Sarah Ryglewski
Mitglied des Deutschen Bundestages
Stellvertretende Landesvorsitzende der SPD Bremen

Namensbeitrag:

Der Datenskandal und seine verbraucherpolitischen Lehren

Vergangene Woche veröffentlichten Hacker private Informationen von rund 1000 Politikern, Prominenten und Journalisten im Internet. Die Datenpakete enthielten private Handynummern, Adressen, Chatverläufe und sogar Urlaubsfotos. Ein Twitter-Account verbreitete die Download-Links. Während das Ausmaß der Veröffentlichung, der Personenkreis der Betroffenen und die zögerliche Reaktion der Sicherheitsbehörden zu einer hitzigen Debatte geführt haben, sind täglich unzählige Bürgerinnen und Bürger von demselben Problem betroffen: Daten- und Identitätsdiebstahl.

Für die Betroffenen hat das gravierende Konsequenzen. Es werden private Informationen missbraucht und finanzielle Schäden verursacht, etwa durch den Diebstahl von Kreditkarteninformationen. Es reicht nicht mehr aus, auf die Eigenverantwortung der Nutzer zu verweisen. Die einzelne Nutzerin kann nicht mit Facebook oder Microsoft darüber verhandeln, welche Verschlüsselungsstandards für Daten angewendet werden oder wie technische Zugangshürden zu privaten Nutzerinformationen ausgestaltet sind. Hier ist die Bundesregierung gefragt. Sie muss all jene in Verantwortung nehmen, die die mit dem Anbieten digitaler Dienste Geld verdienen.

Betroffene schildern, dass es mehrere Wochen gedauert habe, bis sie wieder die Hoheit über ihren E-Mail-Account erhalten haben. Eine zwei-Faktor-Authentifizierung für Online Dienstleistungen ist immer noch nicht Standard und Name und Geburtsdatum reichen, um sich zu identifizieren und online Bestellungen auszulösen. Wenn Daten erbeutet werden, dann sind sie zumeist nicht verschlüsselt und erlauben so Unbefugten, ohne weitere Hürden Einsicht darin zu nehmen. Dabei gibt es längst Verschlüsselungsstandards, die zusätzliche Sicherheit gewähren. Hier muss die Bundesregierung aktiv werden und gesetzliche Ansprüche auf Datensicherheit schaffen.

Das so geschaffene Rahmenwerk nimmt Anbieter von Online-Dienstleistungen stärker in die Pflicht, die Daten ihrer Nutzerinnen und Nutzer zu schützen. Betriebssysteme sollten die höchsten verfügbaren Sicherheitsstandards anbieten und zwar so, dass sie für den Verbraucher ohne vertiefte Kenntnisse nutzbar sind. Im Idealfall als Voreinstellung. Dieser Anspruch könnte als ein „Recht auf Einfachheit“ bei Datensicherheit im Internet verwirklicht werden. Die besten Sicherheitsvorkehrungen nützen nichts, wenn sie von den Verbraucherinnen und Verbrauchern nicht genutzt werden, weil ihre Anwendung zu kompliziert ist.

Darüber hinaus müssen stärkere Vorkehrungen gegen Identitätsmissbrauch getroffen werden, um die Folgen von Datendiebstahl einzugrenzen. Es kann nicht sein, dass mit dem guten Namen und der guten Bonität anderer im Internet auf Rechnung eingekauft werden kann und die Betroffenen mit dem Ärger und den Auswirkungen auf ihre Kreditwürdigkeit hängen gelassen werden. Unternehmen müssen verpflichtet werden diese Form der Bezahlung nur nach vorheriger Identifikation zuzulassen und einen Kundenservice einrichten, der bei Problemen, insbesondere wenn sie die Datensicherheit betreffen sofort reagiert und nicht erst nach Wochen. Hier braucht es eine gesetzliche Regelung, die eine Frist definiert und keinen Unterschied macht, ob es sich um eine Dienstleistung handelt, die mit Geld oder mit Daten bezahlt wird.

Sarah Ryglewski
Mitglied des Deutschen Bundestages
Stellvertretende Landesvorsitzende der SPD Bremen

Es gilt den politischen Diskurs zu überwinden, nachdem Sicherheit nur auf Kosten von Freiheit realisiert wird. Dieser Diskurs entspringt einer schiefen Argumentationslogik und hat in der Debatte die Oberhand gewonnen. Wenn der Zugang zu Daten schon nicht sicher geregelt werden kann, dann müssen Daten zumindest wirksam verschlüsselt sein. Hier aber treten bisher die Sicherheitsbedenken der Innenpolitiker zutage. Verschlüsselte Bürgerdaten sind aber keine Gefahr für die Sicherheit des Landes. Im Gegenteil: So verzeichnet zum Beispiel, dass Hasso-Plattner-Institut der Uni Potsdam täglich um die 900.000 unberechtigten Zugriffe auf Nutzeraccounts. Hierin liegt das wahre Sicherheitsrisiko: in der Unsicherheit, der die Bürgerinnen und Bürger täglich ausgeliefert sind. Dieses gilt es wirksam zu bekämpfen.

Berlin, den 7.01.2019