

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Roman-Francesco Rogat (FDP)

vom 30. März 2022 (Eingang beim Abgeordnetenhaus am 31. März 2022)

zum Thema:

Virenschutzsoftware in Berliner Verwaltungen

und **Antwort** vom 14. April 2022 (Eingang beim Abgeordnetenhaus am 21. April 2022)

Herrn Abgeordneten Roman-Francesco Rogat (FDP)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/11406
vom 30.03.2022
über Virenschutzsoftware in Berliner Verwaltungen

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

Vorbemerkung:

Die Beantwortung der Fragen erfolgt mit Bezug auf den Geltungsbereich des E-Government-Gesetzes Berlin.

1. Wie wird der Schutz vor Schadsoftware wie Viren und Trojanern etc. in den einzelnen Berliner Verwaltungen, Bezirksamtern und nachgelagerten Behörden und Betrieben allgemein sichergestellt? (Bitte tabellarisch auflisten)
 - a. Welche Instanz ist in den einzelnen Berliner Verwaltungen, Bezirksamtern und nachgelagerten Behörden und Betrieben für Cybersicherheit zuständig? (Bitte tabellarisch auflisten.)

Zu 1.:

Der Schutz vor Schadsoftware wird für die Verwaltung des Landes Berlin im Rahmen der Umsetzung der IKT-Sicherheitsarchitektur sichergestellt. Das beinhaltet das Handeln nach methodischen und technisch-organisatorischen Richtlinien, die Nutzung von IKT-Basisdiensten zur IKT-Sicherheit, die Umsetzung von Standard IKT-Sicherheitsvorgaben im Sinne der dezentralen Verantwortung auf der Basis zentraler Vorgaben der IKT-Steuerung.

Zu 1a:

Cybersicherheit ist ein Querschnittsthema und umfasst alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik insbesondere bei der Kommunikation via Internet. Im Sinne der Informationssicherheit in den Behörden und Einrichtungen der Berliner Verwaltung ist sie ein Bestandteil bei den zu betrachtenden Risiken und den dazu abzuleitenden Maßnahmen.

Für die über das Informationssicherheitsmanagement hinausgehenden Sachverhalte liegt die Zuständigkeit in der bei SenInnDS tätigen Arbeitsgruppe Cybersicherheit, die sich mit Grundsatzangelegenheiten der Computer- und Internetkriminalität sowie dem Schutz der digitalisierten kritischen Infrastrukturen unter sicherheitspolitischen Aspekten befasst.

In der Polizei Berlin bündelt die Zentralstelle Cybercrime des Landeskriminalamts Berlin die Kompetenzen hinsichtlich der Cybersicherheit in Bezug auf strafrechtliche Ermittlungen und polizeirechtliche Tätigkeiten.

Dem Ressortprinzip folgend beschäftigen sich darüber hinaus Behörden im Kontext der Digitalisierung mit Fragen der Cybersicherheit, wie z.B. die SenWiEnBe und die Digitalagentur Berlin im Bereich der Umsetzung der Berliner Digitalisierungsstrategie für die Berliner Wirtschaft.

2. Welche Virenschutzsoftware wird von den Berliner Verwaltungen, den Bezirksamtern und nachgelagerten Behörden und Betrieben verwendet? (Bitte tabellarisch nach auflisten.)
 - a. Welchen Kriterien gibt es für die Auswahl einer Virenschutzsoftware? (Bitte nach Verwaltungen und nachgelagerten Behörden und Betrieben einzeln beantworten.)
 - b. Welche dieser Kriterien werden durch die aktuell implementierte Virenschutzsoftware erfüllt? (Bitte nach Verwaltungen und nachgelagerten Behörden und Betrieben einzeln beantworten.)

Zu 2.:

Die für den BerlinPC und die IKT der Verwaltung genutzten Virens Scanner sind in der IKT-Architekturliste für das Land Berlin verbindlich festgesetzt. Der Bezug erfolgt aus Rahmenverträgen über das ITDZ Berlin. Die Ausschreibung der Rahmenverträge erfolgte nach Anforderungen gemäß dem BSI IT-Grundschutz und den betrieblichen Anforderungen des ITDZ Berlin für verfahrensunabhängige und verfahrensabhängige IKT.

Aus Gründen der Informationssicherheit werden die im ITDZ Berlin im Einsatz befindlichen Produkte nicht veröffentlicht. Es werden ausschließlich Lösungen nach BSI-Grundschutzanforderungen eingesetzt. Da das ITDZ Berlin ein mehrstufiges Antivirenkonzept umsetzt, werden unterschiedliche Produkte von unterschiedlichen Herstellern an verschiedenen Punkten eingesetzt.

Von einer detaillierten Auflistung der verwendeten Virenschutzsoftware in den Berliner Verwaltungen, den Bezirksamtern und nachgelagerten Behörden und Betrieben, die noch nicht migriert sind, wird mit Blick auf die Sensibilität dieser Informationen und zum Schutz der IKT-Sicherheit im Land Berlin ebenso abgesehen. Die gleiche Einschätzung hinsichtlich der Sicherheitsbedenken für diese Angaben gilt auch für die Auswahlkriterien für die aktuell implementierte Virenschutzsoftware.

3. Gibt es regelmäßige Penetrationstests in den Verwaltungen, den Bezirksämtern und nachgelagerten Behörden und Betrieben, um die Belastbarkeit des Schutzes praktisch zu erproben? Wenn ja,
 - a. in welchen Verwaltungen und nachgelagerten Behörden und Betrieben?
 - b. zu welchem Ergebnis kamen die Tests? (Bitte nach Verwaltungen und nachgelagerten Behörden und Betrieben einzeln beantworten.)
 - c. welche Handlungsempfehlungen wurden hieraus abgeleitet? (Bitte nach Verwaltungen und nachgelagerten Behörden und Betrieben einzeln beantworten.)

Zu 3.:

Das Instrument des Penetrationstestes wird in der Mehrzahl der Senatsverwaltungen und Bezirke nicht standardmäßig eingesetzt.

Penetrationstest werden regelmäßig bei Berliner Feuerwehr im Rahmen von IT-Sicherheitsüberprüfung und zur Simulation von Cyberangriffen, der Gedenkstätte Deutscher Widerstand, sowie in der SenSBW und der SenUMVK bei der Einführung neuer Techniken und in besonders sicherheitskritischen Einsatzfeldern durchgeführt.

Weiterhin kommen Penetrationstest als Maßnahme gemäß den Anforderungen aus dem BSI IT-Grundschutz im Ergebnis der Risiko-Analyse bei Fachanwendungen bzw. Plattformen sowie anlassbezogen bei der Polizei Berlin, dem LABO, SenBJF und SenFin zur Anwendung.

Von einer detaillierten Auflistung der Ergebnisse zu den durchgeführten Penetrationstests wird mit Blick auf die Sensibilität dieser Informationen und zum Schutz der IKT-Sicherheit im Land Berlin abgesehen. Die gleiche Einschätzung hinsichtlich der Sicherheitsbedenken für diese Angaben gilt auch für die aus den Ergebnissen abzuleitenden Handlungsempfehlungen.

4. Wer ist für die Implementierung von Virenschutz in den Berliner Verwaltungen und nachgelagerten Behörden und Betrieben verantwortlich? (Bitte tabellarisch auflisten.)

Zu 4.:

Die Implementierung von Virenschutz als Teil der Umsetzung von Standard IKT-Sicherheitsvorgaben erfolgt in den Behörden in dezentraler Verantwortung auf der Basis zentraler Vorgaben der IKT-Steuerung.

Das ITDZ Berlin verantwortet die Implementierung des Virenschutzes für die zum ITDZ Berlin migrierten Behörden/Betrieben (Übernahme des dezentralen IKT-Betriebs) auf der Grundlage der sogenannten ITIS-Verträge (ITIS, BerlinPC). Die Behörden sind in den nachstehenden Tabellen aufgeführt.

Aus Gründen der Informationssicherheit werden die eingesetzten Produkte im ITDZ Berlin nicht veröffentlicht. Es werden ausschließlich Lösungen nach BSI-Grundschutzanforderungen eingesetzt. Da das ITDZ Berlin ein mehrstufiges Antivirenkonzept umsetzt, werden unterschiedliche Produkte von unterschiedlichen Herstellern an verschiedenen Punkten eingesetzt.

Kunde	Client-umgebungen	Verantwortung	eingesetztes Produkt
ITDZ Berlin	BerlinPC	ITDZ Berlin	Produkt A
IToG	JustizPC	ITDZ Berlin	Produkt A
Kammergericht	JustizPC	ITDZ Berlin	Produkt A
KITA NO	ITIS2.0	ITDZ Berlin	Produkt B
KITA NW	ITIS2.0	ITDZ Berlin	Produkt B
KITA SW	ITIS2.0	ITDZ Berlin	Produkt B
LAF	ITIS2.0	ITDZ Berlin	Produkt B
LEA - ehemals LABO, Abteilung 4	ITIS2.0	ITDZ Berlin	Produkt B
LVwA	ITIS2.0	ITDZ Berlin	Produkt B
Polizeipräsident - BOWI/Magazinstraße	ITIS2.0	ITDZ Berlin	Produkt B
Senatskanzlei - Standort Warschauer Straße	ITIS2.0	ITDZ Berlin	Produkt B
SenBJF - Standort Flottenstraße	ITIS2.0	ITDZ Berlin	Produkt B
SenBJF - ZSVU inkl. SchullPV	eGoV@school	ITDZ Berlin	Produkt B
SenInnDS - Standort Klosterstraße	ITIS2.0	ITDZ Berlin	Produkt B
SenInnDS - Standort Martin-Hofmann-Straße	BerlinPC	ITDZ Berlin	Produkt A
SenInnDS - Standort Olympiapark	BerlinPC	ITDZ Berlin	Produkt A

Kunde	Serverumgebungen	Verantwortung	eingesetztes Produkt
Berliner Verwaltung	PaaS	ITDZ Berlin	Produkt C
Berliner Verwaltung	BerlinCloud - Windows Server	ITDZ Berlin	Produkt C
Berliner Verwaltung	BerlinCloud - Linux Server	ITDZ Berlin	Produkt C
Berliner Verwaltung	BerlinCloud - FileServer	ITDZ Berlin	Produkt C
Berliner Verwaltung	BerlinCloud - Filetransferserver	ITDZ Berlin	Produktkombination
Berliner Verwaltung	BerlinCloud - Mailserver	ITDZ Berlin	Produkt D

Behörden/Betriebe, die bislang nicht zum ITDZ Berlin migriert sind und bei denen noch keine Übernahme des dezentralen IKT-Betriebs durch das ITDZ Berlin vorliegt, implementieren die genutzte Virenschutzsoftware unter Nutzung der Update-Funktionalität der Antivirussystemanbieter in eigener Verantwortung

auf Grundlage zentraler Vorgaben der IKT-Steuerung und nach BSI IT-Grundschutz.

5. In welchen Abständen wird der Virenschutz aktualisiert? (Bitte nach Verwaltungen und nachgelagerten Behörden und Betrieben tabellarisch aufschlüsseln.)

Zu 5.:

Der Updatezyklus des Virenschutzes ist für die vom ITDZ Berlin betreuten Behörden in nachstehenden Tabellen aufgeführt:

Kunde	Client-umgebungen	Verantwortung	eingesetztes Produkt	Updatezyklus
ITDZ Berlin	BerlinPC	ITDZ Berlin	Produkt A	2x täglich
IToG	JustizPC	ITDZ Berlin	Produkt A	2x täglich
Kammergericht	JustizPC	ITDZ Berlin	Produkt A	2x täglich
KITA NO	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
KITA NW	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
KITA SW	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
LAF	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
LEA - ehemals LABO, Abteilung 4	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
LVwA	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
Polizeipräsident - BOWI/Magazinstraße	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
Senatskanzlei - Standort Warschauer Straße	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
SenBJF - Standort Flottenstraße	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
SenBJF - ZSVU inkl. SchullPV	eGoV@school	ITDZ Berlin	Produkt B	2x täglich
SenInnDS - Standort Klosterstraße	ITIS2.0	ITDZ Berlin	Produkt B	2x täglich
SenInnDS - Standort Martin-Hofmann-Straße	BerlinPC	ITDZ Berlin	Produkt A	2x täglich
SenInnDS - Standort Olympiapark	BerlinPC	ITDZ Berlin	Produkt A	2x täglich

Kunde	Server-Umgebungen	Verantwortung	eingesetztes Produkt	Updatezyklus
Berliner Verwaltung	PaaS	ITDZ Berlin	Produkt C	mehrmals täglich
Berliner Verwaltung	BerlinCloud - Windows Server	ITDZ Berlin	Produkt C	mehrmals täglich

Berliner Verwaltung	BerlinCloud - Linux Server	ITDZ Berlin	Produkt C	mehrmals täglich
Berliner Verwaltung	BerlinCloud – FileServer	ITDZ Berlin	Produkt C	mehrmals täglich
Berliner Verwaltung	BerlinCloud – Filetransferserver	ITDZ Berlin	Produkt-kombination	mehrmals täglich
Berliner Verwaltung	BerlinCloud – Mailserver	ITDZ Berlin	Produkt D	mehrmals täglich

Behörden/Betriebe, die bislang nicht zum ITDZ Berlin migriert sind und bei denen noch keine Übernahme des dezentralen IKT-Betriebs durch das ITDZ Berlin vorliegt, aktualisieren die genutzte Virenschutzsoftware unter Nutzung der Update-Funktionalität der Antivirussystemanbieter eigenverantwortlich.

6. In welcher Form unterstützt das Land Berlin die Bezirke bei dem Thema Virenschutzsoftware?

Zu 6.:

In der IKT-Architekturliste für das Land Berlin werden verbindliche Virenscanner für die Nutzung des standardisierten IKT-Arbeitsplatzes bzw. Berlin-PCs aufgeführt. Die IKT-Architekturliste ist maßgeblich für die Produktauswahl von Virenschutzsoftware für Behörden, die noch nicht migriert sind und ihre IT-Systeme eigenverantwortlich vor Schadsoftware schützen.

Das ITDZ Berlin unterstützt die Berliner Verwaltungen einschließlich der Bezirke durch den Abschluss von Rahmenverträgen für Virenschutzsoftware mit Abrufmöglichkeiten aus dem ITDZ Webshop. Im Webshop sind unterschiedliche Produkte für verschiedene Anwendungszwecke erhältlich. Hierzu zählen Produkte für Endgeräte (Clients) und Server, Produkte für Mailserver und Produkte für die Absicherung der Internetanbindung. Alle angebotenen und im ITDZ Berlin eingesetzten Produkte entsprechen den Anforderungen des BSI-Grundschutzes.

Die Behörden, die Virenschutzsoftware/Lizenzen abrufen, betreiben die Software selbst. Die Kunden werden vom ITDZ Berlin proaktiv vor Ablauf der Lizenzen an eine Verlängerung erinnert, um den Virenschutz sicherzustellen. Die Bezirke nutzen das Angebot des Webshops des ITDZ Berlin. Darüber hinaus bietet das ITDZ Berlin Beratungsleistungen zum Thema Informationssicherheit und über Rahmenverträge mit Dienstleistern Unterstützung bei der Implementierung von IT-Sicherheitslösungen an und unterstützt alle am Berliner Landesnetz angeschlossenen Behörden und Einrichtungen aktiv durch den Einsatz von Virenschutzmaßnahmen am zentralen Zugang zum Internet und zu den Netzen des Bundes. Hier werden sowohl E-Mails inklusive Anhängen als auch Web-Traffic auf Viren und Schadcode hin untersucht und gegebenenfalls herausgefiltert.

Weiterhin wurde das ITDZ Berlin vom BA-FK um Unterstützung bei der Implementierung der Antivirenlösung für die Windows Endgeräte gebeten und hat durch direkten technischen Support aus dem Infrastrukturbetrieb des ITDZ Berlin und der Vermittlung eines externen Dienstleisters über den ITDZ Webshop unterstützt.

Berlin, den 14. April 2022

In Vertretung

Dr. Ralf Kleindiek
Senatsverwaltung für Inneres, Digitalisierung und Sport