Datenschutz

Verantwortung übernehmen

[01.04.2019] Im Interview erklärt der Bundesdatenschutzbeauftragte Ulrich Kelber, was Behörden und Bürger in Bezug auf Datensicherheit beachten sollten und welche Lehren aus den jüngsten Hacker-Angriffen gezogen werden können.

Herr Kelber, Sie sind Ende vergangenen Jahres zum neuen Bundesdatenschutzbeauftragten (BfDI) gewählt worden. Welche Schwerpunkte haben Sie sich für Ihre Amtszeit gesetzt?

Ein wesentlicher Fokus wird darauf liegen, die Regeln der Datenschutz-Grundverordnung (DSGVO) europaweit einheitlich anzuwenden und durchzusetzen. Gerade in Bezug auf die großen internationalen Internet-Firmen haben wir mittlerweile wirksame Mittel, um die Vorgaben der DSGVO auch durchzusetzen. Schließlich geht es beim Datenschutz nicht nur um die Grundrechte einzelner Bürgerinnen und Bürger. Es geht auch um den Schutz unserer freiheitlichen, demokratischen und pluralistischen Gesellschaft. Wer sich ständig überwacht fühlt, egal ob von privaten Unternehmen oder vom Staat, ändert sein Verhalten. Wenn über Personen große Datensammlungen und Verhaltensvorhersagen existieren, können diese leichter manipuliert werden. Das müssen wir verhindern. Nicht unsere Grundrechte müssen sich staatlichem Handeln oder Geschäftsmodellen unterwerfen, sondern Staat und Konzerne müssen sich an unseren Grundrechten ausrichten. Ein weiterer Fokus wird darauf liegen, im Bereich der Informationsfreiheit für noch mehr Transparenz zu sorgen. Hier prüfe ich aktuell, wie der BfDI mit gutem Beispiel vorangehen und aktiv Dokumente veröffentlichen kann, ohne dass es zu einer Anfrage nach dem Informationsfreiheitsgesetz gekommen ist.

Gleich zu Beginn Ihrer Amtszeit herrschte große Aufregung, da Hacker persönliche Daten und Dokumente Hunderter deutscher Politiker öffentlich gemacht haben. Wie bewerten Sie diesen Angriff?

Der Fall reiht sich in eine immer längere Liste von Vorfällen ein, bei denen Daten aus dem Internet unberechtigt abgegriffen und Dritten zugänglich gemacht wurden. Auch wenn dieser Fall in Bezug auf die Quantität ein eher kleinerer war, muss angesichts der Qualität der veröffentlichten Daten, die teilweise sogar Informationen aus den intimsten Lebensbereichen erfassen, von einer massiven Datenschutzverletzung gesprochen werden.

Welche Lehren sollten aus diesem Hacker-Angriff auf Politikerdaten gezogen werden?

Nach allem, was wir wissen, konnten die Daten insbesondere deshalb gesammelt und veröffentlicht werden, weil die Passwörter zu privaten E-Mail-Konten, Cloud-Diensten und sozialen Netzwerken zu leicht zu erraten waren oder durch Phishing-Angriffe oder Ausnutzung von Passwort-Rücksetzungsverfahren erbeutet wurden. Auch wenn wir Missbrauch nie zu hundert Prozent verhindern können, gibt es Maßnahmen, um hier in Zukunft gewappnet zu sein. Nutzer müssen einen besseren Eigenschutz betreiben. Dazu gehören zum Beispiel starke Passwörter, die sich für jeden Dienst unterscheiden, die Nutzung von Zwei-Faktor-Authentifizierung, eine sensibilisierte Verwendung von Cloud-Diensten und der Einsatz von Verschlüsselung auch im privaten Bereich. Ansonsten hilft eine gesunde Skepsis etwa beim Öffnen von E-Mail-Anhängen. Jeder sollte aber auch bei der Nutzung sozialer Medien genau überlegen, welche privaten Details er veröffentlichen möchte. Zudem sollten die Anbieter von Diensten verpflichtet werden, Vorkehrungen zu treffen, um das Risiko entsprechender Angriffe so weit wie möglich zu reduzieren. So dürften beispielsweise zu einfache Passwörter nicht mehr zugelassen werden. Im Fall

eines Angriffs müssten die Anbieter schnell und unkompliziert mit den Behörden kooperieren, um den entstandenen Schaden und eine weitergehende Verbreitung von illegal veröffentlichten Daten bestmöglich einzudämmen. Darüber hinaus müssen die Datenschutzaufsichtsbehörden bei Cyber-Angriffen, die auch den Datenschutz gefährden, unverzüglich informiert und eingebunden werden. Wenn die zuständigen Behörden aus den Medien von entsprechenden Vorfällen erfahren, ist das eindeutig zu spät.

Ist ein Rückzug aus den sozialen Medien, wie in Robert Habeck praktiziert, für Politiker das Mittel der Wahl?

Diese Entscheidung muss letztlich jeder selbst treffen. Ich persönlich halte den völligen Verzicht auf soziale Medien, die für viele Menschen heute fest zum Alltag gehören, für falsch. Aber sicherlich ist es wichtig zu überlegen, welche sozialen Medien man nutzt und bedient. Es gibt oft datenschutzfreundliche Alternativen. Ich habe ein Problem mit Geschäftsmodellen, bei denen eine unglaubliche Datenmenge produziert wird, die vielfältige kommerzialisierbare Rückschlüsse auf die Nutzer zulässt, wenn gleichzeitig völlig unklar ist, wie mit diesen Informationen umgegangen wird.

„Bei allen Kanälen, auf denen Behörden kommunizieren, müssen sie sicherstellen, dass die Datenschutzvorgaben beachtet werden.“
Was sollten Behörden, die sensible Bürgerdaten verwalten, in Bezug auf die Datensicherheit beachten?

Alle Behörden sind verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um ein angemessenes Schutzniveau für die verarbeiteten Daten zu gewährleisten. Die Auswahl der Maßnahmen sollte auf der Grundlage einer Risikobewertung erfolgen. Dabei sind Art, Umfang, Umstände und Zwecke der Verarbeitung und das Risiko für die Rechte und Freiheiten des Betroffenen zu berücksichtigen. Konkrete gängige Maßnahmen wären beispielsweise die Zutrittskontrolle zu Räumlichkeiten, die Zugangskontrolle zu den verwendeten IT-Verfahren, die Beschränkung des Zugriffs auf gespeicherte Daten durch ein aufgabenbasiertes Rechte- und Rollenkonzept, der Schutz vor unberechtigtem Zugriff beim Transport oder der Übertragung von Daten, etwa durch Verschlüsselung, die Nachvollziehbarkeit und Dokumentation von Dateneingaben, -pflege und -verwaltung, die Sicherstellung der Verfügbarkeit und der Schutz vor Datenverlusten sowie die Trennung von Daten, die zu verschiedenen Zwecken erhoben werden.

Wie sollten Behörden ihre Mitarbeiter zum Thema Datenschutz sensibilisieren?

Wichtig sind aus meiner Sicht Schulungen durch die behördlichen Datenschutzbeauftragten, die auf die Besonderheiten und Gegebenheiten der jeweiligen Behörde eingehen können. Zudem sollte man mit den Datenschutzaufsichtsbehörden im Austausch stehen.

Wie bewerten Sie Auftritte öffentlicher Verwaltungen bei Facebook und die Kommunikation von Stadtoberhäuptern via WhatsApp?

Bei allen Kanälen, auf denen Behörden kommunizieren, müssen sie sicherstellen, dass die Datenschutzvorgaben beachtet werden. Liegt dies nicht in ihrer Hand, sollten bestimmte Kanäle gemieden werden, um sich nicht der Gefahr auszusetzen, bei Datenschutzverletzungen des genutzten Mediums zur Verantwortung gezogen zu werden. Dies sollte spätestens seit der Entscheidung des Europäischen Gerichtshofs über die gemeinsame Verantwortung von Facebook und Fanpage-Betreibern jedem klar sein. Die Datenschutzkonferenz hat dazu eine Entschließung mit dem sehr passenden Titel „Die Zeit der Verantwortungslosigkeit ist vorbei“ herausgegeben. Gerade Behörden sollten hier mit gutem Beispiel vorangehen. Das gilt auch noch für einen anderen Grundsatz: Alle Informationen, die man über Facebook

& Co. veröffentlicht, müssen für Bürger auch erreichbar sein, ohne dass dabei ihre Daten abgegriffen werden, etwa via RSS-Feed.

()

Dieser Beitrag ist in der Ausgabe April 2019 von Kommune21 im Schwerpunkt Datenschutz erschienen. Hier können Sie ein Exemplar bestellen oder die Zeitschrift abonnieren.

Stichwörter: IT-Sicherheit, BfDI, Datenschutz, Facebook, Social Media, Ulrich Kelber, WhatsApp