Stadtverordnetenversammlung der
Landeshauptstadt Potsdam

Große Anfrage

Drucksache Nr. (ggf. Nachtragsvermerk)

20/SVV/0232

Einreicher:
Fraktion DIE aNDERE

öffentlich

Betreff:
Cyberattacke auf Rathaus-IT

Erstellungsdatum	17.02.2020
Eingang 502:	18.02.2020/ 17.08.2020
Datum der Sitzung:	01.04.2020
weitergeleitet an das Büro OBM:	

Anlass des Auskunftsersuchens gem. § 29 Abs. 1 BbgKVerf.:

Seit Wochen ist die Arbeit der Stadtverwaltung durch den Cyberangriff beeinträchtigt, der offenbar durch eine Sicherheitslücke in der Software Citrix ermöglicht wurde.

Wir fragen den Oberbürgermeister:

1. **Welche Versionen des Citrix ADC und des Citrix Gateway sind aktuell durch die Landeshauptstadt Potsdam deployed?**
   Durch die Landeshauptstadt Potsdam (LHP) werden zurzeit die aktuellsten Citrix- Versionen, -Patches und -Releases eingesetzt.

2. **Welche Versionen, Releases und Patches sind von der Sicherheitslücke betroffen?**
   Von der Sicherheitslücke sind der Citrix NetScaler ADC and NetScaler Gateway version 11.1 earlier than build 55.13 betroffen.

3. **Welches sind die aktuellsten Versionen, Releases und Patches der Produkte?**
   Die aktuellsten Versionen, Releases und Patches der Produkte sind 13.0 47.24.nc .

4. **Welche Differenz der beiden Produkte besteht zur letzten Full Version, zum letzten Release, zum letzten Patch?**
   Vgl. Fragen 2 und 3. Eine inhaltliche Beschreibung der Differenzen ist nicht ohne umfassende technische Ausführungen bzw. Anfragen beim Hersteller möglich.

5. **Welches Support Pack und welche Service Level Agreements sind für die beiden Produkte mit dem Anbieter vereinbart?**
   Die Landeshauptstadt Potsdam hat über einen Dienstleister einen Kaufvertrag der Citrix-Software mit Pflege geschlossen. Dieser beinhaltet den Kauf der Software sowie die dazugehörigen Updates. Die aktuelle Vertragslaufzeit endet am 01.12.2020.

Unterschrift

Im Rahmen der Aufarbeitung des Vorfalls wurde der Pflegevertrag mit dem Hersteller funktional erweitert und die Vertragslaufzeit auf den 01.12.2022 verlängert. Zusätzlich wurde ein Servicevertrag mit einer Laufzeit von 24 Monaten mit einem regionalen IT-Dienstleister für die fortlaufende Unterstützung bei der Betreuung der Systeme geschlossen.

6. **Wann wurde die Stadtverwaltung aufmerksam auf die Sicherheitslücke?**
   Die Landeshauptstadt Potsdam wurde am 15.01.2020 auf die Sicherheitslücke in dem eingesetzten Netzkoppelelement Citrix NetScaler aufmerksam.

7. **Wie wurde sie aufmerksam auf die Sicherheitslücke?**
   Die Landeshauptstadt Potsdam wurde von einem Vertragspartner am 15.01.2020 mit einem Schreiben auf die Sicherheitslücke aufmerksam gemacht.

8. **Wurde die Stadtverwaltung vom Anbieter auf das Sicherheitsrisiko und die -lücke aufmerksam gemacht?**
   Weder der Anbieter Citrix noch der Dienstleister, mit welchem die entsprechende Vertragsbeziehung besteht (siehe Frage 5), haben gegenüber der Landeshauptstadt Potsdam auf das bestehende Sicherheitsrisiko und die -lücke hingewiesen.

9. **Wurde die LHP von dritter Seite auf das Sicherheitsrisiko und die -lücke aufmerksam gemacht?**
   Vgl. Frage 7

10. **Wurde sie vom Anbieter oder von dritter Seite über Maßnahmen informiert, auf welche Art und Weise das Sicherheitsrisiko zu entschärfen ist?**
    Der Dienstleister, welcher die Landeshauptstadt Potsdam am 15.01.2020 über die Sicherheitslücke informiert hat (siehe Frage 5), gab Empfehlungen zum weiteren Vorgehen. Diese Schritte entsprachen auch dem von der Landeshauptstadt Potsdam vorgesehenen und angewendeten Vorgehen.

11. **Welche Maßnahmen wurden zur Vermeidung des Auftretens eines derartigen Sicherheitsproblems ergriffen?**
    Vergleichbare Sicherheitsprobleme werden auf unterschiedlichen Wegen festgestellt. Regelmäßig erfolgt dies über Informationen durch sogenannte Computer Emergency Responce Teams (CERT) oder durch Meldungen von Lizenzgebern bzw. Vertragspartnern. Die Informationen werden durch den IT-Sicherheitsbeauftragten bewertet. Sofern die Bewertung eine Relevanz für das Sicherheitsniveau hat, werden geeignete Maßnahmen geplant, initiiert, realisiert und evaluiert.

    Bis zum Januar 2020 hat die Landeshauptstadt Potsdam regelmäßig primär Meldungen des CERT-Brandenburg bzw., wie dargelegt, von Vertragspartnern erhalten. Meldungen von Herstellern erfolgen regelmäßig nur dann, wenn diese in einer direkten vertraglichen Beziehung zur Landeshauptstadt Potsdam stehen.

    Eine kurzfristige Maßnahme aus den Erkenntnissen des Ereignisses vom Januar 2020 war die Bewertung der Qualität und Aussagekraft der bisherigen CERT-Meldungen. Im Ergebnis wurde entschieden sich direkt in die Meldungskette des CERT-Bund (BSI) einzubinden und im Umfeld des IT-Sicherheitsbeauftragten im Rahmen der Möglichkeiten täglich über einschlägige Quelle parallel Recherchen vorzunehmen.

12. Wann wurden diese Maßnahmen ergriffen?

Die unter Frage 11 genannten Maßnahmen werden fortlaufend ergriffen. Im konkreten Fall, der Schwachstelle beim Citrix NetScaler, wurden Meldungen des CERT-Bund, welche der Landeshauptstadt Potsdam über das CERT-Brandenburg zur Verfügung gestellt werden, nicht in der erforderlichen Sensibilität bewertet.

13. War dem Oberbürgermeister die Sicherheitslücke vor dem 24. Januar 2020 bekannt?

Am 15.01.2020 wurden das Büro des Oberbürgermeisters sowie alle Beigeordneten telefonisch durch den Fachbereichsleiter E-Government erstmalig über die Citrix-Schwachstelle sowie dessen Entscheidung zur umgehenden Außerbetriebnahme des Systems informiert.

14. Welche Maßnahmen wurden zwischen dem 23.12.2019 und 24.01.2020 ergriffen, um das Sicherheitsrisiko zu entschärfen?

Am 15.01.2020 wurden die beiden Citrix-NetScaler heruntergefahren und am Tag danach ein externer Dienstleister zur Erstanalyse einer möglichen Ausnutzung der Sicherheitslücke sowie zur Analyse der Bedrohung der Systemlandschaft beauftragt. Mit dem Zeitpunkt der Außerbetriebnahme der Systeme war dieser mögliche Angriffsweg nicht mehr verfügbar. Damit wurde das Sicherheitsrisiko wirksam entschärft.

Die Erstanalyse durch den beauftragten Dienstleister am 21.01.2020 ergab, dass es einen nichtautorisierten Zugriff auf den aktiven Citrix NetScaler gab. Am 22.01.2020 wurde zur Bewertung der Lage eine externe IT-Sicherheitsberatung hinzugezogen. Auf der Grundlage einer umfassenden Ergebnisdiskussion wurde dem Oberbürgermeister empfohlen, die Internetverbindung sowie die Verbindung zur Landeshauptstadt Potsdam zu trennen. Zuvor waren die zuständigen Stellen (LKA, BSI, CERT-BB) zu informieren. Entsprechend der Empfehlung verfügte der Oberbürgermeister, die Netzverbindungen ab 17:00 Uhr zu trennen. Mit dieser Maßnahme wurde eine mögliche Ausnutzung der Schwachstelle unterbunden.

15. Wurden explizite Maßnahmen zur Identifikation von Attacken auf der Basis von verschärften Firewall-Regeln auf dedizierten Firewall Applicances oder Application-Firewalls vorgenommen?

Zum Zeitpunkt der Cyberattacke griffen die IT-Sicherheitssysteme der Landeshauptstadt Potsdam, weshalb, wie die Analysen zeigten, der Versuch, Schadsoftware zu installieren, fehlschlug. Die durch den Fachbereich E-Government administrierten Firewall-Systeme haben den Angriff damit bestimmungsgemäß abgebrochen bzw. auf den Citrix NetScaler begrenzt.
Auch weiterhin werden die Firewall-Einstellungen fortlaufend optimiert und für die Zukunft LHP-seitig erhöhte IT-Sicherheitsstandards definiert und umgesetzt.

Weitere Maßnahmen zur Optimierung der Identifizierung und der Abwehr von Angriffen über die Internetanbindung der LHP wurden zwischenzeitig im Zusammenhang mit der Wiederinbetriebnahme der sog. Onlineservices durchgeführt. Diese beinhalten die Aktualisierung der Härtung der Perimeter-Firewall nach aktuellsten Erfahrungen vom Hersteller und der dazugehörigen Community, sowie die Erweiterung des Schutzes von Web Anwendungen.

16. Wurden verfügbare Patches eingespielt?

Der Landeshauptstadt Potsdam wurden von der Firma Citrix neue Festplatten zur Verfügung gestellt, welche im Rahmen der Neueinrichtung auf die Version 13.0.47.24.nc upgedated wurden. Die seit der Version 11.x verfügbaren Patche sind in dieser Version enthalten. Es ist

anvisiert, die seit Kurzem verfügbare Version 13.0.25.24, vor Inbetriebnahme der Citrix NetScaler einzuspielen.

Im Ergebnis der Verwundbarkeit des Systems und der aufgedeckten Kommunikationslücken hat der Hersteller eine Prozessoptimierung bzgl. der Mitteilung über die Verfügbarkeit von Patches und Versionen vorgenommen. Im Zuge der Maßnahmen werden die Kunden (inkl. der LHP) über regelmäßig zu prüfende Kommunikationsdaten (E-Mail-Adressen) informiert. Die LHP hat diesen Optimierungsschritt ebenfalls zum Anlass genommen Ihre Kommunikationsschnittstellen zu optimieren und eine höhere Redundanz erzeugt, d.h. mehr Personen und insbesondere das IT-Sicherheitsmanagement in die Benachrichtigungskette eingebunden.

17. **Wurden nicht mehr aktuelle Releases oder Full Versions aktualisiert?**
Vgl. Frage 16

18. **Unter Anwendung welcher Standardmethodik wurde und wird regelmäßig der Reifegrad der Cyber-Security geprüft?**
Eine Reifegraddefinition der Cyber-Security wird in der Landeshauptstadt Potsdam nicht angewendet. Eine solche isolierte Betrachtung entspräche auch nicht dem notwendigen und umfassenden Betrachtungsfokus der Informationssicherheit. Diese begrenzt sich nicht auf das Gebiet der Cyber-Security. Eine etablierte Standardmethodik zur Bewertung des Reifegrades der Cyber-Security ist der Landeshauptstadt Potsdam zudem nicht bekannt.

Ein Reifegradmodell zur Bewertung der Qualität des Informationssicherheitsprozesses, bspw. in Anlehnung bzw. auf Basis von IT-Grundschutz, wird bisher nicht angewendet. Es ist aktuell anvisiert, das vorhandene Informationssicherheitsmanagementsystem (ISMS) schrittweise zu evaluieren und aus den dabei gewonnenen Erkenntnissen notwendige Schlussfolgerungen zu ziehen und daraufhin ggf. im Ergebnis ein Reifegradmodell für das ISMS bei der Landeshauptstadt Potsdam zu etablieren. Grundsätzlich wird allerdings angestrebt, die Informationssicherheit der Landeshauptstadt Potsdam an den BSI-Standards 100-x auszurichten.

19. **Welche Art von kontinuierlichem Assessment wird durchgeführt, um regelmäßig bei Bekanntwerden von Risiken oder nach Incidents vorliegende Risiken und Probleme zu identifizieren und Maßnahmen zu Abschwächung der Risiken (Risk Management), zur Behebung der Probleme (Issue Management) und zur Beseitigung der Ursachen (Problem Management) zu ergreifen?**
Bisher werden Probleme und Risiken auf verschiedenen Wegen identifiziert, bewertet und behandelt. Regelmäßig wird die LHP durch das Computer Emergency Response Team (CERT) des Landes über Sicherheitslücken informiert. Das CERT-Land nutzt dazu insbesondere Tageslageberichte oder Sicherheitsmeldungen des CERT-Bund. Diese stellt das CERT-Land auf einer Plattform (https://dialog.brandenburg.de) zur Verfügung. Verschiedene Beschäftigte des Fachbereichs E-Government der LHP werden automatisiert über auf der Plattform bereitgestellte Meldungen informiert. Nach der Sichtung der Meldungen erfolgt eine Bewertung hinsichtlich der Relevanz und Dringlichkeit und erforderlichenfalls die Planung und Initiierung von Maßnahmen. Eine weitere Quelle für ein analoges Vorgehen sind Meldungen von Supportfirmen bzw. Vertragspartnern der LHP.

Die LHP hat bisher keine Prozesse auf Basis von ITIL (IT-Infrastructure Library) wie Risk Management, Issue Management und Problem Management etabliert. Jedoch ist die

grundsätzliche Herangehensweise in der LHP durchaus dem ITIL-Rahmenwerk zuordenbar. Insbesondere in der Dokumentation der Prozesse, der personifizierten Rollenzuweisung sowie einer geschlossenen Dokumentation des Prozesses hat die LHP Qualifizierungsbedarf, weshalb hierfür die notwendigen personellen und technischen Voraussetzungen geschaffen werden sollen.

Mit dem Beschluss des Haushalts 2020/2021 wurden dem Fachbereich E-Government eine zusätzliche Anzahl von Stellen zugewiesen. Auf dieser Grundlage war es möglich organisatorische Veränderungen in der Struktur des Fachbereichs E-Government, die die rollenbasierende Prozessunterstützung nachhaltiger unterstützen, zu planen. In diesem Zusammenhang wurden bereits erste Stellenbeschreibungen und Kompetenzprofile an die notwendigen Prozessunterstützungen ausgerichtet.

20. Auf welche Art und Weise stellt der Oberbürgermeister sicher, dass die Mitarbeiter*innen der Stadtverwaltung kontinuierlich auf dem aktuellsten Stand der Cyber-Security Technik bleiben und in der Lage sind, Risiken proaktiv zu identifizieren ohne auf externe Hilfe angewiesen zu sein?

Angriffsszenarien auf IT-Systeme bzw. Informationen entwickeln bzw. verändern sich hochdynamisch, wobei hier von einer täglichen neuen Lage auszugehen ist. Es kann und wird einzelnen Kommunen, einschließlich der LHP, nicht möglich sein, kontinuierlich auf dem aktuellen Stand der Cyber-Security Technik zu sein. Dies ist der Anspruch hochspezialisierter IT-Sicherheitsunternehmen und entsprechenden Forschungseinrichtungen.

Die LHP hat hier abgestuft und differenziert mit umzugehen, was künftig verstärkt durch eine Angriffsvektorbasierte Planung, Implementierung und Evaluation von Maßnahmen erfolgen wird. Im Sinne einer angemessenen Qualifikation sind zunächst Maßnahmen zur Sicherstellung eines hohen Sicherheitsbewusstseins zu sehen. Auf Basis eines Sicherheitsbewusstseins werden konkrete Qualifikationsmaßnahmen bei den IT-Administratoren erfolgreich sein. Die entsprechenden Beschäftigten im Fachbereich E-Government werden im Rahmen von Schulungs- und Sensibilisierungsmaßnahmen auch künftig für die qualifizierte Nutzung der in ihrer Zuständigkeit befindlichen IT-Systeme qualifiziert. Dies ist Voraussetzung dafür, die notwendigen Sicherheitsaspekte kontinuierlich technisch umzusetzen.

Die Inanspruchnahme externer Unterstützung ist ein Standardvorgehen bei komplexen Fragestellungen bzw. bei nicht vorhandenen Kapazitäten und Wissen. Dieses Vorgehen ist notwendig, etabliert und wird auch nicht geändert werden. Wichtig dabei ist, dass entsprechende Dienstleister vertraglich gebunden sind bzw. kurzfristig, je nach Anforderung, gebunden werden können. In dem konkreten Sicherheitsvorfall erfolgte dies vollständig und erfolgreich.

Zur Verbesserung der proaktiven Handlungsfähigkeit ist im Zuge der Stellenbereitstellung über den Haushalt 2020/2021 der Stellen- und Kompetenzaufbau im Sinne einer internen IT-Sicherheitsleitstelle vorgesehen. Diese Stellen sind bereits fest in geplanten organisatorischen Veränderungen in der Struktur des Fachbereichs E-Government integriert.

Begründung:

Nach einer Cyberattacke auf die IT des Rathauses im Januar 2020 sind die Arbeitsprozesse der Stadtverwaltung noch immer erheblich beeinträchtigt.

Mit der Großen Anfrage möchte unsere Fraktion transparent machen, welche Sicherheitslücken aus welchen Gründen auftraten, welche Gegenmaßnahmen möglich waren und ergriffen wurden und welche Konsequenzen der Oberbürgermeister aus dem Vorfall gezogen hat oder noch ziehen will.

Unsere Fraktion geht damit auch mehreren Beschwerden von betroffenen Bürger*innen nach.
Gleichzeitig sind die erbetenen Antworten zur Kontrolle der Verwaltung erforderlich. Geprüft werden soll, ob der Oberbürgermeister seiner Sorgfaltspflicht im Umgang mit persönlichen Daten und bei der Sicherung der Funktionsfähigkeit der Verwaltung hinreichend nachkommt.