An den Grossen Rat **16.5158.02**

JSD/P165158

Basel, 4. Mai 2016

Regierungsratsbeschluss vom 3. Mai 2016

Interpellation Nr. 53 von Alexander Gröflin betreffend «Cybercrime»

(Eingereicht vor der Grossratssitzung vom 13. April 2016)

«Gemäss Informatik-Professor Hannes Lubich kommt es pro Woche in der Schweiz zu hunderten von Angriffen. Der Wirtschaftsstandort Basel wird davon leider auch betroffen sein. Aktuelle Schätzungen gehen davon aus, dass Cybercrime weltweit gleich viel Umsatz pro Jahr erzielt wie der Drogenhandel. Viele Angriffe sind zwar unkoordiniert und versuchen aus der Masse Einfallstore zu finden, dennoch darf von einer grossen Dunkelziffer ausgegangen werden. Viele Betroffene melden Vorfälle aus Imagegründen nicht oder bemerken es einfach nicht.

Zurzeit werden Internetnutzer hauptsächlich von zwei verschiedenen Angriffsmethoden bedroht. Zum einen Denial-of-Service-Attacken, wobei mit Anfragen ein Angriffsziel überlastet und überlistet wird. Zum andern werden Private und Unternehmen durch Erpressungstrojaner (engl. Ransomware) angegriffen. Eine solche Schadsoftware verschlüsselt alle Dateien auf dem angegriffen System mit einem Schlüssel. Nur gegen Bezahlung eines Lösegelds wird den Betroffenen vielleicht ein Schlüssel zur Entschlüsselung zugestellt.

Der Regierungsrat wird deshalb um Beantwortung folgender Fragen gebeten:

1. Wie viele polizeilich registrierte Straftaten wurden wegen Cybercrime in den Jahren 2013 – 2015 aufgenommen?
2. Wie viele strafrechtliche Ermittlungsverfahren wurden wegen Cybercrime in den Jahren 2013 – 2015 eingeleitet?
3. Wie viele Verurteilungen wurden wegen Cybercrime ausgesprochen?
4. Wie hoch beziffert der Kanton Basel-Stadt das Schadenspotential im Bereich Cybercrime für den Kanton, Private und Unternehmen?
5. Gibt es im Kanton Basel-Stadt einen Notfallplan oder dergleichen gegen Cyberangriffe auf Infrastruktur- und Informationssysteme sowie den ansässigen Unternehmen?

- Falls ja, was beinhaltet dieser Plan und seit wann existiert dieser?

6. Prüft der Kanton Basel-Stadt seine Informationssysteme auf Sicherheit intern und extern? Darunter fallen z.B. Versionskontrollen von Software (insbesondere Browser wie IE mit bekannten Sicherheitslücken, Netzwerk und Nutzer-Berechtigungen etc.).

- Falls ja, welche grösseren Schwachstellen konnten in jüngster Zeit identifiziert und behoben werden?

7. Wie viele Personen sind im Kanton Basel-Stadt involviert bei der Bekämpfung von Cybercrime?
8. Erachtet der Regierungsrat die Ressourcen und personellen Mittel als ausreichend?

- Falls ja, weshalb?

9. Erachtet es der Regierungsrat für sinnvoll im Bereich Cybercrime, für welche die Kantonsgrenzen kaum massgebend sind, an der kantonalen Strafverfolgungs-kompetenz festzuhalten?

- Falls ja, weshalb?

Alexander Gröflin»

Wir beantworten diese Interpellation wie folgt:

1. Vorbemerkungen

Mit der zunehmenden Durchdringung aller Lebensbereiche durch die Informatik, beginnend vom einfachen Personalcomputer über die immer komplexer werdenden Mobiltelefone bis hin zum «Internet of things», hat sich auch die Kriminalität verlagert. Einerseits werden Geräte der IT als einfache Speichermedien genutzt, andererseits eröffnen sich aber ganz neue Möglichkeiten der Dokumentation und Begehung von Straftaten. Während etwa Buchhaltungen und darin verschriftete Verfehlungen bzw. Tatvorgehen oder pornographische Produkte auf Speichern mit rasant steigender Kapazität abgelegt werden, ergeben sich über elektronische Kommunikationsmittel Wege, mit Dritten in Verbindung zu treten und weitestgehend anonym zu bleiben. Zudem eröffnen sich mit dem Handel im Internet oder dem Bedarf verschiedenster Teilnehmer am Wirtschaftsleben nach möglichst schneller und ungehinderter elektronischer Kommunikation und Transaktion neue Handlungsspielräume in den Bereichen Betrug, Diebstahl, Erpressung etc.

Gestützt auf diese Entwicklung erarbeiten die Konferenz der Kantonalen Polizeikommandanten (KKPKS) und die Direktion fedpol im Auftrag des Bundesrates aktuell eine nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS). Dabei wird erstmals der Versuch unternommen, die Phänomene einheitlich zu definieren und auch Zuständigkeiten für die Verfolgung von Straftaten festzulegen, um danach gezielt Handlungsvorgehen festlegen zu können. Dieser Prozess ist allerdings noch nicht abgeschlossen, zumal namentlich in Bezug auf die Zuständigkeiten offene Fragen bestehen, die es zu klären gilt. Immerhin wurde 2015 ein Katalog mit mehr als 20 Phänomenen definiert, die weitestgehend unbestritten sind. Dies stellt sicher, dass künftig zumindest alle vom gleichen reden.

Bei diesen Phänomenen handelt es sich einerseits um solche klassischer Kriminalität wie Pornographie oder Betrug mit den Mitteln des Internet, andererseits aber auch um solche (Malware), die erst und nur im Zusammenhang mit dem Internet möglich sind und zum Teil direkt schädigend in Datenspeicher oder Kommunikationswege eingreifen (Hacking, Ransomware, Trojaner etc.).

Entsprechend dieser Entwicklung gab und gibt es derzeit noch keine einheitlichen Kriterien für die statistische Erfassung der Straftaten. Diese werden oft ohne weitere Differenzierung, d.h. ohne Bezug zu Tatvorgehen oder Tatmittel in das klassische Wertungssystem eingelesen (Betrug, Erpressung, Drohung, Pornographie etc.) oder vereinfachend als Computerdelikte ausgewiesen. Es bestehen daher Wissenslücken in Bezug auf das, was gemeinhin als Cyberkriminalität bezeichnet wird. Diesen Mangel soll die bereits erwähnte NCS beheben.

Ebenfalls entsprechend dieser Entwicklung bedarf es ganz unterschiedlicher Fachkompetenzen für die Kriminalitätsbekämpfung bzw. -aufklärung. Während es noch – wenn auch zunehmend schwieriger – vergleichsweise einfach ist, Datenspeicher von verschiedenen Geräten auszulesen, ist es nicht nur technisch, sondern durch die internationale Vernetzung der von der Täterschaft genutzten Server auch rechtlich höchst komplex, Datenwege bis zum Verursacher zurück zu verfolgen, um diesen ins Recht fassen oder zumindest die Fortsetzung der Delinquenz beenden zu können.

2. Zu den Fragen

ad 1 bis 3
Aus den eingangs erwähnten Gründen werden bisher nur die auch gesetzlich als solche definierten, «klassischen» IT-Delikte statistisch erfasst und in der polizeilichen Kriminalstatistik als solche ausgewiesen. Für den Zeitraum 1. Januar 2013 bis 31. Dezember 2015 wurden zur Anzeige gebracht:
- 195 Fälle unbefugter Datenbeschaffung gemäss Art. 143 StGB,
- 64 Fälle unbefugten Eindringens in ein Datensystem gemäss Art. 143bis StGB,
- 768 Fälle betrügerischen Missbrauchs einer Datenverarbeitungsanlage gemäss Art. 147 StGB.

Mit Cyberkriminalität im eingangs erwähnten Sinn hat dies allerdings oft wenig zu tun. Dieser Mangel an statistischer Verfügbarkeit der interessierenden Informationen ergibt sich nicht nur in Bezug auf die Anzeigen, sondern auch hinsichtlich der Verurteilungen. Es ist davon auszugehen, dass im Rahmen der NCS diese Lücke geschlossen wird, weil sich nur so effiziente Bekämpfungsstrategien entwickeln und begründen lassen.

ad 4
Es bestehen keine finanziellen Schätzungen für dieses Schadenspotential, zumal die Dunkelziffer sehr hoch sein dürfte. Man muss aber davon ausgehen, dass erfolgreiche Angriffe aus dem Cyberspace einen erheblichen negativen Einfluss auf die Verfügbarkeit von Informationssystemen haben, d.h. Informatikdienstleistungen stehen nur teilweise oder gar nicht zur Verfügung. Dies kann zu erheblichen Reputationsschäden führen.

ad 5
Zum Schutz von IT-Infrastrukturen der kantonalen Verwaltung verfügen die Zentralen Informatikdienste (ZID) über Prozesse und Personal (Pikettorganisation, Verträge mit externen Dienstleistern), um bei Angriffen auf die Systeme in ihrem Zuständigkeitsbereich die Schadensminderung aktiv durchzuführen. Diese Massnahmen bestehen seit mehreren Jahren, seit 2014 wurden die Vorkehrungen im Rahmen des Informationssicherheitsmanagementsystems (ISMS) weiter ausgebaut und ein Informationssicherheitsbeauftragter steuert ZID-intern die Aktivitäten.

ad 6
Bei den von den ZID bereitgestellten IT-Services werden laufend und zeitnah die von den Herstellern publizierten Aktualisierungen eingespielt und so bekannte Schwachstellen behoben. Zudem erfolgen Sicherheitsaudits der Systeme durch spezialisierte externe Firmen. Die ZID betreiben ein Informationssicherheitsmanagementsystem (ISMS), über das Risikoanalysen systematisch durchgeführt werden, Risiken identifiziert und erforderliche Massnahmen zur Risikominderung veranlasst werden. Bei den Informatiksystemen in der Verantwortung der Departemente und Dienststellen obliegt diesen die Risikoanalyse und -minderung.

Als Schwachstelle in jüngster Zeit zeigte sich, dass die Entwicklung neuer Viren schneller erfolgt als die Anpassung der Virenschutzsoftware durch die Hersteller. Alleine technische Massnahmen vermögen den Schutz der Daten und Infrastrukturen nicht vollständig sicherzustellen. Der vorsichtigen Nutzung insbesondere von Email durch die Mitarbeiterinnen und Mitarbeiter kommt ebenfalls eine hohe Bedeutung zu (diesbezüglich erfolgte eine Information im Intranet, und die Weisung über die Benutzung von Informatikmitteln wird entsprechend angepasst).

Zur wirksamen Bekämpfung von Angriffen aus dem Cyberspace werden – zusätzlich zu den klassischen Protect-Massnahmen (z.B. Virenschutz, Systemhärtung etc.) – vermehrt Detect-Controls eingesetzt, d.h. Prozesse und Verfahren, die Systemanomalien (z.B. auf Netzwerkebene) erkennen, entsprechende Notifikationen absetzen und, im Idealfall, adäquate Gegenmassnahmen au-

tomatisiert einleiten. Innerhalb der Kantonalen Informationssicherheit sind solche Verfahren im Rahmen eines kontinuierlichen Verbesserungsprozesses bereits angedacht.

ad 7
Die Bekämpfung von Cybercrime (zur Begrifflichkeit siehe Vorbemerkungen) erfolgt delikt-spezifisch durch die Ermittler und Ermittlerinnen in den Fachgruppen der Kriminalpolizei und in der Abteilung Wirtschaftsdelikte. Diese werden massgeblich von 7 IT-Forensiker/-innen unterstützt, die als Spezialistinnen bzw. Spezialisten bei der Sicherstellung, Aufbereitung und Auswertung sämtlicher elektronischer Geräte, Datenträger und Netzwerkdaten sowie Mobiltelefone beigezogen werden (müssen).

ad 8
Die personelle Dotation im Bereich IT-Forensik inklusive Mobiltelefonie-Auswertung im Nordwestschweizer Polizeikonkordat (NWPK) präsentiert sich wie folgt:

Kanton	Personal (in Vollzeitäquivalent, FTE)
Kanton Bern	14 FTE
Kanton Aargau	10 FTE
Kanton Basel-Stadt	7 FTE
Kanton Basel-Landschaft	7 FTE
Kanton Solothurn	6 FTE

Im direkten Vergleich innerhalb des NWPK ist Basel-Stadt gut aufgestellt. Die stetig steigenden Datenmengen bei sämtlichen elektronischen Geräten und die hohe Zahl von durchschnittlich 600 Mobiltelefonauswertungen pro Jahr zeigen allerdings, dass die bestehenden Personalressourcen bereits in naher Zukunft ausgeschöpft sein werden.

ad 9
Wie eingangs erwähnt erarbeiten die Konferenz der Kantonalen Polizeikommandanten (KKPKS) und die Direktion fedpol aktuell eine nationale Gesamtstrategie zu sämtlichen Aspekten der Verfolgung der Cyberkriminalität (NCS). Diese soll die eigentliche Ermittlungsarbeit sowie Fragen der Organisation, der Infrastruktur und der Ausbildung umfassen. Im Rahmen dieser Gesamtstrategie sollen dereinst als Teilaspekte auch die Umsetzungsmodalitäten der Massnahmen und Bedarfsschätzungen aufgezeigt werden, die Gegenstand des Grundauftrages der KOBIK (Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität) ist.

Im Namen des Regierungsrates des Kantons Basel-Stadt

Dr. Guy Morin
Präsident

Barbara Schüpbach-Guggenbühl
Staatsschreiberin