

Ausgewählte Beiträge zur Schweizer Politik

Suchabfrage	20.04.2024
Thema	Keine Einschränkung
Schlagworte	Cyberkriminalität
Akteure	Reynard, Mathias (sp/ps, VS) 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

Baltisser, Lena
Frick, Karin

Bevorzugte Zitierweise

Baltisser, Lena; Frick, Karin 2024. *Ausgewählte Beiträge zur Schweizer Politik: Cyberkriminalität, 2019 - 2022*. Bern: Année Politique Suisse, Institut für Politikwissenschaft, Universität Bern. www.anneepolitique.swiss, abgerufen am 20.04.2024.

Inhaltsverzeichnis

Allgemeine Chronik	1
Grundlagen der Staatsordnung	1
Rechtsordnung	1
Datenschutz und Statistik	1
Kriminalität	1

Abkürzungsverzeichnis

NCS Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken
NCSC Nationales Zentrum für Cybersicherheit

SNPC Stratégie nationale de protection de la Suisse contre les cyberrisques
NCSC Centre national pour la cybersécurité

Allgemeine Chronik

Grundlagen der Staatsordnung

Rechtsordnung

Datenschutz und Statistik

POSTULAT
DATUM: 21.06.2019
KARIN FRICK

Mit dem Internet verbundene Produkte – etwa «smarte» Haushaltsgeräte, Spielzeuge oder Fahrzeuge und digitale Heimassistenten wie «Siri» oder «Alexa» – erfassen und übermitteln individuelle Daten über ihre Nutzerinnen und Nutzer. Diese Daten seien oft schlecht gesichert und leichte Beute für eine zweckentfremdete Nutzung, stellte Nationalrat Mathias Reynard (sp, VS) fest. Sein Postulat mit dem Auftrag, zu prüfen, wie der **Datenschutz** in diesem Bereich verbessert werden könnte, überwies die grosse Kammer in der Sommersession 2019 stillschweigend. Der Bundesrat hatte die Annahme des Postulats beantragt, weil er den Auftrag zusammen mit einem bereits 2017 überwiesenen Postulat Glättli (gp, ZH; Po. 17.4295) erfüllen könne.¹

BERICHT
DATUM: 29.04.2020
KARIN FRICK

Wie bereits anlässlich der Überweisung des Postulats Reynard (sp, VS) zur **Verbesserung der Sicherheit von mit dem Internet verbundenen Produkten** angekündigt, erfüllte der Bundesrat das Anliegen im selben Bericht wie das thematisch verwandte Postulat Glättli (gp, ZH; Po. 17.4295). Der entsprechende Bericht zu Sicherheitsstandards für Internet-of-Things-Geräte wurde Ende April 2020 veröffentlicht.²

POSTULAT
DATUM: 07.06.2022
LENA BALTISSE

Im Sommer 2022 genehmigte der Nationalrat die **Abschreibung** eines Postulats Reynard (sp, VS) zur **Verbesserung der Sicherheit von mit dem Internet verbundenen Produkten**. Der Bundesrat hatte sich im Bericht zu Sicherheitsstandards für Internet-of-Things-Geräte mit dem Postulat befasst und im Anschluss dessen Abschreibung beantragt.³

Kriminalität

BERICHT
DATUM: 29.04.2020
KARIN FRICK

In Erfüllung zweier Postulate Glättli (gp, ZH; Po. 17.4295) und Reynard (sp, VS; Po. 19.3199) erstellte der Bundesrat einen **Bericht zu Sicherheitsstandards für Internet-of-Things-Geräte**. Er hielt darin mehrere Ansatzpunkte für die Gewährleistung der Sicherheit des Internet of Things (IoT) fest. Erstens seien es oft die Nutzerinnen und Nutzer selber, die die Sicherheit ihrer IoT-Geräte durch leichtfertigen Gebrauch oder Einsatz unsicherer Produkte negativ beeinflussten. Hier gelte es, die Bevölkerung verstärkt zu sensibilisieren und zur Einhaltung grundlegender Verhaltensgrundsätze für einen sicheren Betrieb zu motivieren. Zweitens sei es für den sicheren Einsatz von IoT-Geräten in Unternehmen entscheidend, das IoT als integralen Bestandteil der IT-Infrastruktur zu sehen und bestehende Standards für die IT-Sicherheit auch darauf anzuwenden. Hierzu könnten vom Staat Leitfäden erstellt und der Austausch unter Anwenderinnen und Anwendern gefördert werden. Drittens müssten auch die Hersteller von IoT-Geräten ihre Verantwortung wahrnehmen und Mindestanforderungen an die Informationssicherheit und den Datenschutz erfüllen. Der Staat könne dies durch Erlassen entsprechender Richtlinien und Vorschriften unterstützen. Allerdings müssten neue Vorgaben in internationaler Zusammenarbeit erarbeitet werden, da Vorschriften einzelner Staaten keine ausreichende Wirkung auf die Hersteller hätten und damit höchstens zu Marktverzerrungen führen würden. Alles in allem könne bei konsequenter Umsetzung der bestehenden Richtlinien für IoT-Geräte bereits ein hohes Mass an Cybersicherheit erreicht werden. Das Thema werde vom NCSC im Rahmen der NCS weiterverfolgt, kündigte der Bundesrat abschliessend an. Dabei solle geprüft werden, inwiefern Lösungsansätze wirtschaftsverträglich realisiert werden können.⁴

1) AB NR, 2019, S. 1325; Po. 19.3199

2) Bericht BR vom 29.4.20

3) BBI 2022 858 (S. 38 f.)

4) Bericht BR vom 29.4.20