Senatsverwaltung für Inneres, Digitalisierung und Sport

Herrn Abgeordneten Jan Lehmann (SPD)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/10397
vom 14.12.2021
über log4J-Lücke in der Berliner Verwaltung?

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

1. Wird in den IT-Systemen der Senatsverwaltungen und der Bezirke die Java-Bibliothek log4J genutzt? Wenn ja, in welchen Verwaltungen und in welchen Anwendungen?

Zu 1.:
Ja, in den IT-Systemen der Senatsverwaltungen und der Bezirke wird die Java-Bibliothek log4J genutzt. Im Einzelnen gibt es folgende Rückmeldungen:

Verwaltung	**Betroffene Systeme**	**Bisheriges Vorgehen zur Umsetzung**
Senatskanzlei	1 Anwendung	Patch vom Hersteller
SenBJF	mehrere Anwendungen IKT-Basisdienst mehrere Kleinst-Anwendungen	Java-Update eingespielt 2x Patch eingespielt Risiken durch Einstellungen mitigiert. Weitere Updates von Herstellern werden erwartet.
SenFin und Berliner Finanzämter	Portal-Anwendung mehrere IT-Verfahren	2x Updates eingespielt Patches und Java-Updates mit zusätzlichen Ressourcen
SenGPG	mehrere Anwendungen	2x Updates eingespielt 1 Anwendung gepatcht
SenInnDS	mehrere IKT-Basisdienste mehrere Anwendungen	Risiken durch Einstellungen, angepasstes Monitoring und aktuel-

		le Patche mitigiert. Erste Updates und Patches installiert. Weitere Updates von Herstellern werden erwartet.
SenIAS	1 Anwendung	Risiken durch Einstellungen mitigiert. Updates des Herstellers wird erwartet.
SenJustVA	mehrere IT-Systeme	1x Update installiert. Weitere Updates von Herstellern werden erwartet.
SenKultEuropa	Fehlanzeige	entfällt
SenStadtWohn	mehrere Anwendungen	Erste Updates und Patches installiert. Risiken durch Einstellungen mitigiert. Weitere Updates von Herstellern werden erwartet.
SenUVK	mehrere Anwendungen	Erste Updates und Patches installiert. Risiken durch Einstellungen mitigiert. Weitere Updates von Herstellern werden erwartet.
SenWiEnBe	mehrere Anwendungen	Risiken durch Einstellungen mitigiert. Updates von Herstellern werden erwartet.
BA Charlottenburg-Wilmersdorf	mehrere Anwendungen	Risiken durch Einstellungen und aktuelle Patche mitigiert. Weitere Updates von Herstellern werden erwartet.
BA Friedrichshain-Kreuzberg	mehrere Anwendungen	Risiken durch Einstellungen, angepasstes Monitoring und aktuelle Patche mitigiert. Weitere Updates von Herstellern werden erwartet.
BA Lichtenberg	mehrere Anwendungen und IT-Systeme	Risiken durch Einstellungen und aktuelle Patche mitigiert. Updates von Herstellern werden erwartet.
BA Marzahn-Hellersdorf	mehrere Anwendungen / IT-Systeme benannt	Risiken durch Einstellungen und aktuelle Patche mitigiert. 1 außerplanmäßige Wartung durchgeführt. Weitere Updates von Herstellern werden erwartet.

BA Mitte	mehrere Anwendungen und IT-Systeme	Risiken durch Einstellungen und aktuelle Patche mitigiert. Weitere Updates und Patches von Herstellern werden erwartet.
BA Neukölln	mehrere Anwendungen	Risiken durch erste aktuelle Patche mitigiert. Weitere Updates und Patches von Herstellern werden erwartet.
BA Pankow	mehrere Anwendungen	Risiken durch erste aktuelle Patche, Einstellungen und angepasstes Monitoring mitigiert. Weitere Updates und Patches von Herstellern werden erwartet.
BA Reinickendorf	mehrere Anwendungen	Risiken durch erste aktuelle Patche mitigiert. Weitere Updates und Patches von Herstellern werden erwartet.
BA Spandau	mehrere Anwendungen und Systeme	Risiken durch Einstellungen und erste aktuelle Patche mitigiert. Weitere Updates und Patches von Herstellern werden erwartet.
BA Steglitz-Zehlendorf	mehrere Anwendungen und IT-Systeme	Risiken durch Einstellungen und erste aktuelle Patche mitigiert. Weitere Updates und Patches von Herstellern werden erwartet.
BA Tempelhof-Schöneberg	mehrere Anwendungen	Risiken durch Einstellungen und erste aktuelle Patche mitigiert. Weitere Updates und Patches von Herstellern werden erwartet.
BA Treptow-Köpenick	mehrere Anwendungen	Risiken durch Einstellungen und erste aktuelle Patche mitigiert. Weitere Updates und Patches von Herstellern werden erwartet.
ITDZ	- zentrale und dezentrale IT-Sicherheitssysteme - mehrere Umgebungen für IKT-Basisdienste - IT-Systeme in Betriebsverantwortung des ITDZ	- mit spezifischen Updates versorgt - Erste Patches und Updates wurden installiert. - Weitere Updates von Herstellern werden erwartet.

2. Wurden bereits Maßnahmen ergriffen, um ein Ausnutzen der vom BSI am 11.12.21 im CSW 2021-549032-1232 bekannt gemachten Sicherheitslücke zu verhindern? Welche Maßnahmen sind dies und für wann sind sie geplant?

Zu 2.:
Im ITDZ wurden durch das Cyber Defense Center der Landesverwaltung in Unterstützung des Berlin-CERT unmittelbar nach Bekanntwerden der initialen Log4J-Schwachstelle am 10.12.2021 präventive Maßnahmen gegen eine Ausnutzung am Übergang zum Internet umgesetzt. Sowohl die vom BSI benannten Maßnahmen, als auch Folgemaßnahmen gegen eine Ausnutzung bzw. zur Feststellung von Indikatoren einer Ausnutzung wurden und werden tagesaktuell umgesetzt. Dazu gehören unter anderem die Aktualisierung der Schutzsysteme am Übergang zum Internet, die Filterung von mit Schadsoftware behafteten Daten, sowie die reaktive Blockierung auf die Ausnutzung der Schwachstellen zielender Aktivitäten.

Das Berlin-CERT hat unmittelbar nach Eingang der Meldungen zur kritischen Schwachstelle CVE-2021-44228 [MIT2021] (Log4Shell) sowie zwei weitere Schwachstellen (CVE-2021-45046, CVE-2021-45105) hat das Berlin-CERT alle Einrichtungen mit Zugang zum Berliner Landesnetz mittels CERT-Meldungen informiert. Diese CERT-Meldungen enthielten neben der originären BSI-IT-Sicherheitswarnung spezifisch aufbereitete Sachverhalte und Empfehlungen für die Verwaltung.

Ergänzend wurden vom Landesbevollmächtigten für Informationssicherheit am 13.12.2021 die behördlichen Informationssicherheitsbeauftragten angeschrieben, sowie am 16.12.2021 im Arbeitskreis der IT-Manager zum Sachverhalt informiert.

Aus den Rückmeldungen der Verwaltung ist ersichtlich, dass die Beseitigung der Schwachstellen mit hoher Priorität erfolgt. Dabei sind neben der erforderlichen Zulieferung seitens der Hersteller auch die abschließende Bereitstellung einer wirksamen Beseitigung der Schwachstellen wesentliche Faktoren. Bis zum Zeitpunkt der Beantwortung der schriftlichen Anfrage wurde wiederholt eine nicht vollständige Beseitigung der Schwachstellen festgestellt. In deren Folge ergaben sich durch die teils sehr umfänglichen Test- und Freigabeprozesse aus deren wiederholt erforderlichen Durchführung erhebliche Mehraufwände.

3. Wurden Fälle dokumentiert, in denen die Sicherheitslücke in der Berliner Verwaltung ausgenutzt wurde?

Zu 3.:
Bisher wurden in der Berliner Verwaltung keine Fälle mit Bezug auf die Ausnutzung der Schwachstellen Log4Shell gemeldet.

4. Ist der Beantwortung vonseiten des Senats noch etwas hinzuzufügen?

Zu 4.:
Eine zur Veröffentlichung bestimmte vollumfänglich detaillierte Beantwortung der Fragen 1 und 2, hat nach Abwägung des gemäß Art. 45 Abs. 1 der Verfassung von Berlin verbürgten Informationsanspruchs des Abgeordneten auf

Grund der überwiegenden öffentlichen Interessen einschließlich des Kernbereichs exekutiver Eigenverantwortung an der Geheimhaltung zu unterbleiben. Zu den benannten Schwachstellen existiert bis zum Zeitpunkt der Beantwortung keine nachweislich vollständige und vollumfängliche Lösung zur Beseitigung.
Eine detaillierte Veröffentlichung der betroffenen IT-Systeme, sowie des Standes der bisherigen Maßnahmen der Ausnutzung entgegen zu wirken, würde einer Ausnutzung zum Nachteil und zur Schädigung des Landes Berlin Vorschub leisten.
Eine Einsicht kann nur unter Wahrung der Geheimhaltung erfolgen.

Berlin, den 22. Dezember 2021

In Vertretung

Torsten Akmann
Senatsverwaltung für Inneres, Digitalisierung und Sport