Beantwortung der Anfrage

Kreis Bergstraße

Vorlage Nr.: **19-1043/1**
erstellt am: 14.06.2024

Abteilung: Moderne Verwaltung, E-Government und IT
Verfasser/in: Dr. Johannes Bunsch
Aktenzeichen: L 1.4 - KT - Infrastruktur

Beantwortung der Anfrage der AfD-Fraktion vom 29.05.2024 betreffend Cyberkriminalität

Beratungsfolge:

Gremium	Sitzungsdatum	Status	Zuständigkeit
Kreistag		Ö	Kenntnisnahme

Beantwortung der Anfrage:

1. Wie sind die kommunalen Wasserwerke im Landkreis Bergstraße vor Cyberangriffen geschützt und welche Herausforderungen sind noch zu meistern?
2. Wie sind die kommunalen Wasseraufbereitungsanlagen im Landkreis Bergstraße vor Cyberangriffen geschützt und welche Herausforderungen sind noch zu meistern?
3. Wie sind die kommunalen Energieversorger im Landkreis Bergstraße vor Cyberangriffen geschützt und welche Herausforderungen sind noch zu meistern?

Die Fragen 1-3 können nicht beantwortet werden, da diese nicht in die Zuständigkeit des Kreises fallen. Betreiber Kritischer Infrastruktur müssen den Nachweis über die Erfüllung der Anforderungen nach dem IT-Sicherheitsgesetz gegenüber dem BSI erbringen (siehe § 8a (3) IT-Sicherheitsgesetz).

4. Gibt es konkrete Planungen, sollte im Falle eines erfolgreichen Cyberangriffes auf die Kreisverwaltung oder die Verwaltung der Städte und Gemeinden im Kreisgebiet, auf den „Schrank auf Rädern“ von Hessen 3C (CyberCompetenceCentrum) zurückgegriffen werden müssen ? Falls ja, welche Planungen sind das ? Falls nein, in welchem Zeitraum werden entsprechende Planungen fertiggestellt ?

Im Fall eines erfolgreichen schweren Cyberangriffs ist die Aufsichtsbehörde direkt zu informieren. Diese behält sich dann Entscheidungen über die weitere Steuerung und Maßnahmen in der Abwicklung des Angriffsgeschehens zu. In diesem Zusammenhang stehen dem Landkreis natürlich auch alle Unterstützungsangebote des Landes Hessen für Cybernotlagen zur Verfügung.

5. Welche Unternehmen und Dienstleister im Kreisgebiet aus den Bereichen Verwaltung, Energieversorgung, IT/Telekommunikation,Transport-/Verkehrswesen, Medien/Kultur, Gesundheitversorgung, Wasserversorgung/Wasseraufbereitung, Nahrungsmittelversorgung, Finanzwesen, Abfallentsorgung zählen NICHT zur kritischen Infrastruktur (KRITIS) im Sinne des BSI-Gesetzes?

Die Frage kann nicht beantwortet werden, da diese nicht in die Zuständigkeit des Kreises fällt. Zentrale Meldestelle für Betreiber Kritischer Infrastrukturen ist das BSI (siehe § 8b (1) IT-Sicherheitsgesetz).

6. Deutschlandweit werden pro Monat etwa 2 Angriffe auf kommunale Verwaltungen per sogenannter Ransomware bekannt. Welche Abwehrmechanismen wurden installiert um Angriffen per Ransomware im Bereich der Verwaltung zu begegnen?

Das Haupteinfallstor für Ransomware-Angriffe ist nach wie vor der PC-Nutzer. Zu nennen sind hier Phishingattacken, aber auch die Kontamination von Downloadprodukten beliebter Webseiten oder von häufig genutzten Webseiten. Über diese Wege wird im Regelfall eine Schadsoftware installiert, die Zugangsdaten und Aktivitäten des Nutzers aufzeichnet, dem Angreifer übermittelt und so diesem weiteren Zugang zum angegriffenen System ermöglicht.

Die Kreis-IT setzt hierbei auf eine Reihe von Maßnahmen, welche die gesamte mögliche Angriffskette im Blick haben:

1. Schutz des Nutzers vor Phishingattacken. Vorrangig zu nennen wären hier Firewall und Mailfilter.
2. Prüfung von eingehenden Mails
3. Ggf. Sandboxverfahren
4. Sensibilisierung von Mitarbeitern
5. Überwachung des Systems auf besondere Ereignisse (SIEM)
6. Mobile Device Management
7. zentral verwaltete Endpoint Security auf allen Clients und Server
8. kein direkter Internetzugang der Clients, Zugriff erfolgt geschützt über einen Proxyserver
9. automatisches Patchmanagement auf den Clients fürs Betriebssystem, MS Office und Standardsoftware

Weiterhin geplante Maßnahmen für 2024/2025 sind:

- Ausweitung Mailsecurity
- Durchführung Pen-Test
- Durchführung Active-Directory-Audit
- Etablierung SOC
- Etablierung BCM
- Beginn Umsetzung BSI-Basisabsicherung (erhöhter Schutzbedarf) mit späterem Ziel Zertifizierung.

Seltener ausgenutzt werden Schwachstellen in Softwarelösungen, insbesondere Fachanwendungen. In diesem Bereich hat die Kreis-IT nur wenige bis gar keine Eingriffsmöglichkeiten. Einziges Mittel bleibt, veraltete bzw. fehlerhafte Software zu deaktivieren und auszutauschen.

Leider sind viele Fachverfahren nicht auf dem technischen Stand der Zeit. Die Hersteller wissen um ihre jeweilige Marktmacht, in der nicht selten die öffentliche Verwaltung auf bestimmte Produkte angewiesen ist, weil es keine besseren Alternativprodukte gibt. Dies ist ein Grundproblem, dem auch die Kreisverwaltung des Kreises Bergstraße gegenübersteht.

Um Betriebsrisiken zu minimieren verfolgt der Kreis Bergstraße die Strategie, den Betrieb von Anwendungen in den Schutzbereich BSI-zertifizierter Rechenzentren zu verlagern. Der Aufbau eines eigenen, BSI-zertifizierten Rechenzentrums wäre im Vergleich hierzu bei weitem nicht wirtschaftlich. Es ist in diesem Zusammenhang jedoch festzuhalten, dass damit höhere Betriebskosten für den IT-Betrieb einhergehen.

7. Wie kann sichergestellt werden, dass ein Angriff per APT (Advanced Persistant Thread) möglichst schnell bemerkt wird? Wurden bereits Tests durchgeführt, um festzustellen welche Zeitspanne vom Angriff bis zur erfolgreichen Bekämpfung vergeht? Falls nicht, ist das geplant?

Selbst in den bislang bekannten Fällen, in denen eine Kreisverwaltung erfolgreich gehackt wurde (Bsp. Anhalt-Bitterfeld), konnte im Nachgang nicht genau determiniert werden, wie lange sich die Angreifer bereits im Netzwerk aufgehalten haben.

Die Kreisverwaltung stützt sich bei der Abwehr solcher Angriffslagen auf ein SIEM, hinter dem softwaregestützte Abwehrfunktionen in Verbindung mit menschlicher Analytik stehen. Die etablierten Prozesse haben bislang stets eine schnelle Reaktionszeit ermöglicht.

8. Das BSI registriert pro Tag etwa 70 neue Schwachstellen in Softwareprodukten, welche von Verwaltungen eingesetzt werden, 15% dieser Schwachstellen werden als kritisch eingestuft. Wie ist sichergestellt, dass Schwachstellen der Software, welche von Kreisverwaltung oder den Verwaltungen der Städte und Gemeinden im Kreisgebiet eingesetzt werden, entdeckt, gemeldet und behoben werden?

Wenn Schwachstellen entdeckt werden, werden diese dem Anbieter (ekom21 oder Softwarehersteller) zurückgemeldet. Diese müssen dann durch den Softwarehersteller behoben werden. Die Softwarehersteller stellen sogenannte „Patches“ (Softwarekorrekturen) bereit, die von der Kreis-IT unverzüglich installiert werden. Da Softwarehersteller jedoch zunehmend als Application Service Provider auftreten (ASP), werden Sicherheitslücken durch die Softwarehersteller direkt behoben.

9. Deutschlandweit werden in der Software der Verwaltungen pro Jahr etwa 250000 Schadprogramm-Varianten gefunden. Wie ist sichergestellt, dass diese Schadsoftware in der Software der Kreisverwaltung und den Verwaltungen der Städte/Gemeinden im Kreisgebiet möglichst rasch entdeckt und eleminiert wird?

Es wird auf die Antwort zu Frage 6 verwiesen.

10. Die Entwicklung der künstlichen Intelligenz befeuert geradezu die Professionalisierung der Cyberkriminalität. Gibt es von seiten der Kreisverwaltung Pläne bzw. konkrete Umsetzungen, seinerseits KI zur Bekämpfung der Cyberkriminalität einzusetzen?

Die Allgemeinverfügbarkeit von KI-Technologie hat auch zu einem erkennbar sprunghaften Anstieg insbesondere der Qualität der Cyberangriffe geführt. Es ist ohne Zweifel zu erkennen, dass diese Technologien bereits von Anfang an von Cyberkriminellen genutzt werden, um ihre Angriffe zu verbessern.

Die Maßnahmen der öffentlichen Verwaltung sind rein defensiv. Die IT-Systeme müssen angesichts der skizzierten Bedrohungslage ständig weiterentwickelt und auf dem neuesten Stand gehalten werden. Dies bedeutet auch für den Kreis Bergstraße, dass kontinuierlich auf die technischen Entwicklungen reagiert werden muss, bspw. durch Einführung neuer technisches Barrieren. Hierbei können auch Produkte zum Einsatz kommen, die KI einbinden.

Die Investitionen in die Cybersicherheit des Kreises werden deshalb auch weiterhin steigen. Bereits heute liegen die Kosten bereits bei rund 25 % des IT-Budgets. Vor wenigen Jahren waren es gerade einmal 10 %. Es ist davon auszugehen, dass der prozentuale Anteil weiter rasant steigen wird, um die Kreisverwaltung vor Cyber-Angriffen möglichst gut zu schützen. Abschließend sei jedoch angemerkt, dass es trotz aller Maßnahmen schlussendlich keine Garantie gibt, dass es nicht doch zu einem erfolgreichen umfassenden Angriff kommt. Alle Maßnahmen können nur dem Zweck dienen, das Risiko weiter zu reduzieren.

11. Wieviele Cyberangriffe erfolgten 2023 auf die Kreisverwaltung oder die Verwaltungen der Städte/Gemeinden im Kreisgebiet? Wie ist die Entwicklung?

Die Anzahl der Cyberangriffe lässt sich nicht genau beziffern, da diese schlussendlich nicht registriert werden. Die Zahl der Angriffe bewegte sich in 2023 im 7-stelligen Bereich. Es sei darauf hingewiesen, dass die Zählweise für Cyberangriffe unterschiedlich sein kann: Zählt bspw. jede eingegangene Phishing-Mail als ein Cyberangriff? Zählt der Versuch eines Angriffs oder nur Angriffe, die zumindest teilweise erfolgreich waren? Diese Parameter führen zu sehr unterschiedlichen Ergebnissen.
Die Zahl der erfolgreichen Angriffe auf den Kreis lag in 2023 unter fünf. Die Angriffe waren nur sehr begrenzt erfolgreich, die Angriffe konnten jeweils binnen weniger Stunden eingedämmt werden.
Festgehalten werden kann, dass die Tendenz der Angriffe weiter steigend ist, qualitativ und quantitativ. Im Vorfeld des russischen Angriffskriegs gegen die Ukraine (ca. 6 Monate im Vorfeld) stieg das Angriffsniveau deutlich an, mit Beginn der Kriegshandlungen erhöhte sich das Niveau signifikant weiter. Die Angriffe, soweit feststellbar, lassen sich regelmäßig in den russischen Raum zurückverfolgen.
Bislang hat der Kreis Bergstraße glücklicherweise keinen erfolgreichen schweren Cyberangriff zu verzeichnen gehabt, auch dank der getroffenen Maßnahmen.