| **Die Regionaldirektorin** | REGIONALVERBAND RUHR |
|---|---|

# Drucksache Nr.:14/1249-1

| | |
|---|---|
| | 10.10.2023 |
| Fraktionsanfrage Antwort | öffentlich |

| Beratungsfolge | Beratungsstatus | Sitzung am | TOP |
|---|---|---|---|
| Ausschuss für Digitalisierung, Bildung und Innovation | zur Kenntnis | 09.11.2023 | 7.2 |

**Betreff: Antwort auf die Anfrage der FDP-Fraktion Cybersicherheit IT**

**Antwort:**

**1. Wie viele Cyberattacken gab es in den letzten fünf Jahren auf die Verwaltung des RVR und/oder Systeme des Essener Systemhauses? Wie wurden diese abgewehrt?**

Außer laufender Portscans (Prüfung auf vorhandene exponierte Dienste von außen) gab es keine gezielten Cyberattacken.

**2. Welche kritischen Cyberattacken auf die Verwaltung des RVRs und/oder Systeme des Essener Systemhauses gab es? Kam es dabei zu einem Datenverlust und welche Kosten mussten für die Beseitigung der Folgen einer etwaigen Cyberattacke aufgebracht werden?**

Es gab keine kritischen Cyberattacken auf die Verwaltung des RVR. Beim Essener Systemhaus kommt es hin und wieder zu DDOS-Attacken von außen auf die Serverinfrastruktur. Diese Angriffe haben zum Ziel, Dienste lahmzulegen oder einzuschränken. I. d. R. werden solche Angriffe durch Ändern von Routen behoben. Für den RVR bestanden bis auf eine zeitweise verlangsamte Internetleitung, die beim ESH gemietet ist, keine Einschränkungen. Die SAP-Instanz, die der RVR beim ESH nutzt, war bisher kein Ziel von Angriffen.

**3. Sind seitens des RVRs Akutmaßnahmen nach der Cyberattacke auf die Verwaltung der Stadt Witten im Oktober 2021 vorgenommen werden und falls nicht, warum nicht?**

Ja, es wurden u. a. alle externen Schnittstellen an den Arbeitsstationen gesperrt, sowie Regeln für den Zugriff auf externe Netze (z. B. Internet), Daten und Dienste verschärft. Auch Regeln für den E-Mail-Verkehr wurden überprüft und ggf. angepasst.

**4. Welche Konsequenzen zieht die Verwaltung des RVRs aus den Cyberattacken auf Kommunen im Verbandsgebiet (und darüber hinaus)?**

Als Konsequenz wird neben der Aufrüstung bestehender technischer Abwehrsysteme ein Informationsmanagementsystem eingeführt (ISMS), mit dem IT-Sicherheit auch institutionell und organisatorisch eingeführt wird. Zudem wird im Jahr 2024 ein Sicherheitsbeauftragter bzw. eine Sicherheitsbeauftragte eingestellt. Es wird eine Zertifizierung nach ISO 27001 angestrebt. Bis zum Erreichen dieser Ziele handelt die IT nach den Empfehlungen und „best practises“ des BSI.

**5. Wie oft werden die IT-Systeme des RVRs/des Essener Systemhauses hinsichtlich der IT-Sicherheit geprüft und durch wen? In welcher Regelmäßigkeit werden diese Systeme aktualisiert, um bestmöglich vor unberechtigtem Zugriff geschützt zu sein?**

Bzgl. des ESH kann hier keine Aussage getroffen werden. Die RVR-Systeme werden derzeit nur sporadisch überprüft. Eine regelm. Prüfung ist im Zuge der o. g. ISMS-Einführung unter der Federführung der Sicherheitsbeauftragten bzw. des Sicherheitsbeauftragten geplant.

**6. Findet ein Austausch zwischen dem RVR und den (Ruhrgebiets-) Kommunen statt, um die eigenen Abwehrmaßnahmen gegen Cyberangriffe zu verbessern?**

Nein. Aufgrund der speziellen Struktur des RVR sind die Anforderungen an die IT-Sicherheit zu Städten und Kommunen grundverschieden. Beim RVR sind beispielsweise keine Dienste, die direkt mit internen Abläufen verknüpft sind, über das Internet erreichbar (z. B. Online-Bürgerservices). Dagegen ist es eine besondere Herausforderung für die RVR-IT, die Sicherheit etwa mit der besonders großen Anzahl an Fachanwendungen und individuellen Arbeitsweisen in Einklang zu bringen.

**7. Über welche Backups verfügt der RVR oder das Essener Systemhaus, damit im Falle eines Systemausfalls vor Ort die Daten zügig wiederhergestellt werden können?**

Der RVR verfügt über Backups in verschiedenen Brandabschnitten des ESH-Rechenzentrums. Das Risiko eines kompletten Datenverlustes ist dadurch minimiert. Backups finden je nach Datenkategorie stündlich bis täglich statt. Alle Backups enthalten entsprechend viele Datenbestände vor, sodass z. B. auch nach einem Ransomware-Angriff ein „sauberer“ Gesamtbestand vorliegt und zügig wiederhergestellt werden kann. Es finden Tests statt, ob gesicherte Datenbestände konsistent sind und wiederhergestellt werden können.

**8. Wie werden die Mitarbeiterinnen und Mitarbeiter der Verwaltung in IT-Sicherheit geschult und mit welcher Regelmäßigkeit?**

Derzeit finden noch keine regelmäßigen Schulungen statt. Zu einzelnen Themen werden anlassbezogen Intranet-Einträge mit Verhaltensempfehlungen zu sicherheitsbezogenen Themen veröffentlicht. Es fand eine hausweite, verpflichtende Online-Schulung mit einem Abschlusstest zum Thema Datenschutz statt. Der RVR plant im Zuge der Einführung des ISMS wiederkehrenden Schulungen und Kampagnen zur „Awareness"-Verbesserung der Mitarbeitenden.

**9. Wie wird das Arbeiten von Mitarbeiterinnen und Mitarbeitern der Stadtverwaltung im Homeoffice vor Cyberattacken geschützt?**

Der Fernzugriff auf sämtliche RVR-Systeme erfolgt ausschl. über eine Remote-Desktop-Technik (Citrix). Im Gegensatz zu oft verwendeten VPN-Zugängen, die ein nicht vertrauenswürdiges Gerät (dazu zählen alle nicht von der IT ausgegebenen und konfigurierten Systeme) mehr oder weniger komplett in das Firmennetz integrieren, findet bei der Remote-Desktop-Technik der einzige Datenaustausch in Form von Eingaben durch Eingabegeräte (Maus, Tastatur, Stift) und der Übertragung von Bildschirminhalten statt. Es kann kein weiterer Datenaustausch zwischen einem gefährdenden Endgerät und der IT-Infrastruktur des RVR stattfinden. Weitere Maßnahmen etwa zur Unterbindung eines Datenaustausches über die Zwischenablage sind zusätzlich vorgesehen.
Generell verfolgt der RVR bei der Einbindung und beim Austausch von externen Diensten und Daten eine „Zero-Trust" Strategie, bei der sämtliche Systeme, die nicht vollständig unter der Kontrolle der RVR-IT stehen, als potentiell gefährdend angesehen werden.

**10. Über welche Qualifikationen verfügen Mitarbeiterinnen und Mitarbeiter in der Verwaltung des RVR, in den Kommunen und beim Essener Systemhaus hinsichtlich IT-Sicherheit?**

Die IT-Sicherheit wird bei sämtlichen Projekten bereits seit vielen Jahren an erster Stelle mitgedacht. Alle Mitarbeitenden sind ausgebildete und erfahrene Fachkräfte, die auf Grund ihrer Ausbildungen Sicherheitsmaßnahmen umsetzen können. Mitarbeitende, die besonders sensible und oder gerade für die Sicherheit angeschaffte Systeme betreuen, sind im Rahmen gezielter Produktschulungen besonders befähigt, diese Systeme sicher zu konfigurieren, zu warten und mit Sicherheitsupdates zu versorgen. Für das IT-Personal des ESH kann hier keine Aussage getroffen werden.

**11. Mit welchen Unternehmen arbeitet die Verwaltung des RVRs bei der IT-Sicherheit zusammen, um die digitale Selbstverteidigung zu verbessern?**

Der RVR arbeitet derzeit mit den Firmen Secunet (ISMS-Einführung), Ritter Technologie (Beratung Sicherheit Linux, Firewall), März (Firewall) und SoftwareOne (Sicherheit bei der MS 365-Einführung) in verschiedenen Gewerken und Projekten bzgl. der IT-Sicherheit zusammen.

**12. In der Stellungnahme zum GPA-Bericht wurde seinerzeit gesagt, der RVR strebe an, sich Sicherheits- und Notfallmanagement zertifizieren zu lassen. Ist das inzwischen erfolgt? Falls ja, durch wen und falls nicht, warum nicht?**

Die Zertifizierung steht am Ende des o. g. Prozesses zur Einführung des ISMS. Der RVR erarbeitet nach Beschluss in der VK vom 18.09.2023 gemeinsam mit der Fa. SecuNet ein Konzept, dessen Bestandteil auch ein Sicherheits- und Notfallmanagement ist.

Die Antwort wurde von Ref. 18 RVR im Auftrag von Ref. 3 RVR erstellt.

| Sachbearbeiter/in | Referat / Referatsleiter/in | Bereich / Beigeordnete/r | Regionaldirektorin Karola Geiß-Netthöfel |
|---|---|---|---|
| **Rieso, Silke** | **Horch, Claudia** | **R3 Bildung und Soziales** | |
| Akt.zeichen | | | |
| | | | |