kaspersky

Stellungnahme von Kaspersky zur Warnung des BSI nach § 7 BSIG

Zur Warnung des BSI haben wir an das BSI folgende Stellungnahme geschickt:

Wir halten die Warnung des BSI für nicht gerechtfertigt. Sie scheint nicht auf der Grundlage einer objektiven technischen Analyse der Risiken beim Einsatz von Kaspersky-Software und -Lösungen erfolgt zu sein. **Die Warnung, die am 15. März 2022 veröffentlicht wurde, ohne dass Kaspersky ausreichend Zeit für eine ausführliche Stellungnahme hatte, scheint mit Blick auf eines der weltweit größten und renommiertesten Cybersicherheitsunternehmen und langjährigen Partner des BSI weder verfahrenstechnisch noch sachlich gerechtfertigt zu sein.**

Im Einzelnen:

- Das BSI stellt in der Warnung fest: „Im Fall der von Kaspersky vertriebenen Anti-Virenschutzsoftware kommt das BSI zum Schluss, dass derzeit ein hohes Risiko durch den weiteren Einsatz dieses Produktes allein schon dadurch entstehen kann, dass die für den Anti-Virenschutz auf den zu schützenden Zielsystemen gewährten Systemrechte eine Manipulation und Missbrauch durch Kaspersky und/oder Dritte ermöglichen."

Diese Aussage gilt nicht nur für Kaspersky-Software, sondern für alle auf dem Markt befindlichen Antivirenprogramme. Kaspersky hat kontinuierlich Maßnahmen ergriffen, um die Transparenz und Integrität seiner Produkte zu gewährleisten. Dazu gehört unter anderem, dass das BSI und andere interessierte Organisationen eingeladen sind, den Quellcode, Updates und die Softwarearchitektur im Transparenzzentrum in Zürich und seit März 2022 auch per Fernzugriff einzusehen.

- Das BSI schreibt des Weiteren: „Da somit hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI in Erfüllung seiner gesetzlichen Aufgaben vor dem Einsatz des Produktes warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG)."

Welche Anhaltspunkte eine Gefährdung der Sicherheit der Informationstechnik darstellen können, teilt das BSI nicht mit. Das Risiko staatlicher Eingriffe durch die russische Regierung ist bei Kaspersky deutlich geringer als bei allen anderen Cybersicherheitsunternehmen der Welt. Kaspersky setzt seit mehr als zehn Jahren technische, infrastrukturelle, organisatorische und unternehmensinterne Maßnahmen zur Verbesserung der Transparenz und Sicherheit um, die kontinuierlich von anerkannten Organisationen geprüft und zertifiziert werden.

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

Wenn Gefahr im Verzug besteht, dann gilt diese Gefahr nicht nur für Kaspersky-Software, sondern für alle sicherheitsrelevante Soft- und Hardware, die in Deutschland eingesetzt wird. Die sofortige Entfernung von Sicherheitssoftware setzt zudem die Kunden der realen und gegenwärtigen Gefahr von Cyberangriffen aus, die ein weitaus größeres Risiko darstellt als theoretische Szenarien einer Manipulation durch Dritte. Wir ergreifen kontinuierlich Maßnahmen, um jegliche Beeinflussung von Kaspersky-Produkten zu verhindern, und diese Bemühungen wurden durch unabhängige Prüfungen und Bewertungen Dritter bestätigt. Wir laden das BSI ein, dies in unseren Transparenzzentren oder in einem Remote-Format selbst zu überprüfen.

- „Das BSI darf nach § 7 Abs. 1 BSIG u. a. vor Sicherheitslücken in informationstechnischen Produkten warnen und Informationen an die Öffentlichkeit über sicherheitsrelevante IT-Eigenschaften in Produkten richten."

Wenn das BSI vor einer möglichen, potenziellen Gefahr durch Kaspersky-Software warnt, gelten genau diese potenziellen Gefahren für alle Cybersicherheitsunternehmen, globale IT-Dienstleister und Softwareprodukte. Wir regen an, mit dem BSI Kriterien und Maßnahmen zu entwickeln, die der politischen Lage und der Bedrohung im Cyberspace gerecht werden. Tatsächlich ist Kaspersky nach wie vor einer der wichtigsten Lieferanten von Informationen über Schwachstellen kritischer Soft- und Hardwaresysteme, auch bei führenden deutschen Unternehmen. Die Warnung, Kaspersky Software nicht mehr einzusetzen, wird die Sicherheit deutscher Unternehmen nicht erhöhen. Das Gegenteil ist der Fall, denn die Schwachstellen in der Software von Drittanbietern werden weiterhin unentdeckt bleiben oder nicht gemeldet werden.

Wir möchten noch einmal deutlich machen, dass wir die politischen Bedenken im Zusammenhang mit dem Krieg in der Ukraine sehr gut nachvollziehen können. Ungeachtet der politischen Risiken liegt jedoch der einzige objektive Weg, diesen Risiken zu begegnen, in der Technologie, ihrer Transparenz und anerkannten Validierungsmaßnahmen. Hierfür setzen wir uns ebenso wie das BSI seit Jahren ein. Wir bitten Sie herzlich und höflich, unsere Argumente zu berücksichtigen, eine umfassende Prüfung durchzuführen und eine faktenbasierte Entscheidung zur Stärkung der Cybersicherheit und -resilienz in Deutschland zu treffen. Weitere Dokumente haben wir für Sie zur Prüfung beigefügt.

kaspersky

Als globales Cybersicherheitsunternehmen leistet Kaspersky seit mehr als 20 Jahren einen vertrauenswürdigen Beitrag zum Cybersicherheitsökosystem in Deutschland und der gesamten Europäischen Union. Kaspersky ist ein privates, international tätiges Unternehmen. Unsere lokalen Geschäfte werden von lokalen Einheiten geführt. Das gibt uns die Möglichkeit, internationale und lokale Aktivitäten effektiv und unabhängig zu koordinieren. Kaspersky ist in mehr als 200 Ländern und Territorien tätig.

Kaspersky unterliegt nicht dem russischen System of Operational Investigative Measures (SORM) oder anderen ähnlichen Gesetzen und ist daher nicht verpflichtet, Informationen zu teilen. Dies wurde durch eine unabhängige rechtliche Bewertung der russischen Datenverarbeitungsgesetze durch Dritte bestätigt. **Die Ergebnisse sind online frei zugänglich und bieten eine unvoreingenommene und faire rechtliche Bewertung. Darüber hinaus haben wir klar zum Ausdruck gebracht, dass unser wichtigstes Transparenzprinzip darin besteht, Dritten niemals den Zugang zu unseren Daten oder unserer Infrastruktur zu gestatten. Anfragen nach nicht deklarierten Funktionen werden stets abgelehnt.**

Es ist unser oberstes Ziel und unser Antrieb, Bürger, Unternehmen und Behörden in Deutschland bestmöglich zu schützen. Wir sind offen für einen Dialog mit dem BSI und anderen Interessierten, und stellen uns einer genaueren Prüfung der Kaspersky-Produkte und -Verfahren.

Wir arbeiten daran, die Cyberwelt sicherer zu machen. Politische und ungerechtfertigte Entscheidungen gegen ein Unternehmen, das seit 25 Jahren an der Spitze des weltweiten Kampfes gegen alle Arten von Cyberbedrohungen steht, schwächen die Cybersicherheit, Und das kann nicht im Interesse des BSI sein.

15. März 2022, Jochen Michels, Head of Public Affairs Europe bei Kaspersky