Anfrage gemäß § 18 Geschäftsordnung der Fraktion Parteilose Fraktion Heinsberg vom 8.8.2022 betreffend Cybersicherheit

Wortlaut der Anfrage:

In der Vergangenheit wurden schon mehrfach Kommunen und Städte in Deutschland zum Ziel von Hackerangriffen, die zum Teil darin mündeten, dass diese Kommunen/Städte erhebliche Summen zahlen mussten, um eine Freischaltung ihrer Systeme durch die Hacker zu erwirken.
Diesem Szenario könnte auch die Stadt Heinsberg einmal ausgesetzt sein.

Aus diesem Grund fragen wir an, ob und wenn ja, welche Maßnahmen die Stadt Heinsberg zur Verhinderung/Abmilderung solcher Angriffe bereits prophylaktisch getroffen hat bzw. welche Maßnahmen noch beabsichtigt werden in diesem Zusammenhang zu treffen.

Darüber hinaus interessiert uns, ob die Stadt Heinsberg den neuen Warn- und Informationsdienst des Landes NRW nutzt (siehe nachstehender Link)?
https://www.land.nrw/pressemitteilung/nordrhein-westfalen-staerkt-cybersicherheit-den-kommunen-mit-neuem-warn-und

Wir bitten um Information hierzu.

Antwort der Verwaltung:

Das Thema Informationssicherheit (Cybersicherheit) wird bei der Stadt Heinsberg als sehr wichtig angesehen.

Maßnahmen zur Umsetzung der Informationssicherheit wurden bei der Stadt Heinsberg bereits im Jahr 2015 getroffen. Seinerzeit erfolgte in Zusammenarbeit mit unserem IT-Dienstleister regio iT eine Bestandsaufnahme der städtischen Infrastruktur (Gebäude und IT). Auf Grundlage dieser Bestandsaufnahme und unter Berücksichtigung der Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfolgte die Umsetzung von erforderlichen Maßnahmen.

Ebenfalls im Jahr 2015 wurden eine „Dienstanweisung Datenschutz und Datensicherheit“ sowie eine „Leitlinie zum Datenschutz und zur Informationssicherheit“ erlassen.

Nachdem die Grundschutzkataloge und die dazugehörige Software durch das BSI nicht mehr aktualisiert wurden, wurde die Entscheidung getroffen, die Informationssicherheit durch die Beauftragung eines externen Informationssicherheitsbeauftragten sicherzustellen, um den steigenden Gefahren von Angriffen weiterhin begegnen zu können. Seit April dieses Jahres wird dies durch einen Mitarbeiter der regio iT übernommen. Zu seinen Aufgaben gehört u.a.

- Beratung der Verwaltung in Fragen zur Informationssicherheit
- Überarbeitung und Fortschreibung der Leitlinie zur Informationssicherheit
- Aufbau, Betrieb und Weiterentwicklung der Informationssicherheitsorganisation
- Erstellung und Fortschreibung des Informationssicherheitskonzeptes
- Aufbau und Pflege der aktuellen Dokumentation von Informationssicherheitsmaßnahmen
- Information der Beschäftigten bei Fragen zur Informationssicherheit
- Information der Beschäftigten über aktuelle Bedrohungen
- Etablierung eines Management Zyklus (PDCA) für die Informationssicherheit
- Stichprobenprüfungen inkl. Dokumentation hinsichtlich der Einhaltung von Vorgaben zum Ziel der stetigen Verbesserung

Generell erfolgt die Ausrichtung der Informationssicherheit hierbei am aktuellen Standard 200-2 des BSI unter Anwendung des IT-Grundschutz-Profils „Basis-Absicherung Kommunalverwaltung“

Um gravierende Sicherheitsvorfälle möglichst abwenden zu können, hat die Stadt Heinsberg auch im Bereich der technischen IT eine Vielzahl von konkreten Maßnahmen etabliert:

- Alle von außen zugängliche Zugriffe auf IT-Systeme und Informationen der Stadt Heinsberg erfolgen über die **DMZ** des Rechenzentrums regio iT in Aachen.
  So z.B. der gesamte E-Mail-Verkehr, alle Webserver, das Bürgerserviceportal usw. sowie der Zugang aller Mitarbeiter(-innen) zum Internet.
  Diese DMZ ist bei der regio iT durch ein mehrstufiges Firewallkonzept und verschiedenen Virenscanmechanismen abgesichert.
  *(Die Abkürzung **DMZ** steht für **Demilitarized Zone** und bezeichnet ein speziell kontrolliertes Netzwerk, das sich zwischen dem externen Netzwerk (Internet) und dem internen Netz befindet. Es stellt eine Art Pufferzone dar, die die Netze durch strenge Kommunikationsregeln und Firewalls voneinander trennt.)*
- Jedes Endgerät und die zentralen Serversysteme der Stadt Heinsberg sind mit einem aktuellen Virenscanner ausgestattet.
- Es kommen nur vom Hersteller supportete aktuelle Betriebssysteme und Softwareprodukte zum Einsatz.
- Seitens der IT-Abteilung erfolgt regelmäßig und zeitnah die Einspielung von aktuellen Updates und Sicherheitspatches.
- Es gibt ein mehrstufiges Datensicherungskonzept (Backup aller Daten) auf verschiedenen Systemen und Auslagerung eines Datensicherungssatzes an einen zweiten Standort.

- Die Überwachung der gesamten Netzwerkstruktur erfolgt in enger Zusammenarbeit mit dem Rechenzentrum der regio iT in Aachen (zertifiziert nach ISO 9001 und ISO 27001).
- Es finden regelmäßige Sicherheitschecks und Schwachstellenscans der gesamten IT-Infrastruktur statt. Auch hierbei erfolgt eine Unterstützung durch die regio iT im Rahmen des gemeinsamen Netzverbundes.

Des Weiteren ist die Stadt Heinsberg Kunde im bundesweiten CERT-Verbund über die KomCERT-Mitgliedschaft.

***(CERT**, das **C**omputer **E**mergency **R**esponse **T**eam für Bundesbehörden, ist die zentrale Anlaufstelle für präventive und reaktive Maßnahmen bei sicherheitsrelevanten Vorfällen in Computer-Systemen.)*

Folgende Leistungen (Auszug der Wichtigsten) werden der Stadt Heinsberg von der KomCERT zur Verfügung gestellt:

- Tägliche (sofern vorhanden) Informationen über Schwachstellen in Softwareprodukten sowie Informationen über aktuelle Sicherheitsvorfälle, kritische Schwachstellen, neue Bedrohungslagen und Themen zur Cybersicherheit. Die Meldungen erfolgen zeitnah per E-Mail an die IT-Abteilung und sind zudem über die entsprechenden Webportale abrufbar.
  Insofern geht die Informationsvielfalt weit über den „Warn- und Informationsdienst des Landes NRW“ hinaus.
- Die IT-Mitarbeiter der Stadt Heinsberg sind angewiesen, zeitnah auf wichtige Informationen zu reagieren.
- Ein Zugriff auf eine Tool- und Linkssammlung zur Unterstützung bei Sicherheitsvorfällen und zu möglichen Selbsthilfe ist möglich.
- Es erfolgt eine Koordinierungsunterstützung bei Bedarf durch folgende Institutionen: Landes-CERT, CERT-Bund, Verfassungsschutz, ZAC (Zentrale Ansprechstelle für Cyberkriminalität in NRW, Staatsanwaltschaft Köln), Ermittlungsbehörden und weitere Einrichtungen.

Alle Maßnahmen unterliegen einer ständigen Überprüfung und werden auch in Absprache mit der regio iT bedarfsgerecht angepasst.