Datenschutz gibt es nicht ohne Datensicherheit

27. Januar 2022 | Drew Bagley, VP & Counsel, Privacy & Cyber Policy | CrowdStrike

Datenschutz und Datensicherheit bedingen einander. Zumindest legen dies alt hergebrachte Grundprinzipien des Datenschutzes nahe. Dennoch werden beide nicht selten isoliert betrachtet und sogar in Opposition gesetzt. Warum dies weder sachgerecht noch zweckdienlich ist, zeigt dieser Beitrag anlässlich des Tags des Datenschutzes.

Nicht erst seit der Einführung der EU Datenschutz-Grundverordnung (DSGVO) ist Datensicherheit wesentlich für den angemessenen Schutz personenbezogener Daten, d.h. Datenschutz. Bereits in den 70er Jahren hat die US-amerikanische Federal Trade Commission (FTC) mit der Statuierung seiner Fair Information Practice Principles (FIPPs) und später in den 80er Jahren die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) mit ihren Guidelines on the Protection of Privacy and Transborder Flows of Personal Data konstatiert, dass personenbezogenen Daten mit geeigneten Sicherheitsmaßnahmen gegen Risiken des Verlusts, unautorisierten Zugriff, Zerstörung, unbefugte Nutzung, Veränderung und Enthüllung zu schützen sind.

Trotzdem werden Datenschutz und Datensicherheit oftmals getrennt voneinander beurteilt und miteinander in Konkurrenz gesetzt. Dies hängt insbesondere damit zusammen, dass die DSGVO einerseits Datensicherheit beispielsweise in Art. 5 und Art. 32 verlangt, andererseits aber gesetzlich nicht hinreichend privilegiert. Dies führt dazu, dass Datenverarbeitung zum Zweck der Datensicherheit mit allen übrigen Zwecken was etwa die Rechtmäßigkeit der Verarbeitung und die Drittlandsübertragung anbelangt gleichgestellt ist. Dies führt dazu, dass Datenverarbeitungen zum Zweck der Datensicherheit teilweise gesetzlich untersagt sind, weil etwa keine Rechtfertigung nach Art. 6 Abs. 1 DSGVO existiert. Die Bekundung des Gesetzgebers, die Datenverarbeitung zu Zwecken der Informations- und Netzwerksicherheit als legitimes Interesse nach Art. 6 Abs. 1 lit. f DSGVO durch den Erwägungsgrund 49 der DSGVO herauszustellen, ist diesbezüglich nicht weitreichend genug.

Verschärft hat sich diese Lage durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH) in der Rechtssache Schrems II. Durch sie hat der EuGH den Datentransfer in Nicht-EU-Länder unter besondere Bedingungen gestellt. Gestützt auf sie wiederum hat der Europäische Datenschutzausschuss, der Zusammenschluss der nationalen Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten, durch seine Recommendations 1/2020 neue Hürden aufgebaut, die ihrerseits nicht zwischen Datentransfers zum Zweck der Datensicherheit und sonstigen Zwecken differenzieren und zusätzliche Herausforderungen darstellen.

In Zeiten massiv ansteigender und zunehmend ausgefeilter Cyber-Bedrohungen (vgl. CrowdStrike 2021 Global Threat Report), die SecOps in Form von "24x7 follow the sun" unabdingbar machen, verhindert dies teilweise die Gestaltung von Datensicherheit nach dem Stand der Technik, wie sie etwa von der Agentur der Europäischen Union für Cybersicherheit (ENISA) in ihrem Leitfaden zum Stand der Technik empfohlen wird.

Zur Wiederherstellung des Gleichgewichts zwischen Datenschutz und Datensicherheit sowie der Förderung der Zusammenarbeit von Datenschutz- und Datensicherheitsbeauftragten wird von CrowdStrike daher am Tag des Datenschutzes eine Verbesserung der Möglichkeit der Datenverarbeitung zu Zwecken der Datensicherheit als anzustrebendes Ziel formuliert. Orientiert am Privacy by Design Grundprinzip von Full Functionality – Positive Sum, Not Zero Sum von Ann Cavoukian möge sie den Weg dafür ebnen, dass ganzheitlicher Datenschutz nach Maßgabe der DSGVO bei kalkulierbaren Risiko, ohne Einschränkung der Datensicherheit nach dem Stand der Technik gefördert wird und Datenschutz sowie Datensicherheit nebeneinander effektiv erreicht werden können.