Guten Tag Herrn Nemitz, bitte leiten Sie folgende Anfrage an den Oberbürgermeister der Landeshauptstadt Schwerin weiter.

Konsequenzen aus dem Cyberangriff

Sehr geehrter Herr Oberbürgermeister Dr. Badenschier,

vor dem Hintergrund des Cyberangriffs aus die EDV der Landeshauptstadt Schwerin bitte ich Sie als Stadtvertreter um Beantwortung folgender Fragen

1. Hatten die IT-Dienstleister der Landeshauptstadt Schwerin im Vorfeld des erfolgreich durchgeführten Cyberangriffs im Rahmen des Risikomanagements auf bestehende Sicherheitslücken in der IT der Landeshauptstadt. Schwerin und daraus resultierten Handlungs- und Investitionsbedarfe im Sinne der Datensicherheit hingewiesen? Auch, um zum Beispiel die Ausfallzeiten nach einem etwaigen Cyberangriff auf einen möglichst kurzen Zeitraum des Ausfalls zu begrenzen und die Funktionsfähigkeit der EDV der Stadtverwaltung nach einer Höchstausfallzeit wieder sicherzustellen?

2. Wer war für die augenscheinlich unzureichende, nicht gegebene Cybersicherheit der IT der Stadtverwaltung und die kurzfristig nicht erfolgte Wiederherstellung der Funktionszeit der EDV verantwortlich? Welche Ziele und Vorgaben und Interventionszeiten bzw. maximalen Zeiträume zur Wiederherstellung der Funktionsfähigkeit der EDV nach einem Cyberangriff hatte die Stadt in der Vergangenheit gegenüber den beauftragten IT-Dienstleistern als Krisenszenario formuliert und was wurde / ist darzu mit den Dienstleistern vertraglich vereinbart worden?

3. Welche personellen und organisatorischen sowie Konsequenzen haben Sie im Nachgang aus dem Cyberangriff gezogen? Auch, um einen etwaigen erneuten Cyberangriff zukünftig besser abwehren zu können und einen über viele Wochen andauernde Ausfall der EDV mit massiven Auswirkungen für die Arbeitsfähigkeit der Stadtverwaltung zukünftig zu vermeiden?

4. War und ist die Landeshauptstadt Schwerin im Rahmen ihres Risikomanagements gegen die Schäden durch Cyberangriffen versichert? Waren ggf. die beauftragten IT-Dienstleister der Landeshauptstadt Schwerin gegen Schäden, die bei Kunden durch Cyberangriffe entstehen versichert, so dass der Stadt Schwerin kein Eigenschaden durch den Cyberangriff entstanden ist / entstehen wird? Wie sieht es dazu aus?

Mit freundlichen Grüßen

Stephan Martini

Schäden wegen des Cyberangriff 1

Sehr geehrter Herr Oberbürgermeister Dr. Badenschier,

nachdem nunmehr scheinbar weitgehenst die Folgen des Cyberangriffs auf die Stadtverwaltung behoben worden sind, ich bitte Sie als Stadtvertreter um die Beantwortung folgender Fragen:

1. Sind im Rahmen des Cyberangriffs Daten der Stadtverwaltung oder kommunaler Gesellschaften vernichtet worden und ist die EDV der Stadtverwaltung und der kommunalen Gesellschaften nunmehr wieder voll arbeitsfähig und alle verschlüsselten Daten wieder hergestellt worden?

2. Welche finanziellen oder sonstigen Schäden haben die Landeshauptstadt Schwerin und die kommunalen Gesellschaften aktuell durch den Cyberangriff - Stand 31.03.2022- erlitten und wie setzen sich die Schadenspositionen zusammen?

3. Wer war für die augenscheinlich unzureichende, nicht gegebene Cybersicherheit der EDV der Stadtverwaltung und das Krisenkonzept zur Sicherstellung des weiteren Betriebs der EDV nach einer kurzen Ausfallzeit verantwortlich? Welche Ziele und Vorgaben und Interventionszeiten hatte die Stadt hierzu formuliert und mit den Dienstleistern vereinbart?

4. War und ist die Landeshauptstadt Schwerin gegen die Schäden von Cyberangriffen versichert? Sind ggf. die EDV-Dienstleister der Landeshauptstadt Schwerin gegen Schäden, die bei Kunden durch Cyberangriffe entstehen versichert, so dass der Stadt Schwerin kein Eigenschaden durch den Cyberangriff entstanden ist / entstehen wird?

Mit freundlichen Grüßen

Stephan Martini

LANDESHAUPTSTADT SCHWERIN

Landeshauptstadt Schwerin•Der Oberbürgermeister•10•PF 11 10 42•19010 Schwerin

Der Oberbürgermeister

115 IHRE BEHÖRDENNUMMER

Mitglied der Stadtvertretung
Herrn Stephan Martini

Hausanschrift: Am Packhof 2-6•19053 Schwerin
Zimmer: 4.114
Telefon: 0385 545-1251
Fax: 0385 545-1209
E-Mail: hwollenteit@schwerin.de

Ihre Nachricht vom/Ihr Zeichen	Unsere Nachricht vom/Unser Zeichen	Ansprechpartner/in	Datum
03.04.2022		Herr Wollenteit	12.05.2022

Ihre Anfragen zu den Themen **A. „Konsequenzen aus dem Cyberangriff“**
B. „Schäden wegen des Cyberangriff 1“

Sehr geehrter Herr Martini,

Ihre Anfragen beantworte ich wie folgt:

A. „Konsequenzen aus dem Cyberangriff“

1.) Hatten die IT-Dienstleister der Landeshauptstadt Schwerin im Vorfeld des erfolgreich durchgeführten Cyberangriffs im Rahmen des Risikomanagements auf bestehende Sicherheitslücken in der IT der Landeshauptstadt. Schwerin und daraus resultierten Handlungs- und Investitionsbedarfe im Sinne der Datensicherheit hingewiesen? Auch, um zum Beispiel die Ausfallzeiten nach einem etwaigen Cyberangriff auf einen möglichst kurzen Zeitraum des Ausfalls zu begrenzen und die Funktionsfähigkeit der EDV der Stadtverwaltung nach einer Höchstausfallzeit wieder sicherzustellen?

Die SIS nutzt im Rahmen ihrer Risikofrüherkennung ein risikobasiertes Managementsystem, wobei Konfigurationsänderungen entsprechend der Risikobewertung präventiv durchgeführt werden. In der Umsetzung der gesetzlichen Forderungen des KonTraG hat die SIS das bereits eingerichtete System von Kontrollmaßnahmen um die Strategien zur Aufbereitung relevanter Daten als Voraussetzung für eine effiziente Handhabung bestandsgefährdender und wesentlicher Risiken bzw. Chancen erweitert. Hierzu werden halbjährliche Risiko-Inventuren durchgeführt und zu den identifizierten Risiken erforderliche Maßnahmen und Verantwortlichkeiten festgelegt. Auch im Zuge der Zertifizierung nach ISO 27001 werden im Speziellen die IT-Risiken unter Einbeziehung der Grundanforderungen aus der Informationssicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) betrachtet. Informationen zu Sicherheitsvorfällen und Sicherheitslücken werden von den diversen Sicherheitsbehörden (CERT-M-V, BSI, Verfassungsschutz,) gemeldet und entsprechend vom Sicherheitsteam der SIS/KSM bewertet und erforderliche Maßnahmen daraus abgeleitet und initiiert.

2.) Wer war für die augenscheinlich unzureichende, nicht gegebene Cybersicherheit der IT der Stadtverwaltung und die kurzfristig nicht erfolgte Wiederherstellung der Funktionszeit der EDV verantwortlich? Welche Ziele und Vorgaben und Interventionszeiten bzw. maximalen Zeiträume zur Wiederherstellung der Funktionsfähigkeit der EDV nach einem Cyberangriff hatte die Stadt in der Vergangenheit gegenüber den beauftragten IT-Dienstleistern als Krisenszenario formuliert und was wurde / ist darzu mit den Dienstleistern vertraglich vereinbart worden?

Die Cybersicherheit wurde in den vergangenen Jahren stetig ausgebaut und verbessert. Neben der technischen Aufrüstung wurden auch diverse Sensibilisierungsmaßnahmen bei den Mitarbeitern durchgeführt. Eine 100%-ige Sicherheit ist niemals erreichbar. Sicherheit und Aufwand müssen in einem wirtschaftlichen Verhältnis stehen. Es werden daher immer gewisse Risiken zu akzeptieren sein. Die Aufgabe ist, im Falle eines Angriffs die Schäden zu begrenzen und die Betriebsbereitschaft schnellstmöglich wiederherzustellen.
Die Dauer der Abschaltung der Systeme begründet sich nicht mit einem massiven Datenverlust bzw. deren Rekonstruktion, sondern in der forensischen Analyse, um IT-Systeme und Daten auf Schadcode zu prüfen und keine (eventuell versteckte) Infektionen zu übersehen. Die Arbeiten daran wurden unverzüglich aufgenommen und mit der notwendigen Sorgfalt vorangetrieben, wie es mit dem Dienstleister vereinbart war.

3.) Welche personellen und organisatorischen sowie Konsequenzen haben Sie im Nachgang aus dem Cyberangriff gezogen? Auch, um einen etwaigen erneuten Cyberangriff zukünftig besser abwehren zu können und einen über viele Wochen andauernde Ausfall der EDV mit massiven Auswirkungen für die Arbeitsfähigkeit der Stadtverwaltung zukünftig zu vermeiden?

Im Nachgang des Cyberangriffs gab es eine Auswertung der Aktivitäten nach Eintritt des Schadensereignisses. Hierbei wurden einige Punkte erkannt, die verbessert werden sollen:

- Dokumentation der Infrastruktur, der IT-Verfahren sowie der Datenbestände
- Kontaktmöglichkeiten und Erreichbarkeit nach Ausfall der IT-Infrastruktur
- Priorisierung der IT-Verfahren für den Wiederanlauf
- Enge Abstimmung der IT-Sicherheitsbeauftragten der LHS und des Dienstleisters

Es hat sich gezeigt, dass das Vorhalten regelmäßiger Datensicherungen grundlegend für eine schnelle Wiederherstellung der Betriebsbereitschaft ist. Die Sicherungen waren vorhanden und dem Zugriff des Angreifers physisch entzogen. Dies ist einer der Hauptgründe, weshalb die IT-Verfahren in relativ kurzer Zeit wieder zur Verfügung standen und der reale Datenverlust sich zwischen einigen Stunden und wenigen Tagen bewegte. Dies soll strikt beibehalten werden.

4.) War und ist die Landeshauptstadt Schwerin im Rahmen ihres Risikomanagements gegen die Schäden durch Cyberangriffen versichert? Waren ggf. die beauftragten IT-Dienstleister der Landeshauptstadt Schwerin gegen Schäden, die bei Kunden durch Cyberangriffe entstehen versichert, so dass der Stadt Schwerin kein Eigenschaden durch den Cyberangriff entstanden ist / entstehen wird? Wie sieht es dazu aus?

Die Landeshauptstadt Schwerin hat die Aufgabe IT-Betrieb an die KSM Kommunalservice Mecklenburg AöR (KSM) übertragen. Die KSM ist gegen Schäden aus Cyber-Angriffen versichert. Hinsichtlich der Schadensregulierung läuft aktuell die Abstimmung mit dem Versicherer.

B. „Schäden wegen des Cyberangriff 1“

1.) Sind im Rahmen des Cyberangriffs Daten der Stadtverwaltung oder kommunaler Gesellschaften vernichtet worden und ist die EDV der Stadtverwaltung und der kommunalen Gesellschaften nunmehr wieder voll arbeitsfähig und alle verschlüsselten Daten wieder hergestellt worden?

Es sind keine Daten vernichtet worden; alle Systeme konnten aus den vorhandenen Datensicherungen (nach forensischer Prüfung auf Schadsoftware) wiederhergestellt werden. Es wurden keine verschlüsselten Daten wiederhergestellt, da der Schlüssel nicht vorhanden war und auf die Erpressung nicht eingegangen wurde.

2.) Welche finanziellen oder sonstigen Schäden haben die Landeshauptstadt Schwerin und die kommunalen Gesellschaften aktuell durch den Cyberangriff - Stand 31.03.2022- erlitten und wie setzen sich die Schadenspositionen zusammen?

Durch die schnellen Reaktionen konnte der Schaden enorm begrenzt werden (siehe zum Vergleich Schäden und Ausfallzeiten bei anderen Vorfällen wie z.B. dem Landkreis Anhalt-Bitterfeld). Auf Grund der vorhandenen Datensicherungen konnten verschlüsselte/vernichtete Daten fast vollständig rekonstruiert werden und die Datenverluste hielten sich stark in Grenzen. Durch das eingerichtete Notsystem wurden die wesentlichen Funktionen kurz nach dem Angriff wiederhergestellt. Die forensische Analyse beanspruchte allerdings seine Zeit. Hier ging Gründlichkeit vor Schnelligkeit. Die Ausfallszeit von Systemen beruht überwiegend auf die gründliche Untersuchung und ist keinesfalls ein Index für den entstandenen Schaden. Die sekundär entstandenen Kollateralschäden durch Verfristungen, zusätzliche Aufwände für analoge Bearbeitung und nicht nutzbare Systeme (z.B. mobile Geschwindigkeitsüberwachung) sind nur schwer ermittelbar. Sie sind unter Berücksichtigung der Schwere des Angriffs jedoch als gering anzusehen.
Die genaue Ermittlung von Schäden sowie deren Übernahme durch die Versicherung sind Gegenstand von Verhandlungen mit den Versicherungsunternehmen.

3.) Wer war für die augenscheinlich unzureichende, nicht gegebene Cybersicherheit der EDV der Stadtverwaltung und das Krisenkonzept zur Sicherstellung des weiteren Betriebs der EDV nach einer kurzen Ausfallzeit verantwortlich? Welche Ziele und Vorgaben und Interventionszeiten hatte die Stadt hierzu formuliert und mit den Dienstleistern vereinbart?

Die installierten Sicherheitsmechanismen entsprachen zum Zeitpunkt des Cyberangriffs der Bedrohungslage, waren angemessen und verhältnismäßig. Die Mitarbeiter waren entsprechend sensibilisiert. Eine 100%ige Sicherheit ist auf Grund der Komplexität und der technischen Entwicklung in der IT nicht zu erreichen. Nach Entdeckung des Angriffs wurden umgehend Gegenmaßnahmen eingeleitet, um weiteren Schaden zu verhindern und im Rahmen der Cyberversicherung ein externer Forensikdienstleister hinzugezogen, der umgehend seine Arbeit aufnahm. Der Schwachstelle, die für den Angriff genutzt wurde, konnte damit stark eingegrenzt und der Weg des Angreifers größtenteils nachvollzogen werden. Die Reaktion entsprach den Vereinbarungen zwischen LHS und Dienstleister.

4.) War und ist die Landeshauptstadt Schwerin gegen die Schäden von Cyberangriffen versichert? Sind ggf. die EDV-Dienstleister der Landeshauptstadt Schwerin gegen Schäden, die bei Kunden durch Cyberangriffe entstehen versichert, so dass der Stadt Schwerin kein Eigenschaden durch den Cyberangriff entstanden ist / entstehen wird?

Die Landeshauptstadt Schwerin hat die Aufgabe IT-Betrieb an die KSM Kommunalservice Mecklenburg AöR (KSM) übertragen. Die KSM ist gegen Schäden aus Cyber-Angriffen versichert. Hinsichtlich der Schadensregulierung läuft aktuell die Abstimmung mit dem Versicherer.

Mit freundlichen Grüßen

Dr. Rico Badenschier