

Mit dem verbundenen Anstieg der Nutzung von elektronischen Geräten (Computer, Mobilgeräte und Onlineangebote) ist eine hohe Cyberkriminalität festzustellen. Fast täglich berichten die Medien von gehakten Firmen- und privaten Accounts und gestohlenen Daten oder sonstigen Verbrechen, wie Erpressung usw.

Die aktuelle Bedrohungslage ist gemäss nationalen Cybersicherheitszentrum NCSC kritisch und wird dauerhaft auch so bleiben. Die Professionalisierung von kriminellen Hackerbanden aus verschiedenen Staaten nimmt stetig zu. Oft ist den Nutzern der vielen digitalen Angeboten nicht bewusst, dass sie ihre Daten und Geräte schützen müssen und auch nicht wie. Da der Schutz von Daten Aufgabe des Staates ist, muss dieser für Aufklärung, Ahndung, Verfolgung und Sensibilisierung sorgen. Wichtig sind eine schnelle Prüfung, Anpassung und Erweiterung der Massnahmen und, da wo nötig, der Gesetzgebung. Basel-Stadt kann und soll bei der Cybersicherheit Schweizweit eine Vorreiterrolle einnehmen und die Sicherheit der verschiedenen Anspruchsgruppen erhöhen. Um diese Sicherheit zu gewährleisten, muss der Kanton, analog der Sicherheit im Verkehr, bei Kriminalität, Terrorismus und anderen Bedrohungen, die entsprechenden technischen und organisatorischen Massnahmen treffen.

### **Geforderte Massnahmen**

#### **Cybercrime-Meldestelle:**

Die Meldestelle muss so ausgebaut werden, dass alle Bürgerinnen und Bürger und alle Firmen immer und in Echtzeit, im Sinne einer Gefahrenkarte (z.B. auf [map.geo.bs.ch](http://map.geo.bs.ch)) über Cyber-Bedrohungen aller Art informiert sind. Per Gesetz muss jede Straftat und Bedrohung sofort gemeldet werden.

Auf diese Informationen muss per Alert (PUSH) und auch auf Abruf (PULL) zugegriffen werden können. Firmen, ab einer zu definierenden Grösse, müssen Cybersicherheitsbeauftragte mit Kompetenzen im IT-Bereich einsetzen.

#### **Awareness-Kampagnen:**

Der Kanton soll mit regelmässigen Kampagnen auf die Cyberbedrohungen aufmerksam machen und so die Bürgerinnen und Bürger sensibilisieren. Dabei sollen Prävention und Vorsichtsmassnahmen im Vordergrund stehen.

Genaue Anleitungen, sowie schnelle und unkomplizierte Hilfen im Falle eines Angriffs oder Diebstahls müssen angeboten und jederzeit abrufbar sein.

Das Prinzip: "Meine Daten gehören mir"; bei Firmen "Die Daten der Kunden gehören ihnen", muss bekannt und gestärkt werden. Es braucht eine Sensibilisierung im Umgang mit der Freigabe persönlicher- und Kundendaten.

#### **Staatliche Aufgaben und Angebote:**

Der Kanton muss, wie bei der "physischen" Kriminalität, Prävention, Schutz und Massnahmen übernehmen. Solange der Kanton diese Aufgaben an ausserkantonale Stellen abgibt, kann er keine eigene Kompetenz aufbauen und die viele Firmen, Bürgerinnen und Bürger nehmen die Cyberkriminalität nicht ernst genug.

#### **Personen bezogene Daten:**

Personenbezogene Daten sind ein sehr hohes und wertvolles Gut. Diese Daten müssen wie eine offizielle Währung behandelt und entsprechend durch technische und organisatorische Massnahmen geschützt werden. Der Kanton muss die Speicherung der sensiblen Daten, analog der monetären Verwaltung und Reserven selbst übernehmen.

#### **Aufbau Kompetenz-Zentrum Cybercrime:**

Um die oben erwähnten Aufgaben bezüglich Cybercrime sicherzustellen, schlagen die Unterzeichnenden den Aufbau eines Kompetenzzentrums Cybercrime im Bereich JSD vor.

Die Unterzeichnenden bitten den Regierungsrat, die Voraussetzungen zu schaffen, damit die Cybersicherheit von Staatlichen Verwaltungen, Firmen und Privaten in Basel-Stadt gestärkt wird.

Philip Karger, Thomas Müry, Mahir Kabakci, Lukas Faesch, Michael Hug, Raoul I. Furlano, Joël Thüring, Christoph Hochuli, Beatrice Isler, Beat von Wartburg, Semseddin Yilmaz, Balz Herter, Niggi Daniel Rechsteiner, Alex Ebi, Luca Urgese