Stadt Balve
Der Bürgermeister

Balve, 05.11.2024

Informationsvorlage
Nr. ESDS 07/2024

Zuständig:	Fachbereich 3	**öffentlich**
Beteiligt:		**ja**
Bearbeiter:	Frau Schlebrowski/ Herr Flöper	

Tagesordnungspunkt:

Cyberattacke auf die Südwestfalen-IT

Gremium ⇩	**Sitzungstermin ⇩**
Ehrenamt, Schule, Digitalisierung, Soziales	27.11.2024

Finanzielle Auswirkungen: ja

Zuständiges Produkt: 01 04 01

Beschlussvorschlag:

Der Ausschuss nimmt die Ausführungen zur Kenntnis.

Sachdarstellung:

In der Nacht des 29./30.10.2023 wurde die Südwestfalen-IT (SIT) Opfer eines Cyberangriffs des weltweit agierenden, hochprofessionellen Hackerkollektivs AKIRA. Auch wenn dank bestehender Sicherheitsfeatures sowie umgehend ergriffener Maßnahmen die Kompromittierung der gesamten Systemlandschaft verhindert wurde, musste ihr Betrieb aus Gründen der Sicherheit und Forensik zeitweise ganz ausgesetzt werden. Dies, sowie der Neuaufbau des betroffenen Teils im Rechenzentrum und der Wiederanlauf aller übrigen Systeme, führten einerseits zu erheblichen Einbußen in der Leistungserbringung, andererseits zu erhöhten finanziellen Aufwendungen.

Im Folgenden wird der erreichte Stand des Wiederaufbaus zum 30.09.2024 zusammenfassend dargestellt und auf die Aufwendungen seitens der SIT eingegangen und dabei der Zeitraum bis zum 30.09.2024 beleuchtet.
Außerdem wird über die getroffenen Maßnahmen durch die Stadt Balve zur Erhöhung der IT-Sicherheit berichtet.

Erreichter Stand des Wiederanlaufs per 30.09.2024

98% der über 100 durch die Mitglieder des Zweckverbandes priorisierten technischen Dienstleistungen und Produkte sind wieder angelaufen und nahezu gänzlich im Normalbetrieb[1] verfügbar. Für die als besonders prioritär eingestuften Anwendungen – darunter fallen Bürger-, Finanz- und Sozialdienste – wurde der Normalbetrieb bereits vor mehreren Wochen bzw. Monaten erreicht. Zudem konnten zahlreiche weitere Dienste bereitgestellt und neu eingerichtete Zugriffe für eine dreistellige Anzahl externer Webanwendungen ermöglicht werden.
Das IT-Sicherheitsniveau wurde verbandsweit signifikant erhöht, indem sowohl die vom IT-Forensikunternehmen r-tec empfohlenen kurzfristigen, als auch zusätzliche Maßnahmen umgesetzt wurden.

Kosten der Cyberkrise

Die untenstehende Tabelle gliedert die bis zum Stichtag 30.09.2024 entstandenen externen Kosten in die Blöcke IT-Sicherheit und Krisenbewältigung auf.

[1] Normalbetrieb bedeutet: Die Funktionalität (oder: der Funktionsumfang) der jeweiligen Anwendung liegt bei 95-100%. Die Angaben verstehen sich immer als eine verbandsweite Einschätzung; vereinzelt sind kleine Restarbeiten zu erledigen oder die SIT wartet auf eine Zuarbeit externer Partner.

Aufwendungen in EUR (IST-Zahlen)	Nov. und Dez. 2023	Jan. bis Sept. 2024
IT-Sicherheit	378.000,00	458.200,00
davon Lizenzkosten	84.800,00	426.400,00
Krisenbewältigung2	802.700,00	1.161.200,00
davon Lieferantenunterstützung	257.800,00	115.400,00
Gesamt pro Jahr	1.180.600,00	1.619.500,00
Gesamt	2.800.100,00	

*geringe Rundungsunterschiede möglich

Ungefähr 80% dieser externen Aufwendungen haben einmaligen Charakter.

Des Weiteren sind verringerte Umsatzerlöse zu verzeichnen, da die Produkte zeitweise gar nicht zur Verfügung standen und durch den eng an den Prioritäten und Erfordernissen der Zweckverbandsmitglieder orientiertem Wiederaufbau zunächst mit den wichtigsten Funktionen und dann sukzessive im vollen Funktionsumfang bereitgestellt wurden. Sowohl für die hier genannten Zeiträume in 2023, als auch in 2024, ergaben sich Erlösminderungen im einstelligen Millionenbereich. Soweit die Erlösminderungen die Zweckverbandsmitglieder betreffen, erfolgte der finanzielle Ausgleich der Entgeltausfälle 2023 durch eine im September 2024 beschlossene Umlage zur Deckung des Jahresfehlbetrags in 2023 (4,2 Mio.). Im Ergebnis führte dies zu keiner finanziellen Mehrbelastung der Verbandsmitglieder. Diese mussten jedoch durch nicht vollständig verfügbare Verfahren Qualitätseinbußen bei der Softwarenutzung bei identischen Kosten hinnehmen. Für das erste Halbjahr 2024 wurde analog verfahren, so dass die Kosten des Verfahrensbetriebs nicht als Entgelt, sondern per Umlage erhoben wurden.

Bedeutung und Einordnung der Kosten für die Zweckverbandsmitglieder

Die Cyberkrise brachte finanziell verschiedene Auswirkungen mit sich.
Neben kundenindividuellen Aufwendungen, z.B. durch eigene IT-Investitionen, verlustig gegangene Zahlungsansprüche, o.Ä., stand im besonderen Fokus die Umlage der Verbandsmitglieder an die SIT. Diese wurde nachträglich angepasst und um Zusatzbeiträge von mindestens 1,00 Euro je Einwohner erhöht, um den Mehraufwand zu kompensieren.[3]

Wie stark sich die - nicht nur durch die Art und Größe, sondern insbesondere durch den Leistungsbezug - ergebene Belastung insgesamt für jedes

[2] Zur Krisenbewältigung zählen die Maßnahmen für den Neuaufbau, Wiederanlauf und alle Aspekte des Projektmanagements.
[3] Die genaue Betragshöhe je Verwaltung hängt von der Art (z.B. Kreis-/Stadtverwaltung), dem Standort (der Verbandssüden war stärker betroffen) und der Einwohneranzahl ab.

Zweckverbandsmitglied letztlich auswirkt, ergibt sich aus der jeweiligen Aufrechnung der Umlageerhöhungen mit den Gutschriften.

Für die Stadt Balve ergibt sich aus den Nachträgen der Südwestfalen-IT aktuell eine Mehrbelastung von 10.809,22 EUR.

Da die Bedrohungslage durch Hackerangriffe, die Spionage, Sabotage, Datendiebstahl und Erpressung zum Ziel haben, auch in Zukunft akut bleiben wird, muss die SIT mitsamt ihren Eigentümern entsprechend reagieren und ihre Resilienz weiter stärken. Davon profitieren alle, denn ein erneuter Verlust der (teilweisen) Leistungserbringung wiegt schwerer. Dem gilt es, so gut es geht vorzubeugen und dies technisch zu erschweren. Entsprechend werden die – nicht zuletzt in den und durch die Gremien geforderten und beschlossenen – Aufwendungen in die IT-Sicherheit beibehalten und ausgebaut werden. Im Wirtschaftsplan für 2025 sind fast 800.000 Euro anlaufenden Kosten von IT-Sicherheitsmaßnahmen berücksichtigt; beispielsweise wird die jährliche CrowdStrike-Lizenz (Software zur Angriffserkennung) knapp 600.000 Euro p.a. kosten.
Dies wird voraussichtlich zu einer moderaten, allgemeinen Preissteigerung auf das Gesamtproduktportfolio führen.

Sachbericht über die getroffenen Maßnahmen zur Erhöhung der IT-Sicherheit der Stadt Balve

Im Rahmen der Aufarbeitung der Cyberattacke bei der SIT wurden bei der Stadt Balve folgende Maßnahmen zur Verbesserung der IT-Sicherheit angestoßen, um die Systeme und Daten der Stadt Balve zu schützen. Dieser Bericht erläutert die getroffenen und geplanten Maßnahmen zur Erhöhung die Sicherheit in der IT-Infrastruktur.

1. Risikoanalyse

Im ersten Schritt wurde eine umfassende Risikoanalyse mit der Fa. Bechtle durchgeführt, um potenzielle Bedrohungen zu identifizieren. Diese Analyse wurde vom Land NRW finanziert. Sie läuft unter dem Begriff „B-Hard“ und umfasste:

- Bewertung von bestehenden Sicherheitslücken
- Identifizierung kritischer Systeme und Daten
- Einschätzung der Auswirkungen möglicher Angriffe

Die Vorstellung des kompletten Berichts für die Stadt Balve wird Ende des Jahres 2024 stattfinden. Aus den Ergebnissen dieses Berichts wird die Stadt Balve eine Sicherheitsstrategie für die nächsten Jahre ableiten.

2. Technische Maßnahmen

2.1. Komplette Scans aller relevanten Serversysteme

Um Sicherheitslücken frühzeitig zu erkennen, wurden alle relevanten Serversysteme mit den IOC-Scannern Loki und Thor komplett gescannt. Diese Scans ermöglichen die Identifikation bekannter Bedrohungen und Schwachstellen.

2.2. Erweiterte Passwortpolicy

Eine strengere Passwortpolicy wurde eingeführt, um die Sicherheit der Benutzerkonten zu erhöhen. Dies umfasst:

- Anforderungen an Passwortlänge und -komplexität
- Regelmäßige Passwortwechsel

2.3. Redundante Serverarchitektur (bestand bereits)

Die Serverbetriebsarchitektur war bereits redundant ausgelegt, indem eine Spiegelung an zwei Standorten eingerichtet ist. Fällt ein Serverhost aus, kann der Betrieb nahtlos über den anderen Serverstandort weiterlaufen.

2.4. Veeam Backup and Replication Software (bestand bereits)

Die Daten werden mit der Veeam Backup and Replication Software gesichert. Die Maßnahmen umfassen:

- Laufende Replikas (4x täglich)
- Tägliche und wöchentliche Backups
- Vollbackup auf externes Speichermedium

2.5. Multifaktorauthentifizierung (MFA)

MFA wurde bereits für den Zugriff auf unser Netzwerk via VPN-Tunnel implementiert (z.B. für mobile Arbeitsplätze). Bis Ende des Jahres wird die MFA auch für alle Mitarbeiter des Rathauses für Fachanwendungen eingeführt.

2.6. Microsoft LAPS

Die Microsoft Local Administrator Password Solution (LAPS) wurde implementiert. Diese Windows-Funktion verwaltet automatisch die Kennwörter von lokalen Administratorkonten auf Geräten, die in Active Directory eingebunden sind.

2.7. Ersatz des Antivirusprogramms

Bis zum 31.12.2024 wird das bisherige Antivirusprogramm G-Data Enterprise durch eine EDR (Endpoint Detection and Response) oder XDR (Extended Detection and Response) Software ersetzt, um die Sicherheit weiter zu erhöhen.

3. Schulungen

Um die Sensibilität der Mitarbeiter zu erhöhen, wurden folgende Schulungsmaßnahme umgesetzt:

- SoSafe Phishing-Simulation und E-Learning zur Sensibilisierung für Phishing-Angriffe.

4. Netzwerk- und Systemmanagement

4.1. Netzwerksegmentierung

Die Netzwerksegmentierung wird sukzessive umgesetzt, um potenzielle Sicherheitsrisiken zu minimieren und die Zugriffskontrollen zu verbessern.

4.2. Active Directory Cleaning

Eine Bereinigung des Active Directory (Rathaus- und SIT-Domain) wird durchgeführt, um veraltete und nicht mehr benötigte Konten zu entfernen und die Sicherheitsstruktur zu optimieren.

5. Notfallmanagement

Um auf Sicherheitsvorfälle reagieren zu können, wird folgende Maßnahmen getroffen:

- Erstellung eines Notfallplans, der Schritte zur Schadensbegrenzung und Wiederherstellung beschreibt.
- Durchführung von regelmäßigen Notfallübungen, um die Reaktionsfähigkeit zu testen.

6. Risikominimierung durch Diversifikation

Grundsätzlich wurde bereits in der Vergangenheit versucht, durch die Wahl eines anderen Anbieters das Risiko einer zentralen Abhängigkeit zu reduzieren.

6.1 Hosting der Internetseite / Balve APP nicht bei SIT

Die Entscheidung, die Internetseite nicht bei der SIT zu hosten, war ein wichtiger Schritt zur Risikoverteilung. Durch die Wahl eines anderen Anbieters wurde das Risiko einer zentralen Abhängigkeit reduziert. Dadurch war die Stadt Balve auch während des Ausfalls durch die Cyberattacke jederzeit in der Lage Informationen an den Bürger zu übermitteln:

- Erhöhung der Verfügbarkeit: Bei Ausfällen eines Anbieters bleibt die Internetseite bei einem anderen Anbieter online.
- Flexibilität: Die Möglichkeit, Anbieter zu wechseln oder zusätzliche Funktionen zu integrieren, ohne an einen spezifischen Dienstleister gebunden zu sein.

6.2 DMS-Hosting inhouse

Das Hosting des Dokumentenmanagementsystems (DMS) inhouse bietet mehrere Vorteile:

- Kontrolle über Daten: Die Organisation behält die volle Kontrolle über sensible Daten und deren Sicherheit.
- Anpassungsfähigkeit: Interne IT-Abteilungen können das System gezielt an die Bedürfnisse der Organisation anpassen.
- Geringeres Risiko von Ausfällen: Bei Inhouse-Lösungen sind interne IT-Teams oft schneller in der Lage, Probleme zu identifizieren und zu beheben.

Allerdings ist auch zu beachten, dass Inhouse-Lösungen höhere Investitionen in Hardware und Software, sowie Personal erfordern.

6.3 Ratsinformationssystem als Cloudlösung in Planung

Der Ausfall des Ratsinformationssystems während der Cyberattacke hat gezeigt, dass hier eine unabhängige Cloudlösung als optimale Alternative eingeführt werden sollte.

Dies hat zahlreiche Vorteile, insbesondere in Bezug auf die Risikoverteilung:

- Zugänglichkeit: Mitarbeiter können von überall auf das System zugreifen, was die Zusammenarbeit verbessert und die Reaktionsfähigkeit erhöht.
- Skalierbarkeit: Cloudlösungen ermöglichen eine flexible Anpassung ansteigende Nutzerzahlen oder Datenmengen.

Dennoch ist es insbesondere bei Cloudlösungen wichtig, die Sicherheit und den Datenschutz zu berücksichtigen, insbesondere bei der Speicherung sensibler Informationen in der Cloud.

6.4 SIT-unabhängiger WLAN-Zugang

Neben dem gesicherten Netzzugang über die SIT unterhält die Stadt Balve einen SIT-unabhängigen WLAN-Zugang. Der unabhängige WLAN-Zugang kann von Ratsmitgliedern und Besuchern genutzt werden, was die digitale Teilhabe fördert und den Zugang zu Informationen erleichtert. Während der Cyberattacke bestand so die Möglichkeit über Notebooks und einen freien E-Mail-Zugang Daten zu empfangen und zu versenden.

Fazit

Die Risikoverteilung durch die Wahl verschiedener Anbieter und durch unterschiedliche Hosting-Strategien ist ein effektiver Ansatz, um die Sicherheit und Verfügbarkeit digitaler Systeme zu erhöhen. Durch die Kombination von externen Anbietern, Inhouse-Lösungen und Cloud-Diensten kann eine resiliente Infrastruktur geschaffen werden, die flexibel auf Veränderungen reagieren kann.

Die getroffenen / geplanten Maßnahmen zur IT-Sicherheit haben das Sicherheitsniveau der Stadt erheblich verbessert. Eine kontinuierliche Überwachung und Anpassung der Strategien sind jedoch unerlässlich, sowie laufend Anpassungen vorzunehmen, um mögliche Risiken proaktiv zu managen.

Ausblick

Für die Zukunft sind weitere Schulungen und die Integration neuer Technologien geplant, um die IT-Sicherheit weiter zu erhöhen.

H. Mühling
Bürgermeister

A. Flöper
Fachbereichsleiter