IFG-Akte zur Kaspersky Warnung

Hinweise

Jeder Vorgang beginnt mit einer Nummer. Die Nummerierung der Vorgänge richtet sich dabei nach der Gerichtsakte. Nach der Nummer wird zur besseren Nachvollziehbarkeit der intern verwendete Dateiname genannt.

Dokumente, die als VS – NUR FÜR DEN DIENSTGEBRAUCH eingestuft waren, wurden der IFG-Akte beigefügt, wenn der Grund der Einstufung entfallen ist oder die Einstufung durch die Schwärzung von Inhalten zurückgenommen werden konnte. Die Rücknahme der Einstufung wurde entsprechend gekennzeichnet.

Technische Anhänge (wie Julia-Parser-Messages) wurden nicht beigefügt, da sie keine relevanten Inhalte enthalten.

Wenn in einem Dokument andere Dokumente zitiert wurden (z. B. bei Antworten auf E-Mails), wurden diese Zitate zur besseren Übersicht nicht erneut aufgenommen, wenn sie an anderer Stelle bereits abgedruckt wurden.

Inhalt

Nr.	Datum	Kurzbezeichnung
037	8.3.2022	Unterrichtung der Amtsleitung 5. Sitzung BT Ausschuss Inneres
041		Mail von Kaspersky an WG und Anweisung Amtsleitung zum Umgang
042	10.3.2022	Erlassbericht an BMI wegen weiterer Unternehmen in Russland
044	11.3.2022	Unterrichtung über Erkenntnisse der Partner von BL25
045	11.3.2022	Bitte des BMI, die Warnung vorzubereiten
046	11.3.2022	Auftrag der Amtsleitung zur Vorbereitung der Warnung für Mittwoch
047		Information des Pressereferats
048	14.3.2022	Auslösung der Abschlussarbeiten, Bitte um Mitzeichnung
050	14.3.2022	Weisung des Präsidenten zur weiteren Vorgehensweise und bedingte Freigabe der Warnmeldung (nach erfolgter Freigabe durch alle mitzeichnenden AL)
051	14.3.2022	Finale Mitzeichnung AL TK
052	14.3.2022	Finale Mitzeichnung AL OC
053	14.3.2022	Nachfrage bei BL23 zur Einhaltung der Formerfordernisse
054	14.3.2022	BL23 Hinweise zur Einhaltung der Formerfordernisse
055	14.3.2022	Mitzeichnung AL BL
056	14.3.2022	Feststellung der Anschrift von Kaspersky und eröffnete Kommunikationswege
057	14.3.2022	Vorlage der PM bei der Amtsleitung zur Freigabe
058	14.3.2022	Formale Prüfung des Anschreibens durch BL23
059	14.3.2022 13:52 Uhr	Anschreiben von Kaspersky mit Gelegenheit zur Stellungnahme bis 17:00 Uhr
060	14.3.2022 13:57 Uhr	Unterrichtung der Amtsleitung und Abteilungen über erfolgtes Anschreiben von Kaspersky
061	14.3.2022 14:30 Uhr	Freigabe der PM durch den Präsidenten
062	14.3.2022 15:29 Uhr	Unterrichtung des BMI CI1 über das erfolgte Anschreiben von Kaspersky
063	14.3.2022 17:50 Uhr	Unterrichtung des BMI AL CI und abschriftlich Staatssekretär Richter über erfolgtes Anschreiben Kasperskys
064	14.3.2022 17:53 Uhr	Unterrichtung aller Abteilungsleitungen und Stab1, Stab2 über die erfolgte Unterrichtung des BMI und die Warnung nebst Begründung
065	14.3.2022 17:54 Uhr	Antwort BMI AL CI zur Unterrichtung und Weisung zum weiteren Vorgehen
066	15.3.2022 7:02 Uhr	Unterrichtung des Präsidenten über die nicht erfolgte Rückmeldung seitens Kasperskys
067	15.3.2022 7:27 Uhr	Weisung des Präsidenten zur weiteren Vorgehensweise
068	15.3.2022 7:52 Uhr	Unterrichtung des BMI AL CI über die nicht erfolgte Rückmeldung seitens Kasperskys und Ankündigung der Veröffentlichung für 9:00 Uhr
069	15.3.2022 7:55 Uhr	Entgegennahme der Information seitens BMI AL CI
070	15.3.2022 9:07 Uhr	Erscheinen der Pressemitteilung zur Warnmeldung

1

001_0_geschwärzt.pdf

Von: GP Poststelle
An: GP Abteilung KM
Cc: GP Geschaeftszimmer KM; GP Stab 3 - Strategie und Leitungsunterstuetzung
Betreff: 0303_22 Erlass CI 3 - Kaspersky & Co. im Lichte der Russland-Ukraine-Krise
Datum: Dienstag, 1. März 2022 08:41:12
Anlagen: Julia Parser Messages.txt

Liebe Kolleginnen und Kollegen,

FF:KM
Btg: -
Aktion: Bitte um Antwort
Frist: 01.03.2022, 14: 00 Uhr

Für Rückfragen stehe ich Ihnen gerne zur Verfügung.

Vielen Dank und freundliche Grüße,

[redacted]

Referat Z 23 - Innerer Dienst
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 -189
53175 Bonn

Telefon:+49 (0) 228 99 9582[redacted]
Mobil:+49[redacted]
E-Mail [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Es folgt 001_Anhang_geschwärzt.pdf als Zitat.

001_Anhang_geschwärzt.pdf

-----Ursprüngliche Nachricht-----
Von: Andreas.Reisen@bmi.bund.de <Andreas.Reisen@bmi.bund.de>
Gesendet: Dienstag, 1. März 2022 08:12
An: GP Poststelle <poststelle@bsi.bund.de>
Cc: [redacted]@bsi.bund.de>; Welsch, Günther <guenther.welsch@bsi.bund.de>; [redacted]@bmi.bund.de; CI3@bmi.bund.de
Betreff: WG: Kaspersky & Co. im Lichte der Russland-Ukraine-Krise

Liebe Kolleginnen und Kollegen,

ich nehme Bezug auf den bisherigen Austausch mit[redacted] und bitte zu der beiliegenden Presseanfrage um einen weiterverwendbaren Antwortbeitrag (je Frage) bis heute 14 Uhr.

Mit freundlichen Grüßen, Andreas Reisen

-----Ursprüngliche Nachricht-----
Von: Könen, Andreas <Andreas.Koenen@bmi.bund.de>
Gesendet: Montag, 28. Februar 2022 19:32
An: CI3_ <CI3@bmi.bund.de>; Reisen, Andreas <Andreas.Reisen@bmi.bund.de>
Cc: ALCI_ <CI@bmi.bund.de>; SVALCI_ <SVCI@bmi.bund.de>; CI1_ <CI1@bmi.bund.de>; Presse <Presse@bmi.bund.de>; [redacted]@bmi.bund.de>
Betreff: WG: Kaspersky & Co. im Lichte der Russland-Ukraine-Krise

@CI3: Mit der Bitte um Übernahme. Termin 01.03.22 DS
@ALCI: Bitte TÜL.
-----Ursprüngliche Nachricht-----
Von [redacted]@bmi.bund.de>
Gesendet: Montag, 28. Februar 2022 18:55
An: CI1_ <CI1@bmi.bund.de>
Cc: ALCI_ <CI@bmi.bund.de>; SVALCI_ <SVCI@bmi.bund.de>; PKII1_ <PKII1@bmi.bund.de>
Betreff: WG: Kaspersky & Co. im Lichte der Russland-Ukraine-Krise

Liebe Kolleginnen und Kollegen,

für diese Presseanfrage, die bei uns offenbar liegen geblieben ist, bitte ich um einen kurzen Antwortvorschlag, möglichst bis morgen, DS.
Die Verzögerung bitte ich zu entschuldigen.

Mit freundlichen Grüßen
Im Auftrag
[redacted]

_____
Pressestelle | Pressesprecher
Bundesministerium des Innern und für Heimat

Alt Moabit 140, D-10557 Berlin
Telefon: +49 30 18 681[redacted]
Mobil: +49[redacted]
E-Mail [redacted]@bmi.bund.de
E-Mail: Presse@bmi.bund.de
Internet: www.bmi.bund.de

-----Ursprüngliche Nachricht-----
Von: [redacted]
Gesendet: Montag, 28. Februar 2022 11:51
An: Presse <Presse@bmi.bund.de>
Cc: BSI grp: Presse <presse@bsi.bund.de>
Betreff: FW: Kaspersky & Co. im Lichte der Russland-Ukraine-Krise

Hallo,

ich wollte nach dem telefonischen Nachhaken auch noch mal per Mail daran erinnern, dass die Anfrage auch nach knapp einer Woche noch offen ist. Ich bitte nun um Antwort zum morgigen Dienstag, [redacted]

Am 22.02.22, 14:10 schrieb [redacted]:

Hallo an die Presseteams von BMI & BSI,

ich würde gern für [redacted] etwas schreiben über Kaspersky & Co. -- angesichts der Russland-Ukraine-Krise fragen sich Leser nämlich verstärkt, ob man überhaupt noch etwa Antiviren-Software von Kaspersky bzw. andere Programme russischer Hersteller einsetzen kann bzw. sollte.

Dazu gab es 2018 mal eine Antwort der Bundesregierung zu Fragen der FDP-Fraktion: Das BSI wurde demnach bis dahin nur in einem Fall damit beauftragt, die Sicherheit von Software ausländischer Hersteller zu überprüfen (Windows 10). Auch andere Stellen sind nicht tätig geworden. Eine Einsicht in den Quellcode von Software ausländischer Hersteller wurde in Fällen von beauftragten Überprüfungen bislang gar nicht genommen.. Welche konkrete ausländische Software hiesige Sicherheitsbehörden einsetzen: streng geheim. Für Kaspersky wollte die Bundesregierung -- anders als UK oder USA -- keine prinzipielle öffentliche Warnung aussprechen. Bei Behördeneinsatz gelte prinzipiell die "No-Spy-Klausel". Dem BSI lagen damals auch keine Erkenntnisse vor, die eine Manipulation von Kaspersky-Software belegen (s.u.a. https://www.golem.de/news/kaspersky-palantir-co-bsi-macht-keine-sicherheitschecks-bei-behoerdensoftware-1811-137956.html).

Dazu würde ich gern wissen, ob sich seit 2018 an den Einschätzungen etwas geändert hat oder ob diese aktuell anders gesehen werden?

Hat es in diesem Bereich Entwicklungen/neue Analysen/Untersuchungen gegeben?

Ist der Einsatz von Kaspersky-Produkten hierzulande aus Behördensicht legitim bzw. werden solche in Behörden verwendet?

Gibt es andere russische Software oder Dienstleister, die beim BMI bzw. BSI als problematisch gelten bzw. zu denen Untersuchungen durchgeführt wurden/werden?

Reicht die No-Spy-Klausel aus oder gibt es da Bedarf an Nachschärfungen?

Sind aktuell im Bereich IT Sanktionen gegen russische Firmen geplant?

Über eine zeitnahe Antwort würde ich mich freuen [redacted]

--

[redacted]

2

002_geschwärzt.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

Ergebnis-Protokoll

Stab 3	Datum: 09.03.2022
Az.:	

Anlass: Leitungsrunde			
Datum: 02.03.2022	Ort: virtuell (Zoom)	Uhrzeit: von 10:00 Uhr bis 13:05 Uhr	
Besprechungsleiter: P	Teilnehmende: - siehe Liste -	Verfasser: [redacted]	Seite: 1-5
Weitere Verteiler (über Teilnehmende hinaus):			

Besprechungsergebnisse:

Nr.	Art[1]	Darstellung/Beschreibung[2]	Verantwortlich	Termin
1	I	[redacted]		
2	I			
3				

[1] **A = Auftrag** (Aufgabe, die bis zu einem vereinbarten Zeitpunkt vom Verantwortlichen zu erledigen ist),
B = Beschluss (verbindliche Einigung z.B. über künftiges Verfahren/Verhalten, Ziel),
E = Empfehlung (unverbindlicher Vorschlag, Auftrag, Hinweis),
F = Feststellung (Information),
D = Darstellung (von Alternativen zur Entscheidungsfindung (inkl. Konsequenzen)).

[2] **Die Beschreibung, die Darstellung sollte so ausführlich sein, dass hinsichtlich des Inhaltes kein Spielraum zur Interpretation besteht. Herkunft, Zusammenhang und Bedeutung müssen sofort erschlossen werden können!**

Bundesamt
für Sicherheit in der
Informationstechnik

4		[redacted]		
5		[redacted]		
6	A	[redacted]	[redacted]	[redacted]

Bundesamt
für Sicherheit in der
Informationstechnik

7		[redacted]		
8	B	[redacted]		
9	A	[redacted]	[redacted]	
10		**TOP 4 Aktuelle Lage** (*wurde nach Top 1 vorgezogen*) <u>Umgang mit Kaspersky und Co.</u> Notwendigkeit zu grundlegender Positionierung/dringende Notwendigkeit zur Überarbeitung der Sprachregelung zu Kaspersky im Hinblick auf Aussagen zum Einsatz in der Bundesverwaltung sowie auf die Empfehlung zur generellen Verwendung durch Staat, Wirtschaft und Gesellschaft in der Bundesrepublik Deutschland.		

Bundesamt
für Sicherheit in der
Informationstechnik

		Hierbei muss zwischen aktueller geopolitischer Lage/strategischer Positionierung und fachlichen Argumenten unterschieden werden. Bei strategischer Positionierung ist grundsätzlich das BM miteinzubeziehen.		
11	A	Beteiligte Abteilungen stellen etwaige Erkenntnisse/technische Gründe im Nfd-fähigen Aufschlag zusammen, die eine Warnung vor Kaspersky-Produkten nach § 7 BSIG nachvollziehbar und begründbar rechtfertigen. Hierbei sollen verschiedene Einsatzbereiche (Kommunen, Bundesbehörden, privater Verbraucher) separat betrachtet bzw. bewertet werden. Anstelle der vorgelegten Sprachregelung wird eine Warnung nach § 7 BSIG erstellt und gemäß den gesetzlichen Vorgaben veröffentlicht. Die zugrundeliegende Strategie wird mit BMI abgestimmt. Kommunikation über Kaspersky wird bis dahin zurückgehalten.	FF: KM (KM14) Btg.: TK, OC, BL	04.02.2022, 16 Uhr
12	A	Auch Umgang mit weiteren Anbietern [redacted] muss in den Blick genommen werden. Ein genereller Abgleich mit bestehenden Sanktionen ist hierbei erforderlich. SZ 11 erstellt Übersicht über russische Unternehmen im IT-Umfeld; in einem weiteren Schritt sollte eine Übersicht über chinesischen Unternehmen erstellt werden.	SZ (SZ11)	Asap
13		[redacted]	[redacted]	

Bundesamt
für Sicherheit in der
Informationstechnik

		[redacted]		
14		[redacted]		
15	B	[redacted]	[redacted]	
16	A	[redacted]	[redacted]	
17		[redacted]		
18		[redacted]		
19		[redacted]		
20		[redacted]		

Nächster (Besprechungs-)Termin: 30.03.2022	Anlagen:
Zur Kenntnisnahme der Ergebnisse an andere Abteilungen durch Übersendung einer Kopie ☐ nein ☑ ja	

Im Auftrag

gez.

[redacted]

Teilnehmendenliste			
Nr.	Vertretende Stelle (Behörde/Firma, Referat/Abteilung) ggf. Anschrift/Ort	Name (ggf. Bezeichnung, Stellung)	Telefon/Fax/E-Mail
1.	P	Schönbohm	
2.	VP	Schabhüser	
3.	LLS	[redacted]	
4.	AL BL	Samsel	
5.	ALn DI	Bargstädt-Franke	
6.	AL KM	Welsch	
7.	AL OC	Häger	
8.	AL SZ	Amendola	
9.	AL TK	Caspers	
10.	ALn WG	Nagel	
11.	AL Z	Pieper	
12.	Stab 1	[redacted]	
13.	Stab 3	[redacted]	
14.	[redacted] (zu TOP 3)	[redacted]	
15.	[redacted] (zu TOP 3)	[redacted]	
16.	[redacted] (zu TOP 3)	[redacted]	

3

003_0_geschwärzt.pdf

Von: Andreas.Reisen@bmi.bund.de
An: Welsch, Günther
Betreff: AW: Kaspersky & Co. im Lichte der Russland-Ukraine-Krise
Datum: Mittwoch, 2. März 2022 14:57:05
Anlagen: Julia Parser Messages.txt

Ok, danke, lieber Herr Welsch.

Mit freundlichen Grüßen, Andreas Reisen

-----Ursprüngliche Nachricht-----
Von: Welsch, Günther <guenther.welsch@bsi.bund.de>
Gesendet: Mittwoch, 2. März 2022 14:54
An: Reisen, Andreas <Andreas.Reisen@bmi.bund.de>
Cc [redacted]@bsi.bund.de>; [redacted]@bmi.bund.de>; CI3_ <CI3@bmi.bund.de>; BSI Poststelle <poststelle@bsi.bund.de>; CI4_ <CI4@bmi.bund.de>; BSI grp: Leitungsstab <leitungsstab@bsi.bund.de>; BSI grp: GPLeitungsstab 3 <stab3@bsi.bund.de>; BSI grp: GPAbteilung KM <abteilung-km@bsi.bund.de>
Betreff: AW: Kaspersky & Co. im Lichte der Russland-Ukraine-Krise
Priorität: Hoch

Einstufung aufgehoben

Lieber Herr Reisen,

in Abstimmung mit der Amtsleitung des BSI und allen Abteilungsleitern erarbeiten wir gerade eine Warnmeldung nach §7 BSIG zur Nutzung von Kasperky. Aus diesem Grund müssen wir die Erlassbeantwortung zurückstellen, damit wir die Stringenz unserer Aussagen erhalten können [redacted] ist gerade aktiv im BSI beauftragt, diese Warnmeldung mit den Kollegen im BSI abzustimmen. Wir werden Sie umgehend mit aktuellen und weitergehenden Informationen versorgen.

Beste Grüße,
Günther Welsch

Es folgt 001_Anhang_geschwärzt.pdf als Zitat.

4

004_0.pdf

Von:	Welsch, Günther
An:	GP Abteilung OC; GP Abteilung BL; GP Abteilung TK
Cc:	GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Stab 3 - Strategie und Leitungsunterstuetzung; Schönbohm, Arne; Schabhüser, Gerhard; GP Referat BL 23; GP Abteilung Z; GP Abteilung WG; GP Abteilung SZ; GP Abteilung DI; GP Abteilung KM
Betreff:	EILT!: BSIG § 7 Warnung Kaspersky
Datum:	Donnerstag, 3. März 2022 17:57:21
Anlagen:	Kaspersky_Warnung_final.odt VS-NfD_Kaspersky_Begründung_final.odt
Dringlichkeit:	Hoch

EILT!: Warnung gem. BSIG § 7 vor Kaspersky

P/VP zur Billigung

über

parallele MZ: Abteilungen OC, BL, TK

zK: BL 23

Nachrichtlich: Abteilungen Z, WG, SZ, DI, Leitungsstab, Stab 1, Stab 3

1) Anbei lege ich die seitens Referat KM14 unter Mitwirkung von BL23 und weiterer Referate erarbeitete Warnung vor Kaspersky Anti-Virenschutz zur Billigung vor. Es handelt sich um zwei Dokumente: 1. Die Warnung an sich. 2. Die Begründung der Rechtmäßigkeit der Warnung. Die Kommentare seitens BL23 wurden bei der Finalisierung berücksichtigt.
2) Nach Billigung durch die Amtsleitung ist beabsichtigt, dem BMI die Warnung mit einem Tag Vorlagefrist zur Kenntnis vorzulegen. Einer Billigung seitens der Fachaufsicht bedarf es aufgrund der gesetzlichen Regelung nicht, jedoch sollte das BMI Gelegenheit haben, ggf. in den Dialog mit dem BSI vor Veröffentlichung einzutreten.

Dr. Welsch

004_1_Kaspersky_Warnung_final..pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

IT-Sicherheitsprodukte des Herstellers Kaspersky und weitere IT-Produkte aus Russland

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware einschließlich der damit verbundenen echtzeitfähigen Clouddienste bergen ein besonderes Risiko für eine zu schützende IT-Infrastruktur, da diese über weitreichende Systemberechtigungen verfügen, um einen aktuellen und wirksamen Schutz vor Schadsoftware zu gewährleisten. Zudem müssen sie systembedingt eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten, über die sie jederzeit dynamisch aktualisiert werden können. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. Viren-Schutzsoftware 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 Angriffs mit weitreichenden Konsequenzen verbunden.

Die Bedrohungssituation durch offensive Cyber-Operationen von russischer Seite führen in der aktuellen Lage zu einer neuen Risikobewertung. Ein russischer IT-Hersteller kann selbst entsprechende 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/Nutzer der Viren-Schutzsoftware 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 Interesse des Staates, 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 aber auch Opfer von Kollateralauswirkungen werden.

3 Betroffene Produkte

Betroffen sind alle russischen IT-Hersteller, insbesondere das komplette Portfolio von Kaspersky (Hardware, Software und Clouddienste).

4 Handlungsempfehlung

Produkte von Kaspersky sollten 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 vom zuständigen Landesamt für Verfassungsschutz bzw. vom Bundesamt für Verfassungsschutz individuell beraten zu lassen.

Der Wechsel wesentlicher Bestandteile einer IT-Sicherheitsinfrastruktur muss im Enterprise-Bereich sorgfältig geplant und durchgeführt werden. Würden IT-Sicherheitsprodukte ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der notfallmäßige Umstieg auf einen anderen Hersteller ist auf jeden Fall mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden. Das BSI empfiehlt daher in jedem Fall eine individuelle Bewertung 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/DasBSI/Gesetz/gesetz_node.html
[2] Darstellung Risikostufen
https://www.cert-bund.de/risk

004_1_VS-NfD_Kaspersky_Begründung_final_geschwärzt.pdf

Referat KM 14 02. 03. 2021

Az. KM14-210 01 03 / VS-NfD

[redacted]

Betr. Bewertung von IT-Sicherheitsprodukten
hier: Warnung vor Kaspersky-Produkten nach § 7 BSIG

Bezug

Anlagen Entwurf Warntext

1) Vermerk zur Begründung der Warnung

A Begründung der Warnung nach § 7 Abs. 1 BSIG

Die Ereignisse rund um Kaspersky werden vom BSI seit Jahren aufmerksam verfolgt. Mehrere westliche Staaten wie USA und Niederlande warnen seit Jahren öffentlich vor Kaspersky und haben die Software für den Einsatz im Behördenumfeld gesperrt. Auch deutsche Nachrichtendienste haben immer abgeraten, Kaspersky in kritischen Bereichen einzusetzen. Das BSI hat sich aber bislang mit öffentlichen Warnungen zu Kaspersky zurückgehalten.

Der russische Angriff auf die Ukraine, der mit hybriden Mitteln - also auch im Cyberraum - geführt wird und von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt wurde, verändert die Lagebeurteilung. Russland ist kein demokratischer Rechtsstaat und sieht Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als Feind an. Mit feindlichen Übergriffen auf deutsche Institutionen, Unternehmen und IT-Infrastrukturen ist daher zu rechnen. Russische Unternehmen könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden, zum anderen selbst Ziel massiver Cyberangriffe werden. Die Gefahr, dass Kaspersky in die kriegerischen Auseinandersetzungen hineingezogen wird, ist daher so groß, dass eine Warnung angemessen ist. Es ist nicht sicher, dass Kaspersky noch die vollständige Kontrolle über seine Software und IT-Systeme hat bzw. diese nicht in Kürze verlieren wird.

[redacted]

Neben dem BSI haben auch andere Organisationen ihre Risikobewertung angepasst. Frankreich hat beispielsweise eine vergleichbare Warnung veröffentlicht[1]. [redacted]

1 https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

[redacted] Die Teilnehmer waren sich einig, dass der Einsatz von Kaspersky-Produkten hoch problematisch ist. Zum Schutz ihrer IT-Systeme wurden daher automatische Updates abgestellt und Schritte eingeleitet, um die Software schnellstmöglich durch eine sicherere Alternative abzulösen.

Die beschriebenen Angriffsvektoren sind nicht neu. Am 10.06.2015 hat beispielsweise Kaspersky selbst in einer Pressemitteilung[2] mitgeteilt, dass das Unternehmensnetzwerk gehackt wurde und Angreifer mit teils neuen Methoden versucht haben, vertrauliche Daten zu stehlen, die dann für Angriffe auf die Kunden missbraucht werden könnten.

B Prüfung der Verhältnismäßigkeit

Durch manipulierte IT-Sicherheitsprodukte wie Virenschutz hat ein Angreifer nahezu unbegrenzte Möglichkeiten IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste große Vorfall öffentlich bekannt wird.

C Ausnahme von der vorherigen Informationspflicht nach § 7 Abs. 1 a Nr. 1 BSIG

Kaspersky sollte 1 Stunde vor der Veröffentlichung informiert werden. Es ist Gefahr im Verzug. Hacker könnten ihre Vorbereitungen bereits abgeschlossen haben und nur noch auf einen Einsatzbefehl warten. Kaspersky selbst hat zudem keine Möglichkeit, durch technische oder sonstige Maßnahmen die Risikoeinschätzung positiv zu beeinflussen. Eine Beteiligung des Herstellers kann daher an dem zugrunde liegenden Sicherheitsproblem nichts ändern, da der Hersteller keinen Einfluss auf die Gefährdung hat.

D Verfügung

2) BL 23 zur Kenntnis

3) KM zur Mitzeichnung [MZ. AL KM vom 3.3.2002]

4) TK zur Mitzeichnung

5) OC zur Mitzeichnung

6) BL zur Mitzeichnung

7) P/VP z. Billigung

Im Auftrag

[redacted]

2 https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

5

005_0_geschwärzt.pdf

Von:	GP Abteilung TK
An:	Welsch, Günther
Cc:	GP Abteilung OC; GP Abteilung BL; GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Stab 3 - Strategie und Leitungsunterstuetzung; Schönbohm, Arne; Schabhüser, Gerhard; GP Referat BL 23; GP Abteilung Z; GP Abteilung WG; GP Abteilung SZ; GP Abteilung DI; GP Abteilung KM; GP Geschaeftszimmer TK
Betreff:	AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum:	Donnerstag, 3. März 2022 18:09:28

Lieber Günther,

vielen Dank! Abteilung TK zeichnet beide Dokumente sowie das von Dir beschriebene weitere Vorgehen mit.

Viele Grüße

Thomas

--
Thomas Caspers
Abteilungsleiter
Technik-Kompetenzzentren

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Telefon: +49 (0)228 99 9582-[redacted]
E-Mail: thomas.caspers@bsi.bund.de
Internet: www.bsi.bund.de

Von: Welsch, Günther <guenther.welsch@bsi.bund.de>
Gesendet: Donnerstag, 3. März 2022 17:57
An: GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>
Cc: GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung Z <abteilung-z@bsi.bund.de>; GP Abteilung WG <abteilung-wg@bsi.bund.de>; GP Abteilung SZ <abteilung-sz@bsi.bund.de>; GP Abteilung DI <abteilung-di@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>
Betreff: EILT!: BSIG § 7 Warnung Kaspersky
Priorität: Hoch

EILT!: Warnung gem. BSIG § 7 vor Kaspersky

P/VP zur Billigung

über

parallele MZ: Abteilungen OC, BL, TK

zK: BL 23

Nachrichtlich: Abteilungen Z, WG, SZ, DI, Leitungsstab, Stab 1, Stab 3

1) Anbei lege ich die seitens Referat KM14 unter Mitwirkung von BL23 und weiterer Referate erarbeitete Warnung vor Kaspersky Anti-Virenschutz zur Billigung vor. Es handelt sich um zwei Dokumente: 1. Die Warnung an sich. 2. Die Begründung der Rechtmäßigkeit der Warnung. Die Kommentare seitens BL23 wurden bei der Finalisierung berücksichtigt.
2) Nach Billigung durch die Amtsleitung ist beabsichtigt, dem BMI die Warnung mit einem Tag Vorlagefrist zur Kenntnis vorzulegen. Einer Billigung seitens der Fachaufsicht bedarf es aufgrund der gesetzlichen Regelung nicht, jedoch sollte das BMI Gelegenheit haben, ggf. in den Dialog mit dem BSI vor Veröffentlichung einzutreten.

Dr. Welsch

6

006_0_geschwärzt.pdf

Von:	GP Leitungsstab
An:	Welsch, Günther; GP Abteilung OC; GP Abteilung BL; GP Abteilung TK
Cc:	GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Stab 3 - Strategie und Leitungsunterstuetzung; Schönbohm, Arne; Schabhüser, Gerhard; GP Referat BL 23; GP Abteilung KM
Betreff:	AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum:	Donnerstag, 3. März 2022 20:03:28
Anlagen:	Kaspersky_Warnung_final-sfd.pdf VS-NfD_Kaspersky_Begründung_final.pdf Kaspersky_Warnung_final-sfd.odt

Liebe Kolleginnen und Kollegen,

obwohl nur im cc habe ich mir erlaubt zu kommentieren und im Änderungsmodus Änderungsvorschläge zu machen – siehe anbei.

Zum Hintergrund: die verwendeten Begrifflichkeiten sind mE nicht ganz stringent. Ich habe versucht, dies, auch unter Hinzuziehung der rechtlichen Begründung, anzupassen. „Gestoßen“ habe ich mich letztlich am Begriff „Hardware“, der im Übrigen nicht verwendet wird. Sofern ich falsch liege, gerne meine Änderungen ablehnen und vielleicht ein weiterer klarstellender Satz, was mit Hardware gemeint ist.

@P/VP: Ihnen auch als .pdf.

Gruß
[redacted]

im Auftrag
[redacted]
Leiterin Leitungsstab

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Telefonische Erreichbarkeit:
[redacted]

#DeutschlandDigitalSicherBSI

Von: Welsch, Günther <guenther.welsch@bsi.bund.de>
Gesendet: Donnerstag, 3. März 2022 17:57
An: GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>
Cc: GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung Z <abteilung-z@bsi.bund.de>; GP Abteilung WG <abteilung-wg@bsi.bund.de>; GP Abteilung SZ <abteilung-sz@bsi.bund.de>; GP Abteilung DI <abteilung-di@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>
Betreff: EILT!: BSIG § 7 Warnung Kaspersky

Priorität: Hoch

EILT!: Warnung gem. BSIG § 7 vor Kaspersky

P/VP zur Billigung

über

parallele MZ: Abteilungen OC, BL, TK

zK: BL 23

Nachrichtlich: Abteilungen Z, WG, SZ, DI, Leitungsstab, Stab 1, Stab 3

1) Anbei lege ich die seitens Referat KM14 unter Mitwirkung von BL23 und weiterer Referate erarbeitete Warnung vor Kaspersky Anti-Virenschutz zur Billigung vor. Es handelt sich um zwei Dokumente: 1. Die Warnung an sich. 2. Die Begründung der Rechtmäßigkeit der Warnung. Die Kommentare seitens BL23 wurden bei der Finalisierung berücksichtigt.
2) Nach Billigung durch die Amtsleitung ist beabsichtigt, dem BMI die Warnung mit einem Tag Vorlagefrist zur Kenntnis vorzulegen. Einer Billigung seitens der Fachaufsicht bedarf es aufgrund der gesetzlichen Regelung nicht, jedoch sollte das BMI Gelegenheit haben, ggf. in den Dialog mit dem BSI vor Veröffentlichung einzutreten.

Dr. Welsch

Weiterer Anhang: 004_1_VS-NfD_Kaspersky_Begründung_final_geschwärzt.pdf

006_1_geschwärzt.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

IT-Sicherheitsprodukte des Herstellers Kaspersky und weitere IT-Produkte aus Russland

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware einschließlich der damit verbundenen echtzeitfähigen Clouddienste bergen ein besonderes Risiko für eine zu schützende IT-Infrastruktur, da diese über weitreichende Systemberechtigungen verfügen, um einen aktuellen und wirksamen Schutz vor Schadsoftware zu gewährleisten. Zudem müssen sie systembedingt eine dauerhafte, verschlüsselte und nicht prüfbare Verbindung zu Servern des Herstellers unterhalten, über die sie jederzeit dynamisch aktualisiert werden können. Daher ist Vertrauen in die Zuverlässigkeit und den Eigenschutz eines Herstellers sowie seiner authentischen Handlungsfähigkeit entscheidend für den sicheren Einsatz solcher Systeme. Viren-Schutzsoftware 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 Angriffs mit weitreichenden Konsequenzen verbunden.

Die Bedrohungssituation durch offensive Cyber-Operationen von russischer Seite führen in der aktuellen Lage zu einer neuen Risikobewertung. Ein russischer IT-Hersteller kann selbst entsprechende 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/Nutzer der Viren-Schutzsoftware können je nach ~~I~~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 Interesse des Staates, 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 ~~aber~~ auch Opfer von Kollateralauswirkungen werden.

3 Betroffene Produkte

Betroffen sind alle entsprechenden IT-Sicherheitsprodukte rus[1]schen~~nr~~ IT-Hersteller, insbesondere das komplette IT-Sicherheits~~P~~portfolio von Kaspersky (Hardware, So[2]ware und Clouddienste).

4 Handlungsempfehlung

IT-Sicherheits~~P~~produkte von Kaspersky sollten 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 vom zuständigen Landesamt für Verfassungsschutz bzw. vom Bundesamt für Verfassungsschutz individuell beraten zu lassen.

Der Wechsel wesentlicher Bestandteile einer IT-Sicherheitsinfrastruktur muss im Enterprise-Bereich sorgfältig geplant und durchgeführt werden. Würden IT-Sicherheitsprodukte ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der notfallmäßige Umstieg auf einen anderen Hersteller ist auf jeden Fall mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden. Das BSI empfiehlt daher in jedem Fall eine individuelle Bewertung 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/DasBSI/Gesetz/gesetz_node.html
[2] Darstellung Risikostufen
https://www.cert-bund.de/risk

Kommentarzusammenfassung für BSI-E-CS Vorlage

Seite: 2

Nummer: 1 Verfasser: Unbekannter Autor, 03.03.22 Datum: Unbestimmt

Ergänzungsvorschlag aufgrund des nachfolgenden Kommentars.

Nummer: 2 Verfasser: Unbekannter Autor, 03.03.22 Datum: 20.04.2022 10:40:49

Der Sachverhalt und die Auswirkung unter 1 und 2 lassen mE diese Schlussfolgerung nicht zu. Dort wird nur von Clouddiensten und SW gesprochen – und auch dies eingeschränkt auf Virenschutzprogramme. Auf HW wird gar nicht eingegangen.

Nummer: 3 Verfasser: XXXXXXXXX, 03.03.22 Datum: Unbestimmt

Zum schluss anpassen.
Nach meinem Kenntnisstand wäre das die 4. formale Warnung ge. §7 (Also BSI-W 004)
Im Webbereich BSI:
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Technische-Sicherheitshinweise-und-Warnungen/Warnungen-nach-Par-7/Archiv/archiv_node.html

7

007_geschwärzt.pdf

Von: GP Abteilung BL
An: Welsch, Günther; GP Abteilung KM
Cc: GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Stab 3 - Strategie und Leitungsunterstuetzung; Schönbohm, Arne; Schabhüser, Gerhard; GP Referat BL 23; GP Abteilung Z; GP Abteilung WG; GP Abteilung SZ; GP Abteilung DI; GP Abteilung KM; GP Abteilung OC; GP Abteilung BL; GP Abteilung TK; GP Referat BL 23; [redacted] GP Fachbereich BL 2
Betreff: AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum: Freitag, 4. März 2022 09:53:32

Liebe Kolleginnen und Kollegen,

aus Sicht von BL ist die Begründung noch nicht hinreichend substantiiert, um die Warnung mitzeichnen zu können und sollte deshalb noch nachgeschärft werden.

Die Hauptprobleme sehen wir vor allem hierin:

- Die Voraussetzungen des § 7 – insbesondere das Vorliegen einer Sicherheitslücke - werden nicht sauber dargelegt. Das scheint mir hier jedoch besonders wichtig, da wir eine technische Sicherheitslücke derzeit nicht nachweisen können.
- Es wird nirgendwo darauf eingegangen, dass Kaspersky nach der Krim-Krise bereits organisatorische Maßnahmen ergriffen hat, die eine russische Einflussnahme ausschließen sollen (Serververlegung in die CH usw.). Ein Gutachten einer schwedischen Uni bescheinigt Kaspersky, nicht bestimmten russischen Gesetzen zu unterliegen, die eine Kooperation mit der russ. Regierung erzwingen könnten. Damit setzen sich die Dokumente nicht auseinander. Meines Erachtens laufen wir damit schon formal in einen Ermessensnichtgebrauch und damit die Rechtswidrigkeit. (Das Gutachten findet sich unter https://media.kasperskydaily.com/wp-content/uploads/sites/92/2015/02/02060120/REPORT-OF-PROF-DR-KAJ-HOBER.pdf).
- In der „Begründung“ wird einerseits vor einer Einflussnahme Russlands und andererseits durch die die Gefahr von Hackern geschrieben. Das ist nicht konsistent. Wenn wir den Krieg als „Sicherheitslücke“ ansehen, warum sind dann plötzlich Hacker das Problem?

Es fehlt mithin an den notwendigen Erkenntnissen, die eine entsprechende Warnung rechtfertigen. Wir müssen deutlicher machen, auf welche Fallgestaltung von § 7 Abs. 1 wir uns beziehen. Und auch bei der Verhältnismäßigkeitsprüfung muss noch deutlicher werden, dass und wie eine Abwägung vorgenommen wurde..

Wenn wir uns auf weitere Erkenntnisse in als VS eingestuften Dokumente berufen, dann sollten die in der Begründung eindeutig bezeichnet werden (Autor/Absender, Datum, TagebuchNr. Der VS-Reg)

Schließlich erweitern wir die Warnung auf „alle russischen IT-Hersteller“. Wir müssen mindestens ein bis zwei Sätze in der Begründung dafür aufwenden, wie wir dazu kommen. Das war auch nicht Auftrag aus der LR. Und sind die dann hinreichend bestimmbar? Sitz in Russland? Russische Eigentümer? Dazu müsste ggf. der Text der Warnung selbst nachgeschärft werden. Denkbar wäre insoweit aber eine allgemeine Sensibilisierung für den Einsatz von Software russischer Produkte, ähnlich wie es Frankreich getan hat.

Die Verkürzung der Frist auf eine Stunde müsste besser begründet werden. Vielleicht kann OC 2 da etwas aus dem aktuellen Lagebild beisteuern.
Wir lassen dem BMI immerhin auch einen Tag Zeit, da ist eine Stunde für den Betroffenen

schwer nachvollziehbar.

BL 23 und auch ich unterstützen auch weiterhin jederzeit – auch kurzfristig.

Mit freundlichen Grüßen
Im Auftrag

Horst Samsel

Abteilungsleiter BL

_____
Abteilung BL - Beratung für Bund, Länder und Kommunen
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: abteilung-bl@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Von: Welsch, Günther <guenther.welsch@bsi.bund.de>
Gesendet: Donnerstag, 3. März 2022 17:57
An: GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>
Cc: GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung Z <abteilung-z@bsi.bund.de>; GP Abteilung WG <abteilung-wg@bsi.bund.de>; GP Abteilung SZ <abteilung-sz@bsi.bund.de>; GP Abteilung DI <abteilung-di@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>
Betreff: EILT!: BSIG § 7 Warnung Kaspersky
Priorität: Hoch

EILT!: Warnung gem. BSIG § 7 vor Kaspersky

P/VP zur Billigung

über

parallele MZ: Abteilungen OC, BL, TK

zK: BL 23

Nachrichtlich: Abteilungen Z, WG, SZ, DI, Leitungsstab, Stab 1, Stab 3

1) Anbei lege ich die seitens Referat KM14 unter Mitwirkung von BL23 und weiterer Referate erarbeitete Warnung vor Kaspersky Anti-Virenschutz zur Billigung vor. Es handelt sich um zwei Dokumente: 1. Die Warnung an sich. 2. Die Begründung der Rechtmäßigkeit der Warnung. Die Kommentare seitens BL23 wurden bei der Finalisierung berücksichtigt.
2) Nach Billigung durch die Amtsleitung ist beabsichtigt, dem BMI die Warnung mit einem Tag Vorlagefrist zur Kenntnis vorzulegen. Einer Billigung seitens der Fachaufsicht bedarf es aufgrund der gesetzlichen Regelung nicht, jedoch sollte das BMI Gelegenheit haben, ggf. in den Dialog mit dem BSI vor Veröffentlichung einzutreten.

Dr. Welsch

8

008.pdf

Von:	Welsch, Günther
An:	Schönbohm, Arne; Schabhüser, Gerhard
Cc:	GP Leitungsstab; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Abteilung BL; GP Abteilung KM; GP Abteilung OC; GP Abteilung TK
Betreff:	AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum:	Freitag, 4. März 2022 10:37:06
Dringlichkeit:	Hoch

An P/VP

Die Abteilungen KM und TK haben den Nicht-Mitzeichnungsvermerk der Abt. BL durchgesehen.

Der von KM 14 dargelegte Sachvortrag und die enthaltenen stützenden sicherheitstechnischen Argumente sind plausibel und werthaltig. Insbesondere in der jetzigen kriegerischen Auseinandersetzung ist zu befürchten, dass jederzeit von der Möglichkeit Gebrauch gemacht werden kann, die Anti-Virenschutzsoftware von Kaspersky als Angriffswerkzeug zu missbrauchen. Ein Nachweis einer spezifischen technischen Schwachstelle ist in diesem Sinn gar nicht möglich bzw. erforderlich, da es bereits ausreicht, die systembedingt vorhandene Root-Berechtigung zum Zugriff auf die eigentlich durch die AV Software zu schützenden IT-Infrastrukturen für maliziöse Aktivitäten zu missbrauchen. Dieser Fall kann technisch nicht ausgeschlossen werden. Mutmaßungen darüber, ob die organisatorischen Strukturen bei Kaspersky bzw. die rechtliche Verfassung in Russland ausreichen, einen Missbrauch zu verhindern, sind müßig, da es weder derzeit eine Rechtsstaatlichkeit in Russland gibt noch Russland sich konform zu Gesetzen verhält. Russland führt einen durch die UNO verurteilten, völkerrechtswidrigen Angriffskrieg auf die Ukraine. Es gibt somit keinen einzigen Beleg für eine Garantie, dass eine solche potente Software im unmittelbaren Zugriff der russischen Behörden, wie es ein AV Schutz ist, nicht missbraucht werden könnte. Wir müssen dazu nicht erst den möglichen und wahrscheinlichen Eintritt eines solchen Ereignisse abwarten. Das BSI hat nicht die Aufgabe, ein Rechtschutzverfahren für Kaspersky zu begründen oder die Position von Kaspersky mit anderen möglichen Argumenten zu stützen und gegen die Sicherheitsinteressen der Bundesrepublik Deutschland abzuwiegen. Die Aufgabe des BSI ist es, präventiv die IT-Infrastrukturen in Deutschland vor möglichen IT-Angriffen zu schützen, von denen ein großes Risiko (sowohl potentieller Schaden wie auch hoher Eintrittswahrscheinlichkeit) ausgeht. Es ist Gefahr im Verzug und daher ist seitens BSI zu handeln, selbst wenn keine abschließende Sicherheit zu erlangen ist.

Eine positive Entscheidung in der Sache ist möglich. Eine Warnung sollte daher unverzüglich ausgesprochen werden. Die Rechtswidrigkeit wird hiermit vollumfänglich verneint. Weitere stützende juristische Argumente können seitens Abt. BL jederzeit beigetragen werden.

Die Anpassungen seitens LLS tragen wir mit.

Wir bitten um Entscheidung seitens der Amtsleitung.

Dr. Welsch
Thomas Caspers

Es folgt 007_geschwärzt.pdf als Zitat.

9

009.pdf

Von: GP Abteilung OC
An: GP Abteilung KM
Cc: GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Stab 3 - Strategie und Leitungsunterstuetzung; Schönbohm, Arne; Schabhüser, Gerhard; GP Abteilung BL; GP Abteilung TK
Betreff: AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum: Freitag, 4. März 2022 12:13:04

Hallo Günther,

ich zeichne mit!

Anmerkungen: Ich würde eine niederschwelligere Pressemitteilung gegenüber der formalen Warnung nach §7 präferieren, aber die Argumentation ist meines Erachtens schlüssig.

Ciao Dirk

Von: Welsch, Günther <guenther.welsch@bsi.bund.de>
Gesendet: Donnerstag, 3. März 2022 17:57
An: GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>
Cc: GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung Z <abteilung-z@bsi.bund.de>; GP Abteilung WG <abteilung-wg@bsi.bund.de>; GP Abteilung SZ <abteilung-sz@bsi.bund.de>; GP Abteilung DI <abteilung-di@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>
Betreff: EILT!: BSIG § 7 Warnung Kaspersky
Priorität: Hoch

EILT!: Warnung gem. BSIG § 7 vor Kaspersky

P/VP zur Billigung

über

parallele MZ: Abteilungen OC, BL, TK

zK: BL 23

Nachrichtlich: Abteilungen Z, WG, SZ, DI, Leitungsstab, Stab 1, Stab 3

1) Anbei lege ich die seitens Referat KM14 unter Mitwirkung von BL23 und weiterer Referate erarbeitete Warnung vor Kaspersky Anti-Virenschutz zur Billigung vor. Es handelt sich um zwei Dokumente: 1. Die Warnung an sich. 2. Die Begründung der Rechtmäßigkeit der Warnung. Die Kommentare seitens BL23 wurden bei der Finalisierung berücksichtigt.
2) Nach Billigung durch die Amtsleitung ist beabsichtigt, dem BMI die Warnung mit einem Tag Vorlagefrist zur Kenntnis vorzulegen. Einer Billigung seitens der Fachaufsicht bedarf es aufgrund der gesetzlichen Regelung nicht, jedoch sollte das BMI Gelegenheit haben,

ggf. in den Dialog mit dem BSI vor Veröffentlichung einzutreten.

Dr. Welsch

10

010_geschwärzt.pdf

Von: Schabhüser, Gerhard
An: GP Leitungsstab; Welsch, Günther; Schönbohm, Arne
Cc: GP Stab 1 - Strategische Kommunikation und Presse
Betreff: AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum: Freitag, 4. März 2022 13:59:02

So wie wir das schreiben, heizen wir m.E. eine Eskalation im Cyberraum an.

(Auch wenn ich grundsätzlich der Argumentation so zustimme)

Greift mir auch zu weit: Bei reinen onPremise Systemen, ohne zwingende oder mit abschaltbarer Verbindung zum Netz, als auch bei reiner Hardware, können wir m.E. keine besondere Bedrohung deklarieren.

Für Antivir und nahe Verwandte sicher.

Also mein Rat: Deutlich weniger eskalierend schreiben und auf besonders vulnerable Anwendungen beschränken.

shbr

Dr. Gerhard Schabhüser

_____

Vizepräsident
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: gerhard.schabhueser@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Von: GP Leitungsstab <leitungsstab@bsi.bund.de>
Gesendet: Donnerstag, 3. März 2022 20:03
An: Welsch, Günther <guenther.welsch@bsi.bund.de>; GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>
Cc: GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>
Betreff: AW: EILT!: BSIG § 7 Warnung Kaspersky

Liebe Kolleginnen und Kollegen,

obwohl nur im cc habe ich mir erlaubt zu kommentieren und im Änderungsmodus Änderungsvorschläge zu machen – siehe anbei.

Zum Hintergrund: die verwendeten Begrifflichkeiten sind mE nicht ganz stringent. Ich habe versucht, dies, auch unter Hinzuziehung der rechtlichen Begründung, anzupassen. „Gestoßen“ habe ich mich letztlich am Begriff „Hardware“, der im Übrigen nicht verwendet wird. Sofern ich falsch liege, gerne meine Änderungen ablehnen und vielleicht ein weiterer klarstellender Satz, was mit Hardware gemeint ist.

@P/VP: Ihnen auch als .pdf.

Gruß
[redacted]

im Auftrag
[redacted]
Leiterin Leitungsstab

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Telefonische Erreichbarkeit:
[redacted]

#DeutschlandDigitalSicherBSI

Von: Welsch, Günther <guenther.welsch@bsi.bund.de>
Gesendet: Donnerstag, 3. März 2022 17:57
An: GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>
Cc: GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung Z <abteilung-z@bsi.bund.de>; GP Abteilung WG <abteilung-wg@bsi.bund.de>; GP Abteilung SZ <abteilung-sz@bsi.bund.de>; GP Abteilung DI <abteilung-di@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>
Betreff: EILT!: BSIG § 7 Warnung Kaspersky
Priorität: Hoch

EILT!: Warnung gem. BSIG § 7 vor Kaspersky

P/VP zur Billigung

über

parallele MZ: Abteilungen OC, BL, TK

zK: BL 23

Nachrichtlich: Abteilungen Z, WG, SZ, DI, Leitungsstab, Stab 1, Stab 3

1) Anbei lege ich die seitens Referat KM14 unter Mitwirkung von BL23 und weiterer Referate erarbeitete Warnung vor Kaspersky Anti-Virenschutz zur Billigung vor. Es handelt sich um zwei Dokumente: 1. Die Warnung an sich. 2. Die Begründung der Rechtmäßigkeit der Warnung. Die Kommentare seitens BL23 wurden bei der Finalisierung berücksichtigt.
2) Nach Billigung durch die Amtsleitung ist beabsichtigt, dem BMI die Warnung mit einem Tag Vorlagefrist zur Kenntnis vorzulegen. Einer Billigung seitens der Fachaufsicht bedarf es aufgrund der gesetzlichen Regelung nicht, jedoch sollte das BMI Gelegenheit haben, ggf. in den Dialog mit dem BSI vor Veröffentlichung einzutreten.

Dr. Welsch

11

011_0_geschwärzt.pdf

Von:	Welsch, Günther
An:	GP Referat BL 23; GP Abteilung BL; GP Abteilung OC; GP Abteilung TK
Cc:	Schabhüser, Gerhard; Schönbohm, Arne; Caspers, Thomas; Samsel, Horst; Häger, Dirk; GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Referat KM 14 [redacted] GP Stab 3 - Strategie und Leitungsunterstuetzung
Betreff:	AW: AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum:	Freitag, 4. März 2022 19:13:00
Anlagen:	Kaspersky_Warnung_V6.odt VS-NfD_Kaspersky_Begründung_V6.odt
Dringlichkeit:	Hoch

P/VP

über

Abt. BL
Referat BL23

parallel: Abt. OC, Abt. TK

Anbei lege ich die in Rücksprache mit BL23 von KM14 überarbeiteten Entwürfe für die Warnung und die Begründung vor. Die Mitzeichnung seitens Abt. Änderungsvorschläge von LLS wurden übernommen. Der Fokus wurde auf die Viren-Schutzsoftware von Kaspersky gelegt, die allgemeine Warnung vor russischen Produkten zurückgenommen.

Ich bitte um Billigung und Freigabe der Übermittlung an das BMI.

Dr. Welsch

Von: Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>
Gesendet: Freitag, 4. März 2022 11:28
An: Caspers, Thomas <thomas.caspers@bsi.bund.de>; Samsel, Horst <horst.samsel@bsi.bund.de>; Welsch, Günther <guenther.welsch@bsi.bund.de>
Cc: Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>
Betreff: WG: AW: EILT!: BSIG § 7 Warnung Kaspersky
Priorität: Hoch

Liebe Kollegen,

Ich kann diese Warnung nicht freigeben bis die Fragestellung rechtlich geklärt ist. Bitte formulieren Sie die Warnung gemeinsam, damit die rechtlichen Hürden nach unserer Einschätzung ausgeräumt sind. Ziel ist es, diesen Entwurf am Montag im BMI zu besprechen. Des Weiteren bitte ich darum Sorge zu tragen, das keine Aussagen im teilweise öffentlichen Bereich ([redacted]) zu einer Produktwarnung des BSI zu Kaspersky gemacht wird, bevor diese vom BMI/BSI frei gegeben ist.

Mit freundlichen Grüßen

Arne Schönbohm

- via SecurePIM gesendet -

Es folgt 008.pdf als Zitat.

011_1_Kaspersky_Warnung_V6.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

Virenschutz-Software des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Viren-Schutzsoftware 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. Viren-Schutzsoftware 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 Angriffs mit weitreichenden Konsequenzen verbunden.

Die Bedrohungssituation durch offensive Cyber-Operationen von russischer Seite führen in der aktuellen Lage zu einer neuen Risikobewertung. Ein russischer IT-Hersteller kann selbst entsprechende 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/Nutzer der Viren-Schutzsoftware 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 Interesse des Staates, 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 aber auch Opfer von Kollateralauswirkungen werden.

3 Betroffene Produkte

Betroffen ist das Portfolio von Viren-Schutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Viren-Schutzsoftware 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 vom zuständigen Landesamt für Verfassungsschutz bzw. vom Bundesamt für Verfassungsschutz individuell beraten zu lassen.

Allgemeiner Hinweis: Der Wechsel wesentlicher Bestandteile einer IT-Sicherheitsinfrastruktur muss im Enterprise-Bereich immer sorgfältig geplant und durchgeführt werden. Würden IT-Sicherheitsprodukte (also insbesondere Viren-Schutzsoftware) 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/DasBSI/Gesetz/gesetz_node.html
[2] Darstellung Risikostufen
https://www.cert-bund.de/risk

011_2_VS-NfD_Kaspersky_Begründung_V6_geschwärzt.pdf

Einstufung nach Schwärzung aufgehoben.

Referat KM 14 02. 03. 2021

Az. KM14-210 01 03 / VS-NfD

[redacted]

Betr. Bewertung von IT-Sicherheitsprodukten
hier: Warnung vor Kaspersky-Produkten nach § 7 BSIG

Bezug

Anlagen Entwurf Warntext

1) Vermerk zur Begründung der Warnung

A Begründung der Warnung nach § 7 Abs. 1 BSIG

Das BSI darf nach § 7 Abs. 1 BSIG u.a. vor Sicherheitslücken in informationstechnischen Produkten und Diensten öffentlich warnen. Sicherheitslücken in diesem Sinne sind nach § 2 Abs. 6 BSIG *„Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.“* Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1.d BSIG). Dabei ist nach Meinung in der Literatur zwar noch ein Bezug zur Gefahrenvorsorge notwendig, aber keine konkrete Gefahrenlage mehr (vgl. Ritter-*Schulte,* Die Weiterentwicklung des IT-Sicherheitsgesetzes, Art. 1 Nr. 9 IT-SiG 2.0, Rn. 307). Solche Sicherheitseigenschaften von Produkten können sich auch aus der Struktur des Anbieters ergeben. Da hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI vor dem Einsatz des Produktes warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG).

Die Ereignisse rund um Kaspersky werden vom BSI seit Jahren aufmerksam verfolgt. Mehrere westliche Staaten wie USA und Niederlande warnen seit Jahren öffentlich vor Kaspersky und haben die Software für den Einsatz im Behördenumfeld gesperrt [redacted] Das BSI hat sich aber bislang mit öffentlichen Warnungen zu Kaspersky zurückgehalten.

Der russische Angriff auf die Ukraine, der mit hybriden Mitteln - also auch im Cyberraum - geführt wird und von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt wurde, verändert die Lagebeurteilung. Russland ist kein demokratischer Rechtsstaat und sieht Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als Feind an. Mit feindlichen Übergriffen auf deutsche Institutionen,

Einstufung nach Schwärzung aufgehoben.

Unternehmen und IT-Infrastrukturen ist daher zu rechnen. Russische Unternehmen könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden, zum anderen selbst Ziel massiver Cyberangriffe werden. Die Gefahr, dass Kaspersky in die kriegerischen Auseinandersetzungen hineingezogen wird, ist daher so groß, dass eine Warnung angemessen ist. Es muss damit gerechnet werden, dass Kaspersky nicht mehr die uneingeschränkte Kontrolle über seine Software und IT-Systeme hat bzw. diese in Kürze verlieren wird.

[redacted]

Bereits in den letzten Jahren wurden Fälle bekannt, in denen staatliche Stellen Einfluss auf Kaspersky genommen haben:

[redacted]

In den Jahren 2018 und 2019 wurden russische VPN-Anbieter gezwungen, bestimmte Verbindungen auf Anordnung der Regierung zu blocken. Während die meisten Anbieter die Kooperation verweigerten, kam Kaspersky den Anordnungen nach[2]:

"Although not all VPNs are banned, a 2018 law introduced fines for search engines that brought up results to proxy sites (including VPNs) that would give Russians access to prohibited content or instructions on how to get access to that content.
The following year, VPNs and search engines were compelled to block any websites that appeared on the federal government blacklist. Later, 10 VPN providers were ordered to hand over access to their servers or face being banned. Only one, Kaspersky Lab, which is based in Russia, agreed, while others - like ExpressVPN and NordVPN - shut down their Russian servers."

Neben dem BSI haben auch andere Organisationen ihre Risikobewertung angepasst. Frankreich hat beispielsweise eine vergleichbare Warnung veröffentlicht[3]. [redacted] Die Teilnehmer waren sich einig, dass der Einsatz von Kaspersky-Produkten hoch

1 [redacted]
2 https://www.techradar.com/vpn/which-websites-and-services-are-banned-in-russia
3 https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

problematisch ist. Zum Schutz ihrer IT-Systeme wurden daher automatische Updates abgestellt und Schritte eingeleitet, um die Software schnellstmöglich durch eine sicherere Alternative abzulösen.

Die in der Warnung beschriebenen Angriffsvektoren sind nicht neu. Im Folgenden einige Beispiele, die belegen, welchen Schaden ein Angreifer mit Viren-Schutzsoftware anrichten könnte:

- ✗ Am 10.06.2015 hat Kaspersky selbst in einer Pressemitteilung[4] mitgeteilt, dass das Unternehmensnetzwerk gehackt wurde und Angreifer mit teils neuen Methoden versucht haben, vertrauliche Daten zu stehlen, die dann für Angriffe auf die Kunden missbraucht werden könnten.
- ✗ Am 05. Januar 2012 hat die Hacker-Gruppe „The Lords of Dharmaraja“ geheimen Sourcecode von Symantec bei Pastebin veröffentlicht. Symantec hat die Echtheit des Codes bestätigt und die sicherheitsrelevanten Auswirkungen mit dem BSI-Präsidenten in einem vertraulichen Gespräch erörtert.
- ✗ Alle Hersteller von Viren-Schutzprogrammen hatten in der Vergangenheit Schwachstellen, die für Angriffe auf Kundensysteme hätten genutzt werden können. Mit Kenntnis des Sourcecode oder noch nicht veröffentlichter Schwachstellen wäre eine Angreifer nicht auf offiziell gemeldete Schwachstellen angewiesen, um einen Angriff durchzuführen. Wenn schon Schwachstellen ausreichen, um Systeme komplett stillzulegen, wäre dies mit einer Backdoor noch sehr viel leichter.
- ✗ Es sind zahlreiche Vorfälle bei allen Herstellern von Viren-Schutzsoftware bekannt, in denen eine fehlerhafte Erkennungssignatur Windows-Systemdateien als schädlich klassifiziert und damit das IT-System blockiert hat.
- ✗ Es sind auch Vorfälle bekannt, bei denen nach einem Signaturupdate bestimmte Schadprogramme irrtümlich nicht mehr detektiert wurden.
- ✗ Alle Viren-Schutzprogramme haben Funktionen eingebaut, mit denen sich Schadsoftwareausbrüche begrenzen lassen. Dazu können sie beliebige Dateien blockieren oder löschen. Auch in der Bundesverwaltung hat es bereits einen Sicherheitsvorfall gegeben, bei dem durch eine Fehlbedienung der "Outbreak-Prevention"-Funktion eine ganze Behörde für einen Tag lahmgelegt wurde.
- ✗ Bei Updates werden nicht immer nur Signaturen übertragen. Es ist auch möglich, dass größere Softwarebestandteile (z. B. Scan-Engines) aktualisiert werden müssen, um mit neuen Signaturen/Erkennungsverfahren kompatibel zu bleiben. Dem BSI sind Fälle bekannt, bei denen durch Updates eines Viren-Schutzprogramms neue Funktionen installiert oder Konfigurationen überschrieben wurden, ohne dass die Nutzer dies bemerken konnten. In der Folge wurde Kundendaten ohne Genehmigung an den Hersteller übertragen.

Derartige Vorfälle mussten alle Hersteller bereits vermelden. Sie sind immer unbeabsichtigt aufgrund von Fehlern oder Nachlässigkeiten geschehen. Eigene Entwickler oder Hacker, die in die Systeme des Herstellers eingedrungen sind, sind nicht auf Schwachstellen oder Fehler angewiesen, und könnten daher sehr einfach die folgenden Funktionen auf Kundensystemen implementieren:

- Zielsysteme analysieren (Systemeigenschaften, Hardwareeigenschaften, verwendete Software etc.)
- Daten zum Hersteller übertragen (z. B. Dateien, URLs)
- Dateien sperren oder löschen

Um die gewollten Funktionalität bieten zu können, laufen Viren-Schutzprogramme zudem mit hohen Systemrechten, schützen sich vor Veränderungen und haben Zugriff auf das gesamte Filesystem. Durch die

4 https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig ist, könnten theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Manipulationen lassen sich auch temporär vornehmen und dadurch sehr gut tarnen. Beispielsweise könnte für wenige Stunden ein bestimmter Schadcode bewusst nicht erkannt werden, um anderen Angreifern den Weg zu bereiten.

Wenn die Kaspersky-Produkte für Angriffe entweder durch Anweisung der russischen Regierung oder durch staatliches Eindringen in deren Systeme instrumentalisiert werden, ist es daher möglich, dass auf die Systeme auf denen Kaspersky-Produkte installiert sind, unberechtigt zugegriffen oder Einfluss genommen werden kann.

Kaspersky ist sich dieser Gefahren bewusst und hat in der Vergangenheit diverse Maßnahmen zur Vertrauensbildung ergriffen, die aber alle nicht geeignet sind, die aktuelle Gefahrenlage zu entschärfen.

✗ Kaspersky hat versucht, sich dem Einfluss russischer Behörden zu entziehen und betreibt eine Dateninfrastruktur in zwei Rechenzentren in Zürich zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden aus Europa, den Vereinigten Staaten und Kanada sowie in mehreren asiatisch-pazifischen Ländern. Für die Bereitstellung von Updates/Virensignaturen stehen bei Bedarf verschiedene Server in Europa zur Verfügung, unter anderem in Frankfurt.

  Es ist unerheblich, wo die Kundendaten gehostet werden. Entscheidend ist, wer Sourceodeänderungen vornehmen und Signaturdaten erstellen kann und wie diese qualitätsgesichert und geprüft werden. Kaspersky kann nicht nachweisen, dass diese Prozesse komplett unabhängig vom russischen Hauptquartier durchgeführt werden. Es ist auch nicht transparent, wer administrativen Zugang zu den Systemen in Westeuropa hat. Aufgrund der Erfahrungen mit anderen Cloudanbietern ist es extrem unwahrscheinlich, dass die Rechenzentren in West-Europa komplett autark arbeiten und keine administrativen Eingriffe aus anderen Regionen erfolgen können.

✗ Die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren und Datendienste von Kaspersky wurden von zwei externen, unabhängigen Prüforganisationen bestätigt. Kaspersky hat das SOC-2-Audit (Service Organization Control for Service Organizations) Typ 1 durch einen Big-Four-Auditor erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigte. Darüber hinaus wurden Datendienste vom TÜV AUSTRIA nach ISO/IEC 27001:2013 zertifiziert.

  Eine Zertifizierung sagt nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus. Sie ist keine Garantie für den Ist-Zustand.

✗ Kaspersky sagt über sich selbst, als global agierendes privates Unternehmen (Sitz der Holding ist London, UK) keine Verbindungen zur russischen Regierung zu haben.

  Diese Aussage ist nicht glaubhaft. Kaspersky hat seinen Hauptsitz in Moskau und weist eine russische Eigentümerstruktur auf. Als eines der wichtigsten IT-Security-Unternehmen Russlands arbeitet Kaspersky eng mit Ermittlungsbehörden zusammen (s. o.). Wesentliche Teile der Belegschaft arbeiten daher in Russland oder haben familiäre Bindungen in Russland und sind daher dem direkten Einfluss und Druck der Behörden ausgesetzt.

✗ Kaspersky unterliegt nach eigenen Angaben nicht dem russischen System operativer Ermittlungsmaßnahmen (SORM) oder anderen ähnlichen Gesetzen und sei deswegen nicht zur Auskunftserteilung verpflichtet.

  Diese faktischen Einflussmöglichkeiten der russischen Regierung entfallen nicht deswegen, weil Kaspersky nach russischem Recht keinen Mitwirkungspflichten unterliegt (zu den Pflichten s. Gutachten Prof. Hober). Angesichts des eklatanten Bruchs von internationalem Recht durch Russland muss damit

gerechnet werden, dass faktisch möglicher Einfluss der russischen Regierung auch gegen geltendes russisches Recht ausgeübt werden wird.

Fazit:

Durch manipulierte Viren-Schutzprogramme hat ein Angreifer nahezu unbegrenzte Möglichkeiten, IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste Vorfall öffentlich bekannt wird. Vielmehr ist die Warnung zum jetzigen Zeitpunkt angezeigt, um rechtzeitig präventiv zu handeln und die relevanten Anwender vor potentiellem Schaden zu bewahren. Mildere Mittel zum Schutz der Informationssicherheit sind nicht ersichtlich.

B Vorherige Stellungnahmemöglichkeit nach § 7 Abs. 1 a Nr. 1 BSIG

Kaspersky sollte vor der Veröffentlichung nur mit kurzer Frist informiert und Gelegenheit zur Stellungnahme gegeben werden. Es ist Gefahr im Verzug. Hacker könnten ihre Vorbereitungen bereits abgeschlossen haben und nur noch auf einen Einsatzbefehl warten. Es ist nicht ersichtlich, dass Kaspersky eine Möglichkeit hätte, durch technische oder sonstige Maßnahmen die Risikoeinschätzung positiv zu beeinflussen. Es ist nicht wahrscheinlich, dass der Hersteller an dem zugrunde liegenden strukturellen Sicherheitsproblem etwas ändern kann, da er kaum Einfluss auf die Gefährdung hat. Angesichts der Gefährdungslage erscheint eine kurze Frist daher verhältnismäßig und fachlich angemessen.

C Verfügung

2) BL 23 zur Kenntnis

3) KM zur Mitzeichnung [MZ. AL KM vom 3.3.2002]

4) TK zur Mitzeichnung

5) OC zur Mitzeichnung

6) BL zur Mitzeichnung

7) P/VP z. Billigung

Im Auftrag

[redacted]

12

012_geschwärzt.pdf

Von: GP Abteilung TK
An: Welsch, Günther
Cc: Schabhüser, Gerhard; Schönbohm, Arne; Caspers, Thomas; Samsel, Horst; Häger, Dirk; GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Referat KM 14; [redacted] GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer_TK; GP Referat BL 23; GP Abteilung BL; GP Abteilung OC; GP Abteilung KM
Betreff: AW: AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum: Freitag, 4. März 2022 19:30:41

Lieber Günther,

Abteilung TK zeichnet mit.

Viele Grüße

Thomas

--
Thomas Caspers
Abteilungsleiter
Technik-Kompetenzzentren

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
E-Mail: thomas.caspers@bsi.bund.de
Internet: www.bsi.bund.de

Es folgt 011_0_geschwärzt.pdf als Zitat.

13

013_0_geschwärzt.pdf

Von: Samsel, Horst
An: Schönbohm, Arne; Schabhüser, Gerhard
Cc: Häger, Dirk; Caspers, Thomas; Welsch, Günther; [redacted]
Betreff: EILT!: BSIG § 7 Warnung Kaspersky
Datum: Freitag, 4. März 2022 19:51:18
Anlagen: Kaspersky_Warnung_V6.odt
VS-NfD_Kaspersky_Begründung_V6.odt
Dringlichkeit: Hoch

P/VP

über

Abt. BL [Sam 4/3] Mitzeichnung für BL
Referat BL23

Es folgt 011_0_geschwärzt.pdf als Zitat inkl. der Anhänge 011_1_Kaspersky_Warnung_V6.pdf und 011_2_VS-NfD_Kaspersky_Begründung_V6_geschwärzt.pdf.

14

014_geschwärzt.pdf

Von:	GP Abteilung OC
An:	Welsch, Günther; GP Referat BL 23; GP Abteilung BL; GP Abteilung TK
Cc:	Schabhüser, Gerhard; Schönbohm, Arne; Caspers, Thomas; Samsel, Horst; GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Referat KM 14; [redacted] GP Stab 3 - Strategie und Leitungsunterstuetzung
Betreff:	AW: AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum:	Freitag, 4. März 2022 20:07:07

Hallo Günther,

ich zeichne auch mit.

Eine Anmerkung zu den Handlungsempfehlungen (also keine Kritik an der Warnung an sich, sondern an den Ratschlägen am Ende):
Wir schreiben: „Sie haben die Möglichkeit, sich vom zuständigen Landesamt für Verfassungsschutz bzw. vom Bundesamt für Verfassungsschutz individuell beraten zu lassen.“
Damit dies so drin bleiben kann, sollte zeitgleich zum Versand an das BMI auch das BfV informiert werden. Außerdem fände ich es besser, wenn wir KRITIS-Unternehmen nicht einfach an den Verfassungsschutz verweisen, sondern auch Rückfragen beim BSI anbieten. Insofern folgender Formulierungsvorschlag:
„Sie haben die Möglichkeit, sich von den zuständigen Verfassungsschutzbehörden bzw. vom BSI beraten zu lassen.“

Tut mir leid, dass ich damit erst jetzt komme, aber bisher lag mein Augenmerk auf „wie begründen wir die Warnung“, und nicht auf den Maßnahmen.

Ciao Dirk

Es folgt 011_0_geschwärzt.pdf als Zitat.

15

015_geschwärzt.pdf

Von: Schönbohm, Arne
An: GP Abteilung OC; Welsch, Günther; GP Abteilung TK; GP Referat BL 23; GP Abteilung BL
Cc: Samsel, Horst; GP Stab 1 - Strategische Kommunikation und Presse; GP Leitungsstab; GP Stab 3 - Strategie und Leitungsunterstuetzung; [redacted] GP Referat KM 14; Schabhüser, Gerhard [redacted]; Caspers, Thomas
Betreff: AW: AW: AW: EILT!: BSIG § 7 Warnung Kaspersky
Datum: Freitag, 4. März 2022 20:52:33

Freigabe mit dem Hinweis von OC. Herr Dr. Welsch würden Sie dies an CI weiterleiten?

Mit freundlichen Grüßen

Arne Schönbohm

- via SecurePIM gesendet -

Am 4. März 2022 20:07, hat "GP Abteilung OC" geschrieben:

Hallo Günther,

ich zeichne auch mit.

Eine Anmerkung zu den Handlungsempfehlungen (also keine Kritik an der Warnung an sich, sondern an den Ratschlägen am Ende):
Wir schreiben: „Sie haben die Möglichkeit, sich vom zuständigen Landesamt für Verfassungsschutz bzw. vom Bundesamt für Verfassungsschutz individuell beraten zu lassen."
Damit dies so drin bleiben kann, sollte zeitgleich zum Versand an das BMI auch das BfV informiert werden. Außerdem fände ich es besser, wenn wir KRITIS-Unternehmen nicht einfach an den Verfassungsschutz verweisen, sondern auch Rückfragen beim BSI anbieten. Insofern folgender Formulierungsvorschlag:
„Sie haben die Möglichkeit, sich von den zuständigen Verfassungsschutzbehörden bzw. vom BSI beraten zu lassen."

Tut mir leid, dass ich damit erst jetzt komme, aber bisher lag mein Augenmerk auf „wie begründen wir die Warnung", und nicht auf den Maßnahmen.

Ciao Dirk

> **Von:** Welsch, Günther <guenther.welsch@bsi.bund.de>
> **Gesendet:** Freitag, 4. März 2022 19:14
> **An:** GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>
> **Cc:** Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Caspers, Thomas <thomas.caspers@bsi.bund.de>; Samsel,

Horst <horst.samsel@bsi.bund.de>; Häger, Dirk <dirk.haeger@bsi.bund.de>; GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Referat KM 14 <referat-km14@bsi.bund.de>; [redacted]@bsi.bund.de>; [redacted]@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>
Betreff: AW: AW: EILT!: BSIG § 7 Warnung Kaspersky
Priorität: Hoch

P/VP

über

Abt. BL
Referat BL23

parallel: Abt. OC, Abt. TK

Anbei lege ich die in Rücksprache mit BL23 von KM14 überarbeiteten Entwürfe für die Warnung und die Begründung vor. Die Mitzeichnung seitens Abt. Änderungsvorschläge von LLS wurden übernommen. Der Fokus wurde auf die Viren-Schutzsoftware von Kaspersky gelegt, die allgemeine Warnung vor russischen Produkten zurückgenommen.

Ich bitte um Billigung und Freigabe der Übermittlung an das BMI.

Dr. Welsch

Von: Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>
Gesendet: Freitag, 4. März 2022 11:28
An: Caspers, Thomas <thomas.caspers@bsi.bund.de>; Samsel, Horst <horst.samsel@bsi.bund.de>; Welsch, Günther <guenther.welsch@bsi.bund.de>
Cc: Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>
Betreff: WG: AW: EILT!: BSIG § 7 Warnung Kaspersky
Priorität: Hoch

Liebe Kollegen,

Ich kann diese Warnung nicht freigeben bis die Fragestellung rechtlich geklärt ist. Bitte formulieren Sie die Warnung gemeinsam, damit die rechtlichen Hürden nach unserer Einschätzung ausgeräumt sind. Ziel ist es, diesen Entwurf am Montag im BMI zu besprechen. Des Weiteren bitte ich darum Sorge zu tragen, das keine Aussagen im teilweise öffentlichen Bereich [redacted] zu einer Produktwarnung des BSI zu Kaspersky gemacht wird, bevor diese vom BMI/BSI frei gegeben ist.

Mit freundlichen Grüßen

Arne Schönbohm

- via SecurePIM gesendet -

Von: "Welsch, Günther" <guenther.welsch@bsi.bund.de>
Gesendet: 4. März 2022 10:37
An: "Schönbohm, Arne" <arne.schoenbohm@bsi.bund.de>, "Schabhüser, Gerhard" <gerhard.schabhueser@bsi.bund.de>
Cc: "GP Leitungsstab" <leitungsstab@bsi.bund.de>, "GP Stab 3 - Strategie und Leitungsunterstuetzung" <stab3@bsi.bund.de>, "GP Abteilung BL" <abteilung-bl@bsi.bund.de>, "GP Abteilung KM" <abteilung-km@bsi.bund.de>, "GP Abteilung OC" <abteilung-oc@bsi.bund.de>, "GP Abteilung TK" <abteilung-tk@bsi.bund.de>
Betreff: WG: AW: EILT!: BSIG § 7 Warnung Kaspersky

An P/VP

Die Abteilungen KM und TK haben den Nicht-Mitzeichnungsvermerk der Abt. BL durchgesehen.

Der von KM 14 dargelegte Sachvortrag und die enthaltenen stützenden sicherheitstechnischen Argumente sind plausibel und werthaltig. Insbesondere in der jetzigen kriegerischen Auseinandersetzung ist zu befürchten, dass jederzeit von der Möglichkeit Gebrauch gemacht werden kann, die Anti-Virenschutzsoftware von Kaspersky als Angriffswerkzeug zu missbrauchen. Ein Nachweis einer spezifischen technischen Schwachstelle ist in diesem Sinn gar nicht möglich bzw. erforderlich, da es bereits ausreicht, die systembedingt vorhandene Root-Berechtigung zum Zugriff auf die eigentlich durch die AV Software zu schützenden IT-Infrastrukturen für maliziöse Aktivitäten zu missbrauchen. Dieser Fall kann technisch nicht ausgeschlossen werden. Mutmaßungen darüber, ob die organisatorischen Strukturen bei Kaspersky bzw. die rechtliche Verfassung in Russland ausreichen, einen Missbrauch zu verhindern, sind müßig, da es weder derzeit eine Rechtsstaatlichkeit in Russland gibt noch Russland sich konform zu Gesetzen verhält. Russland führt einen durch die UNO verurteilten, völkerrechtswidrigen Angriffskrieg auf die Ukraine. Es gibt somit keinen einzigen Beleg für eine Garantie, dass eine solche potente Software im unmittelbaren Zugriff der russischen Behörden, wie es ein AV Schutz ist, nicht missbraucht werden könnte. Wir müssen dazu nicht erst den möglichen und wahrscheinlichen Eintritt eines solchen Ereignisse abwarten. Das BSI hat nicht die Aufgabe, ein Rechtschutzverfahren für Kaspersky zu begründen oder die Position von Kaspersky mit anderen möglichen Argumenten zu stützen und gegen die Sicherheitsinteressen der Bundesrepublik Deutschland abzuwiegen. Die Aufgabe des BSI ist es, präventiv die IT-Infrastrukturen in Deutschland vor möglichen IT-Angriffen zu schützen, von denen ein großes Risiko (sowohl potentieller Schaden wie auch hoher Eintrittswahrscheinlichkeit) ausgeht. Es ist Gefahr im Verzug und daher ist seitens BSI zu handeln, selbst wenn keine abschließende Sicherheit zu erlangen ist.

Eine positive Entscheidung in der Sache ist möglich. Eine Warnung sollte daher unverzüglich ausgesprochen werden. Die Rechtswidrigkeit wird hiermit vollumfänglich verneint. Weitere stützende juristische Argumente können seitens Abt. BL jederzeit beigetragen werden.

Die Anpassungen seitens LLS tragen wir mit.

Wir bitten um Entscheidung seitens der Amtsleitung.

Dr. Welsch
Thomas Caspers

Von: GP Abteilung BL <abteilung-bl@bsi.bund.de>
Gesendet: Freitag, 4. März 2022 09:54
An: Welsch, Günther <guenther.welsch@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>
Cc: GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung Z <abteilung-z@bsi.bund.de>; GP Abteilung WG <abteilung-wg@bsi.bund.de>; GP Abteilung SZ <abteilung-sz@bsi.bund.de>; GP Abteilung DI <abteilung-di@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>; GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; [redacted]@bsi.bund.de>; GP Fachbereich BL 2 <fachbereich-bl2@bsi.bund.de>
Betreff: AW: EILT!: BSIG § 7 Warnung Kaspersky

Liebe Kolleginnen und Kollegen,

aus Sicht von BL ist die Begründung noch nicht hinreichend substantiiert, um die Warnung mitzeichnen zu können und sollte deshalb noch nachgeschärft werden.

Die Hauptprobleme sehen wir vor allem hierin:

- <!--[if !supportLists]-->- <!--[endif]-->Die Voraussetzungen des § 7 – insbesondere das Vorliegen einer Sicherheitslücke - werden nicht sauber dargelegt. Das scheint mir hier jedoch besonders wichtig, da wir eine technische Sicherheitslücke derzeit nicht nachweisen können.
- <!--[if !supportLists]-->- <!--[endif]-->Es wird nirgendwo darauf eingegangen, dass Kaspersky nach der Krim-Krise bereits organisatorische Maßnahmen ergriffen hat, die eine russische Einflussnahme ausschließen sollen (Serververlegung in die CH usw.). Ein Gutachten einer schwedischen Uni bescheinigt Kaspersky, nicht bestimmten russischen Gesetzen zu unterliegen, die eine Kooperation mit der russ. Regierung erzwingen könnten. Damit setzen sich die Dokumente nicht auseinander. Meines Erachtens laufen wir damit schon formal in einen Ermessensnichtgebrauch und damit die Rechtswidrigkeit. (Das Gutachten findet sich unter https://media.kasperskydaily.com/wp-content/uploads/sites/92/2015/02/02060120/REPORT-OF-PROF-DR-KAJ-HOBER.pdf).
- <!--[if !supportLists]-->- <!--[endif]-->In der „Begründung" wird einerseits vor einer Einflussnahme Russlands und andererseits durch die die Gefahr von Hackern geschrieben. Das ist nicht konsistent. Wenn wir den Krieg als „Sicherheitslücke" ansehen, warum sind dann plötzlich Hacker das Problem?

Es fehlt mithin an den notwendigen Erkenntnissen, die eine entsprechende Warnung

rechtfertigen. Wir müssen deutlicher machen, auf welche Fallgestaltung von § 7 Abs. 1 wir uns beziehen. Und auch bei der Verhältnismäßigkeitsprüfung muss noch deutlicher werden, dass und wie eine Abwägung vorgenommen wurde..

Wenn wir uns auf weitere Erkenntnisse in als VS eingestuften Dokumente berufen, dann sollten die in der Begründung eindeutig bezeichnet werden (Autor/Absender, Datum, TagebuchNr. Der VS-Reg)

Schließlich erweitern wir die Warnung auf „alle russischen IT-Hersteller". Wir müssen mindestens ein bis zwei Sätze in der Begründung dafür aufwenden, wie wir dazu kommen. Das war auch nicht Auftrag aus der LR. Und sind die dann hinreichend bestimmbar? Sitz in Russland? Russische Eigentümer? Dazu müsste ggf. der Text der Warnung selbst nachgeschärft werden.
Denkbar wäre insoweit aber eine allgemeine Sensibilisierung für den Einsatz von Software russischer Produkte, ähnlich wie es Frankreich getan hat.

Die Verkürzung der Frist auf eine Stunde müsste besser begründet werden. Vielleicht kann OC 2 da etwas aus dem aktuellen Lagebild beisteuern.
Wir lassen dem BMI immerhin auch einen Tag Zeit, da ist eine Stunde für den Betroffenen schwer nachvollziehbar.

BL 23 und auch ich unterstützen auch weiterhin jederzeit – auch kurzfristig.

Mit freundlichen Grüßen
Im Auftrag

Horst Samsel

Abteilungsleiter BL

_____
Abteilung BL - Beratung für Bund, Länder und Kommunen
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: abteilung-bl@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Von: Welsch, Günther <guenther.welsch@bsi.bund.de>
Gesendet: Donnerstag, 3. März 2022 17:57
An: GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>
Cc: GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung

<stab3@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; GP Abteilung Z <abteilung-z@bsi.bund.de>; GP Abteilung WG <abteilung-wg@bsi.bund.de>; GP Abteilung SZ <abteilung-sz@bsi.bund.de>; GP Abteilung DI <abteilung-di@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>
Betreff: EILT!: BSIG § 7 Warnung Kaspersky
Priorität: Hoch

EILT!: Warnung gem. BSIG § 7 vor Kaspersky

P/VP zur Billigung

über

parallele MZ: Abteilungen OC, BL, TK

zK: BL 23

Nachrichtlich: Abteilungen Z, WG, SZ, DI, Leitungsstab, Stab 1, Stab 3

<!--[if !supportLists]-->1) <!--[endif]-->Anbei lege ich die seitens Referat KM14 unter Mitwirkung von BL23 und weiterer Referate erarbeitete Warnung vor Kaspersky Anti-Virenschutz zur Billigung vor. Es handelt sich um zwei Dokumente: 1. Die Warnung an sich. 2. Die Begründung der Rechtmäßigkeit der Warnung. Die Kommentare seitens BL23 wurden bei der Finalisierung berücksichtigt.

<!--[if !supportLists]-->2) <!--[endif]-->Nach Billigung durch die Amtsleitung ist beabsichtigt, dem BMI die Warnung mit einem Tag Vorlagefrist zur Kenntnis vorzulegen. Einer Billigung seitens der Fachaufsicht bedarf es aufgrund der gesetzlichen Regelung nicht, jedoch sollte das BMI Gelegenheit haben, ggf. in den Dialog mit dem BSI vor Veröffentlichung einzutreten.

Dr. Welsch

16

016_0_geschwärzt.pdf

Einstufung nach Schwärzung aufgehoben.

Von:	Welsch, Günther
An:	"Andreas.Koenen@bmi.bund.de"; "CI@bmi.bund.de"
Cc:	Schönbohm, Arne; Schabhüser, Gerhard; Caspers, Thomas; Samsel, Horst; Häger, Dirk; [redacted] GP Stab 3 - Strategie und Leitungsunterstuetzung; CI3@bmi.bund.de; CI4@bmi.bund.de; "ci1@bmi.bund.de"; "Katja.Papenkort@bmi.bund.de"; "Andreas.Reisen@bmi.bund.de"; Michael Baum; "Barbara.Kluge@bmi.bund.de"; GP Leitungsstab
Bcc:	[redacted] GP Stab 1 - Strategische Kommunikation und Presse; Welsch, Günther
Betreff:	§ 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Samstag, 5. März 2022 07:44:00
Anlagen:	Kaspersky_Warnung_VZ.odt VS-NfD_Kaspersky_Begründung_VZ.odt VS-NfD_Kaspersky_Begründung_VZ.pdf Kaspersky_Warnung_VZ.pdf
Dringlichkeit:	Hoch

VS-NfD

Lieber Herr Könen,

anbei sende ich Ihnen im Auftrag von Herrn Schönbohm die vorbereitete BSI-Warnung gemäß BSIG § 7 zu Produkten des Unternehmens Kaspersky inkl. der fachlichen Begründung.

Durch manipulierte Viren-Schutzprogramme des Unternehmens Kaspersky hat ein Angreifer nahezu unbegrenzte Möglichkeiten, IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste Vorfall öffentlich bekannt wird. Vielmehr ist die Warnung zum jetzigen Zeitpunkt angezeigt, um rechtzeitig präventiv zu handeln und die relevanten Anwender vor potentiellem Schaden zu bewahren. Mildere Mittel zum Schutz der Informationssicherheit in Deutschland sind nicht ersichtlich.

Herr Schönbohm würde gerne mit Ihnen im Jour Fixe am kommenden Montag das weitere Vorgehen des BSI mit Blick auf die Veröffentlichung der Warnung seitens BSI abstimmen. Seitens des BSI sind wir an einer starken politischen Flankierung durch das BMI interessiert.

Für fachlich-technische Rückfragen stehen Ihnen Herr Caspers, Herr Dr. Häger [redacted] sowie ich gerne zur Verfügung. Für die rechtlichen Rückfragen steht Ihnen Herr Samsel zur Verfügung.

[redacted]

Mit freundlichen Grüßen,
im Auftrag
Günther Welsch

--- --- --- --- --- --- --- ---

Dr. Günther Welsch
Abteilungsleiter KM
Bundesamt für Sicherheit in der Informationstechnik
53175 Bonn

Tel: 0228 9582 [redacted]
Mobil: [redacted]

Es folgt 003_0_geschwärzt.pdf als Zitat.

016_1_Kaspersky_Warnung_V7.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

Viren-Schutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Viren-Schutzsoftware 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. Viren-Schutzsoftware 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.

Die Bedrohungssituation durch offensive Cyber-Operationen von russischer Seite führen in der aktuellen Lage zu einer neuen Risikobewertung. Ein russischer IT-Hersteller kann selbst entsprechende 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 Viren-Schutzsoftware 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 Interesse des Staates, 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 Viren-Schutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Viren-Schutzsoftware 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 Viren-Schutzsoftware) 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/DasBSI/Gesetz/gesetz_node.html
[2] Darstellung Risikostufen
https://www.cert-bund.de/risk

016_2_VS-NfD_Kaspersky_Begründung_V7_geschwärzt.pdf

Referat KM 14 04. 03. 2022

Az. KM14-210 01 03 / VS-NfD

[redacted]

Betr. Bewertung von IT-Sicherheitsprodukten
hier: Warnung vor Kaspersky-Produkten nach § 7 BSIG

Bezug

Anlagen Entwurf Warntext

1) Vermerk zur Begründung der Warnung

A Begründung der Warnung nach § 7 Abs. 1 BSIG

Das BSI darf nach § 7 Abs. 1 BSIG u. a. vor Sicherheitslücken in informationstechnischen Produkten und Diensten öffentlich warnen. Sicherheitslücken in diesem Sinne sind nach § 2 Abs. 6 BSIG *„Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.“* Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1.d BSIG). Dabei ist nach Meinung in der Literatur zwar noch ein Bezug zur Gefahrenvorsorge notwendig, aber keine konkrete Gefahrenlage mehr (vgl. Ritter-Schulte, Die Weiterentwicklung des IT-Sicherheitsgesetzes, Art. 1 Nr. 9 IT-SiG 2.0, Rn. 307). Solche Sicherheitseigenschaften von Produkten können sich auch aus der Struktur des Anbieters ergeben. Da hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI vor dem Einsatz der Produkte warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG).

Die Ereignisse rund um Kaspersky werden vom BSI seit Jahren aufmerksam verfolgt. Mehrere westliche Staaten wie USA und Niederlande warnen seit Jahren öffentlich vor Kaspersky und haben die Software für den Einsatz im Behördenumfeld gesperrt [redacted] Das BSI hat sich aber bislang mit öffentlichen Warnungen zu Kaspersky zurückgehalten.

Der russische Angriff auf die Ukraine, der mit hybriden Mitteln - also auch im Cyberraum - geführt wird und von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt wurde, verändert die Lagebeurteilung. Russland ist kein demokratischer Rechtsstaat und sieht Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als Feind an. Mit feindlichen Übergriffen auf deutsche Institutionen,

Einstufung nach Schwärzung aufgehoben.

Unternehmen und IT-Infrastrukturen ist daher zu rechnen. Russische Unternehmen könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden, zum anderen selbst Ziel massiver Cyberangriffe werden. Die Gefahr, dass Kaspersky in die kriegerischen Auseinandersetzungen hineingezogen wird, ist daher so groß, dass eine Warnung angemessen ist. Es muss damit gerechnet werden, dass Kaspersky nicht mehr die uneingeschränkte Kontrolle über seine Software und IT-Systeme hat bzw. diese in Kürze verlieren wird.

[redacted]

Bereits in den letzten Jahren wurden Fälle bekannt, in denen staatliche Stellen Einfluss auf Kaspersky genommen haben:

[redacted]

In den Jahren 2018 und 2019 wurden russische VPN-Anbieter gezwungen, bestimmte Verbindungen auf Anordnung der Regierung zu blocken. Während die meisten Anbieter die Kooperation verweigerten, kam Kaspersky den Anordnungen nach[2]:

"Although not all VPNs are banned, a 2018 law introduced fines for search engines that brought up results to proxy sites (including VPNs) that would give Russians access to prohibited content or instructions on how to get access to that content.
The following year, VPNs and search engines were compelled to block any websites that appeared on the federal government blacklist. Later, 10 VPN providers were ordered to hand over access to their servers or face being banned. Only one, Kaspersky Lab, which is based in Russia, agreed, while others - like ExpressVPN and NordVPN - shut down their Russian servers."

Neben dem BSI haben auch andere Organisationen ihre Risikobewertung angepasst. Frankreich hat beispielsweise eine vergleichbare Warnung veröffentlicht[3]. [redacted] Die Teilnehmer waren sich einig, dass der Einsatz von Kaspersky-Produkten hoch

1 [redacted]
2 https://www.techradar.com/vpn/which-websites-and-services-are-banned-in-russia
3 https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

problematisch ist. Zum Schutz ihrer IT-Systeme wurden daher automatische Updates abgestellt und Schritte eingeleitet, um die Software schnellstmöglich durch eine sicherere Alternative abzulösen.

Die in der Warnung beschriebenen Angriffsvektoren sind nicht neu. Im Folgenden einige Beispiele, die belegen, welchen Schaden ein Angreifer mit Viren-Schutzsoftware anrichten könnte:

- ✗ Am 10.06.2015 hat Kaspersky selbst in einer Pressemitteilung[4] mitgeteilt, dass das Unternehmensnetzwerk gehackt wurde und Angreifer mit teils neuen Methoden versucht haben, vertrauliche Daten zu stehlen, die dann für Angriffe auf die Kunden missbraucht werden könnten.
- ✗ Am 05. Januar 2012 hat die Hacker-Gruppe „The Lords of Dharmaraja“ geheimen Sourcecode von Symantec bei Pastebin veröffentlicht. Symantec hat die Echtheit des Codes bestätigt und die sicherheitsrelevanten Auswirkungen mit dem BSI-Präsidenten in einem vertraulichen Gespräch erörtert.
- ✗ Alle Hersteller von Viren-Schutzprogrammen hatten in der Vergangenheit Schwachstellen, die für Angriffe auf Kundensysteme hätten genutzt werden können. Mit Kenntnis des Sourcecode oder noch nicht veröffentlichter Schwachstellen wäre ein Angreifer nicht auf offiziell gemeldete Schwachstellen angewiesen, um einen Angriff durchzuführen. Wenn schon Schwachstellen ausreichen, um Systeme komplett stillzulegen, wäre dies mit einer Backdoor noch sehr viel leichter.
- ✗ Es sind zahlreiche Vorfälle bei allen Herstellern von Viren-Schutzsoftware bekannt, in denen eine fehlerhafte Erkennungssignatur Windows-Systemdateien als schädlich klassifiziert und damit das IT-System blockiert hat.
- ✗ Es sind auch Vorfälle bekannt, bei denen nach einem Signaturupdate bestimmte Schadprogramme irrtümlich nicht mehr detektiert wurden.
- ✗ Alle Viren-Schutzprogramme haben Funktionen eingebaut, mit denen sich Schadsoftwareausbrüche begrenzen lassen. Dazu können sie beliebige Dateien blockieren oder löschen. Auch in der Bundesverwaltung hat es bereits einen Sicherheitsvorfall gegeben, bei dem durch eine Fehlbedienung der "Outbreak-Prevention"-Funktion eine ganze Behörde für einen Tag lahmgelegt wurde.
- ✗ Bei Updates werden nicht immer nur Signaturen übertragen. Es ist auch möglich, dass größere Softwarebestandteile (z. B. Scan-Engines) aktualisiert werden müssen, um mit neuen Signaturen/Erkennungsverfahren kompatibel zu bleiben. Dem BSI sind Fälle bekannt, bei denen durch Updates eines Viren-Schutzprogramms neue Funktionen installiert oder Konfigurationen überschrieben wurden, ohne dass die Nutzer dies bemerken konnten. In der Folge wurde Kundendaten ohne Genehmigung an den Hersteller übertragen.

Derartige Vorfälle mussten alle Hersteller bereits vermelden. Sie sind immer unbeabsichtigt aufgrund von Fehlern oder Nachlässigkeiten geschehen. Eigene Entwickler oder Hacker, die in die Systeme des Herstellers eingedrungen sind, sind nicht auf Schwachstellen oder Fehler angewiesen, und könnten daher sehr einfach die folgenden Funktionen auf Kundensystemen implementieren:

- Zielsysteme analysieren (Systemeigenschaften, Hardwareeigenschaften, verwendete Software etc.)
- Daten zum Hersteller übertragen (z. B. Dateien, URLs)
- Dateien sperren oder löschen

Um die gewollten Funktionalität bieten zu können, laufen Viren-Schutzprogramme zudem mit hohen Systemrechten, schützen sich vor Veränderungen und haben Zugriff auf das gesamte Filesystem. Durch die

4 https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig ist, könnten theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Manipulationen lassen sich auch temporär vornehmen und dadurch sehr gut tarnen. Beispielsweise könnte für wenige Stunden ein bestimmter Schadcode bewusst nicht erkannt werden, um anderen Angreifern den Weg zu bereiten.

Wenn die Kaspersky-Produkte für Angriffe entweder durch Anweisung der russischen Regierung oder durch staatliches Eindringen in deren Systeme instrumentalisiert werden, ist es daher möglich, dass auf die Systeme auf denen Kaspersky-Produkte installiert sind, unberechtigt zugegriffen oder Einfluss genommen werden kann.

Kaspersky ist sich dieser Gefahren bewusst und hat in der Vergangenheit diverse Maßnahmen zur Vertrauensbildung ergriffen, die aber alle nicht geeignet sind, die aktuelle Gefahrenlage zu entschärfen.

✗ Kaspersky hat versucht, sich dem Einfluss russischer Behörden zu entziehen und betreibt eine Dateninfrastruktur in zwei Rechenzentren in Zürich zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden aus Europa, den Vereinigten Staaten und Kanada sowie in mehreren asiatisch-pazifischen Ländern. Für die Bereitstellung von Updates/Virensignaturen stehen bei Bedarf verschiedene Server in Europa zur Verfügung, unter anderem in Frankfurt.

  Es ist unerheblich, wo die Kundendaten gehostet werden. Entscheidend ist, wer Sourceodeänderungen vornehmen und Signaturdaten erstellen kann und wie diese qualitätsgesichert und geprüft werden. Kaspersky kann nicht nachweisen, dass diese Prozesse komplett unabhängig vom russischen Hauptquartier durchgeführt werden. Es ist auch nicht transparent, wer administrativen Zugang zu den Systemen in Westeuropa hat. Aufgrund der Erfahrungen mit anderen Cloudanbietern ist es extrem unwahrscheinlich, dass die Rechenzentren in West-Europa komplett autark arbeiten und keine administrativen Eingriffe aus anderen Regionen erfolgen können.

✗ Die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren und Datendienste von Kaspersky wurden von zwei externen, unabhängigen Prüforganisationen bestätigt. Kaspersky hat das SOC-2-Audit (Service Organization Control for Service Organizations) Typ 1 durch einen Big-Four-Auditor erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigte. Darüber hinaus wurden Datendienste vom TÜV AUSTRIA nach ISO/IEC 27001:2013 zertifiziert.

  Eine Zertifizierung sagt nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus. Sie ist keine Garantie für den Ist-Zustand.

✗ Kaspersky sagt über sich selbst, als global agierendes privates Unternehmen (Sitz der Holding ist London, UK) keine Verbindungen zur russischen Regierung zu haben.

  Diese Aussage ist nicht glaubhaft. Kaspersky hat seinen Hauptsitz in Moskau und weist eine russische Eigentümerstruktur auf. Als eines der wichtigsten IT-Security-Unternehmen Russlands arbeitet Kaspersky eng mit Ermittlungsbehörden zusammen (s. o.). Wesentliche Teile der Belegschaft arbeiten daher in Russland oder haben familiäre Bindungen in Russland und sind daher dem direkten Einfluss und Druck der Behörden ausgesetzt.

✗ Kaspersky unterliegt nach eigenen Angaben nicht dem russischen System operativer Ermittlungsmaßnahmen (SORM) oder anderen ähnlichen Gesetzen und sei deswegen nicht zur Auskunftserteilung verpflichtet.

  Diese faktischen Einflussmöglichkeiten der russischen Regierung entfallen nicht deswegen, weil Kaspersky nach russischem Recht keinen Mitwirkungspflichten unterliegt (zu den Pflichten s. Gutachten Prof. Hober). Angesichts des eklatanten Bruchs von internationalem Recht durch Russland muss damit

gerechnet werden, dass faktisch möglicher Einfluss der russischen Regierung auch gegen geltendes russisches Recht ausgeübt werden wird.

Fazit:

Durch manipulierte Viren-Schutzprogramme hat ein Angreifer nahezu unbegrenzte Möglichkeiten, IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste Vorfall öffentlich bekannt wird. Vielmehr ist die Warnung zum jetzigen Zeitpunkt angezeigt, um rechtzeitig präventiv zu handeln und die relevanten Anwender vor potentiellem Schaden zu bewahren. Mildere Mittel zum Schutz der Informationssicherheit sind nicht ersichtlich.

B Vorherige Stellungnahmemöglichkeit nach § 7 Abs. 1 a Nr. 1 BSIG

Kaspersky sollte vor der Veröffentlichung nur mit kurzer Frist informiert und Gelegenheit zur Stellungnahme gegeben werden. Es ist Gefahr im Verzug. Hacker könnten ihre Vorbereitungen bereits abgeschlossen haben und nur noch auf einen Einsatzbefehl warten. Es ist nicht ersichtlich, dass Kaspersky eine Möglichkeit hätte, durch technische oder sonstige Maßnahmen die Risikoeinschätzung positiv zu beeinflussen. Es ist nicht wahrscheinlich, dass der Hersteller an dem zugrunde liegenden strukturellen Sicherheitsproblem etwas ändern kann, da er kaum Einfluss auf die Gefährdung hat. Angesichts der Gefährdungslage erscheint eine kurze Frist daher verhältnismäßig und fachlich angemessen.

C Verfügung

2) BL 23 zur Kenntnis

3) KM zur Mitzeichnung [gez. AL KM 4.3.2002]

4) TK zur Mitzeichnung [gez. AL TK 4.3.2022]

5) OC zur Mitzeichnung [gez. AL OC 4.3.2022]

6) BL zur Mitzeichnung [gez. AL BL 4.3.2022]

7) P/VP z. Billigung [gez. P 4.3.2022]

Im Auftrag

[redacted]

17

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

18

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

19

019_geschwärzt.pdf

Von: Andreas.Koenen@bmi.bund.de
An: Welsch, Günther
Cc: Schönbohm, Arne; Schabhüser, Gerhard; Caspers, Thomas; Samsel, Horst; Häger, Dirk; [redacted] GP Stab 3 - Strategie und Leitungsunterstuetzung; CI3@bmi.bund.de; CI4@bmi.bund.de; CI1@bmi.bund.de; Katja.Papenkort@bmi.bund.de; Andreas.Reisen@bmi.bund.de; Michael Baum; GP Leitungsstab; CI@bmi.bund.de; SVCI@bmi.bund.de; [redacted]@bmi.bund.de; [redacted]@bmi.bund.de
Betreff: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Samstag, 5. März 2022 09:32:30
Anlagen: CDR_Kaspersky_Warnung_V7.odt
CDR_VS-NfD_Kaspersky_Begründung_V7.odt
CDR_VS-NfD_Kaspersky_Begründung_V7.pdf
CDR_Kaspersky_Warnung_V7.pdf
Julia Parser Messages.txt

Lieber Herr Welsch,

vielen Dank für die Einbeziehung meiner Abteilung und des BMI. Wir werden das Thema für den JF am Montag aufnehmen.

Um Ihre Entscheidung in Gänze nachvollziehen zu können, bitte ich um Vorlage aller Informationen, die dieser Entscheidung zugrunde liegen, vor allem auch mit direktem Bezug zur aktuellen Lageentwicklung. Dies betrifft insbesondere auch die von Ihnen zitierte Verschlusssache.

Weiterhin bitte ich um Darstellung, welche weiteren Unternehmen bzw. Produkte auch anderer Produktkategorien ebenfalls betrachtet werden müssten. Hier habe ich vor allem Unternehmen mit signifikanter russischer Anteilseignerschaft im Blick, die im Vergleich zum hier vorliegenden Fall betrachtet werden müssten.

In meiner Abteilung werde ich CI1 um Wahrnehmung des Themas bitten. Dies betrifft insbesondere die rechtliche Würdigung.

Beste Grüße und weiterhin ein schönes Wochenende!

Andreas Könen
Abteilungsleiter CI
Cyber- und Informationssicherheit
Bundesministerium des Innern und für Heimat
Alt-Moabit 140, 10557 Berlin
DEUTSCHLAND

Telefon: +49 30 18681[redacted]
E-Mail: andreas koenen@bmi.bund.de
Internet: www.bmi.bund.de

Es folgt 016_0_geschwärzt.pdf als Zitat.

Die Anhänge sind identisch zu 016.

20

020_geschwärzt.pdf

Von: Häger, Dirk
An: Schönbohm, Arne
Cc: Schabhüser, Gerhard; Welsch, Günther; Caspers, Thomas
Betreff: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Sonntag, 6. März 2022 12:50:05

Hallo Arne,

ich habe in die Fragestellung "welche weiteren Unternehmen bzw. Produkte auch anderer Produktkategorien ebenfalls betrachtet werden müssten" etwas Zeit investiert. Hier mein Ergebnis:

Auf den deutschen und englischen Wikipediaseiten gibt es Auflistungen über russische Softwarefirmen. Eine Durchsicht dieser Firmen ergibt, dass diese in der Regel vor allem für den russischen oder zumindest osteuropäischen Markt tätig sind. Außerdem sind viele dieser Firmen eher Beratungshäuser (Telemedizin, KI, VK-Lösungen). Relevant sind meines Erachtens vor allem Firmen, deren Software einfach gekauft werden kann [redacted]

[redacted]

Ciao Dirk

Ps: Völlig außen vor gelassen habe ich den Smartphone-Markt. Sowohl im Apple- als auch im Google-Appstore gibt es eine Vielzahl an Apps von russischen Entwicklern. Eine Schwachstelle im Betriebssystem voraus gesetzt, könnte auch darüber eine Menge Unheil angerichtet werden. Aber ein Vergleich zur Kaspersky-AV hinkt, denn dort bräuchte es eine solche Schwachstelle nicht: die Software von Kaspersky hat die Recht schon!

Es folgt 019_geschwärzt.pdf als Zitat.

21

021.pdf

Von: Schönbohm, Arne
An: Häger, Dirk
Cc: Caspers, Thomas; Welsch, Günther; Schabhüser, Gerhard
Betreff: AW: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Sonntag, 6. März 2022 14:21:07

Sehr gut vielen Dank. Habe das heute morgen in der BM/ Sts Runde hinsichtlich der möglichen Danktionsliste angesprochen. Gibt hier noch keine Klärung aber Warnung ist etwas anderes - führt aber zum gleichen Ergebnis.

Mit freundlichen Grüßen

Arne Schönbohm

via SecurePIM gesendet

Es folgt 020_geschwärzt.pdf als Zitat.

22

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

23

023_0.pdf

Von: Welsch, Günther
An: GP Abteilung OC; GP Abteilung TK; GP Abteilung BL
Cc: GP Geschaeftszimmer KM; GP Fachbereich KM 1; GP Referat KM 14; GP Stab 3 - Strategie und Leitungsunterstuetzung
Betreff: WG: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 7. März 2022 08:39:00
Dringlichkeit: Hoch

LK,

ich bitte um kurzfristige Zusammenstellung und Übermittlung der in den Abteilungen vorhandenen und der Bewertung der Warnung zugrundeliegenden Informationen an KM14.

Weiterhin bitte ich um Darstellung, welche weiteren Unternehmen bzw. Produkte auch anderer Produktkategorien ebenfalls betrachtet werden müssten. Dirk hatte dazu bereits am Wochenende eine erste Recherche getätigt. Ich bitte auch hierzu um Zulieferung an KM14.

KM14 wird einen Nachbericht an das BMI übermitteln. Es wäre gut, alle Informationen heute im Laufe des Tages zu erhalten. besten Dank!

Viele Grüße
Günther Welsch

Es folgt 019_geschwärzt.pdf als Zitat.

24

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

25

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

26

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

27

027_geschwärzt.pdf

Von: Welsch, Günther
An: "Katja.Papenkort@bmi.bund.de"
Cc: "Caspers, Thomas"
Betreff: Telefonat bez. Warnmeldung
Datum: Montag, 7. März 2022 13:19:00
Dringlichkeit: Hoch

Sehr geehrte Frau Papenkort,

bezugnehmend auf den JF zwischen BMI und Amtsleitung BSI bin ich gerade gebeten worden, mit Ihnen Kontakt aufzunehmen, um das Thema der Kaspersky Warnung zu diskutieren. Ich würde Sie gerne dazu anrufen und Herrn Caspers mit ins Gespräch hinzunehmen. Geben Sie mir ein kurzes Signal, wie ich Sie am besten erreichen kann?

Vielen Dank und Gruß
Günther Welsch

--- --- --- --- --- --- --- ---
Dr. Günther Welsch
Abteilungsleiter KM
Bundesamt für Sicherheit in der Informationstechnik
53175 Bonn

Tel: 0228 9582 [redacted]
Mobil: [redacted]

28

028_geschwärzt.pdf

Von: [redacted]
An: GP Abteilung KM; GP Abteilung BL; GP Abteilung TK; GP Abteilung OC
Cc: Schönbohm, Arne; Schabhüser, Gerhard; GP Stab 1 - Strategische Kommunikation und Presse
Betreff: WG: Kaspersky Viren-Schutzsoftware
Datum: Montag, 7. März 2022 14:06:42
Anlagen: ATT00001.htm
Julia Parser Messages.txt

---

z.K. - zum geplanten vorgehen unserer Nachbarn - soweit ich sehe nichts Neues für uns.

Gruß
[redacted]

im Auftrag
[redacted]
Leiterin Leitungsstab

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Telefonische Erreichbarkeit:
[redacted]

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----
Von [redacted]@bmi.bund.de [redacted]
Gesendet: Montag, 7. März 2022 13:26
An: [redacted]@bsi.bund.de>
Cc: Katja.Papenkort@bmi.bund.de
Betreff: Kaspersky Viren-Schutzsoftware

Liebe [redacted],

Frau Papenkort bat mich Ihnen die folgenden Informationen zuzusenden:

ITA befindet sich derzeit auch noch in der Prüfung, ob sie sich rechtlich verbindlich oder unverbindlich äußern sollen.

NLD hatte sich 2018 zu folgendem Schritt entschieden: Dutch government stops using Kaspersky anti-virus software, warns of security risk<https://www.dutchnews nl/news/2018/05/dutch-government-stops-using-kaspersky-anti-virus-software-warns-of-security-risk/>.

CERT FRA hat einen Bericht<https://www.cert.ssi.gouv fr/cti/CERTFR-2022-CTI-001/> veröffentlicht (unten komplett maschinell übersetzt). Der relevante Part ist der folgende:

VERWENDUNG DIGITALER TOOLS MIT BEZUG ZU RUSSLAND

Im aktuellen Kontext kann die Verwendung bestimmter digitaler Tools, insbesondere der Tools der Firma Kaspersky, aufgrund ihrer Verbindung zu Russland in Frage gestellt werden. Zum gegenwärtigen Zeitpunkt gibt es keinen objektiven Grund, die Bewertung des Qualitätsniveaus der bereitgestellten Produkte und Dienstleistungen zu ändern. Dennoch sollten elementare Vorsichtsmaßnahmen getroffen werden:

Die Trennung von Cybersicherheitstools in einem Kontext von Spannungen im Cyberspace und verschärfter Cyberkriminalität kann die Cybersicherheit Ihrer Organisation erheblich schwächen. Wenn es keine Alternativen gibt, kann eine solche Trennung nicht empfohlen werden.

Die Isolation Russlands auf der internationalen Bühne und das Risiko von Angriffen auf mit Russland verbundene Industrieunternehmen kann die Fähigkeit dieser Unternehmen beeinträchtigen, ihre Produkte und Dienstleistungen zu aktualisieren und damit auf dem neuesten Stand der Technik zu halten, der für den Schutz ihrer Kunden erforderlich ist. Mittelfristig sollte daher eine Strategie zur Diversifizierung der Cybersicherheitslösungen in Betracht gezogen werden.

Komplettübersetzung:

BERICHT ÜBER BEDROHUNGEN UND VORFÄLLE DES CERT-DE

Betrifft: Internationale Spannungen - Cyberbedrohung

VERWALTUNG DES DOKUMENTS

Referenz CERTFR-2022-CTI-001

Titel Internationale Spannungen - Cyberbedrohung

Datum der ersten Version 02. März 2022

Datum der letzten Version 02. März 2022

Quelle(n)

Anlage(n) Keine(r)

Tabelle 1: Verwaltung des Dokuments

Eine detaillierte Versionsverwaltung befindet sich am Ende dieses Dokuments.

Warnung : Das Tempo der militärischen Operationen in der Ukraine sowie die internationalen Reaktionen führen zu sehr schnellen Veränderungen der Situation. Darüber hinaus sind viele der online kursierenden Informationen ungeprüft. Die dargestellten Elemente sollten nicht als erschöpfend betrachtet werden und können zum Zeitpunkt der Lektüre veraltet sein. ANSSI wird sich bemühen, diesen Abschnitt regelmäßig zu aktualisieren, wenn sich die Lage ändert.

Die aktuellen internationalen Spannungen, die durch die russische Invasion in der Ukraine verursacht werden, gehen mit Auswirkungen im Cyberspace einher. Während die Kämpfe in der Ukraine hauptsächlich konventionell ausgetragen werden, stellt das ANSSI den Einsatz von Cyberangriffen im Rahmen des Konflikts fest. In einem grenzenlosen digitalen Raum können diese Cyberangriffe französische Einrichtungen betreffen, und es ist ratsam, dies zu antizipieren und sich darauf vorzubereiten, ohne in Panik zu verfallen. Um die Wahrscheinlichkeit solcher Ereignisse zu minimieren und ihre Auswirkungen zu begrenzen, teilt die ANSSI bewährte Sicherheitspraktiken und Informationen über die Bedrohung und fordert alle Akteure auf, diese zu nutzen. Zu diesem Zweck werden in diesem Bulletin die für den Cyberbereich relevanten Elemente im

Zusammenhang mit dem aktuellen Kontext zentralisiert und verbreitet, um die Stärkung des Schutzniveaus aller französischen Einrichtungen zu fördern. Er wird regelmäßig aktualisiert.

BEDROHUNGSLAGE

Seit dem 23. Februar 2022, dem Tag vor dem Beginn der russischen Militäroperation in der Ukraine, wurden recht unterschiedliche Cyberangriffe festgestellt:

DDoS-Angriffe (Distributed Denial of Service), die sich insbesondere gegen die Websites von Regierungseinrichtungen, aber auch von ukrainischen Banken gerichtet haben sollen. Hacker-Gruppen, von denen einige dem Aufruf der ukrainischen Regierung folgten, führten ebenfalls DDoS-Angriffe auf russische Ziele durch;

Verunstaltungen von Webseiten in der Ukraine, Russland und Weißrussland ;

Es wurde auch von Versuchen berichtet, in E-Mail-Nachrichten mit gezieltem Phishing gegen ukrainische Institutionen oder Streitkräfte einzudringen ;

Cyberangriffe mit bösartigem Sabotagecode (Wiper) wurden identifiziert. Diesen Aktionen, die am zerstörerischsten sind, scheinen manchmal Datenexfiltrationen vorausgegangen zu sein.

Die Auswirkungen dieser Cyberangriffe sind derzeit noch begrenzt.

Schließlich hat sich ein Teil des russischsprachigen cyberkriminellen Ökosystems in dem aktuellen Konflikt positioniert, wobei die cyberkriminelle Gruppe Conti beispielsweise die russische Regierung unterstützt. Andere Gruppen erklärten jedoch, dass sie neutral blieben und sich nur auf ihre lukrativen Ziele konzentrierten. Schließlich erklärten Cyberkriminelle, dass sie kritische russische Infrastrukturen ins Visier nehmen wollen und können. Diese Spaltung des cyberkriminellen Ökosystems in Verbindung mit möglichen Mitnahmeeffekten mahnt zur Vorsicht bei Cyberangriffen, die nicht zu schnell als eine im Rahmen des Konflikts in Auftrag gegebene Aktion interpretiert werden sollten.

BEWÄHRTE VERFAHREN

Prioritäre präventive Cyber-Maßnahmen :

https://www.ssi.gouv fr/uploads/2022/02/20220226_mesures-cyber-preventives-prioritaires.pdf

Krisenkommunikation :

https://www.ssi.gouv fr/uploads/2021/12/anssi-guide-communication_crise_cyber.pdf

Krisenmanagement :

https://www.ssi.gouv fr/uploads/2021/12/anssi-guide-gestion_crise_cyber.pdf

VERWENDUNG DIGITALER TOOLS MIT BEZUG ZU RUSSLAND

Im aktuellen Kontext kann die Verwendung bestimmter digitaler Tools, insbesondere der Tools der Firma Kaspersky, aufgrund ihrer Verbindung zu Russland in Frage gestellt werden. Zum gegenwärtigen Zeitpunkt gibt es keinen objektiven Grund, die Bewertung des Qualitätsniveaus der bereitgestellten Produkte und Dienstleistungen zu ändern. Dennoch sollten elementare Vorsichtsmaßnahmen getroffen werden:

Die Trennung von Cybersicherheitstools in einem Kontext von Spannungen im Cyberspace und verschärfter Cyberkriminalität kann die Cybersicherheit Ihrer Organisation erheblich schwächen. Wenn es keine Alternativen gibt, kann eine solche Trennung nicht empfohlen werden.

Die Isolation Russlands auf der internationalen Bühne und das Risiko von Angriffen auf mit Russland verbundene Industrieunternehmen kann die Fähigkeit dieser Unternehmen beeinträchtigen, ihre Produkte und Dienstleistungen zu aktualisieren und damit auf dem neuesten Stand der Technik zu halten, der für den Schutz ihrer Kunden erforderlich ist. Mittelfristig sollte daher eine Strategie zur Diversifizierung der Cybersicherheitslösungen in Betracht gezogen werden.

TECHNISCHE ELEMENTE

Haftungsausschluss: Die vom ANSSI freigegebenen Marker stammen aus offen zugänglichen Quellen und sollen technisches Grundwissen im Zusammenhang mit der Bedrohung vermitteln und zu Erkennungs- und Schutzzwecken verwendet werden. Sie wurden vom ANSSI einer ersten Qualifizierung unterzogen, sollten aber dennoch mit Vorsicht behandelt werden. Diese Liste ist nicht erschöpfend und wird regelmäßig aktualisiert, wenn sich die Situation ändert.

Beste Grüße

[redacted]

[redacted] _

[redacted] | CI 1 [redacted] / Mobil [redacted]

29

029_geschwärzt.pdf

Von: Welsch, Günther
An: Samsel, Horst
Cc: Schabhüser, Gerhard; [redacted] "Caspers, Thomas"
Betreff: Kaspersky Warnung
Datum: Montag, 7. März 2022 16:08:00
Dringlichkeit: Hoch

Hallo Horst,

gerade ist es mir gelungen, Frau Papenkort zu erreichen. Sie gibt sich deutlich fest in der Überzeugung, dass die von uns vorgetragenen Sachverhalte zur Situation des Herstellers zu sehr aus der Vergangenheit stammen. Um rechtlich ausreichend die Warnung zu begründen, müssen/sollen wir auf die jetzige Situation mit Russland intensiv eingehen. Die grundsätzlich geänderte Situation soll die Begründung zur Warnung geben und deutlich machen, warum zu einem früheren Zeitpunkt keine Warnung notwendig gewesen sei (z.B. im letzten Jahr und davor). Mein Einwand, dass wir dieses bereits aufgeschrieben hätten und das Wertvolle insbesondere die auf fachliche Gründe gestützte Argumentation sei, zieht bei Ihr nicht. Sie möchte gerne die politisch-rechtliche Argumentation seitens BL vertieft haben. Ich habe angeregt, dass Ihr beide dann telefoniert. Leider hat sie jetzt erst einmal keine Zeit, würde sich dann aber später telefonisch bei Dir melden. Ich habe angeboten, um keine Zeit zu verlieren, mit BL23 schon einmal zu telefonieren, was ich dann auch gleich tun werde.

Mit freundlichen Grüßen,
Dr. Günther Welsch

--- --- --- --- --- --- --- ---

Dr. Günther Welsch
Abteilungsleiter KM
Bundesamt für Sicherheit in der Informationstechnik
53175 Bonn

Tel: 0228 9582 [redacted]
Mobil: [redacted]

30

030_0_geschwärzt.pdf

Von: Welsch, Günther
An: Schabhüser, Gerhard; Schönbohm, Arne
Cc: [redacted]; "Caspers, Thomas"; Samsel, Horst; [redacted]
Betreff: Warnung vor Kaspersky. Ergebnis des Abstimmung mit CI1
Datum: Montag, 7. März 2022 17:56:00
Anlagen: VS-NfD_Kaspersky_Begründung_V6_ErgSR.odt
VS-NfD_Kaspersky_Begründung_V6_ErgSR (002).pdf
Dringlichkeit: Hoch

VS-NfD

Hallo Herr Schönbohm, hallo Gerd,

gerade konnten wir uns in einer Telko mit Frau Dr. Papenkort darauf verständigen, dass die von uns erweiterte Begründung nun Grundlage für die Hausleitungsbefassung im BMI wird (siehe Anlage). Frau Dr. Papenkort meinte vorbehaltlich noch einer intensiveren Prüfung, dass die Begründung nun ausreichen könnte. Die Entscheidung soll bei St E getroffen werden, eine Beteiligung des AA angestrebt werden. Die Vorlage an die Hausleitung würde heute Abend noch auf den Weg gebracht. Ob unsere Eilbedürftigkeit seitens BMI geteilt wird, bin ich mir nicht sicher. Eine Entscheidung heute Abend oder morgen am Feiertag in Berlin ist nicht gesichert. Eine Publikation der Warnung vor der Sitzung des Innenausschusses wird kaum zu realisieren sein. Frau Dr. Papenkort wird ab Mittwoch im Rheinland sein, ggf. steht sie auch persönlich für weitere Klärungen vor Ort zur Verfügung.

Viele Grüße
Günther Welsch

030_1_VS-NfD_Kaspersky_Begründung_V6_ErgSR_geschwärzt.pdf

Einstufung nach Schwärzung aufgehoben.

Referat KM 14 02. 03. 2021

Az. KM14-210 01 03 / VS-NfD

[redacted]

Betr. Bewertung von IT-Sicherheitsprodukten
hier: Warnung vor Kaspersky-Produkten nach § 7 BSIG

Bezug

Anlagen Entwurf Warntext

1) Vermerk zur Begründung der Warnung

A Begründung der Warnung nach § 7 Abs. 1 BSIG

Das BSI darf nach § 7 Abs. 1 BSIG u.a. vor Sicherheitslücken in informationstechnischen Produkten und Diensten öffentlich warnen. Sicherheitslücken in diesem Sinne sind nach § 2 Abs. 6 BSIG *„Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.“* Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1.d BSIG). Dabei ist nach Meinung in der Literatur zwar noch ein Bezug zur Gefahrenvorsorge notwendig, aber keine konkrete Gefahrenlage mehr (vgl. Ritter-*Schulte,* Die Weiterentwicklung des IT-Sicherheitsgesetzes, Art. 1 Nr. 9 IT-SiG 2.0, Rn. 307). Solche Sicherheitseigenschaften von Produkten können sich auch aus der Struktur des Anbieters ergeben. Da hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI vor dem Einsatz des Produktes warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG).

Die Ereignisse rund um Kaspersky werden vom BSI seit Jahren aufmerksam verfolgt. Mehrere westliche Staaten wie USA und Niederlande warnen seit Jahren öffentlich vor Kaspersky und haben die Software für den Einsatz im Behördenumfeld gesperrt [redacted] Das BSI hat sich aber bislang mit öffentlichen Warnungen zu Kaspersky zurückgehalten.

Der russische Angriff auf die Ukraine, der mit hybriden Mitteln - also auch im Cyberraum - geführt wird und von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt wurde, verändert die Lagebeurteilung. Russland ist kein demokratischer Rechtsstaat und sieht Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als Feind an. Mit feindlichen Übergriffen auf deutsche Institutionen,

Einstufung nach Schwärzung aufgehoben.

Unternehmen und IT-Infrastrukturen ist daher zu rechnen. Russische Unternehmen könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden, zum anderen selbst Ziel massiver Cyberangriffe werden. Die Gefahr, dass Kaspersky in die kriegerischen Auseinandersetzungen hineingezogen wird, ist daher so groß, dass eine Warnung angemessen ist. Es muss damit gerechnet werden, dass Kaspersky nicht mehr die uneingeschränkte Kontrolle über seine Software und IT-Systeme hat bzw. diese in Kürze verlieren wird.

[redacted]

Bereits in den letzten Jahren wurden Fälle bekannt, in denen staatliche Stellen Einfluss auf Kaspersky genommen haben:

[redacted]

In den Jahren 2018 und 2019 wurden russische VPN-Anbieter gezwungen, bestimmte Verbindungen auf Anordnung der Regierung zu blocken. Während die meisten Anbieter die Kooperation verweigerten, kam Kaspersky den Anordnungen nach[2]:

"Although not all VPNs are banned, a 2018 law introduced fines for search engines that brought up results to proxy sites (including VPNs) that would give Russians access to prohibited content or instructions on how to get access to that content.
The following year, VPNs and search engines were compelled to block any websites that appeared on the federal government blacklist. Later, 10 VPN providers were ordered to hand over access to their servers or face being banned. Only one, Kaspersky Lab, which is based in Russia, agreed, while others - like ExpressVPN and NordVPN - shut down their Russian servers."

Neben dem BSI haben auch andere Organisationen ihre Risikobewertung angepasst. Frankreich hat beispielsweise eine vergleichbare Warnung veröffentlicht[3]. [redacted] Die Teilnehmer waren sich einig, dass der Einsatz von Kaspersky-Produkten hoch

1 [redacted]
2 https://www.techradar.com/vpn/which-websites-and-services-are-banned-in-russia
3 https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

problematisch ist. Zum Schutz ihrer IT-Systeme wurden daher automatische Updates abgestellt und Schritte eingeleitet, um die Software schnellstmöglich durch eine sicherere Alternative abzulösen.

Die in der Warnung beschriebenen Angriffsvektoren sind nicht neu. Im Folgenden einige Beispiele, die belegen, welchen Schaden ein Angreifer mit Viren-Schutzsoftware anrichten könnte:

- ✗ Am 10.06.2015 hat Kaspersky selbst in einer Pressemitteilung[4] mitgeteilt, dass das Unternehmensnetzwerk gehackt wurde und Angreifer mit teils neuen Methoden versucht haben, vertrauliche Daten zu stehlen, die dann für Angriffe auf die Kunden missbraucht werden könnten.
- ✗ Am 05. Januar 2012 hat die Hacker-Gruppe „The Lords of Dharmaraja“ geheimen Sourcecode von Symantec bei Pastebin veröffentlicht. Symantec hat die Echtheit des Codes bestätigt und die sicherheitsrelevanten Auswirkungen mit dem BSI-Präsidenten in einem vertraulichen Gespräch erörtert.
- ✗ Alle Hersteller von Viren-Schutzprogrammen hatten in der Vergangenheit Schwachstellen, die für Angriffe auf Kundensysteme hätten genutzt werden können. Mit Kenntnis des Sourcecode oder noch nicht veröffentlichter Schwachstellen wäre eine Angreifer nicht auf offiziell gemeldete Schwachstellen angewiesen, um einen Angriff durchzuführen. Wenn schon Schwachstellen ausreichen, um Systeme komplett stillzulegen, wäre dies mit einer Backdoor noch sehr viel leichter.
- ✗ Es sind zahlreiche Vorfälle bei allen Herstellern von Viren-Schutzsoftware bekannt, in denen eine fehlerhafte Erkennungssignatur Windows-Systemdateien als schädlich klassifiziert und damit das IT-System blockiert hat.
- ✗ Es sind auch Vorfälle bekannt, bei denen nach einem Signaturupdate bestimmte Schadprogramme irrtümlich nicht mehr detektiert wurden.
- ✗ Alle Viren-Schutzprogramme haben Funktionen eingebaut, mit denen sich Schadsoftwareausbrüche begrenzen lassen. Dazu können sie beliebige Dateien blockieren oder löschen. Auch in der Bundesverwaltung hat es bereits einen Sicherheitsvorfall gegeben, bei dem durch eine Fehlbedienung der "Outbreak-Prevention"-Funktion eine ganze Behörde für einen Tag lahmgelegt wurde.
- ✗ Bei Updates werden nicht immer nur Signaturen übertragen. Es ist auch möglich, dass größere Softwarebestandteile (z. B. Scan-Engines) aktualisiert werden müssen, um mit neuen Signaturen/Erkennungsverfahren kompatibel zu bleiben. Dem BSI sind Fälle bekannt, bei denen durch Updates eines Viren-Schutzprogramms neue Funktionen installiert oder Konfigurationen überschrieben wurden, ohne dass die Nutzer dies bemerken konnten. In der Folge wurde Kundendaten ohne Genehmigung an den Hersteller übertragen.

Derartige Vorfälle mussten alle Hersteller bereits vermelden. Sie sind immer unbeabsichtigt aufgrund von Fehlern oder Nachlässigkeiten geschehen. Eigene Entwickler oder Hacker, die in die Systeme des Herstellers eingedrungen sind, sind nicht auf Schwachstellen oder Fehler angewiesen, und könnten daher sehr einfach die folgenden Funktionen auf Kundensystemen implementieren:

- Zielsysteme analysieren (Systemeigenschaften, Hardwareeigenschaften, verwendete Software etc.)
- Daten zum Hersteller übertragen (z. B. Dateien, URLs)
- Dateien sperren oder löschen

Um die gewollten Funktionalität bieten zu können, laufen Viren-Schutzprogramme zudem mit hohen Systemrechten, schützen sich vor Veränderungen und haben Zugriff auf das gesamte Filesystem. Durch die

4 https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig ist, könnten theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Manipulationen lassen sich auch temporär vornehmen und dadurch sehr gut tarnen. Beispielsweise könnte für wenige Stunden ein bestimmter Schadcode bewusst nicht erkannt werden, um anderen Angreifern den Weg zu bereiten.

Wenn die Kaspersky-Produkte für Angriffe entweder durch Anweisung der russischen Regierung oder durch staatliches Eindringen in deren Systeme instrumentalisiert werden, ist es daher möglich, dass auf die Systeme auf denen Kaspersky-Produkte installiert sind, unberechtigt zugegriffen oder Einfluss genommen werden kann.

Kaspersky ist sich dieser Gefahren bewusst und hat in der Vergangenheit diverse Maßnahmen zur Vertrauensbildung ergriffen, die aber alle nicht geeignet sind, die aktuelle Gefahrenlage zu entschärfen.

✗ Kaspersky hat versucht, sich dem Einfluss russischer Behörden zu entziehen und betreibt eine Dateninfrastruktur in zwei Rechenzentren in Zürich zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden aus Europa, den Vereinigten Staaten und Kanada sowie in mehreren asiatisch-pazifischen Ländern. Für die Bereitstellung von Updates/Virensignaturen stehen bei Bedarf verschiedene Server in Europa zur Verfügung, unter anderem in Frankfurt.

  Es ist unerheblich, wo die Kundendaten gehostet werden. Entscheidend ist, wer Sourceodeänderungen vornehmen und Signaturdaten erstellen kann und wie diese qualitätsgesichert und geprüft werden. Kaspersky kann nicht nachweisen, dass diese Prozesse komplett unabhängig vom russischen Hauptquartier durchgeführt werden. Es ist auch nicht transparent, wer administrativen Zugang zu den Systemen in Westeuropa hat. Aufgrund der Erfahrungen mit anderen Cloudanbietern ist es extrem unwahrscheinlich, dass die Rechenzentren in West-Europa komplett autark arbeiten und keine administrativen Eingriffe aus anderen Regionen erfolgen können.

✗ Die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren und Datendienste von Kaspersky wurden von zwei externen, unabhängigen Prüforganisationen bestätigt. Kaspersky hat das SOC-2-Audit (Service Organization Control for Service Organizations) Typ 1 durch einen Big-Four-Auditor erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigte. Darüber hinaus wurden Datendienste vom TÜV AUSTRIA nach ISO/IEC 27001:2013 zertifiziert.

  Eine Zertifizierung sagt nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus. Sie ist keine Garantie für den Ist-Zustand.

✗ Kaspersky sagt über sich selbst, als global agierendes privates Unternehmen (Sitz der Holding ist London, UK) keine Verbindungen zur russischen Regierung zu haben.

  Diese Aussage ist nicht glaubhaft. Kaspersky hat seinen Hauptsitz in Moskau und weist eine russische Eigentümerstruktur auf. Als eines der wichtigsten IT-Security-Unternehmen Russlands arbeitet Kaspersky eng mit Ermittlungsbehörden zusammen (s. o.). Wesentliche Teile der Belegschaft arbeiten daher in Russland oder haben familiäre Bindungen in Russland und sind daher dem direkten Einfluss und Druck der Behörden ausgesetzt.

✗ Kaspersky unterliegt nach eigenen Angaben nicht dem russischen System operativer Ermittlungsmaßnahmen (SORM) oder anderen ähnlichen Gesetzen und sei deswegen nicht zur Auskunftserteilung verpflichtet.

  Diese faktischen Einflussmöglichkeiten der russischen Regierung entfallen nicht deswegen, weil Kaspersky nach russischem Recht keinen Mitwirkungspflichten unterliegt (zu den Pflichten s. Gutachten Prof. Hober). Angesichts des eklatanten Bruchs von internationalem Recht durch Russland muss damit

Einstufung nach Schwärzung aufgehoben.

gerechnet werden, dass faktisch möglicher Einfluss der russischen Regierung auch gegen geltendes russisches Recht ausgeübt werden wird. Soweit das BSI die Maßnahmen von Kaspersky in der Vergangenheit für ausreichend hielt, um die Produkte von Kaspersky weiter einsetzen zu können, lag dem die Annahme zu Grunde, dass die russische Regierung keine Schritte einleiten würde, die bei Bekanntwerden (bzw. Entdeckung) sowohl Kaspersky als auch der russischen Regierung wirtschaftlichen und Reputationsschaden zufügen würden. Angesichts der nunmehr offenen Konfrontation Russlands mit der EU und den NATO-Staaten und der Hinnahme selbst existenzvernichtender Sanktionen für russische Unternehmen, kann diese Grundannahme nicht weiter aufrechterhalten werden. Wir gehen jetzt davon aus, dass die russische Regierung jetzt keine Rücksicht mehr auf das internationale Geschäft und die Reputation von Kaspersky nehmen würde. [redacted]

✗

Fazit:

Durch manipulierte Viren-Schutzprogramme hat ein Angreifer nahezu unbegrenzte Möglichkeiten, IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste Vorfall öffentlich bekannt wird. Vielmehr ist die Warnung zum jetzigen Zeitpunkt angezeigt, um rechtzeitig präventiv zu handeln und die relevanten Anwender vor potentiellem Schaden zu bewahren. Mildere Mittel zum Schutz der Informationssicherheit sind nicht ersichtlich.

B Vorherige Stellungnahmemöglichkeit nach § 7 Abs. 1 a Nr. 1 BSIG

Kaspersky sollte vor der Veröffentlichung nur mit kurzer Frist informiert und Gelegenheit zur Stellungnahme gegeben werden. Es ist Gefahr im Verzug. Hacker könnten ihre Vorbereitungen bereits abgeschlossen haben und nur noch auf einen Einsatzbefehl warten. Es ist nicht ersichtlich, dass Kaspersky eine Möglichkeit hätte, durch technische oder sonstige Maßnahmen die Risikoeinschätzung positiv zu beeinflussen. Es ist nicht wahrscheinlich, dass der Hersteller an dem zugrunde liegenden strukturellen Sicherheitsproblem etwas ändern kann, da er kaum Einfluss auf die Gefährdung hat. Angesichts der Gefährdungslage erscheint eine kurze Frist daher verhältnismäßig und fachlich angemessen.

C Verfügung

2) BL 23 zur Kenntnis

3) KM zur Mitzeichnung [MZ. AL KM vom 3.3.2002]

4) TK zur Mitzeichnung

5) OC zur Mitzeichnung

6) BL zur Mitzeichnung

7) P/VP z. Billigung

Einstufung nach Schwärzung aufgehoben.

Im Auftrag

[redacted]

31

031_0_geschwärzt.pdf

Von:	GP Abteilung KM
An:	Schönbohm, Arne; Schabhüser, Gerhard
Cc:	GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer_KM; GP Referat KM 14; GP Abteilung KM
Betreff:	WG: 0348_22 Erlass CI 1 - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Montag, 7. März 2022 19:03:51
Anlagen:	Bericht_zu_Erlass_0348_22_CI1.docx

Hallo Herr Schönbohm, hallo Gerd,

KM14 hat noch den Nachbericht zu den Fragen von AL CI erstellt, den ich hiermit zur Freigabe vorlege. Da morgen Feiertag in Berlin ist, reicht sicherlich eine Versendung morgen im Laufe des Tages. Nach Erteilung der Freigabe veranlasse ich dann die Finalisierung und Versendung.

Viele Grüße
Günther Welsch

-----Ursprüngliche Nachricht-----
Von: GP Poststelle <poststelle@bsi.bund.de>
Gesendet: Montag, 7. März 2022 12:39
An: GP Abteilung KM <abteilung-km@bsi.bund.de>
Cc: GP Geschaeftszimmer_KM <geschaeftszimmer-km@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>
Betreff: 0348_22 Erlass CI 1 - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware

Liebe Kolleginnen und Kollegen,

FF: KM
Btg: -
Aktion: Bitte um Informationen
Frist: -

Für Rückfragen stehe ich Ihnen gerne zur Verfügung.

Vielen Dank und freundliche Grüße,

[redacted]

Referat Z 23 - Innerer Dienst
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 -189
53175 Bonn
Telefon:+49 228 99 9582[redacted]
Fax:+49[redacted]
E-Mail:[redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----
Von: [redacted]@bsi.bund.de>
Gesendet: Montag, 7. März 2022 12:33

An: GP Poststelle <poststelle@bsi.bund.de>
Cc: GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; [redacted]@bsi.bund.de>; GP Fachbereich KM 1 <fachbereich-km1@bsi.bund.de>
Betreff: WG: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware

Hallo,

bitte in den Geschäftsgang aufnehmen. Ich brauche möglichst schnell eine Erlassnummer. FF ist bei KM.

Viele Grüße

[redacted]

Es folgt 019_geschwärzt.pdf als Zitat.

031_1_Bericht_zu_Erlass_0348_22_CI1_geschwärzt.pdf

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Bundesministerium des Innern,
für Bau und Heimat
CI 1
Alt-Moabit 140
10557 Berlin

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. [redacted]
Fax [redacted]

referat-km14@bsi.bund.de,

www.bsi.bund.de

De-Mail-Adresse:
poststelle@bsi-bund.de-mail.de

Betreff: Weitergehende Informationen zu russischen IT-Unternehmen

Bezug: Entwurf zur § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware vom 05.03.2022
Geschäftszeichen: KM14-210 01 03
Berichterstatter: [redacted]
Datum: 14.04.2022
Seite 1 von 1

Mit Bezugserlass vom 07.03.2022 bat CI (1) um Vorlage weiterer Informationen zur aktuellen Lageentwicklung inkl. VS-Informationen und (2) um Darstellung, welche weiteren Unternehmen bzw. Produkte auch anderer Produktkategorien ebenfalls betrachtet werden müssten. Dazu berichte ich wie folgt.

(1) VS- und Lageinformationen

[redacted]

(2) IKT-Unternehmen mit russischem Anteilsbesitz

Grundsätzliche Fragen

Um die Sicherheit einer IT-Lieferkette beurteilen zu können, müssen zu jedem IT-Produkt die folgenden Fragen geklärt werden:

1. *Wer nimmt Einfluss auf die Geschäftspolitik des Herstellers und das operative Geschäft?*

Neben Unternehmen mit russischem Anteilsbesitz müssen für die aktuelle Lageeinschätzung auch russische Unternehmen berücksichtigt werden, welche ihre Produkte z. B. über Onlinevertriebswege anbieten, ohne jedoch ein Büro oder eine Niederlassung in Deutschland zu haben. Relevant könnten auch Unternehmen sein, die über russisches Fremdkapital (Kredite) – aber nicht Eigenkapital (i.e.S. Anteilsbesitz) finanziert sind oder deren Geschäftstätigkeiten einen starken russischen Bezug haben und so entsprechender Einflussnahme ausgesetzt sein könnten.

Hinweis: Häufig wird GData aus Bochum aufgrund einer russischen Investorin als „kritisch“ angesehen. Die Geschäftsführung von GData hat jedoch glaubhaft versichert, dass die Investorin keinen Einfluss auf das operative Geschäft oder den Sourcecode nehmen kann. Anders muss der Hersteller Kaspersky beurteilt werden. Kaspersky wird von einer Holding in London geführt, der Hauptsitz ist aber nach wie vor in Moskau. Auch alle Führungspersonen haben russischen Hintergrund, sodass russische Behörden mannigfaltige Einflussmöglichkeiten auf wesentliche Teile der Unternehmensführung und die Produktentwicklung haben.

2. Welche Funktionalitäten hat das IT-Produkt?

Um zu analysieren, welche Gefahren von einem bestimmten IT-Produkt ausgehen könnten, müssen seine Funktionen sowie die Implementierung analysiert werden. Bei Software sind z. B. Viren-Schutzprogramme besonders kritisch, weil sie Root-Rechte haben, auf alle Dateien zugreifen können und mehrfach am Tag aktualisiert werden. Eine Software mit beschränkten Rechten ohne Internetzugriff bietet eine sehr viel kleinere Angriffsfläche.

3. Wer kann Einfluss auf den Sourcecode bzw. eine IT-Komponente/ Hardware und die Erstellung von Updates nehmen?

Eine Gefahr kann von Unternehmen ausgehen, die in nennenswertem Umfang Mitarbeiter (Leitung, Programmierer etc.) in/aus Russland beschäftigen. Bei Hardware müsste geprüft werden, wo Einzelteile produziert werden, wo die Endmontage stattfindet und ob Teile beim Transport manipuliert werden könnten.

Recherchen des BSI

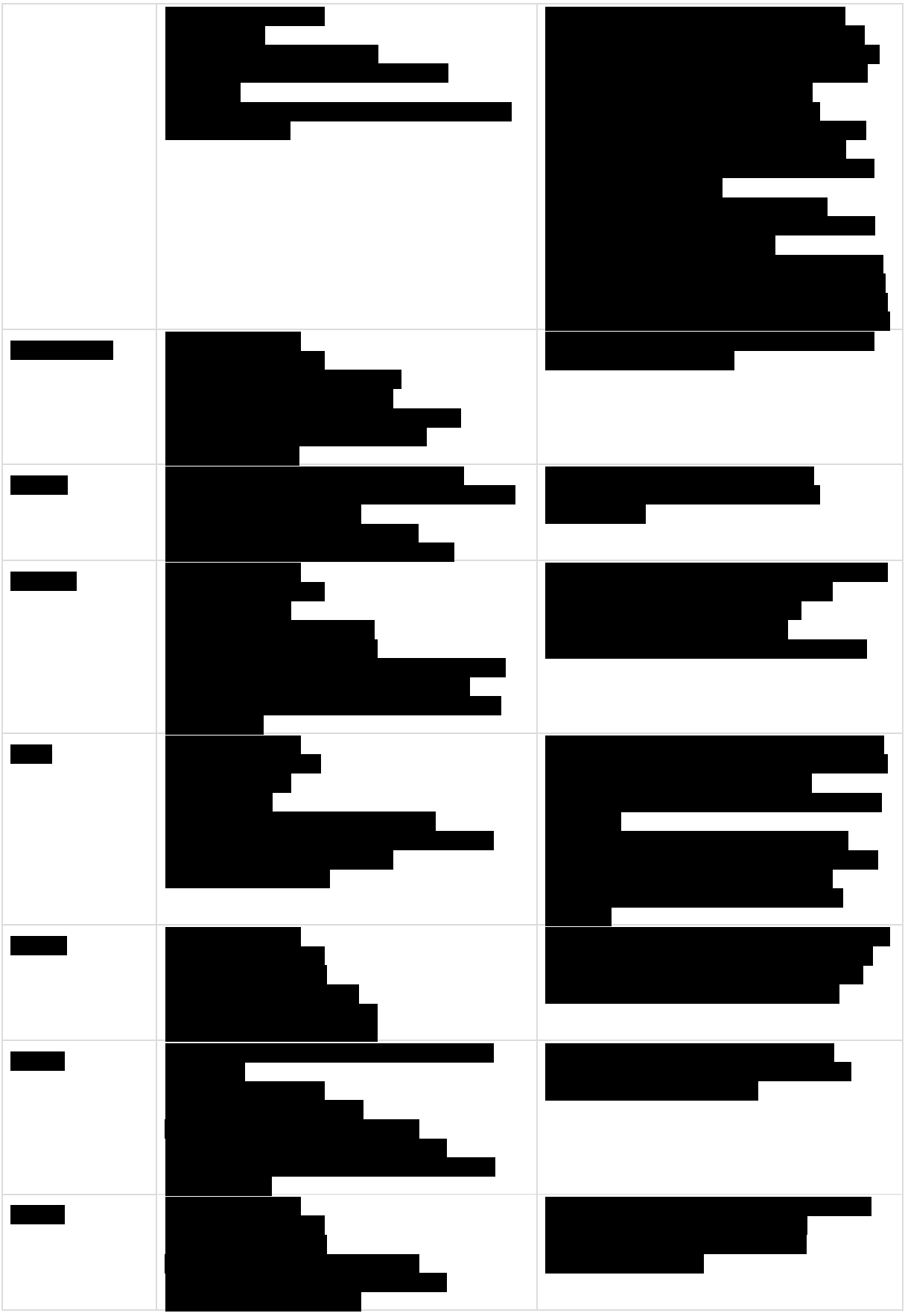
Anfragen innerhalb des BSI [redacted] haben ergeben, dass niemandem eine Liste potenziell kritischer IT-Produkte vorliegt. Grundsätzlich ist es nicht möglich, durch eine Massenabfrage in den gängigen Recherchetools IKT-Unternehmen auf das Merkmal der Nationalität eines Anteilseigners hin zu suchen bzw. nach diesem Merkmal zu filtern. Weiterhin sind die zur Verfügung stehenden Informationen zu Unternehmen aus Russland sehr lückenhaft, sofern auf diese überhaupt zugegriffen werden kann. Bei einigen - und insbesondere größeren Unternehmen- handelt es sich zudem mitunter um

verschachtelte Holdinggesellschaften, bei denen die Anteilseigner letztendlich ohne großen Aufwand oder der Beteiligung von ND-Quellen nicht zurückzuverfolgen sind. Schließlich deuten auch vermeintlich einfache Indikatoren wie russische Namen von Anteilseignern keinesfalls gesichert auf die Nationalität einer Person hin – oder umgekehrt.

Eine Recherche der Abteilung SZ beim Statistischen Bundesamt (destatis) hat ergeben, dass es in Deutschland im Jahr 2018 insgesamt 114.209 Unternehmen aus dem Bereich der Informations- und Telekommunikationstechnik mit russischem Anteilsbesitz gab.

Eine systematische Analyse aller in DE aktiven IKT-Unternehmen in Bezug auf russische Anteilseigner bzw. maßgeblichen russischem Einfluss ist daher nicht möglich. Folgende Unternehmen wurden durch eine unsystematische und offene Ad-hoc-Webrecherche ermittelt, wobei eine Validierung der Daten häufig nicht möglich war.

Unternehmen	Überblick	Einschätzung
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



Bundesamt
für Sicherheit in der
Informationstechnik

Einstufung nach Schwärzung aufgehoben.

Deutschland
Digital·Sicher·BSI·

Weitere Maßnahmen

Aufgrund der aktuell vorliegenden Erkenntnisse ergibt sich nicht die Notwendigkeit, vor anderen Unternehmen außer Kaspersky konkret zu warnen.

Große deutsche Konzerne lassen zur Sicherstellung ihrer Lieferkette pro Jahr mehr als 100 potenzielle Partner im Rahmen eines Audits individuell überprüfen, um mögliche Risiken zu bewerten. Um Ressourcen zu sparen, nutzen einige DAX-Unternehmen und verlangen von möglichen Partnern ein erfolgreiches Audit, bevor sie in eine geschäftliche Beziehung eintreten. Für die meisten Behörden ist der Aufwand für individuelle Überprüfungen und Audits zu hoch. Es sollte daher überlegt werden, über einen Rahmenvertrag eine entsprechende Dienstleistung zentral bereitzustellen und ein Repository für die öffentliche Verwaltung aufzubauen.

Im Auftrag

Dr. Günther Welsch

32

032_geschwärzt.pdf

Von: Welsch, Günther
An: Schabhüser, Gerhard; Schönbohm, Arne; [redacted] "Caspers, Thomas"; Samsel, Horst; [redacted]"; Häger, Dirk
Betreff: AW: Warnung vor Kaspersky. Ergebnis des Abstimmung mit CI1
Datum: Montag, 7. März 2022 19:23:00

LK:

Mit Blick auf den Entschließungsantrag ist es doch sogar mehr als erwünscht, dass wir als BSI eine Warnung aussprechen! Das ist doch schon mehr als ein Weckruf des Parlaments, unser Mandat und Verantwortung wahrzunehmen! Wann, wenn nicht jetzt, ist der richtige Zeitpunkt für eine akute Warnung! Wir dürfen nicht warten, bis der Schaden auch noch eintritt. Das ist nicht das, was man von uns erwarten darf, wenn man Russland mit Angriffen auf digitale Infrastrukturen im Rahmen der Kriegsführung attributieren muss.

Inhalt des Entschließungsantrages mit BSI-Bezug:
• Der Deutsche Bundestag stellt fest: „Gezielt lancierte Desinformationen **und Angriffe auf digitale Infrastrukturen, auch und gerade solche aus dem Bereich der kritischen Infrastrukturen sind integraler Teil der russischen Kriegsführung**. Der Bundestag verurteilt solche auch und gerade auf zivile Infrastrukturen abzielende Praktiken auf das Schärfste.“ (S. 2)
• Der Deutsche Bundestag begrüßt „dass die Bundesregierung der ukrainischen Regierung frühzeitig Unterstützung durch deutsche Expertinnen und Experten bei der Analyse und Abwehr hybrider Bedrohungen zugesagt und entsprechende Kapazitäten bereitgestellt hat.“ (S. 3)
• Der Deutsche Bundestag fordert die Bundesregierung **auf „für einen möglichst effektiven Schutz kritischer Infrastrukturen sowie der Abwehr von Spionage und Sabotage** Abwehrmaßnahmen über bestehende Koordinierungsgremien, sowohl auf bundesdeutscher wie europäischer Ebene, zu intensivieren sowie potentiell betroffene Betreiber und Unternehmen **insbesondere durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zu beraten und nötigenfalls zu unterstützen…**

-----Ursprüngliche Nachricht-----
Von: Welsch, Günther
Gesendet: Montag, 7. März 2022 17:56
An: Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>
Cc [redacted]@bsi.bund.de>; 'Caspers, Thomas' <thomas.caspers@bsi.bund.de>; Samsel, Horst <horst.samsel@bsi.bund.de>; [redacted]@bsi.bund.de>
Betreff: Warnung vor Kaspersky. Ergebnis des Abstimmung mit CI1
Priorität: Hoch

VS-NfD

Hallo Herr Schönbohm, hallo Gerd,

gerade konnten wir uns in einer Telko mit Frau Dr. Papenkort darauf verständigen, dass die von uns erweiterte Begründung nun Grundlage für die Hausleitungsbefassung im BMI wird (siehe Anlage). Frau Dr. Papenkort meinte vorbehaltlich noch einer intensiveren Prüfung, dass die

Begründung nun ausreichen könnte. Die Entscheidung soll bei St E getroffen werden, eine Beteiligung des AA angestrebt werden. Die Vorlage an die Hausleitung würde heute Abend noch auf den Weg gebracht. Ob unsere Eilbedürftigkeit seitens BMI geteilt wird, bin ich mir nicht sicher. Eine Entscheidung heute Abend oder morgen am Feiertag in Berlin ist nicht gesichert. Eine Publikation der Warnung vor der Sitzung des Innenausschusses wird kaum zu realisieren sein. Frau Dr. Papenkort wird ab Mittwoch im Rheinland sein, ggf. steht sie auch persönlich für weitere Klärungen vor Ort zur Verfügung.

Viele Grüße
Günther Welsch

33

033_0_geschwärzt.pdf

Von: Schabhüser, Gerhard
An: GP Abteilung KM; Schönbohm, Arne
Cc: GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer KM; GP Referat KM 14
Betreff: AW: 0348_22 Erlass CI 1 - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 7. März 2022 19:40:13

Beim Überfliegen ist mir aufgefallen, dass in der Tabelle an einer Stelle "Information von OC 3" stand. Auch an anderen Stellen wurde auf Aktionen von z.B. von SZ verwiesen.

Wir differenzieren doch in einem Bericht das BSI nicht nach Herkunft der Info im BSI, oder?

Das sollten wir anpassen.

Ich würde auch die explizite Würdigung GDATA vs Kaspersky herausnehmen. Kasperky ist ja gesondert betrachtet worden.

Ansonsten aus meiner Sicht ok

shbr

_____
Vizepräsident
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: gerhard.schabhueser@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Es folgt 031_0_geschwärzt.pdf als Zitat.

34

034_0_geschwärzt.pdf

Von: GP-Referat-KM-14
An: Schabhüser-Gerhard
Cc: Welsch-Günther
Betreff: AW: 0348 22 Erlass CI 1 § 7 BSIG Warnung des BSI vor Kaspersky Viren Schutzsoftware
Datum: Montag, 7. März 2022 19:49:53

Hallo Herr Schabhüser,

GData hatte ich reingenommen, weil Herr Schönbohm GData am Freitag erwähnte und als potenziell gefährlich eingestuft hatte. Da die russische Investorin die Ex-Frau von Eugene Kaspersky ist und GData früher einmal eine Scan-Engine von Kaspersky eingesetzt hat, müssen sich die Bochumer seit Jahren immer wieder gegen Misstrauen zur Wehr setzen. Ich wollte GData damit einen Gefallen tun und den Kollateralschaden für sie begrenzen.

Viele Grüße

[redacted]

Es folgt 033_geschwärzt.pdf als Zitat.

35

035_0.pdf

Von:	Schönbohm, Arne
An:	GP Abteilung KM; Schabhüser, Gerhard
Cc:	GP Referat KM 14; GP Abteilung KM; GP Geschaeftszimmer_KM; GP Stab 3 - Strategie und Leitungsunterstuetzung
Betreff:	AW: WG: 0348_22 Erlass CI 1 - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Dienstag, 8. März 2022 04:02:47

Lieber Herr Dr. Welsch vielen Dank für den Nachbericht. Gerade beim ersten Punkt - die VS-Informationen - wurden nicht im JF besprochen, da dies nicht eine entsprechend gesicherte Verbindung war.

Mit freundlichen Grüßen

Arne Schönbohm

- via SecurePIM gesendet -

Es folgt 031_0_geschwärzt.pdf als Zitat.

36

036_1.pdf

Von: GP Abteilung KM
An: GP Geschaeftszimmer KM
Cc: GP Referat KM 14; GP Fachbereich KM 1
Betreff: WG: WG: 0348_22 Erlass CI 1 - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Dienstag, 8. März 2022 10:20:00
Anlagen: Bericht_zu_Erlass_0348_22_CI1_final.docx
Dringlichkeit: Hoch

---

1) Schlusszeichnung des noch etwas sprachlich angepassten Erlassberichts
2) GeschKM: Bitte finalisieren und versenden.

Dr. Welsch

Es folgt 035.pdf als Zitat.

036_2_geschwärzt.pdf

Von:	GP Geschaeftszimmer_KM
An:	CI1@bmi.bund.de
Cc:	GP Abteilung KM; GP Referat KM 14; GP Fachbereich KM 1; GP Poststelle; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer_KM
Betreff:	0348_22 Erlass CI 1 - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Dienstag, 8. März 2022 11:06:33
Anlagen:	Bericht_zu_Erlass_0348_22_CI1.pdf

Sehr geehrte Damen und Herren,

anbei sende ich Ihnen den Bericht zu o. a. Erlass.

Mit freundlichem Gruß
Im Auftrag
[redacted]

Bundesamt für Sicherheit in der Informationstechnik
Geschäftszimmer KM
Godesberger Allee 185 – 189
53175 Bonn
Telefon: +49 228 99 9582[redacted]
Mobil: +49 [redacted]
E-Mail: geschaeftszimmer-km@bsi.bund.de

Es folgt 019_geschwärzt.pdf als Zitat.

036_Bericht_zu_Erlass_0348_22_CI1_geschwärzt.pdf

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Bundesministerium des Innern
und für Heimat
CI 1
Alt-Moabit 140
10557 Berlin

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +[redacted]
Fax +[redacted]

referat-km14@bsi.bund.de,

www.bsi.bund.de

De-Mail-Adresse:
poststelle@bsi-bund.de-mail.de

Betreff: 0348_22 Weitergehende Informationen zu russischen IT-Unternehmen

Bezug: Entwurf zur § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware vom 05.03.2022
Geschäftszeichen: KM14-210 01 03
Berichterstatter [redacted]
Datum: 08.03.2022
Seite 1 von 5

Mit Bezugserlass vom 07.03.2022 bat CI (1) um Vorlage weiterer Informationen zur aktuellen Lageentwicklung inkl. VS-Informationen und (2) um Darstellung, welche weiteren Unternehmen bzw. Produkte auch anderer Produktkategorien ebenfalls betrachtet werden müssten. Dazu berichten wir wie folgt.

(1) VS- und Lageinformationen

[redacted]

(2) IKT-Unternehmen mit russischem Anteilsbesitz

Grundsätzliche Fragen

Um die Sicherheit einer IT-Lieferkette beurteilen zu können, müssen zu jedem IT-Produkt die folgenden Fragen geklärt werden:

1. *Wer nimmt Einfluss auf die Geschäftspolitik des Herstellers und das operative Geschäft?*

Neben Unternehmen mit russischem Anteilsbesitz müssen für die aktuelle Lageeinschätzung auch russische Unternehmen berücksichtigt werden, welche ihre Produkte z. B. über Onlinevertriebswege anbieten, ohne jedoch ein Büro oder eine Niederlassung in Deutschland zu haben. Relevant könnten auch Unternehmen sein, die über russisches Fremdkapital (Kredite) – aber nicht Eigenkapital (i.e.S. Anteilsbesitz) finanziert sind oder deren Geschäftstätigkeiten einen starken russischen Bezug haben und so entsprechender Einflussnahme ausgesetzt sein könnten.

Hinweis: Häufig wird GData aus Bochum aufgrund einer russischen Investorin als „kritisch“ angesehen. Die Geschäftsführung von GData hat jedoch glaubhaft versichert, dass die Investorin keinen Einfluss auf das operative Geschäft oder den Sourcecode nehmen kann.

2. Welche Funktionalitäten hat das IT-Produkt?

Um zu analysieren, welche Gefahren von einem bestimmten IT-Produkt ausgehen könnten, müssen seine Funktionen sowie die Implementierung analysiert werden. Bei Software sind z. B. Viren-Schutzprogramme besonders kritisch, weil sie Root-Rechte haben, auf alle Dateien zugreifen können und mehrfach am Tag aktualisiert werden. Eine Software mit beschränkten Rechten ohne Internetzugriff bietet eine sehr viel kleinere Angriffsfläche.

3. Wer kann Einfluss auf den Sourcecode bzw. eine IT-Komponente/ Hardware und die Erstellung von Updates nehmen?

Eine Gefahr kann von Unternehmen ausgehen, die in nennenswertem Umfang Mitarbeiter (Leitung, Programmierer etc.) in/aus Russland beschäftigen. Bei Hardware müsste geprüft werden, wo Einzelteile produziert werden, wo die Endmontage stattfindet und ob Teile beim Transport manipuliert werden könnten.

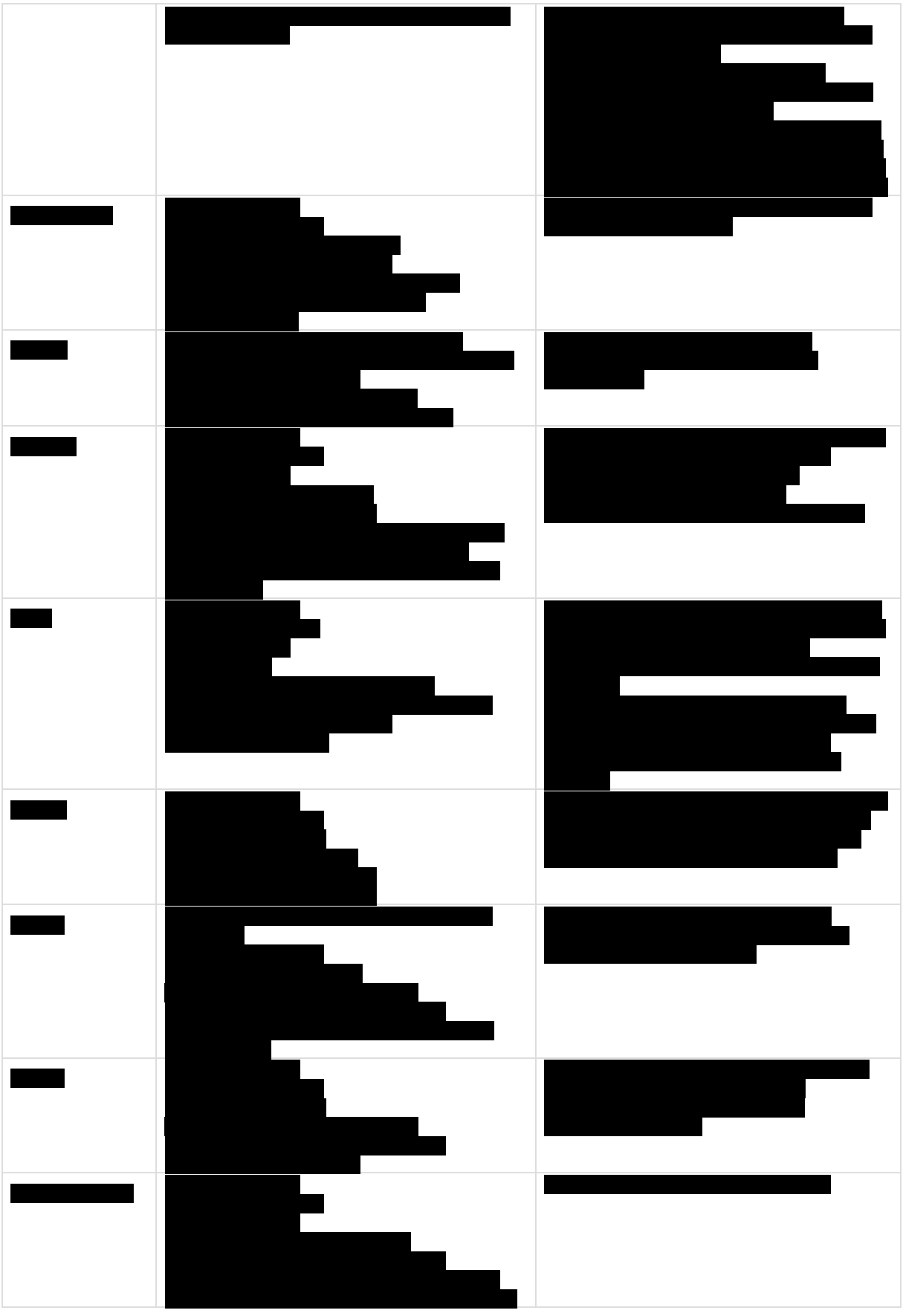
Recherchen des BSI

Anfragen innerhalb des BSI[redacted] haben ergeben, dass keiner der genannten Organisationen eine Liste potenziell kritischer IT-Produkte vorliegt. Grundsätzlich ist es nicht möglich, durch eine Massenabfrage in den gängigen Recherchetools IKT-Unternehmen auf das Merkmal der Nationalität eines Anteilseigners hin zu suchen bzw. nach diesem Merkmal zu filtern. Bedauerlicherweise sind die zur Verfügung stehenden Informationen zu Unternehmen aus Russland sehr lückenhaft, sofern auf diese überhaupt zugegriffen werden kann. Bei einigen - und insbesondere größeren Unternehmen- handelt es sich zudem mitunter um verschachtelte Holdinggesellschaften, bei denen die Anteilseigner letztendlich nicht ohne großen Aufwand oder der Beteiligung von ND-Quellen zurückzuverfolgen sind. Schließlich deuten auch vermeintlich einfache Indikatoren wie russische Namen von Anteilseignern keinesfalls gesichert auf die Nationalität einer Person hin – oder umgekehrt.

Eine Recherche beim Statistischen Bundesamt (destatis) hat ergeben, dass es in Deutschland im Jahr 2018 insgesamt 114.209 Unternehmen aus dem Bereich der Informations- und Telekommunikationstechnik mit russischem Anteilsbesitz gab.

Eine systematische Analyse aller in DE aktiven IKT-Unternehmen in Bezug auf russische Anteilseigner bzw. maßgeblichen russischem Einfluss ist daher nicht möglich. Das BSI hat auf Basis einer Ad-hoc Recherche öffentlich zugänglicher Quellen im Internet Unternehmen mit Bezug zu Russland ermittelt. Die so gewonnenen Daten stellen eine erste Sichtung dar und haben somit keinen Anspruch auf Vollständigkeit und Validität.

Unternehmen	Überblick	Einschätzung
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]



Weitere Maßnahmen und Anregungen

1. Aufgrund der aktuell vorliegenden Erkenntnisse ergibt sich derzeit keine Notwendigkeit, vor IT-Produkten anderer Unternehmen außer den Viren-Schutzprogrammen des Unternehmens Kaspersky zu warnen.
2. [redacted]
3. Aufbau eines Lieferantenverzeichnisses im Sinne der Lieferkettensicherheit. Große deutsche Konzerne lassen zur Sicherstellung ihrer Lieferkette pro Jahr mehr als 100 potenzielle Partner im Rahmen eines Audits individuell überprüfen, um mögliche Risiken zu bewerten. Um Ressourcen zu sparen, nutzen einige DAX-Unternehmen [redacted] und verlangen von möglichen Partnern ein erfolgreiches Audit, bevor sie in eine geschäftliche Beziehung eintreten. Für die meisten Behörden ist der Aufwand für individuelle Überprüfungen und Audits von Lieferanten zu hoch. Es sollte daher überlegt werden, über einen Rahmenvertrag eine entsprechende Dienstleistung zentral bereitzustellen und ein Verzeichnis für die öffentliche Verwaltung aufzubauen.

Im Auftrag

elektr. gez.

Dr. Günther Welsch

37

037_0_geschwärzt.pdf

Von:	GP Referat BL 22
An:	GP Leitungsbuero
Cc:	GP Abteilung BL; GP Fachbereich BL 2; GP Referat BL 22; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Referat BL 21; GP Abteilung OC; GP Abteilung KM; GP Leitungsstab
Betreff:	WG: [VS-NfD] [Terminvorbereitung] WG: 5. Sitzung des Ausschusses für Inneres und Heimat am Mittwoch, dem 9. März 2022, 16.00 Uhr - Sondersitzung - Bitte um Vorbereitung
Datum:	Dienstag, 8. März 2022 14:25:00
Anlagen:	TO der 5. Sitzung des Ausschusses für Inneres und Heimat am Mittwoch dem 9. März 2022 16.00 Uhr - Sondersitzung.msg Anlage_2_WP_20_Mitglieder_Ausschuss für Inneres und Heimat.pdf Anlage_3_VS-NfD_20220308_BSI_Tägliche_Lage_UKR.pdf Anlage_4_DER_SPIEGEL_Bundesregierung Cyberangriff auf deutsche »Hochwertziele« könnte schon bald starten.pdf Anlage_5_Bericht_zu_Erlass_0348_22_CI1_Weitergehende Informationen zu russischen IT-Unternehmen.pdf 20220309_Kontextinformationen_Mitglieder_Ausschuss f. Inneres und Heimat_v.1.1.docx 20220309_Terminuebersicht_Sondersitzung_Innenausschuss_V1.0.docx Anlage_1_Tagesordnung_5. Sitzung_Sondersitzung_09.03.2022.pdf Anlage_6_VS-NfD_Kaspersky_Begründung_V6_ErgSR.pdf Anlage_7_Kaspersky_Warnung_V7.pdf VS-NFD_Sprechzettel IT-Sicherheitslage_Sondersitzung_Innenausschuss.docx

---

An:
Leitungsbüro zwV.

Über:
AL KM z.K. (wg. Kaspersky Produkten)
AL OC z.K. (wg. Lage Ukraine)
RL'in BL21 z.K. (wg. Bezug Sicherheitsbehörden)
LLS / Stab 3 z.K.
AL BL z.K.
FBL BL2 z.K.
RL BL22 z.M. [JW, 08.03.]

Anbei erhalten Sie die Terminvorbereitung für die Teilnahme von P an der morgigen Sondersitzung des Innenausschusses.

Begleitung: [redacted]

Frist finale Unterlagen: 08.03.2022, 12:00 Uhr

Hinweise:
1) Wegen heutigem Feiertag in Berlin:
- Einlassort: Genauer Einlassort am Bundestagsgebäude wird am morgigen Mittwochvormittag durch BL22/Leitungsbüro geklärt und übermittelt.
- Sitzungscharakter: Die Sitzung ist nach bisherigem Wissensstand zwar nicht-öffentlich, aber auch nicht eingestuft. BL22 wird letzteren Punkt abschließend klären und P informieren.

2) Aktualisierung der Unterlagen: Morgen Vormittag wird BL22 eine aktualisierten VS-NfD-Lagebericht zuliefern.

3) Kaspersky Produkte:
- Da es nicht ausgeschlossen ist, dass einige Abgeordnete zu Kaspersky Produkten fragen, wurde dieser Punkt unter "reaktiv" aufgenommen [redacted]

4) [redacted]

Bei Rückfragen stehe ich gerne zur Verfügung.

Mit besten Grüßen
[redacted]

[redacted]

Referat BL 22
Strategien und neue Ansätze der Informationssicherheit
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 -189
53175 Bonn
Telefon: +49(0)22899 9582[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----
Von: GP Leitungsbuero
Gesendet: Freitag, 4. März 2022 14:35
An: GP Abteilung BL <abteilung-bl@bsi.bund.de>; GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Fachbereich OC 2 <fachbereich-oc2@bsi.bund.de>
Cc: GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; GP Leitungsbuero <leitungsbuero@bsi.bund.de>
Betreff: 5. Sitzung des Ausschusses für Inneres und Heimat am Mittwoch, dem 9. März 2022, 16.00 Uhr - Sondersitzung - Bitte um Vorbereitung

Liebe Kolleginnen und Kollegen,

für den o.g. Termin benötigen wir Ihre Unterstützung in Form von Vorbereitung und Begleitung sowie Nachbereitung (Protokoll und Aussteuerung).

Datum: 09.03.2022 – 16:00 - 18:00 Uhr
Ort: Reichstagsgebäude, Raum 3 S 001
(Fraktionssitzungssaal der SPD)
Platz der Republik 1, 11011 Berlin

Beteiligte Institution:
Initiator (Anfragender): BMI (siehe beigefügte Mail)
Initiale Themen: siehe beigefügte Tagesordnung

Kontext:
FF: BL
Btg: OC

PR/ÖA: -

Abgabe-Fristen – bitte beachten:
Vorbereitungstermin: Termin am 07.03.2022 um 13:30 Uhr
Frist finale Unterlagen: 08.03.2022- 12:00 Uhr
Nennung der Begleitung:
Protokoll und Aussteuerung:

Wichtige Informationen:

- Bitte benutzen Sie die aktuellen Checklisten und Vorlagen aus dem Intranet:
http://intranet.bsi.de/Amtsleitung/Organisatorisches/index.html

Bei Fragen zur Terminorganisation können Sie sich gerne per E-Mail an leitungsbuero@bsi.bund.de wenden, bei inhaltliche Rückfragen senden Sie bitte eine E-Mail an stab3@bsi.bund.de .

Vielen Dank!

Viele Grüße
[redacted]

Leiterin Leitungsbüro
Bundesamt für Sicherheit in der Informationstechnik (BSI)

Telefon: +49 228 99 9582[redacted]
Mobil: +49 [redacted]

#DeutschlandDigitalSicherBSI

Die Anlagen 1,2,3,4 sind im Rahmen der IFG-Anfrage nicht relevant.
Anlage 5 ist 036_Bericht_zu_Erlass_0348_22_CI1_geschwärzt.pdf
Anlage 6 ist 030_1_VS-NfD_Kaspersky_Begründung_V6_ErgSR_geschwärzt.pdf

037_1_Anlage_7_Kaspersky_Warnung_V7.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

Viren-Schutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Viren-Schutzsoftware 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. Viren-Schutzsoftware 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.

Die Bedrohungssituation durch offensive Cyber-Operationen von russischer Seite führen in der aktuellen Lage zu einer neuen Risikobewertung. Ein russischer IT-Hersteller kann selbst entsprechende 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 Viren-Schutzsoftware 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 Interesse des Staates, 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 Viren-Schutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Viren-Schutzsoftware 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 Viren-Schutzsoftware) 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/DasBSI/Gesetz/gesetz_node.html
[2] Darstellung Risikostufen
https://www.cert-bund.de/risk

037_2_VS-NFD_Sprechzettel IT-Sicherheitslage_Sondersitzung_Innenausschuss_geschwärzt.pdf

Einstufung nach Schwärzung aufgehoben.

FF OE:BL22 Beteiligte OE: OC33, KM14 Stand: 07.03.2022

5. Sitzung des Ausschusses für Inneres und Heimat – Sondersitzung
Teilnahme P BSI
Reichstagsgebäude, Raum 3 S 001 (Fraktionssitzungssaal der SPD)
09.03.2022, 16.00-18.00 Uhr

Begleitung: [redacted]

- Sprechzettel -

I. Aktiver Part

1. [redacted]

Einstufung nach Schwärzung aufgehoben.

[redacted]

- [redacted]

[redacted]

Einstufung nach Schwärzung aufgehoben.

[redacted]

Einstufung nach Schwärzung aufgehoben.

[redacted]

II. Reaktiver Part

2. *TOP* 2: *Kaspersky Produkte* (siehe Anlage_5_Bericht_zu_Erlass_0348_22_CI1_Weitergehende Informationen zu russischen IT-Unternehmen; Anlage_6_VS-NfD_Kaspersky_Begründung_V6_ErgSR; Anlage_7_Kaspersky_Warnung_V7)

Kernbotschaften:

- Viren-Schutzsoftware des Unternehmens Kaspersky sollte geordnet durch alternative Produkte ersetzt werden.
- Unternehmen und Behörden mit besonderen Sicherheitsinteressen/Rahmenbedingungen und Einrichtungen Kritischer Infrastrukturen sind in besonderem Maß gefährdet.
- Kaspersky ist in der Branche ein hoch angesehenes Unternehmen. Es ist aber wahrscheinlich, dass das Hauptquartier in Moskau von Hackern oder staatlichen Sondereinheiten gewaltsam übernommen wird.

Sprechpunkte reaktiv:

1. Grundlage für die BSI-Warnung

§ 7 Abs. 1 BSIG:
a) Warnung vor Sicherheitslücken in informationstechnischen Produkten und Diensten
d) Information der Öffentlichkeit über sicherheitsrelevante IT-Eigenschaften von Produkten.

Sicherheitslücken (nach § 2 Abs. 6 BSIG) „Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können."

***2.* Warum Warnung vor Kaspersky?**

- Viren-Schutzprogramme sind für einen sicheren IT-Betrieb unerlässlich und müssen einwandfrei funktionieren. Sie haben hohe Systemberechtigungen, können auf alle Dateien zugreifen, greifen über das Internet auf Daten des Herstellers zu und werden regelmäßig aktualisiert.
- Kaspersky hat seinen Hauptsitz in Moskau. Entscheidend ist, dass der russische Staat Druck auf Mitarbeiter ausüben kann, die Einfluss auf den Sourcecode und die Signaturerstellung haben.
- Es ist daher unerheblich, dass Kundendaten in der Schweiz gehostet werden und eine Holding in London gegründet wurde. Es ist auch unerheblich, dass Kaspersky in der Vergangenheit auditiert wurde. Der IST-Zustand kann kurzfristig geändert werden.

***3.* Gibt es noch andere betroffene Firmen?**

- Zurzeit wird nur Kaspersky kritisch gesehen. [redacted] eine vergleichbare Software, spielt in Deutschland aber keine Rolle.
- GData ist ein deutsches Unternehmen mit russischer Beteiligung. Die Investoren haben aber keine Möglichkeit, den Einbau von Backdoors oder die Manipulation von Erkennungssignaturen durchzusetzen.
- Letztendlich muss sich jeder IT-Betreiber selbst um die Sicherheit seiner Lieferkette kümmern. In diesem Fall kommt es auf technisches und politisches Verständnis an. Es sind keine ND-Informationen erforderlich.

4. [redacted]

Einstufung nach Schwärzung aufgehoben.

3. [redacted]

- [redacted]
- [redacted]
- [redacted]

38

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

39

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

40

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

41

041_geschwärzt.pdf

Von: GP Referat KM 14
An: GP Fachbereich KM 1; [redacted]; GP Abteilung KM; Häger, Dirk; Caspers, Thomas
Betreff: WG: WG: Anfragen unserer Kunden und Partner zum BSI
Datum: Donnerstag, 10. März 2022 10:04:41
Anlagen: image001.png

Kaspersky möchte damit werben, dass das BSI nicht warnt.

Von: Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>
Gesendet: Donnerstag, 10. März 2022 08:24
An: Lagezentrum, BSI <lagezentrum@bsi.bund.de>; [redacted]@bsi.bund.de>; GP Fachbereich OC 2 <fachbereich-oc2@bsi.bund.de>
Cc: GP Referat KM 14 <referat-km14@bsi.bund.de>; GP Fachbereich WG 2 <fachbereich-wg2@bsi.bund.de>; GP Abteilung WG <abteilung-wg@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>
Betreff: AW: WG: Anfragen unserer Kunden und Partner zum BSI

Glaube leider gar nicht antwortem.

Mit freundlichen Grüßen

Arne Schönbohm

- via SecurePIM gesendet -

Am 10. März 2022 07:57, hat [redacted] geschrieben:

Guten Morgen [redacted],

wie gehen wir mit unten stehender Anfrage von Kaspersky um?

Viele Grüße
[redacted]

Referatsleiterin

_____
Referat WG 21 - Kooperation mit Herstellern und Dienstleistern
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 -189
53175 Bonn
Telefon: +49 228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Von: [redacted]@kaspersky.com>
Gesendet: Donnerstag, 10. März 2022 06:46
An: [redacted]@bsi.bund.de>
Betreff: Anfragen unserer Kunden und Partner zum BSI
Priorität: Hoch

[redacted],

Ich hoffe, es geht Ihnen gut. Ich habe eine Frage. Wir erhalten zunehmend mehr Anfragen von Kunden, warum es – im Gegensatz zu 2018 - keine Stellungnahmen des BSI zur Sicherheit von Kaspersky gibt. Wir können diese Frage natürlich nicht beantworten, das steht und auch nicht zu. Meine Kollegen haben mich aber gebeten, eine kurze Formulierung für den unmittelbaren Dialog mit Kunden und Partnern hierzu zu formulieren, damit sie in Gesprächen/Telefonaten und 1-zu-1 E-Mail-Austausch eine geeignete Botschaft aussenden können.

Ich habe hierzu folgenden Text entworfen:

Kaspersky hat höchstes Vertrauen in das BSI. Die BSI ist eine kompetente, international anerkannte und hervorragend vernetzte technisch-wissenschaftliche Cybersicherheits-Behörde. Bisher hat das BSI unserer Einschätzung nach Entscheidungen immer sehr sorgfältig und verantwortungsbewusst abgewogen und faktenbasierte, nachvollziehbare Entscheidungen zur Stärkung der Cybersicherheit getroffen.
[redacted] steht mit dem BSI im Kontakt und stellt dem Bundesamt transparent Informationen zu Kaspersky sowie den technischen und organisatorischen Abläufe unseres Konzerns zur Verfügung.

Ist es aus Sicht des BSI okay, wenn wir eine solche Antwort geben? Oder haben Sie Vorschläge für Änderungen? Ich bedanke mich für Ihre Antwort. **Wir werden nur dann eine Aussage treffen, wenn aus Sicht des BSI nichts dagegen spricht.**

Beste Grüße
[redacted]

[redacted] Kaspersky

[redacted]
Despag-Straße 3, 85055 Ingolstadt, Germany | www.kaspersky.com | https://www.kaspersky.com/about/policy-blog
Kaspersky Labs GmbH - Ingolstadt - Geschäftsführer: Tanguy Le Bescond de Coatpont - Amtsgericht Ingolstadt: HRB 3527

42

042_0_geschwärzt.pdf

Von: GP Geschaeftszimmer_KM
An: CI1@bmi.bund.de
Cc: GP Abteilung KM; GP Fachbereich KM 1; GP Referat KM 14; GP Poststelle; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Abteilung TK; GP Abteilung WG; Schabhüser, Gerhard
Betreff: Nachgang 1 zu 0360_22 Erlass CI 1 - Kaspersky Viren-Schutzsoftware
Datum: Donnerstag, 10. März 2022 12:51:37
Anlagen: Nachgang 1_zu_Erlass_0360_22_CI1.pdf

Sehr geehrte Damen und Herren,

anbei sende ich Ihnen den Bericht zu o. a. Erlass.

Mit freundlichem Gruß
Im Auftrag
[redacted]

Bundesamt für Sicherheit in der Informationstechnik
Geschäftszimmer KM
Godesberger Allee 185 – 189
53175 Bonn
Telefon: +49 228 99 9582[redacted]
Mobil: [redacted]
E-Mail: geschaeftszimmer-km@bsi.bund.de

Von: [redacted]@bmi.bund.de [redacted]@bmi.bund.de>
Gesendet: Mittwoch, 9. März 2022 18:44
An: GP Poststelle <poststelle@bsi.bund.de>
Cc: CI1@bmi.bund.de; [redacted]@bmi.bund.de; [redacted]@bmi.bund.de
Betreff: Frist 10.03.22 - Erlass: Kaspersky Viren-Schutzsoftware

Bundesministerium
des Innern und für Heimat

CI1-20403/14#7

Sehr geehrte Damen und Herren,

ich bitte um Beantwortung folgender drei Fragen bis 10.03.2022 12 Uhr.

. Welche Erkenntnisse liegen vor, die eine Warnung substantiieren und zu mehr Rechtssicherheit führen könnten?
. Welche IT-Sicherheitsfolgen hätte eine Warnung für DEU? Hierzu: Gibt es alternative Produkte zu Kaspersky?
. Mit welchen wirtschaftlichen Folgen und Gegenreaktionen wäre zu rechnen?

Mit freundlichen Grüßen!

[redacted]

Bundesministerium des Innern und für Heimat
Alt-Moabit 140, 10557 Berlin
Raum B 3.259

Referat CI 1 - Grundsatz; Cyber- und Informationssicherheit

Tel.: +49 30 / 18 681 [redacted]
Mobil: [redacted]
eM@il: [redacted]@BMI.Bund.de<mailto:[redacted]@BMI.Bund.de>

042_1_Nachgang
1_zu_Erlass_0360_22_CI1_geschwärzt.pdf

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Bundesministerium des Innern
und für Heimat
CI 1
Alt-Moabit 140
10557 Berlin

[redacted]
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +49 228 99 9582[redacted]
Fax +49 228 99 10 9582[redacted]

referat-km14@bsi.bund.de,

www.bsi.bund.de

De-Mail-Adresse:
poststelle@bsi-bund.de-mail.de

Betreff: Software von Kaspersky

Bezüge:

1. Nachgang 1 zu Erlass 0360_22 CI1 vom 09.03.3022, Az. CI1-20403/14#7
2. Entwurf zur § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware vom 05.03.2022

Geschäftszeichen: KM14-210 01 03/VS-NfD
Berichterstatter [redacted]
Datum: 10.03.2022

Mit Nachgang 1 vom 09.03.2022 bat CI 1 um Antwort auf die folgenden Fragen:

(1) Welche Erkenntnisse liegen vor, die eine Warnung substantiieren und zu mehr Rechtssicherheit führen könnten?
(2) Welche IT-Sicherheitsfolgen hätte eine Warnung für DEU? Hierzu: Gibt es alternative Produkte zu Kaspersky?
(3) Mit welchen wirtschaftlichen Folgen und Gegenreaktionen wäre zu rechnen?

Dazu berichte ich wie folgt:

(1) Erkenntnisse

Die Übermittlung der angefragten Geheiminformationen wird separat behandelt.

Unabhängig davon erachten wir die Argumentation für die Warnung nach § 7 BSIG für ausreichend und schlüssig begründet.

[redacted]

(2) IT-Sicherheitsfolgen einer Warnung

Eine BSI-Warnung erhöht signifikant das Bewusstsein für potenziell möglichen Gefährdungen, die sich mit dem Einsatz der Software in der aktuellen politischen Lage ergeben.

Software von Kaspersky hat einen sehr guten Ruf und ist im Consumermarkt relativ weit verbreitet. Auch im Enterprise-Bereich ist Software von Kaspersky verbreitet – entweder als alleiniges Produkt bei KMU (i.d.R. Endpoint Protection) oder als Teil einer Multi-Vendor-Strategie auch in großen Unternehmen. Sie wird daher mutmaßlich in allen KRITIS-Sektoren Deutschlands eingesetzt.

Im Consumerbereich gibt es eine Vielzahl an alternativen Viren-Schutzprogrammen, die z. T. sogar kostenlos sind. Windows selbst bringt ein ausreichendes Schutzprogramm mit, das nach der Deinstallation von Kaspersky aktiviert wird. Für Privatkunden ist ein Umstieg daher sehr einfach und ohne erkennbare Risiken möglich.

Im Enterprisebereich ist der Aufwand größer, aber auch hier stehen ausreichend gleichwertige Alternativprodukte zur Verfügung. Hier muss jeder Anwender allerdings eine individuelle Risikobetrachtung vornehmen (s. Hinweis in der Warnung), da der Migrationsaufwand erheblich sein kann. Wichtige Komponenten einer komplexen IT-Sicherheitsinfrastruktur dürfen keinesfalls notfallmäßig abgeschaltet werden, ohne alternative Maßnahmen umzusetzen. In der BSI-Warnung wird daher auch sehr deutlich auf diesen Umstand hingewiesen.

Die Situation für russische Unternehmen bzw. Standorte deutscher Unternehmen in Russland muss separat betrachtet werden. Aufgrund von Boykottmaßnahmen und Sanktionen beliefern viele amerikanische IT-Unternehmen russische Kunden nicht mehr. Dies führt dazu, dass auch IT-Sicherheitsprodukte keine Updates mehr bekommen und aus Russland heraus die Clouddienste der Hersteller nicht mehr erreichbar sind. Die betroffenen Unternehmen sind sich dieser Situation aber sehr bewusst und arbeiten bereits an Lösungen oder haben (nicht nur aus IT-Sicherheitsgründen) ihre Tätigkeiten in Russland vorübergehend eingestellt.

Da durch die Warnmeldung des BSI das Bewusstsein für potenzielle Gefahren geschaffen wird und damit der Einsatz der Kasperski Software nicht verhindert wird, muss letztendlich jeder Anwender eine individuelle Risikobetrachtung durchführen (vgl. „Allgemeiner Hinweis“ im Warntext). Diese Risikobetrachtung ist für IT-Sicherheitsexperten ohne VS-Hintergrundinformationen durchführbar, da die technischen Aspekte offensichtlich sind und in den Medien ausreichende Informationen zum Wirken der russischen Regierung verfügbar sind.

In einer vertraulichen Sitzung [redacted] wurde deutlich, dass die meisten DAX-Unternehmen bereits einen Tag nach der russischen

Kriegserklärung gegen die Ukraine Maßnahmen zur Reduzierung potenzieller Sicherheitsrisiken eingeleitet haben.

Die Folgen eines Missbrauchs von Antiviren-Software ist grundsätzlich unüberschaubar groß. Anti-Viren-Software greift tief in die Systeme ein, läuft grundsätzlich mit den höchsten Rechten und wird jeden Tag mehrfach aktualisiert. Wenn der russische Staat hier Schaden anrichten möchte, wäre AV-Software ein ideales Werkzeug.

Wenn das BSI sich nicht anderen europäischen Staaten und der EU anschließt, die bereits vor Kaspersky gewarnt haben, besteht hingegen die Gefahr, dass dies von der Öffentlichkeit als „Unbedenklichkeits-Testat“ des BSI missverstanden wird.

(3) Wirtschaftliche Folgen und Gegenreaktionen

Für Kaspersky bedeutete eine BSI-Warnung einen weiteren Imageverlust. Wie sich dieser auswirken könnte, ist nicht vorhersagbar, da bereits andere westliche Staaten seit Jahren den Einsatz von Kaspersky-Produkten in ihrer Verwaltung verbieten und viele Staaten und EU ihre Warnungen anlässlich des Kriegs erneuert haben.

Die wirtschaftlichen Folgen für Enterprise-Kunden von Kaspersky können spürbar sein, wenn sie sich zum Umstieg auf alternative Produkte entschließen. Die Entscheidung muss individuell nach ausgiebiger Analyse getroffen werden. Eine Warnung des BSI wäre nur ein Teilaspekt in der Analyse.

In der Verwaltung ist die Situation vermutlich anders. Hier würde eine BSI-Warnung vermutlich stärker beachtet als in der Wirtschaft.

Für Privatnutzer wäre der Schaden überschaubar.

Technische Gegenreaktionen von Kaspersky sind unwahrscheinlich, da dies einen nicht mehr zu heilenden Vertrauensverlust zur Folge hätte. Wahrscheinlicher wäre der Versuch, sich juristisch gegen eine Warnung zu wehren. Die Folgen wären aus hiesiger Sicht verkraftbar (und im Vergleich zu den sonstigen Sanktionsfolgen vernachlässigbar), da die Botschaft, den Einsatz von Kaspersky-Produkten kritisch zu hinterfragen, bereits über andere Kanäle kommuniziert worden ist.

Mögliche Reaktionen und Gegenmaßnahmen staatlicher Stellen können nicht vorhergesagt werden.

Im Auftrag

elektr. gez.

Dr. Günther Welsch

43

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

44

044_1_geschwärzt.pdf

Von: GP Referat BL 25
An: GP Abteilung KM
Cc: GP Fachbereich BL 2; GP Referat BL 25
Betreff: AW: Nachgang 1 zu 0360_22 Erlass CI 1 - Kaspersky Viren-Schutzsoftware
Datum: Freitag, 11. März 2022 11:34:52

Lieber Herr Welsch,

hier von einigen unserer Partner deren Position zur Kaspersky-Frage.
Falls wir mehr bekommen, leite ich Ihnen das ebenfalls noch zu.

Frankreich
Siehe https://www.cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/.
Hier mal eine Google Translate Übersetzung des relevanten Absatzes: „Im aktuellen Kontext kann die Nutzung bestimmter digitaler Tools, insbesondere der Tools der Firma Kaspersky, aufgrund ihrer Verbindung zu Russland in Frage gestellt werden. Zum jetzigen Zeitpunkt rechtfertigt kein objektives Element eine Änderung der Bewertung des Qualitätsniveaus der bereitgestellten Produkte und Dienstleistungen. Es sollten jedoch grundlegende Vorsichtsmaßnahmen getroffen werden. Das Abschalten von Cybersicherheitstools in einem Kontext von Spannungen im Cyberspace und verschärfter Cyberkriminalität kann die Cybersicherheit Ihres Unternehmens erheblich schwächen. Ohne eine alternative Lösung kann diese Trennung auch nicht empfohlen werden. Russlands Isolation auf der internationalen Bühne und das Risiko eines Angriffs auf mit Russland verbundene Industrieunternehmen können die Fähigkeit dieser Unternehmen beeinträchtigen, Aktualisierungen ihrer Produkte und Dienstleistungen bereitzustellen und sie daher auf dem neuesten Stand der Technik zu halten, der zum Schutz ihrer Kunden erforderlich ist . Mittelfristig muss daher über eine Strategie der Diversifizierung von Cybersecurity-Lösungen nachgedacht werden.“

Niederlande
Dort gab es bereits vor einigen Jahren einen Bann von Kaspersky aus Regierungsnetzen. Kaspersky hatte ca. 2017/18 gegen die Entscheidung geklagt und verloren. Aktuelle Statements: https://jidachen.com/2022/03/10/ncsc-is-silent-on-the-risk-of-kaspersky-software/
Außerdem leider nur auf Niederländisch:
https://www.rijksoverheid.nl/documenten/wob-verzoeken/2022/03/03/herziening-besluit-op-bezwaar-en-herziening-besluit-wob-verzoek-inzake-antivirussoftware-kaspersky-lab-b.v

USA
“US officials argued that the company's products could be under the influence of the Kremlin, and so represent a threat to US national security. These measures were taken following concerns that Russian nation-state hackers had influenced the 2016 presidential election.
"The case against Kaspersky is well documented and deeply concerning," Democratic Senator Jeanne Shaheen said in 2017. Kaspersky Lab's repeated attempts to overturn the ban have so far proved unsuccessful.”

GBR
NCSC UK hat ebenfalls 2017 vor Kaspersky gewarnt, aber damals eine Hintertür offen gehalten und wollte mit Kaspersky über ein Abkommen verhandeln:
„As well as keeping this guidance under review, we are in discussions with Kaspersky Lab, by far the largest Russian player in the UK, about whether we can develop a framework that we and

others can independently verify, which would give the Government assurance about the security of their involvement in the wider UK market. In particular we are seeking verifiable measures to prevent the transfer of UK data to the Russian state. We will be transparent about the outcome of those discussions with Kaspersky Lab and we will adjust our guidance if necessary in the light of any conclusions."

VG, [redacted]

Im Weiteren wird ein VS-NfD eingestufter Vorgang zitiert.

044_2_geschwärzt.pdf

Von: GP Referat KM 14
An: GP Referat BL 25
Cc: GP Abteilung KM
Betreff: WG: Nachgang 1 zu 0360_22 Erlass CI 1 - Kaspersky Viren-Schutzsoftware
Datum: Freitag, 11. März 2022 13:57:01

[redacted]

da habe ich noch eine Einschätzung aus 2018 für Deine Sammlung:

https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_EN.html?redirect

Die EU bezeichnet darin Kaspersky-Produkte als „malicious“.

Viele Grüße

[redacted]

Von: GP Abteilung KM <abteilung-km@bsi.bund.de>
Gesendet: Freitag, 11. März 2022 13:51
An: GP Referat KM 14 <referat-km14@bsi.bund.de>; GP Fachbereich KM 1 <fachbereich-km1@bsi.bund.de>
Betreff: WG: Nachgang 1 zu 0360_22 Erlass CI 1 - Kaspersky Viren-Schutzsoftware

zwV.

Im Folgenden wird 044_1_geschwärzt.pdf zitiert.

45

045_0_geschwärzt.pdf

Von: Andreas.Koenen@bmi.bund.de
An: Schönbohm, Arne
Cc: Schabhüser, Gerhard; Markus.Richter@bmi.bund.de; Welsch, Günther
Betreff: WG: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Freitag, 11. März 2022 20:57:09
Anlagen: CDR_Kaspersky_Warnung_V8_ÄndKö.docx
CDR_VS-NfD_Kaspersky_Begründung_V8_ErgSR_ÄndKö.docx
Julia Parser Messages.txt

Lieber Herr Schönbohm,

nach erfolgter interner Abstimmung bitte ich Sie Sie nun, die Warnung weiter vorzubereiten. Bitte berücksichtigen Sie dabei die markierten Änderungen.

Darüber hinaus bitte ich Sie, den finalen Entwurf der Warnung sowie die abschließende Begründung rechtzeitig vor der Veröffentlichung erneut Herrn Staatssekretär Richter und mir vertraulich zur Kenntnis zu bringen sowie gleichzeitig die Presse des BMI zu informieren.

Beste Grüße

Andreas Könen
Abteilungsleiter CI
Cyber- und Informationssicherheit
Bundesministerium des Innern und für Heimat
Alt-Moabit 140, 10557 Berlin
DEUTSCHLAND

Telefon: +49 30 18681 [redacted]
E-Mail: andreas koenen@bmi.bund.de
Internet: www.bmi.bund.de

Im Folgenden wird 016_0_geschwärzt.pdf zitiert.

045_1_CDR_Kaspersky_Warnung_V8_ÄndKö.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

Viren-Schutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Viren-Schutzsoftware 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. Viren-Schutzsoftware 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.

~~Die Bedrohungssituation durch offensive Cyber-Operationen von russischer Seite führen in der aktuellen Lage zu einer neuen Risikobewertung.~~ Ein russischer IT-Hersteller kann selbst entsprechende 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 Viren-Schutzsoftware 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 Staates~~, 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 Viren-Schutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Viren-Schutzsoftware 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 Viren-Schutzsoftware) 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)
Fehler! Linkreferenz ungültig.~~https://www.bsi.bund.de/DE/DasBSI/Gesetz/gesetz_node.html~~

[2] Darstellung Risikostufen
Fehler! Linkreferenz ungültig.~~https://www.cert-bund.de/risk~~

045_2_CDR_VS-NfD_Kaspersky_Begründung_V8_ErgSR_ÄndKö_geschwärzt.pdf

Referat KM 14 02. 03. 2021

Az. KM14-210 01 03 / VS-NfD

[redacted]

Betr. Bewertung von IT-Sicherheitsprodukten
hier: Warnung vor Kaspersky-Produkten nach § 7 BSIG

Bezug

Anlagen Entwurf Warntext

1) Vermerk zur Begründung der Warnung

A Begründung der Warnung nach § 7 Abs. 1 BSIG

Das BSI darf nach § 7 Abs. 1 BSIG u.a. vor Sicherheitslücken in informationstechnischen Produkten und Diensten öffentlich warnen. Sicherheitslücken in diesem Sinne sind nach § 2 Abs. 6 BSIG *„Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.“* Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1.d BSIG). Dabei ist nach Meinung in der Literatur zwar noch ein Bezug zur Gefahrenvorsorge notwendig, aber keine konkrete Gefahrenlage mehr (vgl. Ritter-*Schulte,* Die Weiterentwicklung des IT-Sicherheitsgesetzes, Art. 1 Nr. 9 IT-SiG 2.0, Rn. 307). Solche Sicherheitseigenschaften von Produkten können sich auch aus der Struktur des Anbieters ergeben. Da hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI vor dem Einsatz des Produktes warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG).

Die Ereignisse rund um Kaspersky werden vom BSI seit Jahren aufmerksam verfolgt. Mehrere westliche Staaten wie USA und Niederlande warnen seit Jahren öffentlich vor Kaspersky und haben die Software für den Einsatz im Behördenumfeld gesperrt (Quellen werden nachgereicht) [redacted] ~~Das BSI hat sich aber bislang mit öffentlichen Warnungen zu Kaspersky zurückgehalten.~~

Der russische Angriff auf die Ukraine, der mit hybriden Mitteln - also auch im Cyberraum - geführt wird und von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt wurde, verändert die Lagebeurteilung. Russland ist kein demokratischer Rechtsstaat und sieht Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als ~~Feind~~ Kontrahent an. Mit feindlichen Übergriffen auf deutsche Institutionen, Unternehmen und IT-Infrastrukturen ist daher zu rechnen. Russische Unternehmen wie Kaspersky könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden, zum anderen selbst Ziel massiver Cyberangriffe werden. Die Gefahr, dass Kaspersky in die kriegerischen Auseinandersetzungen

hineingezogen wird, ist daher so groß, dass eine Warnung angemessen ist. Es muss damit gerechnet werden, dass Kaspersky nicht mehr die uneingeschränkte Kontrolle über seine Software und IT-Systeme hat bzw. diese in Kürze verlieren wird.

[redacted]

Bereits in den letzten Jahren wurden Fälle bekannt, in denen staatliche Stellen Einfluss auf Kaspersky genommen haben:

[redacted]

In den Jahren 2018 und 2019 wurden russische VPN-Anbieter gezwungen, bestimmte Verbindungen auf Anordnung der Regierung zu blocken. Während die meisten Anbieter die Kooperation verweigerten, kam Kaspersky den Anordnungen nach[2]:

"Although not all VPNs are banned, a 2018 law introduced fines for search engines that brought up results to proxy sites (including VPNs) that would give Russians access to prohibited content or instructions on how to get access to that content.
The following year, VPNs and search engines were compelled to block any websites that appeared on the federal government blacklist. Later, 10 VPN providers were ordered to hand over access to their servers or face being banned. Only one, Kaspersky Lab, which is based in Russia, agreed, while others - like ExpressVPN and NordVPN - shut down their Russian servers."

Neben dem BSI haben auch andere Länder und Organisationen ihre Risikobewertung angepasst. Frankreich hat beispielsweise eine vergleichbare Warnung veröffentlicht[3]. [redacted] Die Teilnehmer waren sich einig, dass der Einsatz von Kaspersky-Produkten hoch problematisch ist. Zum Schutz ihrer IT-Systeme wurden daher automatische Updates abgestellt und Schritte eingeleitet, um die Software schnellstmöglich durch eine sicherere Alternative abzulösen.

[redacted]

[2]https://www.techradar.com/vpn/which-websites-and-services-are-banned-in-russia
[3]https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

Die in der Warnung beschriebenen Angriffsvektoren sind nicht neu. Im Folgenden einige Beispiele, die belegen, welchen Schaden ein Angreifer mit Viren-Schutzsoftware anrichten könnte:

- ✗ Am 10.06.2015 hat Kaspersky selbst in einer Pressemitteilung[4] mitgeteilt, dass das Unternehmensnetzwerk gehackt wurde und Angreifer mit teils neuen Methoden versucht haben, vertrauliche Daten zu stehlen, die dann für Angriffe auf die Kunden missbraucht werden könnten.
- ✗ Am 05. Januar 2012 hat die Hacker-Gruppe „The Lords of Dharmaraja" geheimen Sourcecode von Symantec bei Pastebin veröffentlicht. Symantec hat die Echtheit des Codes bestätigt und die sicherheitsrelevanten Auswirkungen mit dem BSI-Präsidenten in einem vertraulichen Gespräch erörtert.
- ✗ Alle Hersteller von Viren-Schutzprogrammen hatten in der Vergangenheit Schwachstellen, die für Angriffe auf Kundensysteme hätten genutzt werden können. Mit Kenntnis des Sourcecode oder noch nicht veröffentlichter Schwachstellen wäre ein~~e~~ Angreifer nicht auf offiziell gemeldete Schwachstellen angewiesen, um einen Angriff durchzuführen. Wenn schon Schwachstellen ausreichen, um Systeme komplett stillzulegen, wäre dies mit einer Backdoor noch sehr viel leichter.
- ✗ Es sind zahlreiche Vorfälle bei allen Herstellern von Viren-Schutzsoftware bekannt, in denen eine fehlerhafte Erkennungssignatur Windows-Systemdateien als schädlich klassifiziert und damit das IT-System blockiert hat.
- ✗ Es sind auch Vorfälle bekannt, bei denen nach einem Signaturupdate bestimmte Schadprogramme irrtümlich nicht mehr detektiert wurden.
- ✗ Alle Viren-Schutzprogramme haben Funktionen eingebaut, mit denen sich Schadsoftwareausbrüche begrenzen lassen. Dazu können sie beliebige Dateien blockieren oder löschen. Auch in der Bundesverwaltung hat es bereits einen Sicherheitsvorfall gegeben, bei dem durch eine Fehlbedienung der "Outbreak-Prevention"-Funktion eine ganze Behörde für einen Tag lahmgelegt wurde.
- ✗ Bei Updates werden nicht immer nur Signaturen übertragen. Es ist auch möglich, dass größere Softwarebestandteile (z. B. Scan-Engines) aktualisiert werden müssen, um mit neuen Signaturen/Erkennungsverfahren kompatibel zu bleiben. Dem BSI sind Fälle bekannt, bei denen durch Updates eines Viren-Schutzprogramms neue Funktionen installiert oder Konfigurationen überschrieben wurden, ohne dass die Nutzer dies bemerken konnten. In der Folge wurde Kundendaten ohne Genehmigung an den Hersteller übertragen.

Derartige Vorfälle mussten alle Hersteller bereits vermelden. Sie sind immer unbeabsichtigt aufgrund von Fehlern oder Nachlässigkeiten geschehen. Eigene Entwickler oder Hacker, die in die Systeme des Herstellers eingedrungen sind, sind nicht auf Schwachstellen oder Fehler angewiesen, und könnten daher sehr einfach die folgenden Funktionen auf Kundensystemen implementieren:

- Zielsysteme analysieren (Systemeigenschaften, Hardwareeigenschaften, verwendete Software etc.)
- Daten zum Hersteller übertragen (z. B. Dateien, URLs)
- Dateien sperren oder löschen

Um die gewollte Funktionalität bieten zu können, laufen Viren-Schutzprogramme zudem mit hohen Systemrechten, schützen sich vor Veränderungen und haben Zugriff auf das gesamte Filesystem. Durch die hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig ist, könnten theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Manipulationen lassen sich auch temporär vornehmen

[4] https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

und dadurch sehr gut tarnen. Beispielsweise könnte für wenige Stunden ein bestimmter Schadcode bewusst nicht erkannt werden, um anderen Angreifern den Weg zu bereiten.

Wenn die Kaspersky-Produkte für Angriffe entweder durch Anweisung der russischen Regierung oder durch staatliches Eindringen in deren Systeme instrumentalisiert werden, ist es daher möglich, dass auf die Systeme auf denen Kaspersky-Produkte installiert sind, unberechtigt zugegriffen oder Einfluss genommen werden kann.

Kaspersky ist sich dieser Gefahren bewusst und hat in der Vergangenheit diverse Maßnahmen zur Vertrauensbildung ergriffen, die aber alle nicht geeignet sind, die aktuelle veränderte Gefahrenlage zu entschärfen.

✗ Kaspersky hat versucht, sich dem Einfluss russischer Behörden zu entziehen und betreibt eine Dateninfrastruktur in zwei Rechenzentren in Zürich zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden aus Europa, den Vereinigten Staaten und Kanada sowie in mehreren asiatisch-pazifischen Ländern. Für die Bereitstellung von Updates/Virensignaturen stehen bei Bedarf verschiedene Server in Europa zur Verfügung, unter anderem in Frankfurt.

Es ist unerheblich, wo die Kundendaten gehostet werden. Entscheidend ist, wer Sourcecodeänderungen vornehmen und Signaturdaten erstellen kann und wie diese qualitätsgesichert und geprüft werden. Kaspersky kann nicht nachweisen, dass diese Prozesse komplett unabhängig vom russischen Hauptquartier durchgeführt werden. Es ist auch nicht transparent, wer administrativen Zugang zu den Systemen in Westeuropa hat. Aufgrund der Erfahrungen mit anderen Cloudanbietern ist es extrem unwahrscheinlich, dass die Rechenzentren in West-Europa komplett autark arbeiten und keine administrativen Eingriffe aus anderen Regionen erfolgen können.

✗ Die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren und Datendienste von Kaspersky wurden von zwei externen, unabhängigen Prüforganisationen bestätigt. Kaspersky hat das SOC-2-Audit (Service Organization Control for Service Organizations) Typ 1 durch einen Big-Four-Auditor erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigte. Darüber hinaus wurden Datendienste vom TÜV AUSTRIA nach ISO/IEC 27001:2013 zertifiziert.

Eine Zertifizierung sagt nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus. Sie ist keine Garantie für den Ist-Zustand.

✗ Kaspersky sagt über sich selbst, als global agierendes privates Unternehmen (Sitz der Holding ist London, UK) keine Verbindungen zur russischen Regierung zu haben.

Diese Aussage ist nicht glaubhaft. Kaspersky hat seinen Hauptsitz in Moskau und weist eine russische Eigentümerstruktur auf. Als eines der wichtigsten IT-Security-Unternehmen Russlands arbeitet Kaspersky eng mit Ermittlungsbehörden zusammen (s. o.). Wesentliche Teile der Belegschaft arbeiten daher in Russland oder haben familiäre Bindungen in Russland und sind daher dem direkten Einfluss und Druck der Behörden ausgesetzt.

✗ Kaspersky unterliegt nach eigenen Angaben nicht dem russischen System operativer Ermittlungsmaßnahmen (SORM) oder anderen ähnlichen Gesetzen und sei deswegen nicht zur Auskunftserteilung verpflichtet.

Diese faktischen Einflussmöglichkeiten der russischen Regierung entfallen nicht deswegen, weil Kaspersky nach russischem Recht keinen Mitwirkungspflichten unterliegt (zu den Pflichten s. Gutachten Prof. Hober).

Angesichts des mit dem Einmarsch in die Ukraine erfolgten eklatanten Bruchs von internationalem Recht durch Russland muss damit gerechnet werden, dass die russische Regierung auch gegen geltendes russisches Recht verstößt, wenn ihr dies opportun erscheint.

Soweit das BSI die Maßnahmen von Kaspersky in der Vergangenheit für ausreichend hielt, um die Produkte von Kaspersky weiter einsetzen zu können, lag dem die Annahme zu Grunde, dass die russische Regierung keine Schritte einleiten würde, die bei Bekanntwerden (bzw. Entdeckung) sowohl Kaspersky als auch der russischen Regierung wirtschaftlichen Schaden und einen Reputationsverlust zufügen würden. Angesichts der nunmehr offenen Konfrontation Russlands mit der EU und den NATO-Staaten und der Hinnahme selbst existenzvernichtender Sanktionen für russische Unternehmen, kann diese Grundannahme nicht weiter aufrechterhalten werden. Wir müssen nunmehr davon ausgehen, dass die russische Regierung in der jetzigen Situation keine Rücksicht mehr auf das internationale Geschäft und die Reputation von Kaspersky nehmen würde [redacted] Als Konsequenz sollten diese Einrichtungen keine Produkte des Herstellers Kaspersky einsetzen.

Formatiert: Schriftart: 11 Pt.

Formatiert: Schriftart: BundesSerif Office, 11 Pt.

Eine Warnung des BSI ist auch mit dem Grundsatz der Verhältnismäßigkeit vereinbar: zum einen weist das BSI in seiner Warnung darauf hin, dass private Anwender weniger bedroht sein können, was zur Folge haben kann, dass diese die Produkte von Kaspersky weiterhin nutzen. Ein erfolgreicher Angriff auf ein KRITIS-Unternehmen könnte jedoch die Versorgung der Bevölkerung mit lebenswichtigen Diensten wie Wasser oder Energie beeinträchtigen und bis hin zu einem Ausnahmezustand führen. Das potentielle Schadensrisiko ist hier mithin enorm. Dem steht das Interesse des einzelnen Herstellers (hier Kaspersky) an der freien Ausübung seines Gewerbes gegenüber. Hier ist zwar zu berücksichtigen, dass eine Warnmeldung mit hoher Wahrscheinlichkeit spürbare Folgen auf die wirtschaftliche Tätigkeit des Herstellers in Deutschland hätte. Allerdings überwiegt hier der Schutz der Allgemeinheit aufgrund der besonderen Schwere des Schadensrisikos das Interesse des einzelnen Herstellers.

✗

Fazit:

Durch manipulierte Viren-Schutzprogramme hat ein Angreifer nahezu unbegrenzte Möglichkeiten, IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste Vorfall öffentlich bekannt wird. Vielmehr ist die Warnung zum jetzigen Zeitpunkt angezeigt, um rechtzeitig präventiv zu handeln und die relevanten Anwender vor potentiellem Schaden zu bewahren. Mildere Mittel zum Schutz der Informationssicherheit sind nicht ersichtlich.

B Vorherige Stellungnahmemöglichkeit nach § 7 Abs. 1 a Nr. 1 BSIG

Formatiert: Schriftart: 12 Pt.

Formatiert: Schriftart: 12 Pt.

Kaspersky sollte vor der Veröffentlichung nur mit kurzer Frist informiert und Gelegenheit zur Stellungnahme gegeben werden. Es ist Gefahr im Verzug. Hacker könnten ihre Vorbereitungen bereits abgeschlossen haben und nur noch auf einen Einsatzbefehl warten. Es ist nicht ersichtlich, dass Kaspersky eine Möglichkeit hätte, durch technische oder sonstige Maßnahmen die Risikoeinschätzung positiv zu beeinflussen. Es ist nicht wahrscheinlich, dass der Hersteller an dem ~~zugrunde liegenden~~zugrundeliegenden strukturellen Sicherheitsproblem etwas ändern kann, da er kaum Einfluss auf die Gefährdung hat. Angesichts der Gefährdungslage erscheint eine kurze Frist daher verhältnismäßig und fachlich angemessen.

C Verfügung

2) BL 23 zur Kenntnis

3) KM zur Mitzeichnung ~~[MZ. AL KM vom 3.3.2002]~~

4) TK zur Mitzeichnung

5) OC zur Mitzeichnung

6) BL zur Mitzeichnung

7) P/VP z. Billigung

Im Auftrag

[redacted]

46

046_0_geschwärzt.pdf

Von: Schönbohm, Arne
An: Welsch, Günther
Cc: [redacted]; Schabhüser, Gerhard
Betreff: WG: WG: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Freitag, 11. März 2022 22:47:48
Anlagen: CDR_Kaspersky_Warnung_V8_ÄndKö.docx
CDR_VS-NfD_Kaspersky_Begründung_V8_ErgSR_Än dKö.docx
Julia Parser Messages.txt

Können Sie dies bitte übernehmen? Verööfentlichung am Mitteoch?

Mit freundlichen Grüßen

Arne Schönbohm

via SecurePIM gesendet

Im Folgenden wird 045_0_geschwärzt.pdf zitiert (inkl. der Anhänge).

47

047_0_geschwärzt.pdf

Von: [redacted]
An: Welsch, Günther
Cc: Schönbohm, Arne; Schabhüser, Gerhard [redacted]
Betreff: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Samstag, 12. März 2022 00:09:20
Anlagen: WG WG VS-NfD - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware.msg
Presseanfragen AV-Produkte Kaspersky .msg

Lieber Günther,

falls möglich, bitte ich die Warnung seitens BSI bis zum Di., 15.03.2022, 12:00h presse-öffentlich zu machen.

Dann können wir damit in die nächste c't und in Die Zeit hineinkommen und das BSI als Akteur positionieren.

Zum Verständnis: Ich lasse mich in meiner Aufgabe als Pressesprecher des BSI grundsätzlich nicht extern treiben. Wenn sinnstiftend, nutze ich wie ein Surfer (der mit dem Brett auf dem Wasser) die Welle bzw. ein Momentum.

Mit [redacted] hatte ich letzte Woche (Freitag vor Wochenlage) telefoniert und dann mit [redacted] auch danach.
Die Abstimmung mit BMI Presse (PK II 1) übernehmen wir (Stab 1) wie gewohnt und geübt.

[redacted]

Daher unterstützen [redacted] und [redacted], TK 21, Stab 1 zu Presse vorübergehend.
[redacted] nehme ich daher dazu in cc.; [redacted] und [redacted] sind derzeit erkrankt.

Vielen Dank!

Beste Grüße,
[redacted]

i.A.
[redacted]
Pressesprecher
Leiter Stab1 – Strategische Kommunikation und Presse

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Alle 185-189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49 [redacted]
Fax: +49 (0)228 99 10 9582[redacted]

E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Der Anhang "WG: WG: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware" ist identisch mit 046_0_geschwärzt.pdf.

047_1_geschwärzt.pdf

Von: [redacted] im Auftrag von GP Stab 1 - Strategische Kommunikation und Presse
An: [redacted]@bmi.bund.de
Cc: Presse@bmi.bund.de; CI@bmi.bund.de; GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; GP Stab 3 - Strategie und Leitungsunterstuetzung
Betreff: Presseanfragen AV-Produkte / Kaspersky
Datum: Freitag, 11. März 2022 19:59:00
Anlagen: AW Kaspersky Anti-Viren-Software und russische Cyberbedrohung FunkeMedien.msg
Anfrage zu Kaspersky und weiteren SW-Produkten .msg

[redacted]

ich weiß, dass derzeit die Themen Migration und Energieversorgung in Zusammenhang mit dem Krieg in der Ukraine in den Vordergrund gerückt sind.
Allerdings steht seitens des Bundes noch eine Position zu den AV-Produkten und -Services von Kaspersky aus.

[redacted] fragt nun mit Fristsetzung Di., 15.03.2022, 12:00h, erneut nach. Die Zeit bittet für die nächste Ausgabe ebenfalls um entsprechende Information (Input möglich bis Di., 15.03.2022, 21:00h latest). Auch Einrichtungen wie [redacted] bitten das BSI um eine Einordnung und fragen hierzu bei BSI Presse an.

Können Sie uns eine Einschätzung geben, ob wir eine Position bis Dienstag Mittag presse-öffentlich kommunizieren können?
Falls die Position dazu bis dahin nicht möglich sein sollte, müssen wir uns meines Erachtens auf eine gemeinsame Sprachregelung verständigen.

Zur generellen Lageeinschätzung im Cyber-Raum verweisen wir weiterhin auf die BSI-Web-Veröffentlichung (https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2022/220225_Angriff-Ukraine-Statement html).

Besten Dank im Voraus!

Viele Grüße,
[redacted]

i.A.
[redacted]
Pressesprecher
Leiter Stab1 – Strategische Kommunikation und Presse

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Alle 185-189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49 [redacted]
Fax: +49 (0)228 99 10 9582[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----
Von: [redacted]
Gesendet: Freitag, 11. März 2022 12:00

An: GP Presse <presse@bsi.bund.de>
Betreff: Kaspersky / Ukraine-Krieg

Sehr geehrter [redacted],

erneut melde ich mich bezüglich der Frage, ob das BSI den Einsatz der Kaspersky-Schutzsoftware aktuell noch für unbedenklich hält.

Wir werden das Thema in [redacted] aufgreifen. Diese erscheint [redacted] -- falls Sie mir also Vorabinformationen zukommen lassen möchten, können wir eine etwaige Sperrfrist berücksichtigen.

Da das Heft bereits kommende Woche gedruckt wird, benötige ich jedoch bis kommenden Dienstag, 12 Uhr eine Rückmeldung.

Ich würde mich freuen, bis dahin eine zitierfähige Antwort von Ihnen zu erhalten, da der akuelle Stand für alle Parteien unbefriedigend ist. Es ist keinem damit geholfen, wenn wir die Situation, wie sich sich aktuell darstellt, am 25. März noch mal erzählen.

Meine Fragen entsprechen im Wesentlichen meiner ersten Anfrage zu diesem Thema, ich habe sie nur unten etwas ergänzt:

Aufgrund der aktuellen Kriegssituation in der Ukraine und den daraus resultierenden Sanktionen für Russland stellen uns viele Leser die Frage, ob sie die Kaspersky-Virenschutzsoftware weiterhin bedenkenlos einsetzen können.

Im Jahr 2017, als die US-Regierung vor dem Einsatz von Kaspersky-Produkten warnte, stellte sich das BSI auf die Seite von Kaspersky: https://www.sueddeutsche.de/digital/it-sicherheit-fbi-warnt-vor-kaspersky-software-1.3640805

* Hält das BSI den Einsatz der Kaspersky-Produkte im privaten Umfeld, Unternehmen und Behörden weiterhin für unbedenklich? Oder sollte man die Software gar deinstallieren?

* Welche Risiken gehen aus dem Einsatz der Kaspersky-Software nach Einschätzung des BSI hervor?

* Plant das BSI eine amtliche Warnung vor dem Einsatz der Kaspersky-Software herauszugeben?

Viele Grüße

[redacted]

047_1_1_geschwärzt.pdf

[redacted]

Von: [redacted] im Auftrag von GP Stab 1 - Strategische Kommunikation und Presse
Gesendet: Donnerstag, 10. März 2022 16:21
An: [redacted]@bmi.bund.de
Cc: PKII1@bmi.bund.de; GP Stab 1 - Strategische Kommunikation und Presse
Betreff: AW: Kaspersky Anti-Viren-Software und russische Cyberbedrohung / [redacted]

[redacted]

ich habe [redacted] heute kurz informiert, dass er sobald möglich Informationen erhält, wie weitere MedienvertreterInnen auch.
Ich hatte mit ihm gestern und vorgestern gesprochen, u.a. auch zu so genannten Hochwertzielen.

Sobald wir, Stab1 bzw. BSI Presse, eine konkrete Presseaktion zu diesem Thema absehen können bzw. in die Umsetzung nehmen, melden wir uns bei Ihnen bzw. BMI Presse, PK II 1.

Beste Grüße,
[redacted]

i.A.
[redacted]
Pressesprecher
Leiter Stab1 – Strategische Kommunikation und Presse

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Alle 185-189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49 [redacted]
Fax: +49 (0)228 99 10 9582[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----
Von: [redacted]@bmi.bund.de [redacted]@bmi.bund.de>
Gesendet: Donnerstag, 10. März 2022 14:04
An: [redacted]@bsi.bund.de>
Cc: PKII1@bmi.bund.de
Betreff: WG: Kaspersky Anti-Viren-Software und russische Cyberbedrohung / FunkeMedien

[redacted],
hatten Sie schon Zeit, mit [redacted] zu sprechen?

Schöne Grüße
[redacted]

Von: [redacted]
Gesendet: Donnerstag, 10. März 2022 14:03
An [redacted]@bmi.bund.de>
Betreff: AW: Kaspersky Anti-Viren-Software und russische Cyberbedrohung / FunkeMedien

[redacted],

Wollte mal nachfragen: Wie sieht es aus mit den Antworten zu dem Thema?

Beste Grüße, [redacted]

_____
Von: [redacted]@bmi.bund.de>
[redacted]@bmi.bund.de<mailto[redacted]@bmi.bund.de>>
Gesendet: Mittwoch, 9. März 2022 11:34
An: [redacted]
Cc: Presse@bmi.bund.de<mailto:Presse@bmi.bund.de> <Presse@bmi.bund.de<mailto:Presse@bmi.bund.de>>
Betreff: AW: Kaspersky Anti-Viren-Software und russische Cyberbedrohung[redacted]

[redacted],

ich unterstütze für ein paar Tage im Pressereferat. Ich hoffe, die letzten Jahre waren gut zu Ihnen. Ihre Anfrage hat uns erreicht, ich fürchte, heute 12:00 Uhr werden wir nicht halten können – wir sind aber dran und antworten so schnell wie möglich.

Schöne Grüße

[redacted]

_____

Pressestelle |

Bundesministerium des Innern und für Heimat

Alt Moabit 140, D-10557 Berlin

Telefon: +49 30 18 681[redacted]

E-Mail: [redacted]@bmi.bund.de<mailto:[redacted]@bmi.bund.de>

E-Mail: Presse@bmi.bund.de<mailto:Presse@bmi.bund.de>

Internet: www.bmi.bund.de<http://www.bmi.bund.de>
(https://eur02.safelinks.protection.outlook.com/...)<https://eur02.safelinks.protection.outlook.com/?url=http%3A%[redacted]

Von: [redacted]
Gesendet: Dienstag, 8. März 2022 14:24
An: Presse <Presse@bmi.bund.de<mailto:Presse@bmi.bund.de>>
Betreff: Kaspersky Anti-Viren-Software und russische Cyberbedrohung / FunkeMedien

Sehr geehrte Damen und Herren,

aktuell arbeite ich an einem Artikel zum Thema Cybersicherheitslage in Deutschland angesichts des Krieges in der Ukraine. Dazu interessiert mich die Einschätzung des BMI als federführendes Ressort der Bundesregierung – speziell der Blick auf die Nutzung des russischstämmigen Anti-Viren-Programmes Kaspersky durch deutsche Behörden und Firmen. Mit der Bitte um eine Antwort im Laufe des Tages, sofern angesichts des Feiertags möglich, wäre das klasse. Sonst bitte bis spätestens morgen, Mittwoch, 12 Uhr.

1. Wie bewertet das BMI das Risiko der Nutzung des Anti-Viren-Programms Kaspersky durch deutsche Privatpersonen, Firmen und Behörden angesichts einer möglichen Cyberbedrohung durch russischstämmige/russisch-staatliche Hackergruppen?
2. Welche Erkenntnis hat das BMI darüber, das die Firma Kaspersky zur Zusammenarbeit mit russischen Behörden verpflichtet ist?
3. Welche Erkenntnisse hat das BMI darüber, wie viele Personen/Firmen/Behörden in Deutschland ein Anti-Viren-Programm der Firma Kaspersky nutzen?

Herzlichen Dank und beste Grüße,

[redacted]

[redacted]

[redacted]

[redacted]

047_1_2 _geschwärzt.pdf

Von: [redacted]
An: GP Presse
Betreff: Anfrage zu Kaspersky und weiteren SW-Produkten
Datum: Mittwoch, 9. März 2022 17:41:16
Anlagen: smime.p7m

Sehr [redacted],

ich beziehe mich auf unser heutiges Telefonat mit der Bitte um zeitnahe Informationen zum Umgang u.a. mit der AV-Lösung Kaspersky.
[redacted] ist letztes Jahr für den Virenschutz vollständig auf Kaspersky gewechselt.
Vor dem Hintergrund der aktuellen Pressemeldungen erwägen [redacted] zeitnah auf eine Alternativ-Lösung zu wechseln.
Wie ist Ihre BSI-Einschätzung zu Kaspersky?

Daneben werden eine größere Zahl von weiteren Russischen SW-Produkten incl. Open-Source Produkten , wie [redacted] für Datensicherung und Backup verwendet.
Wie ist hierzu Ihre BSI-Einschätzung

Im Voraus bersten Dank für Ihre zeitnahe Einschätzung

Viele Grüße

[redacted]

[redacted]

48

048_1_geschwärzt.pdf

Von:	Welsch, Günther
An:	GP Stab 1 - Strategische Kommunikation und Presse; GP Abteilung BL; GP Abteilung TK; GP Abteilung OC; Schabhüser, Gerhard; Schönbohm, Arne
Cc:	Caspers, Thomas; Samsel, Horst; Häger, Dirk; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Leitungsstab; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Referat KM 14 [redacted]; GP Referat BL 23; GP Abteilung KM; GP Fachbereich KM 1
Betreff:	AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Montag, 14. März 2022 08:53:00
Anlagen:	Kaspersky_Warnung_final.docx Warnung_Kaspersky_Begründung.pdf CDR_Kaspersky_Warnung_V8_ÄndKö.docx CDR_VS-NfD_Kaspersky_Begründung_V8_ErgSR_Än dKö.docx
Dringlichkeit:	Hoch

LK,
anbei finden Sie die auf Basis der Hinweise aus dem BMI aktualisierten Fassungen der Warnung vor Kaspersky und die Begründung zur Warnung. Die Änderungen betreffen nur kleinere Dinge. Zum Vergleich liegen die Dokumente mit Änderungsmarkierungen ebenfalls bei.

Es sind folgende Aktionen zu tätigen:

1. Ich bitte um kurzfristige Bestätigung der Mitzeichnung durch die Abteilungen TK, OC und BL.

2. Welche Stelle im BSI führt das Stellungnahmeverfahren von Kaspersky durch, bevor wir die Warnung aussprechen?

3. Frage an die Amtsleitung: In welcher Form wird die Übersendung an das BMI gewünscht? Erneuter Initiativbericht durch KM/KM14 oder werden Sie eine direkte Kommunikation mit AL CI aufnehmen?

4. Stab1 wird gebeten, die PM zu erstellen und mit Pressestelle BMI abzustimmen.

Viele Grüße
G. Welsch

Im Folgenden wird 016_0_geschwärzt.pdf zitiert.

Die Anlagen

- **CDR_Kaspersky_Warnung_V8_ÄndKö.docx und**
- **CDR_VS-NfD_Kaspersky_Begründung_V8_ErgSR_Än dKö.docx**

sind identisch mit den Anlagen zu 045.

048_1.1_Kaspersky_Warnung_final.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

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

Viren-Schutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Viren-Schutzsoftware 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. Viren-Schutzsoftware 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 entsprechende 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 Viren-Schutzsoftware 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 Viren-Schutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Viren-Schutzsoftware 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 Viren-Schutzsoftware) 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)
Fehler! Linkreferenz ungültig.
[2] Darstellung Risikostufen
Fehler! Linkreferenz ungültig.

048_1.2_Warnung_Kaspersky_Begründung_geschwärzt.pdf

Einstufung nach Schwärzung aufgehoben.

Referat KM 14 14. März 2022

Az. KM14-210 01 03 / VS-NfD

[redacted]

Betr. Bewertung von IT-Sicherheitsprodukten
hier: Warnung vor Kaspersky-Produkten nach § 7 BSIG

Bezug

Anlage Text der BSI-Warnung gemäß BSIG § 7

1) Vermerk zur Begründung der Warnung

A Begründung der Warnung nach § 7 Abs. 1 BSIG

Das BSI darf nach § 7 Abs. 1 BSIG u.a. vor Sicherheitslücken in informationstechnischen Produkten und Diensten öffentlich warnen. Sicherheitslücken in diesem Sinne sind nach § 2 Abs. 6 BSIG „*Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.*“ Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1.d BSIG). Dabei ist nach Meinung in der Literatur zwar noch ein Bezug zur Gefahrenvorsorge notwendig, aber keine konkrete Gefahrenlage mehr (vgl. Ritter-*Schulte,* Die Weiterentwicklung des IT-Sicherheitsgesetzes, Art. 1 Nr. 9 IT-SiG 2.0, Rn. 307). Solche Sicherheitseigenschaften von Produkten können sich auch aus der Struktur des Anbieters ergeben. Da hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI vor dem Einsatz des Produktes warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG).

Die Ereignisse rund um Kaspersky werden vom BSI seit Jahren aufmerksam verfolgt. Mehrere westliche Staaten wie USA und Niederlande warnen seit Jahren öffentlich vor Kaspersky und haben die Software für den Einsatz im Behördenumfeld gesperrt (Quellen werden nachgereicht). [redacted]

Der russische Angriff auf die Ukraine, der mit hybriden Mitteln - also auch im Cyberraum - geführt wird und von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt wurde, verändert die Lagebeurteilung. Russland ist kein demokratischer Rechtsstaat und sieht Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als Kontrahent an. Mit feindlichen Übergriffen auf deutsche Institutionen, Unternehmen und IT-Infrastrukturen ist daher zu rechnen. Russische Unternehmen wie Kaspersky könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden, zum anderen selbst Ziel massiver Cyberangriffe werden. Die Gefahr, dass Kaspersky in die kriegerischen Auseinandersetzungen hineingezogen wird, ist daher so groß, dass eine Warnung angemessen ist. Es muss damit gerechnet werden,

Einstufung nach Schwärzung aufgehoben.

dass Kaspersky nicht mehr die uneingeschränkte Kontrolle über seine Software und IT-Systeme hat bzw. diese in Kürze verlieren wird.

[redacted]

Bereits in den letzten Jahren wurden Fälle bekannt, in denen staatliche Stellen Einfluss auf Kaspersky genommen haben:

[redacted]

In den Jahren 2018 und 2019 wurden russische VPN-Anbieter gezwungen, bestimmte Verbindungen auf Anordnung der Regierung zu blocken. Während die meisten Anbieter die Kooperation verweigerten, kam Kaspersky den Anordnungen nach[2]:

"Although not all VPNs are banned, a 2018 law introduced fines for search engines that brought up results to proxy sites (including VPNs) that would give Russians access to prohibited content or instructions on how to get access to that content.
The following year, VPNs and search engines were compelled to block any websites that appeared on the federal government blacklist. Later, 10 VPN providers were ordered to hand over access to their servers or face being banned. Only one, Kaspersky Lab, which is based in Russia, agreed, while others - like ExpressVPN and NordVPN - shut down their Russian servers."

Neben dem BSI haben auch andere Länder und Organisationen ihre Risikobewertung angepasst. Frankreich hat beispielsweise eine vergleichbare Warnung veröffentlicht[3] [redacted] Die Teilnehmer waren sich einig, dass der Einsatz von Kaspersky-Produkten hoch problematisch ist. Zum Schutz ihrer IT-Systeme wurden daher automatische Updates abgestellt und Schritte eingeleitet, um die Software schnellstmöglich durch eine sicherere Alternative abzulösen.

Die in der Warnung beschriebenen Angriffsvektoren sind nicht neu. Im Folgenden einige Beispiele, die belegen, welchen Schaden ein Angreifer mit Viren-Schutzsoftware anrichten könnte:

[redacted]

[2]https://www.techradar.com/vpn/which-websites-and-services-are-banned-in-russia
[3]https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

- Am 10.06.2015 hat Kaspersky selbst in einer Pressemitteilung[4] mitgeteilt, dass das Unternehmensnetzwerk gehackt wurde und Angreifer mit teils neuen Methoden versucht haben, vertrauliche Daten zu stehlen, die dann für Angriffe auf die Kunden missbraucht werden könnten.
- Am 05. Januar 2012 hat die Hacker-Gruppe „The Lords of Dharmaraja“ geheimen Sourcecode von Symantec bei Pastebin veröffentlicht. Symantec hat die Echtheit des Codes bestätigt und die sicherheitsrelevanten Auswirkungen mit dem BSI-Präsidenten in einem vertraulichen Gespräch erörtert.
- Alle Hersteller von Viren-Schutzprogrammen hatten in der Vergangenheit Schwachstellen, die für Angriffe auf Kundensysteme hätten genutzt werden können. Mit Kenntnis des Sourcecode oder noch nicht veröffentlichter Schwachstellen wäre ein Angreifer nicht auf offiziell gemeldete Schwachstellen angewiesen, um einen Angriff durchzuführen. Wenn schon Schwachstellen ausreichen, um Systeme komplett stillzulegen, wäre dies mit einer Backdoor noch sehr viel leichter.
- Es sind zahlreiche Vorfälle bei allen Herstellern von Viren-Schutzsoftware bekannt, in denen eine fehlerhafte Erkennungssignatur Windows-Systemdateien als schädlich klassifiziert und damit das IT-System blockiert hat.
- Es sind auch Vorfälle bekannt, bei denen nach einem Signaturupdate bestimmte Schadprogramme irrtümlich nicht mehr detektiert wurden.
- Alle Viren-Schutzprogramme haben Funktionen eingebaut, mit denen sich Schadsoftwareausbrüche begrenzen lassen. Dazu können sie beliebige Dateien blockieren oder löschen. Auch in der Bundesverwaltung hat es bereits einen Sicherheitsvorfall gegeben, bei dem durch eine Fehlbedienung der "Outbreak-Prevention"-Funktion eine ganze Behörde für einen Tag lahmgelegt wurde.
- Bei Updates werden nicht immer nur Signaturen übertragen. Es ist auch möglich, dass größere Softwarebestandteile (z. B. Scan-Engines) aktualisiert werden müssen, um mit neuen Signaturen/Erkennungsverfahren kompatibel zu bleiben. Dem BSI sind Fälle bekannt, bei denen durch Updates eines Viren-Schutzprogramms neue Funktionen installiert oder Konfigurationen überschrieben wurden, ohne dass die Nutzer dies bemerken konnten. In der Folge wurde Kundendaten ohne Genehmigung an den Hersteller übertragen.

Derartige Vorfälle mussten alle Hersteller bereits vermelden. Sie sind immer unbeabsichtigt aufgrund von Fehlern oder Nachlässigkeiten geschehen. Eigene Entwickler oder Hacker, die in die Systeme des Herstellers eingedrungen sind, sind nicht auf Schwachstellen oder Fehler angewiesen, und könnten daher sehr einfach die folgenden Funktionen auf Kundensystemen implementieren:

- Zielsysteme analysieren (Systemeigenschaften, Hardwareeigenschaften, verwendete Software etc.)
- Daten zum Hersteller übertragen (z. B. Dateien, URLs)
- Dateien sperren oder löschen

Um die gewollte Funktionalität bieten zu können, laufen Viren-Schutzprogramme zudem mit hohen Systemrechten, schützen sich vor Veränderungen und haben Zugriff auf das gesamte Filesystem. Durch die hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig ist, könnten theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Manipulationen lassen sich auch temporär vornehmen und dadurch sehr gut tarnen. Beispielsweise könnte für wenige Stunden ein bestimmter Schadcode bewusst nicht erkannt werden, um anderen Angreifern den Weg zu bereiten.

Wenn die Kaspersky-Produkte für Angriffe entweder durch Anweisung der russischen Regierung oder durch staatliches Eindringen in deren Systeme instrumentalisiert werden, ist es daher möglich, dass auf die Systeme

[4]https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

auf denen Kaspersky-Produkte installiert sind, unberechtigt zugegriffen oder Einfluss genommen werden kann.

Kaspersky ist sich dieser Gefahren bewusst und hat in der Vergangenheit diverse Maßnahmen zur Vertrauensbildung ergriffen, die aber alle nicht geeignet sind, die aktuelle veränderte Gefahrenlage zu entschärfen:

- Kaspersky hat versucht, sich dem Einfluss russischer Behörden zu entziehen und betreibt eine Dateninfrastruktur in zwei Rechenzentren in Zürich zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden aus Europa, den Vereinigten Staaten und Kanada sowie in mehreren asiatisch-pazifischen Ländern. Für die Bereitstellung von Updates/Virensignaturen stehen bei Bedarf verschiedene Server in Europa zur Verfügung, unter anderem in Frankfurt.

  Es ist unerheblich, wo die Kundendaten gehostet werden. Entscheidend ist, wer Sourcecodeänderungen vornehmen und Signaturdaten erstellen kann und wie diese qualitätsgesichert und geprüft werden. Kaspersky kann nicht nachweisen, dass diese Prozesse komplett unabhängig vom russischen Hauptquartier durchgeführt werden. Es ist auch nicht transparent, wer administrativen Zugang zu den Systemen in Westeuropa hat. Aufgrund der Erfahrungen mit anderen Cloudanbietern ist es extrem unwahrscheinlich, dass die Rechenzentren in West-Europa komplett autark arbeiten und keine administrativen Eingriffe aus anderen Regionen erfolgen können.

- Die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren und Datendienste von Kaspersky wurden von zwei externen, unabhängigen Prüforganisationen bestätigt. Kaspersky hat das SOC-2-Audit (Service Organization Control for Service Organizations) Typ 1 durch einen Big-Four-Auditor erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigte. Darüber hinaus wurden Datendienste vom TÜV AUSTRIA nach ISO/IEC 27001:2013 zertifiziert.

  Eine Zertifizierung sagt nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus. Sie ist keine Garantie für den Ist-Zustand.

- Kaspersky sagt über sich selbst, als global agierendes privates Unternehmen (Sitz der Holding ist London, UK) keine Verbindungen zur russischen Regierung zu haben.

  Diese Aussage ist nicht glaubhaft. Kaspersky hat seinen Hauptsitz in Moskau und weist eine russische Eigentümerstruktur auf. Als eines der wichtigsten IT-Security-Unternehmen Russlands arbeitet Kaspersky eng mit Ermittlungsbehörden zusammen (s. o.). Wesentliche Teile der Belegschaft arbeiten daher in Russland oder haben familiäre Bindungen in Russland und sind daher dem direkten Einfluss und Druck der Behörden ausgesetzt.

- Kaspersky unterliegt nach eigenen Angaben nicht dem russischen System operativer Ermittlungsmaßnahmen (SORM) oder anderen ähnlichen Gesetzen und sei deswegen nicht zur Auskunftserteilung verpflichtet.

  Diese faktischen Einflussmöglichkeiten der russischen Regierung entfallen nicht deswegen, weil Kaspersky nach russischem Recht keinen Mitwirkungspflichten unterliegt (zu den Pflichten s. Gutachten Prof. Hober).

  Angesichts des mit dem Einmarsch in die Ukraine erfolgten eklatanten Bruchs von internationalem Recht durch Russland muss damit gerechnet werden, dass die russische Regierung auch gegen geltendes russisches Recht verstößt, wenn ihr dies opportun erscheint.

Soweit das BSI die Maßnahmen von Kaspersky in der Vergangenheit für ausreichend hielt, um die Produkte von Kaspersky weiter einsetzen zu können, lag dem die Annahme zu Grunde, dass die russische Regierung keine Schritte einleiten würde, die bei Bekanntwerden (bzw. Entdeckung) sowohl Kaspersky als auch der russischen Regierung wirtschaftlichen Schaden und einen Reputationsverlust zufügen würden. Angesichts

der nunmehr offenen Konfrontation Russlands mit der EU und den NATO-Staaten und der Hinnahme selbst existenzvernichtender Sanktionen für russische Unternehmen, kann diese Grundannahme nicht weiter aufrechterhalten werden. Wir müssen nunmehr davon ausgehen, dass die russische Regierung in der jetzigen Situation keine Rücksicht mehr auf das internationale Geschäft und die Reputation von Kaspersky nehmen würde. [redacted] Als Konsequenz sollten diese Einrichtungen keine Produkte des Herstellers Kaspersky einsetzen.

Eine Warnung des BSI ist auch mit dem Grundsatz der Verhältnismäßigkeit vereinbar: zum einen weist das BSI in seiner Warnung darauf hin, dass private Anwender weniger bedroht sein können, was zur Folge haben kann, dass diese die Produkte von Kaspersky weiterhin nutzen. Ein erfolgreicher Angriff auf ein KRITIS-Unternehmen könnte jedoch die Versorgung der Bevölkerung mit lebenswichtigen Diensten wie Wasser oder Energie beeinträchtigen und bis hin zu einem Ausnahmezustand führen. Das potentielle Schadensrisiko ist hier mithin enorm. Dem steht das Interesse des einzelnen Herstellers (hier Kaspersky) an der freien Ausübung seines Gewerbes gegenüber. Hier ist zwar zu berücksichtigen, dass eine Warnmeldung mit hoher Wahrscheinlichkeit spürbare Folgen auf die wirtschaftliche Tätigkeit des Herstellers in Deutschland hätte. Allerdings überwiegt hier der Schutz der Allgemeinheit aufgrund der besonderen Schwere des Schadensrisikos das Interesse des einzelnen Herstellers.

Fazit:

Durch manipulierte Viren-Schutzprogramme hat ein Angreifer nahezu unbegrenzte Möglichkeiten, IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste Vorfall öffentlich bekannt wird. Vielmehr ist die Warnung zum jetzigen Zeitpunkt angezeigt, um rechtzeitig präventiv zu handeln und die relevanten Anwender vor potentiellem Schaden zu bewahren. Mildere Mittel zum Schutz der Informationssicherheit sind nicht ersichtlich.

B Vorherige Stellungnahmemöglichkeit nach § 7 Abs. 1 a Nr. 1 BSIG

Kaspersky sollte vor der Veröffentlichung nur mit kurzer Frist informiert und Gelegenheit zur Stellungnahme gegeben werden. Es ist Gefahr im Verzug. Hacker könnten ihre Vorbereitungen bereits abgeschlossen haben und nur noch auf einen Einsatzbefehl warten. Es ist nicht ersichtlich, dass Kaspersky eine Möglichkeit hätte, durch technische oder sonstige Maßnahmen die Risikoeinschätzung positiv zu beeinflussen. Es ist nicht wahrscheinlich, dass der Hersteller an dem zugrundeliegenden strukturellen Sicherheitsproblem etwas ändern kann, da er kaum Einfluss auf die Gefährdung hat. Angesichts der Gefährdungslage erscheint eine kurze Frist daher verhältnismäßig und fachlich angemessen.

Im Auftrag

[redacted]

49

Der gesamte Vorgang ist als

VS – NUR FÜR DEN DIENSTGEBRAUCH

eingestuft.

50

050_geschwärzt.pdf

Von: Schönbohm, Arne
An: GP Abteilung TK; Welsch, Günther; GP Abteilung OC; GP Stab 1 - Strategische Kommunikation und Presse; Schabhüser, Gerhard; GP Abteilung BL
Cc: Samsel, Horst; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Leitungsstab; Häger, Dirk; GP Abteilung KM [redacted] GP Referat KM 14; GP Fachbereich KM 1; GP Referat BL 23; Caspers, Thomas
Betreff: AW: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 14. März 2022 09:00:21

Bitte an das Leitungsbüro, diese Informationen nach Freigabe durch die AL an AL CI und in Kopie an Herrn Sts. Richter verteilen. Die offiziellen Verlautbarungen sollten bitte morgen ab 9:00 erfolgen.

Mit freundlichen Grüßen

Arne Schönbohm

- via SecurePIM gesendet -

Im Folgenden wird 048_1_geschwärzt.pdf zitiert.

51

051_geschwärzt.pdf

Von: GP Abteilung TK
An: Welsch, Günther; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Abteilung BL; GP Abteilung OC
Cc: Schönbohm, Arne; Schabhüser, Gerhard; GP Stab 1 - Strategische Kommunikation und Presse; Caspers, Thomas; Samsel, Horst; Häger, Dirk; GP Leitungsstab; GP Referat KM 14; [redacted] GP Referat BL 23; GP Abteilung KM; GP Fachbereich KM 1
Betreff: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 14. März 2022 09:42:11
Anlagen: Kaspersky_Warnung_final.docx

Liebe Kolleginnen und Kollegen,

Abteilung TK zeichnet mit.

Im Text der finalen Warnung empfehle ich noch folgende kleineren Änderungen vorzunehmen:

"Ein russischer IT-Hersteller kann selbst entsprechende 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."
--> "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."

(Durch die Streichung des ursprünglich vorhergehenden Satzes durch BMI AL CI ist der Bezug von „entsprechende“ nicht mehr klar, daher die Änderung, sowie Ergänzung eines noch fehlenden Kommas.)

Viele Grüße

Thomas Caspers

--
Thomas Caspers
Abteilungsleiter
Technik-Kompetenzzentren

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
E-Mail: thomas.caspers@bsi.bund.de
Internet: www.bsi.bund.de

Im Folgenden wird 048_1_geschwärzt.pdf zitiert. Der Anhang ist identisch mit 048_1.1_Kaspersky_Warnung_final.pdf.

52

052_0.pdf

Von:	GP Abteilung OC
An:	Welsch, Günther; GP Stab 1 - Strategische Kommunikation und Presse; GP Abteilung BL; GP Abteilung TK; Schabhüser, Gerhard; Schönbohm, Arne
Cc:	GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Leitungsstab; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Referat KM 14; GP Referat BL 23; GP Abteilung KM; GP Fachbereich KM 1
Betreff:	AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Montag, 14. März 2022 09:57:13

Hallo Günther,

ich zeichne mit (inklusive der Vorschläge vom Thomas).

Zur Frage "Welche Stelle im BSI führt das Stellungnahmeverfahren von Kaspersky durch, bevor wir die Warnung aussprechen?" votiere ich für BL23 mit Unterstützung von KM14. Es ist ein formaler Verwaltungsakt, und da hatte sich CERT-Bund bei den bisherigen Warnungen natürlich eng mit BL23 abgestimmt. Da es hier weniger um Technik geht, erscheint mit die Unterstützung durch das Fachreferates KM14 hier eher nachrangig.

Ciao Dirk

Im Folgenden wird 048_1_geschwärzt.pdf zitiert.

53

053_geschwärzt.pdf

Von: Welsch, Günther
An: GP Referat BL 23
Cc: GP Referat KM 14
Betreff: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 14. März 2022 10:13:00

Hallo [redacted],

gibt es eine rechtliche Hilfestellung, mit welchem Text das Unternehmen angeschrieben wird? Welche Stelle im Unternehmen ist zu adressieren, z.B. der Vertriebler, der uns bekannt ist, oder muss die Geschäftsleitung in Brief/Text/Mail-Form angeschrieben werden?

Wenn wir eine Stellungnahme erhalten (sollten wir eine Frist setzen?), muss KM14 dann noch eine ergänzende Bewertung in den MZ-Prozess der Abteilungen geben, bevor alle Formalvorgaben erfüllt sind?

Viele Grüße
Günther Welsch

-----Ursprüngliche Nachricht-----
Von: GP Referat BL 23 <referat-bl23@bsi.bund.de>
Gesendet: Montag, 14. März 2022 10:05
An: GP Abteilung OC <abteilung-oc@bsi.bund.de>; GP Abteilung BL <abteilung-bl@bsi.bund.de>
Cc: GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; GP Leitungsstab <leitungsstab@bsi.bund.de>; GP Stab 3 - Strategie und Leitungsunterstuetzung <stab3@bsi.bund.de>; GP Referat KM 14 <referat-km14@bsi.bund.de>; GP Abteilung KM <abteilung-km@bsi.bund.de>; GP Fachbereich KM 1 <fachbereich-km1@bsi.bund.de>; Schönbohm, Arne <arne.schoenbohm@bsi.bund.de>; Schabhüser, Gerhard <gerhard.schabhueser@bsi.bund.de>; GP Abteilung TK <abteilung-tk@bsi.bund.de>; GP Stab 1 - Strategische Kommunikation und Presse <stab1@bsi.bund.de>; Welsch, Günther <guenther.welsch@bsi.bund.de>; GP Referat BL 24 <referat-bl24@bsi.bund.de>; [redacted]@bsi.bund.de>
Betreff: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware

Hallo Dirk,

das Stellungnahmeverfahren ist stets durch die OE durchzuführen, die für die Warnung zuständig ist, da es dazu dient, mögliche fachliche(!) Einwände gegen die Warnung vorzubringen. Die Juristen sind bei formalen Akten des BSI erst die Widerspruchsstelle des BSI daher schon formal nicht für den Erlass von Ausgangsescheiden zuständig. Selbstverständlich unterstützen wir durch Beratung, wie das auch bisher schon bei den Warnungen von CERT der Fall war.

Ich verstehe ehrlich gesagt auch nicht, warum wir bei dieser Warnung von dem etablierten und abgestimmten Warnprozess abweichen sollte.

Beste Grüße
[redacted]

Im Folgenden wird 052_0.pdf zitiert.

54

054_geschwärzt.pdf

Von: [redacted]
An: Welsch, Günther; GP Referat BL 23
Cc: GP Referat KM 14 [redacted]
Betreff: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 14. März 2022 10:31:39

Hallo Herr Welsch,

hier helfe ich gerne weiter. Das Template für die Benachrichtigung findet sich in der Hausanordnung für Warnungen: http://intranet.bsi.de/verwaltung/Hausanordnungen/Hausanordnung_Warnungen_nach_BSIG.pdf

Dort ab S. 35 f. Da wir Gefahr in Verzug annehmen, ist der entsprechende Baustein zu nutzen. Wenn keine direkten Ansprechpartner bekannt sind, sollte
die Geschäftsleitung / PR und Unternehmenskommunikation adressiert werden. Mail wird ob der Eilbedürftigkeit ausreichend sein. Eine Frist ist zu setzen, vgl. Hausanordnung.

WENN die Stellungnahme durchschlagende neue Tatsachen enthält, so müssten diese nochmals bewertet werden (Bsp.: "Eine Einflussnahme durch Regierungsorgane ist nicht möglich, weil [KONKRETE GRÜNDE!]). Wird lediglich "ins Blaue hinein" behauptet, dass eine solche Einflussnahme nicht möglich sei, so wird das unsere Bewertung nicht mehr ändern. Gleiches gilt natürlich auch für etwaige technische Maßnahmen von Kaspersky, die eine Einflussnahme verhindern sollen/können.

Mit freundlichen Grüßen
im Auftrag

[redacted]

Referat BL 23
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Im Folgenden wird 053_geschwärzt.pdf zitiert.

55

055_geschwärzt.pdf

Von:	GP Abteilung BL
An:	GP Abteilung KM
Cc:	GP Abteilung BL; GP Fachbereich BL 2; GP Referat BL 23; GP Abteilung TK; GP Abteilung OC; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Leitungsstab; Schönbohm, Arne; Schabhüser, Gerhard; GP Referat KM 14; [redacted]
Betreff:	WG: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Montag, 14. März 2022 10:45:47
Anlagen:	Kaspersky_Warnung_final.docx Warnung_Kaspersky_Begründung.pdf CDR_Kaspersky_Warnung_V8_ÄndKö.docx CDR_VS-NfD_Kaspersky_Begründung_V8_ErgSR_Än dKö.docx
Dringlichkeit:	Hoch

---

1. Mitzeichnung für BL
2. Auch der weitere "Schriftverkehr" mit dem BMI und auch der mit dem betroffenen Unternehmen sollte durch den Federführer (KM) wahrgenommen werden. BL unterstützt gern.

Mit freundlichen Grüßen
Im Auftrag

Horst Samsel

Abteilungsleiter BL

Abteilung BL - Beratung für Bund, Länder und Kommunen
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: abteilung-bl@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Im Folgenden wird 048_1_geschwärzt.pdf inkl. der Anhänge zitiert.

56

056_geschwärzt.pdf

Von: GP Abteilung KM
An: [redacted]
Betreff: Anschrift Kaspersky
Datum: Montag, 14. März 2022 11:08:00

Hallo [redacted],

das scheint die offizielle Adresse von Kaspersky zu sein:

European Headquarters
2 Kingdom Street
London
W2 6BD
United Kingdom
+44 (0)20 3549 3499
info@kaspersky.com
www.kaspersky.co.uk

Wenn wir parallel den Vertriebler/Politikvertreter anschreiben, müsste es reichen.

[redacted] <kaspersky.policy.germany@kasp-cyber.com>

57

057_0_geschwärzt.pdf

Von: [redacted] im Auftrag von GP Stab 1 - Strategische Kommunikation und Presse
An: Schabhüser, Gerhard; Schönbohm, Arne
Cc: GP Leitungsstab; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Referat KM 14; [redacted]; GP Referat BL 23; GP Abteilung KM; GP Abteilung OC; GP Abteilung TK; GP Abteilung BL; GP Stab 1 - Strategische Kommunikation und Presse
Betreff: EILT: ZUR FREIGABE: Pressemitteilung zur § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 14. März 2022 13:26:35
Anlagen: 2022_03_15_Kaspersky_Warnung.docx

Hallo Herr Schönbohm,

anbei mit der Bitte um kurzfristige Prüfung und Freigabe der Entwurf der Pressemitteilung zur anstehenden Kaspersky-Warnung. Wir haben uns hier eng an die fachliche Warnung gehalten und wie vorab besprochen diesmal auch auf ein Zitat verzichtet.

Nach Ihrer Freigabe stellen wir die PM auch BMI Presse zur Verfügung.

Danke und viele Grüße
[redacted]

Im Folgenden wird 048_1_geschwärzt.pdf zitiert.

057_1_2022_03_15_Kaspersky_Warnung.pdf

BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten

Bonn, 15. März 2022. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.

Antivirensoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, verfügt 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. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur.

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs verbunden. Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen 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.

Alle Nutzerinnen und Nutzer der Virenschutzsoftware können von solchen Operationen betroffen sein. Unternehmen und Behörden mit besonderen Sicherheitsinteressen und Betreiber Kritischer Infrastrukturen sind in besonderem Maße gefährdet. Sie haben die Möglichkeit, sich vom BSI oder von den zuständigen Verfassungsschutzbehörden beraten zu lassen.

Unternehmen und andere Organisationen sollten den Austausch wesentlicher Bestandteile ihrer IT-Sicherheitsinfrastruktur sorgfältig planen und umsetzen. Würden IT-Sicherheitsprodukte und insbesondere Virenschutzsoftware ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der Umstieg auf andere Produkte ist mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden. Das BSI empfiehlt, eine individuelle Bewertung und Abwägung der aktuellen Situation vorzunehmen und dazu gegebenenfalls vom BSI zertifizierte IT-Sicherheitsdienstleister hinzuzuziehen.

58

058_0_geschwärzt.pdf

Von: [redacted]
An: GP Abteilung KM; GP Referat KM 14; GP Referat BL 23 [redacted]
Cc: [redacted]
Betreff: AW: WICHTIG: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 14. März 2022 13:34:11
Anlagen: Anschreiben_Kaspersky_BL23.docx

Hallo Herr Welsch,
[redacted]

anbei die nur ganz marginal geänderte Fassung. Ich würde vermuten, dass unser Anschreiben ohnehin bei Kaspersky intern an die geeigneten Kanäle verteilt wird. Passt alles.

Viele Grüße

[redacted]

Referat BL 23
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

-----Ursprüngliche Nachricht-----
Von: GP Abteilung KM <abteilung-km@bsi.bund.de>
Gesendet: Montag, 14. März 2022 13:14
An: GP Referat KM 14 <referat-km14@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>; [redacted]
Betreff: AW: WICHTIG: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Priorität: Hoch

LK,

ich habe mal umformuliert, damit es etwas formaler wirkt. Den Bezug zum Schreiben [redacted] habe ich entfernt. Den brauchen wir nicht, denke ich.

Bitte kurzfristig durchsehen!

Gruß
G. Welsch

-----Ursprüngliche Nachricht-----
Von: GP Referat KM 14 <referat-km14@bsi.bund.de>
Gesendet: Montag, 14. März 2022 13:09
An: GP Abteilung KM <abteilung-km@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>
Betreff: WICHTIG: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware

Hallo,

im Anschreiben ist ein Fehler: Die Bezugs-E-Mail ist vom 26.02., nicht vom 28.02! (Am 28.02. kam die E-Mail, dass wir Kaspersky-Produkte umsonst einsetze dürfen.)

VG

-----Ursprüngliche Nachricht-----
Von: GP Referat KM 14
Gesendet: Montag, 14. März 2022 12:31
An: GP Abteilung KM <abteilung-km@bsi.bund.de>; GP Referat BL 23 <referat-bl23@bsi.bund.de>
Betreff: AW: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware

Hallo,

anbei ein Entwurf des Anschreibens zur QS.

Versand bei E-Mail an info@kaspersky.com und [redacted]@kaspersky.com

Die Warnung musste ich komplett neu setzen, da das BMI unsere Dokumentenvorlage beschädigt hatte.

Mit freundlichen Grüßen

[redacted]

-----Ursprüngliche Nachricht-----
Von: Welsch, Günther <guenther.welsch@bsi.bund.de>
Gesendet: Montag, 14. März 2022 10:33
An: GP Referat KM 14 <referat-km14@bsi.bund.de>
Betreff: WG: § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware

KM14 zur weiteren Bearbeitung.

Im Folgenden wird 054_geschwärzt.pdf zitiert.

058_1_Anschreiben_Kaspersky_BL23_geschwärzt.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital·Sicher·BSI·

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Kaspersky
European Headquarters
2 Kingdom Street
London
W2 6BD
United Kingdom

nachrichtlich:
[redacted]

Dr. Günther Welsch
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Postanschrift:
Postfach 20 03 63
53133 Bonn
Tel. +49 228 99 9582[redacted]
Fax +49 228 99 10 9582[redacted]
abteilung-km@bsi.bund.de
www.bsi.bund.de

Betreff: BSI Warnung nach § 7 BSIG: Gelegenheit~~Bitte~~ zur ~~um~~ Stellungnahme

~~Bezug: E-Mail von H. Michels an den BSI-Präsidenten vom 28.02.~~
Geschäftszeichen: KM14-210 01 03
Anlage: Entwurf der Warnmeldung
Datum: 20.04.2022
Seite 1 von 2

Sehr geehrte Damen und Herren,

das Bundesamt für Sicherheit in der Informationstechnik (BSI) analysiert und bewertet ~~ist~~ regelmäßig im Rahmen seiner Aufgabenwahrnehmung die Sicherheit von Software und IT-Sicherheitsprodukten, so z.B. Viren-Schutzsoftware.

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. ~~und Diensten öffentlich warnen. Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1 d BSIG).~~

Im Zuge der kriegerischen Auseinandersetzungen zwischen Russland und der Ukraine ist eine neue Sicherheitslage für die Bundesrepublik Deutschland entstanden. Die damit einhergehenden Bedrohungen werden im Rahmen des IT-Risikomanagements mit Blick auf Software und IT-Sicherheitsprodukte neu bewertet.

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

Bundesamt
für Sicherheit in der
Informationstechnik

~~Einstufung wählen oder Eler~~ Deutschland
Digital·Sicher·BSI·

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.

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).

~~Kaspersky-Produkten anlässlich des Krieges zwischen Russland und der Ukraine analysiert und bewertet. Wir haben dabei Ihre Argumente in der Bezugs-E-Mail angemessen berücksichtigt.~~
Es besteht aufgrund der besonderen Sicherheitssituation Gefahr im Verzug. Das BSI hält~~at~~ daher eine unverzügliche Reaktion für angemessen. ~~zu handeln.~~ Wir beabsichtigen morgen, Dienstag, den 15. März 2022 um 9:00 Uhr eine öffentlichkeitswirksame Produktwarnung zu publizieren.

Formatiert: Schriftart: Fett

Wir gewähren dem Unternehmen Kaspersky eine Frist bis heute,

Montag den 14. März 2022 um 16:30 Uhr,

Formatiert: Schriftart: Fett

Formatiert: Zentriert

uns eine Stellungnahme in der Sache zukommen zu lassen. Sie haben damit die Möglichkeit, für Sie günstige Sachargumente zum weiteren Entscheidungsprozess im BSI beizutragen. Über unsere Entscheidung werden wir Sie informieren.

~~Wir sind leider zu dem Ergebnis gekommen, dass der Einsatz Ihrer Produkte mit erheblichen Risiken verbunden und nach unserer Einschätzung Gefahr im Verzug ist. Daher werden wir morgen gemäß unseres Auftrags (BSIG §7) eine öffentlichkeitswirksame Produktwarnung veröffentlichen.~~

~~Das BSI darf nach § 7 Abs. 1 BSIG u. a. vor Sicherheitslücken in informationstechnischen Produkten und Diensten öffentlich warnen. Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1 d BSIG). Da hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI vor dem Einsatz des Produktes warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG).~~

~~Wir informieren Sie hiermit über unsere Absicht, um Ihnen die Gelegenheit zu bieten, kurzfristig bis heute 16:00 Uhr neue Argumente zu liefern, um unsere Einschätzung der Gefahrenlage zu entkräften.~~
~~Sofern sich die uns vorliegenden Informationen nicht wesentlich ändern, beabsichtigen wir aufgrund der Einschätzung der Gefährdungslage die Produktwarnung am15.03.2022 um 9:00 Uhr zu veröffentlichen.~~

Mit freundlichen Grüßen

Im Auftrag

Dr. Günther Welsch

59

059_0_geschwärzt.pdf

Von:	GP Abteilung KM
An:	"info@kaspersky.com"; "kaspersky.policy.germany@kasp-cyber.com"
Cc:	GP Geschaeftszimmer_KM; Welsch, Günther
Betreff:	BSI Warnung nach § 7 BSIG: Gelegenheit zur Stellungnahme
Datum:	Montag, 14. März 2022 13:51:00
Anlagen:	Kaspersky_Warnung_Entwurf_Kaspersky.pdf Anschreiben_Kaspersky_BSI_Warnung.pdf
Dringlichkeit:	Hoch

An:

Kaspersky
European Headquarters
2 Kingdom Street
London
W2 6BD
United Kingdom

nachrichtlich:
[redacted]
Head of Public Affairs Europe

Sehr geehrte Damen und Herren,

das Bundesamt für Sicherheit in der Informationstechnik (BSI) analysiert und bewertet regelmäßig im Rahmen seiner Aufgabenwahrnehmung die Sicherheit von Software und IT-Sicherheitsprodukten, so z.B. Viren-Schutzsoftware.

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.

Im Zuge der kriegerischen Auseinandersetzungen zwischen Russland und der Ukraine ist eine neue Sicherheitslage für die Bundesrepublik Deutschland entstanden. Die damit einhergehenden Bedrohungen werden im Rahmen des IT-Risikomanagements mit Blick auf Software und IT-Sicherheitsprodukte neu bewertet.

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.

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).

Es besteht aufgrund der besonderen Sicherheitssituation Gefahr im Verzug. Das BSI hält daher eine unverzügliche Reaktion für angemessen. Wir beabsichtigen morgen, Dienstag, den 15. März 2022 um 9:00 Uhr eine öffentlichkeitswirksame Produktwarnung zu publizieren.

Wir gewähren dem Unternehmen Kaspersky eine Frist bis heute,

Montag den 14. März 2022 um 17:00 Uhr,

uns eine Stellungnahme in der Sache zukommen zu lassen. Sie haben damit die Möglichkeit, für Sie günstige Sachargumente zum weiteren Entscheidungsprozess im BSI beizutragen. Über unsere Entscheidung werden wir Sie informieren.

Mit freundlichen Grüßen,
im Auftrag

Dr. Günther Welsch

--- --- --- --- --- --- --- ---
Dr. Günther Welsch
Abteilungsleiter KM
Bundesamt für Sicherheit in der Informationstechnik
53175 Bonn

Tel: 0228 9582 [redacted]
Mobil [redacted]

059_1.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

Viren-Schutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Viren-Schutzsoftware 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. Viren-Schutzsoftware 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 Viren-Schutzsoftware 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 Viren-Schutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Viren-Schutzsoftware 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 Viren-Schutzsoftware) 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/DasBSI/Gesetz/gesetz_node.html
[2] Darstellung Risikostufen
https://www.cert-bund.de/risk

059_2_geschwärzt.pdf

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Kaspersky
European Headquarters
2 Kingdom Street
London
W2 6BD
United Kingdom

nachrichtlich:
[redacted]
Head of Public Affairs Europe

Dr. Günther Welsch
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +49 228 99 9582[redacted]
Fax +49 228 99 10 9582[redacted]

abteilung-km@bsi.bund.de

www.bsi.bund.de

Betreff: BSI Warnung nach § 7 BSIG: Gelegenheit zur Stellungnahme

Geschäftszeichen: KM14-210 01 03
Anlage: Entwurf der Warnmeldung
Datum: 14.03.2022
Seite 1 von 2

Sehr geehrte Damen und Herren,

das Bundesamt für Sicherheit in der Informationstechnik (BSI) analysiert und bewertet regelmäßig im Rahmen seiner Aufgabenwahrnehmung die Sicherheit von Software und IT-Sicherheitsprodukten, so z.B. Viren-Schutzsoftware.

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.

Im Zuge der kriegerischen Auseinandersetzungen zwischen Russland und der Ukraine ist eine neue Sicherheitslage für die Bundesrepublik Deutschland entstanden. Die damit einhergehenden Bedrohungen werden im Rahmen des IT-Risikomanagements mit Blick auf Software und IT-Sicherheitsprodukte neu bewertet.

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.

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).

Es besteht aufgrund der besonderen Sicherheitssituation Gefahr im Verzug. Das BSI hält daher eine unverzügliche Reaktion für angemessen. Wir beabsichtigen morgen, **Dienstag, den 15. März 2022 um 9:00 Uhr** eine öffentlichkeitswirksame Produktwarnung zu publizieren.

Wir gewähren dem Unternehmen Kaspersky eine Frist bis heute,

Montag den 14. März 2022 um 17:00 Uhr,

uns eine Stellungnahme in der Sache zukommen zu lassen. Sie haben damit die Möglichkeit, für Sie günstige Sachargumente zum weiteren Entscheidungsprozess im BSI beizutragen. Über unsere Entscheidung werden wir Sie informieren.

Mit freundlichen Grüßen

Im Auftrag

Dr. Günther Welsch

60

060_0.pdf

Von:	Welsch, Günther
An:	Schönbohm, Arne; Schabhüser, Gerhard
Cc:	GP Referat KM 14; GP Referat BL 23; GP Referat WG 21; GP Abteilung BL; GP Abteilung OC; GP Abteilung WG; GP Abteilung TK; GP Leitungsstab; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Stab 1 - Strategische Kommunikation und Presse
Betreff:	WG: BSI Warnung nach § 7 BSIG: Gelegenheit zur Stellungnahme
Datum:	Montag, 14. März 2022 13:57:00
Anlagen:	Kaspersky_Warnung_Entwurf_Kaspersky.pdf Anschreiben_Kaspersky_BSI_Warnung.pdf
Dringlichkeit:	Hoch

Hallo Herr Schönbohm, halle Gerd,

1) Kaspersky ist nun von mir angeschrieben worden. Ich habe eine Rückäußerungsfrist bis 17:00 Uhr eingeräumt.

2) Parallel dazu liegt seitens Stab1 eine PM vor. Die Abstimmung mit Presse BMI steht noch aus.

3) Sobald die Stellungnahme seitens Kaspersky eingeht, werde ich eine Nachbewertung über KM14 mit nachfolgender MZ durch OC und BL vorlegen. Ich gehe davon aus, dass wir die Warnung aussprechen werden.

4) Die Dokumente stelle ich dann dem Leitungsstab zur Verfügung, der von Ihnen beauftragt ist, die Informationen an Hr. Könen und St R zu übermitteln.

Sofern Sie weiteren Support seitens KM benötigen, stehen wir gerne zur Verfügung.

Beste Grüße
Günther Welsch

Im Folgenden wird 059_0_geschwärzt.pdf (inkl. Anhängen) zitiert.

61

061_geschwärzt.pdf

Von:	Schönbohm, Arne
An:	GP Stab 1 - Strategische Kommunikation und Presse [redacted] Schabhüser, Gerhard
Cc:	GP Stab 1 - Strategische Kommunikation und Presse; GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Abteilung TK; GP Leitungsstab; GP Abteilung KM; [redacted] GP Referat KM 14; GP Abteilung OC; GP Abteilung BL; GP Referat BL 23
Betreff:	AW: EILT: ZUR FREIGABE: Pressemitteilung zur § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Montag, 14. März 2022 14:29:51

Freigabe

Mit freundlichen Grüßen

Arne Schönbohm

- via SecurePIM gesendet -

Im Folgenden wird 057_0_geschwärzt.pdf zitiert.

62

062_0_geschwärzt.pdf

Von: GP Referat KM 14
An: CI1@bmi.bund.de
Cc: [redacted]@bmi.bund.de; GP Abteilung KM
Betreff: Kaspersky: Aktuelle Unterlagen
Datum: Montag, 14. März 2022 15:29:17
Anlagen: Kaspersky_Warnung_Entwurf_Kaspersky.pdf
Warnung_Kaspersky_Begründung.pdf
2022_03_15_Kaspersky_Warnung_Pressemeldung.docx
Dringlichkeit: Hoch

Liebe Kolleginnen und Kollegen,

anbei finden Sie den aktuellen Entwurf der Warnung sowie die Begründung und den von Herrn Schönbohm Entwurf der Pressemeldung. Wir haben alle Änderungen von Herrn Könen übernommen und lediglich die folgende Änderung vorgenommen:

Ersetzt: "Ein russischer IT-Hersteller kann selbst entsprechende 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."

Neu: "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."

(Durch die Streichung des ursprünglich vorhergehenden Satzes durch BMI AL CI ist der Bezug von „entsprechende“ nicht mehr klar, daher die Änderung.)

Herr Dr. Welsch hat heute Kaspersky (Sitz in London und [redacted]) über die bevorstehende Warnung informiert und bis 17:00 Uhr Zeit für eine Stellungnahme eingeräumt. Sollte Kaspersky keine neuen Argumente liefern, wird die Warnung morgen früh um 9:00 Uhr veröffentlicht.

Mit freundlichen Grüßen

Im Auftrag

[redacted]
Referatsleiter

_____
Referat KM 14 - IT-Sicherheitssysteme und -produkte
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 -189
53175 Bonn

Telefon: +49 (0)228 99 9582[redacted]
Mobil: +49[redacted]
E-Mail: [redacted]@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Alle Informationen zum Umgang mit Ihren personenbezogenen Daten finden Sie hier:
http://bsi.bund.de/datenschutz

062_1_Kaspersky_Warnung_Entwurf_Kaspersky.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

Viren-Schutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Viren-Schutzsoftware 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. Viren-Schutzsoftware 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 Viren-Schutzsoftware 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 Viren-Schutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Viren-Schutzsoftware 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 Viren-Schutzsoftware) 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/DasBSI/Gesetz/gesetz_node.html
[2] Darstellung Risikostufen
https://www.cert-bund.de/risk

062_2_Warnung_Kaspersky_Begründung_geschwärzt.pdf

Referat KM 14 14. März 2022

Az. KM14-210 01 03 / VS-NfD

[redacted]

Betr. Bewertung von IT-Sicherheitsprodukten
hier: Warnung vor Kaspersky-Produkten nach § 7 BSIG

Bezug

Anlage Text der BSI-Warnung gemäß BSIG § 7

1) Vermerk zur Begründung der Warnung

A Begründung der Warnung nach § 7 Abs. 1 BSIG

Das BSI darf nach § 7 Abs. 1 BSIG u.a. vor Sicherheitslücken in informationstechnischen Produkten und Diensten öffentlich warnen. Sicherheitslücken in diesem Sinne sind nach § 2 Abs. 6 BSIG „*Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.*“ Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1.d BSIG). Dabei ist nach Meinung in der Literatur zwar noch ein Bezug zur Gefahrenvorsorge notwendig, aber keine konkrete Gefahrenlage mehr (vgl. Ritter-*Schulte,* Die Weiterentwicklung des IT-Sicherheitsgesetzes, Art. 1 Nr. 9 IT-SiG 2.0, Rn. 307). Solche Sicherheitseigenschaften von Produkten können sich auch aus der Struktur des Anbieters ergeben. Da hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI vor dem Einsatz des Produktes warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG).

Die Ereignisse rund um Kaspersky werden vom BSI seit Jahren aufmerksam verfolgt. Mehrere westliche Staaten wie USA und Niederlande warnen seit Jahren öffentlich vor Kaspersky und haben die Software für den Einsatz im Behördenumfeld gesperrt (Quellen werden nachgereicht). [redacted]

Der russische Angriff auf die Ukraine, der mit hybriden Mitteln - also auch im Cyberraum - geführt wird und von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt wurde, verändert die Lagebeurteilung. Russland ist kein demokratischer Rechtsstaat und sieht Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als Kontrahent an. Mit feindlichen Übergriffen auf deutsche Institutionen, Unternehmen und IT-Infrastrukturen ist daher zu rechnen. Russische Unternehmen wie Kaspersky könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden, zum anderen selbst Ziel massiver Cyberangriffe werden. Die Gefahr, dass Kaspersky in die kriegerischen Auseinandersetzungen hineingezogen wird, ist daher so groß, dass eine Warnung angemessen ist. Es muss damit gerechnet werden,

Einstufung nach Schwärzung aufgehoben.

dass Kaspersky nicht mehr die uneingeschränkte Kontrolle über seine Software und IT-Systeme hat bzw. diese in Kürze verlieren wird.

[redacted]

Bereits in den letzten Jahren wurden Fälle bekannt, in denen staatliche Stellen Einfluss auf Kaspersky genommen haben:

[redacted]

In den Jahren 2018 und 2019 wurden russische VPN-Anbieter gezwungen, bestimmte Verbindungen auf Anordnung der Regierung zu blocken. Während die meisten Anbieter die Kooperation verweigerten, kam Kaspersky den Anordnungen nach[2]:

"Although not all VPNs are banned, a 2018 law introduced fines for search engines that brought up results to proxy sites (including VPNs) that would give Russians access to prohibited content or instructions on how to get access to that content.
The following year, VPNs and search engines were compelled to block any websites that appeared on the federal government blacklist. Later, 10 VPN providers were ordered to hand over access to their servers or face being banned. Only one, Kaspersky Lab, which is based in Russia, agreed, while others - like ExpressVPN and NordVPN - shut down their Russian servers."

Neben dem BSI haben auch andere Länder und Organisationen ihre Risikobewertung angepasst. Frankreich hat beispielsweise eine vergleichbare Warnung veröffentlicht[3]. [redacted] Die Teilnehmer waren sich einig, dass der Einsatz von Kaspersky-Produkten hoch problematisch ist. Zum Schutz ihrer IT-Systeme wurden daher automatische Updates abgestellt und Schritte eingeleitet, um die Software schnellstmöglich durch eine sicherere Alternative abzulösen.

Die in der Warnung beschriebenen Angriffsvektoren sind nicht neu. Im Folgenden einige Beispiele, die belegen, welchen Schaden ein Angreifer mit Viren-Schutzsoftware anrichten könnte:

[redacted]

[2]https://www.techradar.com/vpn/which-websites-and-services-are-banned-in-russia
[3]https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

Einstufung nach Schwärzung aufgehoben.

- Am 10.06.2015 hat Kaspersky selbst in einer Pressemitteilung[4] mitgeteilt, dass das Unternehmensnetzwerk gehackt wurde und Angreifer mit teils neuen Methoden versucht haben, vertrauliche Daten zu stehlen, die dann für Angriffe auf die Kunden missbraucht werden könnten.
- Am 05. Januar 2012 hat die Hacker-Gruppe „The Lords of Dharmaraja“ geheimen Sourcecode von Symantec bei Pastebin veröffentlicht. Symantec hat die Echtheit des Codes bestätigt und die sicherheitsrelevanten Auswirkungen mit dem BSI-Präsidenten in einem vertraulichen Gespräch erörtert.
- Alle Hersteller von Viren-Schutzprogrammen hatten in der Vergangenheit Schwachstellen, die für Angriffe auf Kundensysteme hätten genutzt werden können. Mit Kenntnis des Sourcecode oder noch nicht veröffentlichter Schwachstellen wäre ein Angreifer nicht auf offiziell gemeldete Schwachstellen angewiesen, um einen Angriff durchzuführen. Wenn schon Schwachstellen ausreichen, um Systeme komplett stillzulegen, wäre dies mit einer Backdoor noch sehr viel leichter.
- Es sind zahlreiche Vorfälle bei allen Herstellern von Viren-Schutzsoftware bekannt, in denen eine fehlerhafte Erkennungssignatur Windows-Systemdateien als schädlich klassifiziert und damit das IT-System blockiert hat.
- Es sind auch Vorfälle bekannt, bei denen nach einem Signaturupdate bestimmte Schadprogramme irrtümlich nicht mehr detektiert wurden.
- Alle Viren-Schutzprogramme haben Funktionen eingebaut, mit denen sich Schadsoftwareausbrüche begrenzen lassen. Dazu können sie beliebige Dateien blockieren oder löschen. Auch in der Bundesverwaltung hat es bereits einen Sicherheitsvorfall gegeben, bei dem durch eine Fehlbedienung der "Outbreak-Prevention"-Funktion eine ganze Behörde für einen Tag lahmgelegt wurde.
- Bei Updates werden nicht immer nur Signaturen übertragen. Es ist auch möglich, dass größere Softwarebestandteile (z. B. Scan-Engines) aktualisiert werden müssen, um mit neuen Signaturen/Erkennungsverfahren kompatibel zu bleiben. Dem BSI sind Fälle bekannt, bei denen durch Updates eines Viren-Schutzprogramms neue Funktionen installiert oder Konfigurationen überschrieben wurden, ohne dass die Nutzer dies bemerken konnten. In der Folge wurde Kundendaten ohne Genehmigung an den Hersteller übertragen.

Derartige Vorfälle mussten alle Hersteller bereits vermelden. Sie sind immer unbeabsichtigt aufgrund von Fehlern oder Nachlässigkeiten geschehen. Eigene Entwickler oder Hacker, die in die Systeme des Herstellers eingedrungen sind, sind nicht auf Schwachstellen oder Fehler angewiesen, und könnten daher sehr einfach die folgenden Funktionen auf Kundensystemen implementieren:

- Zielsysteme analysieren (Systemeigenschaften, Hardwareeigenschaften, verwendete Software etc.)
- Daten zum Hersteller übertragen (z. B. Dateien, URLs)
- Dateien sperren oder löschen

Um die gewollte Funktionalität bieten zu können, laufen Viren-Schutzprogramme zudem mit hohen Systemrechten, schützen sich vor Veränderungen und haben Zugriff auf das gesamte Filesystem. Durch die hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig ist, könnten theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Manipulationen lassen sich auch temporär vornehmen und dadurch sehr gut tarnen. Beispielsweise könnte für wenige Stunden ein bestimmter Schadcode bewusst nicht erkannt werden, um anderen Angreifern den Weg zu bereiten.

Wenn die Kaspersky-Produkte für Angriffe entweder durch Anweisung der russischen Regierung oder durch staatliches Eindringen in deren Systeme instrumentalisiert werden, ist es daher möglich, dass auf die Systeme

[4]https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

auf denen Kaspersky-Produkte installiert sind, unberechtigt zugegriffen oder Einfluss genommen werden kann.

Kaspersky ist sich dieser Gefahren bewusst und hat in der Vergangenheit diverse Maßnahmen zur Vertrauensbildung ergriffen, die aber alle nicht geeignet sind, die aktuelle veränderte Gefahrenlage zu entschärfen:

- Kaspersky hat versucht, sich dem Einfluss russischer Behörden zu entziehen und betreibt eine Dateninfrastruktur in zwei Rechenzentren in Zürich zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden aus Europa, den Vereinigten Staaten und Kanada sowie in mehreren asiatisch-pazifischen Ländern. Für die Bereitstellung von Updates/Virensignaturen stehen bei Bedarf verschiedene Server in Europa zur Verfügung, unter anderem in Frankfurt.

  Es ist unerheblich, wo die Kundendaten gehostet werden. Entscheidend ist, wer Sourcecodeänderungen vornehmen und Signaturdaten erstellen kann und wie diese qualitätsgesichert und geprüft werden. Kaspersky kann nicht nachweisen, dass diese Prozesse komplett unabhängig vom russischen Hauptquartier durchgeführt werden. Es ist auch nicht transparent, wer administrativen Zugang zu den Systemen in Westeuropa hat. Aufgrund der Erfahrungen mit anderen Cloudanbietern ist es extrem unwahrscheinlich, dass die Rechenzentren in West-Europa komplett autark arbeiten und keine administrativen Eingriffe aus anderen Regionen erfolgen können.

- Die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren und Datendienste von Kaspersky wurden von zwei externen, unabhängigen Prüforganisationen bestätigt. Kaspersky hat das SOC-2-Audit (Service Organization Control for Service Organizations) Typ 1 durch einen Big-Four-Auditor erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigte. Darüber hinaus wurden Datendienste vom TÜV AUSTRIA nach ISO/IEC 27001:2013 zertifiziert.

  Eine Zertifizierung sagt nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus. Sie ist keine Garantie für den Ist-Zustand.

- Kaspersky sagt über sich selbst, als global agierendes privates Unternehmen (Sitz der Holding ist London, UK) keine Verbindungen zur russischen Regierung zu haben.

  Diese Aussage ist nicht glaubhaft. Kaspersky hat seinen Hauptsitz in Moskau und weist eine russische Eigentümerstruktur auf. Als eines der wichtigsten IT-Security-Unternehmen Russlands arbeitet Kaspersky eng mit Ermittlungsbehörden zusammen (s. o.). Wesentliche Teile der Belegschaft arbeiten daher in Russland oder haben familiäre Bindungen in Russland und sind daher dem direkten Einfluss und Druck der Behörden ausgesetzt.

- Kaspersky unterliegt nach eigenen Angaben nicht dem russischen System operativer Ermittlungsmaßnahmen (SORM) oder anderen ähnlichen Gesetzen und sei deswegen nicht zur Auskunftserteilung verpflichtet.

  Diese faktischen Einflussmöglichkeiten der russischen Regierung entfallen nicht deswegen, weil Kaspersky nach russischem Recht keinen Mitwirkungspflichten unterliegt (zu den Pflichten s. Gutachten Prof. Hober).

  Angesichts des mit dem Einmarsch in die Ukraine erfolgten eklatanten Bruchs von internationalem Recht durch Russland muss damit gerechnet werden, dass die russische Regierung auch gegen geltendes russisches Recht verstößt, wenn ihr dies opportun erscheint.

Soweit das BSI die Maßnahmen von Kaspersky in der Vergangenheit für ausreichend hielt, um die Produkte von Kaspersky weiter einsetzen zu können, lag dem die Annahme zu Grunde, dass die russische Regierung keine Schritte einleiten würde, die bei Bekanntwerden (bzw. Entdeckung) sowohl Kaspersky als auch der russischen Regierung wirtschaftlichen Schaden und einen Reputationsverlust zufügen würden. Angesichts

der nunmehr offenen Konfrontation Russlands mit der EU und den NATO-Staaten und der Hinnahme selbst existenzvernichtender Sanktionen für russische Unternehmen, kann diese Grundannahme nicht weiter aufrechterhalten werden. Wir müssen nunmehr davon ausgehen, dass die russische Regierung in der jetzigen Situation keine Rücksicht mehr auf das internationale Geschäft und die Reputation von Kaspersky nehmen würde [redacted] Als Konsequenz sollten diese Einrichtungen keine Produkte des Herstellers Kaspersky einsetzen.

Eine Warnung des BSI ist auch mit dem Grundsatz der Verhältnismäßigkeit vereinbar: zum einen weist das BSI in seiner Warnung darauf hin, dass private Anwender weniger bedroht sein können, was zur Folge haben kann, dass diese die Produkte von Kaspersky weiterhin nutzen. Ein erfolgreicher Angriff auf ein KRITIS-Unternehmen könnte jedoch die Versorgung der Bevölkerung mit lebenswichtigen Diensten wie Wasser oder Energie beeinträchtigen und bis hin zu einem Ausnahmezustand führen. Das potentielle Schadensrisiko ist hier mithin enorm. Dem steht das Interesse des einzelnen Herstellers (hier Kaspersky) an der freien Ausübung seines Gewerbes gegenüber. Hier ist zwar zu berücksichtigen, dass eine Warnmeldung mit hoher Wahrscheinlichkeit spürbare Folgen auf die wirtschaftliche Tätigkeit des Herstellers in Deutschland hätte. Allerdings überwiegt hier der Schutz der Allgemeinheit aufgrund der besonderen Schwere des Schadensrisikos das Interesse des einzelnen Herstellers.

Fazit:

Durch manipulierte Viren-Schutzprogramme hat ein Angreifer nahezu unbegrenzte Möglichkeiten, IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste Vorfall öffentlich bekannt wird. Vielmehr ist die Warnung zum jetzigen Zeitpunkt angezeigt, um rechtzeitig präventiv zu handeln und die relevanten Anwender vor potentiellem Schaden zu bewahren. Mildere Mittel zum Schutz der Informationssicherheit sind nicht ersichtlich.

B Vorherige Stellungnahmemöglichkeit nach § 7 Abs. 1 a Nr. 1 BSIG

Kaspersky sollte vor der Veröffentlichung nur mit kurzer Frist informiert und Gelegenheit zur Stellungnahme gegeben werden. Es ist Gefahr im Verzug. Hacker könnten ihre Vorbereitungen bereits abgeschlossen haben und nur noch auf einen Einsatzbefehl warten. Es ist nicht ersichtlich, dass Kaspersky eine Möglichkeit hätte, durch technische oder sonstige Maßnahmen die Risikoeinschätzung positiv zu beeinflussen. Es ist nicht wahrscheinlich, dass der Hersteller an dem zugrundeliegenden strukturellen Sicherheitsproblem etwas ändern kann, da er kaum Einfluss auf die Gefährdung hat. Angesichts der Gefährdungslage erscheint eine kurze Frist daher verhältnismäßig und fachlich angemessen.

Im Auftrag

[redacted]

062_3.pdf

BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten

Bonn, 15. März 2022. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.

Antivirensoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, verfügt 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. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur.

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs verbunden. Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen 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.

Alle Nutzerinnen und Nutzer der Virenschutzsoftware können von solchen Operationen betroffen sein. Unternehmen und Behörden mit besonderen Sicherheitsinteressen und Betreiber Kritischer Infrastrukturen sind in besonderem Maße gefährdet. Sie haben die Möglichkeit, sich vom BSI oder von den zuständigen Verfassungsschutzbehörden beraten zu lassen.

Unternehmen und andere Organisationen sollten den Austausch wesentlicher Bestandteile ihrer IT-Sicherheitsinfrastruktur sorgfältig planen und umsetzen. Würden IT-Sicherheitsprodukte und insbesondere Virenschutzsoftware ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der Umstieg auf andere Produkte ist mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden. Das BSI empfiehlt, eine individuelle Bewertung und Abwägung der aktuellen Situation vorzunehmen und dazu gegebenenfalls vom BSI zertifizierte IT-Sicherheitsdienstleister hinzuzuziehen.

63

063_0_geschwärzt.pdf

Von:	Welsch, Günther
An:	"Andreas.Koenen@bmi.bund.de"
Cc:	Markus.Richter@bmi.bund.de; Schönbohm, Arne; Schabhüser, Gerhard
Betreff:	[VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Montag, 14. März 2022 17:50:00
Anlagen:	Warnung_Kaspersky_Begründung.pdf Kaspersky_Warnung_Entwurf_Kaspersky.pdf Anschreiben_Kaspersky_BSI_Warnung.pdf 2022_03_15_Kaspersky_Warnung_Pressemeldung.docx
Dringlichkeit:	Hoch

Einstufung aufgehoben

Lieber Herr Könen,

Herr Schönbohm hat mich gebeten, Ihnen und abschriftlich Herrn Staatssekretär Richter die Warnung nebst Begründung zu übermitteln. Sie finden diese Informationen anliegend.

Zusätzlich lege ich anbei das Schreiben an Kaspersky, welches ich heute Mittag versendet hatte, mit der Gelegenheit zur Stellungnahme seitens des Unternehmens bis 17:00 Uhr. Bis jetzt ist keine Antwort seitens Kaspersky eingegangen. Somit ist die Frist fruchtlos verstrichen. Dennoch werden wir die Posteingänge weiter beobachten und im Fall einer Äußerung des Unternehmens Sie unverzüglich darüber und unsere Bewertung informieren.

Herr Schönbohm hat entschieden, die Warnung öffentlichkeitswirksam um 9:00 Uhr am morgigen Dienstag zu publizieren. Wir rechnen mit größeren Nachfragen seitens der (Fach-)Öffentlichkeit und zahlreichen Beratungsanfragen. Im BSI ist eine Gruppe eingerichtet worden, welche FAQ Antworten vorformuliert, um skalierend und standardisiert auf Anfragen antworten zu können.

Die morgen erscheinende Pressemitteilung ist/wird zwischen dem Pressereferat des BMI und der Pressestelle des BSI abgestimmt. Der Entwurf der Pressemitteilung zum jetzigen Zeitpunkt liegt ebenfalls der Mail bei.

Für Fragen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen,
im Auftrag
Günther Welsch

--- --- --- --- --- --- --- ---

Dr. Günther Welsch
Abteilungsleiter KM
Bundesamt für Sicherheit in der Informationstechnik
53175 Bonn

Tel: 0228 9582[redacted]
Mobil [redacted]

Im Folgenden wird 045_0_geschwärzt.pdf zitiert.

063_1_Warnung_Kaspersky_Begründung_geschwärzt.pdf

Referat KM 14 14. März 2022

Az. KM14-210 01 03 / VS-NfD

[redacted]

Betr. Bewertung von IT-Sicherheitsprodukten
hier: Warnung vor Kaspersky-Produkten nach § 7 BSIG

Bezug

Anlage Text der BSI-Warnung gemäß BSIG § 7

1) Vermerk zur Begründung der Warnung

A Begründung der Warnung nach § 7 Abs. 1 BSIG

Das BSI darf nach § 7 Abs. 1 BSIG u.a. vor Sicherheitslücken in informationstechnischen Produkten und Diensten öffentlich warnen. Sicherheitslücken in diesem Sinne sind nach § 2 Abs. 6 BSIG „*Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.*“ Zudem kann das BSI Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten an die Öffentlichkeit richten (§ 7 Abs. 1 Satz 1.d BSIG). Dabei ist nach Meinung in der Literatur zwar noch ein Bezug zur Gefahrenvorsorge notwendig, aber keine konkrete Gefahrenlage mehr (vgl. Ritter-*Schulte,* Die Weiterentwicklung des IT-Sicherheitsgesetzes, Art. 1 Nr. 9 IT-SiG 2.0, Rn. 307). Solche Sicherheitseigenschaften von Produkten können sich auch aus der Struktur des Anbieters ergeben. Da hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik von dem Anti-Virenschutz der Firma Kaspersky ausgehen, kann das BSI vor dem Einsatz des Produktes warnen und Empfehlungen aussprechen (§ 7 Abs. 2 BSIG).

Die Ereignisse rund um Kaspersky werden vom BSI seit Jahren aufmerksam verfolgt. Mehrere westliche Staaten wie USA und Niederlande warnen seit Jahren öffentlich vor Kaspersky und haben die Software für den Einsatz im Behördenumfeld gesperrt (Quellen werden nachgereicht). [redacted]

Der russische Angriff auf die Ukraine, der mit hybriden Mitteln - also auch im Cyberraum - geführt wird und von der UNO-Vollversammlung mit großer Mehrheit scharf verurteilt wurde, verändert die Lagebeurteilung. Russland ist kein demokratischer Rechtsstaat und sieht Deutschland durch die Beteiligung an Sanktionen und Waffenlieferungen als Kontrahent an. Mit feindlichen Übergriffen auf deutsche Institutionen, Unternehmen und IT-Infrastrukturen ist daher zu rechnen. Russische Unternehmen wie Kaspersky könnten zum einen für die Unterstützung der russischen Streitkräfte instrumentalisiert werden, zum anderen selbst Ziel massiver Cyberangriffe werden. Die Gefahr, dass Kaspersky in die kriegerischen Auseinandersetzungen hineingezogen wird, ist daher so groß, dass eine Warnung angemessen ist. Es muss damit gerechnet werden,

dass Kaspersky nicht mehr die uneingeschränkte Kontrolle über seine Software und IT-Systeme hat bzw. diese in Kürze verlieren wird.

[redacted]

Bereits in den letzten Jahren wurden Fälle bekannt, in denen staatliche Stellen Einfluss auf Kaspersky genommen haben:

[redacted]

In den Jahren 2018 und 2019 wurden russische VPN-Anbieter gezwungen, bestimmte Verbindungen auf Anordnung der Regierung zu blocken. Während die meisten Anbieter die Kooperation verweigerten, kam Kaspersky den Anordnungen nach[2]:

"Although not all VPNs are banned, a 2018 law introduced fines for search engines that brought up results to proxy sites (including VPNs) that would give Russians access to prohibited content or instructions on how to get access to that content.
The following year, VPNs and search engines were compelled to block any websites that appeared on the federal government blacklist. Later, 10 VPN providers were ordered to hand over access to their servers or face being banned. Only one, Kaspersky Lab, which is based in Russia, agreed, while others - like ExpressVPN and NordVPN - shut down their Russian servers."

Neben dem BSI haben auch andere Länder und Organisationen ihre Risikobewertung angepasst. Frankreich hat beispielsweise eine vergleichbare Warnung veröffentlicht[3]. [redacted] Die Teilnehmer waren sich einig, dass der Einsatz von Kaspersky-Produkten hoch problematisch ist. Zum Schutz ihrer IT-Systeme wurden daher automatische Updates abgestellt und Schritte eingeleitet, um die Software schnellstmöglich durch eine sicherere Alternative abzulösen.

Die in der Warnung beschriebenen Angriffsvektoren sind nicht neu. Im Folgenden einige Beispiele, die belegen, welchen Schaden ein Angreifer mit Viren-Schutzsoftware anrichten könnte:

[redacted]

[2]https://www.techradar.com/vpn/which-websites-and-services-are-banned-in-russia
[3]https://cert.ssi.gouv.fr/cti/CERTFR-2022-CTI-001/

- Am 10.06.2015 hat Kaspersky selbst in einer Pressemitteilung[4] mitgeteilt, dass das Unternehmensnetzwerk gehackt wurde und Angreifer mit teils neuen Methoden versucht haben, vertrauliche Daten zu stehlen, die dann für Angriffe auf die Kunden missbraucht werden könnten.
- Am 05. Januar 2012 hat die Hacker-Gruppe „The Lords of Dharmaraja“ geheimen Sourcecode von Symantec bei Pastebin veröffentlicht. Symantec hat die Echtheit des Codes bestätigt und die sicherheitsrelevanten Auswirkungen mit dem BSI-Präsidenten in einem vertraulichen Gespräch erörtert.
- Alle Hersteller von Viren-Schutzprogrammen hatten in der Vergangenheit Schwachstellen, die für Angriffe auf Kundensysteme hätten genutzt werden können. Mit Kenntnis des Sourcecode oder noch nicht veröffentlichter Schwachstellen wäre ein Angreifer nicht auf offiziell gemeldete Schwachstellen angewiesen, um einen Angriff durchzuführen. Wenn schon Schwachstellen ausreichen, um Systeme komplett stillzulegen, wäre dies mit einer Backdoor noch sehr viel leichter.
- Es sind zahlreiche Vorfälle bei allen Herstellern von Viren-Schutzsoftware bekannt, in denen eine fehlerhafte Erkennungssignatur Windows-Systemdateien als schädlich klassifiziert und damit das IT-System blockiert hat.
- Es sind auch Vorfälle bekannt, bei denen nach einem Signaturupdate bestimmte Schadprogramme irrtümlich nicht mehr detektiert wurden.
- Alle Viren-Schutzprogramme haben Funktionen eingebaut, mit denen sich Schadsoftwareausbrüche begrenzen lassen. Dazu können sie beliebige Dateien blockieren oder löschen. Auch in der Bundesverwaltung hat es bereits einen Sicherheitsvorfall gegeben, bei dem durch eine Fehlbedienung der "Outbreak-Prevention"-Funktion eine ganze Behörde für einen Tag lahmgelegt wurde.
- Bei Updates werden nicht immer nur Signaturen übertragen. Es ist auch möglich, dass größere Softwarebestandteile (z. B. Scan-Engines) aktualisiert werden müssen, um mit neuen Signaturen/Erkennungsverfahren kompatibel zu bleiben. Dem BSI sind Fälle bekannt, bei denen durch Updates eines Viren-Schutzprogramms neue Funktionen installiert oder Konfigurationen überschrieben wurden, ohne dass die Nutzer dies bemerken konnten. In der Folge wurde Kundendaten ohne Genehmigung an den Hersteller übertragen.

Derartige Vorfälle mussten alle Hersteller bereits vermelden. Sie sind immer unbeabsichtigt aufgrund von Fehlern oder Nachlässigkeiten geschehen. Eigene Entwickler oder Hacker, die in die Systeme des Herstellers eingedrungen sind, sind nicht auf Schwachstellen oder Fehler angewiesen, und könnten daher sehr einfach die folgenden Funktionen auf Kundensystemen implementieren:

- Zielsysteme analysieren (Systemeigenschaften, Hardwareeigenschaften, verwendete Software etc.)
- Daten zum Hersteller übertragen (z. B. Dateien, URLs)
- Dateien sperren oder löschen

Um die gewollte Funktionalität bieten zu können, laufen Viren-Schutzprogramme zudem mit hohen Systemrechten, schützen sich vor Veränderungen und haben Zugriff auf das gesamte Filesystem. Durch die hohe Updatefrequenz, die für einen einwandfreien Betrieb notwendig ist, könnten theoretisch beliebige Funktionalitäten unbemerkt hinzugefügt werden. Manipulationen lassen sich auch temporär vornehmen und dadurch sehr gut tarnen. Beispielsweise könnte für wenige Stunden ein bestimmter Schadcode bewusst nicht erkannt werden, um anderen Angreifern den Weg zu bereiten.

Wenn die Kaspersky-Produkte für Angriffe entweder durch Anweisung der russischen Regierung oder durch staatliches Eindringen in deren Systeme instrumentalisiert werden, ist es daher möglich, dass auf die Systeme

[4]https://www.kaspersky.com/about/press-releases/2015_duqu-is-back-kaspersky-lab-reveals-cyberattack-on-its-corporate-network-that-also-hit-high-profile-victims-in-western-countries-the-middle-east-and-asia

auf denen Kaspersky-Produkte installiert sind, unberechtigt zugegriffen oder Einfluss genommen werden kann.

Kaspersky ist sich dieser Gefahren bewusst und hat in der Vergangenheit diverse Maßnahmen zur Vertrauensbildung ergriffen, die aber alle nicht geeignet sind, die aktuelle veränderte Gefahrenlage zu entschärfen:

- Kaspersky hat versucht, sich dem Einfluss russischer Behörden zu entziehen und betreibt eine Dateninfrastruktur in zwei Rechenzentren in Zürich zur Verarbeitung und Speicherung von Cyberbedrohungsdaten von Kunden aus Europa, den Vereinigten Staaten und Kanada sowie in mehreren asiatisch-pazifischen Ländern. Für die Bereitstellung von Updates/Virensignaturen stehen bei Bedarf verschiedene Server in Europa zur Verfügung, unter anderem in Frankfurt.

  Es ist unerheblich, wo die Kundendaten gehostet werden. Entscheidend ist, wer Sourcecodeänderungen vornehmen und Signaturdaten erstellen kann und wie diese qualitätsgesichert und geprüft werden. Kaspersky kann nicht nachweisen, dass diese Prozesse komplett unabhängig vom russischen Hauptquartier durchgeführt werden. Es ist auch nicht transparent, wer administrativen Zugang zu den Systemen in Westeuropa hat. Aufgrund der Erfahrungen mit anderen Cloudanbietern ist es extrem unwahrscheinlich, dass die Rechenzentren in West-Europa komplett autark arbeiten und keine administrativen Eingriffe aus anderen Regionen erfolgen können.

- Die Sicherheit und Zuverlässigkeit der technischen und organisatorischen Verfahren und Datendienste von Kaspersky wurden von zwei externen, unabhängigen Prüforganisationen bestätigt. Kaspersky hat das SOC-2-Audit (Service Organization Control for Service Organizations) Typ 1 durch einen Big-Four-Auditor erfolgreich absolviert, welches die Sicherheit des Kaspersky-Prozesses zur Entwicklung und Freigabe von AV-Updates gegen das Risiko unbefugter Änderungen bestätigte. Darüber hinaus wurden Datendienste vom TÜV AUSTRIA nach ISO/IEC 27001:2013 zertifiziert.

  Eine Zertifizierung sagt nur etwas über den Soll-Zustand zum Zeitpunkt des Audits aus. Sie ist keine Garantie für den Ist-Zustand.

- Kaspersky sagt über sich selbst, als global agierendes privates Unternehmen (Sitz der Holding ist London, UK) keine Verbindungen zur russischen Regierung zu haben.

  Diese Aussage ist nicht glaubhaft. Kaspersky hat seinen Hauptsitz in Moskau und weist eine russische Eigentümerstruktur auf. Als eines der wichtigsten IT-Security-Unternehmen Russlands arbeitet Kaspersky eng mit Ermittlungsbehörden zusammen (s. o.). Wesentliche Teile der Belegschaft arbeiten daher in Russland oder haben familiäre Bindungen in Russland und sind daher dem direkten Einfluss und Druck der Behörden ausgesetzt.

- Kaspersky unterliegt nach eigenen Angaben nicht dem russischen System operativer Ermittlungsmaßnahmen (SORM) oder anderen ähnlichen Gesetzen und sei deswegen nicht zur Auskunftserteilung verpflichtet.

  Diese faktischen Einflussmöglichkeiten der russischen Regierung entfallen nicht deswegen, weil Kaspersky nach russischem Recht keinen Mitwirkungspflichten unterliegt (zu den Pflichten s. Gutachten Prof. Hober).

  Angesichts des mit dem Einmarsch in die Ukraine erfolgten eklatanten Bruchs von internationalem Recht durch Russland muss damit gerechnet werden, dass die russische Regierung auch gegen geltendes russisches Recht verstößt, wenn ihr dies opportun erscheint.

Soweit das BSI die Maßnahmen von Kaspersky in der Vergangenheit für ausreichend hielt, um die Produkte von Kaspersky weiter einsetzen zu können, lag dem die Annahme zu Grunde, dass die russische Regierung keine Schritte einleiten würde, die bei Bekanntwerden (bzw. Entdeckung) sowohl Kaspersky als auch der russischen Regierung wirtschaftlichen Schaden und einen Reputationsverlust zufügen würden. Angesichts

Einstufung nach Schwärzung aufgehoben.

der nunmehr offenen Konfrontation Russlands mit der EU und den NATO-Staaten und der Hinnahme selbst existenzvernichtender Sanktionen für russische Unternehmen, kann diese Grundannahme nicht weiter aufrechterhalten werden. Wir müssen nunmehr davon ausgehen, dass die russische Regierung in der jetzigen Situation keine Rücksicht mehr auf das internationale Geschäft und die Reputation von Kaspersky nehmen würde [redacted] Als Konsequenz sollten diese Einrichtungen keine Produkte des Herstellers Kaspersky einsetzen.

Eine Warnung des BSI ist auch mit dem Grundsatz der Verhältnismäßigkeit vereinbar: zum einen weist das BSI in seiner Warnung darauf hin, dass private Anwender weniger bedroht sein können, was zur Folge haben kann, dass diese die Produkte von Kaspersky weiterhin nutzen. Ein erfolgreicher Angriff auf ein KRITIS-Unternehmen könnte jedoch die Versorgung der Bevölkerung mit lebenswichtigen Diensten wie Wasser oder Energie beeinträchtigen und bis hin zu einem Ausnahmezustand führen. Das potentielle Schadensrisiko ist hier mithin enorm. Dem steht das Interesse des einzelnen Herstellers (hier Kaspersky) an der freien Ausübung seines Gewerbes gegenüber. Hier ist zwar zu berücksichtigen, dass eine Warnmeldung mit hoher Wahrscheinlichkeit spürbare Folgen auf die wirtschaftliche Tätigkeit des Herstellers in Deutschland hätte. Allerdings überwiegt hier der Schutz der Allgemeinheit aufgrund der besonderen Schwere des Schadensrisikos das Interesse des einzelnen Herstellers.

Fazit:

Durch manipulierte Viren-Schutzprogramme hat ein Angreifer nahezu unbegrenzte Möglichkeiten, IT-Systeme auszuspionieren oder zu sabotieren. Da Kaspersky-Produkte auch zur Absicherung Kritischer Infrastrukturen und in der deutschen Verwaltung eingesetzt werden, kann mit einer Warnung nicht gewartet werden, bis der erste Vorfall öffentlich bekannt wird. Vielmehr ist die Warnung zum jetzigen Zeitpunkt angezeigt, um rechtzeitig präventiv zu handeln und die relevanten Anwender vor potentiellem Schaden zu bewahren. Mildere Mittel zum Schutz der Informationssicherheit sind nicht ersichtlich.

B Vorherige Stellungnahmemöglichkeit nach § 7 Abs. 1 a Nr. 1 BSIG

Kaspersky sollte vor der Veröffentlichung nur mit kurzer Frist informiert und Gelegenheit zur Stellungnahme gegeben werden. Es ist Gefahr im Verzug. Hacker könnten ihre Vorbereitungen bereits abgeschlossen haben und nur noch auf einen Einsatzbefehl warten. Es ist nicht ersichtlich, dass Kaspersky eine Möglichkeit hätte, durch technische oder sonstige Maßnahmen die Risikoeinschätzung positiv zu beeinflussen. Es ist nicht wahrscheinlich, dass der Hersteller an dem zugrundeliegenden strukturellen Sicherheitsproblem etwas ändern kann, da er kaum Einfluss auf die Gefährdung hat. Angesichts der Gefährdungslage erscheint eine kurze Frist daher verhältnismäßig und fachlich angemessen.

Im Auftrag

[redacted]

063_2_Kaspersky_Warnung_Entwurf_Kaspersky.pdf

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Warnung gemäß BSIG § 7

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

Viren-Schutzsoftware des Herstellers Kaspersky

Risikostufe [2]: 4 - hoch

1 Sachverhalt

Viren-Schutzsoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, ist essentiell zum Schutz von IT-Systemen. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt aber gerade Viren-Schutzsoftware 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. Viren-Schutzsoftware 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 Viren-Schutzsoftware 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 Viren-Schutzsoftware des Unternehmens Kaspersky.

4 Handlungsempfehlung

Viren-Schutzsoftware 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 Viren-Schutzsoftware) 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/DasBSI/Gesetz/gesetz_node.html
[2] Darstellung Risikostufen
https://www.cert-bund.de/risk

063_3_Anschreiben_Kaspersky_BSI_Warnung_geschwärzt.pdf

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Kaspersky
European Headquarters
2 Kingdom Street
London
W2 6BD
United Kingdom

nachrichtlich:
[redacted]
Head of Public Affairs Europe

Dr. Günther Welsch
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185-189
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +49 228 99 9582[redacted]
Fax +49 228 99 10 9582[redacted]

abteilung-km@bsi.bund.de

www.bsi.bund.de

Betreff: BSI Warnung nach § 7 BSIG: Gelegenheit zur Stellungnahme

Geschäftszeichen: KM14-210 01 03
Anlage: Entwurf der Warnmeldung
Datum: 14.03.2022
Seite 1 von 2

Sehr geehrte Damen und Herren,

das Bundesamt für Sicherheit in der Informationstechnik (BSI) analysiert und bewertet regelmäßig im Rahmen seiner Aufgabenwahrnehmung die Sicherheit von Software und IT-Sicherheitsprodukten, so z.B. Viren-Schutzsoftware.

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.

Im Zuge der kriegerischen Auseinandersetzungen zwischen Russland und der Ukraine ist eine neue Sicherheitslage für die Bundesrepublik Deutschland entstanden. Die damit einhergehenden Bedrohungen werden im Rahmen des IT-Risikomanagements mit Blick auf Software und IT-Sicherheitsprodukte neu bewertet.

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.

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).

Es besteht aufgrund der besonderen Sicherheitssituation Gefahr im Verzug. Das BSI hält daher eine unverzügliche Reaktion für angemessen. Wir beabsichtigen morgen, **Dienstag, den 15. März 2022 um 9:00 Uhr** eine öffentlichkeitswirksame Produktwarnung zu publizieren.

Wir gewähren dem Unternehmen Kaspersky eine Frist bis heute,

Montag den 14. März 2022 um 17:00 Uhr,

uns eine Stellungnahme in der Sache zukommen zu lassen. Sie haben damit die Möglichkeit, für Sie günstige Sachargumente zum weiteren Entscheidungsprozess im BSI beizutragen. Über unsere Entscheidung werden wir Sie informieren.

Mit freundlichen Grüßen

Im Auftrag

Dr. Günther Welsch

063_4_2022_03_15_Kaspersky_Warnung_Pressemeldung (002).pdf

BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten

Bonn, 15. März 2022. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky. Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.

Antivirensoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, verfügt 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. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur.

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs verbunden. Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen 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.

Alle Nutzerinnen und Nutzer der Virenschutzsoftware können von solchen Operationen betroffen sein. Unternehmen und Behörden mit besonderen Sicherheitsinteressen und Betreiber Kritischer Infrastrukturen sind in besonderem Maße gefährdet. Sie haben die Möglichkeit, sich vom BSI oder von den zuständigen Verfassungsschutzbehörden beraten zu lassen.

Unternehmen und andere Organisationen sollten den Austausch wesentlicher Bestandteile ihrer IT-Sicherheitsinfrastruktur sorgfältig planen und umsetzen. Würden IT-Sicherheitsprodukte und insbesondere Virenschutzsoftware ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der Umstieg auf andere Produkte ist mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden. Das BSI empfiehlt, eine individuelle Bewertung und Abwägung der aktuellen Situation vorzunehmen und dazu gegebenenfalls vom BSI zertifizierte IT-Sicherheitsdienstleister hinzuzuziehen.

64

064_0_geschwärzt.pdf

Von:	Welsch, Günther
An:	Samsel, Horst; "Caspers, Thomas"; Häger, Dirk; Nagel, Nadine; [redacted]; GP Leitungsstab; GP Stab 1 - Strategische Kommunikation und Presse; [redacted]; Amendola, Sandro; Bargstädt-Franke, Silke; Pieper, Jörg
Cc:	GP Abteilung BL; GP Abteilung TK; GP Abteilung OC; GP Abteilung WG; GP Geschaeftszimmer KM; GP Referat KM 14 [redacted]@bsi.bund.de); GP Abteilung KM
Betreff:	WG: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Montag, 14. März 2022 17:53:00
Anlagen:	Warnung_Kaspersky_Begründung.pdf Kaspersky_Warnung_Entwurf_Kaspersky.pdf Anschreiben_Kaspersky_BSI_Warnung.pdf 2022_03_15_Kaspersky_Warnung_Pressemeldung.docx
Dringlichkeit:	Hoch

LK,

zu Ihrer Information.

Viele Grüße
G. Welsch

Im Folgenden wird 063_0_geschwärzt.pdf inkl. der Anhänge zitiert.

65

065_0_geschwärzt.pdf

Von: Andreas.Koenen@bmi.bund.de
An: Welsch, Günther; Schönbohm, Arne
Cc: Markus.Richter@bmi.bund.de; Schabhüser, Gerhard
Betreff: AW: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Montag, 14. März 2022 17:54:28
Anlagen: Julia Parser Messages.txt

Lieber Herr Welsch,

besten Dank für Ihre Information, insbesondere zur ausgebliebenen Reaktion von Kaspersky.

Lieber Herr Schönbohm, lieber Herr Welsch,

sollte irgendein Ereignis eintreten, das die Veröffentlichung der Warnung vereitelt, bitte ich Sie um Nachricht per SMS und E-Mail bis spätestens 08:00 Uhr morgen früh.

Beste Grüße

Andreas Könen
Abteilungsleiter CI
Cyber- und Informationssicherheit
Bundesministerium des Innern und für Heimat
Alt-Moabit 140, 10557 Berlin
DEUTSCHLAND

Telefon: +49 30 18681 [redacted]
E-Mail: andreas koenen@bmi.bund.de
Internet: www.bmi.bund.de

Im Folgenden wird 063_0_geschwärzt.pdf zitiert.

66

066_0.pdf

Von:	Welsch, Günther
An:	Schönbohm, Arne
Cc:	Schabhüser, Gerhard
Betreff:	Re: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum:	Dienstag, 15. März 2022 07:01:31
Anlagen:	Julia Parser Messages.txt

Lieber Herr Schönbohm,
bislang ist keine Stellungnahme seitens Kaspersky eingegangen. An unserem Zeitplan der Veröffentlichung muss daher wohl nichts geändert werden.

Möchten Sie, dass ich Herrn Könen kurz vor 8:00 Uhr auch noch einmal ein bestätigendes Signal gebe?

Viele Grüße
Günther Welsch

Von meinem iPad gesendet

Im Folgenden wird 065_0_geschwärzt.pdf zitiert.

67

067_0.pdf

Von: Schönbohm, Arne
An: Welsch, Günther
Cc: Schabhüser, Gerhard
Betreff: AW: Re: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Dienstag, 15. März 2022 07:27:24

Lassen Sie uns um 7:45 telefonieren.

Mit freundlichen Grüßen

Arne Schönbohm

via SecurePIM gesendet

Im Folgenden wird 066_0.pdf zitiert.

68

068_0.pdf

Von: Schönbohm, Arne
An: Andreas.Koenen
Cc: Markus.Richter; Welsch, Günther; Schabhüser, Gerhard
Betreff: AW: AW: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Dienstag, 15. März 2022 07:52:26

Sehr geehrter Herr Könen es gab bis jetzt keinerlei Reaktion von Kaspersky. Die Veröffentlichung findet somit um 9:00 statt.

Mit freundlichen Grüßen

Arne Schönbohm

via SecurePIM gesendet

Im Folgenden wird 065_0_geschwärzt.pdf zitiert.

69

069_0_geschwärzt.pdf

Von: Andreas.Koenen@bmi.bund.de
An: Schönbohm, Arne
Cc: Markus.Richter@bmi.bund.de; Welsch, Günther; Schabhüser, Gerhard
Betreff: AW: AW: [VS-NfD] - § 7 BSIG Warnung des BSI vor Kaspersky Viren-Schutzsoftware
Datum: Dienstag, 15. März 2022 07:55:31
Anlagen: ATT00001.htm
Julia Parser Messages.txt

Lieber Herr Schönbohm,

vielen Dank!

Beste Grüße

Andreas Könen
Abteilungsleiter CI
Cyber- und Informationssicherheit
Bundesministerium des Innern und für Heimat
Alt-Moabit 140, 10557 Berlin
DEUTSCHLAND

Telefon: +49 30 18681[redacted]
E-Mail: andreas koenen@bmi.bund.de<mailto:andreas koenen@bmi.bund.de>
Internet: www.bmi.bund.de<http://www.bmi.bund.de/>

Im Folgenden wird 068_0.pdf zitiert.

70

070.pdf

Von: GP Presse
An: GP Presse
Betreff: Für die Presse: BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten
Datum: Dienstag, 15. März 2022 09:06:39

+++ P R E S S E I N F O R M A T I O N +++

BSI warnt vor dem Einsatz von Kaspersky-Virenschutzprodukten

Bonn, 15. März 2022. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt nach §7 BSI-Gesetz vor dem Einsatz von Virenschutzsoftware des russischen Herstellers Kaspersky (https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Warnungen-nach-P7_BSIG/2022/BSI_W-004-220315 html). Das BSI empfiehlt, Anwendungen aus dem Portfolio von Virenschutzsoftware des Unternehmens Kaspersky durch alternative Produkte zu ersetzen.

Antivirensoftware, einschließlich der damit verbundenen echtzeitfähigen Clouddienste, verfügt 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. Wenn Zweifel an der Zuverlässigkeit des Herstellers bestehen, birgt Virenschutzsoftware ein besonderes Risiko für eine zu schützende IT-Infrastruktur.

Das Vorgehen militärischer und/oder nachrichtendienstlicher Kräfte in Russland sowie die im Zuge des aktuellen kriegerischen Konflikts von russischer Seite ausgesprochenen Drohungen gegen die EU, die NATO und die Bundesrepublik Deutschland sind mit einem erheblichen Risiko eines erfolgreichen IT-Angriffs verbunden. Ein russischer IT-Hersteller kann selbst offensive Operationen durchführen, gegen seinen 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.

Alle Nutzerinnen und Nutzer der Virenschutzsoftware können von solchen Operationen betroffen sein. Unternehmen und Behörden mit besonderen Sicherheitsinteressen und Betreiber Kritischer Infrastrukturen sind in besonderem Maße gefährdet. Sie haben die Möglichkeit, sich vom BSI oder von den zuständigen Verfassungsschutzbehörden beraten zu lassen.

Unternehmen und andere Organisationen sollten den Austausch wesentlicher Bestandteile ihrer IT-Sicherheitsinfrastruktur sorgfältig planen und umsetzen. Würden IT-Sicherheitsprodukte und insbesondere Virenschutzsoftware ohne Vorbereitung abgeschaltet, wäre man Angriffen aus dem Internet möglicherweise schutzlos ausgeliefert. Der Umstieg auf andere Produkte ist mit vorübergehenden Komfort-, Funktions- und Sicherheitseinbußen verbunden. Das BSI empfiehlt, eine individuelle Bewertung und Abwägung der aktuellen Situation vorzunehmen und dazu gegebenenfalls vom BSI zertifizierte IT-Sicherheitsdienstleister hinzuzuziehen.

Pressekontakt:
Bundesamt für Sicherheit in der Informationstechnik
Pressestelle
Tel.: 0228-999582-5777
E-Mail: presse@bsi.bund.de
Internet: www.bsi.bund.de

Twitter: @BSI_Bund
#DeutschlandDigitalSicherBSI