



Dr. Alexander Golland
Schriftleitung
Datenschutz-Berater

Datensicherheit – Fremd- und Selbstschutz

Neben den Brexit-Verhandlungen, die auch datenschutzrechtliche Implikationen haben, hat im Januar vor allem ein Thema für Furore gesorgt: die Veröffentlichung privater Daten in der Vorweihnachtszeit, welche über einen zunächst kaum beachteten Twitter-Account erfolgte.

Öffentliche Debatten über Datenschutz sind schon seit den NSA-Enthüllungen von Edward Snowden keine Seltenheit mehr. Dennoch weist die Diskussion der jüngeren Vergangenheit über den „Hackerangriff“ auf Mitglieder des Bundestages und Prominente einige neue Nuancen auf. Nicht nur, dass erstmals in Deutschland eine politische Komponente von Datensicherheit sichtbar wird, nein, der sogenannte Bundestag-Leak offenbart schonungslos einen von Unternehmen häufig vernachlässigten Aspekt im Bereich der IT-Sicherheit: den Faktor Mensch.

Wo Menschen handeln, passieren naturgemäß Fehler. Der Umstand, dass ein 20-jähriger ohne besondere IT-Sicherheitskenntnisse oder Hardware derart viele Accounts kompromittieren kann, überraschte dennoch viele. Es war kein Hack – es wurde lediglich ausgenutzt, dass Menschen häufig dieselben Passwörter für unterschiedliche Accounts nutzen, diese nicht ändern, auf Zwei-Faktor-Authentisierung verzichten und die Antworten auf ihre Sicherheitsfragen in sozialen Netzwerken öffentlich zugänglich machen. Einmal die Passwort-vergessen-Funktion ausgenutzt, und schon ist alles Weitere ein Kinderspiel. Die Bundestags-Leaks sind vor allem ein Zeugnis mangelnder Bildung im Umgang mit eigenen und fremden Daten; eine Kompetenz, die im 21. Jahrhundert von essen-

tieller Bedeutung ist. Digitalisierung ist längst in der Mitte der Gesellschaft angekommen – die notwendige Datenumgangskompetenz offenbar nicht. Dies erschreckt. Zu recht.

Das Datenschutzrecht adressiert hingegen die andere Seite, wo Gefahren für die informationelle Selbstbestimmung durch gesetzliche Pflichten aufgefangen werden sollen. So sind die Leaks auch ein Aufruf an die Unternehmen, die Anforderungen an Datensicherheit (u. a. Artikel 32 der Datenschutz-Grundverordnung) ernst zu nehmen. Sicherheitsmechanismen müssen entwickelt und implementiert werden, die eine derartige Kompromittierung verhindern. Dazu gehört nicht nur, für Nutzer bestimmte Kennwortvorgaben zu definieren, sondern auch, die eigenen Mitarbeiter – etwa in Bezug auf Social Engineering – zu schulen. Der Faktor Mensch ist überall.

Damit Sie auf aktuelle Entwicklungen im Bereich des Datenschutzrechts stets optimal vorbereitet sind, haben wir auch für diese Ausgabe eine Auswahl hochinteressanter Nachrichten und Beiträge zusammengestellt. Eine spannende Lektüre wünscht

Ihr

Alexander Golland