

Regierungsrat, Rathausstrasse 2, 4410 Liestal

Eidgenössisches Finanzdepartement

Per E-Mail an:  
[ncsc@gs-efd.admin.ch](mailto:ncsc@gs-efd.admin.ch)

Liestal, 29. März 2022

## **Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe, Vernehmlassungsantwort**

Sehr geehrter Herr Bundesrat Maurer  
Sehr geehrte Damen und Herren

Mit Schreiben vom 12. Januar 2022 haben Sie uns eingeladen, im Rahmen der Vernehmlassung zur Meldepflicht von Betreiberinnen kritischer Infrastrukturen für Cyberangriffe unsere Stellungnahme abzugeben.

Wir bedanken uns für diese Einladung und stellen Ihnen im Folgenden unsere Bemerkungen innerhalb der Frist zu.

### **I. Allgemeine Anmerkungen**

Der Regierungsrat des Kantons Basel-Landschaft befürwortet grundsätzlich die Einführung der Meldepflicht und die damit einhergehenden Änderungen des Bundesgesetzes über die Informationssicherheit beim Bund. Die Einführung der Meldepflicht beschränkt einerseits zwar geringfügig den Freiheitsgrad der kantonalen Verwaltung in Bezug auf Zeitpunkt und Umfang von Kommunikation und Information zu allfällig erfolgten Cybercrime-Angriffen. Zudem wird die Meldepflicht zu einer Zunahme von offiziellen Cyberdelikten führen, mit entsprechendem Mehraufwand bei den Strafverfolgungsbehörden. Dies kann zu personellen Ressourcen-Engpässen führen. Andererseits ermöglicht die Gesetzesrevision aber den Zugang und den Zugriff zu unterstützenden Fachkompetenzen beim Nationalen Zentrum für Cybersicherheit, um einen Angriff zu bewältigen und verbessert die Information zur nationalen Bedrohungslage. Das ist sachlich zielführend und wirksam.

**II. Anmerkungen zu einzelnen Bestimmungen:**

*Artikel 73c Absatz 2*

Wir regen an, das Weiterleitungsrecht der Leitung des Nationalen Cybersicherheitszentrums NCSC durch eine Weiterleitungspflicht an die Strafverfolgungsbehörden im Falle des ausdrücklichen Wunsches der Melderin bzw. des Melders im Sinne einer Beschleunigung und zeitnahen Verfahrenseröffnung zu ergänzen.

*Artikel 74d Absatz 2*

Strafrechtlich relevante Begleitumstände eines Cyberangriffs sind gemäss dieser Bestimmung immer zu melden. In Ergänzung zu den bereits aufgeführten Tatbeständen der Erpressung, Drohung oder Nötigung regen wir an, zusätzlich die Datenbeschädigung, begangen durch die Verschlüsselung (encryption) bzw. das Einschleusen (Malware) von Daten, aufzuführen: Zum einen werden bei einem Ransomware-Angriff zuerst die Daten beschädigt. Eine «ransom note» wird durch die Täterschaft nicht zwingend gleichzeitig hinterlegt bzw. kann auch erst mit zeitlicher Verzögerung erfolgen. Diese Zeitspanne bis zur Meldepflicht durch die erfolgte Erpressung, Drohung oder Nötigung gilt es zu verkürzen. Zum anderen stellen staatliche Akteure meist keine Forderungen (z.B. Stuxnet, aktuelle Angriffe auf die digitale Infrastruktur der Ukraine). Diesen Fall gilt es mittels des Tatbestandes der Datenbeschädigung (Verschlüsselung/Malware) abzudecken.

Hochachtungsvoll

Thomas Weber  
 Regierungspräsident

Elisabeth Heer Dietrich  
 Landschreiberin