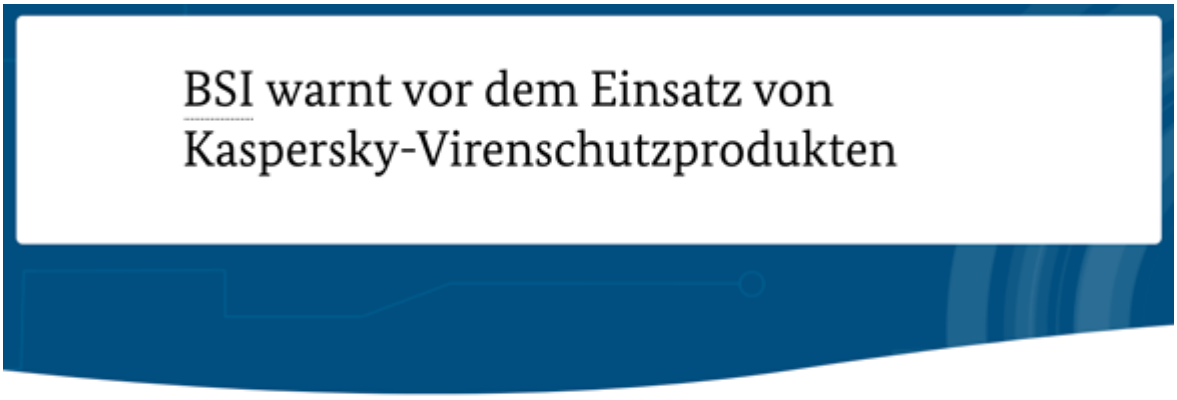
BSI-Warnung vor Kaspersky: Die Chronologie

BSI-Warnung vor Kaspersky: Die Chronologie

Interne Unterlagen beweisen, wie das BSI zusammen mit dem Bundesinnenministerium drei Wochen brauchte, um eine Warnung vor Kaspersky-Produkten auszusprechen.



Ort Bonn
Datum 15.03.2022

Erst am 15. März, rund drei Wochen nach dem Einmarsch Russlands in die Ukraine, veröffentlicht das BSI eine offizielle Empfehlung, keine weiteren Kaspersky-Produkte mehr zu benutzen.
Mitte März sprach das Bundesamt für Sicherheit in der Informationstechnik (BSI) aufgrund des Angriffskrieges auf die Ukraine eine Warnung vor sämtlichen Kaspersky-Produkten aus. Grund: Kaspersky ist ein russischer Antivirenhersteller mit Sitz in Moskau. Daher besteht die realistische Gefahr, dass die russische Regierung die tiefreichenden Rechte ausnutzt, die Antivirenprogramme in Betriebssystemen haben, um beispielsweise an Informationen heranzukommen. 370 Seiten an Dokumenten zeigen nun die Chronologie dieser Entscheidung.

Der Bayerische Rundfunk forderte die Unterlagen durch eine Anfrage nach dem Informationsfreiheitsgesetz an und wertete sie zusammen mit dem Magazin Der Spiegel aus (siehe

ct.de/yu6a). Daraus geht hervor, dass das BSI kurz nach Beginn des Krieges recht schnell die brisante Lage Kaspersky erkannte und nach technischen Gründen suchte, um eine Warnung auszusprechen.

In den internen Mails diskutierten die BSI-Angestellten rege Argumente wie: „Es ist nicht sicher, dass Kaspersky noch die vollständige Kontrolle über seine Software und IT-Systeme hat bzw. diese nicht in Kürze verlieren wird.“ Und man müsse mit „feindlichen Übergriffen auf deutsche Institutionen, Unternehmen und IT-Infrastrukturen“ rechnen. Aber nicht alle waren dieser Meinung, ein Abteilungsleiter schrieb etwa, dass man nicht vorschnell handeln solle oder womöglich sogar rechtswidrig, denn immerhin habe Kaspersky schon vor längerer Zeit angefangen, Server in die Schweiz auszulagern.

Nach einer intensiven Debatte nickte der BSI-Chef Arne Schönbohm am 5. März intern eine mögliche Warnung ab. Es folgten mehrere Absprachen mit dem Bundesinnenministerium (BMI), dem das BSI unterstellt ist. Etwa zeitgleich wendete sich Kaspersky Hilfe suchend an das BSI und erhoffte sich Rückendeckung, was aber innerhalb der Behörde auf taube Ohren stieß.

Erst einen Tag vor dem Aussprechen der Warnung durch das BSI erfuhr Kaspersky per Mail von der Entscheidung, mit der Bitte zu Stellungnahme innerhalb von drei Stunden. Das Unternehmen fühlt sich nach eigener Aussage übergangen und diskreditiert, weswegen es rechtliche Schritte eingeleitet hat. In zwei Instanzen wurde dem BSI recht gegeben, eine abschließende Entscheidung fällt aber erst im langwierigen Hauptverfahren.

Nach dem Okay des BMI sollte die Warnung am 16. März veröffentlicht werden, doch die Presseabteilung grätschte dazwischen und wünschte sich die Erklärung einen Tag früher zu veröffentlichen: „Dann können wir damit in die nächste c’t und in Die Zeit hineinkommen und das BSI als Akteur positionieren.“ So ging die Warnung schließlich am 15. März

raus.

Laut den Dokumenten sollte ursprünglich die Sicherheitsfirma G Data mit in der Erklärung auftauchen, da die ehemalige Frau des Kaspersky-Chefs Natalja Kaspersky 17 Prozent des Unternehmens hält. Diese stehen laut Spiegel aber offenbar zum Verkauf. Deswegen, und vermutlich, weil G Data in Bochum angesiedelt ist und vom BSI als besonders qualifizierter Dienstleister gehandelt wird, hat die Behörde den Namen wohl als „Gefallen“ aus der Warnung herausgehalten, schlussfolgert der Spiegel. (wid@ct.de)

BSI-Warnung und Recherche: ct.de/yu6a