kaspersky

Warnung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) aufgrund der aktuellen geopolitischen Situation

Mit diesem speziellen Impulspapier für Deutschland möchten wir eine tiefergehende fachliche Diskussion mit der Community der Fachanwälte:innen für IT-Recht, IT-Sicherheitsrecht, Datenrecht und Datenschutzrecht anstoßen. Hintergrund: Nach den Recherchen von Kaspersky gibt es in Europa in Art und Umfang keine mit der BSI-Warnung vergleichbare Mitteilung einer Cybersicherheitsbehörde. Zudem gibt es auch keine mit der deutschen Neuauslegung des Begriffes der „Sicherheitslücke" vergleichbare Neuinterpretation in Europa. Deswegen sind wir sehr am Fachdialog mit Ihnen interessiert.

Wir freuen uns auf Ihre Gedanken, Argumente, Ideen und Rückmeldungen!

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 gesteuert. Der größte Teil der GReAT Forscher ist in der EU ansässig.

Das Oberverwaltungsgericht NRW *(OVG)* stellt in seinem Beschluss 4 B 473/22 vom 28.4.2022 zur Rechtmäßigkeit der Warnung des BSI gegen AV-Software von Kaspersky vom 15.3.2022 Folgendes fest:

„Das Bundesamt hat die Entscheidung, die Warnung herauszugeben, ermessensfehlerfrei getroffen und dabei insbesondere den Grundsatz der Verhältnismäßigkeit gewahrt. Die Warnung ist nicht aufgrund sachfremder Erwägungen herausgegeben worden, insbesondere war sie weder politisch motiviert noch stellt sie reine Symbolpolitik dar."

In der Fachöffentlichkeit wurde der Beschluss teilweise sehr kritisch aufgenommen. So schreibt Prof. Dr. Dennis-Kenji Kipker von der Universität Bremen in einer ersten Replik:

„Die Begründung für diesen Beschluss ist jedoch – mit Verlaub – eine juristische Katastrophe und eigentlich selbst eine sachfremde Erwägung."
(Quelle: https://community.beck.de/2022/04/28/bei-virenschutzprogrammen-bestehen-schon-aufgrund-ihrer-funktionsweise-sicherheitsluecken-ovg-nrw-zur-warnung; abgerufen am 5.5.2022, 07:30 CET)

Kaspersky bedauert die Entscheidung des OVG für das Land Nordrhein-Westfalen vom 28.4.2022, die Beschwerde der Kaspersky Labs GmbH gegen den Eilbeschluss des Verwaltungsgerichts Köln vom 1.4.2022 abzulehnen und damit die Warnung des Bundesamts für Sicherheit in der Informationstechnik (BSI) vor der Nutzung von Kaspersky-Virenschutzsoftware als rechtmäßig einzustufen. Kaspersky, seine Anwälte und Teile der Fachöffentlichkeit halten den Beschluss für juristisch fragwürdig und mit Blick auf die Zielsetzung, nämlich die Steigerung von Cybersicherheit und Resilienz, fachlich-technisch für ungeeignet.

Kontakt: Jochen Michels | Head of Public Affairs Europe | Kaspersky Labs GmbH | Despag-Straße 3 | 85055 Ingolstadt | Germany | Geschäftsführer: Tanguy Le Bescond de Coatpont | Amtsgericht Ingolstadt: HRB 3527 | www.kaspersky.com | https://www.kaspersky.com/about/policy-blog |

kaspersky

Kann § 7 BSI-Gesetz (BSIG) Grundlage für die Warnung sein?

Kaspersky und seine Rechtsbeistände können die Neuinterpretation des Begriffs der „Sicherheitslücke" durch das Verwaltungsgericht Köln (VG) und das OVG NRW in Münster nicht nachvollziehen. Das Unternehmen ist der Meinung, dass weder die Tatbestandsvoraussetzungen des § 7 Abs. 1 BSIG noch die des § 7 Abs. 2 BSIG erfüllt sind. Eine rechtliche Grundlage für das BSI, diese Warnung auszusprechen, kann Kaspersky vor diesem Hintergrund nicht erkennen. Dass das OVG und das Verwaltungsgericht Köln Antivirensoftware (AV-Software) als solche per Definition aufgrund der weitreichenden Systemberechtigungen als Sicherheitslücke bezeichnen, verstehen Kaspersky, seine Anwälte und Teile der Fachöffentlichkeit nicht. Die seitens der Justiz definierten Anforderungen an Kompetenz, Zuverlässigkeit und Vertrauenswürdigkeit von Antivirenprogrammen lassen sich nach Einschätzung von Kaspersky nicht aus dem Gesetz ableiten. Wenn ausschließlich die Zuverlässigkeit entscheidend wäre, müsste es Zertifizierungen oder Lizensierungen für Anbieter von AV-Software geben. Tatsächlich gibt es diese aber nicht.

Wird wesentlich Gleiches ungleich behandelt?

Das OVG sieht in der Warnung keine Ungleichbehandlung gegenüber anderen Herstellern von Virenschutzprogrammen im Sinne des allgemeinen Gleichheitssatzes (Art. 3 Abs. 1 GG). Die Anwälte von Kaspersky sowie weitere Fachjuristen teilen diese Auffassung nicht. Eine juristisch fundierte Begründung ist in dem Beschluss nicht zu finden. Zudem verwundert es Kaspersky und seine Anwälte, dass das OVG im Beschluss auf viele Argumente von Kaspersky nicht eingeht. So schreibt das OVG unter anderem:

„Gleiches gilt für den pauschalen Einwand der Antragstellerin, eine Warnung müsse auch mit Blick auf die Nutzung von Software aus den USA gelten."

In der sofortigen Beschwerde hatte Kasperskys Folgendes geschrieben:

„Auch der Blick in die USA zeigt, wie willkürlich die Warnung des BSI ist. Obwohl die USA Bundeskanzlerin Merkel ausspioniert haben und hier konkrete Anhaltspunkte vorlagen, wird Software aus den USA offenbar als völlig problemlos eingestuft. (…)."
(Quelle: Sofortige Beschwerde von Kaspersky vom 6.4.2022 gegen den Beschluss des Verwaltungsgerichts Köln vom 1.4.2022)

Zudem hatte Kaspersky in der Sofortigen Beschwerde sowie in weiteren Schriftsätzen auf den Artikel von Sven Herpig und Manuel Atug vom 7.4.2022 im Tagesspiegel Background Cybersecurity verwiesen: *„Wir erinnern uns sowohl an die weitreichende Kompromittierung der SolarWinds-Software aus dem letzten Jahr als auch an die aus den Snowden-Veröffentlichungen bekanntgewordene Operation der US National Security Agency, die Cisco-Produkte vor Auslieferung mit Spionage-Implantaten versehen hat: https://www.spiegel.de/netzwelt/netzpolitik/neue-dokumente-der-geheime-werkzeugkasten-der-nsa-a-941153.html "*

Kaspersky und seine Anwälte können nicht nachvollziehen, warum das OVG diese Informationen offensichtlich nicht berücksichtigt hat und sind der Auffassung, dass die Begründung des OVG mit Fehlern behaftet ist und dass das OVG in mehreren Punkten unlogische Schlüsse gezogen hat.

Auf der einen Seite gab und gibt es Fälle, wo das BSI trotz Beweisen nicht gewarnt hat oder warnt, wie etwa in den dargestellten Fällen mit US-amerikanischer Beteiligung. Auf der anderen Seite billigt das OVG in dem Beschluss, dass das BSI warnt, obwohl

- **keine Beweise, sondern nur Vermutungen und Möglichkeiten vorliegen,**
- **selbst das BSI bestätigt, dass keine technische Schwachstelle in der Kaspersky Software besteht,**
- **Kaspersky weltweit die mit Abstand höchsten und umfangreichsten Sicherheitsmechanismen seiner Branche implementiert hat und kontinuierlich weiterentwickelt.**

Kontakt: Jochen Michels | Head of Public Affairs Europe | Kaspersky Labs GmbH | Despag-Straße 3 | 85055 Ingolstadt | Germany | Geschäftsführer: Tanguy Le Bescond de Coatpont | Amtsgericht Ingolstadt: HRB 3527 | www.kaspersky.com | https://www.kaspersky.com/about/policy-blog |

kaspersky

Wie sorgfältig wurde der Sachverhalt aufbereitet?

Bei Durchsicht des Beschlusses des OVG sind wir auf sachliche Fehler, Ungenauigkeiten, die ungeprüfte Übernahme von im Rahmen der Prozessführung bisher angeführten Quellenangaben sowie Schlussfolgerungen gestoßen, die nicht logisch erscheinen:

- Als Beleg dafür, dass der Kreml Kaspersky unter Druck setzen könne, wird auf die Verhaftung und Verurteilung eines Kaspersky-Mitarbeiters aus dem Jahr 2017 Bezug genommen. Der Sachverhalt, dass der Tatbestand vor der Beschäftigung des ehemaligen Mitarbeiters bei Kaspersky stattfand, findet keine Erwähnung.
- Das OVG bewertet die Unterstützung von Strafverfolgungsbehörden zur Bekämpfung von Cyberkriminalität auch in Russland (konkret mit dem FSB) ausschließlich durch die Bereitstellung technischer Expertise als Zeichen der Unzuverlässigkeit von Kaspersky. Zudem prangert das OVG eine fehlende Distanzierung Kasperskys von dieser Zusammenarbeit zur Bekämpfung von Cybercrime auch mit russischen Strafverfolgungsbehörden an. Dabei führt das OVG allerdings nicht an, dass Kaspersky ausschließlich auf Basis des gültigen nationalen und internationalen Rechts tätig wird, klare Transparenzkriterien definiert hat und hierüber zweimal im Jahr freiwillig einen Transparenzbericht veröffentlicht.
- Dass sich Kaspersky als globales Unternehmen an die jeweilige nationale Rechtsetzung hält und für russische Nutzer in Russland nationales Recht anwendet, sei kein Zeichen rechtmäßigen Handelns, sondern dem OVG zufolge Zeichen für eine unangemessene Kollaboration mit dem russischen Staat.
- Das OVG behauptet im Beschluss an zwei Stellen, der Leiter des Global Research & Analysis Teams (GReAT) von Kaspersky sitze in Moskau. Tatsächlich ist dieser oberste Sicherheitsexperte des Unternehmens Rumäne und von Bukarest aus tätig.

Welche Zusammenhänge bestehen zwischen geopolitischer Lage und Kaspersky?

Das Gericht geht umfangreich auf die geopolitische Lage ein. Es führt das Vorgehen militärischer und nachrichtendienstlicher Kräfte Russlands auf und verweist auf die im Zuge des aktuellen Krieges gegen die Ukraine jüngst von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO sowie die Bundesrepublik Deutschland. Vor diesem Hintergrund stellt das Gericht fest, dass ein erhebliches Risiko eines erfolgreichen IT-Angriffs seitens Russland besteht. Hierfür werden viele Beispiele genannt, die alle nichts mit Kaspersky zu tun haben. Einen konkreten Bezug zu Kaspersky stellt das Gericht nicht her. Das Gericht zieht auch nicht in Betracht, dass die Kaspersky AV-Software einen wirkungsvollen Schutz gegen eben diese Cyberbedrohung bietet. Auch die Tatsache, dass die Beurteilung der dargestellten Cyberlage unter anderem auf Basis hochwertiger Threat Intelligence von Kaspersky beruhen dürfte, finden keine Würdigung. Faktisch schützt die Kaspersky-Antivirensoftware die Infrastruktur und Systeme der Kunden nach wie vor zuverlässig und in bester Qualität – mehr als zwei Monate, nachdem das BSI am 15.3.2022 Gefahr im Verzuge geltend gemacht hat.

Welche Aussagekraft haben Produkt-Zertifizierungen und Prozess-Audits?

Das OVG schreibt in seinem Beschluss zum Nutzen und die Aussagekraft von Zertifizierungen und internationalen Standards Folgendes:

„Eine abweichende Beurteilung musste sich dem Bundesamt auch nicht deshalb aufdrängen, weil die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren sowie Datendienste von Kaspersky in der Vergangenheit von zwei externen, unabhängigen Prüforganisationen bestätigt worden sind. Eine fundamentale Herausforderung der Zertifizierung ist es gerade, dass Software dynamisch ist und kontinuierlich Updates zum Schließen von Schwachstellen oder zur Verbesserung ihrer

Kontakt: Jochen Michels | Head of Public Affairs Europe | Kaspersky Labs GmbH | Despag-Straße 3 | 85055 Ingolstadt | Germany | Geschäftsführer: Tanguy Le Bescond de Coatpont | Amtsgericht Ingolstadt: HRB 3527 | www.kaspersky.com | https://www.kaspersky.com/about/policy-blog |

Funktionalität erfordert. Die Zertifizierung ist im Grundsatz statisch. Sie sagt, wie das Bundesamt zutreffend in seiner Begründung zur Warnung ausführt, nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus, ist aber keine Garantie für den Ist-Zustand."

Das OVG scheint sich allerdings mit dem Zweck und der Aussagekraft von Zertifizierungen nicht detailliert auseinandergesetzt zu haben. So schreibt das BSI schreibt auf seiner Webseite:

„Das BSI ist DIE Zertifizierungsstelle in Deutschland, die in Zusammenarbeit mit nationalen und internationalen Partnern die Cyber-Sicherheit weltweit voranbringt. Das BSI-Angebot zur Zertifizierung und Anerkennung von Produkten, Dienstleistungen und Personen liefert einen wichtigen Beitrag zur Informationssicherheit in Deutschland."

Und:

„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."

Diese Aussage des BSI teilt Kaspersky und lässt auch deswegen seine Produkte und Prozesse wiederholt zertifizieren und auditieren. Zuletzt geschah dies zwischen Januar und Mai 2022 nach Common Criteria in Spanien und Italien und nach ISO 27001. Zudem wurden Sicherheit, Verfügbarkeit, Vertraulichkeit und Datenschutz in der Entwicklung und Verteilung von AV-Basen nach den Richtlinien des vom American Institute of Certified Public Accountants (AICPA) entwickelten Standards (AICPA Professional Standard) auditiert. In allen 72 Prüfszenarien gab es keine Beanstandung. Dieses Audit heißt SOC 2 Typ 1.

Was schafft mehr Vertrauen als die Überprüfung des Quellcodes?

Wer sich noch mehr Sicherheit und Transparenz verschaffen möchte, kann den Quellcode in einem Transparenzzentrum oder über abgesicherte Remote-Umgebungen analysieren und prüfen. Hiervon haben bereits zahlreiche Behörden, wissenschaftliche Einrichtungen sowie Kunden und Partner Gebrauch gemacht. Das BSI nicht. Die Reviews sind anspruchsvoll und erfordern Expertenwissen. Da aber 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.

Warum ist die BSI-Warnung einmalig in Europa?

Von den 27 Cybersicherheitsbehörden der EU-Mitgliedsstaaten haben (Stand 5.5.2022) unseres Wissens nach lediglich neun Staaten Informationen zur Nutzung russischer Software herausgegeben. Eine mit der des BSI vergleichbare geopolitische Warnung gibt es nirgends in Europa (siehe Kasten rechts). Kaspersky und seine Anwälte sind der Auffassung, dass das OVG mehrere „Warnungen" bzw. „Informationen" von Cybersicherheitsbehörden oder Parlamenten innerhalb und außerhalb Europas in dem Beschluss nicht richtig oder einseitig verkürzend dargestellt hat.

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

Kontakt: Jochen Michels | Head of Public Affairs Europe | Kaspersky Labs GmbH | Despag-Straße 3 | 85055 Ingolstadt | Germany | Geschäftsführer: Tanguy Le Bescond de Coatpont | Amtsgericht Ingolstadt: HRB 3527 | www.kaspersky.com | https://www.kaspersky.com/about/policy-blog |

Bestand jemals Gefahr im Verzug?

„Es besteht aufgrund der besonderen Sicherheitssituation Gefahr im Verzug. Das BSI hält daher eine unverzügliche Reaktion für angemessen."

Das schreibt das BSI am 14.3.2022 um 13:52 Uhr deutscher Zeit an Kaspersky - European Headquarters in seinem per E-Mail versandten Schreiben des Abteilungsleiters KM mit dem Betreff *BSI-Warnung nach § 7 BSIG: Gelegenheit zur Stellungnahme* unter dem Geschäftszeichen: *KM14-210 01 03.*

Die Warnung kam unverzüglich. Am 15.3.2022, 10.00 Uhr deutscher Zeit. In diesem Zusammenhang ist es erwähnenswert, dass bis heute alle Kaspersky-Kunden in Deutschland, Europa sowie weltweit bestens geschützt sind. Es gab zahlreiche tatsächliche Cyberattacken, sowohl aus Russland wie auch aus anderen Regionen der Welt, von staatlich finanzierten APT-Gruppen (APT - Advanced Persistance Threats) und anderen Akteuren. Die Kaspersky-Software hingegen wurde auch gut zwei Monate nach der BSI-Warnung nicht kompromittiert oder für offensive Cyberoperationen missbraucht. In dieser Zeit hat Kaspersky AV alle Arten von Malware auf den Geräten und Infrastrukturen seiner Kunden sicher identifiziert, isoliert und entfernt. Und in dieser Zeit haben die Forscher von Kaspersky mit ihrer Threat Intelligence wertvolle Beiträge zur Stärkung der Cybersicherheit geleistet.

Welche Maßnahmen sind in der aktuellen geopolitischen Lage ausreichend?

Auf die Frage, worin der Unterschied einer BSI-Warnung gemäß § 7 BSIG zu dem restlichen Informationsangebot und anderen Warnmeldungen des BSI besteht, antwortet das BSI auf seiner Website Folgendes:

„Im Gegensatz zu den weiteren Informationsprodukten des BSI, die in der Regel Informationen und Maßnahmen des Herstellers referenzieren, hat der Hersteller zum Zeitpunkt der Veröffentlichung einer BSI-Warnung gem. § 7 BSIG keine, keine ausreichende oder keine rechtzeitige eigene Maßnahme ergriffen, um die von dem Produkt ausgehende Gefährdung zu beseitigen oder einzudämmen."

(Quelle für beide Zitate: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/warnungen-nach-par-7_node.html; aufgerufen am 4.5.2022, 13:28 CET)

Kaspersky stand mit dem BSI immer in einem engen fachliche-technischen Austausch und hat seit vielen Jahren kontinuierlich und proaktiv über die ergriffenen technischen, organisatorischen sowie strukturellen Maßnahmen, über Qualifizierungsinitiativen, Zertifizierungen und Audits sowie über die von Kaspersky angewendeten Prinzipien und Grundsätze von Sicherheit, Verfügbarkeit, Vertraulichkeit und Datenschutz in der Software-Entwicklung und Software-Verteilung informiert.

Bis zur Warnung vom 15.3.2022 hat das BSI nie irgendeinen Zweifel an der Angemessenheit und Wirksamkeit dieser Maßnahmen geäußert.

Heute soll das aufgrund der geopolitischen Lage nicht mehr gelten. Das OVG NRW bestätigt, dass das BSI zurecht festgestellt habe, dass all diese Maßnahmen in der aktuellen Lage nicht mehr ausreichen würden.

Allerdings sagen weder das BSI noch das OVG, welche Maßnahmen in der gegenwärtigen Lage tatsächlich ausreichen würden. Kaspersky würde im engen Austausch mit dem BSI alles daransetzen, diesen Maßnahmenkatalog schnellstens zu erfüllen.

Kontakt: Jochen Michels | Head of Public Affairs Europe | Kaspersky Labs GmbH | Despag-Straße 3 | 85055 Ingolstadt | Germany | Geschäftsführer: Tanguy Le Bescond de Coatpont | Amtsgericht Ingolstadt: HRB 3527 | www.kaspersky.com | https://www.kaspersky.com/about/policy-blog |