren Millionen Nutzern ohne deren Wissen für politische Zwecke verwendet wurden.

An diesem Beispiel zeigt sich, inwiefern das Handeln einer Firma Ausdruck der Unternehmenskultur und -haltung ist. Damit sind Werte und Prinzipien gemeint, die das Selbstverständnis eines Unternehmens prägen und sowohl das Verhalten gegenüber Mitarbeitenden als auch gegenüber Kunden und anderen Stakeholdern beeinflussen. Besonders interessant ist hierbei das Verhältnis zwischen ökonomischen Prinzipien wie Effizienz, Innovationskraft oder Gewinnoptimierung und ethischen Werten wie Freiheit, Menschenwürde und Nachhaltigkeit. Im Idealfall treffen Unternehmen Entscheidungen, die sowohl ökonomisch sinnvoll als auch ethisch vertretbar sind. Aber häufig werden sie als Gegenspieler wahrgenommen, weil ihre Zielsetzungen nicht immer vereinbar scheinen.

Die Cybersicherheitsbranche ist in diesem Zusammenhang ein besonders sensibler Markt. Denn hier verkaufen Unternehmen ein Produkt mit ethischem Wert: Sicherheit. Alle Anbieter eint das Ziel, ihre Kunden vor digitalen Bedrohungen zu schützen. Doch wie steht es um die Haltung der Unternehmen jenseits dieses Schutzziels? Insbesondere in Europa und den USA unterscheiden sich die Marktlogiken und die ethischen Leitplanken der Hersteller in vielen Punkten. Dieses Whitepaper beleuchtet die transatlantischen Werteunterschiede und ihre Auswirkungen auf die jeweiligen Ansätze im Bereich Sicherheit und Technologie. So erhalten Nutzer eine Orientierungshilfe bei der Wahl eines passenden Cybersicherheitsanbieters. Schließlich handelt es sich hierbei nicht nur um eine technische, sondern auch eine strategische Entscheidung, bei der Vertrauen eine wichtige Rolle spielt.

1 ETHIK IN GESELLSCHAFTEN: Wie Werte das Zusammenleben prägen

Ein Blick hinter die ethischen Kulissen

Welche Werte und Prinzipien ein Unternehmen in seiner Haltung und seinem Handeln leiten, hängt unter anderem vom gesellschaftlichen Umfeld ab. Denn insbesondere ethische Werte sind kulturell und historisch geprägt und beeinflussen nicht nur das gesamtgesellschaftliche Zusammenleben. Sie wirken bis in wirtschaftliche Strukturen und unternehmerisches Handeln hinein (siehe Abb. 1). In einer globalisierten und digitalisierten Welt agieren Unternehmen jedoch über Ländergrenzen hinweg und treffen dabei auf unterschiedliche rechtliche und kulturelle Rahmenbedingungen. Das Facebook-Beispiel zeigt, welche Auswirkungen das haben kann. Während in den USA lange ein lockerer Umgang mit Nutzerdaten üblich war, stieß dieselbe Praxis in Europa auf Widerstand. So wurde im Mai 2018 in der EU die ↗Datenschutz-Grundverordnung (DSGVO)[2] verabschiedet, um eine transparente und verantwortungsvolle Datenverarbeitung sicherzustellen. Gerade in einem so sensiblen Bereich wie der Cybersicherheit ist es für Verbraucher deshalb wichtig, die ethischen Leitplanken und die Haltung eines Anbieters zu prüfen. Das gilt insbesondere für Unternehmen, die ihre digitalen Infrastrukturen und Assets schützen wollen. Schließlich vertrauen sie dem Cybersicherheitsanbieter eine unternehmenskritische Aufgabe an.

Abbildung 1: Wertedurchdringung

Werte im transatlantischen Vergleich

Da der Cybersicherheitsmarkt vor allem von US-amerikanischen und europäischen Herstellern geprägt ist, liegt der Fokus dieser Betrachtung auf dem transatlantischen Vergleich. Zwar wird geopolitisch oft von der „westlichen Welt" gesprochen, als sei sie ein homogener Kultur- und Wirtschaftsraum, bei genauerem Hinsehen zeigen sich jedoch deutliche Unterschiede. Trotz gemeinsamer historischer Wurzeln divergieren die ethischen Wertvorstellungen und deren Einfluss auf die Gesellschaft wie auch das unternehmerische Handeln teils erheblich.

Die amerikanische Unabhängigkeitserklärung und die Charta der Grundrechte der Europäischen Union (EU-Grundrechtecharta) stellen zwei historisch relevante Dokumente dar, in denen die ethischen Grundwerte benannt werden, die für die jeweiligen Gesellschaften zentral sind:

Deutsche Übersetzung der ↗Präambel der amerikanischen Unabhängigkeitserklärung[3]:

„Wir halten diese Wahrheiten für ausgemacht, dass alle Menschen **gleich** erschaffen wurden, dass sie von ihrem Schöpfer mit gewissen unveräußerlichen Rechten begabt wurden, worunter sind Leben, **Freiheit** und **das Bestreben nach Glückseligkeit**."

Deutsche Übersetzung der ↗Präambel der EU-Grundrechtecharta[4]:

„In dem Bewusstsein ihres geistig-religiösen und sittlichen Erbes gründet sich die Union auf die unteilbaren und universellen Werte der **Würde des Menschen**, der **Freiheit**, der **Gleichheit** und der **Solidarität**."

Europa: Kollektive Verantwortung

Menschenwürde und Solidarität

Der Verweis auf Solidarität und die Würde des Menschen in der EU-Grundrechtecharta ist Ausdruck eines kollektiven Schutzgedankens. Mit Menschenwürde ist gemeint, dass jedem Menschen ein unveräußerlicher Wert zukommt, der jederzeit von allen anderen zu achten ist. Dieser ethische Wert bildet damit die Grundlage für alle anderen Grundrechte wie Privatsphäre, Sicherheit, Meinungs- und Versammlungsfreiheit oder Nichtdiskriminierung.

Bereits im Zuge der europäischen Aufklärung im 17. und 18. Jahrhundert wurde die Menschenwürde erstmals zu einem umfassenden philosophischen Konzept ausformuliert. Auch in der Weimarer Reichsverfassung von 1919 wurde sie aufgegriffen. Allerdings haben die Nationalsozialisten den entsprechenden Passus gestrichen und die Menschenwürde als universellen Wert verneint. Ihr rassistisches und antisemitisches Weltbild war die Ausgangslage für die systematische Verfolgung und Ermordung von Millionen von Menschen im Zweiten Weltkrieg.

Um eine Wiederholung solcher Gräueltaten zu verhindern, wurde die Anerkennung der Würde eines jeden Menschen in vielen europäischen Ländern als Prinzip der jeweiligen Verfassungsordnungen aufgeführt und gilt als einer der zentralen ethischen Grundwerte der europäischen Kultur. Auch die Solidarität spielt vor diesem historischen Kontext eine wichtige Rolle. Damit soll sichergestellt werden, dass sich die Gemeinschaft um all ihre Mitglieder kümmert, sodass auch für die Schwächeren gesorgt ist und niemand ausgegrenzt wird.

Freiheit

Gemein ist beiden Texten der Verweis auf die Gleichheit und die Freiheit. Allerdings liegen bei der Freiheit unterschiedliche Begriffsverständnisse vor, die sich unter anderem aus dem geschichtlichen Kontext heraus ergeben. Am 4. Juli 1776 sagten sich die britischen Kolonien in Nordamerika von Großbritannien los und gründeten damit die Vereinigten Staaten von Amerika. Freiheit im Sinne der Loslösung von staatlicher Einmischung des Mutterlandes ist hierbei ein zentraler Antrieb der sich neu gründenden Gesellschaft. In diesem Sinne wird Freiheit als Abwesenheit von äußeren Zwängen und Einschränkungen durch den Staat verstanden, die als notwendige Bedingung für die Freiheit des Individuums angesehen wird. Regulierungen werden also grundlegend als Eingriff in die Freiheit des Einzelnen erachtet.

In Europa wird der Staat hingegen als freiheitskonstituierend verstanden, indem er mithilfe von Regulierungen einen Ordnungsrahmen vorgibt und sicherstellt, dass alle Bürgerinnen und Bürger innerhalb dieses Rahmens frei leben und handeln können. Der zugrundeliegende Gedanke dabei ist, dass es Freiheit nur in Kombination mit einem gewissen Grad an Sicherheit geben kann. Insofern kommt dem Staat immer auch eine Schutzfunktion zu, die in der Interpretation des US-amerikanischen Freiheitsbegriffs nicht vorhanden ist.

USA: Individuelle Verantwortung

Glücksstreben

In den USA liegt ein deutlicher Fokus auf dem Individuum. Das zeigt sich bereits am Freiheitsverständnis, das jedem Einzelnen die Möglichkeit zuspricht, das eigene Leben frei von äußeren Zwängen zu gestalten. Noch deutlicher tritt diese Mentalität durch den Verweis auf das Bestreben nach Glückseligkeit hervor. Es unterstreicht die Idee, dass jeder Mensch das Recht hat, nach Wohlbefinden und Selbstverwirklichung zu streben. Doch mit diesem Recht geht auch die Pflicht einher, sich um sein individuelles Glück zu kümmern. Der „American Dream" bringt diese Haltung auf den Punkt, indem er den Glauben verkörpert, dass jeder Mensch durch harte Arbeit und Entschlossenheit den gesellschaftlichen Aufstieg „vom Tellerwäscher zum Millionär" schaffen kann. Auf der einen Seite ist das Ausdruck eines tiefen Optimismus, auf der anderen Seite wird aber auch eine klare Erwartungshaltung formuliert. Denn wer es nicht schafft, ist dieser Logik zufolge selbst dafür verantwortlich.

2 Ethik in Wirtschafts-systemen: Werte als Standortfaktoren

Unternehmerische Handlungsspielräume in Europa und den USA

Bis heute prägen diese historisch bedingten Unterschiede in der Gewichtung ethischer Grundwerte nicht nur die Gesellschaften als Ganzes, sondern auch die jeweiligen Märkte. In den USA wirkt der Fokus auf die Werte der Freiheit und individuellen Selbstverwirklichung im Sinne eines liberalen Pioniergeistes fort. Weniger staatliche Eingriffe, eine hohe Risikobereitschaft und das Ideal von Unternehmertum und Eigenverantwortung führen zu einem dynamischeren, stärker auf Wettbewerb ausgerichteten Wirtschaftssystem. Europa dagegen entwickelte seine Märkte aus einer Geschichte von Monarchien, Kriegen und sozialen Bewegungen heraus, die zu einer stärkeren Fokussierung auf ethische Werte wie den Schutz der Menschenwürde und Solidarität führte. So spielen bis heute staatliche Regulierung, soziale Sicherungssysteme und kollektive Verantwortung eine größere Rolle. Diese Unterschiede wirken sich direkt auf die Art und Weise aus, wie die jeweiligen Märkte regu-liert werden und die Handlungsspielräume von Unternehmen ausgestaltet sind.

USA: So wird in den USA tendenziell ein sogenannter „ex post"-Ansatz (lat.: „im Nachhinein", siehe Abb. 2) in Bezug auf Regulierungen verfolgt: Man lässt dem Markt zunächst freies Spiel und greift erst dann regulatorisch oder mit Sanktionen ein, wenn konkrete Probleme auftreten. Das führt mitunter zu kurios anmutenden Gerichtsprozessen, ↗etwa wenn ein Restaurant verklagt wird, weil sich ein Gast am heißen Kaffee verbrannt hat[5]. Zu den Vorteilen dieses Ansatzes gehört, dass Innovationen sehr schnell vorangetrieben werden können. Allerdings tragen Unternehmen wie auch Verbraucher ein erhöhtes Risiko. Für Firmen kann ein Fehltritt im schlimmsten Fall den finanziellen Ruin bedeuten, für Einzelpersonen bedeutet es unter Umständen den Verlust von Privatsphäre oder Sicherheit.

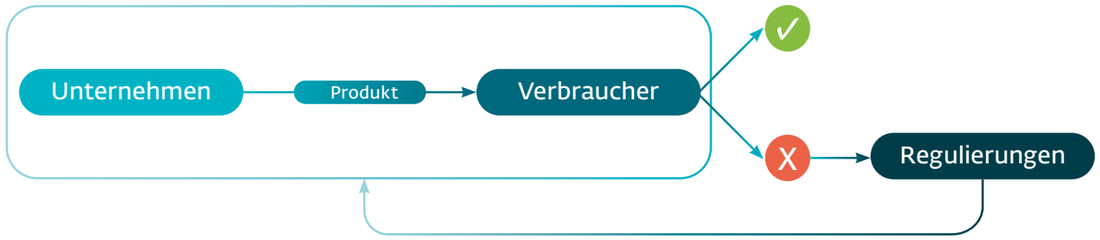


Abbildung 2: "Ex post"-Ansatz

Europa: In Europa, wo der regulatorische Rahmen als freiheitskonstituierend erachtet wird und ein kollektiver Schutzgedanke vorherrscht, besteht tendenziell eher ein „ex ante"-Ansatz (lat.: „im Voraus ", siehe Abb. 3): Der Markt wird von Beginn an gewissen Regulierungen unterworfen. Zu den Vorteilen dieser Herangehensweise gehört, dass die Grundrechte der Menschen gewahrt werden. Gleichzeitig profitieren Unternehmen von einem geringeren Risiko, in Millionenhöhe von Verbrauchern verklagt zu werden (sofern sie entsprechend der Vorgaben agieren). Der Preis dafür ist jedoch eine langsamere Innovationsdynamik und umfangreichere bürokratische Hürden.

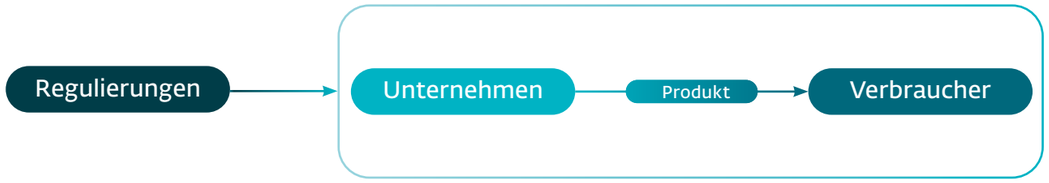


Abbildung 3: "Ex ante"-Ansatz

Künstliche Intelligenz zwischen Regulierung und Innovation

Diese unterschiedlichen Regulierungslogiken spiegeln sich wiederum in der Grundhaltung Innovationen gegenüber wider. In den USA wird der Fokus stärker auf die Chancen gelegt, die mit neuen Technologien und Geschäftsmodellen einhergehen. Fortschritt, Wachstum und Wettbewerb gelten als zentrale Treiber gesellschaftlicher Entwicklung. In Europa hingegen überwiegt die Abwägung von Risiken im Hinblick auf ethische oder soziale Implikationen. Innovation wird hier nicht nur als Möglichkeit, sondern auch als potenzielle Bedrohung verstanden, die kontrolliert und eingehegt werden muss. Besonders gut lässt sich das am Umgang mit künstlicher Intelligenz (KI) verdeutlichen, wo sich sowohl die Grundhaltungen als auch die regulatorischen Ansätze zwischen Europa und den USA deutlich unterscheiden. Mit dem ↗EU AI Act[6], der 2024 in Kraft trat, hat die Europäische Union einen umfassenden Rechtsrahmen geschaffen, der KI-Systeme nach ihrem Risikopotenzial klassifiziert und reguliert. Damit verfolgt die EU einen präventiven „ex ante"-Ansatz, mit dem Grundrechte wie Datenschutz, Privatsphäre und Nichtdiskriminierung geschützt werden sollen. Besonders hochriskante KI-Anwendungen, etwa in der biometrischen Überwachung oder bei automatisierten Entscheidungen im Sozial- und Finanzbereich, unterliegen strengen Auflagen. In den USA existiert bislang kein einheitliches Bundesgesetz zur Regulierung von KI. Stattdessen agieren einzelne Behörden mit sektorspezifischen Leitlinien, zum Beispiel für die Bereiche Gesundheit, Arbeit oder Verbraucherschutz. In ihrem ↗„AI Action Plan"[7] von 2025 betont die US-Regierung die strategische Bedeutung von KI für wirtschaftliche und geopolitische Dominanz. KI soll schnell und umfassend entwickelt werden, mit möglichst wenig regulatorischen Hürden.

„Der EU AI Act bildet eine wichtige rechtliche Grundlage, indem er einen klaren Rahmen für den sicheren und verantwortungsvollen Einsatz von KI schafft und damit das Vertrauen der Verbraucher stärkt."

— Maik Wetzel,
Strategic Business Development Director,
ESET Deutschland GmbH

3 Ethik in Unternehmen: Positionierung von IT-Sicherheitsanbietern

Wertegeleitete Anbieterwahl: Was Nutzer wissen sollten

Nachdem der Einfluss ethischer Werte auf die Gesellschaften und Wirtschaftssysteme beleuchtet wurde, stellt sich nun die Frage: Wie wirkt sich das auf die Haltung von IT-Sicherheitsunternehmen aus? Dazu lohnt sich zunächst ein Blick auf die Entwicklung des Cybersicherheitsmarktes, der in den vergangenen Jahrzehnten ein enormes Wachstum erlebt hat. Die voranschreitende Digitalisierung, eine verschärfte Bedrohungslage sowie der zunehmende rechtliche Druck haben dazu geführt, dass Unternehmen und Staaten verstärkt in digitale Schutzmaßnahmen investieren. Prognosen deuten darauf hin, dass das Wachstum anhalten wird (siehe Wachstumsprognosen unten).

Während der Markt früher in Bezug auf die Herkunft der Hersteller relativ divers war, lässt sich eine zunehmende Verschiebung zugunsten US-amerikanischer Anbieter beobachten – sowohl durch Neugründungen als auch durch Übernahmen und Fusionierungen mit europäischen und internationalen Unternehmen (siehe Übernahmen & Fusionierungen unten). Diese Verschiebung lässt sich als Spiegelbild der gesellschaftlichen und wirtschaftlichen Unterschiede lesen. Als Sicherheit noch eher ein Nischenthema war, gab es viele europäische Unternehmen wie Avast, Avira, Bitdefender, G Data, Sophos, F-Secure oder ESET, die die IT-Security-Branche geprägt haben. Als in Europa ansässige Anbieter agier(t)en sie innerhalb eines gesellschaftlichen und wirtschaftlichen Kontextes, in dem Sicherheit als Grundlage für Freiheit erachtet und der Schutz der Grundrechte Einzelner als kollektive Verantwortung verstanden wird. Mit dem Marktwachstum haben zunehmend US-amerikanische Hersteller das Spielfeld betreten, die Sicherheit als Geschäftsmodell und damit als Chance zur Wohlstandsmaximierung verstehen. Der Schutz der Nutzer bleibt zwar ein zentrales Anliegen der Hersteller, wird aber stärker in ein marktwirtschaftliches Kalkül eingebettet. Dieser ausgeprägtere Fokus auf ökonomische Prinzipien wird insbesondere dort noch verstärkt, wo Investoreninteressen eine Rolle spielen. Das hat weitreichende Auswirkungen auf unternehmerische Haltungen und Handlungen.

So wird zum Beispiel die Rolle des Nutzers unterschiedlich wahrgenommen. Im Sinne einer eher europäisch geprägten Haltung wird er vorrangig als zu schützendes Subjekt gesehen, während eine US-amerikanische ausgerichtete Mentalität den Nutzer in erster Linie als eigenverantwortlichen Marktteilnehmer wahrnimmt. Anhand von drei weiteren Beispielen sollen die unterschiedlichen Haltungen und deren Auswirkungen auf das unternehmerische Handeln von IT-Sicherheitsanbietern veranschaulicht werden.

Wachstumsprognosen (Auswahl)

- ↗www.gartner.com[8]
- ↗www.marketdataforecast.com[9]
- ↗www.statista.com[10]

Übernahmen & Fusionierung (Auswahl)

- ↗www.heise.de/Avira[11]
- ↗www.handelsblatt.com/Avast[12]
- ↗www.heise.de/Hornetsecurity[13]

Umgang mit Daten

	Europäisch geprägt	US-amerikanisch geprägt
Ethischer Bezug	Privatsphäre als Ausdruck der Menschenwürde	Unternehmerische Selbstverwirklichung durch Datenökonomie
Haltung	Fokus auf Datenschutz	Fokus auf Datenverwertung
Handlung	Es werden ausschließlich Daten erhoben, die für den Schutz und die Produktverbesserung notwendig sind. Informationen über das Nutzerverhalten werden weder für Werbung genutzt noch an Dritte weitergegeben.	Neben den für den Schutz erforderlichen Daten werden auch Verhaltensdaten der Nutzer gesammelt. Diese dienen der Produktanpassung, Schaltung personalisierter Werbung oder werden an Dritte verkauft.
Vorteil	Die Privatsphäre der Nutzer bleibt gewahrt.	Zusätzliche Einnahmen ermöglichen günstigere oder kostenlose Produkte.
Nachteil	Die Lösungen sind tendenziell teurer, weil der Hersteller auf eine Datenmonetarisierung verzichtet.	Kunden geben unter Umständen mehr Daten preis als ihnen bewusst und lieb ist.

Strategie bei der Weiterentwicklung von Lösungen

	Europäisch geprägt	US-amerikanisch geprägt
Ethischer Bezug	Sicherheit als ethischer Auftrag	Sicherheit als Geschäftsmodell
Haltung	Fokus auf Evolution	Fokus auf Disruption
Handlung	Die Weiterentwicklung von Produkten erfolgt meist Schritt für Schritt mit dem Ziel, bestehende Systeme zu verbessern, ohne deren Stabilität oder Kompatibilität zu gefährden. So werden z. B. auch Updates und neue Funktionen sorgfältig getestet.	Die Weiterentwicklung von Lösungen zielt unter anderem darauf ab, bestehende Paradigmen zu durchbrechen und neue Standards zu setzen. Neue Funktionen werden zügig ausgerollt.
Vorteil	Die Lösungen bieten bewährten und stabilen Schutz.	Die Lösungen sind innovativ und schnell anpassbar.
Nachteil	Die Hersteller werden mitunter als weniger innovativ und flexibel wahrgenommen.	Sowohl die Unternehmen als auch deren Nutzer gehen ein höheres Risiko für Fehlfunktionen ein.

Umgang mit technologischen Trends

	Europäisch geprägt	US-amerikanisch geprägt
Ethischer Bezug	Kollektive Verantwortung für den Schutz der Grundrechte	Glücksstreben durch Fortschritt
Haltung	Fokus auf Vorsicht	Fokus auf Vorreiterrolle
Handlung	Neue Technologien wie KI werden zunächst umfassend geprüft und getestet, bevor sie in die Lösungen und Produkte integriert werden. Es wird darauf geachtet, dass ethische Werte wie Nichtdiskriminierung, Transparenz und Privatsphäre zu keinem Zeitpunkt gefährdet werden („ex ante"-Haltung).	Neue Technologien wie KI werden frühzeitig getestet und in Produkte implementiert, um „am lebenden Objekt" auf ihre Leistungsfähigkeit geprüft zu werden. Ethische Implikationen werden dabei zunächst außer Acht gelassen und im Nachhinein adressiert, wenn es zu Problemen kommt („ex post"-Haltung).
Vorteil	Nutzer erhalten ausgereifte und zuverlässige Lösungen, die ihre Grundrechte wahren und dadurch das Vertrauen in KI-Systeme stärken.	Die Lösungen sind geprägt von einer schnellen Weiterentwicklung und hohen Innovationsdynamik, die zuweilen neue Standards setzt.
Nachteil	Innovationen gelangen erst später in die Produkte und Unternehmen müssen aufpassen, technologisch nicht ins Hintertreffen zu geraten.	Risiken durch mangelnde Transparenz oder Privatsphäre können unterschätzt werden, was sowohl für Nutzer als auch für Hersteller zu Problemen führen kann.

Ethische Haltung als Entscheidungshilfe

Diese Gegenüberstellung verdeutlicht, dass IT-Sicherheitsanbieter mit dem Schutz Ihrer Kunden zwar grundlegend ein gemeinsames Ziel verfolgen, aber darüber hinaus ethische Werte und wirtschaftliche Prinzipien unterschiedlich gewichten. Die hieraus resultierenden Haltungen und Handlungen sind maßgeblich von den gesellschaftlichen und wirtschaftlichen Rahmenbedingungen geprägt, innerhalb derer die Anbieter agieren. Konkret lässt sich das folgendermaßen zusammenfassen:

Europäische Hersteller operieren in einem Umfeld, in dem kollektive Verantwortung und die Wahrung von Grundrechten zentrale ethische Werte darstellen. Risiken werden frühzeitig analysiert und abgewogen, um potenzielle Schäden für Nutzer zu vermeiden. Sicherheit wird hier nicht allein als Geschäftsmodell verstanden, sondern als gesellschaftlicher Auftrag. Entscheidungen erfolgen deshalb immer auch unter Berücksichtigung ethischer und sozialer Implikationen, insbesondere im Hinblick auf die Integrität und den Schutz der Nutzer.

US-amerikanische Cybersicherheitanbieter hingegen sind Teil eines Systems, das stark auf individuelle Verantwortung, (unternehmerische) Freiheit und wirtschaftlichen Erfolg ausgerichtet ist. Innovation und Wettbewerb stehen im Vordergrund. Im Allgemeinen haben Unternehmen viele Freiräume, in die nur dann mit Regulierungen eingegriffen wird, wenn gravierende Probleme auftreten. In diesem Umfeld werden technologische Chancen schnell ergriffen, um sich Wettbewerbsvorteile zu sichern. Risiken werden dabei unter Umständen weniger umfassend bewertet. So gelangen neue Technologien schneller zur Marktreife, was im besten Fall zu hochmodernen Schutzlösungen führt, im schlechtesten Fall aber auch zu Instabilitäten oder unerwarteten Sicherheitslücken.

4 Ethik als Treiber für eine sichere digitale Zukunft

Schlussbetrachtung

Beide Herangehensweisen haben ihre Stärken und Schwächen. Gerade in der Cybersicherheit, wo wirtschaftliche Interessen und ethische Verantwortung in einem besonderen Spannungsfeld stehen, können Nuancen in der Unternehmenskultur und -haltung entscheidende Auswirkungen haben. Nutzer sollten sich bewusst mit diesen Unterschieden auseinandersetzen, bevor sie eine Kaufentscheidung treffen. Wer Wert auf schnelle Innovationszyklen und technologische Führerschaft legt, muss möglicherweise akzeptieren, dass neue Lösungen gelegentlich nachjustiert werden müssen – sei es aufgrund technischer Probleme oder einer unrechtmäßigen Datenerhebung bzw. -weitergabe. Wer hingegen Stabilität, Nachhaltigkeit und eine werteorientierte Entwicklung bevorzugt, findet diese tendenziell eher bei europäischen Anbietern, die Sicherheit als gesellschaftliche Verantwortung begreifen.

Letztlich hängt die Entscheidung davon ab, welche Prioritäten Anwender setzen: die Geschwindigkeit und Innovationskraft US-amerikanischer Unternehmen, oder die Verlässlichkeit und ethische Verantwortung europäischer Anbieter. Neben den individuellen Abwägungen sollten Entscheider darüber hinaus die kollektive Wirkung berücksichtigen. Schließlich beeinflussen Sie mit ihrer Entscheidung den gesamten Cybersicherheitsmarkt und dessen weitere Entwicklung.Gerade in Europa ist dies angesichts der aktuellen geopolitischen Herausforderungen und dem wachsenden Wunsch nach digitaler Souveränität von besonderer Bedeutung. In einem so sensiblen Bereich wie der Cybersicherheit wäre es riskant, wenn europäische Märkte und Standards langfristig allzu sehr von US-amerikanischen Unternehmen dominiert und geprägt würden. Die Förderung und Unterstützung europäischer Anbieter trägt dazu bei, technologische Unabhängigkeit zu sichern und zentrale ethische Werte wie die Würde des Menschen, Solidarität und Freiheit nachhaltig zu schützen.

Über ESET – Sicherheit mit Haltung

ESET ist ein europäischer Hersteller von IT-Sicherheitslösungen mit Hauptsitz in Bratislava. Seit der Gründung im Jahr 1992 ist das Unternehmen inhabergeführt und verfolgt eine langfristige, werteorientierte Strategie – unabhängig von kurzfristigen Investoreninteressen. Im Zentrum steht die Überzeugung, dass digitale Sicherheit eine Grundvoraussetzung für ein gutes Leben in einer vernetzten Welt ist.

Dabei versteht ESET gemäß der europäischen Tradition Sicherheit nicht nur als technisches Konzept oder Geschäftsmodell, sondern als ethischen Auftrag. Der Schutz von Menschen, ihrer Daten und ihrer digitalen Selbstbestimmung ist fest in der Unternehmenskultur verankert. Diese Haltung zeigt sich auch im gesellschaftlichen Engagement: ESET unterstützt Hochschulen mit Lehraufträgen, Forschungspartnerschaften und technischer Expertise, etwa in den Bereichen Machine Learning und statistische Analyse. Programme zur Nachwuchsförderung und Diversität, wie der „ESET Science Award" oder „Women in Cybersecurity", werden aktiv vorangetrieben.

Auch die Produktstrategie folgt diesem Wertekompass. Mit dem Ansatz „Prevention First" setzt ESET auf proaktive IT-Sicherheit: Systeme werden von Beginn an so konzipiert, dass Risiken frühzeitig erkannt und abgewehrt werden – idealerweise bevor ein Angreifer überhaupt Zugang erhält. Dieser präventive Ansatz ist nicht nur technisch wirksam, sondern Ausdruck einer sicherheitsbewussten Organisationskultur.

„Unsere Werte sind das Fundament unserer gemeinsamen Vision – Menschen und Unternehmen in der digitalen Welt zu schützen. Unser Ziel besteht nicht nur aus geschäftlichem Erfolg, wir wollen durch unser Verhalten, unsere Handlungen und unsere gegenseitigen Beziehungen eine positive Inspiration für unser Umfeld sein."

— Richard Marko, CEO, ESET, spol. s r.o.

Rechtliche Betrachtung

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 auch 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 in Gestalt 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 im Ergebnis beide Seiten 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 NIS2-Richtlinie und damit die Umsetzung im zukünftigen BSI-Gesetz 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.

IT-Sicherheit ist **Vertrauenssache**

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
- Mitarbeitende 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

Trust Seal
www.teletrust.de/itsmie

„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

Sie möchten wissen, wie Sie ihr Unternehmen effektiv absichern?
↗Kontaktieren Sie uns!

Positionspapier

Made in EU - IT-Sicherheit und Digitale Souveränität

↗ Hier herunterladen

Studie

Digitale Souveränität auf dem Prüfstand

↗ Hier herunterladen

Whitepaper

Cybersecurity und die neue Rechtslage

↗ Hier herunterladen

Whitepaper

NIS2 - Der Countdown läuft

↗ Mehr erfahren

Whitepaper

NIS2 und die Lieferkette

↗ Mehr erfahren

Whitepaper

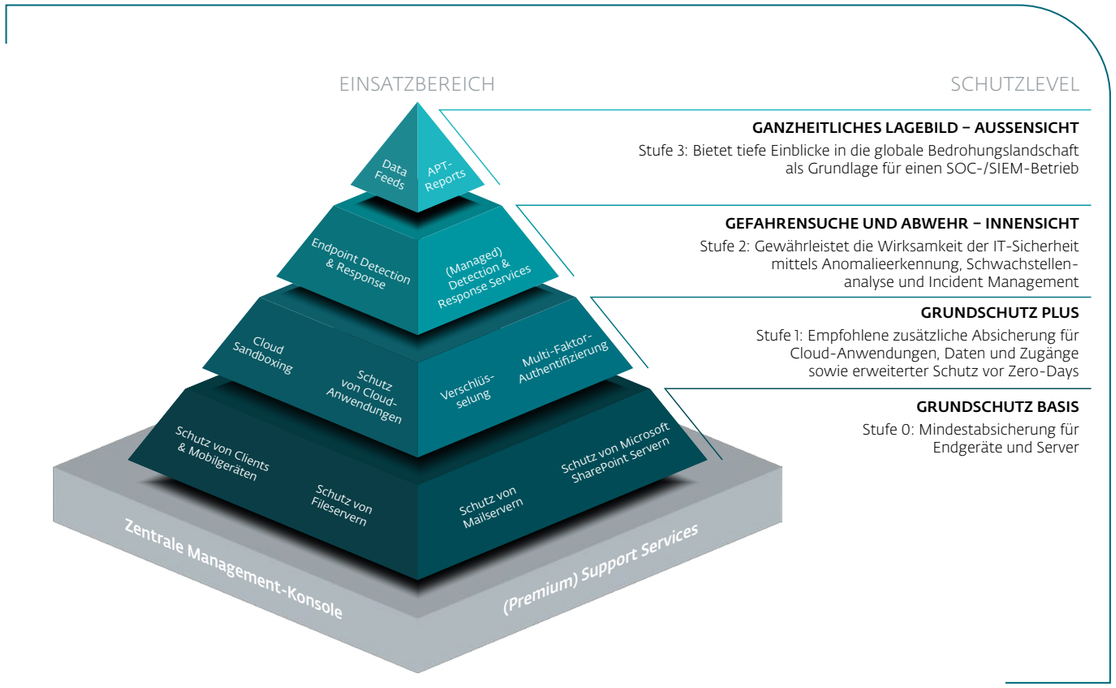
Versichert heißt nicht abgesichert!

↗ Mehr erfahren

↗Erfahren Sie, warum „Made in EU" mehr als ein Gütesiegel ist: ↗**eset.de/eu**.

Zero Trust Security von ESET

Das Zero Trust Security-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 als 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.



ESET MDR: Frühzeitig erkennen, schnell reagieren

ESET bietet Managed Detection & Response (MDR) für KMU und Enterprise. Der Service ESET MDR überwacht Ihre Systeme rund um die Uhr. Die Kombination aus KI und menschlicher Kompetenz sorgt für einen erstklassigen Ransomware-Schutz, auch ohne eigene Sicherheitsspezialisten im Haus.

ESET MDR Ultimate bietet Großunternehmen ein effektives Security Operation Center. Die erfahrenen Spezialisten von ESET führen proaktives Threat Hunting und Threat Monitoring durch, unterstützen Sie bei der Analyse von Sicherheitsvorfällen und ergreifen sofort geeignete Maßnahmen.

Literaturverzeichnis

1 https://netzpolitik.org/2018/cambridge-analytica-was-wir-ueber-das-groesste-datenleck-in-der-geschichte-von-facebook-wissen/

2 https://dsgvo-gesetz.de/

3 https://de.wikisource.org/wiki/Unabh%C3%A4ngigkeitserkl%C3%A4rung_der_Vereinigten_Staaten_von_Amerika

4 https://www.europarl.europa.eu/charter/pdf/text_de.pdf

5 https://de.wikipedia.org/wiki/Stella_Liebeck

6 https://artificialintelligenceact.eu/de/

7 https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

8 https://www.gartner.com/en/articles/information-security

9 https://www.marketdataforecast.com/market-reports/cyber-security-market

10 https://www.statista.com/outlook/tmo/cybersecurity/worldwide

11 https://www.heise.de/news/Zweite-Avira-Uebernahme-in-2020-diesmal-durch-NortonLife-Lock-4983234.html

12 https://www.handelsblatt.com/technik/it-internet/it-sicherheit-milliardendeal-der-anti-viren-firmen-norton-life-lock-uebernimmt-avast/27503356.html

13 https://www.heise.de/news/E-Mail-Sicherheit-Proofpoint-kauft-Hornetsecurity-10385250.html

3 VON ÜBER 500.000 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

T

ISP Security Partner seit 2008
2 Millionen Kunden

BEWÄHRT

Secur IT y made in EU
Trust Seal www.teletrust.de/itsmie

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

ISO 9001 SGS ISO/IEC 27001 SGS

Unsere Lösungen sind nach den Qualitäts- und Informationssicherheitsstandards 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 Entwicklungszentren weltweit

ÜBER ESET

Als europäischer Hersteller mit mehr als 35 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