STADT NEUSTADT AM RÜBENBERGE
Der Bürgermeister

04.08.2025

Beschlussvorlage Nr.: 2025/095 **öffentlich**

Bezugsvorlage Nr.:

Erhöhung der Cybersicherheit auf den Anlagen des ABN - Projektfeststellung

Gremium	Sitzung am	TOP	Beschluss		Stimmen			
			Vorschlag	abweichend	Einst	Ja	Nein	Enth
Betriebsausschuss	**14.08.2025 -**							

Beschlussvorschlag

Der Umsetzung der Maßnahmen zur Erhöhung der Cybersicherheit auf den technischen Anlagen des ABN wird zugestimmt.

Anlass und Ziele

Der Abwasserbehandlungsbetrieb Neustadt a. Rbge. betreibt im Stadtgebiet von Neustadt a. Rbge. drei Kläranlagen und 123 Schmutz- und Niederschlagswasserpumpwerke. Infolge von gestiegenen Cyberrisiken und neuen Anforderungen müssen diverse technische und organisatorische Maßnahmen ergriffen werden, um wieder den aktuellen „Stand der Technik“ zu erreichen und dauerhaft zu gewährleisten. Grundlage für die Auswahl gezielter Maßnahmen ist das vom Bundesamt für Sicherheit in der Informationstechnik (BSI) definierte Regelwerk, welches als branchenspezifischer Sicherheitsstandard anerkannt wird, den „Stand der Technik“ darstellt und im Falle eines Cyberschadens als juristische Grundlage herangezogen werden kann.

Finanzielle Auswirkungen		
Haushaltsjahr: 2025		
Produkt/Investitionsnummer:		
	einmalig	jährlich
Ertrag/Einzahlungen	0,00 EUR	0,00 EUR
Aufwand/Auszahlung	148.750,00 EUR	14.875,00 EUR
Saldo	**148.750,00 EUR**	**14.875,00 EUR**

Begründung

In Zusammenarbeit mit dem langjährigen IT-Dienstleister des ABN wurde bereits eine umfangreiche Statusanalyse auf Grundlage des vom BSI als branchenspezifischer Sicherheitsstandard definierten Regelwerkes durchgeführt, um wesentliche Abweichungen gegenüber dem „Stand der Technik“ aufzuzeigen. Im Ergebnis dieser Statusanalyse wurde deutlich, dass diverse organisatorische und technische Maßnahmen zur Steigerung der Cybersicherheit und somit zum Schutz der kritischen Infrastrukturen ratsam wären.

Zur Steigerung der organisatorischen Sicherheit sollten verbindliche, schriftlich fixierte Regelwerke und Richtlinien erarbeitet werden, die sowohl für das Betriebspersonal als auch für externe Dienstleister gelten. Hierzu zählt ein Notfallhandbuch. Zudem sollten ein interner Sicherheitsbeauftragter benannt und Awareness-Schulungen durchgeführt werden. Darüber hinaus sollen das Sicherheitskonzept sowie das Netzwerk-Design sowie die Segmentierung des Netzwerkes aktualisiert werden.

Um die technische Sicherheit zu erhöhen, gibt es diverse Verbesserungspotenziale zum Schutz gegen Schadsoftware. Hierzu zählen insbesondere Maßnahmen zur Systemhärtung und die Schaffung einer zentralen gesicherten Lösung für die Fernwartung, welche u.a. mittels eines Sprungservers erreicht werden soll. Mit Hilfe einer Datenschleuse soll der ungehinderte Einsatz mobiler Datenträger und der ungesicherte Datentransfer über die Ferneinwahl oder über die Dienstleister-Notebooks verhindert werden. Zudem sollen Regelungen und technische Lösungen für eine ganzheitliche Datensicherung getroffen werden. Ein Netzwerkmonitoring sollte vorgesehen werden, um frühzeitig Anomalien, Unregelmäßigkeiten und Störungen zu erkennen. Ein Update-Server soll die kontrollierte und geplante Durchführung von notwendigen Updates unterstützen. Eine weitere Maßnahme bildet die Einrichtung eines Login-Management-Systems, unter dessen Anwendung sich jeder Nutzer, der Schalthandlungen vornimmt, entsprechend verifiziert. Ein zentraler Punkt hierbei wäre die vom BSI geforderte Einrichtung einer Zwei-Faktor-Authentisierung. Da aktuell direkt auf den Servern gearbeitet wird, sollte zur Steigerung der Sicherheit ein zusätzlicher PC samt Software angeschafft werden, um ein nachhaltiges Client-Server-System aufzubauen. Darüber hinaus sollte die Firewall auf den aktuellsten Stand gebracht werden.

Um die empfohlenen technischen Systeme miteinander zu verknüpfen, soll eine virtuelle Maschine, ein sogenannter VM-Host, eingesetzt werden. Hierfür ist ein weiterer Rechner samt Programmierung erforderlich, zusätzliche Betriebskosten lassen sich jedoch reduzieren und eine Datenwiederherstellung im Schadensfall aufgrund hardwareunabhängiger Rücksicherung vereinfachen.

Zur weiteren Absicherung soll ein Domain-Controller in zweifacher Ausfertigung ausgeführt werden. Der Domain-Controller ist ein Server zur zentralen Authentifizierung von Computern und Benutzern in einem Rechnernetz, er ermöglicht die gemeinsame Nutzung von Ressourcen bei Dateien und Druckern und ermöglicht die Verschlüsselung von Benutzerdaten.

Der ABN beabsichtigt die weitere Planung voranzutreiben und sukzessive einzelne Maßnahmen in Zusammenarbeit mit dem IT-Dienstleister umzusetzen.

Strategische Ziele der Stadt Neustadt a. Rbge.

Die technischen Anlagen des ABN werden auf der Basis ihres baulichen Zustandes, sowie unter betrieblichen und energetischen Aspekten fortlaufend saniert bzw. erneuert, um den Werterhalt der Anlagensubstanz zu gewährleisten. Der Erhalt des bestehenden hohen Entwässerungskomforts ist in Anbetracht des demographischen und klimatischen Wandels ebenso wichtig.

Auswirkungen auf den Haushalt

Die geschätzten Kosten für die Erhöhung der Cybersicherheit und des Erreichens des „Stands der Technik“ belaufen sich auf ca. 148.750 EUR brutto. Ausreichende finanzielle Mittel stehen im Wirtschaftsplan 2025 des Abwasserbehandlungsbetriebes Neustadt a. Rbge. – ABN – zur Verfügung.

So geht es weiter

Nach positivem Beschluss der Projektfeststellung werden sukzessive einzelne Maßnahmen aus dem gesamten Maßnahmenpaket umgesetzt. Mit der Umsetzung soll noch im laufenden Jahr 2025 begonnen werden.

Fachdienst 68 - Abwasserbehandlungsbetrieb Eigenbetrieb -

Anlage 1 öff Kostenschätzung Cybersicherheit