



Conseil d'Etat
Staatsrat

CANTON DU VALAIS
KANTON WALLIS

ANTWORT AUF DAS POSTULAT

Urheber PDCB-Fraktion, durch Eric Lattion (Suppl.) und Sébastien Clerc (Suppl.)
Gegenstand Cyberkriminalität: Walliser KMU sind ideale Ziele
Datum 11.09.2018
Nummer 3.0414

In Zusammenarbeit mit dem DFE

Wie im Postulat hervorgehoben, ist Cyberkriminalität eine grosse Gefahr, die alle Unternehmen, unabhängig von ihrer Grösse, Struktur oder ihrem Tätigkeitsbereich, treffen kann. Dieser Feststellung gilt es Aufmerksamkeit zu schenken, denn es handelt sich um ein bedeutendes Risiko, das alle Unternehmen zu berücksichtigen haben, auch solche, die a priori nicht als Zielscheibe gelten.

Eine umfassende Bestandsaufnahme der Cyberattacken gegen Walliser KMU ist zum aktuellen Zeitpunkt nicht möglich. Mangels angemessener gesetzlicher Grundlagen besteht derzeit keine diesbezügliche Meldepflicht. Eine Bestandsaufnahme könnte nur auf freiwilliger Basis erfolgen und wäre somit definitionsgemäss unvollständig. Im Vorentwurf des Bundesgesetzes über den Datenschutz, der 2019 vom eidgenössischen Parlament behandelt wird, ist jedoch eine Meldepflicht vorgesehen, sobald Personendaten von einer Cyberattacke betroffen sind.

MELANI, die Melde- und Analysestelle Informationssicherung des Bundes, stellt KMUs eine umfassende Website zur Verfügung. Sie beinhaltet zahlreiche Dokumente im Zusammenhang mit dem Schutz von Unternehmen vor Cyberrisiken. Zudem hat das Bundesamt für wirtschaftliche Landesversorgung (BWL) im September 2018 ein Referenzdokument zuhanden der Schweizer Wirtschaft mit dem Titel «Minimalstandard zur Verbesserung der IKT-Resilienz» herausgegeben. Hinsichtlich der Eigenverantwortung der Unternehmen betreffend den Schutz gegen Cyberkriminalität ist die Aussage des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) in seinem «Aktionsplan Cyberdefence» klar.

Unserer Ansicht nach ist es Sache der Walliser Berufsverbände, die Walliser Wirtschaft zu sensibilisieren, wie dies in einigen Fällen bereits geschieht, indem sie Konferenzen zu Cybersicherheit sowie andere Hilfen anbieten. Im Herbst 2018 hat BusiNETvs eine Konferenz für KMU zum Datenschutz organisiert, während die Walliser Industrie- und Handelskammer das 3. Forum zum Thema Cybersicherheit veranstaltet hat.

Zusammenfassend kann also gesagt werden, dass der Bund, die Berufsverbände und die spezialisierten Unternehmen bei den Walliser KMU bereits umfangreiche Sensibilisierungsarbeit leisten, und dass das Prinzip, gemäss dem jedes Unternehmen für seinen eigenen Schutz gegen Cyberrisiken verantwortlich ist, im aktuellen wirtschaftlichen Umfeld pragmatisch erscheint.

Ausserdem kann hervorgehoben werden, dass es nicht für jedes KMU möglich ist, einen hochqualifizierten Sicherheitsexperten einzustellen. Unterstützung durch spezialisierte Unternehmen ist also unter Umständen wünschenswert. Eine weitere Empfehlung für Unternehmen einer bestimmten Grösse mit Blick auf die bessere Berücksichtigung der Sicherheitsaspekte könnte es sein, eine Sicherheitsfunktion einzuführen, die in ein bereits vorhandenes Pflichtenheft integriert wird.

Das Postulat wird zur Ablehnung empfohlen.

Auswirkungen Administration: Vorbereitung eines spezifischen Gesetzes.

Auswirkungen Finanzen (Schätzungen):

- Einmalige Kosten: 50'000 bis 100'000 Franken für die Vorbereitung eines spezifischen Gesetzes.
- Wiederkehrende Kosten: 340'000 bis 390'000 Franken jährlich für die Erstellung, das Hosting und die Betreuung einer Website, die Bereitstellung eines E-Learning-Angebots zur Sensibilisierung von Unternehmen, die Finanzierung von Veranstaltungen zum Thema Sicherheit, die Finanzierung von zwei Arbeitsplätzen (auf der Grundlage des allgemein anerkannten Richtwerts für eine Ressource, nämlich 120'000 Franken/Jahr, wobei anzumerken ist, dass die Kosten für Spezialisten im Sicherheitsbereich pro VZE weitaus höher liegen können) sowie die Beiziehung verschiedener Fachspezialisten.

Auswirkungen Personal (VZE): 2 VZE (Schätzung), nämlich:

- 1 mit der Sensibilisierung der Unternehmen beauftragte Person, welche diese besucht, um sie im Rahmen von Seminaren, Präsentationen und Ausbildungen zu sensibilisieren.
- 1 mit der Unterstützung der Unternehmen beauftragte Person, die deren Fragen beantwortet, mögliche Strategien vorschlägt, Sicherheitsrichtlinien und -empfehlungen sowie bewährte Vorgehensweisen abgibt und sich um die Erfassung und Analyse der gemeldeten Cyberattacken kümmert.

Auswirkungen NFA: keine

Ort, Datum Sitten, den 5. Juni 2019