Datenschutz, Datensicherheit, IT-Security und Cybersecurity – die Unterschiede praxisnah erklärt und eingeordnet

Anja Schmitz, Juristin, Senior Consultant Projektas GmbH (Zug)
Marco Hiestand, Gründer und Geschäftsführer BREVIT AG (Wetzikon)

Das revidierte Datenschutzgesetz stellt auch Anforderungen an die Datensicherheit. In der Praxis werden jedoch die Begrifflichkeiten Datenschutz, Datensicherheit, IT-Security und Cybersecurity nicht sauber getrennt und vielfach vermischt. Eine Abgrenzung und Erläuterung enthält der folgende Beitrag.

Das Thema Datensicherheit wird in Art. 8 des revidierten Datenschutzgesetzes (DSG) abgebildet und stellt einen Bearbeitungsgrundsatz im Umgang mit Personendaten dar. Demnach wird verlangt, dass der Verantwortliche durch geeignete technische und organisatorische Massnahmen für eine angemessene Datensicherheit sorgt. Diese Anforderung wurde dabei nicht neu in das Gesetz aufgenommen, sondern bestand im Wesentlichen bereits unter dem alten Datenschutzrecht.

Neu ist jedoch, dass die vorsätzliche Verletzung von Art. 8 DSG nun mit einer Busse sanktioniert werden kann, und zwar wenn die erforderlichen Mindestanforderungen nicht umgesetzt worden sind. Die Busse kann dabei bis zu CHF 250 000 betragen.

Ebenfalls hinzugekommen ist, dass neu auch eine sog. Meldepflicht für Verletzungen der Datensicherheit besteht (nach Art. 24 DSG). Kommt es somit zu einer Verletzung, im Fachjargon auch «Data Breach» genannt, muss dies – wenn die notwendigen Voraussetzungen gegeben sind – der zuständigen Aufsichtsbehörde gemeldet werden. Die Unternehmen sind somit dazu angehalten, einen entsprechenden Meldeprozess einzuführen. Nach der Legaldefinition ist eine Verletzung der Datensicherheit gegeben, wenn diese dazu führt, dass Personendaten unbeabsichtigt oder widerrechtlich verlorengehen, gelöscht, vernichtet oder verändert werden oder Unbefugten offengelegt oder zugänglich gemacht werden. Kann diese Verletzung voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen, dann sind die Voraussetzungen für eine Meldung gegeben. Somit kann ein einfacher Hackerangriff bereits ausreichen, um eine Meldepflicht auszulösen. Zunächst soll jedoch der Zusammenhang zwischen dem Datenschutz und der Datensicherheit beleuchtet werden.

Zusammenhang zwischen Datenschutz und Datensicherheit

Essenziell ist es, sich erst einmal zu verdeutlichen, welche Schutzziele überhaupt bestehen. Der *Datenschutz* schützt nämlich gerade nicht «die Daten» – auch wenn das Wort dies vermuten lässt –, sondern das DSG bezweckt gemäss Art. 1 den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden. Im Fokus des DSG stehen dabei die sog. Personendaten. Dies sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, wie z.B. Name, Geburtsdatum und AHV-Nummer. Reine technische Daten oder Sachdaten wie z.B. Konstruktionsdaten, Strategien oder Rezepturen fallen nicht unter das DSG und werden nicht durch das Gesetz geschützt (auch wenn diese aus Sicht der Unternehmung ebenfalls sensitiv sind und geschützt werden sollten).

Die *Datensicherheit* hingegen verfolgt als Ziel, grundsätzlich erst einmal alle Informationen (= Daten) zu schützen, egal ob diese einen Personenbezug haben oder nicht. Der Anwendungsbereich der Datensicherheit ist somit weiter gefasst als der des Datenschutzes. Die Schutzziele der Datensicherheit sind dabei die Vertraulichkeit, Integrität und Verfügbarkeit der Daten. «Vertraulichkeit» bedeutet, dass Daten unautorisierten Individuen oder Systemen nicht zugänglich sind. «Integrität» bedeutet, dass Daten durch unautorisierte Individuen oder Systeme nicht verändert oder gelöscht werden können. Und «Verfügbarkeit» bedeutet, dass Daten durch die für die Bereitstellung, Speicherung und Prozessierung verantwortlichen Systeme jederzeit zur Verfügung stehen.

Das DSG schreibt für den Datenbereich der Personendaten verbindlich vor, dass diese entsprechend den gesetzlichen Anforderungen geschützt sein müssen. Dies wird erreicht, indem die sog. TOMs – ein Kürzel für die «technischen und organisatorischen Massnahmen» – hinreichend umgesetzt werden. Dazu behört bspw. ein ausgereiftes Berechtigungskonzept, Firewalls, eine Protokollierung, eine Verschlüsselungslösung oder auch die Reduktion gespeicherter Daten. Diese Massnahmen werden dann durch flankierende Audits und verschiedene Kontrollaktivitäten einer kontinuierlichen Ver-