Datenschutz*aktuell Ausgabe Mai 2019*

Der Datenschutz Newsletter aus Nürnberg

Hier nun die zweite Ausgabe des Datenschutz Newsletters.

Themen im Mai 2019:

- 2019 Neues Jahr - neue Datenrisiken
- Die Verpflichtung auf das Datengeheimnis

2019: Neues Jahr, neue Datenrisiken?

Auch für 2019 haben IT-Sicherheitsexperten wieder ihre Prognosen veröffentlicht über neue Risiken, die personenbezogenen Daten bedrohen. Es wäre aber falsch, sich nun besonders auf diese Risiken zu konzentrieren.

Die Zeichen stehen auf Sturm

Gleich, ob Sie sich die Vorhersagen der Sicherheitsbehörden oder der Sicherheitsanbieter für 2019 ansehen: Kaum ein Security-Experte ist der Meinung, dass die Risiken für personenbezogene und andere zu schützende Daten geringer werden. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht von einer Gefährdungslage auf einem neuen Niveau. Cyber-Angriffe werden 2019 noch intelligenter und ausgereifter, erklären auch die Forscher von Fortinet. Zieht man Parallelen zu den Wetterprognosen, lässt sich sagen, die Sicherheitsspezialisten erwarten eine Zunahme von schweren Unwettern.

Nicht an die steigenden Risiken gewöhnen

Die Berichte der Security-Experten rund um den Jahreswechsel bekommen in den Medien immer viel Aufmerksamkeit. Doch besteht die Gefahr, dass wir Menschen uns daran gewöhnen, dass die Gefahren aus dem Internet und für unsere Daten immer größer werden. Tatsächlich nehmen die Risiken für personenbezogene Daten stetig zu. Die Prognosen der McAfee Labs für 2019 besagen zum Beispiel: Neue mobile Malware wird Smartphones, Tablets und Router austesten, um Zugang zu den digitalen Assistenten, die sie kontrollieren, und zu heimischen IoT-Geräten (IoT = Internet of Things) zu erhalten. Smart Homes werden verstärkt zum Angriffsziel. Was bedeutet das nun konkret für den Datenschutz im neuen Jahr?

Die Risiken folgen der Digitalisierung

Nutzen Unternehmen und Privatpersonen vermehrt Dienste aus der Cloud, werden

Smartphones und Tablets für immer mehr Menschen zum stetigen Begleiter und die Wohnungen immer vernetzter, dann zieht das Angriffswellen auf sich. Überall, wo neue Bereiche digitalisiert werden, ist mit Angriffen der Internetkriminellen zu rechnen.

Doch auch abseits der digitalen Technik lauern Gefahren

Man darf aber nicht vergessen, dass Staat, Wirtschaft und Gesellschaft bei Weitem noch nicht angekommen sind an dem Ziel der digitalen Transformation. Viele Verfahren und Prozesse sind seit Jahren unverändert im Einsatz. Dadurch sind sie aber nicht aus dem Fokus der Angreifer. Die Sicherheitsexperten stellen fest, dass Internetkriminelle mit den klassischen Kriminellen zusammenarbeiten. Jede der kriminellen Seiten lernt und profitiert von der anderen. Deshalb muss weiterhin damit gerechnet werden, dass klassische Einbrüche stattfinden, um an vertrauliche Informationen zu kommen, und nicht nur Hacker-Attacken.

Nur weil die Sicherheitsprognosen die neuen Technologien und ihre Risiken betonen, nehmen die Gefahren in den klassischen Bereichen nicht ab. Im Jahr 2019 muss mit allen bisherigen Bedrohungen gerechnet werden, die wir schon seit vielen Jahren kennen – die neuen Bedrohungen kommen hinzu. Sehen Sie deshalb jede Sicherheitsprognose wie eine Fortsetzungsgeschichte: Es werden neue Kapitel geschrieben, ohne dass man die alten einfach zuschlagen dürfte.

Die Verpflichtung auf das Datengeheimnis

Wer in einem Unternehmen mit personenbezogenen Daten umgeht, muss auf das Datengeheimnis verpflichtet sein. So war man es bisher gewohnt. Die Datenschutz-Grundverordnung (DSGVO) sieht keine förmliche Verpflichtung mehr vor. Trotzdem werden Unternehmen auch in Zukunft eine Verpflichtung unterzeichnen lassen.

Ende eines gewohnten Rituals?

Es gehört zum gewohnten Ritual: Wer neu in ein Unternehmen eintritt, muss eine „Verpflichtung auf das Datengeheimnis“ unterschreiben. Dazu erhält er ein Infoblatt. Hintergrund ist eine entsprechende Regelung im bisherigen Bundesdatenschutzgesetz (BDSG-alt). Am 25. Mai 2018 löst die DSGVO das BDSG-alt ab. Die DSGVO enthält keine Regelung mehr, wonach Beschäftigte auf das Datengeheimnis zu verpflichten sind. Das hört sich zunächst nach einem willkommenen Abbau von Bürokratie an. Doch so einfach ist es nicht.

Herausforderung „Rechenschaftspflicht“

Die DSGVO verpflichtet alle Unternehmen dazu, die Datenschutzvorschriften zu beachten. Zusätzlich sieht sie eine „Rechenschaftspflicht“ vor. Das heißt: Unternehmen

müssen nachweisen können, dass sie die DSGVO tatsächlich beachten. Zur Einhaltung der DSGVO gehört es, den Mitarbeitern zu verdeutlichen, welche Pflichten sie im Datenschutz haben. Dazu braucht es eine Art Belehrung. Sie muss schriftlich dokumentiert sein. Anders lässt sich nicht nachweisen, dass den Mitarbeitern ihre Pflichten klar waren.

Muster der Datenschutzaufsicht

Auf der Webseite des Bayerischen Landesamts für Datenschutzaufsicht findet sich das Muster „Verpflichtung zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DSGVO)“. Es führt die wesentlichen Grundsätze auf, die im Datenschutz zu beachten sind. Damit erinnert es nur an das, was sich ohnehin schon aus dem Gesetz ergibt. Der Text schafft keine Pflichten, die dort nicht enthalten sind. Von daher gibt es keinen Grund für einen Beschäftigten, die Unterschrift zu verweigern.

Kreis der zu Verpflichtenden

Zu verpflichten sind alle Personen, die mit personenbezogenen Daten umgehen. Das sind außer der „Stammbelegschaft“ auch Auszubildende, Praktikanten und Leiharbeiter. Wichtig ist, dass die Verpflichtung bei Aufnahme der Tätigkeit erfolgt. Also spätestens am ersten Arbeitstag. Selbstverständlich kann sie jedoch auch schon vorher geschehen.

Inhalt statt Formalie!

Die Inhalte der Verpflichtung sind das eigentlich Wichtige. Aus diesem Grund wäre es auch nicht gut, die Verpflichtung als eine lästige Formalie anzusehen nach dem Motto: „Das haken wir am ersten Arbeitstag schnell ab, und dann liegt das Formular eben jahrelang in der Personalakte.“ Die Datenschutzaufsicht empfiehlt, alle Beschäftigten immer wieder einmal daran zu erinnern, dass die Verpflichtung weiterhin gilt und was sie bedeutet. Dies kann durch Aushänge, aber auch zum Beispiel durch eine E-Mail an alle oder in Schulungen geschehen. Hier können die Unternehmen wählen.

Impressum:
Redaktion
Peter Brandmann (V.i.S.d.P.)
Externer Datenschutzbeauftragter nach § 40 Abs. 6 BDSG-neu
Zertifizierte Fachkraft DSGVO nach Art. 37 Abs. 5 DSGVO
Anschrift:
pb beratung & training Inhaber: Peter Brandmann
Schnepfenreuther Weg 51
90425 Nürnberg
Telefon: 0911 3506118
info@pb-beratung-training.de