kaspersky

RISIKOMANAGEMENT ZUR GEWÄHRLEISTUNG AUSREICHENDER SICHERHEIT

Das BSI hat in seiner Warnung folgende Risiken identifiziert:

Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen eigenen Willen gezwungen werden, Zielsysteme anzugreifen, oder selbst als Opfer einer Cyber-Operation ohne seine Kenntnis ausspioniert oder als Werkzeug für Angriffe gegen seine eigenen Kunden missbraucht werden.

Quelle: BSI-W 0004 | Version 1.0 vom 15.03.2022; S. 1

Wie Kaspersky den Risiken begegnet:

Selbst wenn die russische Regierung Kaspersky mit Gewalt zwingen würde, Schadsoftware zu integrieren, verhindern die mehrfach verschachtelten Freigabeprozesse mit einem höchst restriktiven Rollen- und Rechte-Modell mit an Sicherheit grenzender Wahrscheinlichkeit, dass Updates mit Schadsoftware auf die Upload Server gelangen!

kaspersky

kaspersky

Die Softwareentwicklung und –verteilung ist vor unberechtigtem Zugriff geschützt!

SOC2 ist ein Blick „hinter die Kulissen“

- **Wer und wie?** Der Wirtschaftsprüfer macht sich ein Bild davon, ob die bei Kaspersky vorherrschenden Regelungen und Maßnahmen gut umgesetzt sind und die geforderten Kriterien für Vertrauensdienste (**Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Vertraulichkeit und Datenschutz**) erfüllt. **Kaspersky** erfüllt **alle 72 Kriterien ohne Einschränkung**.
- **Was?** Prüfungsgegenstand ist die **Entwicklung und Implementierung von Antivirenprogrammen für Windows und Unix Betriebssysteme durch Kaspersky**. Die Prüfung weist nach, dass der Prozess von Kaspersky die Kriterien für Vertrauensdienste erfüllt.
- **Warum?** Das **SOC 2 Typ 1** Audit (**S**ystem and **O**rganization **C**ontrols) ermöglicht Dritten einen transparenten Einblick in die Abläufe der Softwareentwicklung und –bereitstellung bei Kaspersky. Es ist also ein **Blick „hinter die Kulissen“**.
- Weitere Informationen: https://www.kaspersky.com/about/compliance-soc2

Common Criteria (CC)-Zertifizierung für KES und KSC

- *Die **Common Criteria for Information Technology Security Evaluation** (kurz auch **Common Criteria** oder **CC**; zu deutsch: Allgemeine Kriterien für die Bewertung der Sicherheit von Informationstechnologie) sind ein internationaler Standard zur Prüfung und Bewertung der Sicherheitseigenschaften von IT-Produkten.*

- Kaspersky Endpoint Security (KES), das Flaggschiff unter den Unternehmensprodukten, wurde in Spanien nach den Common Criteria (CC) zertifiziert. Die Zertifizierung ist europaweit anerkannt: https://commoncriteriaportal.org/files/epfiles/2018-37-INF-2718.pdf

- Das Kaspersky Security Center (KSC), die Kontrollkonsole für unsere Unternehmensprodukte, wurde ebenfalls nach Common Criteria (CC) in Italien zertifiziert. Die Zertifizierung ist europaweit anerkannt: https://ocsi.isticom.it/documenti/certificazioni/kaspersky/cr_ksc13_v1.0_en.pdf

Common Criteria for Information Technology Security Evaluation

- Die Common Criteria unterscheiden zwischen der **Funktionalität (Funktionsumfang)** des betrachteten Systems und der **Vertrauenswürdigkeit (Qualität)**.
- Die Vertrauenswürdigkeit wird nach den Gesichtspunkten der **Wirksamkeit der verwendeten Methoden** und der **Korrektheit der Implementierung** betrachtet.
- Im Dezember 1999 sind die Common Criteria zum International Standard ISO/IEC 15408 erklärt worden. Der deutsche Anteil an dieser Arbeit wird u. a. vom DIN NIA-01-27 IT-Sicherheitsverfahren betreut.

ISO 27001 Zertifizierung & Re-Zertifizierung

- Der Geltungsbereich der Zertifizierung umfasst die Kaspersky Data Services (KSN), einschließlich:
  - KSN-System für die sichere Speicherung und den Zugriff auf diese Dateien (KLDFS); und
  - KSN-Systeme für die Verarbeitung von Statistiken (genannt KSNBuffer-Datenbank).
- Die Zertifizierung gilt für die **Datendienste des Unternehmens in den Rechenzentren in Zürich, Frankfurt, Toronto, Moskau und Peking**.
- Die Konformität mit ISO/IEC 27001:2013 - einem international anerkannten Best-Practice-Industriestandard und anwendbaren Sicherheitsstandard - bildet den Kern von Kasperskys Ansatz zur Implementierung und Verwaltung der Informationssicherheit.
- Link zur Re-Zertifizierung von 2022; den Abschlussbericht mit der Beschreibung stellen wir unseren Kunden und Partnern auf Anfrage zur Verfügung.
- Weitere Informationen https://www.kaspersky.com/about/iso-27001

kaspersky

Veröffentlichungen von Cybersicherheitsbehörden aus Europa

Weitere Empfehlungen/Bewertungen von europäischen Cybersicherheitsgremien zu Kaspersky

- **FRANKREICH** – Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)
  - „In der aktuellen Situation kann die Verwendung bestimmter digitaler Anwendungen, insbesondere die der Firma Kaspersky, wegen der Verbindung zu Russland in Frage gestellt werden. Zum jetzigen Zeitpunkt gibt es keinen Grund, die Bewertung der (von Kaspersky) angebotenen Produkte und Dienstleistungen zu ändern."

- ÖSTERREICH – Austrian Cert (CERT.at)
  - „CERT.at liegen derzeit keine Informationen vor, dass Kaspersky-Produkte schädliche Funktionen enthalten."

- **SCHWEIZ** – National Cyber Security Center (NCSC)
  - „Bis heute ist dem NCSC **kein Missbrauch der Kaspersky Antiviren-Software** in der Schweiz gemeldet worden. Sollte der NCSC verifizierte Informationen über einen Missbrauch erhalten, wird die Öffentlichkeit umgehend informiert und gewarnt."

Weitere Empfehlungen/Bewertungen von europäischen Cybersicherheitsgremien zu Kaspersky

- **VEREINIGTES KÖNIGREICH** – National Cyber Security Centre (NCSC)
  - „Wir haben Anfragen von Leuten erhalten, die sich Sorgen um ihre heimische IT machen. Es ist ziemlich sicher zu sagen, dass fast alle Privatpersonen im Vereinigten Königreich (und viele Unternehmen) nicht von russischen Cyberangriffen betroffen sein werden, **unabhängig davon, ob sie russische Produkte oder Dienstleistungen nutzen.**“

- **NIEDERLANDE** - National Cyber Security Center (NCSC) and Digital Trust Center (DTC)
  - „Es gibt derzeit keinen Grund zur Annahme, dass der Einsatz von Kaspersky-Software ein erhöhtes Risiko für Unternehmen darstellt.“

- **BELGIEN** – Centre for Cybersecurity Belgium (CCB)
  - „Auch das Centre for Cybersecurity Belgium (CCB) sieht derzeit keine Bedrohung.“

kaspersky

Konzernstruktur und Prinzipien

Was Kaspersky auszeichnet!

Globaler Anbieter – Schlüsselmarkt Europa – Holding UK

In rund **200** Ländern aktiv

34 Landesgesellschaften

North America
Mexico
USA

South America
Brazil
Argentina
Columbia
Mexico

Africa
South Africa

Australia

Europe
Austria
Czech Republic
Denmark
France
Germany
Israel
Italy
Netherlands
Poland
Portugal
Romania
Russia
Spain
Switzerland
UK (Holding)

Asia
China
Hong Kong
India
Japan
Kazakhstan
Malaysia
Singapore
South Korea
Turkey
UAE

Transparency Centers
Zurich, Switzerland
Madrid, Spain
São Paulo, Brazil
Kuala Lumpur, Malaysia
New Brunswick, Canada

Struktur des Kaspersky Konzerns

- **Oberste Konzerngesellschaft (Holding)** ist die **Kaspersky Labs Limited (KLL)** mit Sitz in London, UK
- Sowohl die **Holding** als auch die **Tochtergesellschaften** (unter anderem in Deutschland, Frankreich, Italien, Österreich, Russland, Spanien, Schweiz, Rumänien, den USA, China und vielen anderen Staaten) sind **Gesellschaften mit beschränkter Haftung**

*Die **offiziellen Informationen zur Holding KLL** und zur britischen Tochtergesellschaft Kaspersky Labs UK Limited (KLUK) einschließlich der Steuerberichte, finden Sie auf der **Website des britischen Handelsregisters**:*

- KLL - https://find-and-update.company-information.service.gov.uk/company/04249748
- KLUK - https://find-and-update.company-information.service.gov.uk/company/03654151

Forschung und Entwicklung

>4,300 hochqualifizierte Spezialisten

1/3 R&D-Spezialisten

40+ welweit führende Sicherheitsexperten unsere Elite-Gruppe GReAT

> 400.000.000 Privatnutzer

> 240.000 Geschäftskunden

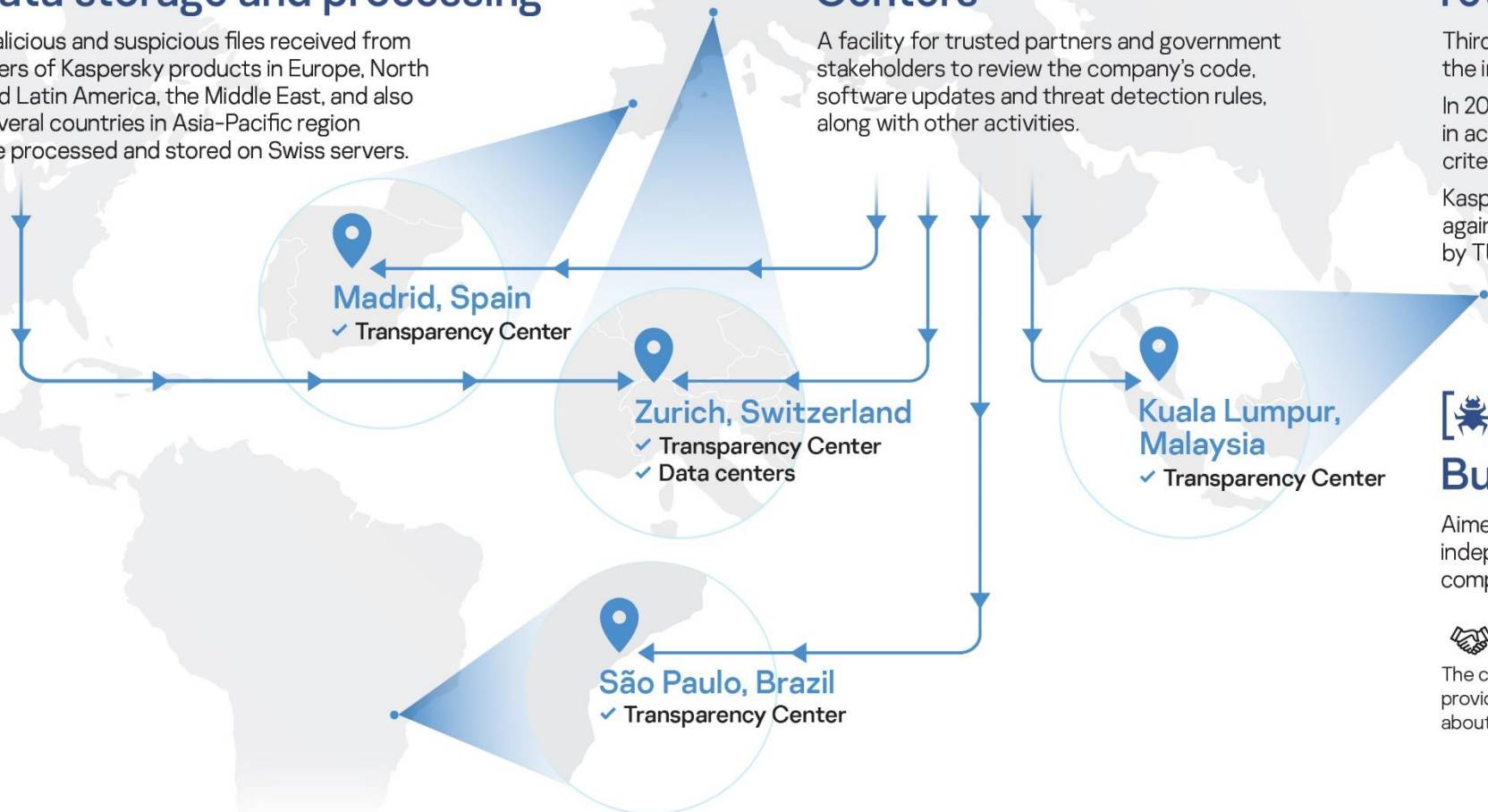
Kaspersky Global Transparency Initiative

Cyberthreat-related user data storage and processing

Malicious and suspicious files received from users of Kaspersky products in Europe, North and Latin America, the Middle East, and also several countries in Asia-Pacific region are processed and stored on Swiss servers.

Transparency Centers

A facility for trusted partners and government stakeholders to review the company's code, software updates and threat detection rules, along with other activities.



Independent review

Third-party assessment of internal processes to verify the integrity of Kaspersky solutions and processes.

In 2019 Kaspersky has achieved the SOC 2 Type 1 report in accordance with the SSAE 18 standard (Security criteria) issued by one of the Big Four accounting firms.

Kaspersky's data services have also been certified against ISO/IEC 27001:2013 international standard by TÜV AUSTRIA.

Bug bounty program

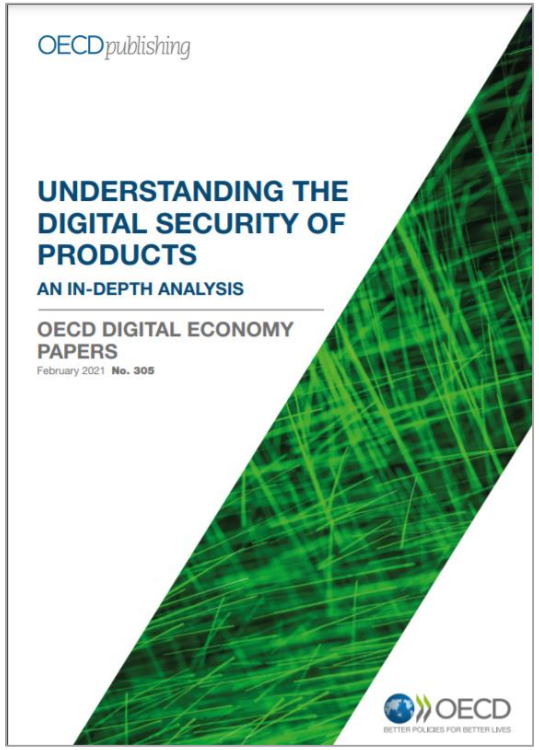
Aimed to make Kaspersky more secure, it encourages independent security researchers to supplement the company's own work in vulnerability detection and mitigation.

The company also supports the Disclose.io framework which provides Safe Harbor for vulnerability researchers concerned about possible negative legal consequences of their discoveries.

kaspersky BRING ON THE FUTURE

Proven. Transparent. Independent.

Internationale Veröffentlichungen, an denen Kaspersky mitgewirkt hat



kaspersky

RISIKOMANAGEMENT ZUR GEWÄHRLEISTUNG AUSREICHENDER SICHERHEIT