Interpellation Nr. 75 (Juni 2023) 23.5304.01
betreffend Datenleck im Erziehungsdepartement und Veröffentlichung von sensiblen Informationen im Darknet

Am 11. Mai hat das Erziehungsdepartement bekanntgegeben, dass es Opfer eines Hacker-Angriffs von Cyberkriminellen geworden ist, welche sich Daten im Gesamtumfang von 1.2 Terabyte bemächtigt haben. Diese Daten wurden nach der Weigerung des Erziehungsdepartements auf die Entrichtung eines Lösegeldes im Darknet veröffentlicht.

Zurzeit laufen gemäss dem Erziehungsdepartement Abklärungen darüber, um welche Daten es sich handelt bzw. welche Personen (Eltern, Schülerinnen und Schüler sowie Fachpersonen und Lehrkräfte) davon betroffen sind bzw. welche Art von Informationen dabei veröffentlicht wurden.

Das Erziehungsdepartement hat zu den Vorkommnissen auf seiner Webseite ein FAQ eingerichtet, auf dem verschiedene, jedoch eher allgemeine Fragen beantwortet werden zur Cyberkriminalität, dem Ablauf dieser Hacker-Attacke und das weitere Vorgehen im aktuellen Fall.

Weniger bzw. praktisch nicht eingegangen wird, wieso diese Attacke erfolgen konnte bzw. warum es den Cyberkriminellen überhaupt möglich war, an Daten in diesem Umfang heranzukommen. Die aktuell wenigen verfügbaren Informationen lassen daher verschiedene Fragen offen. Der Interpellant bittet daher den Regierungsrat um Beantwortung und Stellungnahme zu den folgenden Sachverhalten:

- Werden alle Mitarbeiter über Cyber-Risiken aufgeklärt und wann wurde die letzte Schulung, insbesondere bei der Person, die auf das Phishing-Mail eintrat, durchgeführt?
- Warum konnte der Account dieser Person auf alle diese Daten gleichzeitig zugreifen?
    - Welche Berechtigung gab die Dokumente frei: User, Usergruppe oder Gerät?
    - Brauchte dieser Account für die tägliche Arbeit die entsprechenden Berechtigungen?
    - Auf welcher Basis (z.B. Reglement) wurde diesem Account diese Berechtigungen zugeteilt?
- wie kann es sein, dass Gerät(e) 1.2TB Daten aus dem Netzwerk verschieben können, ohne dass ein Monitoring-System oder die Firewalls eingreifen?
    - Welche Ports/Services dürfen solche Datenmengen über die Firewalls nach aussen verschieben?
    - Warum haben "Outbound" Regeln für die Malware nicht gegriffen? Gab es solche "Outbound" Regeln für den benutzten Service / Port?
    - Oder wurden diese aus Sicht der Firewall(s) innerhalb (Intranet) (und nicht nach aussen (Internet) kopiert? In dem Fall: was für Einschränkungen / Sicherungen bestehen für den Zugriff auf das Intranet von ausserhalb?
- Warum wurde die nicht gerichtete Malware auf dem/n Gerät/en nicht entdeckt?
    - Was ist der Name der Malware und Version? Wie "alt" / bekannt war diese Version zum Zeitpunkt des Vorfalls?
    - Wann wurde der Antivirus das letzte Mal auf dem Einfallsgerät auf den neusten Stand gesetzt?
    - Mit welchen Methoden wurden auf dem Einfallsgerät die Update-Aktualitäten der installierten Softwares/Antiviren-Programmen durchgesetzt?

Im Weiteren ersuche ich den Regierungsrat um die Beantwortung folgender ergänzenden Fragen:

- Wie kann sichergestellt werden, dass künftige solche Hacker-Angriffe vermieden werden können?
- Gemäss dem Informatik-Verantwortlichen des ED, Hrn. Thomas Wenk, im Bericht von SRF 3 am 17.5.2023 bestehen offensichtliche Defizite bei der Informatiksicherheit. Welches sind die akuten Massnahmen, welche getroffen werden, um die Informatik auf einen sicheren Standard zu bringen?

- Wie sieht die Informatik-Sicherheit in den übrigen Departementen des Kantons aus bzw. besteht das Sicherheitsdefizit in der IT des ED auch bei anderen Departementen?
- Gibt es bereits Massnahmen, welcher der Regierungsrat vorsieht, zur allgemeinen Verbesserung der Informatiksicherheit?

Christian C. Moesch