

VERBINDET
UNSER LAND

SESSIONSBRIEF MÄRZ 2023

EDITORIAL

Sehr geehrte Damen und Herren



Ich freue mich sehr, Sie zu unserer Informationsveranstaltung der Frühjahrsession 2023 zu Fragen rund um die «Metaverse» genannten virtuellen Räume einzuladen. Konkret werden wir uns mit dem Thema **«Metaverse - Relevanz für Gesellschaft, Wirtschaft und Politik»** beschäftigen.

Die Veranstaltung findet wie folgt statt:

**Mittwoch, 8. März 2023 von 19.00 - 21.00 Uhr,
Hotel Bellevue Palace Bern, «Orangerie»**

Um was geht es beim Metaverse? Welche Entwicklungen zeichnen sich ab? Und wie relevant sind diese Entwicklungen für Gesellschaft, Wirtschaft und Politik? Diese und weitere Fragen möchten wir mit Ihnen am Sessionsanlass diskutieren.

Programm:

- Ab 19.00 Uhr **Apéro und Stehdinner**
- 19.55 Uhr **Begrüssung und Eröffnung**
Pierre Kohler,
Präsident SUISSEDIGITAL
- 20.00 Uhr **Metaverse - Relevanz für Gesellschaft, Wirtschaft und Politik**
Fabian Wicki, Inhaber Gestalt
Kommunikation (www.gestalt.ch)
und Dozent an der Fachhochschule
Nordwestschweiz
- 21.00 Uhr **Diskussion bei Kaffee und Dessert**

Wir würden uns freuen, wenn Sie am 8. März 2023 dabei sein könnten. Gerne nehmen wir Ihre Anmeldung per E-Mail an info@suissedigital.ch oder per Telefon unter 031 328 27 28 entgegen.

Schliesslich möchte ich Sie noch auf unseren Stellungnahme zur Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen (Änderung des Informationssicherheitsgesetzes, Vorlage 22.073) auf Seite 2 des vorliegenden Sessionsbriefs hinweisen.

Nun wünsche ich Ihnen eine aufschlussreiche Lektüre und eine erfolgreiche Frühjahrsession.

Pierre Kohler
Präsident SUISSEDIGITAL

AKTUELLE GESCHÄFTE

22.073: Informationssicherheitsgesetz. Änderung (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen)

NR, Donnerstag, 16. März 2023

SUISSEDIGITAL begrüsst die Stossrichtung des Änderungsvorschlags. Da jedoch eine Pflicht zur Meldung von Cyberangriffen eingeführt werden soll, die bei Missachtung sogar zu einer strafrechtlichen Verurteilung der im Unternehmen zuständigen Person führen kann, müsste im Gesetz klar bezeichnet werden, welche Unternehmen unter dieses Obligatorium fallen und wann eine Meldung zwingend an das Nationale Zentrum für Cybersicherheit (NCSC) zu machen ist. Diesem Anspruch wird der Gesetzesentwurf noch nicht gerecht:

- Der **Adressatenkreis** der Meldepflicht bei IT- und Informationsdienstleistungen ist mit Bezug auf die gegebene Kritikalität der betriebenen Netze und Dienste nicht präzise genug ausgearbeitet und abgegrenzt. => Der Adressatenkreis muss präzisiert werden.
- Die **Ausnahmen vom Adressatenkreis** der Meldepflicht sollten schon auf Gesetzesstufe klar benannt werden. Gerade von kleineren Fernmelde-diensteanbieter, die Opfer eines Cyberangriffs werden, kann nicht verlangt werden, dass sie in dieser ausserordentlichen Situation noch zu prüfen haben, ob eine Meldung an das NCSC für sie obligatorisch ist. Auch kann nicht verlangt werden, dass sich diese vorher über eine mögliche Meldepflicht beim NCSC erkundigen. Es wäre vor allem auf die freiwillige Kooperation zu setzen und diese mit entsprechender Öffentlichkeits- und Aufklärungsarbeit durch das NSCS zu fördern. => Es ist im Gesetz eine grosszügig abgegrenzte Ausnahmeregelung vorzusehen.
- Die definierten **Auslösungsfälle** für die zwingende Meldung ans NCSC sind zu vage beschrieben, um verlässlich im Voraus abgrenzen zu können, wann bei bestehender persönlicher Meldepflicht eine Meldung im Einzelfall ans NCSC zu ergehen hat. Bei der Implementation des NCSC-Meldeprozesses in die Unternehmensorganisation werden aber klare Kriterien benötigt, wann eine Meldung durch die zuständige Person an das NCSC zwingend ist. Es sollte zudem klargestellt werden, dass Angriffe auf Endkundinnen und Endkunden bzw. deren Endgeräte und eigene Infrastrukturbestandteile (bspw. Heimvernetzung) keine Meldepflicht

auslöst. => Die Auslösungsfälle müssen präziser beschrieben werden.

SUISSEDIGITAL lehnt insbesondere die vorgesehene persönliche Strafbarkeit der im Unternehmen zuständigen Person bei Missachtung der Meldepflicht ab; eine mögliche Busse des Unternehmens ist ausreichend.

Schliesslich erachtet es SUISSEDIGITAL als problematisch, wenn in ausserordentlichen Situationen, bspw. bei Netz- und Systemausfällen, die vielleicht auf einen Cyberangriff zurückgehen, verschiedene Meldepflichten gegenüber Behörden erfüllt werden müssen. Vielmehr sollte eine zentrale Anlaufstelle, je nach Bedarf, automatisch weitere Stellen informieren.

Fazit: Weisen Sie die Gesetzesänderung zur Verbesserung zurück.