westermann

Sascha Dinse

Arbeitswelt 4.0

Informations- und Datensicherheit

1. Auflage

Bestellnummer 221349

Die in diesem Werk aufgeführten Internetadressen sind auf dem Stand zum Zeitpunkt der Drucklegung. Die ständige Aktualität der Adressen kann vonseiten des Verlages nicht gewährleistet werden. Darüber hinaus übernimmt der Verlag keine Verantwortung für die Inhalte dieser Seiten.

service@westermann.de
www.westermann.de

Bildungshaus Schulbuchverlage Westermann Schroedel Diesterweg Schöningh Winklers GmbH, Postfach 33 20, 38023 Braunschweig

ISBN 978-3-14-**221349**-1

westermann GRUPPE

Vorwort

Nicht erst seit den hohen Wellen, die die „Datenschutzgrundverordnung“ (DSGVO) geschlagen hat, ist Datenschutz in aller Munde. Was im privaten Bereich bei der Nutzung sozialer Netzwerke oft als übertriebene Bedenken beiseite geschoben wird, kann im wirtschaftlichen Bereich schnell zu einem kostspieligen Problem werden. Unternehmen müssen nicht nur genau wissen, welche Arten personenbezogener Daten sie erfassen und verarbeiten dürfen, sie müssen auch Vorkehrungen im Bereich der „Datensicherheit“ treffen, um diese Daten vor unauthorisiertem Zugriff, Diebstahl oder versehentlicher Löschung zu schützen. Im Zeitalter digitaler Medien, von Breitband-Internet und mobilen Geräten, kommt besonders der Datensicherheit eine immense Bedeutung für den Geschäftserfolg zu.

Viele Industriezweige klagen zwar darüber, dass die DSGVO Anpassungen an Geschäftsmodellen in großem Maßstab erfordern würde, blenden dabei aber aus, dass sehr vieles, was die neue Datenschutzgrundverordnung fordert, schon seit etlichen Jahren geltendes Recht ist. Grund genug also, sich dem Themenkomplex Datenschutz und Datensicherheit einmal aus einer praxisbezogenen Perspektive zu nähern. Dabei werden aktuelle Themen zur Illustration herangezogen, anhand von realen Vorfällen wird die Tragweite von Problemen verdeutlicht, gleichzeitig werden relevante Teile der geltenden Verordnungen und Gesetze erläutert.

Im zweiten Teil des Buches wird das Augenmerk auf die Einhaltung der IT-Schutzziele gelegt. Neue Technologien bieten nicht nur eine Reihe großartiger Vorteile, sondern eröffnen an anderer Stelle vielleicht auch neuartige Angriffsszenarien, auf die Unternehmen vorbereitet sein müssen. Seien es Denial-of-Service-Attacken oder Phishing, sei es unzureichende Verschlüsselung von Daten, heute kann es schnell gehen, dass aus einem vermeintlich kleinen Problem ein existenzbedrohendes wird. Daher versucht das vorliegende Buch, auf der einen Seite Bewusstsein für die Wichtigkeit von Datenschutz zu schaffen und gibt auf der anderen Seite konkrete Tipps für bessere Datensicherheit im Unternehmen.

Sascha Dinse, Berlin 2018

Kapitel I

1. Bedeutung von Datenschutz und Datensicherheit

Kapitel II

2. Datenschutz im Unternehmen

Kapitel III

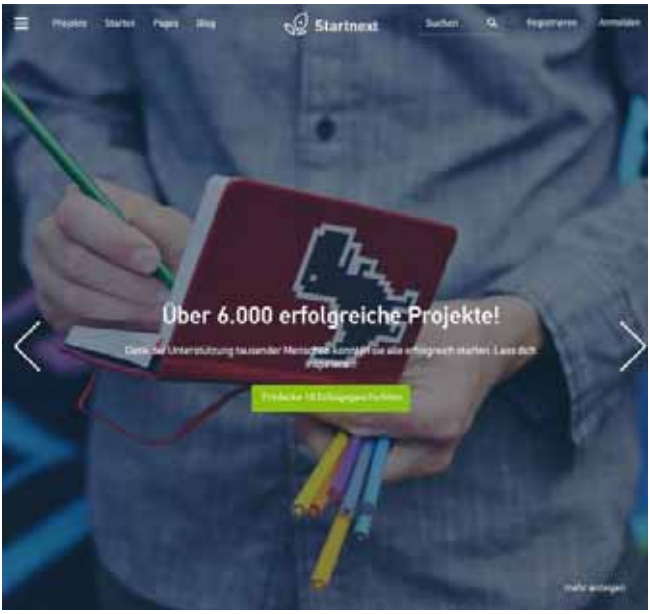
3. Datensicherheit

1. Bedeutung von Datenschutz und Datensicherheit

Datenschutz ist ein Thema, das nicht nur omnipräsent in den Medien auftaucht, es ist auch ein Bereich, der buchstäblich alle Menschen betrifft. Über jeden Deutschen, und natürlich lässt sich dies auf andere Länder ebenso übertragen, sind bei Unternehmen, Behörden oder anderen öffentlichen und nicht-öffentlichen Stellen Informationen gespeichert. Zumeist werden diese Daten benötigt, um beispielsweise Geschäftsbeziehungen zu begründen, Abrechnungen zu erstellen, Beschäftigungsverhältnisse zu verwalten oder behördliche Prozesse zu ermöglichen.

»Personenbezogene Daten«, denn diese sind es, um die es sich beim Themenkomplex Datenschutz dreht, stehen dabei besonders im Fokus. Im Interesse der Betroffenen, also der Bürgerinnen und Bürger, von denen diese Daten erhoben werden, hat der Gesetzgeber Regelungen erlassen, die den Umgang mit diesen Informationen kontrollieren sollen. Gleichzeitig ist es in der heutigen Zeit für den technischen und rechtlichen Laien beinahe unmöglich geworden, auch nur ansatzweise verstehen zu können, welche Auswirkungen das Nutzen moderner Geräte oder digitaler Netzwerke im Internet haben, inwieweit Unternehmen oder Behörden Daten erheben, verarbeiten oder nutzen.

Beispiel gefällig? Auf dem Crowdfundingportal »Startnext« lief Anfang 2018 (Start der Kampagne war der 14.02.2018, Laufzeit bis 15.03.2018) ein Aufruf, sich mit Spenden an einer Aktion namens »Open Schufa« zu beteiligen. Worum geht es dabei? Die »Open Knowledge Foundation Deutschland«, ein gemeinnütziger Verein und »Algorithm Watch«, eine nicht-kommerzielle Organisation, die Automatisierungsprozesse untersucht, haben sich das Ziel gesetzt, den bislang geheimen Algorithmus der Schufa zu verstehen.



Startseite von startnext.com
Quelle: Startnext Crowdfunding GmbH

Die Schufa Holding AG (Schutzgemeinschaft für allgemeine Kreditsicherung) wertet als privatwirtschaftliches Unternehmen enorme Mengen personenbezogener Daten von de facto jedem deutschen Bürger aus. Ob Kreditaufnahme bei einer Bank, Abschluss eines Mobilfunkvertrages oder Bewerbung um einen Mietvertrag für eine Wohnung, in den meisten Fällen geht der Bewilligung oder Ablehnung eine Anfrage bei der Schufa voraus. Der »Schufa-Score« bewertet jeden Bürger hinsichtlich seiner Kreditwürdigkeit und liegt zwischen 0 und 100. Der Maximalwert von 100 kann dabei nicht erreicht werden, er ist rein fiktiv. Je höher jedoch der Schufa-Score, als desto kreditwürdiger und damit vertrauenswürdiger wird der betroffene Bürger eingestuft.

Warum ist die Datenerhebung, -speicherung und -verarbeitung der Schufa möglicherweise problematisch?

Grundlegend ist gegen die Idee einer Bonitätsprüfung kaum etwas einzuwenden. Immerhin möchten Unternehmen, Banken oder Vermieter wissen, auf wen sie sich einlassen, bevor sie mit einem Kunden oder Mieter ein Geschäft abschließen. Und auch für die Verbraucher ist eine solche Prüfung nicht von vornherein negativ, denn letztlich soll sie eine objektive Bewertung darstellen. Soll, wohlgemerkt. Denn, und das ist der Kritikpunkt an der Arbeit der Schufa, auf den sich das »Open Schufa«-Projekt bezieht, die Schufa musste bislang nicht offenlegen, nach welchem Algorithmus das Scoring errechnet wird.

Genau hier liegt das Problem. Datenschutzaktivisten werfen der Schufa vor, die personenbezogenen Daten der Betroffenen zum Teil in unfairer Weise gegen diese einzusetzen. So gibt es Vermutungen, dass neben nicht überprüfbaren Berechnungsfehlern oder falschen, veralteten Daten, die zu fehlerhaften Ergebnissen führen könnten, auch diskriminierende Faktoren verwendet werden. Da die Schufa ihren Algorithmus bisher als Geschäftsgeheimnis schützen konnte, kann niemand der fast 70 Millionen Betroffenen in Deutschland sicher sein, auf welche Art und Weise das persönliche Scoring errechnet wird. Wäre dieser Scoringwert nur eine rein fiktive Zahl für irgendeine Statistik, wäre das vielleicht nicht weiter schlimm. Der Schufa-Score hat aber im Gegenteil sehr konkrete Auswirkungen auf das Leben aller Betroffenen. Ob ein Kredit bewilligt wird oder nicht, ob eine Wohnung gemietet werden kann oder nicht, sind sehr wichtige Entscheidungen. Die Schufa ist nur ein Beispiel unter vielen dafür, welche Bedeutung personenbezogene Daten für Menschen haben können.

Zweites wichtiges Thema neben dem Datenschutz ist der immer wichtiger werdende Bereich der »Datensicherheit«. Geht es beim Datenschutz um den Umgang mit personenbezogenen Daten, so umschließt der Begriff Datensicherheit den gesamten technischen Bereich. Hierbei ist die Einhaltung der IT-Schutzziele oberstes Gebot, mehr dazu später. Datendiebstähle durch Hackerangriffe, von Kryptotrojanern lahmgelegte Systeme, unsichere »smarte« Geräte, Social Engineering, unabsichtliche Löschung von Daten durch technische Probleme, all das und mehr zählt zum Bereich Datensicherheit. Doch Datensicherheit beginnt nicht erst im digitalen Bereich, sondern bereits bei der Gestaltung von Räumlichkeiten und Prozessen.

Im Folgenden werden die Grundsätze von Datenschutz und Datensicherheit dargelegt und anhand von Praxisbeispielen erklärt.

1.1 Definitionen

Um Verwechslungen und Unklarheiten bei Begrifflichkeiten zu vermeiden, folgen an dieser Stelle einige Definitionen und Erklärungen zu wiederkehrenden Fachbegriffen.

Datenschutz

Der Begriff »Datenschutz« bezieht sich auf den Umgang mit personenbezogenen Daten, das schließt die Bereiche der Erhebung, Verarbeitung und Nutzung mit ein. Hierzu zählt beispielsweise, ob die Erhebung von Daten überhaupt erlaubt ist, ob eine rechtswirksame und nachweisbare Einwilligung des Betroffenen vorliegt, ob eine Aufklärung über die Zweckbestimmung der Datenerhebung,

-verarbeitung und -nutzung stattgefunden hat, oder ob der Betroffene weiß, wer Einblick in die erhobenen Daten bekommt.

Beispiel: Der Fall Schrems

Facebook, Google und die meisten anderen Online-Dienste erfassen enorme Mengen personenbezogener Daten von ihren Nutzern. Sehr häufig verstoßen die Dienste dabei gegen gesetzliche Grundlagen, die in Europa und Deutschland gelten, was nicht selten zu Protesten aufseiten von Datenschützern führt. So legen Facebook und Google beispielsweise weder in keiner Weise offen, welche konkreten personenbezogenen Daten ihre Dienste erheben und wie genau das geschieht, noch gewähren sie ihren Nutzerinnen und Nutzern einen Blick darauf, wie diese Daten verwendet, ausgewertet oder weitergereicht werden. Dass Facebooks Vorstellung vom »Löschen« eine vollkommen Andere ist als die der meisten Nutzer, ist nicht erst seit der Klage von Maximilian Schrems gegen Facebook[1] klar. Aufgrund seiner Klage gegen die (Nicht-)Löschpraxis von Facebook wurde vor einigen Jahren das bis dato geltende Datenschutzabkommen »Safe Harbor« zwischen der EU und den USA aufgekündigt und musste durch ein neues ersetzt werden.

Das »Safe-Harbor«-Abkommen stellte die rechtliche Grundlage für den Datenaustausch zwischen der EU und den USA dar, auf dessen Grundlage europäische Unternehmen Dienste wie Facebook, Google oder Amazon nutzten. Als durch die Klage von Maximilian Schrems der Öffentlichkeit bekannt wurde, dass Facebook personenbezogene Daten von Nutzern, die diese gelöscht haben, entgegen der eigenen AGB nicht von den Facebook-Servern löscht, sondern langfristig gespeichert hält, löste dies eine Prüfung der Rechtsgrundlage des »Safe-Harbor«-Abkommens aus. Der Europäische Gerichtshof kam danach zu dem Schluss, dass die im »Safe-Harbor«-Abkommen beschlossenen Regelungen nicht ausreichend seien, um die Daten europäischer Nutzer genügend vor dem Zugriff US-amerikanischer Behörden zu schützen.

Da ohne ein geltendes Abkommen jedoch kein Datenaustausch und damit keine Nutzung der US-Dienste möglich wäre, wurde »Safe Harbor« direkt durch das »EU-US Privacy Shield«-Abkommen ersetzt. Dieses wird von Datenschützern ebenso kritisiert, da nach deren Auffassung noch immer primär wirtschaftliche Interessen geschützt werden anstelle der Daten der betroffenen Personen.

1 *https://netzpolitik.org/2013/max-schrems-im-interview-von-den-netzaktivisten-sehe-ich-zu-wenig-wind/*

SPIEGEL ONLINE SPIEGEL

Menü | Politik Meinung Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft mehr

NETZWELT

Schlagzeilen | Wetter | DAX 12.177,64 | TV-Programm | Abo

Safe Harbor

EuGH erklärt Datenabkommen mit USA für ungültig

Der Europäische Gerichtshof hat ein wichtiges Datenschutzabkommen zwischen Europa und den USA für ungültig erklärt. In dem Urteil geht es auch um die Praktiken von US-Geheimdiensten - die das Gericht erstaunlich deutlich kritisiert.

Europäischer Gerichtshof in Luxemburg: Safe Harbor ist ungültig

Teilen Twittern E-Mail

Dienstag, 06.10.2015 11:55 Uhr Drucken Nutzungsrechte Feedback Kommentieren

Der Gerichtshof der Europäischen Union (EuGH) hat die Regelung zum Austausch von Daten zwischen den USA und der EU für ungültig erklärt. Die EU-Kommission hätte demnach die Befugnisse der nationalen Datenschutzbehörden durch einen Beschluss nicht wie geschehen beschränken dürfen. Die persönlichen Daten europäischer Internetnutzer seien in den USA nicht ausreichend vor dem Zugriff der Behörden geschützt.

In 2015 wurde das bis zu diesem Zeitpunkt bestehende Datenschutzabkommen zwischen den USA und der EU für ungültig erklärt. Quelle: Spiegel-Online

Datensicherheit

Der Bereich »Datensicherheit« bezieht sich auf technische Vorkehrungen, die zur Sicherung von Datenbeständen eingesetzt werden. Hierzu zählen grundlegende Dinge wie abgeschlossene Büros, einheitliche Prozesse oder technische Maßnahmen wie Verschlüsselung von Daten ebenso wie der Schutz der eigenen Datenbestände vor externen Angriffen oder Datenverlust. Im Folgenden wird der Begriff »Datensicherheit« in Bezug auf personenbezogene Daten verwendet. Von ihm abgegrenzt ist die »IT-Sicherheit«, die sich darüber hinaus mit dem Schutz der gesamten technischen Infrastruktur beschäftigt; das Feld der IT-Sicherheit reicht also deutlich über den Bereich der personenbezogenen Daten hinaus.

IT-Sicherheit

Weitgreifender als der Begriff der »Datensicherheit«, so wie er in diesem Buch verwendet wird, fasst die »IT-Sicherheit« alle Bereiche der elektronischen Datenverarbeitung zusammen, die in irgendeiner Weise von potentiellen Risiken betroffen sein könnten. Ein IT-Sicherheitskonzept soll die »Schutzziele« der Informationssicherheit gewährleisten.

Vertraulichkeit

Daten dürfen nur von den dazu berechtigten Personen eingesehen werden. Um dies zu gewährleisten werden Techniken wie Verschlüsselung eingesetzt. Diese sorgen dafür, dass nur autorisierte Empfänger Zugriff auf Daten haben. Besonders bei der Übertragung von Daten sind wirksame Verschlüsselungen und Versiegelungen nötig, um sowohl den Inhalt vor Fremdzugriff zu schützen als auch eine Verschleierung des Absenders unmöglich zu machen.

Beispiel: Unternehmen sollten bei der Übermittlung personenbezogener Daten über digitale Kanäle wann immer möglich eine wirksame »Ende-zu-Ende«-Verschlüsselung einsetzen. Dabei wird sichergestellt, dass die vom Absender verschickten Informationen nur vom berechtigten Empfänger gelesen werden können. Dies dient nicht nur dem Schutz personenbezogener Daten, sondern ist auch für die Wahrung von Geschäftsgeheimnissen nötig. Eine stark verschlüsselte Nachricht kann, selbst wenn sie unterwegs abgefangen wird, nur mit dem privaten (geheimen) Schlüssel des Empfängers decodiert werden. Ist der Abfangende nicht im Besitz dieses Schlüssels, erhält er nur einen wertlosen Klumpen verschlüsselter Daten. Viele Messenger, darunter WhatsApp (seit Ende 2015), Threema oder Signal benutzen eine derartige asymmetrische Ende-zu-Ende-Verschlüsselung (mit je einem Schlüsselpaar pro Nutzer), um die Vertraulichkeit der Nachrichteninhalte sicherzustellen.

Integrität

Datenintegrität bedeutet, dass Daten vor Manipulation oder Beschädigung geschützt werden. Beschädigungen können durch technische Defekte, Programmierfehler oder Materialabnutzung (bei Speichermedien wie CDs, mechanischen Festplatten) auftreten. Manipulationen durch beabsichtigte oder unbeabsichtigte Eingriffe in die Datenstruktur (z. B. Hackerangriff oder Bedienfehler) müssen soweit wie möglich ausgeschlossen sein.

Beispiel: Ein Telekommunikationsanbieter nutzt eine Kundendatenbank, um dort sämtliche Informationen zu Bestandskunden, Verträgen und Abrechnungen zu hinterlegen. Sollte diese Datenbank nicht ausreichend gegen Zugriffe von außen geschützt sein, könnten Hacker nicht nur die Daten der Kunden auslesen, sie könnten eventuell auch Abrechnungen oder Vertragsdetails ändern. Auf diese

Weise ließe sich enormer Schaden anrichten, wenn Angreifer beispielsweise die gesamten Abrechnungsdaten löschten und es vonseiten des Telekommunikationsanbieters kein Backup gäbe.

Verfügbarkeit

Die Gewährleistung der Verfügbarkeit von Daten ist besonders für Unternehmen relevant, die auf komplett digitale Geschäftsmodelle setzen. Eine Direktbank beispielsweise, deren Service ausschließlich online angeboten wird, kann es sich kaum leisten, dass die eigenen Server längere Zeit offline sind. Daher müssen derart wichtige Systeme besonders geschützt werden. Angriffsszenarien wie der DoS (Denial of Service), bei dem Server mit einer Masse von Anfragen überflutet werden, oder die Variante des »Distributed Denial of Service«-Angriffs, bei dem die Anfragen aus einem ganzen Netz verschiedener Rechner auf die Server einprasseln, können kritische Infrastruktur für Stunden lahmlegen.

Beispiel: Systeme wie die Flugsicherung, die der koordinierten Abwicklung komplexer Prozesse wie eben der Nutzung des Luftraums dienen, müssen gegen Angriffe besonders effektiv geschützt sein. Fiele eine derartige Koordinationsstruktur nur für wenigen Minuten flächendeckend aus, könnte dies bereits verheerende Folgen haben.

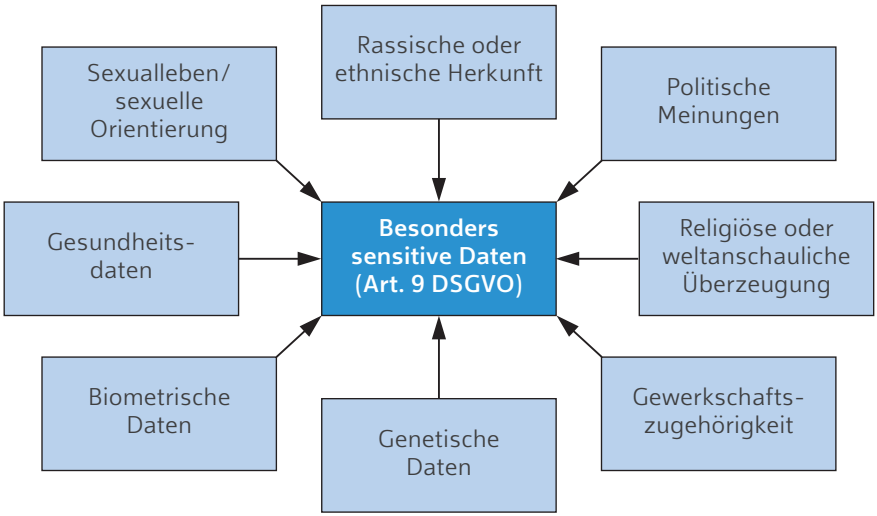
Authentizität

Die »Echtheit« einer Information, einer Nachricht oder einer Absenderadresse ist ein wesentliches Kriterium der IT-Sicherheit. Um nachvollziehen zu können, dass eine bestimmte Nachricht auch wirklich vom angeblichen Absender stammt, können digitale Signaturen verwendet werden, während die Nachrichteninhalte selbst z. B. durch asymmetrische Verschlüsselung geschützt werden können.

Personenbezogene Daten

Als »personenbezogen« gelten diejenigen Datenkategorien, die einen Rückschluss auf konkrete Personen erlauben. Hierunter fallen Informationen wie Name, Geburtstag, Geburtsort, Telefonnummer, E-Mailadresse, dynamische IP-Adresse, Blutgruppe, Haarfarbe und viele weitere. Auch wenn es auf den ersten Blick so scheint, als wären einige dieser Kategorien harmlos, so lassen auch diese sich verwenden, um Rückschlüsse auf Personen zu ziehen.

Personenbezogene Daten werden von der geltenden Gesetzgebung besonders geschützt, da eine missbräuchliche Nutzung in den allermeisten Fällen für den Betroffenen negative Konsequenzen hat. Kategorien wie die ethnische Herkunft, die politische oder sexuelle Orientierung, religiöse Überzeugungen sowie einige andere sind darüber hinaus als »besonders sensitive Daten« noch strenger geschützt.



Beispiel: Sie bewerben sich bei einem Unternehmen. Guten Mutes gehen Sie ins Vorstellungsgespräch, sind gut gelaunt und motiviert. Während des Gesprächs zückt der Personalchef eine Akte und blättert darin herum. Dann beginnt er, aus Ihrer Krankenakte vorzulesen, dass in Ihrer Familie die Wahrscheinlichkeit für ein genetisch bedingtes Rückenleiden deutlich höher ist, als bei den meisten anderen Menschen. Leider kann er Sie aus diesem Grunde nicht einstellen. Das ist es, was oben mit »negativen Konsequenzen« gemeint ist. Fallen personenbezogene oder, wie im Beispiel, gesundheitliche Daten in die Hände andere Personen, werden diese zumeist gegen die Interessen des Betroffenen eingesetzt. Ohne wirksamen Datenschutz lägen all unsere personenbezogenen Daten frei verfügbar herum und könnten von jedem eingesehen werden. Aufgabe des Datenschutzes ist es, genau das zu verhindern.

Privatsphäre

Als »Privatsphäre« wird der Teil des Lebens einer Person bezeichnet, der bereits im Grundgesetz durch das Persönlichkeitsrecht, die Unverletzlichkeit der Wohnung oder das Post- und Fernmeldegeheimnis umrissen wird. Nur in gesetzlich streng geregelten Ausnahmefällen darf der Staat durch seine Institutionen in diesen privaten Lebensbereich eingreifen. So ist es rechtlich zulässig, das Telefon eines Tatverdächtigen abzuhören. Täte der Staat dies »prophylaktisch« bei allen Bürgern, wäre dies ein schwerwiegender Eingriff in die Privatsphäre.

Beispiel: Der Discounter Lidl geriet vor einigen Jahren massiv in die Kritik, als herauskam, dass in einer Vielzahl von Filialen ohne Wissen der Belegschaft Kameras und Mikrofone installiert worden waren. Wäre allein dies schon ein daten-

schutzrechtlich bedenkliches Vorgehen, so ließ Lidl seine Mitarbeiter regelrecht bespitzeln. Es wurden persönliche Informationen über Mitarbeiter gesammelt, die häufig bis in die intimsten Bereiche des Privatlebens reichten. Geplante Schwangerschaften, Krankheiten oder betriebsinterne Liebeleien zwischen Angestellten – all dies und mehr wurde in großem Maßstab aufgezeichnet. Sie können sich vorstellen, dass diese Informationen nicht zum Vorteil der betroffenen Mitarbeiter eingesetzt wurden. Ganz davon zu schweigen, dass Lidl bei diesem Vorgehen gleich eine ganze Reihe teils schwerwiegender Gesetzesverstöße beging.

Verschlüsselung

Das Verschlüsseln von Informationen ist beileibe keine Erfindung der Neuzeit, vielmehr hat der Mensch im Laufe seiner Kulturgeschichte oftmals versucht, Informationen vor den Augen Unbefugter dadurch zu verbergen, dass sie in eine nicht ohne Weiteres lesbare Form gebracht werden. Charakteristisch für Verschlüsselung ist, dass die »Unkenntlichmachung« der Informationen nach einer bestimmten Logik geschieht. So könnten Sie beispielsweise das Wort »Berlin« auch als »Adqkhm« schreiben; die Logik wäre das dahinterstehende logische Prinzip, dass alle Buchstaben der Verschlüsselung einfach um einen nach »links« im Alphabet verschoben werden. Sonderlich sicher wäre diese Art der Verschlüsselung indes nicht. Bereits in der Antike gab es wesentlich raffiniertere Verfahren.

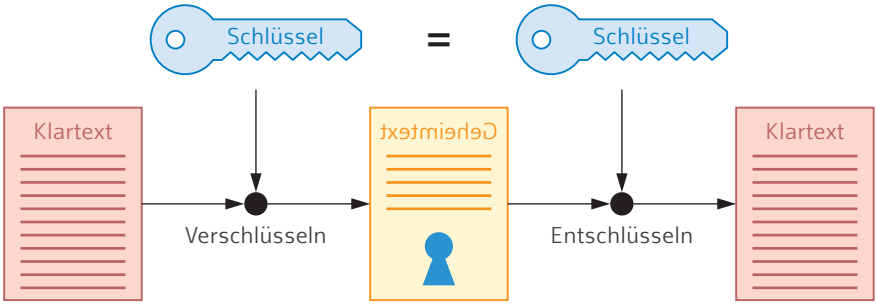
Einwegverschlüsselung/Hashing

Passwörter und andere Nutzerdaten werden auf Servern häufig mittels einer sogenannten »Einwegverschlüsselung« (oft als »Hashing« bezeichnet) verschlüsselt. Dabei führt die Anwendung eines Algorithmus zu einer Ausgabe, die je nach Wert der Originaldaten eindeutig ist. Das Verschlüsseln desselben Wortes wird also immer denselben Hashwert ergeben. Somit lassen sich Hashwerte verwenden, um Eingaben darauf zu überprüfen, ob sie identisch sind, ohne die Originalzeichenfolge zu kennen. Für das Speichern von Passwörtern und ähnlichen Daten in verschlüsselter Form werden kryptologische Hashverfahren eingesetzt. Diese sollen dafür Sorge tragen, dass selbst bei einem Diebstahl der verschlüsselten Daten vom Server der Aufwand für das Entschlüsseln so hoch wäre, dass es sich in der Praxis nicht lohnt. Anders als bei symmetrischen oder asymmetrischen Verfahren gibt es bei kryptologischen Hashingverfahren keinen »Schlüssel«, der ein einfaches Entschlüsseln der Daten ermöglicht.

Symmetrisches Verschlüsseln

Die symmetrische Verschlüsselung verwendet für das Ver- und Entschlüsseln denselben Schlüssel. Gut einsetzbar ist dieses Verfahren bei der Verschlüsselung lokaler Datenträger. Nicht sinnvoll ist es hingegen bei der Übertragung von Daten, da der Schlüssel dem Empfänger ebenso bekannt sein muss und die Übertragung des Schlüssels ein Sicherheitsrisiko darstellt. Stellen Sie sich ein Tür-

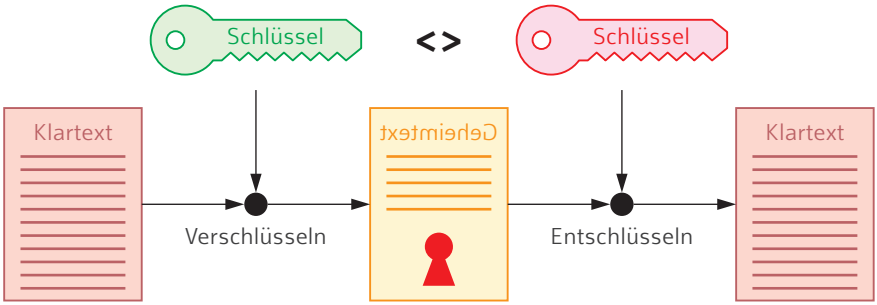
schloss vor: Dieses können Sie mit demselben Schlüssel zu- und wieder aufschließen.



Darstellung der symmetrischen Verschlüsselung, bei der zum Ver- und Entschlüsseln derselbe Schlüssel verwendet wird.

Asymmetrisches Verschlüsseln

Im Gegensatz zum symmetrischen Verfahren ist das asymmetrische sehr gut für die Übertragung verschlüsselter Informationen geeignet. Statt nur eines Schlüssels gibt es hier nämlich zwei: einen »öffentlichen« und einen »privaten«. Möchten Sie jemandem eine asymmetrisch verschlüsselte Nachricht senden, so nutzen Sie dessen »öffentlichen« Schlüssel dafür. Dieser heißt so, weil er öffentlich zugänglich sein muss, damit das Verfahren funktioniert. Beim symmetrischen Verschlüsseln könnten Sie nun die verschlüsselte Nachricht mit demselben Schlüssel wieder entschlüsseln. Das ist beim asymmetrischen Verfahren jedoch nicht der Fall. Stattdessen kann eine mit dem öffentlichen Schlüssel kodierte Nachricht nur mit dem dazugehörenden »privaten« Schlüssel dekodiert werden. Der wiederum heißt so, weil er eben nicht öffentlich zugänglich sein darf, schließlich soll ja ausschließlich der Empfänger der Nachricht in der Lage sein, diese zu entschlüsseln. Auch beim Einsatz digitaler Signaturen kommt das asymmetrische Verfahren zum Einsatz, um die Echtheit eines Absenders zu prüfen.



Darstellung der asymmetrischen Verschlüsselung, bei der zum Ver- und Entschlüsseln unterschiedliche Schlüssel verwendet werden.

Bundeskriminalamt, Wiesbaden: 81.
Dinse, Sascha, Berlin: 65, 67, 71, 72, 77, 93, 94, 95.
Firma Sebastian Bauer, Berlin: Screenshot/onlinewarnungen.de 106.
GitHub, Inc., San Francisco: 2018 111.
iStockphoto.com, Calgary: ByoungJoo 4, 6; keport 4, 40; Sikham, Panuwat 5, 80.
Lithos, Wolfenbüttel: 13, 15, 15, 20, 21, 26, 26, 27, 28, 32, 41, 42, 42, 46, 62, 69, 91, 94, 104.
SPIEGEL ONLINE GmbH, Hamburg: 10, 23, 58, 59, 99, 108.
Startnext Crowdfunding GmbH, Dresden: 7.
stock.adobe.com, Dublin: LVDESIGN Titel; monsitj Titel.