LANDKREIS
VORPOMMERN-RÜGEN
wir nordeln.

Landkreis Vorpommern-Rügen, Carl-Heydemann-Ring 67, 18437 Stralsund

Fraktion AfD im Kreistag V-R

Ihr Zeichen:
Ihre Nachricht vom:
Mein Zeichen: Anfrage/2024/052
Meine Nachricht vom:
Bitte beachten Sie unsere Postanschrift unten!

Fachdienst: **Büro des Landrates und des Kreistages**
Fachgebiet / Team: **Kreistagsangelegenheiten**
Auskunft erteilt:
Besucheranschrift: Carl-Heydemann-Ring 67
18437 Stralsund
Zimmer: 119
Telefon: 03831 357 1214
Fax: 03831 357-444100
E-Mail: Kreistagsbuero@lk-vr.de

Datum: 20. Dezember 2024

Ihre Anfrage zum Sachstand IT-Systeme im Landkreis Vorpommern-Rügen und den anhaltenden Folgen des Hackerangriffs

Sehr geehrter Herr Fraktionsvorsitzender Naulin,
Sehr geehrte Damen und Herren,

zunächst möchte ich mich für Ihre Geduld hinsichtlich des überdurchschnittlich langen Beantwortungszeitraums in Bezug auf Ihre Anfrage vom 21. Juli 2024 bedanken. Auch wenn ich regelmäßig im Kreistag über den Cyberangriff bzw. den Stand der Wiederherstellung der IT-Systeme des Landkreises berichtet habe, so enthält Ihre Anfrage teilweise darüber hinaus gehende Fragestellungen, auf die ich im Folgenden näher eingehen möchte.

Dem vorangestellt möchte ich zunächst nochmals grundlegende Informationen zu dem Sicherheitsvorfall geben, da diese zum Verständnis und zur Einordnung Ihrer Fragestellungen beitragen.

Am 27. November 2023 stellten Mitarbeiter des Fachgebietes IT fest, dass sämtliche AD-Konten mit administrativen Berechtigungen infolge mehrfacher fehlerhafter Eingabe des Kennwortes gesperrt waren. Darüber hinaus wurde vom System der Fund einer Schadsoftware gemeldet.

Nach Wiedererlangung des administrativen Zugriffs auf das AD konnte festgestellt werden, dass auf einem System ein Verschlüsselungsversuch gestartet wurde, welcher von den internen Sicherheitsmechanismen verhindert werden konnte. Eine Verschlüsselung von Daten fand nicht statt. Da aber eine Kompromittierung des Systems anzunehmen war, wurde der Sicherheitsvorfall an die zuständigen Stellen gemeldet. Auch die Ermittlungsbehörden begannen am 28. November 2023 mit ihrer Arbeit.

Aufgrund einer Warnung durch die Ermittlungsbehörden erfolgte am 28. November 2023 eine vorsorgliche Trennung der IT-Systeme vom Internet. Im Ergebnis der Bewertung des Sicherheitsvorfalls durch den BeLVIS wurden Sicherheitsmaßnahmen für das Landesdatennetz CN LAVINE aktiviert. Daraus erging eine Sperrung des Zugangs des LK V-R zum Datennetz des Landes und damit auch zum Netz des Bundes und der EU. Weiterhin ergab sich daraus für eine Wiederanschaltung u.a. die Auflage, einen vom BSI zertifizierten APT-Response-Dienstleister mit den forensischen Untersuchungen zu beauftragen.

Die Untersuchungen des APT-Response-Dienstleisters ergaben eine weitgehende Kompromittierung der AD-Infrastruktur des LK V-R. Datenverschlüsselungen und Datenabflüsse konnten nicht festgestellt werden. Vermutungen zum Datum und Eintrittspunkt sowie zum weiteren Weg der Angreifer

im System konnten nicht zweifelsfrei bestätigt werden. Dementsprechend war es nicht möglich einen Termin zu benennen, an dem das AD nachweislich nicht kompromittiert war. Somit schied eine Disaster-Recovery der AD-Infrastruktur aus und der Aufbau einer neuen AD-Infrastruktur wurde notwendig. Zwischenzeitlich wurden am 19. Februar 2024 die Ermittlungen der Staatsanwaltschaft ohne Ergebnis eingestellt.

Da keine Verschlüsselung der Daten erfolgte, konnten alle Mitarbeiter des LK V-R grundsätzlich weiterarbeiten. Auf das Backup-System des LK V-R musste nicht zurückgegriffen werden. Einschränkungen bei der Kommunikation mittels E-Mail wurden durch die Bereitstellung von Notfall-E-Mail-Adressen und Notfall-Internetzugängen abgemildert. Dienstleistungen, die eine Anbindung an die Netze des Landes oder des Bundes benötigten, wurden - soweit keine Übergangslösungen eingerichtet werden konnten - mittels Unterstützung anderer Behörden wahrgenommen.

Nun konkret zu Ihren Fragen:

1. ***Wie ist der aktuelle Ermittlungsstand zum Hackerangriff nach Kenntnis des Landkreises Vorpommern-Rügen?***

Wie bereits auf der Kreistagssitzung am 11. März 2024 mitgeteilt und hier nochmals einleitend dargestellt, wurden die Ermittlungen der Staatsanwaltschaft am 19. Februar 2024 ergebnislos eingestellt.

Die forensischen Ermittlungen wurden mit dem Abschlussbericht Incident Response des APT-Response-Dienstleisters am 09.02.2024 abgeschlossen.

Grundinformationen des Abschlussberichtes:

- Keine eindeutige Identifizierung des initialen Angriffsvektors,
- Kompromittierung der gesamten Domäne durch Kompromittierung des Verzeichnisdienstes (Active Directory - AD),
- Kompromittierung von 14 Systemen festgestellt,
- keine konkreten Hinweise auf eine Datenexfiltration (Datendiebstahl) und daraus resultierende Erpressung/Veröffentlichung/Verkauf der Daten,
- keine konkreten Hinweise bzgl. einer Tätergruppierung.

2. ***Über welche Schwachstelle konnte der Angreifer auf die Infrastruktur zugreifen?***

Weder der mit der Forensik beauftragte BSI zertifizierten APT-Response-Dienstleister noch die Ermittlungsbehörden konnten den Eintrittsweg zweifelsfrei ermitteln.

3. ***Welche Dienstleistungen hat der Kreis durch den Hackerangriff einbüßen müssen? Welche sind wieder verfügbar?***

Durch die Abschaltung der Zugänge (allgemeiner Internetzugang, Landesdatennetz CN LAVINE und Netz des Bundes) gab es Herausforderungen bzgl. der Aufgabenerfüllung bei Dienstleistungen, welche im Rahmen der Prozessbearbeitung auf diese Verbindungen angewiesen sind. Diese Herausforderungen wurden durch das BCM aufgegriffen und nach Möglichkeit durch Notfall- oder Übergangslösungen (Notbetrieb) bewältigt. Mit dem Aufbau der ,,grünen Zone" stehen die Zugänge in dieser wieder zur Verfügung und der Übergang vom Notbetrieb in den Normalbetrieb wird durchgeführt.

4. ***Wann ist mit der Inbetriebnahme der nach wie vor nicht verfügbaren Dienstleistungen zu rechnen? Bitte für jede Dienstleistung eine Schätzung und den Grund der anhaltenden Nicht-Verfügbarkeit angeben.***

Dem Bürger standen mit wenigen Ausnahmen sämtliche Dienstleistungen, allerdings häufig mit veränderten Zugangswegen, zur Verfügung.

Einschränkungen gab es bis Ende April 2024:

- Im Bereich der KfZ-Zulassung und Führerscheinangelegenheiten. Neben der Vereinbarung mit der Hansestadt Greifswald, der Hansestadt Stralsund und der zur Verfügungstellung dessen Infrastruktur in Stralsund für die Fahrerlaubnis- und Zulassungsangelegenheiten, wurde hier zunächst die Aushändigung der Kartenführerscheine nicht vollzogen. Teilweise behalf sich die Führerscheinstelle mit vorläufigen Führerscheinen. Ab dem 9. Januar 2024 wurde diese Arbeitsweise geändert, da zu diesem Zeitpunkt IT-seitig feststand, dass eine Speicherung und Nachmeldung im alten System möglich sein wird. Der Pflichtumtausch der Papierführerscheine wurde nicht bearbeitet. Das Landesamt MV erteilte hierfür eine Ausnahme, welche noch bis zum 19. Januar 2025 gültig ist. Technische Änderungen an Fahrzeugen und Adressänderungen wurden lediglich im absoluten Ausnahmefall bearbeitet. Die Herausgabe von Wunschkennzeichen war nicht möglich, da über den Zugang der Hansestadt Stralsund zum Kraftfahrt-Bundesamt nur mit der Kennung der Hansestadt Stralsund gearbeitet werden konnte. Ein Zugriff auf das eigene Fahrzeugregister und den Kennzeichenpool des Landkreises VR war in dieser Zeit nicht möglich. Versicherungsanzeigen nach § 51 und $ 49 FZV konnten nur eingeschränkt bearbeitet werden. Diesbezüglich wurden die Polizeidienststellen in unserem Landkreis informiert und bei Unstimmigkeiten auf eine telefonische Nachfrage hingewiesen.
- Im Bereich Jagd und Waffen hinsichtlich der Neuerteilung einer Waffenbesitzkarte und der Neueintragung einer Waffe.

5. ***Gab es ein Disaster-Recovery-Konzept für die IT des Landkreises? Wenn ja, wieso hat dieses nicht gewirkt? Wenn nein, wieso wurde keines entwickelt und wurde zwischenzeitlich eines eingeführt?***

Das vorliegende Disaster-Recovery-Konzept konnte aus den o.g. Gründen nicht zur Anwendung gelangen.

6. ***Welches Backupkonzept gab es für die IT des Landkreises? Wurden die Backups in einer isolierten Infrastruktur aufbewahrt? Zum Beispiel mit Hilfe eines Tape Backups oder bei digitaler Sicherung, war der/die Backup-Controller Teil einer Domäne oder arbeiteten diese mit lokal verwalteten Accounts?***

Backups wurden und werden in einer isolierten Umgebung als Tages-, Wochen- und Monatssicherungen auf einem separaten Storagesystem und zusätzlich auf Band gesichert. Da der Landkreis bei dem Hackerangriff keinen Datenverlust erlitten hat, musste jedoch im vorliegenden Fall nicht auf Backups zurückgegriffen werden.

7. ***Waren Zugriffe über bspw. RDP oder andere Fernwartungsprotokolle (auch Drittanbieterlösungen wie TeamViewer) auf die Backup-Controller möglich (aus dem internen Netz/aus dem Internet)? Wenn ja, wie wurde der Zugriff beschränkt? Wenn der RDP Zugriff über eine AD Gruppe beschränkt war, welcher Personenkreis war Teil dieser Gruppe?***

Auf das Managementsystem der Datensicherung hatte der lokale Administrator des Backupsystems über ein Webinterface Zugriff. Auf die Hardware konnte der lokale Administrator per RDP zugreifen. Beide Zugriffe sind ausschließlich aus dem internen Netz möglich.

8. ***Jedes privatrechtliche Unternehmen, welches der KRITIS-Verordnung unterliegt, muss den Anforderungen des BSI genüge tragen. Wurden generelle IT-Sicherheitsstandards, wie z.B. die ISO 27001 oder die BSI-Standards der Reihe 200 in der IT des Landkreises angewandt?***

Als Landrat ist mir der Stellenwert der Informationssicherheit bekannt und aus diesem Grund schreibt die Informationssicherheitsleitlinie des Landkreises die Umsetzung des BSI-Grundschutzes vor und entsprechend werden die BSI-Standards berücksichtigt und angewandt.

LANDKREIS
VORPOMMERN-RÜGEN
wir nordeln.

9. Hat der Landkreis regelmäßig externe Prüfer beauftragt, um die IT-Sicherheit zu prüfen?

Neben der allgemeinen Prüfung und Beratung durch zwei externe, im Bereich IT-Sicherheit tätige Unternehmen zur IT- und Informationssicherheit in 2022, haben in den letzten Jahren haben folgende Audits stattgefunden:

2020 - Audit der DMZ und der Firewallinfrastruktur
2020 - Audit iKfz
2022 - Audit zur Umsetzung der Anschlussbedingungen CN-LAVINE
2023 - Audit iKFz

Mit freundlichen Grüßen

i.V. K. Kerth

Dr. Stefan Kerth
Landrat