kaspersky

Internationale Zusammenarbeit, Transparenz, Vertrauen, Risikomanagement und lokale Verantwortung: Fünf wichtige Säulen der DNA von Kaspersky

Als weltweit tätiges Cybersicherheitsunternehmen leistet Kaspersky wichtige Beiträge zum Cybersicherheits-Ökosystem in Deutschland und der Europäischen Union. Kaspersky ist ein privat geführtes Unternehmen, die Konzernholding hat ihren Sitz in London, Großbritannien. In den verschiedenen Ländern sind rechtlich selbständige Landesgesellschaften, in Deutschland die Kaspersky Labs GmbH, aktiv. Die Aufgabenverteilung ermöglicht es, internationale und regionale Aktivitäten effektiv, kundenorientiert marktnah zu erbringen.

In diesem Papier erhalten Sie Informationen darüber, wie (i) Kaspersky durch **landesweite aber auch grenz- und branchenübergreifende Zusammenarbeit den Schutz und die Sicherheit der Anwender erhöht,** warum (ii) **die Stärkung der Cybersicherheit und Erhöhung der Cyber-Resilienz unser Handeln bestimmt,** und über (iii) **den herausragenden Stellenwert von Transparenz und Vertrauen als wesentliche Grundlage für eine sichere Digitalisierung.** Antrieb und **Hauptmotivation unserer Arbeit ist es, Bürger, Unternehmen und Behörden in Deutschland bestmöglich zu schützen.**

Die **Unternehmensprozesse von Kaspersky** sind so ausgerichtet, dass Kunden ein **Höchstmaß an Resilienz erwarten und auf eine bestmögliche Geschäftskontinuität vertrauen können.** Ermöglicht wird dieses durch eine ausgewogene und strukturierte Verteilung der Aufgaben und Verantwortlichkeiten zwischen dem HQ und den Landesgesellschaften. Dadurch können wir sicherstellen, unseren Verpflichtungen gegenüber Partnern, Kunden und potenziellen Neukunden bestmöglich nachzukommen – von der Lieferung von Produkten, über den Support bis hin zur Sicherstellung von Finanztransaktionen.

1/ Kooperationen in Deutschland

Kaspersky ist ein wichtiger, innovativer und verantwortungsbewusster Akteur im deutschen und europäischen Cybersicherheits-Ökosystems. Das Unternehmen bringt seine Expertise in zahlreiche Kooperationen ein, zum Beispiel als Partner der **Allianz für Cyber-Sicherheit** des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der Initiative **„Deutschland sicher im Netz“** unter der Schirmherrschaft des Bundesministeriums des Innern und für Heimat, als Mitglied des **Digitalverbands Bitkom,** in der **„Plattform Industrie 4.0“** oder als Mitglied des **Münchner Kreises.** Darüber hinaus arbeitet Kaspersky mit zahlreichen Universitäten, Forschungseinrichtungen und Non-Profit-Organisationen in Deutschland zusammen.

2/ Kooperationen auf europäischer Ebene

Der europäische Binnenmarkt ist weltweit der größte Markt für Cybersicherheit. Dies trifft auch auf Kaspersky zu: Europa ist der größte Markt für das Unternehmen – über alle Branchen hinweg. Daher ist Europa für die Unternehmensstrategie von Kaspersky von zentraler Bedeutung. Hier arbeiten wir mit zahlreichen nationalen und internationalen Organisationen zusammen. So sind wir beispielsweise an mehreren Studien und Publikationen der **Agentur der Europäischen Union für Cybersicherheit ENISA** beteiligt. Ein Forscher aus unserem GReAT-Team ist Mitglied der ENISA Ad-hoc-Arbeitsgruppe zu „EU Cyber Threat Landscapes“. Mit **Europol** pflegen wir eine **enge Zusammenarbeit mit dem EC3,** wo wir **Mitglied des Beirats für Internetsicherheit** sind. Gemeinsam mit Europol, der niederländischen Polizei und McAfee haben wir zudem die globale Initiative **NoMoreRansom** ins Leben gerufen. Wir sind derzeit Konsortialpartner in vier europäischen **„Horizon 2020 Projekten“.** Gemeinsam mit ENISA und dem deutschen **Bundesamt für Sicherheit in der Informationstechnik (BSI)** haben unsere Experten im Januar 2021 an einer Konsultation zu KI und Cybersicherheit des **AIDA-Ausschusses des Europäischen Parlaments** beigetragen.

3/ Weltweite Kooperationen

Kaspersky ist ein Industriepartner des **Europarats** zur Förderung eines offenen und sicheren Internets und ist Partner des **„Geneva Dialogue on Responsible Behavior in Cyberspace".** Wir sind Mitglied von **FIRST,** dem globalen „Forum of Incident Response and Security Teams". Kaspersky hat an den **OECD-Berichten** 2021 zur digitalen Sicherheit und Schwachstellenbehandlung mitgewirkt, gehört zu den Erstunterzeichnern der Deklaration **„Paris Call for Trust & Security in Cyberspace"** und beteiligt sich an Gesprächsformaten der **Vereinten Nationen** – z. B. im Rahmen der Offenen Arbeitsgruppe der UNO zu Entwicklungen im Bereich der Informations- und Kommunikationstechnologie im Kontext der internationalen Sicherheit. Wir engagieren uns in all diesen Gremien und Organisationen, weil in der Cybersicherheit eine vertrauensvolle Zusammenarbeit und Informationsaustausch wesentlich ist. Kaspersky wird als vertrauenswürdiger Partner in Europa und weltweit geschätzt.

4/ Globales Denken – lokales Handeln

Seit 2008 betreibt Kaspersky ein diversifiziertes Finanzsystem. Die Landesgesellschaften betreiben ihr Finanzwesen unabhängig – von der eigenständigen Verwaltung der Einnahmen und Ausgaben bis hin zum Handling von Partnerbeauftragungen. Die Landesgesellschaften führen ihre Finanztransaktionen im jeweiligen Land durch und haben Hausbanken vor Ort.

5/ Globale Transparenz-Initiative (GTI)

Im Rahmen der weltweiten Transparenzinitiative (GTI), hat Kaspersky folgende Maßnahmen ergriffen:

- **Datenspeicherung und Verarbeitung in der Schweiz.** Kaspersky betreibt eine Dateninfrastruktur in zwei hochsicheren Rechenzentren in Zürich zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden aus Europa, den Vereinigten Staaten und Kanada sowie in mehreren asiatisch-pazifischen Ländern.
- **Einrichtung von „Tranzparenzzentren"** für die Überprüfung des Quellcodes, aller Versionen unserer Builds und der AV-Datenbank, der Softwareentwicklung und des Datenmanagements – einschließlich der Überprüfung der Informationen, die Kaspersky-Produkte an das cloudbasierte Kaspersky Security Network (KSN) senden. Darüber hinaus gewähren wir auch Zugang zu unserem Quellcode, um sicherzustellen, dass dieser mit öffentlich verfügbaren Modulen übereinstimmt. Kaspersky stellt auch Software-Stücklisten (SBOM) für seine Produkte zur Verfügung. Unsere Transparenzzentren befinden sich in Zürich, Madrid, Kuala Lumpur, São Paulo und New Brunswick (seit 2021 in Partnerschaft mit der CyberNB Association).
- **Die Sicherheit und Zuverlässigkeit unserer technischen und organisatorischen Verfahren und Datendienste wurden von zwei externen, unabhängigen Prüforganisationen bestätigt.** Kaspersky hat das SOC-2-Audit (Service Organization Control for Service Organizations) Typ 1 durch einen Big-Four-Auditor erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigte. Darüber hinaus wurden unsere Datendienste vom TÜV AUSTRIA nach ISO/IEC 27001:2013 zertifiziert.
- **Vulnerability Management Program.** Im März 2018 haben wir im Rahmen eines Bug Bounty-Programms die Prämien für externe Forscher, die in unseren Produkten kritische Schwachstellen finden, auf bis zu 100.000 US-Dollar erhöht. Seitdem haben wir 53 Prämien vergeben, obwohl noch nie eine kritische Sicherheitslücke gemeldet wurde. Mit diesem Ansatz zur Analyse, Management und Offenlegung von Schwachstellen verbessern wir ständig die Sicherheit unserer Produkte. Um mehr Transparenz im Umgang mit Sicherheitslücken zu schaffen, hat Kaspersky ethische Grundsätze für die verantwortungsvolle Offenlegung von Sicherheitslücken veröffentlicht.