Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

BSI-Warnung gemäß BSIG § 7

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht die vorliegende Warnung im Rahmen seines gesetzlichen Auftrags [1].

Virenschutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Virenschutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur. Um einen aktuellen und wirksamen Schutz vor Schadsoftware zu gewährleisten, verfügt sie über weitreichende Systemberechtigungen und muss systembedingt (zumindest für Aktualisierungen) eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. Virenschutzsoftware ist ein exponiertes Ziel von offensiven Operationen im Cyberraum, um potentielle Gegner auszuspionieren, die Integrität ihrer Systeme zu beeinträchtigen oder sogar die Verfügbarkeit der darauf gespeicherten Daten vollständig einzuschränken.

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts jüngst von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs mit weitreichenden Konsequenzen verbunden.

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.

2 Auswirkung

Durch Manipulationen an der Software oder den Zugriff auf bei Kaspersky gespeicherte Daten können Aufklärungs- oder Sabotageaktionen gegen Deutschland, einzelne Personen oder bestimmte Unternehmen oder Organisationen durchgeführt oder zumindest unterstützt werden.

Alle Anwender und Nutzerinnen der Virenschutzsoftware können je nach Ihrer strategischen Bedeutung von einer schädigenden Operation betroffen sein. Abgestuft ist damit zu rechnen, dass Einrichtungen des Staates, der Kritischen Infrastrukturen, der Unternehmen im besonderen öffentlichen Interesse, des produzierenden Gewerbes sowie wichtiger gesellschaftlicher Bereiche betroffen sein können. Privatanwender ohne wichtige Funktion in Staat, Wirtschaft und Gesellschaft stehen möglicherweise am Wenigsten im Fokus, können aber in einem erfolgreichen Angriffsfall auch Opfer von Kollateralauswirkungen werden.

3 Betroffene Produkte

Betroffen ist das Portfolio von Virenschutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Virenschutzsoftware des Unternehmens Kaspersky sollte durch alternative Produkte ersetzt werden.

Unternehmen und Behörden mit besonderen Sicherheitsinteressen/Rahmenbedingungen und Einrichtungen Kritischer Infrastrukturen sind in besonderem Maß gefährdet. Sie haben die Möglichkeit, sich von den zuständigen Verfassungsschutzbehörden bzw. vom BSI beraten zu lassen.

Allgemeiner Hinweis: Der Wechsel wesentlicher Bestandteile einer IT-Sicherheits-infrastruktur muss im Enterprise-Bereich immer sorgfältig geplant und durchgeführt werden. Würden IT-Sicherheitsprodukte (also insbesondere Virenschutzsoftware) ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der notfallmäßige Umstieg auf andere Produkte ist auf jeden Fall mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden.
Das BSI empfiehlt daher in jedem Fall eine individuelle Bewertung und Abwägung der aktuellen Situation sowie in einem erforderlichen Migrationsfall, Experten zur Umsetzungsplanung und -durchführung hinzuzuziehen.

5 Referenzen

[1] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)
https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Gesetz/bsi-gesetz_node.html
[2] BSI-Warnungen gemäß §7 und §7a BSIG
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
[3] Darstellung Risikostufen
https://www.cert-bund.de/risk