BASEL LANDSCHAFT
REGIERUNGSRAT

Vorlage an den Landrat

Beantwortung der Interpellation 2023/576 von Hannes Hänggi: «Cyberangriffe: Wie gut ist die kantonale Verwaltung geschützt?»
2023/576

vom 6. Februar 2024

1. Text der Interpellation

Am Datum eingeben reichte Hannes Hänggi die Interpellation 2023/576 «Cyberangriffe: Wie gut ist die kantonale Verwaltung geschützt?» ein. Sie hat folgenden Wortlaut:

Mitte Oktober 2023 wurde die Psychiatrie Baselland (PBL) von Computerhackern angegriffen. Die Hacker hatten einen grossen Teil der IT-Infrastruktur verschlüsselt, weshalb die IT-Systeme aus Sicherheitsgründen heruntergefahren worden sind. Während fast zwei Wochen war die PBL nur telefonisch und per Brief erreichbar. In der Presse wurde die Vermutung geäussert, dass hohe Lösegeldforderungen gestellt wurden.

Angesichts der Vielzahl sensibler und persönlicher Daten, die der Kanton von seinen Einwohnerinnen und Einwohnern und seinen Angestellten elektronisch aufbewahrt, stellt sich die Frage nach deren Sicherheit. Mit der fortschreitenden Digitalisierung, Stichwort: «BL digital+», dürfte auch das Interesse von Hackern steigen, an diese Daten zu gelangen. Cyberangriffe dürften in Zukunft an Häufigkeit und Intensität zunehmen.

Der Regierungsrat wird daher gebeten, folgende Fragen zu beantworten:

1. *Wurden im konkreten Fall der Psychiatrie Baselland sensible Patientendaten gestohlen und Lösegeldforderungen gestellt?*
2. *Wie häufig werden Institutionen des Kantons Basel-Landschaft und Institutionen mit strategischen Beteiligungen des Kantons von Hackern attackiert?*
3. *Welche Art von Cyberangriffen gab es in den vergangenen fünf Jahren?*
4. *Kann man Aussagen darüber treffen, wer die Angreifer sind?*
5. *Wie häufig werden Lösegeldforderungen gestellt und in welcher Höhe? Hat der Kanton schon einmal bezahlt?*
6. *Stehen dem Kanton ausrechend Mittel und Personal zur Verfügung, um auf Cyberangriffe reagieren zu können, laufende Angriffe abzuwehren und künftigen Angriffe zu verhindern?*
7. *Arbeitet der Kanton mit Nachbarkantonen und dem Bund bezüglich Cybersecurity zusammen?*
8. *Unterstützt der Kanton die Gemeinden bei der Prävention und Abwehr von Cyberangriffen und*

wenn ja wie?

2. Einleitende Bemerkungen

Analog zu den beiden Postulaten 2023/574 (Cybersecurity) und 2023/578 (Cyber-Crime) adressiert die vorliegende Interpellation wichtige und aktuelle Fragestellungen für die kantonale Verwaltung im Bereich Cyber-Sicherheit. Wir weisen darauf hin, dass viele der Fragen zusätzlich zur Verwaltung auch andere Organisationen adressieren. Aufgrund der klar abgegrenzten Leistungsaufträge halten wir uns bei der Beantwortung an den Verantwortungsbereich der kantonalen Verwaltung Basel-Landschaft.

3. Beantwortung der Fragen

1. Wurden im konkreten Fall der Psychiatrie Baselland sensible Patientendaten gestohlen und Lösegeldforderungen gestellt?

Die Psychiatrie Baselland (PBL) ist von der kantonalen Verwaltung und dem Kantonsspital Baselland rechtlich und organisatorisch unabhängig. Seitens der Verwaltung wurden nach dem Angriff die Schnittstellen zur PBL gesperrt und eine umfassende Sicherheitsprüfung, der Verwaltungsinternen Systeme durchgeführt die über die aktiven Schnittstellen zur PBL betroffen sein konnten. Wir können daher davon ausgehen, dass die IT-Systeme der Verwaltung vom Cyberangriff auf die PBL nicht betroffen waren.

Zur Situation in der PBL stehen den Informatikorganisationen der kantonalen Verwaltung keine detaillierten Informationen zur Verfügung. Wir haben daher direkt bei der Informatik der PBL nachgefragt und am 16.01.2024 die folgende Antwort erhalten (Zitat): «Die Psychiatrie Baselland (PBL) ist immer noch daran, in Kooperation mit externen Cybersicherheits-Spezialisten die Folgen des Cyberangriffes aufzuarbeiten. Analysen haben ergeben, dass bisher keine Daten von Patientinnen und Patienten oder vertrauliche Geschäftsdaten im Netz aufgetaucht sind. Falls sich zeigen sollte, dass es zu Datenverletzungen gekommen ist, werden die Betroffenen von der PBL direkt informiert. Die PBL hat dazu eine Anlaufstelle eingerichtet, bisher sind jedoch sehr wenige Anfragen eingetroffen. Zu einer möglichen Lösegeldforderung können wir keine Angaben machen. »

2. Wie häufig werden Institutionen des Kantons Basel-Landschaft und Institutionen mit strategischen Beteiligung des Kantons von Hackern attackiert?

IT-Systeme welche direkt oder indirekt über Netzwerke mit dem Internet verbunden sind, werden 24x7 nonstop angegriffen. Dies geschieht zum grössten Teil an den Schnittstellen zum Internet und über Emails. Daneben gibt es hunderte von unterschiedlichen Techniken, um Cyberangriffe durchzuführen. Es werden keine Statistiken erstellt zur Anzahl und den Details von erfolgreich abgewehrten Cyberangriffen. Die Situation wird aber von den verantwortlichen Stellen beobachtet, beispielsweise in den Protokollen der Firewalls und weiterer Sicherheitssysteme. Bei Bedarf werden Massnahmen identifiziert und angegangen.

Die Verwaltung konzentriert sich, wie in der Antwort zur Frage Nr. 8 beschrieben, auf den eigenen Verantwortungsbereich. Unabhängige Organisationen melden der Verwaltung nur dann Informationen zu Cyberangriffen, wenn dadurch eine Gefahr für die Geschäftsprozesse oder die Sicherheit der Daten und IT-Systeme der kantonalen Verwaltung ausgehen könnte.

3. Welche Art von Cyberangriffen gab es in den vergangenen fünf Jahren?

In den vergangenen fünf Jahren wurden unterschiedliche Arten von Angriffen registriert. Diese hatten jedoch keine, oder nur beschränkte Auswirkungen auf die Gesamtorganisation der Verwaltung. Die mit Abstand grösste Anzahl an Angriffen waren Phishing-Emails welche entdeckt und gelöscht wurden. In jeweils ungefähr einem Duzend Fällen pro Jahr kam es zu einer

Ausführung von Schadsoftware. Die meisten Fälle davon wurden von den Sicherheitssystemen erkannt und blockiert. In einzelnen Fällen kam es auch zu Verschlüsselungen von einzelnen Arbeitsplatzsystemen. Alle betroffenen Systeme konnten jedoch isoliert und auf einen ursprünglichen Zustand zurückgesetzt werden.

Spürbar waren dagegen in den vergangenen zwei Jahren wiederholt sogenannte Distributed Denial of Service-Attacken (DDoS). Dabei wurden vom Internet erreichbare Systeme mit einer riesigen Anzahl an Anfragen geflutet, bis dies zu einer Überlastung der Systeme und damit zu Verfügbarkeitsproblemen führte. Aufgrund von früheren Erfahrungen wurden die Sicherheitsmassnahmen gegen DDoS-Attacken verstärkt.

Jedes Jahr kommen geschäftliche Laptops, iPads und iPhones abhanden, weil sie gestohlen werden oder verloren gehen. Das Risiko ist in diesem Bereich überschaubar, weil die Geschäftsdaten auf den Geräten verschlüsselt und mit weiteren Massnahmen angemessen abgesichert sind.

Vermehrt relevant sind Cyberangriffe, welche nicht direkt auf die Verwaltung zielen, sondern auf unsere externen Partner und Lieferanten. Die Auswirkungen dabei sind vielfältig. Diese können zu Engpässen bei den Betriebs- und Supportleistungen der Lieferanten führen. Es könnten, sofern vorhanden, Daten des Kantons bei den betroffenen externen Partnern gestohlen werden. Schliesslich bindet die Abklärung und Behandlung von Angriffen auf externe Partner auch verwaltungsintern erhebliche Ressourcen, welche dann für ordentliche betriebliche Aufgaben fehlen.

4. Kann man Aussagen darüber treffen, wer die Angreifer sind?

Die Identifizierung der Angreifer hinter den Cyberattacken ist schwierig. Einerseits erfolgen solche Angriffe heutzutage im Verbund mit unterschiedlichen Akteuren mittels Arbeitsteilung. Andererseits verschleiern die Angreifer den Angriff und ihre eigenen Spuren. Es besteht daher die Möglichkeit, dass eine falsche Partei beschuldigt wird. Aus diesem Grund wird die Täterschaft hinter den Cyberangriffen häufig nicht öffentlich genannt oder nur als Vermutung formuliert. Dazu kommt, dass die Täterschaft oft aus ermittlungstaktischen Gründen nicht öffentlich genannt wird.

Im Rahmen des international anerkannten Verizon Data Breach Reports werden jährlich tausende von erfolgreichen Hacking-Angriffen analysiert. Gemäss dem aktuellen Bericht von 2023 sind 94.6% dieser Angriffe finanziell motiviert und über 70% der Fälle werden dem organisierten Verbrechen zugeordnet. Auch den restlichen 30% der Angreifer inklusive den staatlichen Akteuren geht es demnach überwiegend um Geld.

5. Wie häufig werden Lösegeldforderungen gestellt und in welcher Höhe? Hat der Kanton schon einmal bezahlt?

In den vergangenen Jahren ist es in der Verwaltung zu Fällen von böswilligen Verschlüsselungen einzelner Arbeitsplatzsysteme gekommen. Der Begriff «Ransomware» impliziert, dass diese mit Lösegeldforderungen einhergehen. Die verschlüsselten Systeme konnten bisher aus den regelmässig erstellten Backups wiederhergestellt werden. Auch sind in den vergangenen Jahren keine Fälle bekannt, in denen Daten aus den Systemen der Verwaltung gestohlen wurden. Der Kanton ist aufgrund dieser Situation noch nie in die Situation geraten mit den Angreifern in Kontakt zu treten oder hat eine Aufforderung erhalten Lösegeld zu zahlen. Die Verwaltung des Kantons stellt sich wie das Nationale Zentrum für Cyber-Sicherheit (NCSC) auf den Standpunkt, dass keine Lösegeldforderungen bezahlt werden sollen.

6. Stehen dem Kanton ausreichend Mittel und Personal zur Verfügung, um auf Cyberangriffe reagieren zu können, laufende Angriffe abzuwehren und künftige Angriffe zu verhindern?

In den vergangenen zwei Jahren wurde die Anzahl der Informationssicherheitsbeauftragten von 6 auf 10 Personen mit umgerechnet 8.5 Personaleinheiten ausgebaut. So verfügen alle Direktionen sowie die Gerichte und die Landeskanzlei über mindestens eine/n Informationssicherheitsbeauftragte/n (DIT-SIBE). Mehr als eine/n DIT-SIBE und damit auch eine direkte Stellvertretung ist jedoch nur in 2 Direktionen gegeben. Wo dies nicht der Fall ist, wird die Stellvertretung direktionsübergreifend wahrgenommen. Zurzeit werden basierend auf dem RRB 2023-600 die Organisation, die Aufgaben und Prioritäten im Bereich Cyber-Sicherheit überprüft, um die Umsetzung der nationalen Cybersecurity Strategie im Rahmen der bestehenden Organisation optimal zu gestalten. Im Weiteren ist es Aufgabe jedes einzelnen Digitalisierungsvorhabens, Mittel und Ressourcen für die Konzeption, Umsetzung und betriebliche Sicherung von Schutzmassnahmen bereitzustellen und wo nötig zu beantragen. Die Unterstützung von Projekten zur Identifizierung von Risiken, den darauf ausgerichteten Sicherheitsmassnahmen, sowie deren Entwicklung und Verminderung im Laufe der Zeit wird weiter ein Schwerpunkt der Arbeiten der DIT-SIBE bleiben.

Mit dem technologischen Fortschritt und der zunehmend übergreifenden digitalen Vernetzung von Gemeinwesen und Nutzenden digitaler Lösungen verändern sich auch die Gefahren und Herausforderungen im Bereich Cyber stetig weiter. Das bedingt, dass auch die Informationssicherheit mit diesem Wandel Schritt halten und der Fokus über die Projektunterstützung hinaus erweitert werden muss. Dazu sind vermehrt sicherheitsspezifische Projekte anzustossen, um Veränderungen bei den Bedrohungen und Schwachstellen rechtzeitig adressieren zu können. Beispiele dafür sind das laufende Projekt zur Einführung eines Sensibilisierungssystems für Mitarbeitende oder das geplante Projekt zum Aufbau des Security Operation Center (SOC BL) für die frühzeitige Erkennung und Abwehr von Cyber-Angriffen. Mittel und Personalressourcen für das SOC wurden bereits im AFP 2023 – 2026 genehmigt.

Die Bereitstellung der Ressourcen für präventive, konzeptionelle, operative und reaktive Aufgaben zur Gewährleistung von Informationssicherheit, Datenschutz und Strafverfolgung, steht in Abhängigkeit zu den Erwartungen an die Entwicklungsgeschwindigkeit, den Integrationsgrad und die Individualität von digitalen Lösungen. Im Rahmen der für Prozessdigitalisierung und Informatikbetrieb verfügbaren Mittel ist die Gewichtung dieser drei Faktoren dabei fortlaufend sorgsam abzuwägen. Die Ressourcen zur Bearbeitung von Informationssicherheit, Datenschutz und Cyberkriminalität bilden dabei – vergleichbar mit jenen für öffentliche Sicherheit und Ordnung – immer einen Engpass. Damit gilt grundsätzlich: Je grösser die Erwartungen an die Entwicklungsgeschwindigkeit digitaler Lösungen, die Individualität der eingesetzten Technologien und Produkte sowie die digitale Vernetzung von Prozessen mit Privatpersonen, Unternehmen und anderen Gemeinwesen, desto grösser wird der Ressourcenbedarf für Informationssicherheit, Datenschutz und zur Bekämpfung von Cyberkriminalität.

Hinsichtlich der Informationssicherheit und des Datenschutzes bildet die konzeptionelle und operative Aufrechterhaltung der Sorgfaltspflicht im Umgang mit den entsprechenden Risiken und deren Minimierung auf ein tragbares Mass die Mindestzielsetzung die erreicht werden muss. Entsprechend bedingen die gegebenen Mittel und vorhandenen Möglichkeiten die Fokussierung auf die grössten und relevantesten Risiken. Dabei müssen jedoch neben den aktuellen Risiken auch rechtzeitig Investitionen angegangen werden, um mit der zunehmenden Digitalisierung und Komplexität Schritt halten zu können und für zukünftige Risiken gewappnet zu sein. Der Aufbau eines Security Operations Center (SOC) BL ist ein solch wichtiges Projekt.

7. Arbeitet der Kanton mit Nachbarkantonen und dem Bund bezüglich Cybersecurity zusammen?

Die Spezialistinnen und Spezialisten in der Informatik und Cyber-Sicherheit der kantonalen Verwaltung BL bringen sich in unterschiedliche Organisationen und Gremien ein, in denen auch der Bund und die Nachbarkantone vertreten sind. Dazu gehören unter anderem der Sicherheitsverbund Schweiz (SVS), die Arbeitsgruppen der Digitalen Verwaltung Schweiz (DVS) und das Nationale Cyber Security Center (NCSC). Darüber hinaus bestehen direkte Kontakte und Zusammenarbeiten in kantonsübergreifenden Projekten und im Rahmen von weiteren Organisationen.

8. Unterstützt der Kanton die Gemeinden bei der Prävention und Abwehr von Cyberangriffen und wenn ja wie?

Die Leistungsaufträge des Kantons sehen im Bereich der Cyber-Sicherheit keine Aufgaben und Kompetenzen dahingehend vor, dass der Kanton die Gemeinden proaktiv unterstützt. Aufgrund des Subsidiaritätsprinzips sind die Gemeinden unabhängig in ihren Entscheidungen und Massnahmen, die sie zum Schutz Ihrer IT Infrastrukturen und Daten treffen. Neben dem Leistungsauftrag und den Ressourcen bestehen auch keine gesetzlichen Grundlagen, um verbindliche Vorgaben im Bereich Cybersecurtiy auf Stufe Gemeinde zu erlassen.

Für Leistungen, welche die Gemeinden vom Kanton beziehen, liegt die Gewährleistung der technischen Sicherheit, gemäss den Vorgaben der Informationssicherheit und des Datenschutzes bei den kantonalen Leistungserbringern. Für Gemeinden, welche keine Ansprechpersonen beim NCSC gemeldet haben, steht das Team der/des KIT-SIBE als Kontaktstelle zum NCSC zur Verfügung. Das Team leitet in dieser Funktion, Informationen und Warnungen an die betroffenen Gemeinden weiter.

Für Unterstützung im Bereich der Prävention können die Gemeinden mit dem Sicherheitsverbund Schweiz (SVS) zusammenarbeiten und sich an die Label-Organisation www.cyber-safe.ch wenden. Diese beiden Organisationen richten sich explizit auch an die Gemeinden.

Liestal, 6. Februar 2024

Im Namen des Regierungsrats

Die Präsidentin:

Monica Gschwind

Die Landschreiberin:

Elisabeth Heer Dietrich