

A N F R A G E

gemäß § 8 der Geschäftsordnung für den Rat der Universitätsstadt Siegen
und seine Ausschüsse

Anfragesteller/in	Volt- Fraktion
Eingang	31.01.2024
Federführend	GB 1, Abt. 1/1-3

Beratungsfolge:

☒ öffentlich

☐ nichtöffentlich

Rat

29.05.2024

Betreff:

**Cyberangriff auf die SIT
- Anfrage der VOLT-Fraktion**

Vorbemerkung:

In der Anfrage ist von der „Stadt Siegen“ die Rede. Ich möchte deshalb vorab daran erinnern, dass der Rat der Stadt Siegen ebenso Organ der Stadt ist. Der Rat ist also ebenfalls ein Teil der Stadt Siegen (vgl. § 40 GO NRW). In diesem Sinne wird deshalb auch die Anfrage beantwortet.

Es kann darüber hinaus der Eindruck entstehen, als ginge die anfragende Fraktion von unzutreffenden Vorbedingungen aus. So ist beispielsweise die SIT qua Satzung für die Sicherheit des Betriebes zuständig gewesen und es handelte sich hier um ein vergleichbar „Geschäft der laufenden Verwaltung“. Auch gilt es die Intention des Rates bei der Besetzung der Entscheidungsgremien der SIT gemäß § 113 GO NRW nicht außer Acht zu lassen.

Frage 1: Ist die Stadt Siegen ihrer Verantwortung bei der Aufsicht sowie Steuerung der S-IT nachgekommen?

Die SIT ist mehr als ein kommunales Rechenzentrum, nämlich ein kommunaler IT-Dienstleister. Kommunen beauftragen einen IT-Dienstleister deshalb, weil dieser Experte für Fragen der IT ist und Kommunen sich somit auf ihre Kernkompetenzen konzentrieren können. Mit interkommunalen, zentralen Strukturen geht auch immer ein Schritt weit einher, dass man eigene Entscheidungsfreiheit ein Stück weit einbüßt. Dazu kommt, dass mit Eintritt in einen interkommunalen Zweckverband immer auch die Möglichkeit des steuernden Eingriffs durch eine einzelne Kommune schwindet, während gleichzeitig auf mehr geballtes Wissen und Kompetenz zurückgegriffen werden kann. Durch die Fusion der KDZ und der citkomm zur SIT sind nun 72 Kommunen Träger des Zweckverbands. Damit ist der Einflussmöglichkeit der einzelnen Träger enge Grenzen gesetzt. Dies ist nicht unbedingt negativ zu werten, da eine durch den Verband vorgegebene einheitliche Linie auch Vorteile mit sich bringen kann.

In der Vergangenheit wurden - neben allen Vorteilen - bereits Verbesserungspotenziale identifiziert und an Lösungen gearbeitet, z.B. die Einführung eines verbandsweiten Informationssicherheitsmanagementsystems (ISMS). Auf Grund der Strukturen des Zweckverbands sind solche Veränderungsprozesse aber immer mit einer langwierigen Entscheidungsfindung verbunden.

Im Sinne des eingangs Beschriebenen ist die Verwaltung der Überzeugung, dass die städtischen Vertreterinnen und Vertreter ihrer Verantwortung nachgekommen sind.

Frage 1.1.: Hat Siegen auf die Warnungen, dass insbesondere Kommunen Opfer derartige Cyber-Angriffe werden können, reagiert? Hat die Stadt Siegen auf die steigenden Bedrohungen reagiert?

Die S-IT und die Stadt Siegen haben Bedrohungen jedweder Art immer sehr ernst genommen. Auch im Zuge des Ukraine-Kriegs wurde entsprechend der Bedrohungslage mit technischen und organisatorischen Maßnahmen reagiert. Als Beispiel kann hier die temporäre Sperrung von Microsoft Office-Mailanhängen genannt werden, die durch eine identifizierte Schwachstelle angeraten worden war.

Dazu kommt, dass der Stellenanteil für die Vorbereitung auf außergewöhnliche Ereignisse vergrößert wurde. Die Stadt Siegen begegnet dieser Herausforderung - nicht nur akut, sondern auch schon vor der Krise - mit der Sensibilisierung der Beschäftigten sowie der regelmäßigen Überprüfung von Prozessen, um auszuloten, ob mit der Anpassung von organisatorischen Maßnahmen die Notwendigkeit für technische Sicherungen verringert werden kann.

Frage 1.2.: Wurden die Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) umgesetzt? Gibt es bei der Stadt Siegen einen ausreichenden IT-Grundschutz?

Die vom BSI bereitgestellten Empfehlungen für den IT-Grundschutz beziehen sich nicht nur auf die technische Absicherung von IT-Systemen, sondern umfassen auch organisatorische Maßnahmen, die teilweise erheblichen Einfluss auf die Geschäftsprozesse haben. Vor dem

Hintergrund, dass eine Kommunalverwaltung unserer Größenklasse tausende Geschäftsprozesse mit zugehörigen Unterstützungsprozessen anbietet, ist die Umsetzung des BSI-Grundschutzes eine Daueraufgabe. Die Stadt Siegen begeht diesen Weg seit einigen Jahren mit der Einführung eines Geschäftsprozessmanagements sowie der Umsetzung des IT-Grundschutzes. Hierzu wurden u.a. schon vor dem Cyber-Angriff zwei Mehrstellen für die Geschäftsprozessoptimierung für den Stellenplan 2024 gemeldet.

Frage 1.3.: Gibt es bei der Stadt Siegen IT-Sicherheitsrichtlinien?

Die Stadt Siegen ist sehr frühzeitig den Weg der interkommunalen Zusammenarbeit gegangen, um so wichtige Themen wie IT-Sicherheit mit anderen Kommunen zusammen angehen zu können. Daher lassen sich viele Aspekte auch nur verbandsweit lösen. Nichtsdestotrotz hat die Stadt Siegen auf die in den letzten Jahren immer weiter steigende Bedrohungslage im Cyberraum reagiert und Stellen für eigene Spezialisten geschaffen, die diese Themen noch spezifischer auf die Belange der Stadt Siegen zugeschnitten umsetzen können. So gibt es bei der Stadt Siegen u.a. auch einen Informationssicherheitsbeauftragten. Weiter wurde regelmäßig vor der Gefahr vor Cyber-Angriffen gewarnt. Passwörter, auch die für das VPN, mussten regelmäßig geändert werden. Notfallpläne im Falle eines Angriffes über Mailings als eines der Haupteinfallstore hingen in den Arbeitsstandorten der Stadt aus. Die Sicherheitskultur innerhalb der Stadt Siegen war damit sehr hoch und wurde gegenüber der S-IT auch in Fachgremien eingefordert.

Frage 2: Welches BCM-Konzept hat(te) die Stadt für den Fall eines Cyber-Angriffs?

Intern waren und sind für den Fall eines solchen Angriffs klare Meldekette festgelegt und wurden bei Entdecken dieses Vorfalls umgehend angewendet. Die entsprechenden Notfallrufnummern der Stadtverwaltung Siegen waren der S-IT bekannt, hinterlegt und wurden umgehend nach Entdecken des Vorfalls angewendet. Auch der daraufhin eingeleitete Prozess bei der Stadtverwaltung Siegen, dem Durchgehen der erweiterten Notfallmeldekette und dem daraus folgenden Einberufen des Stabes für außergewöhnliche Ereignisse (SAE) erfolgte nach einem festgelegten und eingeübten Vorgehen. Darüber hinaus hat die Stadtverwaltung Siegen bereits vor dem Angriff die Stelle eines Informationssicherheitsbeauftragten geschaffen und diesen mit der Erstellung zielgerichteter Notfallplänen für verschiedenste Szenarien, darunter auch ein Ransomware-Angriff, beauftragt. Ebenso wurde die Stelle der Notfallmanagerin mit der Bereitschaft zur Weiterbildung im BCM ausgeschrieben und erste Module wurden besucht. Der Cyber-Angriff fiel genau in diesen laufenden Prozess. Durch die gewonnenen Erkenntnisse der Auswirkungen des Angriffs bietet sich nun die Gelegenheit sog. „blinde Flecken“ in den weiteren Planungen zum BCM zu berücksichtigen.

Frage 3: Welche Rolle spielen Open-Source-Anwendungen vor dem Hintergrund der Suche nach neuen Fachverfahren?

Open Source-Anwendungen werden in den anstehenden strategischen Überlegungen eine Rolle spielen, nicht zuletzt aus Gründen der digitalen Souveränität.