

Digitales und IT

Dezernat I

Stadt Freiburg im Breisgau · Digitales und IT
Postfach, D-79095 Freiburg

FDP & Bürger* für Freiburg
Rathausplatz 2 - 4
79098 Freiburg

- per E-Mail in PDF -

Adresse: Fehrenbachallee 12
Gebäude A
D-79106 Freiburg i. Br.
Telefon: +49 761 201-5540
Telefax: +49 761 201-5599
Internet: www.freiburg.de
E-Mail*: digit@stadt.freiburg.de

Ihr Zeichen/Schreiben vom Unser Aktenzeichen

Ihnen schreibt
Herr Schulz

Freiburg, den
24.03.2022

Einzelanfrage nach § 24 Abs. 4 GemO zu Sachthemen außerhalb von Sitzungen - Nutzung von Software des Herstellers Kaspersky Lab

Sehr geehrte Frau Stadträtin,
sehr geehrter Herr Stadtrat,

die oben genannte Anfrage Ihrer Fraktion vom 15.03.2022 an Herrn Oberbürgermeister Horn haben wir zur zuständigen Prüfung und Beantwortung erhalten.

Nach Prüfung können wir wie folgt Stellung nehmen:

Seit dem 15.03.2022 warnt das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor dem Einsatz der Virenschutzsoftware des russischen Herstellers Kaspersky. Diese zentrale Lösung ist in der städtischen IT-Infrastruktur seit längerem im Einsatz, basierend auf früheren allgemeinen Beurteilungen, dass Kaspersky ein weltweit eingesetztes und renommiertes Security-Produkt anbietet. Die technischen Fähigkeiten der Produkte wurden als sehr gut beurteilt. Aufgrund einer möglichen Einflussnahme „militärischer und/oder nachrichtendienstlicher Kräfte in Russland“ besteht eine durch das BSI als „Hoch“ (Stufe 4 von 5) eingestufte Bedrohungslage. Das BSI empfiehlt das Softwareportfolio von Kaspersky durch alternative Produkte zu ersetzen.

Dem gingen bereits in den Tagen davor, kritische Einschätzungen Dritter voraus, zu denen seitens des Herstellers dargestellt wurde, dass auch bei einer Sanktionierung der russischen Gesellschaftssitze ein sicherer Betrieb in Deutschland durch die Rechenzentren in der Schweiz gewährleistet werden kann.

Derzeit wird mit Hochdruck an der Analyse der Auswirkungen gearbeitet, die eine ad-hoc-Ablösung von Kaspersky bedeuten würde. Wir vergleichen aktuell den Funktionsumfang der Kaspersky-Lösung mit kurzfristig zur Verfügung stehenden Alternativlösungen.

Das BSI hatte explizit darauf hingewiesen, dass ein ungeplanter Wechsel eines zentralen Bestandteils der IT-Sicherheitsinfrastruktur, im ungünstigen Fall an anderer Stelle Sicherheitslücken oder Funktionseinbußen mit sich bringt. Dieses Problem sehen wir ebenso. Deshalb müssten bei einem kurzfristigen Wechsel evt. vorübergehend einzelne Dienste oder Funktionalitäten blockiert werden, bis die entsprechende Sicherheitskonfiguration der Alternativlösung angepasst werden kann. Ebenso ist zu prüfen, ob auf nicht mehr vorhandene Sicherheitsfunktionalitäten (z. B. die USB-Schnittstellenkontrolle) zeitweilig verzichtet werden kann oder komplette Sperrungen notwendig werden.

Zu Frage 1:

Die Stadtverwaltung setzt Kaspersky Endpoint Security mit dem Kaspersky-Security-Center ein. Die genutzten Sicherheitsfunktionen beinhalten unter anderem den Schutz vor bedrohlichen Dateien und Netzwerkbedrohungen, Exploit-Prävention sowie den Schutz vor Web-Bedrohungen. Dies ist auf allen Endgeräten und Servern der Stadtverwaltung im Einsatz. Als zusätzliches Modul wird momentan die USB-Gerätekontrolle an den Ämtern ausgerollt (nur vertrauenswürdige USB-Geräte können angeschlossen werden).

Es sind darüber hinaus aber auch andere Sicherheitskomponenten im Einsatz, die nicht von Kaspersky sind, darunter z. B. VPN-Lösungen, Spamfilter und Internetfilter. Grundlegend wird im IT-Sicherheitsbereich konsequent eine Mehr-Produkt-Strategie umgesetzt, um nicht die gesamte Architektur zu gefährden.

Bei der Abfrage der städtischen Gesellschaften hatte nur die ASF GmbH ein spezielles Produkt von Kaspersky im Einsatz, das aber auch schon abgelöst werden konnte. Neben den städtischen Gesellschaften setzt auch die Stiftungsverwaltung Kaspersky Produkte ein. Es besteht zum weiteren Verfahren ein enger Austausch mit der Stiftungsverwaltung.

Zu Frage 2:

Die Mitteilungen des BSI werden durchgängig sehr genau verfolgt. Die Stadt orientiert sich ganz klar nach deren Sicherheitshinweisen zu Schwachstellen und den entsprechenden Empfehlungen. Die IT-technische Bedrohungslage im konkreten Zusammenhang mit der politischen Bedrohungslage als Kommune zu bewerten, ist alles andere als einfach. Die Stadt ist hier in weitgehendem Umfang auf die Einschätzungen der zuständigen Behörden, insbesondere des BSI, angewiesen. Durch die Verbindungen Freiburgs - insbesondere zu Lviv - ist die Bedrohungslage nach unserer Einschätzung gegenüber der ohnehin gegebenen Bedrohungslage nochmals erhöht.

Demzufolge geht die Stadt von einer sehr ernst, aber mit schwer bestimmbarer Eintrittswahrscheinlichkeit versehenen Bedrohung aus, so dass für Maßnahmen zur erneuten und erweiterten Überprüfung des IT-Sicherheitsstatus sowie der kurzfristigen Ablösung der Antivirensoftware-Lösung Eilbedürftigkeit besteht.

Zu Frage 3:

Die Ablösung von Kaspersky wird bereits seit längerem geprüft, zugunsten einer diversifizierten Sicherheitsinfrastruktur. Die bisherigen Arbeiten sind für die aktuelle Situation daher nur bedingt verwendbar. Die Verwaltung analysiert aktuell die kurzfristigen Optionen, die wie oben bereits beschrieben, anderweitige Sicherheitslücken entstehen lassen könnten. Aktuell käme für den kurzfristigen, flächendeckenden Ersatz nur die Aktivierung einer bereits anderweitig verfügbaren Antiviren-Lösung in Frage. Dies wäre allerdings nur als Zwischenlösung auf wenige Monate zu sehen, bis eine neue umfängliche Lösung gefunden und implementiert werden könnte. Es gibt bisher keine Vorfestlegung auf andere mögliche Anbieter.

Die Stadt wird alle Möglichkeiten ergreifen, um eine Kompromittierung oder Schädigung unserer Systeme und damit Beeinträchtigung der Arbeitsfähigkeit der Stadtverwaltung zu vermeiden. Das Ende dieser Bedrohungslage ist nicht absehbar, neben der Kaspersky-Thematik wurden grundlegend verschiedene weitere Maßnahmen getroffen, darunter z. B. die Blockade von Netzwerkverbindungen zu Russland bzw. Belarus.

Mit freundlichen Grüßen



Michael Schulz

Anlage