LOOKING OUT FOR YOU ONLINE

STRATEGIEN ZUM SCHUTZ VOR CYBER-KRIMINALITÄT

WHITEPAPER

owl

INHALT

Strategien zum Schutz vor Cyber-Kriminalität

Sicherheit von Verbraucherdaten im Netz ..... S. 3

Mögliche Handlungsfelder

- IT-Sicherheit in Unternehmen: Vorgehen und Herausforderungen ..... S. 5
- Internet der Dinge oder Industrie 4.0: wachsende Datensammlungen und Angriffsflächen ..... S. 6
- Staatliche Regulierung ..... S. 6
- Ein nutzerfreundliches Sicherheitskonzept ..... S. 7

Fazit ..... S. 7

Quellen ..... S. 8

EXECUTIVE SUMMARY

Die zunehmende Digitalisierung von Diensten, Transaktionen und Prozessen bietet vermehrt Angriffsflächen für Cyber-Kriminalität.

Verbesserte IT-Sicherheit in Unternehmen, staatliche Regulierung, eine transparente Aufklärung der Verbraucher und nutzerfreundliche Services können unerwünschte Zugriffe eindämmen und Datenklau vorbeugen.

Eine Möglichkeit, mit der sich Onliner selbst schützen können, sind effektive und leicht zu bedienende Datenmonitoring-Services.

SICHERHEIT VON VERBRAUCHERDATEN IM NETZ

Immer mehr Services werden heutzutage online genutzt. Neben der E-Mail werden unter den Internetservices vor allem Nachrichtenportale und soziale Netzwerke aber auch Online-Shopping regelmäßig verwendet.[1] Die meisten Online-Dienste erfordern die Erstellung einer Nutzer-Kennung unter Angabe verschiedener persönlicher Daten bis hin zu Zahlungsinformationen, wie Kreditkartendaten oder einer Bankverbindung.

Obwohl die Eingabe persönlicher Daten im Netz für 78% der Deutschen ein Teil des modernen Lebens geworden ist,[2] sind 76% der Konsumenten eher besorgt und vorsichtig im Umgang mit ihren persönlichen Daten im Internet.[3] Dies zeugt von einem gewissen Misstrauen im Umgang mit Online-Diensten.

Weiterhin befinden sich Verbraucherdaten, welche nicht online eingegeben wurden, auf Servern von Unternehmen, wie beispielsweise Gesundheitsdaten bei Krankenkassen, persönliche Daten bei staatlichen Organisationen oder auch gesammelte Daten der Produkte aus dem Internet der Dinge.

Auf diese Weise werden persönliche Daten auf verschiedensten Servern weltweit gesammelt und gespeichert. Für den Verbraucher ist es daher schwer nachvollziehbar, welche persönlichen Daten bei welchem Unternehmen liegen und wie diese dort geschützt sind. Zusammengefasst zieht dies die Gefahr nach sich, dass durch Angriffe von Kriminellen auf Unternehmen oder Privatpersonen persönliche Daten unerlaubt entwendet werden.

So können unachtsame Verbraucher beispielsweise Opfer von Phishing-Attacken oder das verwendete internetfähige Endgerät mit Schadsoftware, wie Spyware infiziert werden. So wurden alleine im letzten Jahr 9,4% der Onliner Opfer von Kauf- bzw. Buchungsbetrug, während 12,5% ein, mit Viren befallenes, Gerät zu verzeichnen hatten.[4] Dies lässt auf eine große Zahl bereits kompromittierter persönlicher Daten schließen, welche im Umlauf sind.

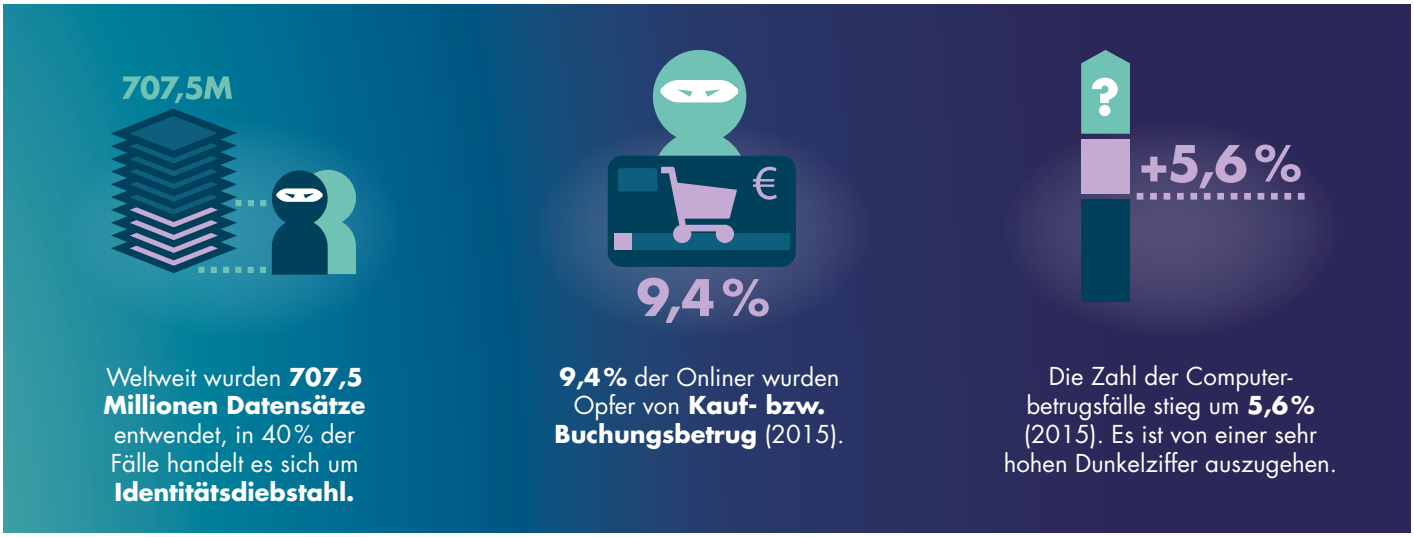
Das bestätigt auch der aktuelle „Gemalto Breach Level Index“[5] zu Datenlecks in Unternehmen:

- **707,5 Millionen** entwendete Datensätze weltweit bei gemeldeten Lecks
- Davon nur **4% verschlüsselt** gespeichert
- Angriffe aus **externen Quellen** (37%), **unbeabsichtigte Datenweitergabe** (36%)
- Bei **47%** der Lecks **keine Angaben zur Menge** entwendeter Daten
- Vor allem **Regierungsorganisationen** (43%) und **Gesundheitssektor** (19%) betroffen
- Mit **40%** der Datensätze ist **Identitätsdiebstahl** weiterhin Hauptgrund für Datenraub

Gestohlene Daten werden entweder missbräuchlich verwendet oder aufgrund der Anonymität, die es bietet, im Darknet gehandelt, was meist zum selben Ergebnis führt.[6] 63% der Onliner haben Angst, dass genau das mit ihren persönlichen Daten passiert.[7] Zusätzlich ist mit über 23.000 Fällen von Computerbetrug im Jahr 2015 ein Zuwachs von 5,6% zu verzeichnen, während das BKA insbesondere im Darknet von einer deutlich höheren Dunkelziffer ausgeht.[8]

Dementsprechend sorgen sich mehr als 60% der Internetnutzer, Opfer eines Identitätsdiebstahls zu werden.[9] Dabei möchten 88% der Onliner ihre persönlichen Daten besser schützen. Hierfür würden 39% einen Datenmonitoring-Service nutzen[10], während 68% generell mehr Informationen zu den Möglichkeiten des Datenschutzes benötigen.[11]

Der Schutz persönlicher Daten vor unautorisiertem Zugriff und illegalem Handel gestaltet sich durch den stetigen technologischen Fortschritt als Herausforderung. Die Verbraucher sind verunsichert. Dabei sehen 72% der Onliner vor allem die Unternehmen, bei denen die Daten gespeichert sind und 69% sich selbst in der Pflicht für angemessenen Datenschutz zu sorgen.[12]



MÖGLICHE HANDLUNGSFELDER

Immer innovativere Angriffsmethoden treffen auf immer effektivere Sicherheitsmechanismen. Erst ein Zusammenspiel von technologischem Fortschritt, staatlicher Regulierung sowie Aufklärungsmaßnahmen bei Verbrauchern und Mitarbeitern macht es möglich, die Datensicherheit deutlich zu erhöhen.

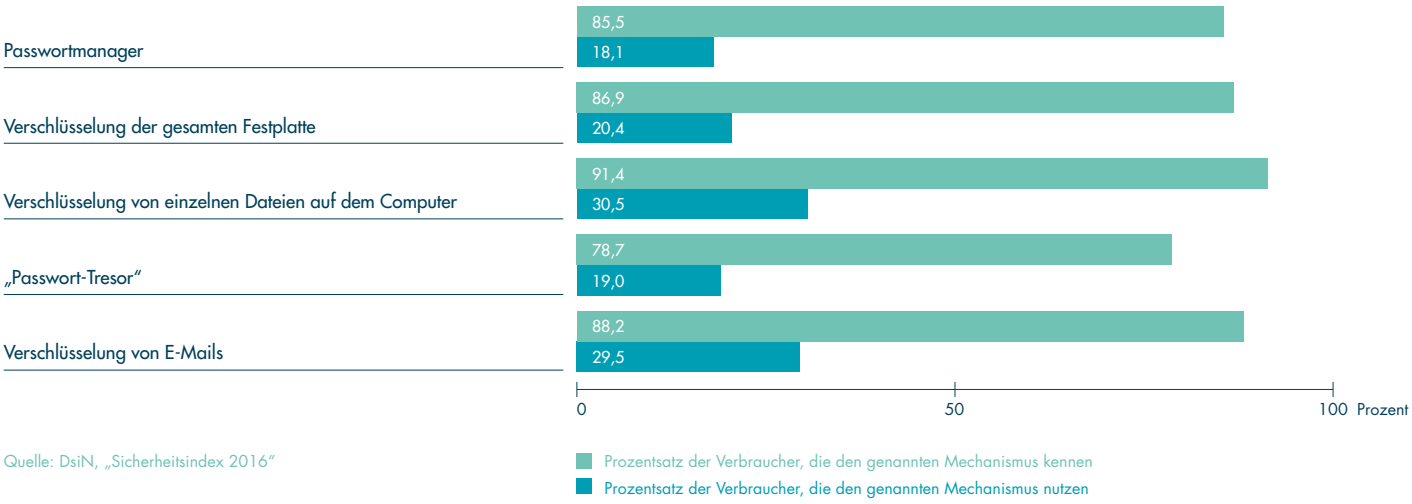
Unternehmen sind in der Verantwortung zu informieren

Aus Sicht des Vereins „Deutschland sicher im Netz" ist es nötig, die Sicherheitskompetenz des einzelnen durch leicht verständliche Informationen zu fördern, um Daten effektiv zu schützen. Auch die Nutzer sind der Meinung, dass sie selbst für adäquaten Datenschutz verantwortlich sind.

Zwar haben sich die deutschen Onliner in grundlegenden Bereichen des Datenschutzes bereits ein umfangreiches Wissen angeeignet. Die hier aufgeführte Graphik zeigt jedoch, dass Kompetenz im Umgang mit komplexeren Schutzvorkehrungen vermittelt werden muss, da diese offenbar nur von wenigen Nutzern eingesetzt werden. Damit die Konsumenten diese digitalen Schutzmaßnahmen nicht nur kennen, sondern auch anwenden, sollten deren Nutzen und Effektivität besser und häufiger erläutert werden. Darüber hinaus ist es empfehlenswert, die Folgen von unzureichendem Datenschutz deutlicher zu kommunizieren. Zudem könnten die Unternehmen für einfach zu bedienende Sicherheits- bzw. Privatsphäre-Einstellungen bei digitalen Diensten sorgen und damit ihr verbraucherorientiertes Datenschutz-Konzept abrunden.[13]

Gleiches gilt auch für die Mitarbeiter von datenverarbeitenden Unternehmen. Es ist besonders wichtig, sie für die Folgen nachlässigen Handelns beim Datenschutz zu sensibilisieren und regelmäßig über neuartige Bedrohungen und Schutzmethoden zu informieren.[14]

Kenntnis versus Nutzung – Schlusslichter



Quelle: DsiN, „Sicherheitsindex 2016"

IT-SICHERHEIT IN UNTERNEHMEN: VORGEHEN UND HERAUSFORDERUNGEN

Im ersten Schritt gilt es, zu analysieren, welche Kundendaten sich im Unternehmen befinden und welche davon geschützt werden müssen. Diese Analyse ist eine zentrale Voraussetzung, um zu identifizieren, welche technischen Sicherungsmaßnahmen notwendig sind und welche Datenschutzkompetenz der Mitarbeiter erforderlich ist.[15]

Eine besondere Gefahr geht von APTs (Advanced Persistent Threats) aus, auch targeted attacks genannt. Bekannt geworden ist diese Bedrohung durch den Angriff auf Sony, Epsilon und RSA. Dabei handelt es sich um komplexe, zielgerichtete Angriffe auf IT-Infrastrukturen und vertrauliche Daten. Hierbei investieren die Täter viel Zeit, Arbeit und auf das Opfer konkret ausgerichtete, spezielle Werkzeuge, um die Schutzmaßnahmen eines Computersystems auszuhebeln und weiter in die IT-Infrastruktur vorzudringen. APTs sollen möglichst lange im Verborgenen bleiben, damit sie unter anderem eine möglichst große Datenmenge ausspähen, Daten unbemerkt kopieren oder Steuerkommandos von Industrieanlagen oder Smart Homes manipulieren können.[16] Besonders gefährdet sind hier Betreiber von kritischen IT-Infrastrukturen wie Banken, Versicherungen oder auch Telekommunikationsunternehmen.

Aufgrund der Komplexität und Einzigartigkeit der APTs sind herkömmliche Schutzmechanismen meist uneffektiv. Ein ganzheitlicher Ansatz zum Schutz der IT-Infrastruktur stellt das Konzept Cyber Kill Chain dar, das erstmals 2011 von Lockheed Martin beschrieben wurde und von WatchGuard Technologies unter dem Namen Kill Chain 3.0 für die Bekämpfung von APTs angepasst wurde. Hierbei werden Cyber-Angriffe in 7 Stufen aufgeteilt, jeder einzelnen Stufe werden konkrete Abwehrmaßnahmen entgegen gestellt.

Beispielsweise helfen Port-Analyse und IP-Erkennung gegen die Auskundschaftung. Die Zustellung kann durch IPS (Intrusion Prevention Services) verhindert werden und regelmäßige Software-Updates beugen Schwachstellen auf Zugriffslevel vor. Wurden die ersten Verteidigungsmaßnahmen ausgehebelt, kann eine Netzwerksegmentierung die horizontale Ausbreitung von Eindringlingen verhindern.[17]

Eine Reihe von Angreifern versucht durch Social Engineering Mitarbeiter so zu manipulieren, dass diese ihnen Zugang zum System verschaffen. Um solch unberechtigte Zugriffe zu verhindern, ist es erforderlich, alle, die auf das Firmennetzwerk zugreifen, umfassend aufzuklären und zu informieren.

Weiterhin zeigt der „Gemalto Breach Level Index", dass ein verstärkter Fokus von IT-Abteilungen darauf liegen muss, Daten verschlüsselt zu speichern, um selbst bei einem unrechtmäßigen Zugriff den Schutz der betroffenen Daten zu gewährleisten.[18]

Cyber Kill Chain nach WatchGuard Technologies: Jeder Stufe eines Cyber-Angriffs werden entsprechende Gegenmaßnahmen zugeordnet.[17]

INTERNET DER DINGE ODER INDUSTRIE 4.0: WACHSENDE DATENSAMMLUNGEN UND ANGRIFFSFLÄCHEN

Mit dem Internet der Dinge (Internet of Things, kurz IoT) verschwimmen die Grenzen zwischen der realen und virtuellen Welt, denn das Internet interagiert nun mit dem Menschen und seiner Umgebung. Im Zuge des IoT können Unternehmen außerdem Produktionsprozesse vernetzen. Damit wurde die vierte industrielle Revolution eingeläutet. Sie heißt Industrie 4.0, auch bekannt als das Internet der Ingenieure. Durch Nutzung von Sensoren und Web-Diensten zur Datenübermittlung zwischen Menschen, Maschinen und Produkten kann das Internet der Dinge die Produktivität in der Industrie und die Customer Experience auf vielfältige Weise optimieren. Laut Deloitte wird der deutsche Markt für das Internet der Dinge bis 2020 ein Umsatzvolumen von 50 Mrd. Euro generieren. Das Sammeln und Nutzen großer Datenmengen sowie die Steuerung von Geräten über mobile Endgeräte, wie Smartphone sind charakteristisch für das Internet der Dinge. Das hat zur Folge, dass neue Angriffsmöglichkeiten für Datendiebstähle über Sicherheitseinbrüche und Cyberangriffe entstehen, die sowohl ein Risiko für Unternehmen als auch für Verbraucher darstellen.[19]

Aufklärungsmaßnahmen sind vor diesem Hintergrund nicht mehr ausreichend. Vielmehr spielen im Kontext von IoT einheitliche Sicherheitsstandards zur Authentifizierung, Steuerung und Verschlüsselung der gesammelten Daten eine übergeordnete Rolle. Wenn Unternehmen planen, Geräte einzusetzen, die sich mit dem Internet verbinden, dann ist bei der Wahl des Anbieters dieser Geräte auf deren jeweilige Sicherheitsstandards zu achten, denn sie arbeiten mit unterschiedlichen sog. Embedded Betriebssystemen. Diese sehr speziellen Betriebssysteme benötigen aufgrund der begrenzten Kapazität der Geräte, nur einen geringen Speicherplatz. Diese Ressourcenbegrenzung erschwert es, umfängliche Sicherheitsmechanismen zu integrieren.[20]

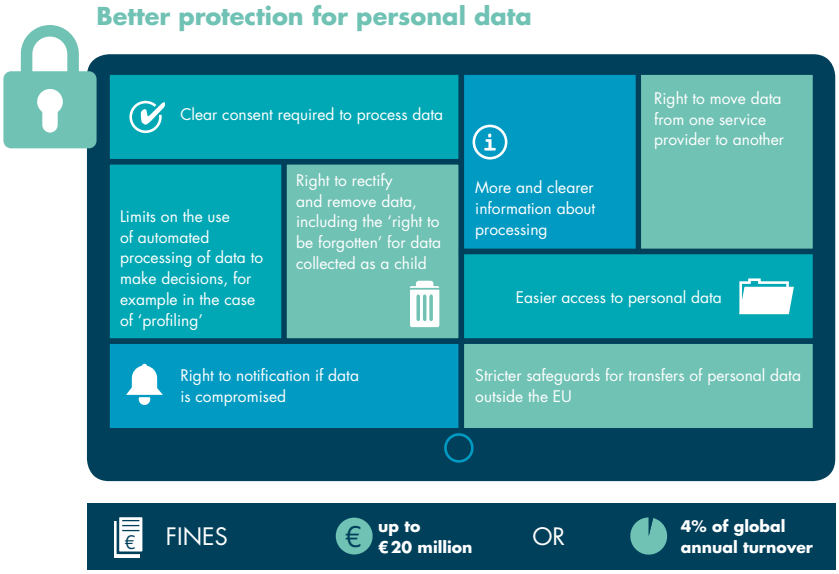
STAATLICHE REGULIERUNG

Der Schutz persönlicher Daten ist auch bei den regulatorischen Instanzen in Deutschland und der EU eines der Schlüsselthemen der Digitalisierung. Die erst kürzlich verabschiedete EU-Datenschutz-Grundverordnung[21] behandelt viele kritische Themen der jüngsten Zeit und ist stark verbraucherorientiert. Sie sieht u. A. Folgendes vor:

Mit dem „Recht auf vergessen werden" besteht der Anspruch auf eine Berichtigung bzw. auch Löschung von persönlichen Daten. Eine solche Löschung ist möglich, wenn keine legitimen Gründe für eine weitere Speicherung vorliegen oder die Datenspeicherung gegen geltendes Recht verstößt. Weiterhin wird die Meldepflicht (Data Breach Notification) für Unternehmen bei kompromittierten Daten verschärft. Ein solcher Angriff muss innerhalb von 72 Stunden bei der zuständigen Aufsichtsbehörde gemeldet werden und gilt nicht mehr nur für sogenannte Risikodaten, sondern jegliche kompromittierte persönliche Daten. Die gleichen Regelungen gelten ebenfalls für staatliche Einrichtungen. Stellt der Datenmissbrauch ein hohes Risiko dar, müssen die jeweiligen betroffenen Konsumenten unverzüglich informiert werden. Ebenfalls werden in Zukunft US-Unternehmen an EU Datenschutzrecht gebunden sein, wenn sie Produkte auf dem europäischen Markt anbieten.

Der in der EU-Datenschutz-Grundverordnung neu eingeführte Punkt „Öffentlichkeitsarbeit" sieht vor, dass Aufsichtsbehörden in Zukunft über datenschutzrelevante Themen wie z. B. Risiken in der Datenverarbeitung informieren sollen, ähnlich, wie es auch schon im deutschen Recht auf informationelle Selbstbestimmung festgelegt ist. Viele Maßnahmen des Selbstdatenschutzes, wie Verschlüsselungstechniken, schränken auch die staatlichen Möglichkeiten der Überwachung ein und können folglich die öffentliche Sicherheit beeinträchtigen. Hierdurch ist ein Interessenkonflikt zwischen Informationsauftrag und staatlichen Überwachungsinteressen entstanden.[22]

Es bleibt abzuwarten, inwiefern diese Verordnung in der Praxis umgesetzt wird. Die möglichen Strafen im Falle von Verstößen werden im Idealfall dafür Sorge tragen, dass Unternehmen mit angemessener Sorgfalt die persönlichen Daten von Verbrauchern schützen. Optimal scheint eine Lösung, welche den Verbraucher ganzheitlich zu einem sicheren Umgang mit dem Internet befähigt oder auf technologischem Weg über persönliche Daten wacht.



Quelle: European Union, 2015

EIN NUTZERFREUNDLICHES SICHERHEITSKONZEPT

Der Datenmonitoring-Service Owl befähigt einerseits den Verbraucher, sich sorgenfrei im Internet zu bewegen und andererseits wacht die Owl-Technologie über die persönlichen Daten.[23] Zur Vorbeugung bietet Owl einfache und praktische Anleitungen, die den Verbrauchern helfen, ihre persönlichen Daten zu schützen und sicher zu surfen.

Der Nutzer kann persönliche Daten wie z. B. Kreditkartennummern, E-Mail-Adressen oder auch Führerscheinnummer registrieren. Owl gleicht diese Daten initial mit der eigenen Datenbank ab, welche die aufgespürten Daten von illegalen Datenhandels-Plattformen und unsicheren Sites der letzten Jahre enthält. Bei einem Treffer wird der Nutzer sofort benachrichtigt.

Datenmissbrauch wird meist erst entdeckt, wenn es zu spät ist und schon ein finanzieller Schaden eingetreten ist. Zum Schutz davor überprüft Owl kontinuierlich die Handelsplätze des Darkwebs auf unbefugten Handel mit persönlichen Daten von Kunden. Besteht die Gefahr kompromittierter Daten, benachrichtigt die integrierte digitale Alarmanlage den Kunden sofort per E-Mail und/oder SMS.

Auf Basis der Ergebnisse dazu stellt Owl eine individuelle Lösung in Form eines klaren Maßnahmenplans zur Verfügung, damit der Kunde Schaden abwenden bzw. minimieren kann. Owl ist ein gänzlich digitales Produkt, welches unkompliziert über den Browser verwaltet wird. Bei Rückfragen stehen die Experten von Owl rund um die Uhr an 7 Tagen in der Woche auch telefonisch zur Verfügung. Ein Angebot für Owl erwarten Verbraucher insbesondere von Zahlungsdienstleistern, wie Kreditkartenemittenten, Anbietern von Sicherheitssoftware, Telekommunikationsunternehmen oder Versicherungen, also von Unternehmen, welche mit sensiblen Daten arbeiten bzw. mit Sicherheit assoziiert werden.[24]

Key Benefit
Owl bietet Verbrauchern das beruhigende Gefühl, sich wieder sorgenfrei im Internet bewegen können.

FAZIT

Durch einen ganzheitlich verantwortungsbewussten Umgang mit Konsumentendaten und die Bereitstellung von Informationen und Services zum Datenschutz können Unternehmen Mehrwert für ihre Kunden schaffen. Durch ein solches Engagement positionieren sich die Unternehmen vertrauenswürdig am Markt und grenzen sich von der Konkurrenz ab.

Daten werden auch als das Gold des 21. Jahrhunderts bezeichnet. Dementsprechend stellt ihre Sicherheit eine der wichtigsten Herausforderungen der heutigen Zeit dar. Sowohl Verbraucher als auch Staat und Unternehmen sind hier in der Pflicht. Es gilt, für eine angemessene Sicherheitskompetenz zu sorgen, eingeführte Regularien umzusetzen und bestehende Datenbanken durch Mitarbeiterkompetenz und technische Mittel effektiv zu schützen.

QUELLEN

[1] AGFA (Horizont Nr. 41, 09.10.2014, Seite 22)
[2, 9] Europäische Kommission, „Eurobarometer"
[3, 7, 10, 12] Markforschung, Mindline, i.A. v. CPP
[4] DsiN, „Sicherheitsindex 2016"
[5] Gemalto, „Breach Level Index 2015"
[6, 8] BKA, „Bundeslagebild Cybercrime 2015"
[11] Bitkom, „Datenschutz in der digitalen Welt"
[13] DsiN, „Sicherheitsindex 2016"
[14] Symantec, „State of privacy report"
[15] Symantec, „State of privacy report"
[16] Search Security, Definition „Advanced Persistent Thread";
Hacking Lab, Dossier „Advanced Persistent Threats: die jüngste und gefährlichste Generation der Sicherheitsbedrohung"
[17] Security Insider, „Cyber Kill Chain als Basis für mehrstufigen Schutz"
[18] Gemalto, „Breach Level Index"
[19] Computerwoche, Industrie 4.0 ist das Internet der Ingenieure;
Politik digital, Internet der Dinge – Teil 7: Industrie 4.0;
Elektroniknet, Industrie 4.0 – die Antwort auf IoT?
[20] Search Security, Internet der Dinge (IoT): Sieben wichtige Risiken für Unternehmen;
Focus, Sicherheitsrisiken wegen fehlendem Speicherplatz
[21] Datenschutzbeauftragter-Info, „10 Vorteile der EU-Datenschutz-Grundverordnung"
[22] Forum Privatheit, „Whitepaper, Selbstdatenschutz"
[23] www.owldetect.de
[24] Markforschung, Mindline, i.A. v. CPP