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, der DACH-Region, in Europa sowie weltweit. Kaspersky ist ein privat geführtes Unternehmen, die Konzernholding (Kaspersky Labs Limited) hat ihren Sitz in London, Großbritannien. In den verschiedenen Ländern sind rechtlich eigenständige Landesgesellschaften, in Deutschland die Kaspersky Labs GmbH, aktiv. Die Aufgabenverteilung ermöglicht es, internationale und regionale Aktivitäten effektiv, kundenorientiert sowie marktnah zu erbringen. Die Kaspersky Labs GmbH zahlt ihre Steuern, Löhne und Sozialabgaben in Deutschland, die Kaspersky Labs Schweiz in der Schweiz.

In diesem Papier erhalten Sie Informationen darüber, wie

- Kaspersky durch **landesweite sowie grenz- und branchenübergreifende Zusammenarbeit den Schutz und die Sicherheit der Anwender erhöht,**
- warum **die Stärkung der Cybersicherheit und Erhöhung der Cyberresilienz unser Handeln bestimmt,** und
- warum Kaspersky **Transparenz und Vertrauen höchste Bedeutung als wesentliche Grundlagen für eine sichere Digitalisierung beimisst.**

Antrieb und **Hauptmotivation der Arbeit von Kaspersky ist es, dass Bürger, Unternehmen und Behörden in Deutschland, in der DACH-Region, in Europa sowie weltweit die Chancen der Digitalisierung sicher, zuverlässig und vertrauenswürdig ergreifen können.**

Die **Unternehmensprozesse von Kaspersky** sind auf ein **Höchstmaß an Resilienz ausgerichtet, so dass Kunden und Partner auch in Zeiten geopolitischer Spannungen auf eine bestmögliche Geschäftskontinuität und höchste Sicherheit vertrauen können.** Ermöglicht wird dies durch eine ausgewogene und strukturierte Verteilung der Aufgaben und Verantwortlichkeiten zwischen dem HQ und den Landesgesellschaften, durch organisatorische, infrastrukturelle und technische Maßnahmen sowie umfangreiche Mitarbeiter:innen-Qualifizierungen. Dadurch kann Kaspersky sicherstellen, seinen 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 innovativer und verantwortungsbewusster Akteur im deutschen und europäischen Cybersicherheits-Ökosystem. Das Unternehmen bringt seine Expertise in zahlreiche Kooperationen ein und unterhält ein umfassendes Partnernetzwerk. Zudem bietet Kaspersky kostenfreie Lösungen, Dienstleistungen und Schulungen an, um die Cybersicherheit und Resilienz in Deutschland nachhaltig zu erhöhen.

2/ Kooperationen auf europäischer Ebene

Der europäische Binnenmarkt ist weltweit der größte Markt für Cybersicherheit. Dies trifft auch auf Kaspersky zu: Europa ist für das Unternehmen eine strategisch wichtige Region – über alle Branchen hinweg. Daher ist Europa für die Unternehmensstrategie von Kaspersky von besonderer Bedeutung. Hier arbeitet Kaspersky mit zahlreichen nationalen und internationalen Organisationen zusammen. Kaspersky hat unter anderem an mehreren Studien und Publikationen der **Agentur der Europäischen Union für Cybersicherheit ENISA** mitgewirkt. Ein Forscher aus dem Global Research and Analysis Team (GReAT-Team) von Kaspersky war Mitglied der ENISA Ad-hoc-Arbeitsgruppe zu „EU Cyber Threat Landscapes“. Gemeinsam mit Europol, der niederländischen Polizei und McAfee hat Kaspersky die globale Initiative **NoMoreRansom** ins Leben gerufen. Zudem ist Kaspersky derzeit Konsortialpartner in vier europäischen **„Horizon 2020 Projekten“**. Gemeinsam mit ENISA und dem deutschen **Bundesamt für Sicherheit in der Informationstechnik (BSI)** haben Kaspersky-Experten im Januar 2021 an einer Konsultation zu KI und Cybersicherheit des **AIDA-Ausschusses des Europäischen Parlaments** mitgewirkt.

kaspersky

3/ Weltweite Kooperationen

Kaspersky ist Industriepartner des **Europarats** zur Förderung eines offenen und sicheren Internets sowie Partner des **„Geneva Dialogue on Responsible Behavior in Cyberspace".** Das Unternehmen 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 oder beim **Internet Governance Forum (IGF)**. Kaspersky verfolgt einen dezidierten Multistakeholder-Ansatz und engagiert sich in diesen Gremien und Organisationen, weil in der Cybersicherheit eine vertrauensvolle Zusammenarbeit und Informationsaustausch wesentlich sind.

4/ Diversifiziertes Finanzsystem

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 Transparenzinitiative (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, Utrecht, Rom, Woburn (USA), Tokyo, Kuala Lumpur (Malaysia), Singapur und São Paulo (Brasilien).
- **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 und Typ 2 erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigt. Darüber hinaus wurden unsere Datendienste 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 zu 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.