kaspersky

Sicherheit, Zuverlässigkeit, Vertrauenswürdigkeit, Transparenz und Qualität:

Worauf Sie sich bei Kaspersky verlassen und wie Sie das überprüfen können!

Seit der Warnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind einige Fragen zur Zuverlässigkeit, Vertrauenswürdigkeit und Sicherheit von Kaspersky und der Kaspersky Antiviren-Software (AV) aufgekommen. Mit diesem Papier möchten wir diese Fragen transparent beantworten und Ihnen Informationen darüber geben,

- wie Kaspersky die Prinzipien und Grundsätze von Sicherheit, Verfügbarkeit, Vertraulichkeit und Datenschutz in der Softwareentwicklung und Softwareverteilung plant, organisiert und umsetzt,
- wie sich das Unternehmen externen Zertifizierungen nach international anerkannten Standards stellt,
- was Kaspersky unter Transparenz versteht und wie das Unternehmen dies im Umgang mit Kunden, Partnern und anderen Stakeholdern lebt.

Als **internationales Cybersicherheitsunternehmen** leistet **Kaspersky** wertvolle Beiträge zu **Cybersicherheit und Resilienz** in Deutschland, der DACH-Region, in Europa sowie weltweit.

Kaspersky ist ein **privat geführtes Unternehmen**. Die **Konzernholding** hat ihren Sitz in **London** (UK).

In den verschiedenen Ländern sind **rechtlich eigenständige Landesgesellschaften** tätig. In Deutschland ist das die Kaspersky Labs GmbH.

Die Kaspersky Labs GmbH zahlt in Deutschland **Steuern, Sozialabgaben, Löhne** und tätigt **Investitionen** in Forschung und Entwicklung.

Kaspersky beschäftigt alleine in **Europa** rund **700 Mitarbeiter:innen**. Das ***Global Research and Analysis Team (GReAT)*** wird aus Bukarest in **Europa** gesteuert. Der größte Teil der GReAT Forscher ist in der EU ansässig.

Trotz der aktuellen geopolitischen Lage sowie der BSI-Warnung erbringt Kaspersky alle vertraglich vereinbarten Leistungen in bester Qualität, in vollem Umfang und ohne jegliche Einschränkungen. Insbesondere funktioniert die Software einwandfrei, sie weist keine technischen Schwachstellen auf *(wie auch das BSI und das Oberverwaltungsgericht Münster (OVG) bestätigen, siehe S. 2)* und bietet ein höchstmögliches Schutzniveau, wie zahlreiche unabhängige externe Tests zeigen.

Zertifizierte und auditierte Sicherheit

Das BSI schreibt auf seiner Homepage: *„Mit einem Zertifikat kann eine Organisation nachweisen, dass ein Produkt oder eine Dienstleistung definierten Sicherheitsanforderungen entspricht. Eine unabhängige Prüfung durch das BSI schafft Vertrauen und weist Vertraulichkeit, Authentizität und Verfügbarkeit transparent nach.“* Kaspersky teilt diese Auffassung und unterzieht sich regelmäßig umfassenden Zertifizierungen nach international anerkannten Standards. Kaspersky Software wurde 2018 und 2022 nach Common Criteria in Spanien und Italien zertifiziert. 2021 wurde das Informationssicherheits-Management System von Kaspersky gemäß ISO 27001 durch den TÜV Austria erneut zertifiziert. Eine der vier großen globalen Wirtschaftsprüfungsgesellschaften (Big Four) hat 2019 und erneut 2022 mit Stichtag 28. April die Software-Entwicklungs- und -Verteilungsprozesse von Kaspersky gemäß SOC 2-Typ 1 nach den Richtlinien des vom American Institute of Certified Public Accountants (AICPA) entwickelten Standards (AICPA Professional Standard) auditiert.

Wie sich die Software zusammensetzt

Kaspersky stellt Kunden, Partnern und Regulierern eine Software Bill of Materials *(SBOM)* zur Verfügung. Hierbei handelt es sich um eine Liste aller Softwarekomponenten. Sie besteht aus Belegmaterialien, die die Teile beschreiben, aus denen eine Software zusammengesetzt ist. SBOM ist eine immer

kaspersky

gängigere bewährte Praxis innerhalb der Branche. Sie erhöht die Transparenz von Software und verbessert die Sichtbarkeit der Software-Zusammensetzung und -Architektur, um den Aufbau einer zuverlässigen und vertrauenswürdigen digitalen Infrastruktur zu fördern.

Analyse des Quellcodes in Echtzeit - zu jeder Zeit

Wenn Sie sich noch mehr Sicherheit und Transparenz verschaffen wollen, können Sie den Quellcode in einem Transparenzzentrum oder über abgesicherte Remote-Umgebungen analysieren und prüfen. Hiervon haben bereits zahlreiche europäische Behörden, wissenschaftliche Einrichtungen sowie Kunden und Partner Gebrauch gemacht. Die Reviews erfordern professionelles IT-Wissen aus Ihrem Hause oder von Dienstleistern. Da nicht nur die aktuelle Software-Version, sondern alle Vorversionen überprüft und mit der tatsächlich ausgelieferten Version verglichen werden können, bietet diese Prüfung das höchste Maß an Sicherheit. Im Markt für Antiviren-Software ist dieses Angebot weltweit einmalig.

Frankreich - Nationale Agentur für die Sicherheit von Informationssystemen (ANSSI)
"Im aktuellen Kontext kann die Verwendung bestimmter digitaler Tools, insbesondere der Firma Kaspersky, aufgrund ihrer Verbindung zu Russland in Frage gestellt werden. Zum jetzigen Zeitpunkt gibt es keinen objektiven Grund, die Bewertung der Qualität der angebotenen Produkte und Dienstleistungen zu ändern."
Quelle: https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

Schweiz - Nationales Zentrum für Cybersicherheit (NCSC)
Das NCSC erklärt auf Anfrage, dass es keine Kenntnis von einem Missbrauch seitens Kaspersky hat. *"Wenn das NCSC irgendwelche Beweise in dieser Hinsicht hätte, würde es die Öffentlichkeit entsprechend warnen und informieren", schreibt Pascal Lamia, der operative Leiter des Zentrums.*
Quelle: https://www.inside-it.ch/deutsches-bundesamt-fuer-cybersicherheit-raet,-kaspersky-software-zu-verbannen-20220315

Belgien - Zentrum für Cybersicherheit Belgien (CCB)
„Auch das Centre for Cybersecurity Belgium (CCB) sieht derzeit keine Bedrohung."
Quelle:https://www.computable.nl/artikel/nieuws/security/7329186/250449/duitse-overheid-waarschuwt-voor-kaspersky.html

Österreich - Austrian CERT (cert.at)
„CERT.at liegen derzeit keine Informationen vor, dass Kaspersky-Produkte schädliche Funktionen enthalten."
Quelle: CERT.at-Mitteilung an österreichische Unternehmen

Die BSI Warnung ist in Europa einmalig

Von den 27 Cybersicherheitsbehörden in den EU-Mitgliedsstaaten haben *(Stand 4.5.2022)* nach unserem Kenntnisstand lediglich 9 Behörden Informationen zur Nutzung russischer Software herausgegeben. Eine mit der des BSI vergleichbare geopolitische Warnung gibt es in keinem anderen europäischen Staat. *(Einige Beispiele sind im Kasten rechts oben aufgeführt).*

Kaspersky gewährleistet robuste, sichere und verlässliche Geschäftsprozesse

Das Kaspersky-Team prüft kontinuierlich und proaktiv alle potenziellen Risiken, die sich aus der geopolitischen Situation ergeben und ist in der Lage, bei Bedarf sehr schnell zu handeln. Dabei bewertet Kaspersky auch potenzielle Auswirkungen der Einschränkungen des zwischenstaatlichen Datenaustauschs auf die Produkte und Dienstleistungen des Unternehmens. Alle bisherigen Tests und Untersuchungen haben gezeigt, dass die globale Serverinfrastruktur den unterbrechungsfreien Betrieb des Portfolios von Kaspersky ermöglicht, und dass das Kaspersky Security Network KSN zur Verarbeitung von Cybersicherheitsdaten nicht beeinträchtigt wird. Die Cloud-Server-Infrastruktur ist global verteilt, unter anderem in der Schweiz, Deutschland, China und Kanada. Verfügbarkeit, Kontinuität und Verarbeitungsgeschwindigkeit der Server erfüllen höchste Ansprüche. Daten, die Kaspersky-Nutzer in Europa freiwillig an das KSN zur automatischen Malware-Analyse übermitteln, werden nur an europäische Server gesendet.

BSI empfiehlt individuelle Risikoanalyse
Auf seiner Website weist das Bundesamt darauf hin, dass jede Einrichtung eine individuelle Risikoanalyse durchführen sollte. Die Entscheidung, ob ein Unternehmen oder eine Behörde Kaspersky nutzen möchte, muss deswegen jede Einrichtung gemäß individueller Risikoanalyse selbst treffen. Das OVG NRW schreibt in seinem Beschluss, dass das BSI in der Warnung deutlich macht, dass **keine konkreten Hinweise** dafür vorliegen, *„dass **mit Hilfe der Virenschutzprogramme von Kaspersky Daten unberechtigt abgegriffen würden oder sonst Tatsachen bekannt seien**, durch die Software sei bereits **Missbrauch** erfolgt. **Ebenfalls deutlich wird, dass die Warnung nicht auf konkreten technischen Mängeln an den von der Antragstellerin vertriebenen Virenschutzprogrammen beruht."*** Zudem bestätigt das OVG, *„**dass das Bundesamt aufgrund der aktuellen geopolitischen Lage und den damit verbundenen Risiken eines russischen Cyberangriffs vor der Nutzung der Virenschutzsoftware des Herstellers Kaspersky warnt**."*

Auch in Zukunft können Sie auf Kaspersky als verlässlichen Vertragspartner und leistungsfähigen IT-Sicherheitsanbieter setzen!