Helmut Reimer

Report

ULD Datenschutzbericht für das Jahr 2019

Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, hat am 27.März 2020 ihren Tätigkeitsbericht für das Jahr 2019 vorgelegt: Auf knapp 150 Seiten werden die Themen Datenschutz und Informationsfreiheit beleuchtet, Empfehlungen gegeben und Verbesserungen eingefordert. Interessante Fälle dienen als mahnendes Beispiel, wie es die Verantwortlichen nicht machen sollen.

Datenschutz in Zeiten der Corona-Pandemie?

„Ja, besonders in Krisenzeiten ist Datenschutz wichtig", sagt Hansen. „Fast täglich melden sich Menschen bei uns, die Angst um ihre Daten haben. Sie fühlen sich nicht gut genug informiert, um verstehen zu können, wie der Staat, Firmen oder ihr Arbeitgeber mit den Daten umgehen, die dort mit der Begründung „Corona" gesammelt und ausgewertet werden. Auch befürchten sie, dass ihre Daten nicht ausreichend gegen einen unbefugten Zugriff geschützt sind und missbraucht werden könnten. Deswegen informieren wir regelmäßig über unsere Webseite."

Überlegtes Vorgehen statt halbgarer Schnellschüsse – realistisch?

An vielen Stellen werden neue Datenverarbeitungen zurzeit eingeführt, z. B. Registrierungspflichten von Kundinnen und Kunden oder von Beschäftigten im Handwerk. Auch werden Systeme aufgebaut, damit zahlreiche Akteure im Gesundheitsbereich Zugriff auf bestimmte Daten von Kranken oder ihren Kontaktpersonen erhalten. Hansen kann die hohe Geschwindigkeit im Krisenmodus nachvollziehen, aber besteht darauf, dass stets die Verhältnismäßigkeit der geplanten Datenverarbeitungen geprüft wird und ausreichende Garantien für die Rechte und Freiheiten der Menschen gegeben sind.

Datenschutzbeauftragte tragende Säulen

„Im vergangenen Jahr haben wir festgestellt, dass einerseits das Bewusstsein für Datenschutz in der Bevölkerung gestiegen ist – das zeigt sich an der großen Zahl von Beschwerden und Fragen. Andererseits gibt es mit den betrieblichen und behördlichen Datenschutzbeauftragten Vor-Ort-Kompetenz bei den Firmen und Behörden. Das sind die tragenden Säulen für guten Datenschutz, weil sie die internen Prozesse ihrer Organisation in den Blick nehmen und bewerten. Bedingung dafür ist aber, dass sie ihren Job auch machen können, die erforderliche Fachkompetenz haben und die Verantwortlichen ihren Rat einholen – das klappt bisher nicht überall."

Für die aktuelle Situation bedeutet dies: „Wer nun bei den Anpassungen oder Neugestaltungen der Datenverarbeitungen (z. B. für Homeoffice oder die Verarbeitung von Gesundheitsdaten) seine Datenschutzbeauftragte oder seinen Datenschutzbeauftragten nicht darüber informiert hat, sollte dies dringend nachholen!", so Hansen. Für die Beratung der betrieblichen und behördlichen Datenschutzbeauftragten steht Hansens Dienststelle, das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), weiterhin zur Verfügung.

Digitalisierung mit Datenschutz und Sicherheit DSGVO

Hansen erwartet durch die Corona-Pandemie einen Schub für die Digitalisierung: „Allerdings dominieren weiterhin globale Player auf dem Markt, die es mit Datenschutz nicht so genau nehmen. Hier rächt sich, dass man zu wenig auf sichere und datenschutzfreundliche Alternativen gesetzt hat. Eigentlich bietet die Datenschutz-Grundverordnung die Instrumente, um die globalen Marktakteure auf Einhaltung des Datenschutzes zu verpflichten – das erfordert aber einen langen Atem der Aufsichtsbehörden in Europa und den Weg durch die gerichtlichen Instanzen." Dies liegt laut Hansen auch an den abstrakten Formulierungen in der Datenschutz-Grundverordnung (DSGVO), die von den Aufsichtsbehörden und Gerichten konkretisiert werden müssen.

Facebook-Fanpages

Gerichtliche Verfahren können sich über einen langen Zeitraum erstrecken: Seit 2011 läuft das Verfahren zu einem ULD-Bescheid zur Deaktivierung einer Facebook-Fanpage, für das der Europäische Gerichtshof (2018) und das Bundesverwaltungsgericht in Leipzig (2019) deutlich gemacht haben, dass sich keine Organisation, die solche Fanpages einsetzt, der datenschutzrechtlichen (Mit-)Verantwortung entziehen kann. Im Jahr 2020 wird sich erneut das Schleswig-Holsteinische Oberverwaltungsgericht damit beschäftigen.

Zertifizierung

Ein weiteres Instrument der Datenschutz-Grundverordnung – die Zertifizierung der Einhaltung der Datenschutz-Grundverordnung – läuft noch leer, obwohl sich Hansens Dienststelle dafür in besonderem Maße einsetzt. „Viele Leute möchten sich schnell mit einem Datenschutz-Zertifikat einen Überblick verschaffen können, ob eine Datenverarbeitung datenschutzkonform ist – das ist aber zurzeit schwierig. Immerhin geht es nun in Europa voran. Wir erwarten, dass die ersten Zertifizierungsverfahren in Deutschland dieses Jahr begonnen werden können", sagt Hansen.

Pseudonymisierung und Transparenz

Die zunehmende Digitalisierung sieht Hansen als Chance, wenn Datenschutz – und auch Informationsfreiheit – gleich von Anfang an eingebaut werden, also „by Design". Aus ihrer Sicht besonders relevant sind die passenden Pseudonymisierungs- und Anonymisierungsverfahren, wie sie nun auch für die Forschung mit Gesundheits- und Pandemiedaten diskutiert werden. Nachholbedarf besteht zudem in Bezug auf bessere Transparenz.

Datenpannen – ein Grund zur Sorge!

Im Vergleich zum Vorjahr sind 2019 sehr viel mehr Datenpannen an das ULD gemeldet worden als früher. Hansen geht dabei von einer enormen Dunkelziffer aus: „Die Datenpannen, die uns gemeldet werden, zeigen, dass in den Organisationen ein Bewusstsein dafür vorhanden ist und ein Meldeprozess etabliert wurde,

so wie es rechtlich geboten ist. Die Datenpannen sind ganz verschieden: fehladressierte Schreiben, offene E-Mail-Verteiler, verlorene USB-Sticks, Rechner-Infektionen mit Schadsoftware oder Programmierfehler – all dies wird uns fast täglich gemeldet." Sorgen bereiten Hansen aber nicht nur die Zunahmen bei Infektionen mit Schadsoftware, die immer wieder wellenartig auch in Schleswig-Holstein auftreten, sondern vor allem solche Bereiche, in denen gar nicht oder sehr sparsam gemeldet wird: „Es wäre zumindest ungewöhnlich, wenn bei Tausenden von Beschäftigten, die mit personenbezogenen Daten umgehen, nie Datenschutzfehler aufträten." Im Jahr 2019 ist im ULD aus dem Bereich der Justiz nur eine einzige Datenpannenmeldung eingegangen. Der Polizeibereich hat für das ganze Jahr sogar überhaupt keine Datenpanne gemeldet. Hier fragt sich Hansen in ihrem Bericht, ob die Bediensteten ausreichend für das Thema sensibilisiert und Meldewege definiert und bekannt gemacht wurden.

Auch in der aktuellen Situation der Corona-Pandemie ist es Hansen wichtig, dass nicht fahrlässig mit den sensiblen Gesundheitsdaten umgegangen wird – von der Erhebung bis zur Löschung, unabhängig davon, ob sie digital oder auf Papier vorliegen. Sie betont: „Dass letztes Jahr kubikmeterweise Patientendaten in der Innenstadt frei zugänglich waren, darf sich nicht wiederholen." Auch ist Sorgfalt vonnöten, wenn personenbezogene Daten nicht im Büro, sondern im Homeoffice verarbeitet werden. „Zurzeit werden uns weniger Datenpannen gemeldet als früher. Für die nahe Zukunft erwarte ich jedoch eine größere Verbreitung von Schadsoftware, weil viele Rechner außerhalb einer professionellen Unternehmensinfrastruktur ins Internet gehen. Das Risiko für Fehler oder Datenmissbrauch steigt gerade."

Datenschutzbericht für 2019: Zahlen und Fakten

Im Jahr 2019 hat das ULD auf Basis von Beschwerden betroffener Personen in eigener Zuständigkeit 915 Verfahren eingeleitet. Der Anteil der Beschwerden im öffentlichen Bereich lag bei etwa einem Viertel, der überwiegende Teil betraf den nichtöffentlichen Bereich (primär die Datenverarbeitung durch Unternehmen). Ein Teil der Beschwerden wurde mangels Zuständigkeit des ULD an andere Aufsichtsbehörden abgegeben.

Zusätzlich wurden 349 Datenpannen nach Art. 33 Datenschutz-Grundverordnung an das ULD gemeldet. Im Vergleich zum Vorjahr, in dem diese Meldepflicht ab dem 25. Mai 2018 galt, hat sich die durchschnittliche Zahl der gemeldeten Datenpannen pro Monat von knapp 18 auf mehr als 29 Fälle erhöht.

Hier ist der Jahresbericht im Netz zu finden: *https://www.datenschutzzentrum.de/tb/tb38/index.html*

Berliner BfDI: Jahresbericht 2019

Die Berliner Beauftragte für Datenschutz und Informationsfreiheit (BlnBDI), Maja Smoltczyk, veröffentlichte am 03. April 2020 ihren Jahresbericht für das Jahr 2019.

Allgemeine Entwicklungen aus der Dienststelle

Das Arbeitsaufkommen in der Berliner Behörde für Datenschutz und Informationsfreiheit hat sich im Jahr 2019 auf unverändert stark erhöhtem Niveau eingependelt. So hat sich nach dem Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 das Aufkommen an Beschwerden, die in der Behörde eingehen, verdreifacht. Im Schnitt erreichten die Behörde monatlich fast 400 Beschwerden. Thematisch betrafen diese besonders häufig die Missachtung von Betroffenenrechten, insbesondere das Recht auf Auskunft oder Löschung. Ein Großteil der eingehenden Beschwerden richtete sich gegen Unternehmen aus der Digitalwirtschaft, wie z. B. Onlineshops, Lieferdienste oder soziale Netzwerke. Daneben prägten Themen aus den Bereichen der Wohnungswirtschaft, der Gesundheit, den Finanzdienstleistungen und dem Beschäftigtendatenschutz die Arbeit der Behörde in besonderem Maße.

Kaum in einem anderen Bereich stieg das Arbeitsaufkommen so stark an wie bei den sog. Datenpannen. Insgesamt wurden im Jahr 2019 1017 solcher Pannen gemeldet, womit sich das Aufkommen seit Wirksamwerden der DSGVO sogar versiebzehnfacht hat. Ob aus einer Kita gestohlene Digitalkameras, Post-Irrläufer oder Schadsoftware-Angriffe – die Fallkonstellationen im Bereich der Datenpannen sind vielfältig und erfordern oftmals ein unverzügliches Handeln Darüber hinaus waren die Mitarbeiterinnen und Mitarbeiter der BlnBDI im vergangenen Jahr auch wieder mit komplexen Beratungsvorgängen im öffentlichen Bereich, mit zahlreichen Presseanfragen und Hinweisen aus der Presse, mit anonymen Anzeigen und Prüfungen von Amts wegen befasst, soweit es ihre völlig unzureichenden Kapazitäten zuließen.

Die Einführung der DSGVO hat zahlreiche Anpassungen des Landesrechts notwendig gemacht, die der Berliner Gesetzgeber eigentlich bereits zum 25. Mai 2018 hätte erlassen müssen. Fast zwei Jahre nach Ablauf dieser Frist befindet sich Berlin nun auf der Zielgeraden. Mit einem Artikelgesetz sollen Mitte 2020 ca. 80 Berliner Gesetze und Verordnungen an die neue Rechtslage angepasst werden. Leider wurden wichtige Kritikpunkte der BlnBDI von der federführenden Senatsverwaltung für Inneres und Sport bisher nicht berücksichtigt. Bewegt sich der Gesetzgeber in diesen Punkten nicht, wird es teilweise zu europarechtswidrigen Regelungen im Landesrecht kommen.

Themen des Jahresberichts (Auswahl)

Datenschutz ist ein Thema, das jeden denkbaren Lebensbereich berührt. Entsprechend vielfältig war auch im Jahr 2019 die Arbeit der Berliner Datenschutzbehörde.

Ein wichtiges Ziel der Datenschutz-Grundverordnung ist es, die Praxis der Verhängung von Bußgeldern bei datenschutzrechtlichen Verstößen EU-weit anzugleichen. Auf europäischer Ebene wird die konkrete Methodik, nach der die Datenschutzbehörden bei der Verhängung von Bußgeldern vorgehen sollen, derzeit noch diskutiert. Um zumindest deutschlandweit ab sofort schon eine einheitliche, transparente und nachvollziehbare Bußgeldpraxis zu garantieren, haben die deutschen Aufsichtsbehörden in dem von der BlnBDI geleiteten „Arbeitskreis Sanktionen" der Konferenz der unabhängigen deutschen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) ein Bußgeldkonzept erarbeitet, das nun angewendet werden kann, bis entsprechende europäische Leitlinien verabschiedet sind. In ihrem Jahresbericht erklärt die BlnBDI das von der Wirtschaft mit großem Interesse erwartete Konzept.

Auch bei der Prüfung von Beschwerden und Datenpannen hat die Zusammenarbeit der Datenschutzbehörden der EU Fahrt aufgenommen. Die DSGVO sieht vor, dass zwischen den europäischen Aufsichtsbehörden immer dann ein sog. Kooperationsverfahren durchgeführt wird und beabsichtigte Maßnahmen abgestimmt werden, wenn die beanstandete Datenverarbeitung einen grenzüberschreitenden Bezug hat. Im Jahresbericht 2019 legt die BlnBDI dar, wie dieses Kooperationsverfahren in der Praxis aussieht. Anhand von Praxisbeispielen werden die Herausforderungen bei der

Zusammenarbeit aufgezeigt und Instrumente vorgestellt, die die Datenschutz-Grundverordnung dafür vorsieht.

Einen Schwerpunkt widmet der Jahresbericht dem Thema Künstliche Intelligenz. Der Bericht zeigt auf, welche Chancen in der Technik stecken, welche Risiken mit ihr für den Datenschutz verbunden sind und was bei dem Thema dringend beachtet werden muss. Besonders wird in diesem Zusammenhang auf die Aspekte Transparenz und vollautomatische Entscheidungen eingegangen.

Transparenz war ebenfalls im Rahmen intensiver Beratungen zur Umsetzung des Onlinezugangsgesetzes (OZG) auf Landesebene ein wichtiges Thema. Das OZG sieht vor, dass bis Ende 2020 alle Verwaltungsdienstleistungen auch digital zur Verfügung stehen. Die Digitalisierung von Verwaltungsdienstleistungen kann jedoch nur dann erfolgreich verlaufen, wenn die Nutzenden bereit sind, die digitalen Angebote auch wahrzunehmen. Um eine breite Akzeptanz zu fördern, setzte sich die BlnBDI daher u. a. erfolgreich für eine adäquate Transparenzregelung ein.

Ein besonders schwerwiegendes Ereignis, das die Aufsichtsbehörde im vergangenen Jahr beschäftigte, war der Emotet-Befall beim Berliner Kammergericht. Die BlnBDI überwachte die Sicherheitsmaßnahmen, die zur Bewältigung der Probleme ergriffen wurden und begleitet diesen Prozess weiterhin. In ihrem Jahresbericht erklärt sie, wie es zu einem solchen Schadsoftware-Befall kommen kann und welche Lehren Behörden und öffentliche Stellen aus diesem Vorfall ziehen müssen.

Im Gesundheitsbereich wurde die Datenschutzbehörde z. B. häufig von verunsicherten Ärztinnen und Ärzten kontaktiert, die wissen wollten, ob sie die Herausgabe der Kopie einer Patientenakte wie bisher in Rechnung stellen dürften. Dies musste die BlnBDI verneinen. Patientinnen und Patienten haben im Rahmen ihres datenschutzrechtlichen Auskunftsanspruchs das Recht, unentgeltlich eine Kopie ihrer Akte zu erhalten. Eine anderslautende Regelung im Bürgerlichen Gesetzbuch ist seit der Einführung der Datenschutz-Grundverordnung mit europäischem Recht nicht mehr vereinbar.

Weniger einsichtig war ein Bankenverband. Die BlnBDI wies ihn darauf hin, dass es in Beratungsgesprächen für eine Kreditvergabe unzulässig ist, Kundinnen und Kunden nach deren Familienplanung zu fragen, soweit dies nicht ausdrücklich als freiwillige Angabe gekennzeichnet wird. Der Verband wollte dieser Auffassung jedoch nicht folgen und passte seine Empfehlungen an seine Mitgliedsbanken nicht entsprechend an. Banken, die die Familienplanung rechtswidrig abfragen, müssen nun mit aufsichtsrechtlichen Schritten rechnen.

Ein sich immer weiter entwickelndes Arbeitsgebiet ist nach wie vor der Bereich Videotechnik und Biometrie. In der zweiten Phase des Pilotprojekts zur Videoüberwachung am Bahnhof Südkreuz testete die Deutsche Bahn sog. „intelligente" Videosysteme verschiedener Anbieter. Im Jahresbericht wird erklärt, was in dieser Phase des Projekts getestet wird, wie die Maßnahmen datenschutzrechtlich zu bewerten sind und welche Kriterien bei der Frage zu berücksichtigen sind, ob ein Echtbetrieb zulässig ist.

Als höchstproblematisch im Umgang mit Daten von Besucherinnen und Besuchern erwies sich das Stadtportal Berlin.de. Auf dem Webportal, das in Public-Private-Partnerschaft zwischen dem Land Berlin und einem privaten Anbieter betrieben wird, erfolgte ein intensives Tracking durch Drittanbieter. Die umfangreiche Prüfung dauert an. Im Jahresbericht wird der Sachstand dargestellt.

Seit Ende 2016 entwickelt die Berliner Datenschutzbeauftragte Angebote, mit denen Grundschulkinder für den Schutz ihrer Daten in der digitalisierten Welt sensibilisiert werden. Das neugestaltete und ausgeweitete medienpädagogische Angebot www.datakids.de wurde im Jahr 2019 nicht nur für den deutschen Kindersoftwarepreis TOMMI nominiert, sondern auch in mehreren an Schulen durchgeführten Projektstunden von Kindern und Lehrpersonal mit Begeisterung angenommen.

Nachdem neben den Ländern Bremen, Hamburg und Rheinland-Pfalz nun auch Thüringen über ein Transparenzgesetz verfügt, gibt es auch in Berlin erste Schritte in Richtung eines modernen Informationsfreiheitsrechts. Neben einem breiten Bündnis aus zivilgesellschaftlichen Organisationen, das den Volksentscheid Transparenz Berlin ins Leben gerufen hat, brachte auch die FDP-Fraktion im Abgeordnetenhaus von Berlin einen entsprechenden Gesetzesentwurf ein. Die BlnBDI begrüßt diese Initiativen und wird entsprechende Gesetzesvorhaben aktiv begleiten.

Deutschland-Umfrage „IT-Sicherheit im Home-Office"

Aktuellen Digitalisierungsschub mit Security Awareness verbinden

Deutschland im Home-Office: Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) hat in einer deutschlandweiten Umfrage ermittelt, welche IT-Sicherheitsvorkehrungen die Nutzer umsetzen. Das Ergebnis wurde am 31. März 2020 veröffentlicht.

Deutschland im Home-Office-Modus: Die derzeitige Situation führt erzwungenermaßen zu einer enormen Digitalisierungsbeschleunigung. In kürzester Zeit werden zu Hause Arbeitsplätze nachgebildet, um Betriebsstrukturen digital aufrecht zu erhalten. Während technisch gut aufgestellte Unternehmen ihre Mitarbeiter mit professionellem Equipment ausrüsten, ist anderswo Improvisation und Pragmatismus gefragt. Dabei kann die IT-Sicherheit auf der Strecke bleiben. Gerade jetzt aber schwärmen digitale Raubritter aus, um die Gunst der Stunde zu nutzen und mit Spam, Phishing, Malware, Identitätsdiebstahl und Datenklau schnelle Beute zu machen.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) hat in einer deutschlandweiten Umfrage ermitteln lassen, welche der empfohlenen Sicherheitsvorkehrungen die Home-Office-Nutzer vorhalten:

„Welche IT-Sicherheitsmaßnahmen haben Sie im Home Office getroffen?"

- 65% – Rechner passwortgeschützt
- 63% – WLAN passwortgeschützt
- 61% – Virenschutzprogramm installiert
- 49% – Privater Rechner und Dienstrechner getrennt
- 41% – E-Mail-Verschlüsselung
- 38% – Verschlüsselte Datenübermittlung
- 37% – VPN-Verbindung
- 31% – Datensicherung in der Cloud
- 27% – Mehr-Faktor-Authentifizierung (z.B. Passwort und Bestätigungs-Code oder Biometrie)
- 12% – Keine

TeleTrusT-Vorsitzender Prof. Dr. Norbert Pohlmann: „Das Ergebnis zeigt, dass durchaus Problembewusstsein besteht, die technischen Maßnahmen aber noch verbesserungsbedürftig sind. Wenn es gelingt, den jetzt zu verzeichnenden Digitalisierungsschub flächendeckend und nachhaltig mit einem angemessenen Maß an IT-Si-

cherheit zu verbinden, bewirkt die aktuelle Situation hoffentlich etwas Positives."

TeleTrusT-Hilfsaktion:

Die Mitglieder des Bundesverbandes IT-Sicherheit e.V. (TeleTrusT) stellen über eine öffentliche Webseite für 3 Monate kostenfreie IT-Sicherheitslösungen einschließlich Fernberatung zur Verfügung. Die Angebote richten sich an alle Arten von betroffenen Anwendern: *https://www.teletrust.de/kostenfreie-it-sicherheitsloesungen/.*

BSI erkennt SGS Digital Trust Services als Prüfstelle für CC und CEM an

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat am 20. Mäez 2020 die SGS Digital Trust Services GmbH als Prüfstelle anerkannt. Die zum 15. Februar 2020 ausgestellte Urkunde gilt für die Bereiche Common Criteria (CC) und Common Evaluation Methodology (CEM). Dr. Günther Welsch, Abteilungsleiter Krypto-Technik und IT-Management, und Matthias Intemann, BSI-Fachbereichsleiter für den Bereich der Zertifizierungsverfahren, überreichten die Urkunde am 26. Februar an den SGS-Vizepräsidenten Sergio Lombán Lage. Den Rahmen der Übergabe bildete ein Empfang des Bundesverband IT-Sicherheit e.V. (Teletrust) im deutschen Generalkonsulat San Francisco am Rande der RSA Conference.

Diese Anerkennung berechtigt die SGS Digital Trust Services GmbH, IT-Produkte im Hinblick auf ihre Sicherheitseigenschaften gemäß internationaler Sicherheitskriterien (Common Criteria, CC) entsprechend der vom BSI veröffentlichten Schutzprofile (Protection Profiles, PP) zu prüfen.

Post-Quanten-Kryptografie: BSI veröffentlicht Handlungsempfehlungen

Wie man der Bedrohung der Public-Key-Kryptografie durch zukünftige Quantencomputer heute schon begegnen kann, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer Handlungsempfehlung zusammengefasst. Das am 26. März 2020 veröffentlichte Dokument umfasst acht Seiten.

Quantencomputer sind eine immer realer werdende Bedrohung für die heutige Public-Key-Kryptografie und somit für die Sicherheit digitaler Infrastrukturen. Eine verlässliche Prognose, ob und wann sich diese Bedrohung manifestiert, ist schwierig. Die bisher existierenden Quantencomputer stellen noch keine Bedrohung für die heute verwendeten kryptografischen Verfahren dar, es können aber jederzeit technologische Entwicklungssprünge erzielt werden. Zurzeit wird deswegen intensiv an Quantencomputer-resistenten Alternativen zu den heute verwendeten Public-Key Verfahren gearbeitet. 2017 wurde vom US-amerikanischen National Institute for Standards and Technology (NIST) ein Prozess zur Standardisierung solcher Verfahren initiiert. Dieser Prozess wird allerdings frühestens 2022/23 zu Entwürfen für Standards führen.

Langfristiger Schutz von Geheimnissen

Aus Sicht des BSI steht die Frage, ob oder wann es Quantencomputer geben wird, nicht mehr im Vordergrund. Post-Quanten-Kryptografie wird langfristig zum Standard werden. Abhängig vom Anwendungsfall sollte frühzeitig und kontinuierlich im Rahmen eines maßvollen Risikomanagements abgewogen werden, ob und wann ein Umstieg auf Quantencomputer-resistente Verfahren erfolgen soll. Insbesondere für Informationen mit langfristigem Schutzbedarf sollte die Bedrohung durch Quantencomputer berücksichtigt werden. Es besteht die Gefahr, dass verschlüsselte Informationen auf Vorrat gesammelt und später mit Hilfe eines Quantencomputers entschlüsselt werden können. Der Schutz langfristiger Geheimnisse kann also ein zeitnahes Handeln notwendig machen.

Die Handlungsempfehlungen im Netz: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-kryptografie.pdf;jsessionid=90C32E7002651C9406143732225BF5AE.2_cid360?__blob=publicationFile&v=2*

AllianzRisiko Barometer: Unternehmensbewertungen von Sicherheitsvorfällen im Hinblick auf globale Risiken

Ergebnis einer am 03. März 2020 veröffentlichten Umfrage der Allianz zu den wichtigsten Unternehmensrisiken unter mehr als 2.700 Risikoexperten aus mehr als 100 Ländern.

- Cybervorfälle sind weltweit erstmals das wichtigste Geschäftsrisiko für Unternehmen, vor sieben Jahren belegte es nur den 15. Platz im Allianz Risiko Barometer.
- Als zentrale Herausforderung für Unternehmen bleiben Betriebsunterbrechungen: weltweit an zweiter Stelle und in Deutschland weiterhin an der Spitze.

Das Bewusstsein für Cyber-Bedrohungen hat in den letzten Jahren deutlich zugenommen, was darauf zurückzuführen ist, dass Unternehmen zunehmend auf Daten- und IT-Systeme angewiesen sind und eine Reihe bedeutender Schadensfälle aufgetreten sind. Das Risiko durch Cyber-Vorfälle ist für Unternehmen schädlicher und teurer geworden – und führt häufig zu Klagen und Rechtsstreitigkeiten nach dem Ereignis.

Datenverletzungen größer und teurer

Datenschutzverletzungen werden immer größer und kostspielig weil Unternehmen immer größere Mengen personenbezogener Daten sammeln und verwerten. Insbesondere sogenannte Mega-Datenverletzungen (mit mehr als einer Million Datensätzen) sind häufiger und teurer. Im Juli 2019 gab Capital One bekannt, dass es von einem der größten Verstöße im Bankensektor betroffen war, von dem rund 100 Millionen Kunden betroffen waren. Dieser Verstoß ist jedoch keineswegs der größte in den letzten Jahren.

Ransomware verursacht zunehmend höhere finanzielle Schäden

Laut der EU-Strafverfolgungsbehörde Europol ist Ransomware die größte Bedrohung im Bereich Cyberkriminalität. Ausgeklügelte Angriffe auf KMUs finden immer häufiger stat. Sie führen zu immer höheren Erpressungsforderungen und verursachen große finanzielle Schäden. Vor fünf Jahren ging es um einige zehntausend Euro, heute fordern Hacker immer öfter Millionenbeträge Die Folgen eines Angriffs können lähmend sein, insbesondere für Unternehmen, die bei der Bereitstellung von Produkten und Dienstleistungen auf Daten angewiesen sind. Erpressungsforderungen sind nur ein Teil des Bildes. Eine Betriebsunterbrechung bringt die schwerwie-

gendsten Verluste durch Ransomware-Angriffe mit sich. In einigen Fällen war die Ransomware nur ein erster Schritt für das eigentliche Ziel, z. B. der Diebstahl personenbezogener Daten. Industrie- und Fertigungsunternehmen werden zunehmend gezielt attackiert, aber auch Anwaltskanzleien, Arztpraxen, Berater und Architekten erleiden empfindliche Schäden, weil ihre IT nur unzureichend geschützt ist. Vorfälle wie die mit der Ryuk-Malware haben sich in den letzten Jahren als Haupttreiber für Cyber-Versicherungsansprüche herausgestellt. Erstmals im August 2018 gemeldet war sie weltweit für mehrere Angriffe gegen große Unternehmen, Krankenhäuser und Kommunalverwaltungen verantwortlich.

BEC-Angriffe führen zu Milliardenbetrug

Business email compromise (BEC) – oder Spoofing – Angriffe werden immer häufiger. Nach Angaben des FBI in den USA haben BEC-Vorfälle seit 2016 zu weltweiten Verlusten von mindestens 26 Mrd. USD geführt. Die Angriffe umfassen in der Regel Social Engineering- und Phishing-E-Mails, um Mitarbeiter oder leitende Angestellte dazu zu verleiten, Anmeldeinformationen preiszugeben oder betrügerische Transaktionen durchzuführen.

Das Risiko für Rechtsstreitigkeiten steigt

Viele Datenverletzungen lösen heute regulatorische Maßnahmen aus, können aber auch Rechtsstreitigkeiten von betroffenen Verbrauchern, Geschäftspartnern und Investoren auslösen. In diesem Fall können Rechtskosten die Kosten erheblich erhöhen.

M&A können Cyberprobleme mit sich bringen

Cyber-Vorfälle haben sich nach einigen großen Datenverletzungen auch als heißes Thema bei Fusionen und Übernahmen (M&A) herausgestellt. Zum Beispiel wurde der Verstoß gegen Marriott im Jahr 2018 auf einen Eingriff im Jahr 2014 bei Starwood zurückgeführt, einer Hotelgruppe, die 2016 übernommen wurde. Selbst die am besten geschützten Unternehmen sind gefährdet, wenn sie ein Unternehmen mit schwacher Cybersicherheit oder bestehenden Schwachstellen erwerben. Das übernehmende Unternehmen kann für Schäden haftbar gemacht werden, die durch Vorfälle vor dem Zusammenschluss entstanden sind. Letztendlich muss die Berücksichtigung potenzieller Cyber-Schwachstellen und -Positionen für Unternehmen bei Fusionen und Übernahmen eine höhere Priorität erhalten, da viele Unternehmen in diesem Bereich nicht genügend Due Diligence-Prüfungen durchführen. Gleichzeitig beheben viele Unternehmen nach Abschluss eines Geschäfts keine Schwachstellen in erworbenen Systemen schnell genug.

Maßnahmen zur Risikominderung

Der beste Ansatz um Cyber-Risiken entgegenzutreten sind Investitionen in das Bewusstsein der Mitarbeiter sowie die Aktualisierung und kontinuierliche Überwachung von IT-Systemen. Vorbereitung und Schulung sind die effektivsten Formen der Schadensbegrenzung und können die Wahrscheinlichkeit oder die Folgen eines Cybereereignisses erheblich verringern. Viele Vorfälle sind das Ergebnis menschlicher Fehler, die durch Schulungen gemindert werden können. Auch die Aufrechterhaltung sicherer Backups und eine Betriebsfähigkeits- und Kontinuitätsplanung sind Schlüssel zur Reduzierung der Auswirkungen eines Cyber-Vorfalls. In jedem Fall sollten Reaktionspläne getestet, praktiziert und regelmäßig überprüft werden.

Hier steht das Riskobarometer 2020 zum Download bereit: *https://www.allianz.com/de/presse/news/studien/200115_Allianz-Risk-Barometer-2020.html*

Steigende Compliance-Anforderungen stressen Security-Professionals

Eine am 12. März 2020 veröffentlichte Thycotic-Studie zeigt: Hohe Arbeitsbelastung und das Fehlen klarer Karriereziele fördert Fachkräftemangel / Verantwortung für die unternehmensweite Cybersicherheit motiviert Security-Experten.

Steigende Compliance-Anforderungen und die wachsende Zahl an Regulierungen stellen den größten Stressfaktor für Security-Experten dar, wie eine aktuelle Befragung* des PAM-Spezialisten Thycotic nun offenbart. So stimmen 42 Prozent der befragten IT-Sicherheitsverantwortlichen zu, dass die Notwendigkeit, immer mehr Richtlinien erfüllen zu müssen, ihren Stress erhöht. Ein Drittel beklagt darüber hinaus lange Arbeitszeiten und die Unvermeidlichkeit von Überstunden. Weitere Stressfaktoren sind zudem die steigende Zahl an Sicherheitsvorfällen sowie zu kleine Security-Budgets.

Dies stellt die Unternehmen vor große Herausforderungen in Sachen Mitarbeiterbindung: Wie die Befragung von mehr als 500 Sicherheitsentscheidern weltweit zeigt, zählen zu den größten Hürden beim Halten von Mitarbeitern unter anderem Burnout aufgrund übermäßiger Arbeitsbelastung (45 %). Aber auch Faktoren wie das Fehlen klarer Karriereziele und mangelnde Aufstiegsmöglichkeiten (37 %) und mangelnde Unterstützung durch Führungskräfte bei der Schulung, Beurteilung und Entwicklung von Mitarbeitern (40 %) verstärken den Fachkräftemangel.

„Business-Bodyguard": Was Security-Experten motiviert

Gefragt nach der Motivation für ihren Job und den Gründen, die sie jeden Tag aufs Neue ins Büro gehen lassen, nannten mehr als Dreiviertel der Security-Experten ihre Bedeutung und Verantwortlichkeit für die Cybersicherheit ihres Unternehmens. So sehen sich 29 Prozent als „Business-Bodyguard", 25 Prozent als „Hüter der Ethik", der eine entscheidende Rolle beim Schutz der Datenintegrität sowie der Privatsphäre von Kunden und Mitarbeitern spielt, und 23 Prozent nennen sich selbst einen „Rätselmeister", der intellektuelle Herausforderungen im Kampf gegen Cyberangreifer löst. Nur drei Prozent gaben an, dass es ihnen schwerfällt, sich zu motivieren, morgens zur Arbeit zu gehen.

Der Hauptmotivator für den eigenen Job ist für ein Viertel der Befragten „Spaß an der Arbeit", 14 Prozent schätzen es, neue Dinge lernen zu können, und 13 Prozent motivieren sich vor allem mit der Bezahlung und dem damit verbundenen Luxus, sich Dinge kaufen zu können.

Security-Verantwortliche wünschen sich Wertschätzung ihrer Arbeit

„CISOs und Security-Professionals haben heutzutage einen der anspruchsvollsten und dynamischsten Jobs überhaupt und unsere Studie zeigt, dass sich der Großteil von ihnen wünscht, die Wertschätzung und Aufmerksamkeit von ihrem Unternehmen zu erfahren, die sie verdienen", so Joseph Carson, Chief Security Scientist und Advisory CISO bei Thycotic. „Ständig im Dienst zu sein, alle Unternehmens-Assets fortlaufenden schützen zu müssen, den Rest des Unternehmens zu schulen und gleichzeitig den Finger am Puls der Zeit zu halten in Sachen neueste Compliance-Mandate und Vorschriften, fordert jedoch seinen Tribut. So ist es nicht wirklich überraschend, dass Burnout und Stress bei Security-Verantwortlichen an der Tagesordnung sind. Dies fördert klar den Fachkräftemangel, da potenzielle neue Talente abgeschreckt werden und sich

stattdessen für eine ebenso interessante, aber weniger stressige Karriere in einem anderen Bereich entscheiden. Um den Druck auf Sicherheitsexperten zu verringern und neue Talente anzulocken, ist es unerlässlich, dass alle Mitarbeiter in einem Unternehmen Sicherheit als grundlegendes Fundament betrachten und den geschäftlichen Nutzen verstehen. Die Förderung einer Kultur, in der die Mitarbeiter keine Angst haben müssen, ein potenzielles Cyber-Sicherheitsproblem zu melden, ist ebenfalls enorm wichtig, denn je früher ein Problem gemeldet wird, desto geringer sind die Auswirkungen in Form von Stress und Kosten für das Unternehmen."

***Methodik:**
Im Auftrag von Thycotic befragte das unabhängigen Marktforschungsunternehmen Sapio Research im August 2019 insgesamt mehr als 500 IT-Sicherheitsentscheider aus Unternehmen mit jeweils mehr als 500 Mitarbeitern, wie sie Erfolge und ihren Einfluss auf den allgemeinen Geschäftserfolg messen. Die Stichprobe ist branchenübergreifend und enthält Unternehmen aus Deutschland (100), UK (102), USA (203), Australien (100) und Neuseeland (50). Die Interviews wurden online in einem strengen mehrstufigen Screening-Verfahren durchgeführt, um sicherzustellen, dass nur geeignete Kandidaten die Möglichkeit zur Teilnahme hatten.

Die vollständigen Report-Ergebnisse stehen hier zum Download bereit: *www.thycotic.com*

ISO 27701: Datenschutz-Zertifizierung für mehr Unternehmensresilienz

Der bekannte Sicherheitsstandard ISO/IEC 27001 für Informations-Sicherheits-Management-Systeme (ISMS) wurde jüngst mit dem neuen Standard ISO/IEC 27701 um Aspekte des Datenschutzmanagements erweitert. Diese Erweiterung unterstützt Unternehmen unter anderem beim Umgang mit personenbezogenen Daten und hilft beim Nachweis der Einhaltung von globalen Datenschutzbestimmungen. Die CARMAO GmbH (*www.carmao.de*), Spezialist für Unternehmensresilienz, stuft diese Norm als wichtige Entwicklung zur Förderung der organisationalen Resilienz ein.

Die neue Norm trägt die Bezeichnung „ISO/IEC 27701:2019-08 „Informationstechnik – Sicherheitsverfahren – Erweiterung zu ISO/IEC 27001 und ISO/IEC 27002 für das Datenschutzmanagement – Anforderungen und Leitfaden". Sie stellt demnach eine Erweiterung der ISO 27001 und ISO 27002 um Aspekte des Datenschutzes dar.

Die ISO 27701 definiert Anforderungen an ein Informationssicherheits-Management-System (ISMS) von Unternehmen sowie öffentlichen oder gemeinnützigen Organisationen. Das ISMS ist Kern der Zertifizierung und übernimmt die Aufgabe, im Unternehmen Prozesse und Richtlinien zu etablieren, mit denen Informationen verwaltet und geschützt werden. Die Informationssicherheit schließt mit der ISO 27701 auch personenbezogene Daten ein. Dem ISMS obliegt es, die Informationssicherheit unter Berücksichtigung des Datenschutzes zu regeln, aber auch zu kontrollieren und zu dokumentieren. Sicherheitsrisiken können so identifiziert, abgestellt oder reduziert werden.

Welche Vorteile sprechen für die Zertifizierung?
Mit dem Einsatz einer Zertifizierung können sensible Daten zuverlässig vor Verlust und Missbrauch geschützt sowie Haftungsrisiken minimiert werden. Denn mit einem zertifizierten ISMS können Sicherheitsrisiken schnell erkannt werden. Mit der ISO 27701 werden zusätzlich alle Prozesse optimiert, die insbesondere der Verarbeitung und dem Umgang mit personenbezogenen Daten dienen.

Zusätzlicher Effekt: Das Unternehmen fördert durch die Zertifizierung das Vertrauen und Image in Richtung der Kunden, Partner und Dienstleister. Ulrich Heun, Geschäftsführer der CARMAO GmbH, erklärt: „Manche geschäftlichen Beziehungen werden durch ein Zertifikat erst ermöglicht. Des Weiteren findet gleichzeitig eine Sensibilisierung der Mitarbeiter auf dem Feld der Informationssicherheit und des Datenschutzes statt. All diese Faktoren unterstützen die Unternehmensresilienz und machen eine Organisation robuster."

Unternehmensresilienz bzw. organisationale Resilienz stärkt die Fähigkeit eines Unternehmens oder einer Organisation, sich systematisch auf aktuelle und künftige negative Einflüsse vorzubereiten und so darauf einzustellen, dass Schäden vermieden werden und die Zukunftsfähigkeit aufrechterhalten wird. Diese Resilienz wird durch geschicktes Zusammenwirken diverser Managementsysteme erreicht.

Jenoptik:-Aufträge für mehr Verkehrssicherheit in Nordamerika

Der Photonik-Konzern Jenoptik teilte am 17. März 2020 mit, dass er in den USA und Kanada Aufträge für Verkehrssicherheitstechnik im Gesamtwert von über 21 Millionen US-Dollar erhalten hat. Damit wollen die Auftraggeber die „Vision Zero" unterstützen, ein multinationales Verkehrssicherheitsprojekt mit dem Ziel, die Anzahl von Verkehrsunfällen und -toten oder Schwerverletzten im Straßenverkehr zu reduzieren bzw. insbesondere auf Autobahnen und Highways auf Null zu senken.

„Jenoptik will dazu beitragen, die Sicherheit auf Straßen und in Kommunen zu verbessern. In Verbindung mit unseren anderen Produkten zur Verkehrsüberwachung sind unsere VECTOR-Kamera-Lösungen ein Schritt in diese Richtung", sagte Dr. Stefan Traeger, Vorstandsvorsitzender der Jenoptik.

Die Aufträge umfassen die Messtechnik vom Typ TraffiStar sowie die neueste Version der VECTOR-Kameraplattform. Darin integriert ist neben dem bewährten 3D-Tracking-Radar-Modul von Jenoptik eine leistungsfähige Software zur automatischen Kennzeichenerfassung (AKLS, in Englisch ANPR oder ALPR), die dank eines Deep-Learning-Algorithmus die Erkennungsgenauigkeit der Kennzeichenlesesysteme verbessert.

Die von Jenoptik entwickelte neue VECTOR-Kameraplattform ergänzt die klassischen Messgeräte für die Geschwindigkeitskontrolle und automatische Kennzeichenerfassung. Für Orte und Strecken, an denen die Geschwindigkeiten über kurze Entfernungen kontrolliert werden müssen, bietet VECTOR eine praktische und kosteneffiziente Lösung, die es ermöglicht, Unfallschwerpunkte zu entschärfen.

Edge Computing für das Internet of Things

IoT-Anwendungen stellen anspruchsvolle Anforderungen an die IT-Infrastruktur. Sie benötigen geringste Latenzzeiten bei gleichzeitig höchster Skalierbarkeit, Ausfallsicherheit und Verfügbarkeit. Das er-

klärt die Tatsache, dass sich Edge Computing zu einer besonderen und zunehmend wichtigen Disziplin innerhalb einer Netzwerk-Infrastruktur entwickelt hat.

Die verteilte, offene IT-Architektur von Edge Computing verarbeitet viele Daten in Echtzeit direkt vor Ort und reduziert somit drastisch den Bandbreitenbedarf und die Latenzzeiten, die zwangsläufig bei der Datenübertragung und der Datenverarbeitung in einem Rechenzentrum entstehen. Und das unabhängig davon, ob dafür ein Inhouse- oder ein Cloud-Datacenter genutzt wird.

Gleichzeitig führen das hohe und ständig wachsende Datenaufkommen und die Zunahme kritischer Anwendungen an den Endpunkten (Edge) dazu, dass die für ein Datacenter typischen Qualitätsmerkmale wie Skalierbarkeit, Ausfallsicherheit und Hochverfügbarkeit auch für Edge-Infrastrukturen unverzichtbar werden.

Für die Experten von Opengear, Anbieter von smarten Out-of-Band-Managementlösungen für den Schutz kritischer Infrastrukturen, zeichnet sich Edge Computing im IoT-Umfeld gegenüber Cloud- und Datacenter-zentrierten Ansätzen vor allem durch diese vier Vorteile aus:

- Geschwindigkeit: Je länger es braucht, bis Daten verarbeitet werden, desto weniger relevant werden sie. Einerseits reduziert Edge Computing das Gesamtaufkommen des Datenverkehrs und erhöht damit die Performance von Anwendungen und Services. Andererseits werden durch Edge Computing latenzsensible Anwendungen möglich, zum Beispiel Autonomes Fahren, die mit Datacenter-zentrierter Datenverarbeitung oder in Gebieten mit ungenügender Netzabdeckung gar nicht möglich wären.
- Sicherheit: Die Zahl von IoT-Geräten wächst ständig. Damit werden sie zunehmend zum Ziel für potenzielle Netzwerkangriffe. Aufgrund der zentralisierten Struktur ist Cloud Computing anfällig für DDoS-Attacken und Ausfälle. Edge Computing dagegen verteilt Anwendungen und Prozesse über verschiedene Devices, so dass es für Angreifer weitaus schwieriger und aufwändiger wird, das Netzwerk zu infiltrieren. Zudem kann Edge Computing sensitive Informationen filtern und gegebenenfalls nur unkritische Daten übertragen, um Security- und Compliance-Vorgaben zu erfüllen. Dadurch können weniger Daten abgefangen werden, was die Einhaltung von Sicherheitsstandards erleichtert.
- Kosten: Beim Edge Computing können die Daten am Ort ihres Entstehens gefiltert werden und müssen nicht an ein Datacenter geschickt werden. Unternehmen haben deshalb die Wahl, die für sie perfekte Mischung zwischen lokalen Services und Cloud-gestützten Anwendungen für eine kostengünstige IoT-Lösung zu nutzen. Die Datenverarbeitung und -speicherung in Edge-Devices reduziert den teuren Bandbreitenbedarf und optimiert damit die Gesamtkosten.
- Skalierbarkeit: Edge Computing erlaubt es Unternehmen, ihren Kapazitätsbedarf jederzeit und effizient durch eine Kombination von IoT-Devices und Edge-Datacentern zu erweitern. Die Nutzung von Edge-Devices optimiert die Skalierungskosten, weil mit jedem zusätzlichen Gerät ein weitaus geringerer Bandbreitenbedarf für das Netzwerk verbunden ist.

„Edge Computing ist für viele IoT-Szenarien unverzichtbar, denn mit der optimalen Nutzung der Daten kann genau der Mehrwert erzielt werden, durch den entscheidende Wettbewerbsvorteile entstehen", so Dirk Schuma, Opengear Sales Manager Europe. „Um so wichtiger ist es, bei der Implementierung die besten, smartesten Lösungen einzusetzen."

ULD: Datenschutzfragen zu Registrierungspflichten wegen des Corona-Virus

Die Landesbeauftragte für Datenschutz Schleswig-Holstein informiert

Marit Hansen, die Landesbeauftragte für Datenschutz Schleswig-Holstein, kommentiert dies: „Wir leben in einer besonderen Situation, in der das Infektionsrisiko zum Schutz von Menschen und Gesellschaft ein schnelles und zugleich umsichtiges Handeln erfordert. Die datenschutzrechtlichen Vorgaben stehen dem nicht entgegen. Selbstverständlich darf der Schutz personenbezogener Daten aber nicht auf der Strecke bleiben. Bei allen Maßnahmen muss bedacht werden, wie auch in dieser Sondersituation ein sorgsamer Umgang mit sensiblen Daten sichergestellt wird."

Hansen betont: „Viele Menschen sind besorgt, dass mit ihren Daten nicht gut umgegangen wird. Unsere Dienststelle ist weiterhin für Behörden, Unternehmen und Bürgerinnen und Bürger erreichbar, auch wenn wir den Publikumsverkehr einschränken mussten. Sie erreichen uns am besten per E-Mail oder Internet-Formular, wenn es telefonisch nicht klappen sollte. Dies ist auch wichtig, weil sich so viele neue Fragen stellen. Und wie immer gilt auch hier: Wenn ich Hinweise darauf erhalte, dass personenbezogene Daten nicht rechtmäßig verarbeitet oder sogar missbräuchlich genutzt werden, muss ich von Amts wegen einschreiten."

Generell steht das Datenschutzrecht – die Datenschutz-Grundverordnung in Verbindung mit dem Infektionsschutzgesetz – nicht dem entgegen, dass die zuständigen Behörden die notwendigen Schutzmaßnahmen zur Eindämmung von Infektionen auf Basis ihrer fachlichen Einschätzung anordnen. Maßgeblich ist – wie immer im Datenschutzrecht–, dass nur solche Daten erhoben und verarbeitet werden dürfen, die für den konkreten Zweck erforderlich sind. Die Zwecke und die konkrete Erforderlichkeit darzulegen, ist Aufgabe der zuständigen Gesundheitsämter und -behörden.

Grundsätzliche Überlegungen und Hinweise im Zusammenhang mit der Erhebung personenbezogener Daten im Gastronomiebereich (die aufgrund der Schließung dieser Einrichtungen zurzeit nicht mehr im Vordergrund steht) oder nun der Registrierungspflichten für Handwerker und Dienstleister, wie sie dieser Tage angeordnet werden, finden sich auf der Webseite des Unabhängigen Landeszentrums für Datenschutz (ULD).

Wichtig ist für Hansen nun zunächst, den Verpflichteten Hilfestellung zu geben, wie sich die neuen Datenverarbeitungspflichten datenschutzkonform umsetzen lassen: „Der sorgsame Umgang mit den personenbezogenen Daten der Kundinnen und Kunden ist – wie immer – ein Muss. So müssen die Daten vor unbefugten Zugriffen geschützt werden. Sie dürfen nur für die vorgesehenen Zwecke, nämlich den Infektionsschutz, durch die hierzu Berechtigten verwendet werden. Nach der erforderlichen Aufbewahrungsdauer – das kann z. B. ein Monat sein – müssen die Daten vernichtet oder gelöscht werden. Über die Datenverarbeitung und insbesondere über die Zwecke und die Dauer der Speicherung müssen die betroffenen Personen in verständlicher Form informiert werden."

Das ULD steht auch den Behörden, die diese Maßnahmen anordnen, auf Anfrage zur Verfügung, um die Anordnungen und die konkreten Umsetzungen datenschutzgerecht auszugestalten.

Die Informationen der Landesbeauftragten für Datenschutz in der Corona-Krise werden unter dem folgenden Link bereitgestellt und regelmäßig aktualisiert: *https://www.datenschutzzentrum.de/corona/*

Neue Partnerschaft: PrimeKey und achelos

PrimeKey Solutions AB und achelos GmbH gaben am 24. März 2020 ihre neue Partnerschaft bekannt. Gemeinsam bieten die beiden Unternehmen die optimale Mischung aus Produkten und Dienstleistungen an, um die Komplexität zu verringern, die mit der Entwicklung und Aufrechterhaltung eines eIDAS-konformen qualifizierten TSP-Dienstes verbunden ist.

achelos bietet umfangreiches Expertenwissen, Entwicklungsleistungen sowie Werkzeuge und Dienstleistungen für automatisierte Testverfahren zur Unterstützung von eIDAS-Implementierungen und Audit-Prozessen.

Die PKI-Produkte von PrimeKey, EJBCA Enterprise und die eIDAS-Edition, bieten Ausstellungs-, Registrierungs- und Validierungs-PKI-Dienste, die mit der eIDAS-Verordnung konform sind. PrimeKey verfügt über zahlreiche eIDAS-konforme und ETSI-Webtrust-geprüfte Kundeninstallationen. Aktuell arbeitet PrimeKey mit mehr als 30 eIDAS-qualifizierten Trust Service Providern ([Q]TSP) zusammen.

Für den Aufbau einer eIDAS-(Q)TSP-Lösung ist eine Reihe von Bausteinen erforderlich. Um eine solide und langlebige Lösung bereitzustellen, ist es absolut notwendig, dass alle Einzelkomponenten reibungslos und nahtlos zusammenarbeiten. „Mit dem Wissen von achelos über die PrimeKey-PKI-Produkte in Verbindung mit dem Fachwissen und der bewährten Erfahrung bei der Implementierung von eIDAS-geprüften Lösungen werden wir in der Lage sein, weiterhin kostenoptimierte Projekte und Lösungen auf sehr effiziente Weise zu liefern. Mit dieser neuen Partnerschaft sind wir für die Weiterentwicklung des eIDAS-Bedarfs und zusätzliche Kunden gut aufgestellt", erklärt Evangelos Popis, PrimeKey Sales and Partner Manager, DACH.

„Wir glauben, dass eIDAS die Transparenz, Interoperabilität und Innovation in der gesamten Europäischen Union vorantreibt. PrimeKey bietet mit seiner Public Key Infrastructure und den Lösungen für elektronische Signaturen die optimale Plattform für die Implementierung eIDAS-konformer Lösungen. achelos ergänzt dieses Portfolio um eine umfassende Expertise für Entwicklung, Test und Zertifizierung für die europäische eIDAS-Verordnung", sagt Kathrin Asmuth, Managing Partner bei achelos. „Kunden profitieren von einer schnelleren Markteinführung bei der Implementierung und durch das Testsystem eIDAS Inspector von einer hohen Qualitätssicherung", ergänzt Michael Jahnich, Partner Manager bei achelos.

PrimeKey, (*www.primekey.com*) eines der weltweit führenden Unternehmen für PKI- und Signaturlösungen, und achelos (*https://www.achelos.de/de/*) als ein führendes Unternehmen, das hoch spezialisierte Produkte, Lösungen und Dienstleistungen für sicherheitskritische Anwendungen in internationalen Märkten entwickelt und betreibt, sind entschlossen, die Einführung digitaler Signaturen und der eIDAS-Verordnung in ganz Europa weiter voranzutreiben.

Claroty: Bedrohungen durch Cyberangriffe auf kritische Infrastrukturen

74 Prozent der IT-Sicherheitsexperten weltweit halten Angriffe auf kritische Infrastrukturen für bedrohlicher als Brüche der Datensicherheit. Dies ergab eine vom OT-Security-Spezialisten Claroty initiierte und am 25. März 2020 veröffentliche Studie über den globalen Stand der industriellen Cybersicherheit, für die insgesamt 1.000 IT-Sicherheitsexperten aus den Vereinigten Staaten, Großbritannien, Deutschland, Frankreich und Australien befragt wurden.

Mit Blick auf das Gesamtbild der industriellen Cybersicherheit sind 62 Prozent der weltweit Befragten der Meinung, dass Industrienetzwerke angemessen gegen Cyber-Angriffe geschützt sind. 60 Prozent glauben zudem, dass die kritische Infrastruktur ihres Landes angemessen geschützt ist. Gleichwohl gibt es hier starke regionale Unterschiede: So sind die Experten in Australien (93 %) und Deutschland (96 %) wesentlich zuversichtlicher in Bezug auf die Sicherheit von Industrienetzwerken als ihre Kollegen in Großbritannien, den USA und Frankreich. Das Gleiche gilt auch für den Schutz der kritischen Infrastruktur ihres Landes: 90 Prozent der Befragten aus Australien und 99 Prozent aus Deutschland gaben an, dass diese angemessen gesichert sei.

In Bezug auf besonders bedrohte Branchen ergab die Untersuchung, dass weltweit 45 Prozent der IT-Sicherheitsexperten die Energieversorgung als den am stärksten gefährdeten Sektor kritischer Infrastrukturen ansehen, gefolgt von Öl und Gas (21 %). Der Studie zufolge geht dabei die größte Gefahr für industrielle Netzwerke von Hacking aus (43 %), gefolgt von Ransomware-Angriffen (33 %). Große Einigkeit weltweit besteht in der Frage, wer für den Schutz kritischer Infrastrukturen die Verantwortung trägt: Alle Befragten aus Deutschland halten hierfür den Staat zuständig, gefolgt von Australien (98 Prozent), Großbritannien (91 %), Frankreich (89 %) und den USA (87 %).

„Die Konvergenz von IT und OT bringt Unternehmen zahlreiche Vorteile wie höhere Effizienz, Leistung und Servicequalität, birgt aber auch Risiken: gezielte und nicht-gezielte Bedrohungen können sich nun von IT- zu OT-Umgebungen ausbreiten – und umgekehrt", sagt Dave Weinstein, Chief Security Officer von Claroty. „Unsere Aufgabe ist es, die Sicherheitsverantwortlichen dabei zu unterstützen, die Lücke zwischen der IT- und der OT-Cybersicherheit zu schließen und sicherzustellen, dass alle Bereiche vor Cyberangriffen geschützt sind. Vor allem entfernte Mitarbeiter und Anlagen stellen CISOs vor große Herausforderungen, da sie dadurch die Sicherheit der Produktionsumgebungen aus der Ferne sicherstellen müssen."

Der komplette Report mit weiteren Ergebnissen und Analysen kann hier heruntergeladen werden: *https://www.claroty.com/*

SySS GmbH: Penetrationstest, der Homeoffice-Lösungen auf Sicherheitslücken prüft

Aufgrund der aktuellen Corona-Krise müssen viele Unternehmen, Institutionen und Organisationen nahezu sämtliche Mitarbeiterinnen und Mitarbeiter ins Homeoffice schicken. Dass diese Maßnahme so schnell wie möglich umgesetzt werden muss, macht Fehler bei der Einrichtung wahrscheinlich. Um bestmöglich bei der Umstellung zu unterstützen, hat die SySS GmbH einen neuen Test entwickelt und am 25. März 2020 veröffentlicht: den Penetrationstest „HOMEOFFICE". Diese Testvariante hilft das Sicherheitsniveau von Homeoffice-Lösungen zu ermitteln sowie Schwachstellen zu finden und diese zu beheben.

Detaillierte Informationen zum Ablauf des „HOMEOFFICE"-Tests finden Sie hier. *https://www.syss.de/leistungen/penetrationstest/*

SOPHOS: Backup als Schutz vor Ransomware – wenn das Backup geschützt ist

In Zeiten von Ransomware und anderen Gefahren verlassen sich viele Unternehmen auf ihre Backups. Denn wenn die Daten einfach, schnell und vollständig wiederhergestellt werden können, laufen die Datenzerstörungsversuche oder Lösegeldforderungen von Cyberkriminellen ins Leere. Doch Malware wie Emotet hat es neben anderen Daten-Ressourcen eben auch genau auf die Backups abgesehen. Hat es die Malware einmal geschafft, auch die Backups zu zerstören oder derart durcheinander zu bringen, dass kein Administrator mehr den aktuellsten Stand der jeweiligen Backups feststellen kann, tauchen Probleme auf.

Deshalb sollte man beachten, dass Datensicherung und Datensicherheit unmittelbar miteinander zusammenhängen. Eine gute Malware-Prävention mit synchronisiertem und unternehmensüberspannendem intelligenten Schutz hilft, nicht nur das Netzwerk, die Server und die Endpoints zu schützen, sondern auch die Backups, die im Netz, beispielsweise als Share sichtbar sind. Sophos gab am 26. März 2020 fünf wichtige Tipps, um die Backup-Daten vor Cyberkriminellen zu schützen:

- Eine unternehmensweite und intelligent vernetzte Security kann mit Hilfe von Next Generation Löungen und dem Einsatz von Künstlicher Intelligenz auch Backups vor bösartigen Zugriff schützen.
- Backups sollten zusätzlich offline (z.B. in der Cloud oder auf Tapes) und read-only gespeichert werden.
- Es häufen sich die Security-Probleme in der Public Cloud, in der oftmals auch Backups ausgelagert werden. Mit geeigneten Tools können Sicherheitslücken, meist hervorgerufen durch eine fehlerhafte Konfiguration, indentifiziert und damit beseitigt werden.
- Es sollten spezielle Administratoren für die Backup-Systeme festgelegt werden. Es dürfen nicht dieselben Personrn sein, die auf anderen Systemen lokaler oder Domain-Admin sind, um die Zugriffsrechte maximal vom Rest des Netwerks zu entkoppeln.
- Die Multi-Faktor-Authentifizierung sollte für alle Administratoren eingerichtet sein. Diese kann eine wirksame Barriere gegen den Zugriff von Unbefugten darstellen.

Rezensionen

Bücher

Dr. Michael Wächter

Rüpke, Giselher; v. Lewinski, Kai; Eckhardt, Jens: Datenschutzrecht: Grundlagen und europarechtliche Neugestaltung, Verlag C.H.BECK München 2018, 422 Seiten, ISBN 978-3-406-50199-9, 39,80 €

Datenschutzrecht wird für den juristischen Arbeitsmarkt von immer größerer Bedeutung. Ursache hierfür ist, dass in einer digitalen Gesellschaft und Wirtschaft immer mehr Sachverhalte erhoben, erfasst und damit transparent gemacht werden, die in einer analogen Welt nicht transparent waren. Und hier ist dann rechtlich zu beantworten, was zulässig ist und was zu unterlassen ist. Hier setzt das Werk an und führt Studenten an diese Thematik heran. Es unterstützt dabei eine junge Generation von Juristen, Phänomene, die sie als Digital Natives aus ihrer eigenen Lebenswelt kennen, auch rechtlich bewerten zu können.

Diesen Bereich der rechtlichen Fundierung personenbezogener Datenverarbeitung beschreitet das Werk eingehend und geht das Thema auf breiter Basis an. So werden im Werk zunächst die historisch-sozialwissenschaftlichen Bezüge des Datenschutzrechts aufgezeigt. Danach werden zentrale verfassungsrechtliche und europarechtliche Kerninformationen zum Datenschutzrecht vermittelt. In einem dritten Block werden die DSGVO und weitere zentrale Rechtsgrundlagen zur Verarbeitung von Informationen erläutert. Es folgen Ausführungen zum administrativen und technischen Datenschutz sowie zu Gesichtspunkten der Datenschutzkontrolle und der Haftung. Das Werk schließt mit Ausführungen zum Datenschutz in der Telekommunikation.

Das alles wird sehr kompetent umgesetzt. Der Leser muss sich allerings darauf einlassen, dass das Werk von drei Autoren verfasst ist, die im Rahmen ihrer Bearbeitungsteile ihre eigene methodische Herangehensweise auf das Datenschutzrecht einbringen. Das ist aus Sicht des Rezensenten sehr bereichernd. Denn so findet man im wieder Highlights einer sehr interessanten Sichtweise auf das Thema. Ein paar Highlights der Ausführungen zu den verfassungsrechtlichen Grundlagen des Datenschutzrechts sollen genannt werden: 1. Die Ausführungen zum Sozialcharakter der Information (S. 45 f.), 2. Die Erläuterungen zum Zugriff auf informationstechnische Systeme (S. 58 ff.), und 3. Die Ausführungen zu systematischen Datenerhebungen und den hierbei berechtigten Erwartungen auf Vertraulichkeit (S. 93 ff.). Dort werden den Studenten Argumente für weitere Überlegungen an die Hand gegeben, die sie in klassischen Gesetzeskommentaren in dieser Form in der Regel nicht finden werden.

Als Fazit lässt sich festhalten, dass die Autoren ein Werk geschaffen haben, welches sicherlich keinen einfachen Einstieg für Studenten in das Rechtgebiet Datenschutz anbietet. Das macht aber die Qualität des Werks aus. Denn es regt zum Weiterdenken und auch zum Widerspruch an. Und es bietet den Studenten ein Wissen an, welches sie befähigt, die Probleme des Datenschutzes zu erkennen, um dann die rechtlichen Fragestellungen besser beantworten zu können. Der Rezensent wünscht dem Werk deshalb viele weitere Auflagen und einen großen Leserkreis.

Ludwig Gramlich

Kolany-Raiser, Barbara; Heil, Reinhard; Orwat, Carsten; Hoeren, Thomas (Hrsg.): Big Data. Gesellschaftliche Herausforderungen und rechtliche Lösungen. Information und Recht Bd. 86. München, C.H. Beck 2019, XXI, 523 S. ISBN 978-3-406-74349-8, 49.- €

Der Band „versammelt die Ergebnisse des vom BMBF geförderten Projekts ‚Assessing Big Data' (ABIDA)" (Vorwort, S. VII). Big Data fungiere „gleichsam als Chiffre, die nach immer neuen Interpretationen verlangt" und „neue Fragestellungen erzeugt", für die „allum-