Ausgabe 04 | 2019

ExperSite

Das Magazin für Informationssicherheit und Datenschutz

Egal wie gut die IT abgesichtert ist. Sie hat eine Schwachstelle: Uns! 21

Cloud-Technologien machen vieles einfacher. Aus Datenschutzperspektive sind sie allerdings hoch komplex. 27

DATATREE
YOUR COMPLIANCE PROVIDER

www.datatree.eu

Die Hassliebe zur IT

Kennen Sie die sogenannten Silver-Surfer? Was sich anhört wie eine Marvel-Comic-Verfilmung, ist ein von der Netzkultur geprägter Begriff des Internetmarketings und bezeichnet eben die Menschen ab einem Alter von 50 Jahren, die durch den Wechsel von Offline- zu Onlinemedien mit für die rasante Entwicklung des Internets verantwortlich waren. Gleichzeitig sind die Silver-Surfer allerdings mit großem Misstrauen und mangelnder Medienkompetenz ausgestattet, was eben auf das Leben „vor dem technologischen Selbstverständnis“ zurückzuführen ist. Jetzt wäre es meines Erachtens nach jedoch fatal, ausschließlich dieser Gruppe eine mangelnde Medienkompetenz zuzuschreiben. Eine ausreichende Sicherheit im Umgang mit Daten im Internet können sich die wenigsten Menschen zuschreiben. Aber wie sollte es auch anders sein in einer Zeit, in der wir von Daten und technologischen Entwicklungen förmlich überrollt werden? In denen wir eine unglaubliche Abhängigkeit von unseren IT-Systemen haben, eine Abhängigkeit, die uns angreifbar macht und das sowohl im persönlichen, als auch beruflichen Umfeld. Eine Abhängigkeit, die uns in die Pflicht nimmt, uns mit den technischen Feinheiten von technologischen Entwicklungen auseinanderzusetzen und vor allem auch Verantwortung zu übernehmen. Egal ob wir uns in der Rolle des Nutzers, des Softwareanbieters oder als Dienstleister wahrnehmen, nur gemeinsam können wir uns dieser Herausforderung stellen.

„Datenschutz geht ganz oder gar nicht.“

Ihre Nina Richard
(Redaktionsleitung)

Ist der Ruf erst ruiniert …

… bedarf es mehr als fachlicher Kompetenz, um ein Thema nach vorne zu bringen. Die Rolle des Datenschutzbeauftragten ist gesetzlich vorgeschrieben und gehört zu den unbeliebtesten innerhalb eines Unternehmens. Kein Wunder, eilt ihm der Ruf als Bedenkenträger und Verhinderer des agilen Unternehmensvorgehens im Tagesgeschäft voraus. Magnus Welz, langjähriger Datenschutzberater, erläutert den notwendigen Wandel des Berufsbildes und wie er und sein Team sich trauen, den Datenschutz neu zu erfinden.

Interview: Nina Richard

Welche Voraussetzungen muss ein Datenschutzbeauftragter erfüllen?

Der Berufsverband der Datenschutzbeauftragten bietet mit dem Leitbild für Datenschutzbeauftragte eine erste grobe Orientierung. Unter anderem müssen ausreichende Kenntnisse in Themenfeldern, wie Organisation und Prozesse, Informations- und Kommunikationstechnologie (IuK) sowie Recht existieren. Darüber hinaus gilt es natürlich, sich ein gewisses Fachwissen über die eigene Branche anzueignen, beispielsweise betriebswirtschaftliches und organisatorisches Fachwissen. Softskills wie Beratungskompetenz, Präsentationstechniken oder Durchsetzungsvermögen sind inzwischen selbstverständlich. Und das ist erst der Anfang.

Klingt ein bisschen nach der Eier legenden Wollmilchsau … Wie realistisch ist es, all diese Kompetenzen in einer Person zu vereinen?

Naja, das betrachte ich schon als eine große Herausforderung. Um als Datenschutzbeauftragter all diese Kompetenzen in sich zu vereinen, bedarf es einer großen intrinsischen Motivation, um sich kontinuierlich weiterzubilden bzw. sich neues und ergänzendes Wissen anzueignen. Mit dem Besuch eines Wochenendlehrgangs ist es auf jeden Fall nicht getan. Lebenslanges Lernen ist hier die Devise, das trifft allerdings inzwischen auf die meisten Berufsbilder zu. Gerade Einzelkämpfer haben es hier schwer, da es ihnen einfach an einem Sparringspartner fehlt, mit dem sie die diversen Graustufen einer praktikablen Datenschutzlösung diskutieren können.

Wie sieht denn die Realität aus?

Der Klassiker ist immer noch weit verbreitet, erschreckenderweise: Wer sich als Letzter wegduckt, hat den Job. Aber glücklicherweise existieren auch immer mehr, die das Thema mit Leidenschaft angehen.

Wie bekommt man das Ganze dennoch abgedeckt?

Datenschutz braucht Budget, Manpower und kann eben nicht mal eben nebenbei erledigt werden. Wie mit allem, was man beginnt, gilt auch hier die Devise: Ganz oder gar nicht. Überlegen Sie sich im Vorfeld ein Konzept, das den gesetzlichen Anforderungen und dem eigenen Unternehmen gerecht wird. Denn der Datenschutzbeauftragte ist nicht für den Datenschutz im gesamten Unternehmen zuständig - er berät und unterstützt – aber Datenschutz muss von der kompletten Organisation gelebt werden. Viele denken beim Datenschutz an Regulierung und Bürokratie, das ist allerdings falsch. Der Gesetzgeber bietet zahlreiche individuelle Möglichkeiten, die Selbstregulierung wäre hier ein Stichwort. Nehmen Sie sich ausreichend Zeit und treten Sie in den Dialog mit Ihren Kollegen und beziehen Sie diese möglichst umfassend ein. Erfolg und Misserfolg hängen auch von der Unterstützung durch die Geschäftsführung ab.

„Datenschutz geht ganz oder gar nicht."

Datenschutz, das ist für die meisten immer noch zähe Pflicht, stimmt das?

Das ist richtig, also dieses Image ist weit verbreitet. Inzwischen merken aber imnmer mehr, dass ein aktiver, individuell auf das jeweilige Unternehmen konfigurierter Datenschutz in vielerlei Hinsicht alles andere als langweilig oder gar störend ist. Im Gegenteil, gerade durch die fortschreitende Digitalisierung erfährt der Datenschutz eine immer stärkere Wahrnehmung. Unternehmen, die sich umfassend mit dem Schutz personenbezogener Daten befassen, verhindern also nicht nur, dass diese Daten an unbefugte Dritte gelangen und gegebenenfalls Strafen drohen, diese Unternehmen können sich inzwischen auch über einen signifikanten Reputationsgewinn freuen.

Was macht die Rolle des Datenschutzbeauftragten so unbeliebt?

In vielen Köpfen hat sich der gesetzestreue, unflexible Papiertiger festgesetzt. Das ist nun einmal nicht sonderlich attraktiv. Mit dieser Hypothek müssen Sie erst einmal leben. Die Kollegen müssen also vom Gegenteil überzeugt werden. Das kostet Kraft und Rückschläge gehören quasi zum Alltag. Diese Herausforderung möchte natürlich nicht jeder annehmen. Diejenigen, die es trotzdem versuchen und ihren sportlichen Ehrgeiz wecken, haben am Ende dann ein ganz besonderes Erfolgserlebnis. Dafür muss sich aber jeder DSB mit den individuellen Gegebenheiten vor Ort auseinandersetzen und Lösungen anbieten. Der Satz „Das geht aus Datenschutzgründen nicht" wirkt wie ein Gift. Also Probleme benennen und Möglichkeiten aufzeigen, beides gehört dazu.

„Das geht aus Datenschutzgründen nicht."

Wie kann sich das Bild zukünftig ändern?

Das Bild wandelt sich gerade stark. Das hat mehrere Gründe, der Hauptgrund ist das gestiegene Bewusstsein der Menschen. Daten sind heute nicht mehr dieses unbekannte abstrakte Etwas. Alle wissen, dass Daten, vor allen Dingen die eigenen personenbezogenen Daten, einen Wert darstellen, einen schützenswerten Wert. Mit jeder Datenschutzpanne und jedem Datenschutzskandal steigt dieses Bewusstsein. Die Menschen legen daher heute schon großen Wert auf Datenschutz und verlangen diesen. In Zukunft wird ein funktionierender Datenschutz als selbstverständlich und nicht mehr störend wahrgenommen, damit ändert sich dann auch das Bild des DSB nachhaltig. Hierzu muss Datenschutz ein selbstverständlicher Teil des Qualitäts- und Prozessmanagements werden.

Wie gehen Sie persönlich mit diesem Wandlungsprozess um?

Zunächst einmal freue ich mich über diesen Prozess, schließlich kenne ich auch noch die wirklich schweren Zeiten aus der gar nicht einmal so fernen Vergangenheit. Ich versuche aber auch, aktiv an diesem Prozess teilzuhaben. Ich berate Unternehmen zu den Themen Datenschutz und Informationssicherheit. Meine oberste Prämisse ist dabei immer zu gucken, wie ich alles unter einen Hut bekomme: Die gesetzlichen Anforderungen und die eigentlichen Unternehmensabsichten. Mir ist wichtig, dass Datenschutzberater als Berater mit praxisnahen Lösungen gesehen werden und dieses Bild auch selbstständig prägen, indem sie Datenschutz nicht mehr ausschließlich papierbasiert machen.

„Wir müssen den Prozess aktiv mitgestalten.“

Wie ist Ihre Einschätzung der aktuellen Situation, wo stehen wir?

Ich glaube, wir sind auf einem guten Weg. Die DSGVO hat anfangs eher Angst und Schrecken verbreitet, das hat sich doch inzwischen gelegt. Im Gegenteil, Datenschutz genießt mehr und mehr Aufmerksamkeit bei Unternehmen, Kunden und den Menschen allgemein. Dennoch gibt es keinen Grund, sich auf dem Erreichten auszuruhen. Der eingeschlagene Weg ist richtig, doch wir müssen ihn noch eine ganze Weile gehen. Dazu sollte und muss jeder einzelne DSB beitragen. Denn Datenschutz ist eben nicht eine abstrakte nervtötende Angelegenheit, sondern ein hochemotionales Thema; nicht umsonst erreichen gerade Datenschutzverstöße in diesen Tagen ein so großes mediales Echo. //

MAGNUS WELZ

Magnus Welz studierte medizinische Informatik an der Fachhochschule Dortmund. Der Berater ist bei der DATATREE AG schwerpunktmäßig mit der Entwicklung des Datenschutz-Management-Systems betraut. Welz arbeitete branchenunabhängig im komplexen Gebiet des Datenschutzes und war unter anderem als technischer Projektmanager und Business Analyst in agilen Softwareentwicklungsprojekten in den Bereichen e- und mHealth tätig. Außerdem strukturierte er Datenschutz- und IT-Sicherheitsprojekte und setzte diese erfolgreich nach etablierten Sicherheitsleitlinien um.

Bundesweites Berechnungsmodell bei Datenschutzverstößen

Seit dem 16. Oktober gilt in Bezug auf Datenschutzverstöße und Pannen ein neuer Bußgeldkatalog. Die Bundes- und Landesbehörden haben sich auf ein einheitliches Berechnungsmodell verständigt. Dies erzeugt zum einen eine höhere Transparenz und erweitert darüber hinaus den Handlungsspielraum der Datenschutzbehörden.

Text: Jörg Fecke

Fünf Stufen zum individuellen Bußgeld

Das fünfstufige Modell berücksichtigt eine Vielzahl an Parametern, die in Bezug zueinander eine Bußgeldformel ergeben. Neben Firmengröße und Jahresumsatz spielt vor allen Dingen die Schwere der Tat eine Rolle. Hier wird zwischen leichten, mittleren, schweren und sehr schweren Datenschutzverstößen unterschieden. Neu ist im Vergleich zur bisherigen Politik die Größenkategorisierung der betroffenen Unternehmen – diese richtet sich nach dem jährlich erzielten Jahresumsatz. Aus dem Umsatz ergibt sich die Differenzierung zwischen Kleinstunternehmen, kleineren und mittleren Unternehmen sowie Großunternehmen. Unternehmensgröße bzw. der Jahresumsatz dienen als Grundlage für die Bestimmung des sogenannten Grundwertes. Dies ist im Endeffekt ein individuell berechneter Tagessatz. Der Tagessatz wird schließlich mit der Schwere des Verstoßes multipliziert. Schließlich werden noch sogenannte sonstige Umstände berücksichtigt. Dies kann sich strafverschärfend auswirken, etwa bei Wiederholungstätern, aber auch strafmindernde Parameter kommen zum Zug, wenn beispielsweise durch die Strafe eine Zahlungsunfähigkeit des Unternehmens droht.

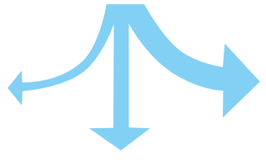
1. Zuordnung anhand der Betriebsgröße in vier Klassen

2. Bestimmung des Jahresumsatzes der jeweiligen Untergruppe

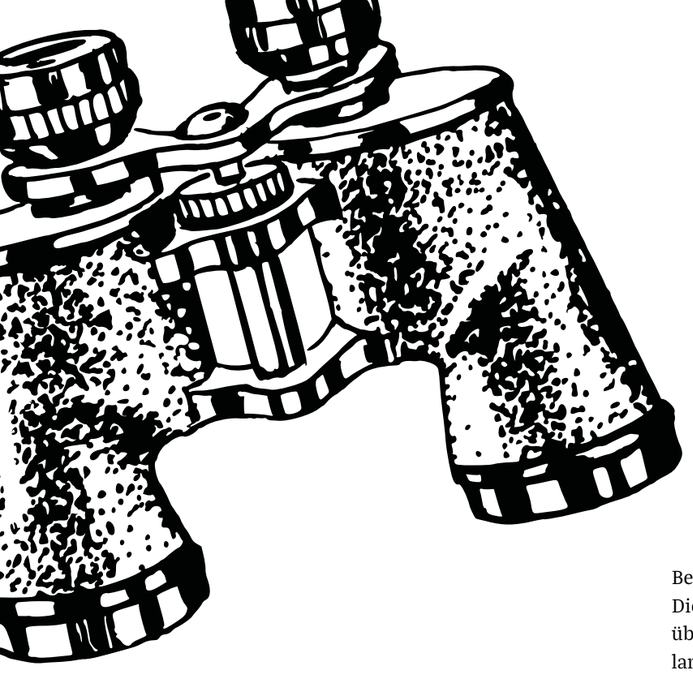
3. Ermittlung des wirtschaftlichen Grundwertes

4. Multiplikation des Grundwertes nach Schweregrad der Tat

5. Anpassung des Grundwertes an individuelle Umstände



Bußgeld



Das Konzept ist für alle Landes- und Bundesbehörden bei der Ermittlung von Strafen im Rahmen der DSGVO bindend. EU-weit hat es dagegen keine Gültigkeit. Und dennoch ist die Maßnahme auch ein Zeichen für eine stärkere Vereinheitlichung auf europäischer Ebene. Während in Großbritannien und auch in Frankreich Strafen in teils dreistelliger Millionenhöhe verhängt wurden, hielten sich Behörden hierzulande eher zurück. Eine Konsequenz aus der Vereinheitlichung sind auch potenziell höhere Strafen hierzulande. Dieses Verfahren soll darüber hinaus nachvollziehbare, transparente und einzelfallgerechte Urteile ermöglichen.

EU-weite Konsolidierung schreitet voran

Für Unternehmen wird es langsam ernst. Bei Datenschutzverstößen wird es in Zukunft deutlich teurer. Während sich British Airways oder die Hotelkette Marriott in Großbritannien jeweils mit einer Strafe um die 200 Millionen Euro auseinandersetzen müssen, Google aus Paris aufgrund von DSGVO-Verstößen eine Rechnung über 50 Millionen Euro serviert bekam, fällt das bisher höchste verhangene Bußgeld in Deutschland bei knapp 200.000 Euro verhältnismäßig moderat aus.

Einiges deutet darauf hin, dass die Strafen in naher Zukunft sprunghaft steigen. Die Berliner Datenschutzbeauftragte Maja Smoltczyk leitete ein Verfahren gegen das Immobilienunternehmen Deutsche Wohnen ein. Die Strafe beläuft sich aufgrund von Datenschutzverstößen auf 14,5 Millionen Euro. Diese bundesweit höchste Strafe ist allerdings noch nicht rechtskräftig, das Unternehmen geht juristisch gegen das Bußgeld vor.

Was tun, um Strafen zu entgehen?

Bevor nun die alltbekannte DSGVO-Panik wieder um sich greift: Die bisherigen Millionenstrafen betreffen Konzerne, die gegenüber der DSGVO streng fahrlässig handelten, dies oft über einen langen Zeitraum und der Kreis der Geschädigten war dabei nicht unerheblich. Außerdem handelte es sich bei British Airways, Marriott und Google nun nicht gerade um kleine oder mittelständische Unternehmen, sondern um milliardenschwere Global Player. Die Strafe, so hoch sie auch erscheinen mag, stellt diese Firmen vor keine großen Herausforderungen, der Imageschaden ist allerdings erheblich. Die beste Möglichkeit, gar nicht erst in Konflikt mit der DSGVO zu kommen, ist die Prüfung der eigenen Datenschutzkultur. Begriffe wie Privacy by Design, also die Idee, den Datenschutz zu Beginn eines Datenverarbeitungsprogramms direkt zu integrieren, oder Privacy by Default, datenschutzfreundliche Voreinstellungen, haben die meisten schon einmal gehört. Hinter diesen Begriffen verbirgt sich aber vor allen Dingen ein solides Fundament für datenschutzkonformes Handeln. Übrigens, Privacy by Design und Privacy by Default sind keine völlig neuen Begriffe, haben allerdings mit Inkrafttreten der DSGVO einen neuen Stellenwert. Es ist daher nur von Vorteil, bei sämtlichen Prozessen der Datenverarbeitung, gerade im Hinblick auf die fortschreitende Digitalisierung, das Thema Datenschutz von Beginn an zu berücksichtigen. Dann besteht überhaupt kein Grund zur Panik. Eine durchdachte und in allen Unternehmensbereichen gelebte Datenschutzkultur schützt Werte, das Image und schließlich vor empfindlichen Strafen. //

Die Regeln bestimmen das Spiel

Nach den letzten Gerichtsurteilen und Einschätzungen der Aufsichtsbehörden findet in Bezug auf den eigenen Internetauftritt ein Umdenken statt.

Text: Christine Thieme

Vor dem Spiel ist nach dem Spiel – was im Fußball schon lange gilt, scheint nun auch auf EU-Verordnungen zuzutreffen. Kaum haben viele Unternehmen die Datenschutzerklärungen ihrer Interneterklärungen an die Anforderungen der DSGVO angepasst, droht neuer Handlungsbedarf. Die ePrivacy-Verordnung (kurz ePVO), die zukünftig den Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation (vor allem im Internet) regelt, soll nun 2020 in Kraft treten.

In Vorwegnahme der ePVO haben die deutschen Aufsichtsbehörden bereits im März 2019 eine Orientierungshilfe für Anbieter von Telemedien herausgegeben (erhältlich unter dem Link https://www.datenschutzkonferenz-online.de > Orientierungshilfen). In dieser Stellungnahme äußern sich die Aufsichtsbehörden recht konkret zum Einsatz von Trackingtools und zur Gestaltung von Cookie-Bannern.

Einwilligung über Cookie-Banner

Im Hinblick auf die DSGVO haben im vergangenen Jahr viele Websitebetreiber ihren Auftritt mit einem Cookie-Banner versehen. Vor dem Hintergrund, dass eine verantwortliche Stelle vor Beginn der Datenverarbeitung über dieselbige informieren sollte, ist ein Banner mit Verlinkung auf die Datenschutzerklärung sicherlich ratsam. Eine Einwilligung zur Datenverarbeitung über das Cookie-Banner einzuholen, ist laut Aufsichtsbehörden jedoch nur wirksam, wenn bestimmte Gestaltungsregeln eingehalten werden. Ein Banner mit dem Wortlaut „Wenn Sie weitersurfen, erklären Sie sich einverstanden“, stellt keine wirksame Einwilligung dar.

Datenverarbeitung über das berechtigte Interesse

Eines stellen die Aufsichtsbehörden auch klar: Das Setzen von Cookies ist nicht per se einwilligungsbedürftig. Insbesondere Cookies, die zum technischen Betrieb der Seite erforderlich sind, bedürfen keiner Einwilligung. Trackingtools können durchaus auf Basis des berechtigten Interesses (Art. 6 Abs. 1 lit. f DSGVO) eingesetzt werden. So gelten die Bereitstellung von Warenkorbfunktionen und Reichweitenmessung, durchaus als berechtigtes Interesse des Websitebetreibers. Bei der Interessensabwägung (Interesse der verantwortlichen Stelle versus Interesse des Betroffenen an Wahrung) sollte der Websitebetreiber genau prüfen, wie die eingesetzten Trackingtools funktionieren. Ein zu großer Eingriff in die Privatsphäre liegt sicherlich immer dann vor, wenn ein eindeutiger Identifier verwendet wird, z. B. IMEI-Nummer, MAC-Adresse oder eine geräteübergreifende Ad-Id. Gerade mit Letzterer wird allerdings oft im Onlinemarketing gearbeitet, um eine Wiedererkennung des Nutzers zwecks Remarketing umzusetzen. Auch die Zusammenführung von Nutzungs- und Inhaltsdaten oder vieler Daten und die Einbindung von Drittanbietern, die die Daten dann zu eigenen Zwecken nutzen, wird im Hinblick auf die Interessensabwägung nicht möglich sein. Eine Einwilligung ist laut Ulrich Kelber, Bundesbeauftragter für Datenschutz und Informationssicherheit, jedoch immer erforderlich, sofern die eingebundenen Drittdienste die Daten auch für eigene Zwecke nutzen. (Weiteres zum Einwilligungserfordernis bei Cookies, dem rechtlichen Hintergrund und dem aktuellen EuGH-Urteil vom 01.10.2019 siehe Seite 12f.)

Gemeinsame Verantwortlichkeit bei Social Media Auftritten

Sowohl im Juni 2018 als im Juli 2019 ergingen Urteile des EuGHs zu dem werblichen Einsatz von Facebook (EuGH-Urteil C-210/16 vom 06.06.2018 und EUGH-Urteil C-40/17 vom 29.07.2019). Bemerkenswert an dem ersten Urteil ist vor allem, dass der EuGH bei einem Unternehmensauftritt in Facebook („Fanpage“) den Fanpage-Betreiber des Unternehmensauftritts als Verantwortlichen für die Datenverarbeitung sieht, auch wenn der Fanpage-Betreiber keinen wirklichen Einfluss auf die Datenverarbeitung durch Facebook hat. Aufgrund dieses Urteils stellt Facebook nun im Rahmen des Accounts eine Vorlage für eine gemeinsame „Verantwortlichkeit“ zur Verfügung. Zudem müssen Fanpage-Betreiber informieren, dass personenbezogene Daten erhoben und an Facebook weitergeleitet werden.

Das diesjährige Urteil des EuGH ist dagegen weniger überraschend: Es bestätigt die gemeinsame Verantwortlichkeit eines Websitebetreibers, der Social-Plug-ins des Netzwerkes auf seiner Seite einsetzt. Bei der Frage, ob die Datenverarbeitung von Social-Plug-ins einer Einwilligung durch den Nutzer bedürfen oder ob diese durch das berechtigte Interesse gerechtfertigt wird, verweist der EuGH die Entscheidung an das vorlegende Gericht (hier: OLG Düsseldorf), das dies nun in einem weiteren Verfahren entscheiden wird. Um die Internetauftritte möglichst rechtssicher zu gestalten, sollten Unternehmen in der praktischen Umsetzung vor allem die folgenden Maßnahmen ergreifen.

CHRISTINE THIEME

Die Diplom-Betriebswirtin arbeitet seit 2011 für die DATATREE AG. Die Datenschutzberaterin kann langjährige Erfahrungen aus dem Direktmarketing und der Marktforschung nachweisen. Das macht sie zur Expertin auf dem Gebiet der datenschutzkonformen Gestaltung von Marketingmaßnahmen. Zu Ihren Fachgebieten gehören darüber hinaus Social-Media-Aktivitäten, Beschäftigtendatenschutz von Unternehmen der Privatwirtschaft sowie kommunaler Einrichtungen.

Was ist konkret zu tun?

Es muss geprüft werden, welche Trackingtools konkret eingesetzt werden, welche Daten diese sammeln, wie diese verarbeitet werden und ob/an wen die Daten übermittelt werden. Sofern das Setzen von Cookies, die nicht technisch erforderlich sind, rechtmäßig ist, sollte ebenfalls die jeweiligen Opt-out-Möglichkeiten auf Funktion geprüft werden. Opt-out-Links, die nicht funktionieren, könnten Aufsichtsbehörden unangenehm auffallen.

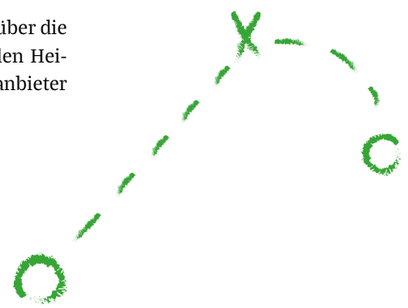
Empfehlenswert ist auch eine Analyse, ob wirklich jedes Trackingtool wirtschaftlich Sinn macht. Manche Anbieter erfüllen die datenschutzrechtlichen Voraussetzungen nicht, wie z. B. den Abschluss einer AV-Vereinbarung, und bringen auch nicht den erhofften Mehrwert.

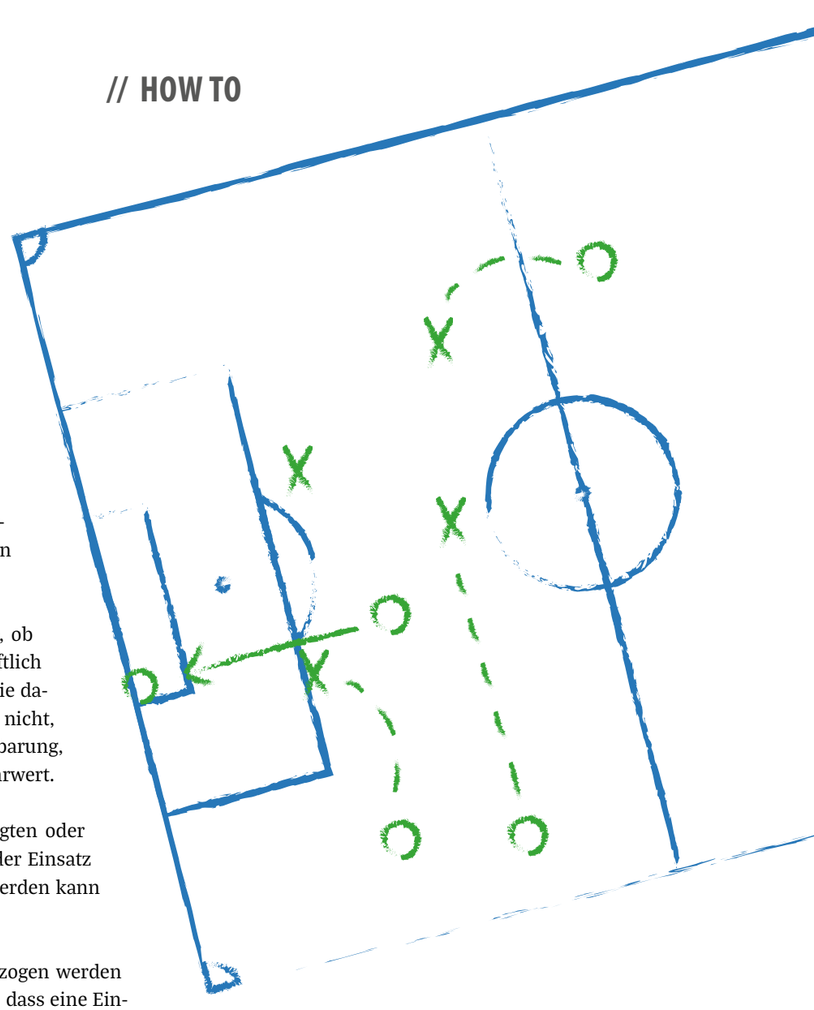
Gemeinsam mit dem Datenschutzbeauftragten oder einem Fachanwalt sollte geprüft werden, ob der Einsatz noch auf das berechtigte Interesse gestützt werden kann oder ob eine Einwilligung erforderlich ist.

Das Cookie-Banner sollte einer Revision unterzogen werden – dient es rein der Information, suggeriert aber, dass eine Einwilligung eingeholt wird, dann sollte der Wortlaut angepasst werden. Falls über das Cookie-Banner eine Einwilligung eingeholt werden soll, müssen unbedingt die Gestaltungsvorgaben der Aufsichtsbehörde eingehalten werden.

Auch wenn sich die oben genannten Gerichtsurteile auf Facebook beziehen, ist davon auszugehen, dass die Konsequenzen daraus auch für andere soziale Netzwerke wie Instagram, Twitter oder Xing gelten. Unternehmen, die dies noch nicht getan haben, sollten prüfen, inwieweit die Möglichkeit besteht, eine Vereinbarung zur gemeinsamen Verantwortlichkeit zu schließen. Informationen zur Datenverarbeitung durch den Fanpage-Auftritt sollten in der Datenschutzerklärung ergänzt werden.

Empfehlenswert ist die Einbindung von Social-Plug-ins über die Zwei-Klick- oder Shariff-Lösung (Bereitstellung durch den Heise-Verlag). Dann erfolgt die Datenübermittlung an Drittanbieter erst bei dem zweiten Klick.





Fazit:
Auch, wenn die ePVO eine Übergangsfrist von zwei Jahren gewährt, werden sich die Einschätzungen der Aufsichtsbehörden und Gerichte nach den zukünftigen Vorgaben richten. Daher sollte die Website kontinuierlich in Hinblick auf ihre rechtssichere Gestaltung geprüft werden. //

Europäischer Gerichtshof urteilt: Keine Cookies ohne Einwilligung

Websitebetreiber müssen beim Cookie-Einsatz nachbessern.

Text: Prof. Dr. Julius Reiter und Dr. Olaf Methner

Wer auf seiner Website Cookies setzt, die nicht zwingend erforderlich sind, benötigt hierfür eine aktive Einwilligung des Internetnutzers. Eine Voreinstellung dieser Einwilligung, die der Nutzer erst mit einem Klick widerrufen muss, ist unzulässig. Dies hat der Europäische Gerichtshof (EuGH) in einem aktuellen Urteil vom 01.10.2019 (Rs. C-673/17) entschieden.

Worum ging es in der Entscheidung?

Der EuGH hatte über Fragen des europäischen Rechts in einer Klage des deutschen Verbraucherzentrale Bundesverbandes (vzbv) gegen den Adresshändler und Gewinnspielbetreiber „Planet 49“ zu urteilen. Um an einem Onlinegewinnspiel teilzunehmen, mussten die Nutzer ihre persönlichen Kontaktdaten in einer Eingabemaske eintragen. In der Eingabemaske für diese Kontaktdaten war eine Einverständniserklärung voreingestellt, dass der Websitebetreiber Cookies zur Auswertung des Surf- und Nutzerverhaltens setzen und so „interessengerichtete Werbung“ ermöglichen sollte. Nutzer, die hiermit nicht einverstanden waren, mussten mit einem zusätzlichen Klick den Haken an der Zustimmung entfernen. Dies hielt der vzbv für unzulässig.

Was hat der EuGH entschieden?

Der EuGH hat erklärt, dass eine solche Voreinstellung unzulässig ist. Dies wurde vor allem damit begründet, dass nach der europäischen „Cookie-Richtlinie“ aus dem Jahr 2009 im Grundsatz ein Opt-in-Verfahren vorgeschrieben ist. Ein solches Verfahren setzt eine aktive Willensbekundung des Nutzers zur Einwilligung in den Einsatz von Cookies voraus. Nach Auffassung des EuGH liegt eine solche aktive Einwilligung nicht vor, wenn sie durch ein voreingestelltes Ankreuzkästchen erteilt werden soll. Hier ist nämlich gerade kein aktives Verhalten des Nutzers notwendig.

Dabei spielt es übrigens keine Rolle, ob Cookies nur pseudonymisierte Daten ohne Bezug zu einer konkreten Person erheben lassen. Der EuGH meint hierzu wörtlich: „Das Unionsrecht (d. h. das europäische Recht; Anm. d. Verf.) soll Nutzer vor jedem Eingriff in ihre Privatsphäre schützen, insbesondere gegen ‚Hidden Identifiers‘ oder ähnliche Instrumente.“

Bei personenbezogenen Daten, wie z. B. der IP-Adresse, folgt auch aus der europäischen Datenschutzgrundverordnung (DSGVO), dass Websitenutzer über die Verarbeitung der Daten, die Dauer der Speicherung, den konkreten Verwendungszweck etc. informiert werden müssen und ihr Einverständnis hiermit erteilen müssen.

Gilt diese Rechtslage unmittelbar in Deutschland?

Ob die Entscheidung des EuGH in vollem Umfang bereits in Deutschland gilt, ist nicht ganz klar.

Die „Cookie-Richtlinie“ wurde in Deutschland nicht weiter umgesetzt, denn der deutsche Gesetzgeber meinte bislang, dass die bestehende Regelung in § 15 Telemediengesetz (TMG) europarechtlich bereits ausreicht. Hieran gibt es aber Zweifel, denn für die Verwendung pseudonymisierter Daten lässt diese Vorschrift genügen, dass der Nutzer „nicht widerspricht“. Die bisherige Opt-out-Lösung erschien damit zulässig.

Nun hat der Bundesgerichtshof (BGH) im Ausgangsverfahren des vzbv gegen Planet 49 noch einmal zu entscheiden, ob die deutschen Vorschriften nach den Vorgaben des EuGH europarechtskonform ausgelegt werden können oder ob der deutsche Gesetzgeber jedenfalls für das Tracking pseudonymisierter Daten nachbessern muss.

Alternativ könnte der europäische Gesetzgeber mit einer neuen Verordnung unmittelbar die Rechtslage in allen Mitgliedstaaten regeln. Hierfür steht der Entwurf der ePrivacy-Verordnung im Raum, die durch die EuGH-Entscheidung nun Rückenwind bekommen könnte und für Rechtsklarheit sorgen würde. Ob und wann es hier zu einer politischen Einigung auf europäischer Ebene kommt, bleibt aber ungewiss.

Was bedeutet das Urteil für die Praxis?

Bislang wurden in der Praxis häufig Cookie-Banner eingesetzt, die relativ wenig Text enthalten und allenfalls einen Hinweis auf den Cookie-Einsatz geben. Oft ist wie im entschiedenen Fall das Einverständnis mit dem Cookie-Einsatz bereits voreingestellt. Aus der Entscheidung des EuGH folgt nun, dass Websitebetreiber hier Anpassungen vornehmen sollen. Die Nutzer müssen umfangreicher über die Verwendung der Cookies informiert werden und hierzu aktiv ihr Einverständnis erklären. Websitebetreiber, die diese Vorgaben ignorieren und die bisherige Praxis fortführen, sollten sich nicht auf die etwas unklare Rechtslage im deutschen Gesetz verlassen. Wenn der BGH im weiteren Verlauf des Verfahrens doch eine vollständige Anwendbarkeit des EuGH-Urteils auch in Deutschland bejaht, riskieren Websitebetreiber Abmahnungen, Unterlassungs- und ggf. Schadenersatzforderungen, wenn sie sich nicht an die europarechtlichen Vorgaben halten.

Übrigens soll angeblich auch das bisherige Cookie-Banner auf der Website des EuGH bislang nicht den selbst definierten Anforderungen genügt haben. Dies zeigt, dass die konkrete Umsetzung des Urteils noch einiger Arbeit in der IT-Praxis bedarf. //

PROF. DR. JULIUS REITER

DR. OLAF METHNER

Prof. Dr. Julius Reiter und Dr. Olaf Methner gründeten 2001 die heutige Kanzlei Baum Reiter & Collegen in Düsseldorf. Sie sind u. a. Fachanwälte für Informationstechnologierecht. Prof. Reiter ist zudem Mitglied der Regierungskommission „Mehr Sicherheit für Nordrhein-Westfalen“ („Bosbach-Kommission“) und Professor für Wirtschaftsrecht mit dem Schwerpunkt IT-Recht an der Hochschule für Oekonomie & Management.

_Internet Security Days

Messe

27. – 28. September 2019

Brühl

_expopharm

Messe

25. – 28. September 2019

Düsseldorf

_Digital FutureCongress

Messe

5. November 2019

Essen

_HEALTH – The Digital Leaders

Jahrestagung

5. – 6. November 2019

Berlin

_DATATREE AKADEMIE

Seminar: Kompaktkurs zum/r Datenschutzbeauftragten

15. November – 6. Dezember 2019

Dortmund

Informationstechnologien

Zwischen großen Herausforderungen und Chancen

Text: Jörg Fecke

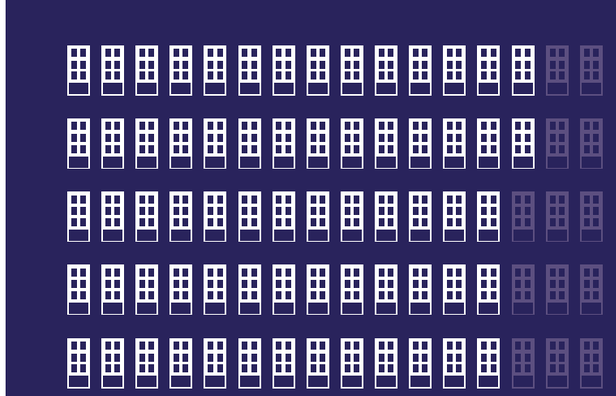
Mit der fortschreitenden Digitalisierung ändert sich die Art und Weise unseres Handelns grundlegend. Wie genau ist noch überhaupt nicht absehbar. Die Chancen, nachhaltige Entwicklungssprünge in fast allen Bereichen zu erreichen, sind schon jetzt enorm. Richtige Euphorie will sich allerdings in vielen Fällen nicht einstellen. Veränderungen erzeugen zwangsläufig Skepsis und Verlustängste. Darüber hinaus ist gerade hierzulande die Angst vor der allzu großen IT-Abhängigkeit sowie Angriffen und Manipulationen stark ausgeprägt. Dazu passt der diesjährige Lagebericht des BSI. Kurz zusammengefasst: Die Gefährdungslage bleibt weiterhin auf einem hohen Niveau!

Die Gefahrenlage spitzt sich zu

Die nackten Zahlen des Berichtszeitraums wirken auf den ersten Blick erschreckend. 114 Millionen neue Schadprogramm-Varianten hat das BSI registriert, Tag für Tag kommen 320.000 dazu. Um so wichtiger sind daher ein ausgeprägtes Sicherheitsbewusstsein und auch der Wille, in die eigene Sicherheitsarchitektur zu investieren. Viele Angriffe verlieren mit dem richtigen Bewusstsein ihren Schrecken – nach wie vor gelangen z. B. die meisten Schadsoftwares über Wechseldatenträger und externe Hardware in die infizierten Netze. Häufig spielt Social Engineering, also die Manipulation von Mitarbeitern, eine herausragende Rolle. Oft werden dabei mit der Unwissenheit und der daraus resultierenden Angst große Erfolge erzielt. Der Mensch ist auch im Zeitalter der Digitalisierung der entscheidende Faktor. Jeder Mitarbeiter, der sich der Gefahren bewusst ist und dementsprechend sein Verhalten anpasst, leistet einen enorm wichtigen Beitrag zu mehr Sicherheit. Das bedeutet allerdings auch, dass jeder, der sich allzu sorglos verhält, eine ernste Gefahr darstellen kann.

Ein kurzer Blick nach China zeigt, wohin die Reise in Sachen Digitalisierung und künstliche Intelligenz gehen kann. Im Vergleich dazu wirken die Diskussionen hierzulande wie aus einer anderen Welt. Personalisierte Begrüßung eines jeden Besuchers in der Boutique, der Check-in via Gesichtserkennung – alles schon längst Alltag im Reich der Mitte. Doch die bisherige Bilanz in China ist mindestens ambivalent. Wie schnell Bürgerrechte auf der Strecke bleiben und die Überwachung eines jeden Einzelnen durch ein – nach unseren Standards – totalitäres Regime gelingt, ist für die allermeisten dann doch der wahrgewordene Albtraum, den wir alle schon einmal geträumt haben.

Es liegt an uns, die Digitalisierung im Sinne der Bürger zu gestalten, mit Innovationen und Prozessen zu revolutionieren und so einen echten Mehrwert zu generieren. Probleme sind dazu da, um gelöst zu werden. //



87 %
der betroffenen Betriebe hatten Störungen und Ausfälle

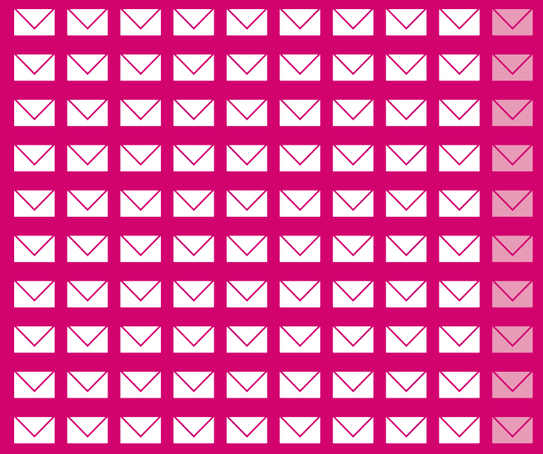
22 %
der Betroffenen verzeichneten Reputationsschäden

40 Mio.
Euro Schaden erlitt ein einzelnes Unternehmen durch Ransomware-Angriff

Die Gefahrenlage im Überblick

Zahlen, Daten, Fakten

Täglich
300.000
neue Schadprogramme



Bei
90 %
der Fälle dienten Anhänge oder Links in Mails als Übermittler der Schadsoftware

11,5 Mio.
Meldungen zu Infektionen übermittelte BSI an deutsche Netzbetreiber

Digitalisierung made in China

Der Preis des Wohlstandes wird mit Daten gezahlt.

Text: Jörg Fecke

Kennen Sie Tik Tok, Taobao, Alipay oder WeChat? Nein? Dabei handelt es sich um Anwendungen, die von bis zu einer Milliarde Menschen genutzt werden – täglich. Auf der anderen Seite des Planeten sind sie längst Teil des Alltags. In China bezahlt man inzwischen auf jedem Provinzmarkt via QR-Code, dank Alipay. Der Unialltag ist ohne WeChat gar nicht mehr möglich. Die Messenger-App ist mehr als nur eine schnöde Social-Media-App. Hier verabredet man sich zwar auch noch zum Lunch, darüber hinaus dient WeChat aber auch als Immatrikulationswerkzeug, Bibliothek und virtueller Hörsaal.

Gesellschaftlicher Wandel

Der Alltag der chinesischen Bevölkerung hat sich in den letzten 20 Jahren fundamental gewandelt. Zig Millionen sind aus ärmsten Verhältnissen auf ihrer Reise in der Mittelschicht angekommen. Allein 1,3 Millionen Millionäre leben in dem kommunistischen Reich. Das alles wurde nur durch einen enormen technologischen Fortschritt möglich. Und dieser Fortschritt schreitet weiter voran. Während hierzulande oft quälend lang über die Einführung einer Gesundheitskarte oder den Ausbau des Mobilfunknetzes diskutiert wird, wird es in China einfach gemacht. Kein Wunder, eine offene Diskussionskultur oder der Wille zum Konsens gelten im Reich der Mitte nicht gerade als gesellschaftliche Säulen.

Digitalisierung als Machterhalt

Womit ein gravierendes Problem des Systems „China“ offen zutage tritt: Die Machtelite, nach wie vor eine totalitäre Partei, sieht in der voranschreitenden Digitalisierung einen Schlüssel zum Machterhalt. Zwei Aspekte spielen dabei gleichermaßen eine Rolle. Die Bürger genießen die offensichtlichen Vorteile. Ein automatischer Check-in am Flughafen via Gesichtserkennung ohne lange Schlangen und Wartezeiten ist zweifellos eine schöne Sache. Datenschutzrechtliche Bedenken spielen nur eine untergeordnete Rolle. Das gilt für viele Bereiche des alltäglichen Lebens, ganz besonders auch im Bereich Finanzen. Wieso Millionen Deutsche nach wie vor einer Währung hinterhertrauern, die seit bald 20 Jahren Geschichte ist, kann im Reich der Mitte wohl niemand nachvollziehen. Bargeld? Braucht kein Mensch, viel zu fälschungsanfällig. Bankautomaten kosten zu viel Geld und sind störanfällig – heimische Banken würden die Dinger am liebsten auch sofort abschaffen, zu oft sind die Geräte Ziel von Kriminellen. Selbst der Bettler auf der Straße nutzt QR-Codes für Spenden und alles wird mit einem Lächeln bezahlt – smile to pay heißt die Anwendung.

Das bequeme Leben funktioniert aber nur mit einer Unmenge an Daten. Daten, die nicht den Nutzern gehören. Daten, deren Auswertung und Nutzung ein Anliegen des Einparteienstaates ist. Einerseits ist die Bevölkerung zufrieden mit einem spürbar besseren Lebensstandard, zumindest aus materieller Sicht, andererseits erhält die Partei anhand der Daten ein detailliertes Bild über jeden einzelnen Bürger. Den Kontrollfantasien sind dabei kaum Grenzen gesetzt. Seit einigen Jahren läuft in mehreren Großstädten Chinas ein Experiment – das Sozialpunktesystem. Die Grundlage auch hier: Daten!

Surfverhalten, Social-Media-Posts, aber auch die Steuererklärung, Schulnoten, selbstverständlich auch Straftaten – der Sammelei sind schier keine Grenzen gesetzt. Fehlverhalten wird sanktioniert, wer etwa zu Fuß eine rote Ampel ignoriert, erhält Minuspunkte. Science-Fiction? Keiner kann den gesamten öffentlichen Raum mit Kameras überwachen?

Bewertung per Punktesystem

Nichts ist unmöglich: Der "Spiegel"-Korrespondent Bernhard Zand lebt seit 13 Jahren in Peking. Wenn der Journalist sein Haus verlässt und die doch recht unscheinbare Wohnstraße entlangschlendert, dann zählt er innerhalb von 500 Metern 60 Kameras, die das Geschehen auf der Straße aufzeichnen. Das Sozialpunktesystem ist keine Fiktion mehr, in ein paar Monaten soll es auf das gesamte Land ausgeweitet werden. Vor einigen Tagen sorgte eine Meldung in westlichen Medien für Aufsehen: „23 Millionen Chinesen am Kauf von Zug- und Flugtickets gehindert" – da ist wohl jemand zu oft über eine rote Ampel gelaufen. Darüber hinaus wird Menschen der Zugang zu Sozialleistungen wie Krankenhausbesuchen, Studienplätzen oder Stellen im Öffentlichen Dienst verwehrt, Ansagen vor einem Telefonat weisen auf den schlechten Status des Gesprächspartners hin, regelmäßig werden Menschen mit vollständigem Namen, Adresse und ihren Missetaten öffentlich bloßgestellt. Doch wer bestimmt, welches Verhalten belohnt wird und welches eine Sanktionierung erfordert? Es scheint so, dass in China weiterhin gilt: Die Partei hat immer recht.

Die Zustimmungswerte in der Bevölkerung sind hoch, sehr hoch sogar. Eine Umfrage der Freien Universität Berlin unter 2200 Chinesen ergab, dass 80 Prozent der Befragten der Einführung positiv gegenüberstehen. Bedenken wegen mangelndem Datenschutz haben zwar auch viele Chinesen. Gesetzliche Grundlagen wie ein DSGVO-Äquivalent existieren im Reich der Mitte allerdings nicht. Zwar gilt seit 1. Juni 2017 ein Cybersicherheitsgesetz, allerdings dient dies vor allen Dingen staatlichen Stellen zur Kontrolle. Vorrangiges Ziel: Kontrolle über den Datenabfluss ins Ausland behalten und diesen möglichst verhindern. Ausländische Unternehmen zwingt es zu hoher Transparenz, teilweise bis zur Offenlegung von Quellcodes. Öffentliche Diskussionen finden quasi nicht statt. Wie auch? Die sozialen Medien werden selbstverständlich kontrolliert und eine kritische Haltung gegenüber der Partei birgt das Risiko des Punktabzugs im System – ein Teufelskreis. Die Diktatur der Daten, in China ist sie längst Realität. //

Schwachstelle Mensch

Das Spiel mit den Emotionen.

Text: Nina Richard

Herr Müller (Name geändert) aus der Finanzabteilung erhält eine E-Mail des Vorstands. Er sitze gerade in einer wichtigen Sitzung und müsse dringend eine Überweisung tätigen. Den Überweisungsschein mit seiner Unterschrift hat der Vorstand bereits beigefügt. Herr Müller hat ein paar Rückfragen zu der Überweisung und mailt ein paar Mal mit ihm hin und her. Nachdem alle offenen Punkte geklärt sind, überweist Herr Müller den Betrag. Was er nicht weiß: Er ist gerade Opfer einer Social-Engineering-Attacke geworden.

Was Herrn Müller passiert ist, nennt sich CEO-Fraud und ist bei Weitem kein Einzelfall, sondern betrifft zahlreiche Unternehmen. Tendenz steigend. Nach einer Umfrage der Unternehmensberatung pwc gaben 40 Prozent der Unternehmen an, bereits einen Versuch von CEO-Fraud festgestellt zu haben, 5 Prozent davon waren erfolgreich. Grundsätzlich klingen 5 Prozent Erfolgsrate aus unternehmerischer Sicht ziemlich gut. Problematisch ist allerdings, dass der wirtschaftliche Schaden erheblich für Unternehmen sein kann. Der Grund, weshalb solche Betrügereien funktionieren, ist so alt wie die Menschheit und tief in unserer Natur verankert. Die Methode ist altbewährt: Sie nutzt Emotionen. Emotionen, die zu unserer Bedürfnisbefriedigung beitragen. Die Grundbedürfnisse, wie schlafen, essen, sind bei den meisten Gesellschaftsschichten in Deutschland befriedigt. Sprich: Die wenigsten von uns haben echte Probleme. Wir leben in einer Wohlstandsgesellschaft, in der wir uns Gedanken über das Restaurant zur Mittagspause, den nächsten Urlaub oder sinnlose Gadgets machen. Nur so bekommen wir die Anerkennung unseres sozialen Gefüges. Das macht uns psychologisch angreifbar.

Social-Engineers arbeiten mit:

- Angst
- Sympathie/Vertrauen
- Hilfsbereitschaft
- Respekt vor Autoritäten

Viele Aspekte des Social Engineerings sind klassische Aspekte der Wirtschaftsspionage. Ein Social Engineer tarnt sich als übernervöser Bewerber und erzeugt Mitleid. Eine Person am Empfang zu bitten, ein Dokument des mitgebrachten und infizierten USB-Sticks auszudrucken, ist

in dieser Situation durchaus erfolgversprechend. Der falsche Techniker ist dagegen ein beliebtes Kostüm, um sich unerlaubt Zugang zum IT-Herzen, dem Serverraum zu verschaffen. Das Vorgehen bleibt in Variationen dabei immer gleich. Allerdings hat sich das Toolkit, mit dem Betrüger heute unterwegs sind, geändert: Denn Werkzeuge wie Software und Kommunikationstools verfügen über eine enorm hohe Komplexität, die kaum ein Nutzer noch durchschaut. Und dann ist da noch die Masse an Informationen, die auf uns einströmt. Um diese zu filtern und zu bewerten, bedarf es Konzentration, Aufwand und Zeit. Alles Dinge, die wir in unserer Schneller-höher-weiter-Instagram-Welt, in der wir auf den reinen Medienkonsum getrimmt sind, nicht mehr haben.

Sensibel werden – von wegen

„Unsere IT-Systeme sind heute so komplex, dass es am einfachsten ist, den Menschen zu hacken. Kriminelle nutzen hier angeborene Verhaltensweisen aus, um ihr Ziel zu erlangen“, meint Sascha Czech, Bereichsleiter IT-Sicherheit der Sana Kliniken AG. Aber das ist kein Grund, in Panik zu verfallen. Das von Experten empfohlene Zauberwort lautet: Awareness – auf deutsch Bewusstsein! „Awareness, das ist die Sensibilität für gewisse Problematiken in Bezug auf die Informationssicherheit“, sagt Max Wölk, Experte Informationssicherheit DATATREE AG.

Es geht für Menschen nicht darum, plötzlich allem und jedem zu misstrauen. Awareness soll nicht das Verhältnis zwischen Menschen zerstören – ganz im Gegenteil. Es soll jedem von uns Handlungssicherheit geben, wenn wir – und das macht uns menschlich – Fehler machen.

Ein entwickeltes und im Unternehmen gelebtes Awareness-Konzept kann hier den Betroffenen Handlungssicherheit geben und für Unternehmen, im wahrsten Sinne des Wortes, Gold wert sein.

Das strukturierte Erfolgsrezept:

Anfälligkeitsanalyse

Der erste Schritt ist der Risiko-Workshop, in dem allgemeine Risiken für das Unternehmen identifiziert, bewertet und priorisiert werden.

Awarenesskampagne 1

Darauf folgt der zweite Schritt, eine erste Awarenesskampagne zur Identifikation des Iststandes:

- Fake-Phishing-Mail
- CEO-Fraud o. Ä.
- persönlicher Zugang zu kritischen Unternehmensbereichen
- Abgriff von Daten bzw. Installation von Schadsoftware

Mitarbeiterbefragung

Hierbei handelt es sich um eine sehr gute Möglichkeit, um die Selbst- und Fremdwahrnehmung einer Unternehmung (und deren Mitarbeiter) sowie die Darstellung in der Benchmark zu ermöglichen.

Schulungskonzept

Anhand der Ergebnisse aus Schritt eins bis drei wird ein Schulungskonzept und Training entwickelt. Diese setzen genau dort an, wo Handlungsbedarf besteht. Hier wird den Mitarbeitern nicht nur die Arbeitsweise von Social Engineers nähergebracht. Sondern auch an den eigenen Schwächen gearbeitet und eine gemeinsame Fehlerkultur entwickelt. Ergebnis: Den Mitarbeitern werden Ängste genommen, das Selbstvertrauen, sich den Herausforderungen zu stellen, steigt signifikant.

Awarenesskampagne 2

In Anlehnung an die erste Awarenesskampagne erfolgt ein erneuter Durchgang von „Angriffsszenarien“. Gemäß der ersten Angriffsphase erfolgt eine Wiederholung ähnlicher Angriffe, um die Erfolgsquote der Trainings zu ermitteln.

Eine 100-prozentige Sicherheit existiert nicht: weder in IT-Systemen und schon gar nicht da, wo Menschen agieren. Muss es aber auch gar nicht. Wichtig ist, dass wir uns trauen, Dinge zu hinterfragen und zu überprüfen. Darüber hinaus muss Mitarbeitern die Angst vor dem Thema Informationssicherheit genommen werden. Dieser Aufruf darf sich jedoch nicht nur an die Mitarbeiter richten, sondern muss zum anderen von der Geschäftsführung mit der nötigen Management-Attention betrachtet werden. //

Literaturverzeichnis:
https://www.pwc.de/de/risk/pwc-wikri-2018.pdf

Das Geschäft mit der Erpressung

Genau hinschauen kann sich lohnen.

Text: Nina Richard

Als ich vor ein paar Tagen meine Mails abrufe, weckt eine Betreffzeile mein berufsbedingtes Interesse: Ihre persönlichen Daten sind gefährdet! Ändern Sie sofort Ihr Passwort! Der Inhalt hinterlässt ein gewisses Unwohlsein in meiner Bauchgegend. Kurz zusammengefasst: Man habe unter anderem Zugriff auf die Kamera meines PCs und vermeintliche sexuelle Abenteuer aufzeichnen können. Gegen die Zahlung einer „fairen“ Bitcoin-Summe erhalte ich allerdings die „faire“ Chance der Erpresser, dass entsprechendes Material eben nicht an all meine Geschäftskontakte verschickt wird.

Nach einem kurzen impulsiv-panischen Gedanken, erinnere ich mich daran, dass ich, nicht nur von Berufs wegen die Echtheit der E-Mail sofort hinterfragen sollte.

Mails nach dieser Strickart landen zu Hunderttausenden in unseren Postfächern. Erste Regel: Don’t panic! Überaus hilfreich sind außerdem ein paar Werkzeuge und psychologische Tricks, die jeder von uns erlernen und vor allen Dingen auch beherzigen sollte.

Textliche und inhaltliche Ungereimtheiten

Nicht selten sind solche E-Mails gespickt mit Grammatik- und Rechtschreibfehlern. Aber sowohl der Betreff als auch der Inhalt der E-Mail sind auf den ersten Blick fehlerfrei formuliert. Hier hat sich jemand also tatsächlich Mühe gegeben. Aber lassen Sie uns die Nachricht einmal Stück für Stück auseinandernehmen.

Von: "Adel Wessely" <adelwessely@reward.dispaint.monster>
Datum: 23. September 2019 um 21:57:48 MESZ
An: nina.richard@datatree.eu
Betreff: Ihre persönlichen Daten sind gefährdet! Ändern Sie sofort Ihr Passwort!
Antwort an: <adelwessely@reward.dispaint.monster>

Die Kopfzeile

Der Absender der E-Mail ist mir unbekannt und nutzt mit seiner Absenderadresse den Faktor Angst, indem er Begrifflichkeiten, wie reward dispaint monster nutzt. Mit der Wahl einer selbst kreierten Domain dieser Art, ist ein Erpresser zumindest beängstigender und anonymer als über eine gmx- oder hotmail-Adresse, die relativ simpel zurückzuverfolgen sind.

Hallo!

Ich bin ein Vertreter der Chaos-Hacking-Gruppe.
Im Zeitraum vom 24/06/2019 bis 23/09/2019 haben wir durch Hacken eines der DATATREE.EU-Mailserver Zugriff auf Ihr Konto nina.richard@datatree.eu erhalten.

Hallo!

Hier fällt auf, der Erpresser adressiert ausschließlich mit einem kurzen knappen „Hallo“. Die fehlende persönliche Ansprache ist ein Hinweis, dass der Autor dieser Nachricht den Namen seines Adressaten gar nicht kennt.

Genauer Zeitraum

Aufgrund der Nennung eines konkreten Zeitraumes und der dort aufgeführten Daten des Mailservers und der konkreten E-Mail-Adresse bekommt man kurz das Gefühl, dass diese Nachricht echt sein muss.

Die Wahrheit: Die „Hacker“, wie sie sich selbst bezeichnen, schreiben mich nicht mit meinem Namen an, da das Herausfinden eines echten Namens einer Person, die hinter einer Mailadresse steckt, um einiges aufwendiger ist, als automatisiert die Mail-Adresse und den Mailserver zu eruieren.

Haben Sie Ihr Passwort schon geändert?
Gut! Aber unser Programm fängt es jedes Mal ab. Und jedes Mal, wenn ich wir Ihr neues Passwort!

Durch den Zugriff auf Ihr E-Mail-Konto war es einfach, eine Verbindung zum Betriebssystem Ihres Geräts herzustellen.

Momentan sind uns alle Ihre Kontakte bekannt. Wir haben auch Zugriff auf Ihre Messenger und Ihre Korrespondenz.
Alle diese Informationen sind bereits auf meinem pendrive gespeichert.

Ziemlich konkret

Die Wahrheit: Lesen Sie nochmal, wie konkret dieser Abschnitt wirklich ist. Nämlich gar nicht. Dem Erpresser ist weder das Betriebssystem noch das E-Mailkonto bekannt. Falls hier konkrete Inhalte vorliegen würden, wäre das doch der Augenblick, in dem ein Hacker hier mal harte Fakten nennen würde, oder?

Wir sind uns auch Ihrer intimen Abenteuer im Internet bewusst.
Wir wissen, dass Sie Websites für Erwachsene lieben und wir wissen über Ihre Sexsucht Bescheid.
Sie haben einen sehr interessanten und einzigartigen Geschmack (verstehen Sie, was ich meine?).

Beim Durchsuchen dieser Seiten wird die Kamera Ihres Geräts automatisch eingeschaltet.
Was Sie sich ansehen, wird aufgezeichnet und auf unserem Server gespeichert.

Im Moment wurden mehrere kompromittierende Videoaufnahmen gesammelt.
Ab dem Moment, in dem Sie diesen Brief gelesen haben, erhalten alle Ihre Kontakte in diesem E-Mail-Posteingang und in Kurieren nach 120 Stunden diese Clips und Dateien zusammen mit der Korrespondenz.

Absolut unangenehm

Für den Fall, dass der Erpresser an ein menschliches Wesen gelangt ist, dem die Geheimnisse des Unternehmens egal sind, wird es jetzt nochmal unangenehm. Denn was könnte schlimmer sein, als das öffentliche Bloßstellen unseres Selbst, gepaart mit dem Verlust unserer gesellschaftlichen Anerkennung? Für die meisten von uns, handelt es sich hierbei um ein Horrorszenario. Aber auch hier gilt, Ruhe bewahren und den Text sorgfältig lesen. Hat es beim genauen Hinsehen nicht eher etwas von einem tollen Horoskop? Der Text lässt sich mit ein wenig Fantasie auf jeden beziehen.

Wenn Sie dies nicht möchten, überweisen Sie 2.000,00 Euro auf unser einzigartiges Bitcoin-Wallet.

Senden Sie genau:
0.22526537 BTC

zu unserer Bitcoin-Wallet:

37P7qWffKMSRRu8Q522beWXLLYuiryyx5w

Die Adresse unterscheidet zwischen Groß- und Kleinschreibung - kopieren Sie sie.

Dann geht’s ums Eingemachte…

Wir werden zeitlich unter Druck gesetzt, bekommen aber auch einen realistischen Zeitraum eingeräumt, um eine Summe von 2000 Euro zu zahlen. Und auch, wenn 2000 Euro eine beachtliche Summe sind, ist die Summe nicht utopisch hoch. Viele kommen hier ins Grübeln.

Du entscheidest ... Bezahle oder lebe in der Hölle mit Schande ...

Wir glauben, dass diese ganze Geschichte Ihnen beibringen wird, wie man die Geräte richtig benutzt!
Jeder liebt Websites für Erwachsene, aber Sie haben kein Glück.
Für die Zukunft - kleben Sie den Aufkleber einfach auf die Kamera Ihres Geräts, wenn Sie Websites für Erwachsene besuchen!

Pass auf dich auf!

Retter in der Not

Eigentlich will der Autor mir doch nur aus meinem selbstverschuldeten Schlamassel helfen. Ein Hauch von edlem Ritter. Letzendlich also ein gar nicht mal so schlechter Tipp. Allerdings findet auch hier ein gravierender Bruch in der Logik statt: Da ja darauf hingewiesen wurde, dass meine komplette Session gelesen und aufgezeichnet wurde, kann mich die Aussicht auf weniger verwackelte Videoaufnahmen nicht wirklich beruhigen.

DATATREE AUSBLICK – VERANSTALTUNGEN 2020

_DSB Kompaktkurs

Zertifikatslehrgang // Februar 2020 // Dortmund

Datenschutzexperten, Juristen und IT-Experten vermitteln an vier Seminartagen das gesamte relevante Wissen, damit die Teilnehmer sich bestens vorbereitet der Prüfung zum zertifizierten Datenschutzbeauftragten stellen können. Der nächste Kurs beginnt im Februar 2020.
Weitere Infos unter: www.datatree.eu

DATATREE AKADEMIE

_Meeting am Meer

Führungskräfte-Meeting // 4. – 6. März 2020 // Heiligendamm

Neben dem langjährigen Bundestagsabgeordneten Wolfgang Bosbach berichten zahlreiche weitere Spitzenkräfte aus Forschung, Klinikbetrieb und Digitalisierungswirtschaft über Chancen, aber vor allen Dingen Herausforderungen des Krankenhauswesens.
Weitere Infos unter www.meeting-am-meer.de

_Digital Change Management in Health

Seminar // 16. und 17. März 2020 // München

Der digitale Wandel ist neben anderen Branchen auch in der Gesundheitswirtschaft zur Konstante geworden. Das Seminar soll hier entscheidende Kompetenzen vermitteln. Raus aus dem futuristischen Buzzword-Bingo, rein in die ungeschönte Praxis! Digital Change Manager berichten ungeschönt aus ihrem Alltag.
Weitere Infos unter: www.euroforum.de/veranstaltungen/digital_change_management_maerz2020

Sollten meine Geschäftskontakte bis heute, keine intimen Abenteuer von mir übermittelt bekommen haben, war meine Einschätzung vermutlich nicht ganz falsch.

Auch wenn wir diese E-Mails an dieser Stelle in eine unterhaltsame Kategorie packen, sollten wir uns darüber im Klaren sein, dass durchaus ernstzunehmende Erpressungsmails existieren. Die folgenenden Punkte vermeiden zusätzlichen Ärger:

1. Fragen Sie bei Unsicherheit bei Ihrer IT-Abteilung nach, aber leiten Sie in keinem Fall eine solche E-Mail weiter, da sie potenziell Schadsoftware enthalten kann. Ganz egal, auf welche peinlichen oder strafbaren Inhalte innerhalb der Mail Bezug genommen wird. Hier besteht nämlich die Möglichkeit zu überprüfen, ob Externe z. B. Zugriff auf den Mailserver hatten.

2. Vorbeugen ist besser als Nachsorge, deshalb: Vorsicht bei Mails, in denen Sie aufgefordert werden, Ihre Daten einzugeben oder auf irgendwelche Links zu klicken. Auch hier gilt: Expertenrat einholen und vorher bloß nicht den Anweisungen Folge leisten.

3. Klicken Sie in keinem Fall auf einen Link, sofern sich einer in der Erpressungsmail befinden sollte. Dahinter könnte sich ein Verschlüsselungstrojaner befinden. Fragen Sie bei Ihrer IT-Abteilung nach. Sollten Sie doch auf den Link geklickt haben und Ihr PC verschlüsselt sich, ziehen Sie sofort das Stromnetz- sowie das Netzwerkkabel und melden den Vorfall umgehend Ihrer IT-Abteilung.

4. Nutzen Sie grundsätzlich für jeden genutzten Dienst, egal ob beruflich oder privat, individuelle Passwörter.

5. Das Abkleben der Kamera ist beliebt und beruhigt. Softwarelösungen können inzwischen genau so gut vor unbefugtem Zugriff schützen. Außerdem muss dann nicht immer der Aufkleber vor der nächsten Skype-Konferenz abgeknibbelt werden. Fragen Sie die Kollegen aus der IT nach Anwendungen, die eine manuelle Zustimmung von Kamera und Mikrofon für Drittprogramme voraussetzen.

Zu guter Letzt sollte uns immer bewusst sein, dass Hacking, digitale Erpressung und auch die digitale Inkompetenz, die sich mittlerweile in unserem alltäglichen Tun eingeschlichen hat, Themen sind, die uns alle beschäftigen. Erpressung wirkt nur, solange wir uns ebendiese Inkompetenz nicht eingestehen und uns aus Angst vor dem sozialen Gesichtsverlust nicht trauen, unsere Erfahrungen zu teilen. Bauen Sie deshalb Ihre Awareness weiter aus – das sind Skills, die Sie zwar nicht zu 100 Prozent vor solchen Angriffen schützen, Ihnen im Notfall allerdings die Handlungskompetenz mitliefern, um brenzlige Situationen richtig zu beurteilen und kompetent zu behandeln. //

Cloud-Hosting:

Augen auf bei der Anbieterwahl

IT betrifft alle Unternehmensaktivitäten

Text: Andreas Bachmann

Das Thema Cloud-Computing ist alternativlos. Kosten-, Nutzen- und Sicherheitsaspekte sind der Grund, weshalb Unternehmen der Cloud kaum noch aus dem Weg gehen können. Weniger als 30 Prozent geben an, dass Cloud-Hosting kein Thema für sie sei (Bitkom, KPMG). Trends für die kommenden Jahre vermuten Experten unter anderem in den Bereichen: Edge-Computing, in Kombination mit KI, oder Robotic Process Automation (RPA). Die Potenziale sind enorm. Zwischen all den Buzzwords ist es aus Unternehmenssicht nicht immer einfach, den Überblick zu behalten – und vor allem, sich auf das Wesentliche zu konzentrieren und in der Masse an Angeboten den richtigen Dienstleister zu finden.

Eines vorweg: Heutzutage gibt es kein standardisiertes Cloud-Modell, das sich für alle Unternehmen gleichermaßen eignet. Jeder muss hier ein individuelles Modell entwickeln, das zu den eigenen Anforderungen und Geschäftszielen passt. Nachdem in den letzten Jahren vor allem die Public-Cloud-Anbieter wie AWS oder Azure Erfolge verzeichnen konnten, kommen inzwischen immer öfter Private-Clouds zum Zug. Das liegt vor allem an den Datenschutz- und Compliance-Anforderungen, wie etwa DSGVO, Safe Harbor, Digital Privacy Act oder PIPEDA (Personal Information Protection and Electronic Documents Act).

Im letzten Jahr nutzten laut „Cloud-Monitor" von Bitkom Research und KPMG mehr als jedes zweite Unternehmen in Deutschland (55 Prozent) Private-Cloud-Computing. Auch Public-Cloud-Computing kam in 35 Prozent der Fälle zum Einsatz. Der größte Vorteil des Private-Cloud-Modells liegt in der höchstmöglichen Sicherheit. Nachteile hat das Modell allerdings auch. Betreibt ein Unternehmen seine Private Cloud als On-Premise-Lösung im eigenen Rechenzentrum, kümmert sich die eigene IT-Mannschaft um die Hardware. Dies verursacht Kosten im Personalbereich, bindet Kapazitäten und macht Unternehmen erstaunlicherweise oft langsamer. Wächst der Bedarf an Ressourcen, können diese nicht einfach ohne Weiteres skaliert werden. Vorab sind Investitionen in zusätzliche Hardware fällig, die gekauft und installiert werden muss.

Managed Cloud statt On-Premise

Nicht jedes Unternehmen kann jedoch Personal, Räumlichkeiten, Budget und vor allem die Expertise bereitstellen, um eine Private Cloud „On-Premise" zu installieren und zu betreiben. Alternativ werden externe Dienstleister beauftragt, um diese Aufgabe im Outsourcing zu übernehmen und Private-Cloud-Lösungen als Managed Cloud-Hosting zu realisieren. Solche Dienstleister richten für den Kunden eine eigene Umgebung in ihrem Serverpark ein, die ihm dann exklusiv zur Verfügung steht. Praktisch bedeutet dies: Alle Daten und Anwendungen befinden sich an diesem Ort.

Managed Cloud-Hosting kombiniert die Vorteile der Private Cloud mit denen der Public Cloud in einem innovativen Bereitstellungsmodell. Dadurch, dass sich die Lösung im Rechenzentrum eines externen Dienstleisters befindet, profitieren die Kunden von der Expertise und vor allem der leistungsfähigen, stets auf dem neuesten Stand gehaltenen Hardware. Der Serviceanbieter kann seine Ressourcen auf mehrere Schultern verteilen und verfügt dadurch über genügend geschulte Mitarbeiter und Hardware-Ressourcen. Anpassungen an gestiegene Kundenbedürfnisse sind so innerhalb kurzer Zeit möglich.

CHECKLISTE:

Der Weg zum passenden Outsourcing-Partner

Bereits mit einer kurzen Checkliste lässt sich relativ schnell die Spreu vom Weizen trennen. Zehn Aspekte sollten bei der Auswahl berücksichtigt werden:

- **Managed-Cloud-Portfolio:**
  Bietet der Anbieter Unterstützung von der Konzeption über die Migration bis zum Regelbetrieb und entwickelt die Plattform gemeinsam mit dem Auftraggeber konstant weiter?
- **Compliance:**
  Verfügt der Anbieter über alle wichtigen Zertifizierungen und bietet individuelle Auftragsdatenverarbeitungsverträge (AVV)?
- **Standort:**
  Liegen die Rechenzentren des Anbieters in Deutschland bzw. zumindest in der EU oder besteht das Risiko, dass die Daten in den USA lagern – Stichwort „Cloud Act"? Betreibt der Anbieter eigene Rechenzentren oder bedient er sich anderer Plattformen und verschleiert damit gegebenenfalls die eigentliche Datenhaltung?
- **Sicherheit:**
  Schützen die angebotenen Sicherheitsmaßnahmen (Firewall, Backup, Datenduplizierungen etc.) Ihre Applikationen und Daten umfassend vor unbefugten Zugriffen Dritter?
- **Unabhängigkeit:**
  Ist die Bereitstellung der Leistungen von Drittfirmen abhängig? Hier gilt es zu klären, wer im Falle eines Falles rechtlich verantwortlich ist.
- **Skalierbarkeit:**
  Kann der Dienstleister mit den Kundenwünschen wachsen?
- **Automatisierung:**
  Wie hoch ist der Grad der Automatisierung? Je einfacher Nutzung und Management der Cloud sind, umso besser.
- **Service-Level-Abkommen (SLA):**
  Sind sämtliche Cloud-Services rund um die Uhr verfügbar? Mit SLAs lässt sich das vertraglich vereinbaren.
- **Service-Management:**
  Ist ein persönlicher, mit dem Projekt vertrauter Ansprechpartner rund um die Uhr verfügbar?
- **Support:**
  Setzt der Anbieter neben einem Ticket-System auf kontinuierlichen Austausch und kurze Kommunikationswege (zum Beispiel via Chat, Direktdurchwahl oder „Jour fixes")?

Seriöse Anbieter für Cloud-Lösungen sollten **ALLE** oben aufgeführten Punkte abdecken.

Ist erst einmal die Entscheidung für das Private-Cloud-Modell und den ausgelagerten Betrieb bei einem Managed-Hosting-Provider gefallen, müssen die Verantwortlichen den für sich besten Dienstleister finden. Im Idealfall sollte dieser alle Anforderungen so umsetzen können, dass die Cloud-Migration und der anschließende Betrieb aller Applikationen reibungslos funktioniert und in kritischen Situationen sofort jemand reagiert. Nur wenn die Cloud und damit die Applikationen stabil laufen, werden Mitarbeiter so entlastet, dass sie sich auf ihre Kernaufgaben konzentrieren können.

Über die Kurzcheckliste hinaus (s. u. l.) hilft es, weitere Elemente der gewählten Cloud-Strategie zu betrachten. Dazu zählen Unternehmensziele und -vorgaben, gesetzliche Bestimmungen und bestehende Prozesse, aber auch der technische Stand der aktuellen Infrastruktur und Anwendungen.

Gute Lösungen gibt es nicht von der Stange

Ist die Entscheidung für einen Managed-Cloud-Hosting-Anbieter gefallen, sollte dieser am besten schon bei der Analyse (z. B. Risiko- und Datenschutzanalysen, Durchführung von ROI- und TCO-Auswertungen usw.) eingebunden werden. Die Private-Cloud-Lösung entfaltet ihr Potenzial am besten, wenn sich der Anbieter aktiv einsetzt. So sollte er die Cloud-Transition unterstützen, den Cloud-Betrieb verantworten und die Lösung effektiv weiterentwickeln können.

Die Entscheidungskriterien für den richtigen Provider sind vielschichtig. Es ist ein gutes Zeichen, wenn sich der Anbieter als Partner präsentiert und eine enge Kooperation anstrebt. Das Angebot sollte darüber hinaus die Betriebsverantwortung für Teile der Cloud umfassen, gemanagte Services beinhalten sowie agile Arbeitsweisen und Automatisierung berücksichtigen. In der Praxis entscheiden sich Unternehmen meist für einen erfahrenen Anbieter, der eine Private Cloud mit komplexen Anforderungen mithilfe von maßgeschneiderten Komponenten bereitstellen kann.

Natürlich spielen bei all dem die Kosten immer eine wichtige Rolle. Da jedoch die Cloud am Ende des Tages die wichtigsten Daten und Anwendungen „hostet" und damit das Herz der meisten Unternehmen ist, sollten die Kosten nicht das ausschlaggebende Element sein. Die hier aufgeführten Aspekte verdeutlichen, auf was es alles ankommt. Gute Dienstleister für Managed Cloud-Hosting gibt es nicht wie Sand am Meer, aber es gibt sie und mit der richtigen Checkliste und genügend Gesprächen im Vorfeld lassen sie sich finden. //

ANDREAS BACHMANN

ist CIO und Mitgründer von Adacor Hosting. Als Geschäftsführer verantwortet er die Bereiche Softwareentwicklung, Marketing, Datenschutz und Compliance. Aktuell entwickelt er eine Reihe von Serviceleistungen für Konzerne und Unternehmen aus dem gehobenen Mittelstand zur schlüsselfertigen Bereitstellung von teilindividualisierten Cloud-Lösungen.

Sozialdaten in die Public Cloud?

Eine Risikobewertung.

Text: Sven Thimm

Cloud-Dienste externer Anbieter sind immer häufiger die „verlängerte Werkbank“ der eigenen IT. Eine Berücksichtigung im eigenen Sicherheitskonzept sowie geeignete Schutzmaßnahmen sind daher unerlässlich. Dies betrifft gerade besonders schützenswerte Sozialdaten z. B. von Krankenkassen oder Gesundheitseinrichtungen.

Verschlüsselung stellt einen zentralen Bestandteil der Schutzmaßnahmen dar. Dazu muss man wissen, dass ernstzunehmende Cloud-Anbieter Verschlüsselung bereits überall dort einsetzen, wo es möglich ist. Dies betrifft vor allem Datenträger wie Festplatten – aber auch sämtliche Transportwege innerhalb der Rechenzentren oder den Weg von und zum Kunden. Ein Schutz vor unbefugtem Zugriff durch Dritte ist also de facto bereits per Design implementiert. Ein häufiger Kritikpunkt an der integrierten Verschlüsselung ist, dass die Sicherheitslösung sozusagen von dem Cloud-Anbieter selbst betrieben wird. Implizit steckt dahinter die Frage, ob es dadurch nicht doch zu einem unbefugten Zugriff kommen kann.

Bei allen Überlegungen rund um den Einsatz von Verschlüsselung und weiterer Sicherheitstechnologien muss immer eine Abwägung der tatsächlich zu erwartenden Risiken erfolgen. Eine maximal erreichbare Sicherheit anzustreben, ist zwar nachvollziehbar – kann aber einen negativen Effekt auf die Wirtschaftlichkeit haben.

In einem Kundenszenario bei einem Sozialversicherungsträger wird beispielsweise Microsoft Azure Information Protection (AIP) zur zusätzlichen Verschlüsselung verwendet. Durch den Einsatz solcher Schutztechnologien können sensible Daten aller Art einfach verschlüsselt werden. Eine weitere Funktion ist die Klassifizierung von Informationen nach vom Kunden definierbaren Bezeichnungen. So können Organisationen eigene Label für unterschiedliche Schutzstufen implementieren.

Eine Alternative ist die Verwendung von Schlüsseln, die vom Kunden verwaltet werden. Dieses Verfahren führt zu einem signifikanten Sicherheitsgewinn, da der Cloud-Anbieter zwar noch das eigentliche Verschlüsselungsverfahren betreibt – aber keinerlei Zugriff auf den Mandantenschlüssel oder davon abgeleitete Schlüssel hat. Allerdings entstehen auch in diesem Szenario zusätzliche Kosten und administrative Tätigkeiten. Verfahren zur kundenseitigen Verwaltung von Schlüsseln und sogenannte Schlüsseltresore werden von verschiedenen Cloud-Anbietern angeboten.

Ökonomische Effekte und strategische Abwägungen

Grundsätzlich sind alle Entscheidungen von Sozialversicherungsträgern strengen Anforderungen hinsichtlich der Wirtschaftlichkeit unterworfen. Dies gilt auch für Überlegungen hinsichtlich des Einsatzes von Cloud-Diensten. Allerdings ist Wirtschaftlichkeit nicht allein ausschlaggebend: Es gilt auch zu verhindern, dass es zu strategischen Abhängigkeiten oder weiteren negativen Effekten kommt.

Im § 80 SGB X werden daher nur zwei mögliche Begründungen für die Nutzung von Cloud-Services nichtöffentlicher Stellen benannt:

1. beim Verantwortlichen können sonst Störungen im Betriebsablauf auftreten – oder
2. die übertragenen Arbeiten können beim Auftragsverarbeiter erheblich kostengünstiger besorgt werden.

Public Cloud Services basieren auf einer massiven Skalierung und einem stark automatisierten Betrieb. Allein aus diesem Grund ist die Wirtschaftlichkeit extrem hoch und ökonomische Effekte sind entsprechend positiv zu bewerten. Allerdings erfüllt eine pauschale Aussage nach dem Motto „in der Cloud ist alles billiger“ nicht die gesetzlichen Anforderungen an eine detaillierte Analyse der ökonomischen und strategischen Effekte.

Der Nutzer der Cloud-Dienste muss also eine umfassende Analyse der wirtschaftlichen Effekte durchführen. Dabei sind nicht nur die direkten Lizenzkosten miteinander zu vergleichen, sondern die Gesamtkosten bzw. der „Total Economic Impact“ ist zu berücksichtigen. Grundlage dafür muss eine detaillierte Betrachtung des Leistungsumfanges der Cloud-Services sein: Mit einem Mail-Server als Software-as-a-Service-Angebot sind beispielsweise in der Regel auch Sicherheitslösungen wie Viren- und Spamschutz und oft auch Back-up und Archivierung kombiniert. An dieser Stelle spielt auch wieder die übergeordnete IT-Roadmap eine zentrale Rolle: Welche Services will man zukünftig noch selbst betreiben und wo gibt es eine strategische Entscheidung Richtung Cloud?

Individuelle Analyse notwendig

Gesetze, Regularien und deren Auslegungen sind zentrale Komponenten in den Überlegungen und Abwägungen zum Thema Cloud-Nutzung. Diese Dinge sind im Fluss und können sich ändern. Die Welt um uns herum ist nicht statisch, sondern verändert sich ständig. Aufgrund des wichtigen gesetzlichen Auftrages ist es daher legitim zu fragen: Was passiert, wenn sich massive Veränderungen ergeben?

Es könnte z. B. passieren, dass sich die Bewertung von Ländern mit angemessenem Datenschutzniveau verändert. Technologische Innovationen können ebenfalls massive Auswirkungen mit sich bringen. So gehen Sicherheitsforscher heute davon aus, dass mit der Marktreife von Quantencomputern zahlreiche Verschlüsselungsmechanismen als nicht mehr sicher eingestuft werden können. Für genau diese Fälle braucht man einen Plan B in der Schublade.

Fazit:
Nach wie vor gilt, dass Sozialdaten ein besonders hohes Schutzniveau haben und daher ein sorgfältiger Umgang mit ihnen zwingend erforderlich ist. Bei sorgfältiger Planung, bei Berücksichtigung der Empfehlungen des BVA und nach sorgfältiger Analyse in Verbindung mit der Erstellung der notwendigen Dokumentationen ist die Nutzung der Cloud auch für die Verarbeitung von Sozialdaten möglich. //

SVEN THIMM

Sven Thimm ist seit 2017 technologischer Strategieberater für Kunden im Bereich des öffentlichen Gesundheitswesens. Zu seinen Kunden gehören Gesetzliche Krankenversicherungen, Berufsgenossenschaften und Kassenärztliche Vereinigungen.

Das sagt der DSB:

Prof. Dr. Thomas Jäschke

Für die Datenverarbeitungen in Cloud-Services gibt es keine Pauschallösung und bedarf somit immer einer individuellen Betrachtung des Sachverhalts. Mitunter ist die Nutzung anhand folgender Fragen zu bewerten: Welche Daten verarbeitet werden sollen? In welchem Land stehen die Server? Unterliegen die Daten einem Berufsgeheimnis? Auch zieht ein positiver Entschluss weitere Aufgaben mit sich, wie die Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten, die Durchführung einer Datenschutz-Folgenabschätzung oder die Einbeziehung einer Datenschutz-Aufsichtsbehörde.

SCHWERPUNKT DER
MÄRZAUSGABE 2020:

Zertifizierung

Impressum

ExperSite Ausgabe 04 2019 | **ISSN-Print** 2364-5636 | **ISSN-Internet** 2364-5644 | **Herausgeber:** DATATREE AG, Heubesstraße 10, 40597 Düsseldorf, T +49 211 93190-700, F +49 211 93190-799, office@datatree.eu, www.datatree.eu | **Sitz der Gesellschaft:** Düsseldorf | **Registergericht:** Amtsgericht Düsseldorf | **Registernummer:** HRB 66132 | **Umsatzsteuer-Identifikationsnummer:** DE 279402614 | **Vorstand:** Prof. Dr. Thomas Jäschke | **Vorsitzender des Aufsichtsrates:** Prof. Dr. Julius Reiter | **Inhaltlich Verantwortlicher gemäß § 1 Abs. 4 TMG, § 55 Abs. 1 RStV und § 55 Abs. 2 RStV:** Prof. Dr. Thomas Jäschke | **Redaktionsleitung:** Nina Richard | **Design und Umsetzung:** Julia Kleineberg | **Druck:** Druckerzeugnisse Gerbrunn | **Auflage:** 5.000 | **Fotos:** Titelbild: iStock, PeopleImages; S. 2: o.: unsplash, denys-nevozhai; Zeichnung: shutterstock, retrorocket; u. li. pixabay, vvadyab; S. 3: Tom Schulte, Oberhausen; S. 4-6: Julia Kleineberg, Dortmund; S. 8. pixabay, OpenClipart-Vectors; S. 9: pixabay, StockSnap; S. 10: Tom Schulte, Oberhausen; S. 12: pixabay, Erich Westendarp; S. 13: Kanzlei Baum Reiter & Collegen, Düsseldorf; S.14-15: v. o. n. u. Jörg Fecke, Dortmund, Julia Kleineberg, Dortmund; ©Uta Wagner, Köln; Julia Kleineberg, Dortmund; S. 18-19: unsplash, denys-nevozhai; S.21-22: shutterstock, retrorocket; S. 23: iStock, PeopleImages; S. 24-25: pixabay, ChrisFiedler; S. 26: pixabay, ChrisFiedler; euroforum Deutschland GmbH, Düsseldorf; S. 27: pixabay, vvadyab; S. 29: Tim Frankenheim, Adacor Hosting GmbH; S. 30-31: unspalsh, Thomas Lefebvre; S. 31: Microsoft Deutschland GmbH, Köln; Tom Schulte, Oberhausen; unsplash, CIker-Free-Vector-Images; S.32: unsplash, pierre-chatel-innocenti.