Antwort des Staatsrats auf einen parlamentarischen Vorstoss
—
Anfrage Demierre Philippe 2021-CE-334
Cyberverteidigung in unseren Freiburger Gemeinden und beim Staat Freiburg

I. Anfrage

In der Nacht von Samstag, den 29. auf Sonntag, den 30. Mai 2021 wurde die Gemeinde Rolle Opfer eines Cyberangriffs. Dabei wurden alle Daten verschlüsselt, was das IT-System der Gemeinde komplett lahmlegte. Laut Watson.ch wurde die Gemeinde am 24. Juni darauf aufmerksam gemacht, dass die Daten im Dark Web auf der Website der Cyberkriminellen Vice Society (Urheber des Angriffs) für die Allgemeinheit zugänglich seien.

In Rolle sind 5393 Einwohnerinnen und Einwohner direkt von diesem Daten-Leak betroffen: Telefonnummern, Festnetz- und Mobiltelefonnummern, E-Mail, AHV-Nummern, Schulzeugnisse der Kinder, Religion usw.

Laut der Zeitung letemps.ch wurden Steuerabkommen mit einem multinationalen Unternehmen und Steuervereinbarungen mit einem reichen Ausländer publik gemacht.

Cybersicherheit ist heute in aller Munde, und auch die Schweizer Gemeinden sind von diesem Phänomen nicht ausgenommen.

Ich habe dieses Problem in meiner Gemeinde Ursy als Vizeamman selber in die Hand genommen, damit wir nicht in eine Situation wie die Gemeinde Rolle geraten.

Der Bund verfügt diesbezüglich über einen sehr präzisen rechtlichen und politischen Rahmen, der immer auf dem neuesten Stand ist.

Obwohl die politischen Organe versuchen, mit gutem Beispiel voranzugehen, gilt es noch eine Unmenge von Lücken zu schliessen.

Es mangelt an Ressourcen mit den erforderlichen Fähigkeiten, und es findet sich in den Organisationen keine Gesamtstrategie.

Fragen:

1. Was gedenkt der Freiburger Staatsrat zu tun, um eine solche Katastrophe auf kommunaler und kantonaler Ebene zu verhindern?
2. Verfügt der Freiburger Staatsrat über eine genaue Liste der eingesetzten Hard- und Softwaretechnologien (Kanton und Gemeinden)?

10. September 2021

II. Antwort des Staatsrats

Einleitend hält der Staatsrat fest, dass sich der Begriff Cyberverteidigung auf nachrichtendienstliche und militärische Massnahmen zur Abwehr von Cyberangriffen bezieht und in erster Linie den Bund und insbesondere die Armee betrifft. Die Massnahmen zur Prävention, zum Incident Management, zum Resilienzmanagement, zur Schulung und Forschung, die die die Kantone im Rahmen der Bekämpfung von Cyberattacken umsetzen können, gehören hingegen zum Bereich der Cybersicherheit.

1. Was gedenkt der Freiburger Staatsrat zu tun, um eine solche Katastrophe auf kommunaler und kantonaler Ebene zu verhindern?

Auf kantonaler Ebene

Der Staatsrat stellt seit mehreren Jahren eine Zunahme der Cyberangriffe fest, die gleichzeitig immer professioneller werden. Der Staat Freiburg ist sich des Wertes seiner digitalen Güter und der Bedeutung seiner Informationssysteme bewusst und ist bestrebt, eine Reihe geeigneter Massnahmen zu ergreifen, um Vorfälle wie den vom Verfasser der Anfrage beschriebenen zu verhindern.

So werden einerseits unter der Federführung des Amtes für Informatik und Telekommunikation (ITA), wo ein Team speziell für die Sicherheit der IT-Ressourcen gebildet wurde und von externen Fachleuten unterstützt wird, regelmässig Schwachstellentests durchgeführt. Dabei handelt es sich um ein Security Operation Center (SOC), das 2019 eingerichtet wurde und einen Mehrwert für das Risikomanagement darstellt.

Der diesbezügliche Zuständigkeits- und Aufgabenbereich des ITA wurde jüngst mit der Verabschiedung der Verordnung über die Governance der Digitalisierung und der Informationssysteme des Staates im Juli 2021 geklärt. Das ITA ist für die Sicherheit der IT-Ressourcen des Staates verantwortlich. Einige Einheiten mit besonderem Status sind zudem in bestimmten Bereichen tätig. So etwa die spezialisierte IT-Einheit der Kantonspolizei und die Fachstelle Fritic für das Unterrichtswesen.

Was die Schulen des Kantons anbelangt, so unterstehen die nachobligatorischen Schulen der technischen Leitung des ITA und ihr Schutz fällt damit unter die oben genannten Cybersicherheitsmassnahmen. Dasselbe gilt für die Verwaltungswerkzeuge der Schulen und die Kommunikations- und Kollaborationswerkzeuge der obligatorischen Schulen. Die Fachstelle Fritic ist für die Sicherheit der personenbezogenen Daten in ihrem zusätzlichen Zuständigkeitsbereich verantwortlich. Die technische Ausstattung und die Infrastruktur der Primar- und Sekundarstufe I fallen hingegen in den Zuständigkeitsbereich der Gemeinden und hängen daher von den von diesen getroffenen Sicherheitsmassnahmen ab.

Gewisse Verwaltungseinheiten wie die Universität oder das freiburger spital (HFR) verfügen über eine rechtliche Autonomie, die es ihnen ermöglicht, ihre IT-Strategie eigenständig zu bestimmen.

In diesem Herbst ist auch eine Arbeitsgruppe eingesetzt worden mit dem Ziel, eine neue Verordnung zur erarbeiten, die die Organisations- und Verantwortlichkeitsfragen im Bereich Informationssicherheit in der Kantonsverwaltung regelt.

2019 beauftragte das ITA ein auf IT-Sicherheit spezialisiertes externes Schweizer Unternehmen mit der Ermittlung des aktuellen Reifegrads der IT-Sicherheit und der Umsetzung kontinuierlicher Verbesserungen. Für die Analyse wurde ein sogenanntes CMMI-Modell (Capability Maturity Model Integration) mit standardisierter Skala verwendet. Die Analyse von 22 Cybersicherheits-prozessen führte zur Initiierung von mehr als zwanzig Projekten und Aufträgen. Aus offensichtlichen Vertraulichkeits- und Sicherheitsgründen werden diese Informationen nicht weitergegeben.

Darüber hinaus arbeitet der Staat Freiburg mit dem Bund zusammen, um seine Massnahmen zu verstärken und punkto bewährte Praktiken im Bereich der Cybersicherheit stets auf einem zufriedenstellenden Stand zu sein. So wirkt er etwa aktiv an der Umsetzung der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) für die Jahre 2018-2022» mit. Diese vom Bund in Zusammenarbeit mit den Kantonen, der Wirtschaft und den Hochschulen erarbeitete Strategie definiert Zielvorgaben in verschiedenen Handlungsfeldern und bildet die Grundlage für die gemeinsamen Anstrengungen zur Reduktion von Cyber-Risiken.

Ein weiteres Handlungsfeld zur Stärkung der Cybersicherheitsstrategie des Staates Freiburg ist die Verbreitung von bewährten Praktiken im Bereich der Computerhygiene. Dabei stützt sich der Staat sich insbesondere auf Referenzdokumente zum Thema, wie den vom Bundesamt für wirtschaftliche Landesversorgung (BWL) 2018 veröffentlichten «Minimalstandard zur Verbesserung der IKT-Resilienz». Der Staatsrat erinnert auch daran, wie wichtig es ist, alle Nutzerinnen und Nutzer innerhalb der kantonalen Verwaltung zu sensibilisieren und sie dazu zu bringen, sich bei der Nutzung der Informatikmittel richtig zu verhalten.

Unter der Federführung des Bundes und im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken beteiligt sich der Staat Freiburg zudem an einer Arbeitsgruppe, die eine Lösung zur Sensibilisierung für die Cybersicherheit für alle öffentlichen Verwaltungen der Schweiz erarbeiten soll.

Die Kantonspolizei ihrerseits interveniert im Bereich der Cyberkriminalität, das heisst, wenn eine Straftat an einem oder mittels eines Computersystems begangen wurde. Zu diesem Zweck verfügt sie seit 2016 über eine Einheit, die sich mit Cyberkriminalität befasst.

Sie ist in der Prävention, Sensibilisierung und Beratung zu neuen Phänomenen der Cyberkriminalität tätig und richtet ihre Kampagnen auf die aktuellen Phänomene aus. In diesem Jahr nahm sie an der nationalen Aktionswoche zum Thema «Sicherheit im digitalen Raum» teil und warnte in ihren Netzen vor Online-Betrug, Online-Investitionsbetrug usw. Auch die Seite der Schweizerischen Kriminalprävention (https://www.skppsc.ch/de/) bietet eine Fülle von Informationen und Ratschlägen zu diesen Phänomenen.

Es ist nicht von der Hand zu weisen, dass die Straftaten im Digitalbereich laufend zunehmen. Die Möglichkeiten, gegen diese Kriminellen vorzugehen, sind begrenzt, da sie in der Regel vom Ausland aus operieren und die internationale Zusammenarbeit kompliziert bleibt. Es ist jedoch wichtig, dass die Opfer eines Angriffs unverzüglich die Polizei verständigen, damit diese sie beraten und so viele Informationen wie möglich für die Ermittlungen sammeln kann. Mit diesen Informationen, die in Schweizer Analyse- und Koordinationsplattform zusammengeführt und aufbereitet werden, lassen sich diese Phänomene besser bekämpfen.

Der Staatsrat weist darauf hin, dass der Staat Freiburg die Cyberangriffe, denen er wie übrigens alle öffentlichen Verwaltungen ausgesetzt war, dank der getroffenen Schutzmassnahmen bisher verringern konnte. Dieser war nicht nur dank der Organisation und der von der kantonalen Verwaltung implementierten spezifischen Instrumente möglich, sondern ist auch dem Engagement aller Staatsmirtarbeitenden zu verdanken.

Dennoch sollte man zurückhaltend bleiben, da es immer zu einem Angriff kommen kann. Die diesbezüglichen Risiken dürfen nicht unterschätzt werden. Offen über die eigene Abwehrbereitschaft zu sprechen, kann kontraproduktiv sein und für Personen und Organisationen mit böswilligen Absichten eine Art Herausforderung sein.

Der Staat Freiburg möchte aus offensichtlichen Vertraulichkeits- und der Sicherheitsgründen keine Einzelheiten über die zur Abwehr auf allfällige Angriffe eingesetzten Instrumente und Technologien bekannt geben. Für den Fall, dass eine Cyberattacke vollumfänglich oder teilweise zustande kommen sollte, ist jedoch eine Krisenorganisation vorgesehen. Sie konnte bereits während der Corona-Krise getestet werden. Schliesslich bieten die Backup-Strategie und die Wiederherstellungsprozesse einen gewissen Schutz, um den Datenverlust im Falle eines «Ransomware»-Angriffs zu begrenzen.

Auf Gemeindeebene

Was den Schutz der Gemeinden betrifft, so erinnert der Staatsrat daran, dass er nicht befugt ist, an ihrer Stelle aktiv zu werden. Er empfiehlt allen Freiburger Gemeinden dringend, sich mit der Cyberbedrohung und den potenziell massiven Folgen eines Angriffs auseinanderzusetzen, und erinnert in diesem Zusammenhang daran, dass mit Lösungen wie dem Label «cyber-safe» IT-Strukturen in Bezug auf ihre Resilienz gegenüber Cyberattacken geprüft werden können. Diese Diagnose sollte dann Massnahmen zur Verbesserung der Antizipationsfähigkeit und der Resilienz des Informationssystems ermöglichen.

Der Staatsrat und der Vorstand des Freiburger Gemeindeverbands haben zudem beschlossen, ihre Zusammenarbeit zu verstärken und die Bestrebungen zur Digitalisierung der öffentlichen Dienstleistungen für die Gemeinden, die Bevölkerung, die Wirtschaft und die Institutionen im Kanton Freiburg zu koordinieren. Sie haben dazu eine Vereinbarung unterzeichnet, in der die Rahmenbedingungen für die Entwicklung und Finanzierung der Digitalisierung der öffentlichen Dienstleistungen im Rahmen des DIGI-FR-Konzepts festgelegt sind. Dieses Zusammenspannen könnte auch als Plattform für eine gemeinsame Cybersicherheit dienen.

2. *Verfügt der Freiburger Staatsrat über eine genaue Liste der eingesetzten Hard- und Softwaretechnologien (Kanton und Gemeinden)?*

Wie bereits gesagt, ist die Publikmachung der genauen Technologien, die die kantonale Verwaltung zur Bekämpfung von Cyberangriffen einsetzt, nicht wünschenswert, und zwar einerseits aus Sicherheitsgründen, andererseits aber auch, um nicht Personen und Organisationen mit böswilligen Absichten anzuziehen.

Der Staatsrat ist vollumfänglich im Bild darüber, welche Lösungen verwendet werden. Er befindet über die Investitionen und Entscheidungen im Zusammenhang mit IT-Sicherheitsprojekten nach den Voraussetzungen der oben genannten Verordnung über die Governance der Digitalisierung und der Informationssysteme des Staates. Er stützt sich dabei insbesondere auf die Rolle der Informatik-

kommission des Staates (IKS) und der Delegation des Staatsrats für die Digitalisierung und die Informationssysteme (DIS).

Hingegen liegt die Cybersicherheit der Gemeinden nicht in der Zuständigkeit des Staates Freiburg, so dass er keine Kenntnisse über die von ihnen verwendeten Technologien hat.

9. November 2021