Kollateralschaden – für die Cybersicherheit

In den letzten drei Wochen hat der Krieg in der Ukraine die Welt, wie wir sie kannten, dramatisch verändert. Familien, Beziehungen und Partnerschaften wurden in der Ukraine, in Russland, in Europa und in der ganzen Welt auf dramatische Weise erschüttert. Die Lawine dieser tragischen Ereignisse hat uns alle erfasst.

Auch mein Unternehmen, das weltweit größte private Cybersicherheitsunternehmen, das mit Stolz meinen Namen trägt, ist davon betroffen. In dieser Woche hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Warnung vor Kaspersky-Produkten herausgegeben, in der auf potenzielle Risiken der Nutzung von Kaspersky-Produkten und -Lösungen hingewiesen wird. Ohne auf Details einzugehen kann ich sagen, dass diese Behauptungen reine Spekulationen sind, die durch keine objektiven Beweise oder technischen Details gestützt werden. Der Grund dafür ist einfach. In der fünfundzwanzigjährigen Geschichte Kasperskys gab es nie einen Beweis für einen Missbrauch unserer Software zu schädlichen Zwecken. Und das trotz unzähliger Versuche, einen Beweis dafür zu finden.

Ohne Beweise kann ich nur zu dem Schluss kommen, dass die Entscheidung des BSI allein aus politischen Gründen getroffen wurde. Ich empfinde es als traurig, ja ironisch, dass die Organisation, die sich für Objektivität, Transparenz und technische Kompetenz einsetzt – im übrigen dieselben Werte, die Kaspersky seit Jahren ebenso wie das BSI und andere europäischen Regulierungsbehörden und Branchenverbände unterstützt –, sich buchstäblich über Nacht dazu entschlossen hat oder gezwungen wurde, diese Prinzipien aufzugeben. Kaspersky, langjähriger vertrauensvoller Partner und Unterstützer des BSI und der deutschen Cybersicherheitsindustrie, hatte lediglich wenige Stunden Zeit, um sich zu diesen falschen und unbegründeten Anschuldigungen zu äußern. Dies ist keine Einladung zum Dialog – es ist eine Beleidigung.

Trotz vieler Angebote seitens Kaspersky, unseren Quellcode, unsere Updates, unsere Architektur und unsere Prozesse in den Transparenzzentren Kasperskys in Europa eingehend zu prüfen, hat das BSI dies bisher nie getan. Die Warnung lässt praktischerweise die Tatsache außer Acht, dass Kaspersky seit Jahren Pionierarbeit für mehr Transparenz leistet, indem es im Rahmen seiner Globalen Transparenzinitiative Bedrohungsdaten seiner europäischen Kunden in die Schweiz verlagert hat. Bei allem Respekt, ich betrachte die Entscheidung des BSI als einen ungerechtfertigten Angriff auf mein Unternehmen und insbesondere auf die Kaspersky-Mitarbeiter in Deutschland und Europa. Vor allem aber ist dies auch ein Angriff auf die große Zahl der Verbraucher in Deutschland, die Kaspersky – in den letzten zwei Wochen als bestes Sicherheitsangebot ausgezeichnet (AV-TEST) – ihr Vertrauen schenken. Es ist auch ein Angriff auf die Arbeitsplätze tausender deutscher IT-Sicherheitsexperten, auf Strafverfolgungsbeamte, die wir für die Bekämpfung fortschrittlichster Cyberkriminalität trainiert haben, auf deutsche Informatikstudenten, denen wir bei ihrer Ausbildung geholfen haben, auf unsere Partner in Forschungsprojekten in den kritischsten Bereichen der Cybersicherheit und auf zehntausende deutsche und europäische Unternehmen aller Größenordnungen, die wir vor dem gesamten Spektrum von Cyberangriffen geschützt haben.

Der Schaden für unsere Reputation und unser Geschäft, der durch die Warnung des BSI entstanden ist, ist bereits erheblich. Mich beschäftigt eine Frage: Was ist der Zweck? Kaspersky nicht in Deutschland zu haben, wird Deutschland oder Europa nicht sicherer machen. Ganz im Gegenteil. Die BSI-Entscheidung bedeutet, dass deutschen Nutzern empfohlen wird, das einzige Antivirenprogramm zu deinstallieren, das laut dem unabhängigen deutschen IT-Sicherheitsinstitut AV-Test, den besten Schutz vor Ransomware garantiert. Sie bedeutet, dass die führenden deutschen Industrieunternehmen keine Informationen mehr über kritische Schwachstellen in ihrer Software und Hardware von Kaspersky ICS-CERT erhalten werden – einer Organisation, die von eben diesen Herstellern für ihre verantwortungsvolle Aufklärungsarbeit gelobt wird. Sie bedeutet, dass deutsche Automobilkonzerne nicht über die Fehler informiert werden, die es einem Angreifer ermöglichen könnten, das gesamte

Bordcomputersystem zu übernehmen und dessen Logik zu verändern. Sie bedeutet einen riesigen blinden Fleck auf der Angriffsfläche für europäische Incident Response-Experten und SOC-Betreiber, die nicht mehr in der Lage sein werden, Bedrohungsdaten aus der ganzen Welt – und insbesondere aus Russland – zu empfangen.

Meine Botschaft an das BSI, das leider den Kontakt zu meinem Team in Deutschland seit kurzer Zeit zu meiden scheint, ist einfach: Wir halten diese Entscheidung für ungerecht und grundfalsch. Nichtsdestotrotz sind wir nach wie vor offen dafür, alle Bedenken, die das BSI hat, auf objektive, technische und ehrliche Weise auszuräumen. Wir sind den europäischen Regulierungsbehörden und Branchenexperten dankbar, die einen ausgewogeneren Ansatz gewählt haben, indem sie eine zusätzliche technische Analyse und Prüfung von Sicherheitslösungen und der IT-Lieferkette gefordert haben, und ich verpflichte mich, dass Kaspersky während dieses Prozesses alle erforderlichen Informationen zur Verfügung stellen und gerne kooperieren wird. Unseren deutschen und europäischen Kunden möchte ich sagen: Wir sind sehr dankbar, dass Sie sich für Kaspersky entschieden haben, und dass wir weiterhin das tun werden, was wir am besten können – Sie vor allen Cyberbedrohungen zu schützen, ganz gleich, woher sie kommen, und dabei unsere Technologie und unsere Tätigkeit völlig transparent zu machen.

Der Krieg in der Ukraine kann nur auf diplomatischem Wege beendet werden, und wir alle hoffen auf die Einstellung der Kampfhandlungen und eine Fortsetzung des Dialogs. Dieser Krieg ist eine Tragödie, die bereits Leid über unschuldige Menschen gebracht hat und sich auf unsere hypervernetzte Welt auswirkt. Die globale Cybersicherheitsindustrie, die auf der Grundlage von Vertrauen und Zusammenarbeit zum Schutz der digitalen Verbindungen zwischen uns allen aufgebaut wurde, könnte einen kollateralen Schaden erleiden – und damit alle weniger sicher machen.

Eugene Kaspersky