SUISSEDIGITAL
VERBAND FÜR KOMMUNIKATIONSNETZE

VERBINDET
UNSER LAND

SESSIONSBRIEF SEPTEMBER 2023

EDITORIAL

Sehr geehrte Damen und Herren

Es freut mich sehr, dass ich Sie zu Beginn dieser Herbstsession zu folgenden zwei Anlässen einladen kann, die für Sie von grossem Nutzen sein dürften:

Sessionsanlass zum Thema **«Soll Künstliche Intelligenz reguliert werden?»**

Mittwoch, 20. September 2023 von 12.30 - 14.30 Uhr, Hotel Bellevue Palace Bern, «Salon Rouge».

Um was geht es bei der Künstlichen Intelligenz? Welche Entwicklungen zeichnen sich ab? Und wie soll die Politik mit diesem Thema umgehen? Diese und weitere Fragen möchten wir mit Ihnen am Sessionsanlass diskutieren.

Programm:

Ab 12.30 Uhr	**Apéro und Stehdinner**
13.30 Uhr	**Begrüssung und Eröffnung** Pierre Kohler, Präsident SUISSEDIGITAL
	Soll Künstliche Intelligenz reguliert werden? Jörg Mäder, Nationalrat, Digitalpolitiker und Programmierer
Ab 14.00 Uhr	**Diskussion bei Kaffee und Dessert**

Branchenveranstaltung SUISSEDIGITAL-DAY
Mittwoch, 22. November 2023, 09:00 - 17.00 Uhr, Kursaal Bern

An unserer traditionellen Branchentagung SUISSEDIGITAL-DAY stehen Themen wie «Hochbreitbandstrategie des Bundes» (Bernard Maissen, Direktor Bakom) und «Strafbarkeit von Ethical Hacking» (verschiedene Rechtsexperten) sowie weitere topaktuelle Themen auf dem Programm. Begleitet wird die Veranstaltung von einer umfassenden Telekommunikationsausstellung.

Nutzen Sie diese Anlässe für den Austausch mit Unternehmern, Branchenvertreterinnen, Telekommunikations-Experten, Vertreterinnen der Verwaltung und Ratskolleginnen und -kollegen. Anmeldungen nehmen wir gerne unter Tel. 031 328 27 28 oder info@suissedigital.ch entgegen.

Schliesslich möchte ich Sie noch auf unsere Stellungnahme zur Einführung einer Meldepflicht von IT-Schwachstellen (Änderung des Informationssicherheitsgesetzes, Vorlage 22.073) auf Seite 2 des vorliegenden Sessionsbriefs hinweisen.

Nun wünsche ich Ihnen eine erfolgreiche Herbstsession.

Pierre Kohler
Präsident SUISSEDIGITAL

AKTUELLE GESCHÄFTE

22.073: Informationssicherheitsgesetz. Änderung (Einführung einer Meldepflicht für Cyberangriffe auf kritische Infrastrukturen)
NR, Montag, 11. September 2023

Während SUISSEDIGITAL die Einführung einer Meldepflicht für Cyberangriffe begrüsst, lehnt der Verband die vorgeschlagene Meldepflicht von IT-Schwachstellen aus folgenden Gründen dezidiert ab (auch das Ausnehmen der Meldung von Schwachstellen in Eigenentwicklungen ist aus Verbandssicht nicht zielführend):

1) Eine Sammlung von Schwachstellen an zentraler staatlicher Stelle gefährdet die kritischen Infrastrukturen mehr, als sie diese schützt (siehe kürzlich erfolgte Cyberangriffe bei den Bundesbehörden Fedpol & BAZG sowie die Website der eidgenössischen Räte). Ins Gewicht fällt dabei insbesondere auch, dass die Liste der meldepflichtigen staatlichen und privaten Stellen sehr lang ist (siehe Art. 74b E-ISG) und unter anderem alle Bundes-, Kantons-, Gemeindebehörden, die Energieversorger, Finanzdienstleister, sowie auch Kommunikations- oder Transportunternehmen etc. umfasst.
⇨ **Das Risiko, alle gemeldeten Schwachstellen an einer zentralen Stelle zu sammeln, ist zu hoch.**

2) Aufgrund der unterschiedlichen IT-Systeme und der darin integrierten Eigenentwicklungen können betriebskritische Schwachstellen unter den Betreiberinnen kritischer Infrastrukturen nicht verglichen werden. Eine Meldung von Schwachstellen generiert somit keinen Mehrwert, da sich die kritische Software von einer Betreiberin zur anderen stark unterscheiden kann.
⇨ **Da IT-Systeme oft nicht vergleichbar sind, generiert eine zentrale Sammlung von IT-Schwachstellen keinen Mehrwert.**

3) Meldungen von Schwachstellen führen zu einer hohen administrativen Mehrbelastung für die meldepflichtigen staatlichen und privaten Stellen und die zuständige Behörde (NCSC), die von echten Cyberangriffen ablenken.
⇨ **Das Sammeln von IT-Schachstellen an einer zentralen Stelle ist eine Ressourcenverschwendung.**

4) Mit der Sammlung von Schwachstellen an einer zentralen Stelle steigt das Risiko, dass bei einem erfolgreichen Cyberangriff schützenswerte Informationen offengelegt werden. Diese können weitere Cyberangriffe auf kritische Infrastrukturen provozieren, die wiederum das Potenzial für weitreichende Schäden haben. Es ist nicht geklärt, wer bei solchen Angriffen für die daraus resultierenden Schäden haftet.
⇨ **Die Haftungsfrage bei erfolgreichen Hackerangriffen ist ungeklärt.**

5) Die Ausdehnung der Meldepflicht auf Schwachstellen in den IT-Systemen der kritischen Infrastrukturen wäre ein typischer Schweizer Alleingang. Die Vielzahl an international tätigen Unternehmen müssten zwischen nationalen und internationalen Vorgaben unterscheiden, was zu Rechtsunsicherheit und administrativem Zusatzaufwand führt.
⇨ **International tätige Unternehmen hätten mit Rechtsunsicherheit und einem unnötigen administrativen Mehraufwand zu kämpfen.**

Verzichten Sie auf die Einführung einer Meldepflicht für IT-Schwachstellen und folgen Sie dem Entscheid des Ständerats (Minderheit Zuberbühler).