



Postanschrift: Stadtverwaltung 53754 Sankt Augustin

An die Fraktionen und Fraktionslosen im Rat der Stadt Sankt Augustin

im Hause (per E-Mail)

Dienststelle Bürgermeister- Ratsbüro Markt 1 Auskunft erteilt: Zimmer: 401 Herr v. Borzyskowski Telefon (0 22 41) 243-0 Durchwahl: 394 (0 22 41) 243-430 Durchwahl: 77394 Telefax E-Mail-Adresse: luca.vonborzyskowski@sankt-augustin.de Internet-Adresse: http://www.sankt-augustin.de Besuchszeiten Rathaus Bürgerservice montags bis freitags: montags bis freitags: 8.30 Uhr - 12.00 Uhr, 7.30 Uhr - 12.00 Uhr, montags: montags und donnerstags: 14.00 Uhr - 18.00 Uhr 14.00 Uhr – 18.00 Uhr

Ihr Schreiben vom

Ihr Zeichen

Mein Zeichen

Datum 18.01.2024

BRB-vB 18.0

IT-Resilienz - Anfrage ohne Ausschuss, Aufbruch!, Ds.-Nr.: 24/0019

Sehr geehrte Damen und Herren,

die aufgeführte Frage beantworte ich wie folgt:

## Fragestellung:

Wie ist die Stadt Sankt Augustin auf eine Cyber-Attacke / einen DDoS-Angriff personell, know-how-mäßig, technisch-strukturell, organisatorisch etc. aufgestellt?

## Antwort:

Die IT-Sicherheits-Organisation fußt auf den drei Säulen Prävention, Detektion und Reaktion. Bei den präventiven Maßnahmen handelt sich u. a. um die technische Sicherung des Netzwerks. Diese geschieht nach aktuellsten Kenntnissen, und wird durch Experten, z. B. des bundesweit anerkannten KomCERT, unterstützt. Zusätzlich werden regelmäßig Anpassungen an der technischen Infrastruktur vorgenommen. Gleichzeit werden die Beschäftigten durch permanente Awareness-Maßnahmen, wie z. B. Präsenz- und Online Schulungen sensibilisiert.

Zur Erkennung von Angriffsversuchen werden entsprechende technische Systeme eingesetzt. Die Struktur wird durch externe Sicherheitstests geprüft. Die nächste Überprüfung findet noch im Januar 2024 statt.

Die Stadt Sankt Augustin hat im Rahmen des Notfallmanagements verschiedene Maßnahmen begonnen, um bei einem längerfristigen IT-Ausfall reaktionsfähig zu sein, z. B. im Bereich des Zahlungsverkehrs, des Meldewesens oder der Notfallorganisation.

Aufgrund der permanent steigenden Bedrohungen in den Datennetzen ist trotz moderner Technik in den Abwehrsystemen ein Angriff nicht ausschließbar. So wurden nach Informationen der Deutschen Telekom (sicherheitstacho.eu) in den letzten 30 Tagen über 150 Mio. Ziele in Deutschland angegriffen.

Dabei ist der Mensch das schwächste Glied in der Kette. Dies betrifft sowohl die Erstellung / Programmierung, die Installation und Konfiguration, als auch die Anwendung von Informationstechnik.

Steyler Bank GmbH

Bei einem erfolgten Angriff auf die IT können alle Szenarien, vom Teilausfall bis zum Totalausfall, eintreten. Die zeitliche Abfolge bei der Wiederherstellung bemisst sich dabei auch an den Vorgaben der Strafverfolgungsbehörden und der forensischen Untersuchungen, welche den Ablauf verzögern könnten.

Die Stadtverwaltung versucht durch Sensibilisierungsmaßnahmen und netzwerkunabhängige Backup-Prozesse vitale Funktionen zu stärken. Ein allumfassender technischer oder organisatorischer Schutz ist nicht möglich.

Mit freundlichen Grüßen

Dr. Max Leitterstorf Bürgermeister

Max leither Tor