

Parlamentarischer Vorstoss. Antwort des Regierungsrates

Vorstoss-Nr.: 277-2018
Vorstossart: Motion
Richtlinienmotion: ☐
Geschäftsnummer:

Eingereicht am: 28.11.2018

Fraktionsvorstoss: Nein
Kommissionsvorstoss: Nein
Eingereicht von: Gerber (Hinterkappelen, Grüne) (Sprecher/in)
Ammann (Bern, AL)
Egger (Hünibach, SP)
Müller (Orvin, SVP)

Weitere Unterschriften: 14

Dringlichkeit verlangt: Nein
Dringlichkeit gewährt:

RRB-Nr.: 451/2019 vom 08. Mai 2019
Direktion: Finanzdirektion
Klassifizierung: Nicht klassifiziert
Antrag Regierungsrat: **Punktweise beschlossen**
1. Annahme und Abschreibung
2. Annahme als Postulat
3. Ablehnung
4. Annahme und Abschreibung



Sichere Kommunikation und Datenaustausch

Der Regierungsrat wird beauftragt, dafür zu sorgen bzw. sicherzustellen, dass

1. auf allen Ebenen der Verwaltung sowie bei Police Bern für die digitale Kommunikation immer die sicherste Software und die sichersten Applikationen verwendet werden
2. auch in Schulen sichere Kommunikationssoftware und -applikationen verwendet werden
3. die Daten auf Schweizer Servern gespeichert und aufbewahrt werden
4. in der Kommunikation mit Externen, wenn es sich um schützenswerte Daten und Dokumente handelt, ebenfalls sichere Kommunikationssoftware und Applikationen verwendet werden

Begründung:

Immer wieder hören wir von Datenlecks. Daten von Whatsapp werden mit Daten von Facebook abgeglichen und die Nutzer individuell beworben, oder die Daten werden an Dritte weiterverkauft.

Gratis # gratis. Konventionelle Messenger mögen kein Geld kosten, aber die Nutzung wird mit Daten bezahlt. Es ist unverantwortlich, wenn Grosskonzerne riesige Profite mit dem Verkauf und der Verwertung von Daten machen, die sie weder besitzen noch erworben haben. Das trifft immer dann im stärkeren Mass zu, wenn die Nutzer nicht volljährig sind.

Es ist angenehmer, Geschäftliches von Privatem zu trennen. Es macht keinen Sinn, dass ich in der gleichen App sowohl die Bilder meiner Familie als auch den Vertragsentwurf meines Vorgesetzten sehe. Zudem muss eine App End zu End verschlüsselt sein.

Es gibt Applikationen, die den Bedürfnissen angepasst werden können. So können zum Beispiel Schulen oder Departemente in der Verwaltung verhindern, dass Dritte eine Schülerin oder Mitarbeiterin direkt kontaktieren.

Die Anzahl Cyber-Angriffe nimmt tendenziell zu. Das heisst nicht, dass ein Angreifer das Handy einer Person direkt angreift. Es reicht, wenn er sich die Nutzungsdaten einer bestimmten Personengruppe kauft und damit Verhaltensmuster erkennt, mit denen er die eigentliche Infrastruktur leichter und wirkungsvoller angreifen kann (zum Beispiel Erkennung von Randzeiten oder bestimmten Altersgruppen, die sich für einen Angriff eignen). D. h. bei der Prävention geht es nicht immer nur um den Schutz des Gerätes selbst. Es gilt, die Informationen, die bei der Planung von Attacken verwendet werden können, auf ein absolutes Minimum zu reduzieren. Diese Metadaten sind sowohl legal als auch auf dem Schwarzmarkt erhältlich.

Es gibt bereits fünf Kantone, die sichere Applikationen für den flächendeckenden Einsatz in der Verwaltung und in den Schulen einsetzen.

Zum Beispiel Threema Work, oder Wire wird in der Politik übrigens ebenfalls verwendet. Nebst dem Bund auch in Deutschland. Daneben auch in etlichen nationalen Ministerien von EU-Mitgliedstaaten sowie Polizeicorps im In- und Ausland.

Antwort des Regierungsrates

1. Der Regierungsrat teilt die Auffassung der Motionäre, dass die Herausforderungen für die Informationssicherheit und den Datenschutz (ISDS) mit der zunehmenden Digitalisierung der Verwaltung und aller anderen Bereiche des Lebens zunehmen. Daher schreiben die Vorschriften über die Informationssicherheit und den Datenschutz in der Kantonsverwaltung vor, dass für jede Applikation eine ISDS-Analyse erfolgt und, wenn ein erhöhtes ISDS-Risiko festgestellt wird, dieses in einem ISDS-Konzept näher beurteilt wird. Das Konzept beschreibt die Massnahmen zum Reduzieren oder Vermeiden der Risiken. Eine absolute Sicherheit gibt es aber nicht. Die sicherste Kommunikation ist das Gespräch von Angesicht zu Angesicht. Jede elektronische Kommunikationsform ist mit bestimmten Restrisiken verbunden, die als noch tragbar erachtet und z.B. aus Zeit-, Kosten-, Benutzerfreundlichkeits- oder organisatorischen Gründen in Kauf genommen werden. Wichtig ist, dass dies bewusst erfolgt.

In der Kantonsverwaltung gelangt für die Kommunikation die Applikation «Skype for Business» zum Einsatz. Diese stellt eine Verschlüsselung sicher. Innerhalb der Verwaltung werden E-Mails ebenfalls automatisch verschlüsselt übermittelt. Für die sichere mobile Kommunikation wird die Verwaltung ab Ende 2019 eine «Enterprise Mobility Management»-Lösung

(EMM) einsetzen. Diese Technologie schafft einen geschützten, verschlüsselten Bereich auf einem Smartphone oder Tablet, in dem die geschäftlichen Applikationen und Daten getrennt von den privaten bearbeitet werden.

Die Kantonspolizei setzt die EMM-Technologie bereits ein. Sie nutzt für die Kommunikation zwischen ihren Mitarbeitenden auch die App IMP (Instant Messenger Police), welche eine End-to-End-Verschlüsselung der Kommunikation und die automatische Löschung der Daten sicherstellt. Diese Lösung wird von mehreren Polizeikorps eingesetzt, so dass auch eine sichere Kommunikation zwischen unterschiedlichen Polizeikorps möglich ist.

Beim ersten Punkt der Motion handelt es sich um ein Daueranliegen («immer»), das gestützt auf die erwähnten Vorschriften laufend umgesetzt wird. In diesem Sinne erachtet der Regierungsrat das Anliegen der ersten Ziffer der Motion als erfüllt und beantragt insoweit ihre Annahme und Abschreibung.

2. Vorschriften zur Nutzung von Kommunikationssoftware kann der Kanton nur für die Sekundarstufe II erlassen. Die Vorgaben richten sich nach der ICT-Strategie für die Schulen der Sekundarstufe II¹ und werden regelmässig in einem Fachausschuss ICT, in dem die Schulen vertreten sind, überprüft. Für Vorgaben für die Volksschule sind die Gemeinden zuständig. Der Kanton kann ihnen lediglich Empfehlungen abgeben.

In Zusammenarbeit mit der Pädagogischen Hochschule Bern unterstützt die Erziehungsdirektion die Schulen beim sicheren und gesetzeskonformen Umgang mit digitalen Daten mittels eines ausgebauten Ampelsystems (<http://kibs.ch/datenschutz>). Zudem wird der Auf- und Ausbau der Medienkompetenz durch die Vorgaben in den Lehrplänen in der Volksschule und auf der Sekundarstufe II gewährleistet. Insbesondere der Austausch von sensiblen Informationen (z.B. über die Gesundheit oder die schulischen Leistungen) unterliegt strengen Vorgaben. Die Schulen sind darüber informiert und die kantonalen Schulen, die ihre Informationsdienstleistungen bei der Erziehungsdirektion beziehen, sind technisch dafür ausgerüstet, besonders schützenswerte Daten auszutauschen.

In Bezug auf einige heute verwendete Messengerdienste besteht ein Widerspruch zwischen ihrer Akzeptanz in der Gesellschaft und datenschutzrechtlichen Vorgaben. Die Fachagentur des Bundes und der Kantone für ICT und Bildung (educa.ch) ist aktuell daran, mit einem schweizerischen Anbieter eine attraktive Alternative zum heutigen weitverbreiteten Gratisangebot auszuhandeln. Nach Vorliegen dieses Angebots wird die Erziehungsdirektion bezüglich Verwendung von Messengerdiensten in der Schule eine verbindliche Vorgabe an die Schulen der Sekundarstufe II und eine Empfehlung an die Volksschulen prüfen.

Der Regierungsrat beantragt daher, die zweite Ziffer der Motion als Postulat anzunehmen.

3. Der physische Standort eines Servers ist keine Garantie dafür, dass die darauf bearbeiteten Daten sicher sind. Auf Schweizer Server kann auch vom Ausland aus zugegriffen werden, und Unternehmen mit Sitz in der Schweiz können durch Personen im Ausland beherrscht werden. Auch in Bezug auf diesen Aspekt der Informationssicherheit muss im Rahmen einer Risikoanalyse im Einzelfall beurteilt werden, mit welchen Massnahmen die Daten risikogemessen geschützt werden sollen. Die Datenhaltung in einem EU-Land kann die Informati-

¹ [ICT-Strategie Schulen Sek II 2017-2021](#)

onssicherheit unter Umständen sogar erhöhen: Die Datenschutzgrundverordnung (DSGVO)² der EU verpflichtet ICT-Unternehmen zu mehr Sorgfalt und Massnahmen zum Schutz von Daten als das zurzeit noch geltende Schweizer Datenschutzrecht. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte führt eine Liste der Staaten, die für natürliche Personen einen angemessenen Datenschutz bieten.

In Bezug auf die Daten, die für die Erfüllung der staatlichen Aufgaben am wichtigsten sind, hat der Regierungsrat im Rahmen der Eigentümerstrategie für die Bedag Informatik AG (Bedag) entschieden, dass sie durch die kantonseigene Bedag in der Schweiz gehalten werden sollen.³ Immer mehr Applikationen werden aber nur noch als «software as a service» entwickelt. Sie können nicht auf einem eigenen Server installiert werden, sondern werden über das Internet, aus einer oft im Ausland betriebenen «Cloud», zur Nutzung angeboten. Dieser technischen Entwicklung kann sich auch die Kantonsverwaltung nicht verschliessen. Sonst müsste sie unter Umständen viel teurere oder technisch ungenügende Lösungen einsetzen, mit denen die Ziele der Digitalisierung der Verwaltung nicht erreicht werden können. Im Einzelfall muss es daher nach einer Risikoanalyse und mit angemessenen Sicherheitsmassnahmen möglich bleiben, auch ausländische Cloud-Lösungen einzusetzen. Das Datenschutzgesetz (KDSG) schliesst dies nicht aus.

Daher beantragt der Regierungsrat die Ablehnung der dritten Ziffer der Motion.

4. Für die sichere elektronische Kommunikation mit Dritten setzt die Kantonsverwaltung verschiedene Methoden ein, die eine verschlüsselte Übermittlung oder eine Verschlüsselung der vertraulichen Inhalte selbst sicherstellen. Dazu gehören unter anderem
 - eine durch Bedag betriebene E-Mail-Lösung, die den Adressaten das Abholen der E-Mails über ein sicheres Web-Portal ermöglicht,
 - Schnittstellen zum Health Info Net (HIN) und zur Bundesverwaltung zum durchgängig verschlüsselten Austausch von E-Mails mit anderen Kantonen, Bundesbehörden und Organisationen des Gesundheitswesens,
 - eine in den kantonalen Arbeitsplatz (KWP) integrierte Lösung zum Verschlüsseln von externen Datenträgern.

Aus diesen Gründen erachtet der Regierungsrat das Anliegen der vierten Ziffer der Motion als erfüllt und beantragt ihre Annahme und Abschreibung.

Verteiler

- Grosser Rat

² [Verordnung \(EU\) 2016/679](#) des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG

³ Vgl. die [Medienmitteilung des Regierungsrates vom 21. September 2018](#).