année politique suisse

DOKUMENTATION · ANALYSE · DIFFUSION

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	**19.04.2024**
Thema	**Keine Einschränkung**
Schlagworte	**Cyberkriminalität**
Akteure	**Graf-Litscher, Edith (sp/ps, TG) NR/CN**
Prozesstypen	**Keine Einschränkung**
Datum	**01.01.1965 - 01.01.2023**

Impressum

Herausgeber

Année Politique Suisse
Institut für Politikwissenschaft
Universität Bern
Fabrikstrasse 8
CH-3012 Bern
www.anneepolitique.swiss

Beiträge von

Ackermann, Marco
Baltisser, Lena
Porcellana, Diane

Bevorzugte Zitierweise

Ackermann, Marco; Baltisser, Lena; Porcellana, Diane 2024. ***Ausgewählte Beiträge zur Schweizer Politik: Cyberkriminalität, 2019 - 2022***. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 19.04.2024.

Inhaltsverzeichnis

Abkürzungsverzeichnis

EFD	Eidgenössisches Finanzdepartement
UREK-SR	Kommission für Umwelt, Raumplanung und Energie des Ständerates
SiK-NR	Sicherheitspolitische Kommission des Nationalrates
ElCom	Eidgenössische Elektrizitätskommission
NCS	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
VSE	Verband schweizerischer Elektrizitätswerke

DFF	Département fédéral des finances
CEATE-CE	Commission de l'environnement, de l'aménagement du territoire et de l'énergie du Conseil des Etats
CPS-CN	Commission de la politique de sécurité du Conseil national
ElCom	Commission fédéral de l'électricité
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
UCS	Union des centrales suisses d'électricité

Allgemeine Chronik

Grundlagen der Staatsordnung

Rechtsordnung

Kriminalität

POSTULAT
DATUM: 08.06.2022
LENA BALTISSER

Im Dezember 2021 reichte Edith Graf-Litscher (sp, TG) ein Postulat zur Prüfung von **Massnahmen für einen besseren Schutz gegen Ransomware-Angriffe** ein. Laut der Postulantin stellten Cyberangriffe über Verschlüsselungstrojaner, sogenannte Ransomware, eine grosse Gefahr für die Wirtschaft und die Verwaltung dar. Besondere Beachtung sollten im Rahmen der auszuarbeitenden Massnahmen die Sicherheitsrichtlinien von Unternehmen mit öffentlichem Auftrag, eine mögliche Meldepflicht für Lösegeldzahlungen bei Cyberangriffen und die engere Zusammenarbeit der betroffenen Unternehmen mit den zuständigen Behörden erhalten. Während der Bundesrat das Postulat zur Annahme beantragte, wurde es von Erich Hess (svp, BE) bekämpft. In der Sommersession 2022 stimmte der Nationalrat dem Postulat mit 87 Ja- zu 86 Nein-Stimmen bei 6 Enthaltungen knapp zu, nachdem sich Judith Graf-Litscher und Bundesrat Maurer für dessen Annahme ausgesprochen hatten. Erich Hess hatte auf ein Votum verzichtet. Gegen das Postulat sprachen sich insbesondere die SVP-, FDP- und Mitte-Fraktion aus. [1]

Landesverteidigung

Landesverteidigung

ANDERES
DATUM: 11.12.2020
DIANE PORCELLANA

L'introduction d'une **obligation de signaler les cyberattaques pour les exploitants d'infrastructures critiques** sera soumise à consultation. Avec cette décision, le Conseil fédéral matérialise la mesure formulée dans la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 et fait écho au postulat d'Edith Graf-Litscher (ps, TG). Pour ce faire, le DFF est chargé de soumettre un projet de loi déterminant les types d'incidents à signaler, les délais et les concernés par l'obligation. Les dispositions concrètes relatives à l'obligation de déclarer figureront dans des actes législatifs distincts en fonction de la situation spécifique des secteurs concernés. Si les adaptations législatives devaient être saluées lors de la consultation et approuvées par la suite, les données récoltées dans le cadre de l'obligation permettraient de diffuser des alertes rapides, de renforcer la sécurité et une meilleure évaluation des menaces. [2]

Infrastruktur und Lebensraum

Energie

Energiepolitik

MOTION
DATUM: 04.06.2019
MARCO ACKERMANN

Der Nationalrat nahm in der Sommersession 2019 eine Motion der Thurgauer Nationalrätin Edith Graf-Litscher (sp, TG) mit 114 gegen 77 Stimmen an. Die Sozialdemokratin forderte im Vorstoss, die gesetzlichen Grundlagen dergestalt zu präzisieren, dass für die **Strombranche ein verpflichtender Grundschutz gegenüber Gefahren wie Cyberangriffen oder Naturgewalten** festgelegt wird. Sie begründete ihr Anliegen mit der essenziellen Bedeutung einer stabilen Stromversorgung für das Wohlergehen der Bevölkerung und für die Volkswirtschaft im Allgemeinen. Ein Cyberangriff auf die Strombranche sowie ein grossflächiger Versorgungsunterbruch hätten milliardenschwere Schäden für die Wirtschaft zur Folge. Der Bundesrat hatte im Vorfeld erklärt, er unterstütze zwar die Stossrichtung der Motion, hatte aber vergebens versucht, eine Mehrheit der grossen Kammer von den bereits laufenden oder abgeschlossenen Arbeiten (wie beispielsweise den international etablierten Standards für die Sicherheit von Informations- und Kommunikationstechnik IKT oder den nationalen Strategien zum Schutz kritischer Infrastrukturen SKI und zum Schutz der Schweiz vor Cyberrisiken NCS) zu überzeugen und eine Ablehnung der Motion zu erreichen. [3]

VERWALTUNGSAKT
DATUM: 10.08.2019
MARCO ACKERMANN

In einem Bericht kam die Eidgenössische Elektrizitätskommission ElCom im Februar 2019 zum Schluss, dass im **Bereich der Cybersicherheit im Schweizer Stromversorgungsnetz diverse Mängel** bestünden. Von den befragten 92 grössten Netzbetreibern verfügten demnach 22 über keine Richtlinien oder Massnahmen bezüglich Cybersicherheit und 21 Unternehmen würden ihre Mitarbeitenden in diesem Thema nicht schulen. Um die Sicherheit zu erhöhen, sollten deshalb einerseits die VSE-Branchenrichtlinien durchgehend umgesetzt und andererseits auf die Energiebranche spezialisierte Computer-Notfallteams (Cert) gebildet werden, empfahl die ElCom in ihrem Bericht. Einen anderen Weg wählte indes Swissgrid, die Betreiberin des Schweizer Stromübertragungsnetzes, die mit eigenen Hackern auf die Suche nach Schwachstellen im System gehen wolle, berichtete der Tages-Anzeiger. Auch im Parlament wurde der Ruf nach mehr Cybersicherheit im Stromsektor laut. Bereits im Jahr 2017 hatte Nationalrätin Edith Graf-Litscher (sp, TG) eine entsprechende Motion eingereicht. [4]

MOTION
DATUM: 05.12.2019
MARCO ACKERMANN

Entgegen dem Nationalrat lehnte der Ständerat in der Wintersession 2019 die Motion Graf-Litscher (sp, TG) für die **Schaffung eines gesetzlich verpflichtenden Grundschutzes für kritische Strominfrastrukturen gegenüber Cyberangriffen und relevanten Naturgefahren** stillschweigend ab. Zuvor hatte die einstimmige UREK-SR wie auch der Bundesrat dafür plädiert, die Motion abzulehnen. Kommissionssprecher Martin Schmid (fdp, GR) erklärte in der kleinen Kammer, weder der Bundesrat noch die ständerätliche Kommission stellten das Ziel der Motionärin infrage, sie sähen jedoch den gesetzgeberischen Handlungsbedarf nicht mehr gegeben. So seien beispielsweise mit der nationalen Strategie zum Schutz kritischer Infrastrukturen 2018–2022 oder mit dem revidierten Energiegesetz, das erst nach Einreichen dieses Vorstosses in Kraft getreten sei und das einige Anpassungen in den Bereichen Datensicherheit erfahren habe, bereits ausreichende Massnahmen erarbeitet worden, um den Schutz dieser wichtigen Infrastrukturen vor Cyberangriffen zu verbessern, erklärte Schmid im Plenum. [5]

Netz und Vertrieb

BERICHT
DATUM: 15.12.2019
MARCO ACKERMANN

Im Dezember 2019 legte der Bundesrat einen **Bericht** in Erfüllung des Postulates Graf-Litscher (sp, TG) vor und präsentierte darin **Varianten für die Ausgestaltung von Meldepflichten von kritischen Infrastrukturen bei schwerwiegenden Sicherheitsvorfällen**. Der Bericht erörterte die derzeitige Ausgangslage, verglich Meldepflichten im Ausland und präsentierte nebst der Variante, keine weiteren Meldepflichten einzuführen, drei Varianten für eine Meldepflicht und für Meldestellen in der Schweiz. Bei diesen drei Möglichkeiten würde entweder eine zentrale Meldestelle etabliert, die bisherigen dezentralen Meldestellen in den Sektoren auf- und ausgebaut oder als letzte Variante eine Kombination der beiden Ansätze umgesetzt, wobei eine zentrale Meldestelle einzig für Cybervorfälle und die bestehenden dezentralen Stellen für alle anderen sicherheitsrelevanten Vorfälle zuständig wären. Die vorgeschlagenen vier Varianten sollen in einem nächsten Schritt mit Wirtschaftskreisen, den Kantonen und den zuständigen Behörden vertieft diskutiert werden und im Sommer 2020 zur Erarbeitung einer entsprechenden gesetzlichen Grundlage führen. [6]

POSTULAT
DATUM: 14.09.2020
MARCO ACKERMANN

Im Rahmen des Berichts des Bundesrates über Motionen und Postulate der eidgenössischen Räte 2019 schrieb der Nationalrat im September 2020 das Postulat Graf-Litscher (sp, TG) zur **Ausgestaltung einer Meldepflicht bei schwerwiegenden Sicherheitsvorfällen bei kritischen Infrastrukturen** stillschweigend ab. Im November desselben Jahres nahm die SiK-NR bei Beratungen zur Cybersicherheit Kenntnis vom Bericht. [7]

---

1) AB NR, 2022, S. 1036; AB NR, 2022, S. 586; Po. 21.4512
2) Communiqué de presse du DDPS du 11.12.20
3) AB NR, 2019, S. 836 f.
4) Bericht ElCom Feb 2019; BaZ, TA, 9.8.19; BaZ, TA, 10.8.19
5) AB SR, 2019, S.1078f.; Bericht UREK-SR vom 10.10.19
6) Bericht BR vom 15.6.17
7) BBl, 2020, S. 3380; Medienmitteilung SiK-NR vom 17.11.2020