C-IAM GmbH: Datenschutzgrundverordnung droht die Blockade Europas?

KW 2: EU Datenschutz Grundverordnung 2018 von Joachim Jakobs (https://blog.c-iam.com)

"Die explodierende Leistungsfähigkeit teilt die Menschheit in zwei Gruppen: Angegriffene und Angreifer; die einen meinen, sie hätten nichts zu verbergen und klicken auf alles, was ihnen vor die Maus kommt, die anderen verwenden künstliche Intelligenz, um menschliche/technische Schwächen automatisiert auszunutzen. Der digitale Graben wächst parallel zur technischen Entwicklung. Der Gesetzgeber verlangt jetzt von den Unternehmen, die Sicherheit ihrer Datenverarbeitung nachweisen zu können. Ansonsten drohen drakonische Strafen und Schadenersatzforderungen. Das kann die Unternehmen in ihrer Existenz bedrohen."

Die Leistungsfähigkeit der Informationstechnik steigt nicht, sie galoppiert. Und das schon seit einem halben Jahrhundert – bis Mitte des kommenden Jahrzehnts soll sich diese Leistungsfähigkeit weiterhin alle zwei Jahre verdoppeln Link . Das Ergebnis: 2011 hat ein sprechender und Sprache verstehender Computer namens Watson die US-Quizsendung „Jeopardy!“ gewonnen und dabei bisherige menschliche „Champions“ dieses Wettbewerbs Medienberichten zufolge „deklassiert“ Link . Hinzu kommt das Erkennen von Bildern – Maschinen sollen mit dem Menschen gar bei der zuverlässigen Erkennung von Hautkrebs konkurrieren Link . Und die Technik kann lernen, reale Menschen zu imitieren – der „Bush-o-Matic“ etwa spricht beliebige Texte mit der Stimme und dem texanischen Dialekt des früheren US-Präsidenten George W. Bush Link . Eine Nachbildung des Kopfs von Kaiser Wilhelm II antwortet auf die Frage „Wer waren Ihre Feinde?“: „Meine Feinde waren die Französische Republik und das British Empire.“ Link

Und das ist noch lang nicht alles: Französische Wissenschaftler behaupten, sie könnten die Bewegungen einer Person aufnehmen und anschließend diese Körpersprache auf einen Avatar übertragen Link : „Durch das Berechnen der Ausdrucksstärke lassen sich personalisierte Animationen berechnen, so dass der Betrachter den Eindruck hat, er interagiere mit einem ausdrucksstarken virtuellen Menschen.“ Künftig könnte noch die Physiologie – die physikalischen und biochemischen Vorgänge in den Zellen – nachgebaut werden Link . Nicht auszuschließen ist, dass eines Tages ein robotischer Klon Link eines Verstorbenen hergestellt werden kann. Und wenn ja, wie viele Kopien des Originals werden dann wo unterwegs sein? Mit all dem Wissen, Erfahrungen und der Persönlichkeit

des Verstorbenen? Dann waren die Selbstquantifizierung Link , die Facebook- und Twitter-Beiträge doch für irgendwas gut! Sogar die in Schuhen verbaute Intelligenz soll künftig die der Menschen übertreffen Link . Dabei taugt die Digitalisierung nicht nur zur Herstellung laufender Rechenzentren: Die Anzahl der vernetzten Geräte soll sich zwischen 2017 und 2020 nach Erkenntnis der Marktforscher von Gartner von 8,4 auf 20 Milliarden mehr als verdoppeln Link und in Autos, Heizungen und Herzschrittmachern Verwendung finden. Doch der TÜV Nord mag nicht in die Begeisterung einstimmen und warnte stattdessen im Mai 2017 „vor Sicherheitslücken durch Digitalisierung“ Link .

Wer hat Zugang zu Daten und das Recht mit diesen Daten zu arbeiten?

Wir müssen präzise überlegen, wer das Recht hat, unseren digitalisierten Vorfahren und anderen Geräten Wissen zu entlocken und anschließend wohin auch immer zu übertragen – egal, ob diese Maschinen als einzelne Computer (oder Roboter) daherkommen, oder das Wissen in den (Computernetzen der) Unternehmen oder ganzen Ländern enthalten ist. Wer hat das Recht (oder die Pflicht!?) diese Daten oder Informationen zu welchem Zeitpunkt und von welchem Ort aus zu löschen? Was bedeutet das fürs Personalmanagement? Welche Qualifikation benötigen die, die im Auftrag des Chefs in welcher Rolle auch immer tätig werden?

Überhaupt: Wer darf Entscheidungen fällen? Oder auf Basis dieser Entscheidungen mit welcher Ausbildung Software entwickeln, einrichten, verwalten oder nutzen, um vernetzte Geräte zu steuern oder personenbezogene Daten damit zu verarbeiten? Um das Leben der Nutzer nicht zu gefährden, sollten wir bis dahin den rechtssicheren Zugriff auf diese Geräte beherrschen.

csoonline.com ist der Ansicht Link , mit einem robusten Identitäts- und Zugangsmanagement (Identity and Access Management, IAM) würde ein konsistentes Regelwerk zu den Benutzerrechten in einer Organisation eingeführt. Damit ginge gar eine zusätzliche Sicherheitsebene einher. Die zentrale Verwaltung der Nutzer führe darüber hinaus zu einer Verringerung der Komplexität und einer Erhöhung der Produktivität. Soweit zu den technischen Möglichkeiten und dem Soll-Zustand.

Die Beratungsresistenz der Entscheider nimmt ab

Tatsächlich scheint es jedoch mau um die Fähigkeiten der Teutonen bestellt zu sein: 2013 bekannte die Kanzlerin: „Das Internet ist für uns alle Neuland.“ Link – Und das über 20 Jahre nachdem Tim Berners Lee die technischen Grundlagen des World Wide Web veröffentlicht hat Link . Offenbar hat Angela Merkel nicht sehr viel unternommen, damit wir in Neuland Fuß fassen: 2014 fand die Unternehmensberatung Pricewaterhouse-Coopers (PwC) in ihrem Informationsrisiko-Index heraus, dass deutsche Unternehmen die am schlechtesten gesicherten in ganz Europa sind Link . Im Sommer 2017 stellte die TÜV Informationstechnik (TÜViT) fest, dass lediglich 3 Prozent – in Worten: Drei! – aller Deutschen Unternehmen auf Angriffe vorbereitet seien Link . Immerhin: 2017 will eine andere Unternehmensberatung festgestellt haben, dass nur noch 38 Prozent der IT-Verantwortlichen den Chefs mangelndes Sicherheitsbewusstsein bescheinigen Link . 2015 solls noch halbe-halbe gewesen sein. Die Bildungsresistenz der Entscheider nimmt ab! Zumindest bei Unternehmen mit mehr als 500 Mitarbeitern. Eine gute Nachricht. Die Schlechte: Sollte es tatsächlich noch 4 von 10 Chefs an Sicherheitsbewusstsein mangeln, ist das für mich noch kein Anlass zur Entwarnung! Und: Was machen die „Kleinen“? Die mittlerweile verantwortungsbewussten Chefs müssen ihren Anwälten, Immobilienmaklern, Steuerberatern und Vermögensverwaltern auf den Zahn fühlen, bevor sie ihnen ihre personenbezogenen Daten anvertrauen. Und: „Alarmierend viele Startups“ sollen „Hacker-Freiwild“ sein Link . Von diesen forschungsintensiven Unternehmen hängt aber die Zukunft unseres Landes ab!

Die Angreifer nutzen die Möglichkeiten bis zum Anschlag aus!

Vor einem Jahr hat die Computerwoche darüber spekuliert Link , ob die Schäden krimineller Angreifer durch künstliche Intelligenz eingedämmt werden könnten – oder mit künstlicher Intelligenz im Gegenteil noch weiter zunehmen würden.

Kriminelle künstliche Intelligenz? 2010 behauptete der damalige Französische Präsident Sarkozy, Bundeskanzlerin Merkel wolle „Roma-Lager" in Deutschland räumen Link . Da es solche Lager hierzulande nicht gibt, können sie auch nicht aufgelöst werden. Wesentlich überzeugender wäre es allerdings, wenn ein Video von Merkel auftauchen würde, indem sie den Austritt aus dem Euro ankündigt. Genauso könnte ein Avatar eines Unternehmers die Insolvenz des eigenen Unternehmens oder die Übernahme eines Konkurrenten bekanntgeben. Eine völlig neue Qualität der „Fake News" – mit massiven Folgen für die wichtigste Währung der Informationsgesellschaft überhaupt: Vertrauen! Das Verständnis dieser Prozesse ist so wichtig, weil die Entwicklung den Angreifern in die Hände spielt: Zum Einen vergrößert die Vernetzung von Allem mit Allem die Angriffsfläche – eine ungesicherte Überwachungskamera kann vom Angreifer zur Manipulation von Industrierobotern und in der Folge zur physikalischen Sabotage dienen Link . Und gleichzeitig trägt die Vernetzungsdichte für den Sicherheitsexperten Steve King zu einer ‚asymetrischen Bedrohung' bei Link : Bei bestimmten Angriffsmaschen müssten die Angreifer heute noch 38 US-Dollar aufwenden, während die Angegriffenen aktuell das Tausendfache, 40.000 US-Dollar, in die technische Abwehr dieser Angriffe stecken. Die technische Entwicklung führe zu einer weiteren Spreizung.

Die knallharten Daumenschrauben der DSGVO

Sind Sie in der Lage, die Sicherheit der Datenverarbeitung Ihres Unternehmens und das Erfüllen des ‚Stands der Technik' nachzuweisen? Der wird nämlich in Artikel 32 Datenschutzgrundverordnung (DSGVO) gefordert. Wenn nicht, empfehle ich die Lektüre dieses Aufsatzes Link vom Teletrust – Bundesverband IT-Sicherheit e.V.; der Verband definiert:

„Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten - wenn dies noch nicht der Fall ist - möglichst im Betrieb mit Erfolg erprobt worden sein. Im Recht der Europäischen Union wird auch die Formulierung "die besten verfügbaren Techniken" verwendet. Dies entspricht weitgehend der Generalklausel "Stand der Technik".

Martin Schallbruch, früher Abteilungsleiter Informationstechnik, Digitale Gesellschaft und Cybersicherheit im Bundesinnenministerium, kommentiert: "Die von TeleTrusT veröffentlichte Handreichung zum 'Stand der Technik' hat mir persönlich sehr gefallen. Warum? Weil ich mir bei der Verabschiedung des ITSiG (IT-Sicherheitsgesetz, Anm. d. Autors) gewünscht habe, dass ein renommierter Fachverband kommt und sagt: 'Seht hier, das ist der geforderte Stand der Technik'. TeleTrusT erklärt in der Handreichung den geforderten Sicherheitsstand und schafft somit Klarheit über die notwendigen Maßnahmen." Wenn einer wie Schallbruch das mit seiner Autorität sagt, ist die Wahrscheinlichkeit groß, dass sich diese Definition selbst zum Stand der Technik entwickelt; und sich fix bei Gutachtern, Anwälten und Richtern herumspricht.

Einen weiteren Hinweis darauf, dass man die Latte lieber nicht zu niedrig legen sollte, liefert die Berliner Landesbeauftragte für den Datenschutz Maja Smoltczyk: Eine Empfehlung der „VdS 3473" Link als Basis für ein Datenschutzmanagementsystem könne sie „aus aufsichtsbehördlicher Sicht nicht mittragen". Die VdS 3473 könne keine Alternative für den BSI Grundschutz oder die ISO 27001 darstellen.

Der Mittelstand würde sich aber wohl die Finger danach lecken, wenn er den Premium-Standard VdS 3473 erfüllen würde. Premium scheint aber nicht ausreichend zu sein. Stand der Technik ist die Super-Luxusklasse mit Goldrand: Die 15. Ergänzungslieferung des BSI-Grundschutzes vom Januar 2016 umfasst 5082 Seiten Link ! Und das soll der Mittelstand bis 25. Mai 2018 vollständig umsetzen?

Der Nachweis der Datensicherheit („Integrität und Vertraulichkeit“) gehört zu Ihrer „Rechenschaftspflicht“ (Art. 5, Absatz 2 DSGVO Link) – Absatz 1 dieses Artikels fordert darüber hinaus „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“, „Zweckbindung“, „Datenminimierung“, „Richtigkeit“ und „Speicherbegrenzung“.

Der Chef haftet nicht nur für die eigenen, sondern auch die Böcke seiner Mitarbeiter: „Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.“ (Art. 32 (4) DSGVO Link).

Bei Verstoß gegen die DSGVO drohen „Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes Link je nachdem, welcher der Beträge höher ist“ (Art. 83 (6) DSGVO Link). Der Präsident des Bayerischen Landesamts für Datenschutzaufsicht Thomas Kranig warnt Link sogar Zahnärzte vor Geldbußen „bis zu 10 Mio. EUR“ und fordert nicht nur „alle Unternehmen“ sondern auch „Vereine, Verbände und freiberuflich Tätigen“ auf, sich vorzubereiten.

Die Feinheiten verleihen der Verordnung eine besondere Würze: Stephan Hansen-Oest, Fachanwalt für IT-Recht glaubt, die DSGVO werde „ein neues Feld für Abmahnungen werden. Viele Regelungen der DSGVO werden sog. Marktverhaltensregelungen im Sinne des §3a UWG Link sein. Das weckt sicher Begehrlichkeiten bei einigen Kreisen.“

In diesem Paragraphen des Gesetzes gegen den unlauteren Wettbewerb heißt es: „Unlauter handelt, wer einer gesetzlichen Vorschrift zuwiderhandelt, die auch dazu bestimmt ist, im Interesse der Marktteilnehmer das Marktverhalten zu regeln, und der Verstoß geeignet ist, die Interessen von Verbrauchern, sonstigen Marktteilnehmern oder Mitbewerbern spürbar zu beeinträchtigen.“

Außerdem gibt’s peinliche Informationspflichten: „Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.“ (Art. 34 DSGVO Link). Wieviel 1.000 Kunden/Mitarbeiter haben Sie? Wie lang es wohl dauern wird, bis diese Benachrichtigung auf Facebook veröffentlicht ist?

Weiterhin drohen Schmerzensgeldansprüche: „Jede Person, der wegen eines Verstoßes gegen diese Verordnung (die DSGVO, Anm. d. Autors) ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter“ (Art. 82 (1) DSGVO Link).

Das einzige Schlupfloch: „Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 2 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“ (Art. 82 (3) DSGVO). Die Rechenschaftspflicht gilt mit der Anwendbarkeit der DSGVO ab 25. Mai 2018. Den Verbraucherschützern räumt der Gesetzgeber dabei ein eigenes Verbandsklagerecht ein (Art. 80 DSGVO Link). Der Betroffene (Mitarbeiter, Kunde, Patient, Bürger) braucht also noch nicht einmal selbst einen Anwalt anzuheuern.

Im Juli 2017 sollen nur zwei Prozent der Unternehmen ab 1.000 Mitarbeitern die Forderungen der DSGVO tatsächlich bereits erfüllt haben Link . Womöglich hängt der geringe Umsetzungsgrad auch damit zusammen, dass es den CIO und IT-Verantwortlichen an einem umfassenden Verständnis der EU-DSGVO-Zusammenhänge mangeln soll Link .

Die Berliner Aufsichtsbehörde kündigte gegenüber Chefsache: Datensicherheit! bereits per Mail an: „Betriebsprüfungen werden künftig verstärkt auch standardisiert, d. h. anhand einheitlicher Fragebögen, erfolgen. Bereits jetzt erfolgen schon vereinzelte, zwischen mehreren Aufsichtsbehörden koordinierte, branchenspezifische Prüfverfahren, in denen im selben Zeitraum eine Vielzahl einer bestimmten Branche zugehöriger Unternehmen in standardisierter Form geprüft wird. Ein Beispiel für einen solchen – unspezifischen! – Fragebogen gibt's hier Link: Die Behörden können es dabei gar nicht abwarten, die kräftigen Daumenschrauben anzulegen Link .

Die schlimmste Sanktion droht von den Betroffenen selbst: Europaweit sollen 59 Prozent der Verbraucher in Europa bereits von einem Datenvorfall gehört haben, 57 Prozent Link besorgt über den Umgang mit ihren Daten und 64 Prozent der Verbraucher weltweit wollen ihre Geschäftsbeziehung mit einem Unternehmen beenden Link , dem die Daten gestohlen wurden.

Der Vertrauensmangel kann sich fix auswirken auf Kunden, Lieferanten, Investoren, Banken und Versicherer. Jeder Verantwortliche haftet dabei persönlich – nicht nur nach Art. 4 Nr. 7 DSGVO Link , sondern die Vorstände auch noch nach Aktiengesetz Link und die Geschäftsführer nach GmbH-Gesetz Link ; die Geheimnisträger (Ärzte, Anwälte, Steuerberater etc.) und ihre Auftragsverarbeiter stehen zusätzlich mit einem Bein im Gefängnis, wenn's schief geht Link .

Wir müssen unser Bildungssystem aktualisieren und überlegen: Über welche Qualifikation müssen Chefs, IT'ler und Nutzer künftig verfügen, bevor sie für Dritte tätig werden dürfen. Und: Haftet der Personal-"Verantwortliche", wenn der Mitarbeiter das erforderliche Wissen nicht nachweisen kann und es dadurch zu Verstößen kommt?

Die Datenschutzgrundverordnung ist in der Lage, das zu leisten, was die Banken-, Finanz- und Flüchtlingskrise bislang nicht geschafft haben: Die Blockade Europas. Chefsache: Datensicherheit! will jede Woche einen Beitrag dazu leisten, das zu verhindern.

Kontakt

Jamshed Kharkan
Geschäftsführer

Tel: +49 228 53459235
E-Mail: info@c-iam.com
blog@c-iam.com

C-IAM GmbH
Ballindamm 39
D-20095 Hamburg

https://www.c-iam.com
https://blog.c-iam.com