EU-DATENSCHUTZ-GRUNDVERORDNUNG IN DEUTSCHLAND

Der Countdown läuft!

IDC ANALYZE THE FUTURE

OKTOBER 2017
GESPONSERT VON MICROSOFT

EINLEITUNG

Autoren:
Laura Hopp
Consultant, IDC

Matthias Zacher
Manager, Research & Consulting, IDC

Deutschland hat schon seit mehr als 40 Jahren strenge Datenschutzbestimmungen. Die Relevanz des Themas wird nun durch die EU-Datenschutz-Grundverordnung (DSGVO) noch einmal erhöht. Die DSGVO beinhaltet Vorschriften für die Verarbeitung von personenbezogenen Daten und betrifft alle Unternehmen, die Daten von EU-Bürgern verarbeiten. Selbst Organisationen, die außerhalb der EU ansässig sind, müssen sich somit an die Verordnung halten.

Mit der Verabschiedung der DSGVO verfolgt der Gesetzgeber zwei primäre Ziele. Zum einen soll der Datenschutz in der EU an neue technologische Entwicklungen angepasst werden und die Nutzung neuer Technologien wie Cloud, Big Data/Analytics oder das Internet der Dinge berücksichtigen. Zum anderen sollen die gesetzlichen Rahmenbedingungen innerhalb der EU vereinheitlicht und eine länderübergreifende Geschäftstätigkeit vereinfacht werden. In Deutschland wurde die DSGVO im Rahmen des Bundesdatenschutzgesetzes neu (BDSG-neu) in nationales Recht umgesetzt, welches – wie die DSGVO auch – im Mai 2018 in Kraft tritt.

Warum müssen sich Unternehmen genau jetzt mit der DSGVO beschäftigen?

- **Der Zeitfaktor.** Bis zum Stichtag 25. Mai 2018 bleiben nur noch wenige Monate. IDC empfiehlt für eine umfassende und strukturierte Vorgehensweise 15 Monate. Unternehmen, die jetzt noch nicht begonnen haben, ihren DSGVO-Reifegrad zu ermitteln, müssen einzelne Schritte zur Umsetzung parallel durchlaufen oder werden zum Stichtag nicht compliant sein.

- **Der Gesetzgeber wird bei Verstößen hart durchgreifen.** Organisationen, die nach Ablauf der Übergangsfrist im Mai 2018 nicht compliant sind, müssen mit schwerwiegenden Konsequenzen rechnen. Bußgelder in Höhe von 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes können erhoben werden. In der Vergangenheit wurden Verstöße gegen den Datenschutz eher lax gehandhabt und Kontrollen kaum durchgeführt. Abschreckende Maßnahmen sind künftig zu erwarten.

- **Compliance schafft Transparenz.** Transparente Daten und damit nachvollziehbare Abläufe und Prozesse sind wichtige Voraussetzungen für die Einführung automatisierter Geschäftsprozesse, auch über Unternehmensgrenzen hinweg. Das senkt langfristig Kosten auf Technologie- und Geschäftsebene.

- **Der Datenschutz macht Unternehmen fit für die digitale Transformation.** Mit der DSGVO wird ein einheitlicher und verbindlicher Rechtsrahmen geschaffen. Die Rechtssicherheit erleichtert geschäftliche Beziehungen und eröffnet Chancen für digitale Geschäftsmodelle.

- **Die Umsetzung der DSGVO ist ein kontinuierlicher Prozess.** Mit ihr verbundene Aufgaben enden nicht im Mai 2018. Interne Veränderungen in den Unternehmen müssen DSGVO-konform konzipiert und gestaltet werden. Zudem wird der Gesetzgeber weitere Anforderungen erheben, die neue Anstrengungen in eine Compliance mit sich bringen.

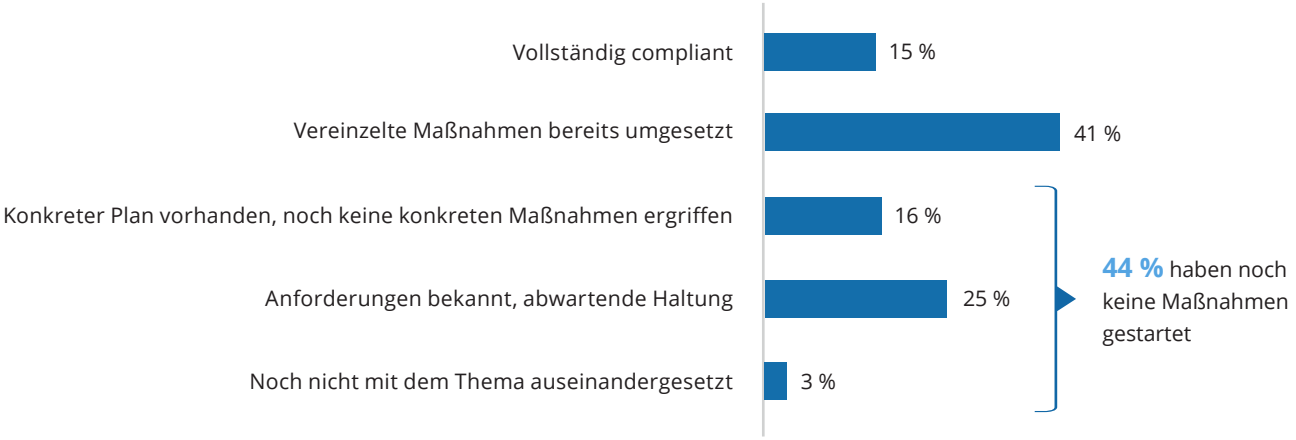
Deutsche Unternehmen befinden sich in der Situation, mit geeigneten Prozessen und Technologien den Datenschutz zu gewährleisten. Vor diesem Hintergrund hat IDC im August 2017 251 Unternehmen in Deutschland befragt, wie sie zur DSGVO stehen, wie gut sie ihre Daten im Griff haben und welche Schritte sie gehen, um DSGVO-compliant zu sein. Dieser Executive Brief fasst die wichtigsten Einschätzungen der befragten Fach- und Führungskräfte zusammen und gibt Empfehlungen, welche Schritte notwendig sind, um ab Mai 2018 compliant zu sein.

UNTERNEHMEN IN DEUTSCHLAND NEHMEN DIE DSGVO AUF DIE LEICHTE SCHULTER

Alle Organisationen in Deutschland, die personenbezogene Daten verarbeiten, sind von der DSGVO betroffen. IDC geht davon aus, dass Strafen bei einer Nicht-Compliance so gravierend sein werden, dass viele diese nur schwer verkraften würden. Dennoch erfährt die DSGVO nicht bei allen Befragten die erforderliche Priorität. So haben 44 Prozent noch keine Maßnahmen gestartet. Darunter sind auch Firmen, die immer noch in einer abwartenden Haltung verharren. Demnach erwarten auch 27 Prozent, dass sie bis zum Stichtag im Mai 2018 nicht compliant sein werden. Der Mittelstand schätzt die eigene Situation am negativsten ein: 39 Prozent sind skeptisch, alle Prozesse und Maßnahmen rechtzeitig umgesetzt zu haben. Hier besteht demnach der größte Nachholbedarf.

Abbildung 1: Stand der Vorbereitungen auf die DSGVO (August 2017)

Wie weit sind die Vorbereitungen Ihres Unternehmens auf die DSGVO bereits fortgeschritten?



N = 249; ohne „Weiß nicht "

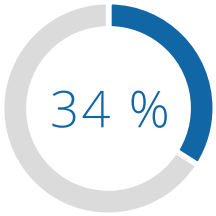
Die Vorbereitungen auf die DSGVO werden somit nicht mit der erforderlichen Ernsthaftigkeit verfolgt. Grund hierfür ist, dass potenzielle Folgen offensichtlich verharmlost werden: Konsequenzen, seien es Strafzahlungen, ein Reputationsverlust oder das Verbot der Datenverarbeitung, werden im Durchschnitt nicht als besonders „bedrohlich" eingeschätzt. Viele Unternehmen sind sich der Tragweite eines Verstoßes nicht bewusst. Diese Einstellung ist fahrlässig. Zum einen erhöht die Untätigkeit die Risiken eines Datenschutzvorfalls. Zum anderen kann die Compliance bis Mai 2018 nicht gewährleistet werden und Unternehmen müssen im Falle von Kontrollen durch die Aufsichtsbehörden mit drastischen Konsequenzen rechnen.

IDC schätzt, dass Organisationen, die erst jetzt mit der Bewertung ihres DSGVO-Reifegrads beginnen, mindestens 9 Monate zu spät starten. Die verbleibende Zeit muss jetzt intensiv genutzt werden, um die Vorbereitungen auf die Compliance voranzutreiben. Verantwortliche sollten mit der Bewertung des DSGVO-Reifegrads, einer GAP-Analyse sowie der Etablierung einer Steuerungsgruppe starten. Danach folgen die Umsetzung organisatorischer und technologischer Maßnahmen – sowie die Überprüfung umgesetzter Maßnahmen.

DER DATENDSCHUNGEL MUSS NOCH GELICHTET WERDEN – UNTERNEHMEN FEHLT DER ÜBERBLICK

Die Grundvoraussetzung für die Einhaltung der Compliance ist der ganzheitliche Überblick über sämtliche personenbezogene Daten im Unternehmen. Die Verantwortlichen müssen ihre Daten kennen, um sie auch schützen zu können, und sollten sich unter anderem folgende Fragen stellen:

- Wo werden die Daten gespeichert?
- Wer hat darauf Zugriff?
- Wie lange dürfen die Daten gespeichert werden?
- Wie werden die Daten verarbeitet?
- Was sind die Risiken, die bei einer Datenschutzverletzung auftreten?

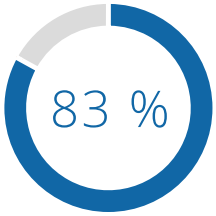


der befragten Unternehmen wissen nicht, wann personenbezogene Daten gelöscht werden müssen

Diese Informationen liegen in den Organisationen noch nicht ausreichend vor. 23 Prozent wissen nicht, wo Daten gespeichert werden, 27 Prozent können nicht genau sagen, wer auf die Daten Zugriff hat und 34 Prozent sind die Löschfristen nicht bekannt. Darüber hinaus geben 37 Prozent der Befragten an, dass Dokumente unkontrolliert auf den Fileservern unter der Obhut der Mitarbeiter liegen. Um die Grundsätze der DSGVO wie das „Recht auf Vergessenwerden" oder die Datenminimierung überhaupt erfüllen zu können, müssen diese grundlegenden Informationen vorliegen. Die Datentransparenz ist somit eine wesentliche Voraussetzung sämtlicher nachfolgender Maßnahmen. Unternehmen, die sich noch keinen Überblick über ihre Daten verschafft haben, sollten nun handeln. Denn der Aufwand, der dahintersteckt, ist erheblich und steigt mit der Unternehmensgröße.

Die Datentransparenz ist nicht nur Grundlage für die Einhaltung der Compliance, sondern auch für die digitale Transformation. Denn mit steigender Datenmenge wird es umso wichtiger, die Daten in den Griff zu bekommen und Datenverarbeitungsprozesse stärker automatisieren zu können.

DATENSCHUTZBEAUFTRAGTE NICHT FLÄCHENDECKEND VORHANDEN



der Unternehmen haben noch keinen Datenschutzbeauftragten ernannt oder extern engagiert

Eine Rolle, die künftig häufiger anzutreffen sein wird, ist die des Datenschutzbeauftragten (DSB). Dieser ist für die Überwachung der Einhaltung der DSGVO verantwortlich und primärer Ansprechpartner für Datenschutzfragen innerhalb der Organisation sowie für die Aufsichtsbehörden. Er sollte zudem Mitglied eines breit aufgestellten Teams aus IT- und Business-Entscheidern sowie Risk- und Compliance-Verantwortlichen bei der Umsetzung der DSGVO sein.

Unternehmen müssen einen DSB bestellen, sobald mindestens zehn Personen mit der automatischen Verarbeitung personenbezogener Daten beschäftigt sind. Das BDSG-neu übernimmt somit die Anforderung des bisherigen BDSG und macht damit von bestimmten Auslegungsfreiheiten, den sogenannten Öffnungsklauseln, Gebrauch.

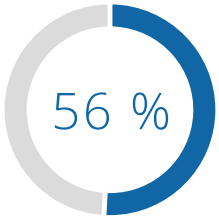
Die Ergebnisse zeigen jedoch, dass erst 17 Prozent der befragten Firmen einen DSB beschäftigen. Das ist ein sehr geringer Anteil. Ein Bestellen eines DSB wurde in der Vergangenheit aufgeschoben oder für nicht notwendig gehalten, da Verstöße nur selten geahndet wurden. Stärkere Sanktionen resultierend aus der DSGVO werden nun der Treiber für Neueinstellungen sein. So wollen 50 Prozent der befragten Unternehmen einen DSB in den nächsten Monaten beschäftigen. IDC geht davon aus, dass der Arbeitsmarkt für DSB stark umkämpft ist und es durchaus schwierig sein wird, diese Experten zu finden. Eine Alternative ist die Qualifizierung eigener Mitarbeiter zum DSB.

MITARBEITER GENIESSEN ZU VIEL FREIRAUM UND SIND GLEICHZEITIG NICHT AUSREICHEND SENSIBILISIERT

Mehr Datentransparenz und ein DSB werden allein nicht ausreichen. Denn Mitarbeiter spielen bei der Gewährleistung des Datenschutzes eine wesentliche Rolle. Personenbezogene Daten werden von ihnen täglich verarbeitet – seien es Mitarbeiterdaten in der Personalabteilung oder Kundendaten im Vertrieb oder der Produktentwicklung. Für Verantwortliche ist es daher wichtig zu wissen, wer auf die Daten Zugriff hat, um Datenschutzlösungen an der richtigen Stelle platzieren zu können. Der Zugriff wird jedoch nur in 50 Prozent der befragten Unternehmen erfasst. Zudem haben 45 Prozent kein zentrales Rollen- und Rechtemanagement. Auch ein Identity and Access Management ist

erst bei 43 Prozent der befragten Organisationen im Einsatz. Damit wird deutlich, dass Mitarbeiter bezogen auf den Umgang mit Daten viel Spielraum haben und zu wenig Kontrolle stattfindet.

Zudem müssen Mitarbeiter für den gewissenhaften Umgang mit personenbezogenen Daten sensibilisiert sein. Denn Sicherheitsvorfälle sind häufig auf ein Fehlverhalten und Unwissenheit zurückzuführen. In der Praxis zeigt sich, dass die Mitarbeiter in rund jedem zweiten Unternehmen nicht ausreichend sensibilisiert sind. Schulungen sind daher nach wie vor sehr wichtig. Dabei sollte insbesondere auch auf Neuerungen der DSGVO hingewiesen werden. Ohne eine ausreichende Sensibilisierung der Mitarbeiter wird es sehr schwer, Datenschutzverstöße zu vermeiden.



der Unternehmen geben an, dass ihre Mitarbeiter nicht ausreichend sensibilisiert sind

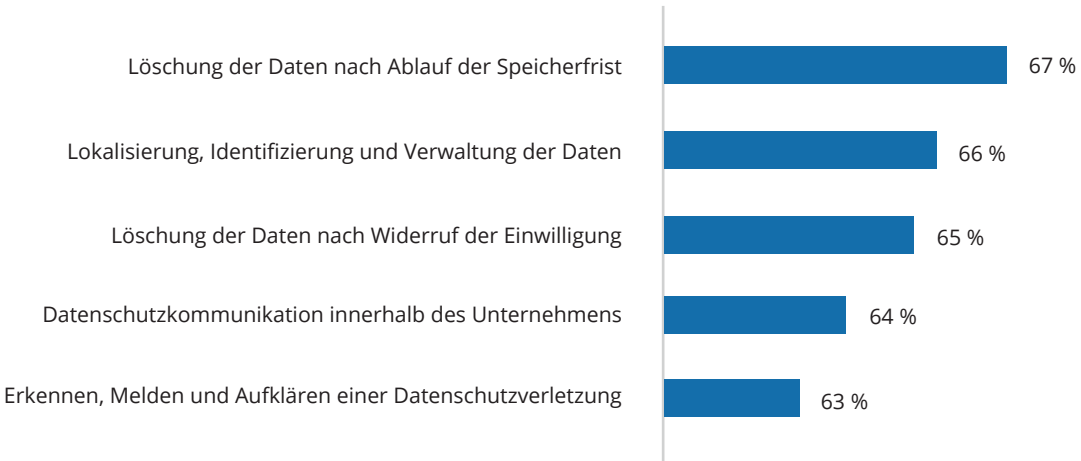
NOCH DEUTLICHE LÜCKEN BEI DSGVO-RELEVANTEN PROZESSEN SICHTBAR

Neben Organisationsstrukturen müssen auch die Prozesse angepasst werden. Die Ergebnisse zeigen, dass DSGVO-relevante Prozesse bei der Mehrheit der Firmen und Organisationen vorhanden sind oder ihre Umstellung auf die veränderten Anforderungen zumindest geplant wird. Beispiele hierfür sind Prozesse für die Löschung der Daten nach Ablauf der Speicherfrist (67 Prozent), die Lokalisierung, Identifizierung und Verwaltung der Daten (66 Prozent) sowie die Löschung der Daten nach Widerruf der Einwilligung (65 Prozent). Diese Prozesse sind notwendig, um Datenschutzgrundsätze wie die Datenminimierung einhalten zu können.

Rund 40 Prozent der Befragten planen, nicht alle relevanten Prozesse einzuführen, obwohl diese zum Erreichen der DSGVO-Compliance erforderlich sind. Sie betrachten diese Prozesse für nicht notwendig, oder sie warten ab, ob sich eine Umstellung überhaupt lohnt bzw. ob eine manuelle Bearbeitung gegebenenfalls ausreicht. Aus Sicht von IDC muss sehr genau geprüft werden, welche Prozesse relevant sind und wie diese Prozesse in IT-Lösungen abgebildet werden können. Denn die Automatisierung von Prozessen sichert Nachvollziehbarkeit sowie eine konsistente und schnelle Bearbeitung von Aufgaben. Für das Erkennen und Melden einer Datenschutzverletzung haben Unternehmen maximal 72 Stunden Zeit. Wenn hier keine genauen IT-gestützten Prozesse hinterlegt sind, besteht die Gefahr einer verzögerten Bearbeitung oder manueller Eingriffe – und somit schwer kalkulierbarer Risiken.

Abbildung 2: DSGVO-relevante Prozesse, Top-Fünf-Nennungen

Welche der folgenden DSGVO-relevanten Prozesse sind in Ihrem Unternehmen bereits vorhanden?



N = 251; Abbildung gekürzt; Mehrfachnennungen

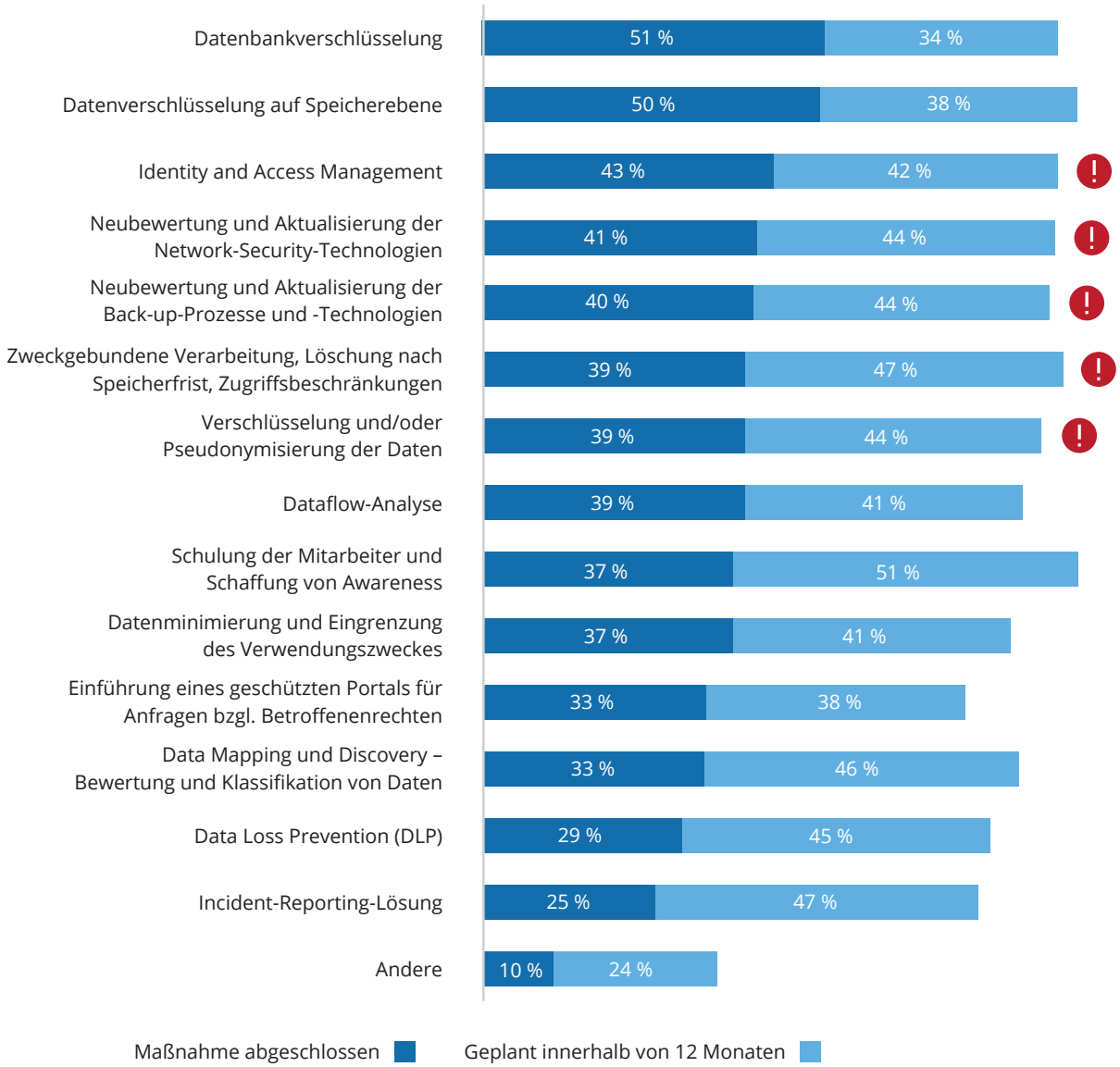
IT-SECURITY-STRATEGIE MUSS STÄRKER AUF DIE DSGVO AUSGERICHTET WERDEN

Im Zusammenhang mit der Auswahl geeigneter Technologien verwendet die DSGVO den Begriff „Stand der Technik“. Dieser muss immer wieder geprüft und technische Maßnahmen gegebenenfalls angepasst werden, um die Datensicherheit gewährleisten zu können und mit der aktuellen Bedrohungslage und dem Datenschutz Schritt zu halten. Aus Sicht von IDC ist Compliance nur mit moderner Technik erreichbar. Hierzu zählen auch Security-Lösungen. Diese spielen beim Datenschutz schon immer eine wichtige Rolle und gewinnen durch die DSGVO noch einmal zusätzlich an Bedeutung. Allerdings zeigt sich, dass grundlegende Aktivitäten wie eine Neubewertung und Aktualisierung der Netzwerk-Security-Technologien oder der Back-up-Prozesse und -Technologien erst bei knapp 40 Prozent der befragten Unternehmen erfolgt sind.

Die DSGVO fordert in Artikel 25, dass solche Technologien zu nutzen sind, die den Datenschutz durch Technikgestaltung („Privacy by Design“) und datenschutzfreundliche Voreinstellung („Privacy by Default“) unterstützen. D.h. Tools, die bei Datenverarbeitungsprozessen zum Einsatz kommt, müssen so gestaltet werden, dass sie den Datenschutz von Anfang an berücksichtigt. Zudem müssen Standardeinstellungen darauf ausgerichtet sein, nur für den Verarbeitungszweck erforderliche Daten zu verarbeiten. Die Menge der Daten soll somit von Anfang an auf ein Minimum reduziert und Daten nach Ablauf der Speicherfrist gelöscht werden.

Abbildung 3: Maßnahmen zum Schutz von Daten

Welche Maßnahmen hat Ihr Unternehmen bisher umgesetzt oder plant es, um personenbezogene Daten zu schützen und die neuen Anforderungen der DSGVO zu erfüllen?



N = 251

Einige der Maßnahmen, die bereits umgesetzt wurden und in direktem Zusammenhang mit den Anforderungen der DSGVO stehen, sind das Identity and Access Management (43 Prozent), die zweckgebundene Verarbeitung, Löschung und Zugriffbeschränkungen von Daten (39 Prozent) und die Verschlüsselung/Pseudonymisierung von Daten (39 Prozent).

Mit Blick auf Aktivitäten der Unternehmen zeigt sich, dass es bis Mai 2018 für viele schwierig wird, ihre Technologie umfassend auf die DSGVO hin auszurichten. So haben erst 33 Prozent eine Bewertung und Klassifikation der Daten vorgenommen, eine Maßnahme, auf der weitere Schritte, wie ein umfassendes Datenmanagement, aufbauen.

Data Loss Prevention und Breach Detection ist ein Schlüsselfaktor

Maßnahmen, um Datenlecks zu vermeiden oder schnell aufzudecken, sind besonders relevant, da ein ungewollter Datenabfluss eine entsprechende Meldung an die Aufsichtsbehörden erfordert, falls die betroffenen Personen einem Risiko ausgesetzt sind.

Die Ergebnisse zeigen jedoch, dass lediglich 29 Prozent der Befragten Lösungen für Data Loss Prevention nutzen. Das ist ein erschreckend geringer Wert. Kommt es tatsächlich zu einem Datenleck, müssen Firmen in der Lage sein aufzuzeigen, dass vorbeugende Maßnahmen getätigt wurden sowie Mechanismen vorhanden sind, die die Datenpanne zügig aufgedeckt haben. Kann dies nicht nachgewiesen werden (Dokumentationspflicht), können Bußgelder verhängt werden. Wie bereits erwähnt, ist zu erwarten, dass die Aufsichtsbehörden hier deutlich stärker als in der Vergangenheit Sanktionen verhängen werden, um die Anforderungen durchzusetzen.

Vermeidung von Datenlecks – Top-3-Maßnahmen:

1. Restriktive Zugriffsrechte
2. Kennzeichnung vertraulicher Daten
3. Regelmäßige Überprüfung von Berechtigungen

Darüber hinaus kommen auch Lösungsansätze, die eine Datenpanne zügig aufdecken, noch viel zu wenig zum Einsatz. Hier wurde in der Vergangenheit äußert nachlässig gehandelt. Weder für Betroffene noch für Aufsichtsbehörden ist es akzeptabel, wenn Wochen oder Monate vergehen, bis Datenlecks angezeigt werden. Insbesondere Next-Gen-IT-Security-Lösungen wie Breach Detection oder Threat Detection werden erst in geringem Maße eingesetzt, obwohl diese Lösungen sehr geeignet sind, um die Anforderungen der DSGVO zu unterstützen. Unternehmen müssen weitere Erfahrungen mit diesen Tools sammeln, um ihre Relevanz insgesamt und mit Blick auf die DSGVO bewerten zu können.

Print-und-Document-Management wird vernachlässigt

Drucker- und Printumgebungen sind ebenfalls eine potenzielle Gefahrenquelle für den Abfluss von Daten. Die Druckersicherheit muss daher gewährleistet werden. Printer und Multifunktionsgeräte werden bei den Vorbereitungen auf die DSGVO jedoch zu wenig berücksichtigt. Erst 38 Prozent der befragten Unternehmen führen regelmäßige Updates ihrer Geräte durch und 32 Prozent haben die Sicherheitseinstellungen der Drucker überprüft. Viele verlassen sich hier auf ihren Managed Print Services Provider. Die Diskussion der DSGVO mit den Providern ist unbedingt erforderlich.

Cloud und Outsourcing auf dem Prüfstand

Ein weiterer Aspekt, der im Rahmen der DSGVO zu berücksichtigen ist, sind Cloud Services. Cloud-Anbieter und Service Provider gehören zu den Auftragsverarbeitern, wenn sie personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten. Kommt es zu einer Datenschutzverletzung auf Seiten der Cloud Provider, sind Unternehmen mitverantwortlich, falls sie den Anbieter vorab nicht sorgfältig ausgesucht haben. Ein Anbieterwechsel wird daher häufig in Betracht gezogen. So wollen 54 Prozent der Befragten die Zusammenarbeit mit ihrem bisherigen Cloud Provider auf den Prüfstand stellen. Das ist ein hoher Wert, denn auch Cloud-Anbieter mit Rechenzentren außerhalb der EU unterliegen der DSGVO. Dennoch wird das „subjektive Gefühl" bei der Auswahl sicherlich eine Rolle spielen.

DIE DSGVO STÄRKT DIE COMPLIANCE UND UNTERSTÜTZT DIE DIGITALE TRANSFORMATION

Mit der DSGVO können die Unternehmen ihre Compliance signifikant verbessern, und zwar in mehrfacher Hinsicht:

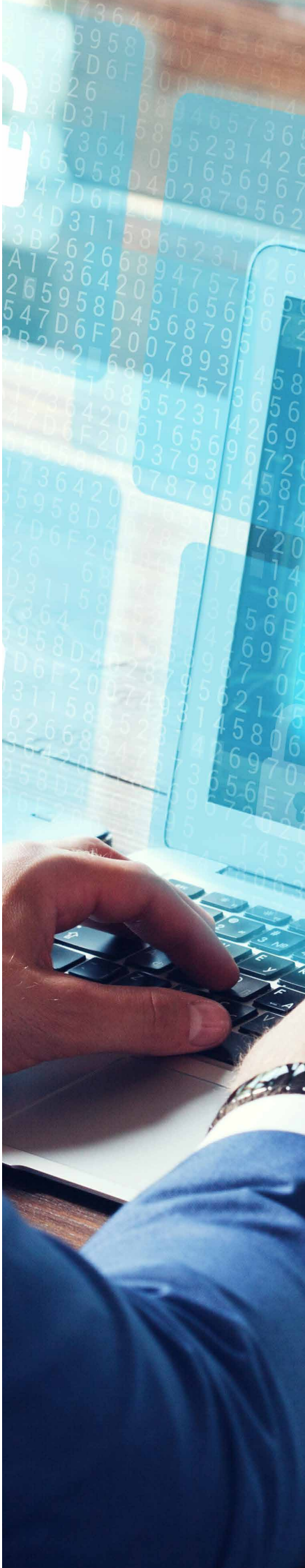
- **Verbesserte IT-Security:** Eine hohe IT-Sicherheit ist eine zwingende Voraussetzung, um die Vorteile digitaler Ökosysteme stärker zu nutzen. Unternehmen sind in der Lage, als vertrauenswürdiger Partner zu agieren, und sind zugleich befähigt, Cyberrisiken besser abzuwehren.

- **Automatisierte Prozesse:** Datentransparenz ist ein wichtiger Baustein für die Automatisierung von Geschäftsprozessen. Gut aufbereitete Daten bilden eine sehr gute Basis für die Digitalisierung aller Geschäftsprozesse und die immer bessere Verknüpfung von Prozessketten.

- **Neue Geschäftsmodelle:** Die umfassende Transparenz der Daten ist eine sehr gute Voraussetzung, die Daten für die Verbesserung bestehender Geschäftsprozesse und die Entwicklung neuer Geschäftsmodelle zu nutzen. Die aufbereiteten personenbezogenen Daten helfen Entscheidern, ihre Kunden besser zu kennen und zu verstehen. Das ist ein großer Mehrwert, den die DSGVO mit sich bringt.

- **Stärkung der Unternehmenskultur:** Compliance, die vom Management und den Mitarbeitern gelebt wird, erhöht die Bindung an den Arbeitgeber und verbessert das Image gegenüber Kunden und der Öffentlichkeit. Das sind zwei Aspekte, die in einem Wettbewerbsumfeld, in dem Produkte immer ähnlicher werden, entscheidende Erfolgsfaktoren sein können.

Die Gewährleistung der Compliance ist mehr als nur lästige Pflicht und gibt den Anstoß für die Realisierung zahlreicher Vorteile und Chancen.



FAZIT

Für Unternehmen in Deutschland bleibt nicht mehr viel Zeit, um sich auf die neuen Anforderungen der DSGVO vorzubereiten und nach Ablauf der Übergangsfrist im Mai 2018 compliant zu sein. Zwar haben viele bereits organisatorische Maßnahmen ergriffen, einzelne Prozesse angepasst und in Technologie investiert. Dennoch ist der Nachholbefarf zur Schließung vorhandener Lücken groß. Dies zeigt, dass zahlreiche deutsche Organisationen die Relevanz und Dringlichkeit immer noch nicht verstanden und sich nicht umfassend genug mit dem Thema auseinandergesetzt haben – trotz der Brisanz und der drohenden Sanktionen.

Die verbleibende Zeit muss nun intensiv dafür genutzt werden, um die Umsetzung der notwendigen Maßnahmen zumindest anzustoßen und den Rückstand, so gut es geht, aufzuholen. Die Studie zeigt, dass Aktivitäten geplant und die Umsetzung konkret in Angriff genommen wird. IDC geht dennoch davon aus, dass es viele nicht schaffen werden, nach Ablauf der Übergangsfrist compliant zu sein.

Die Umsetzung der Maßnahmen ist mit einem hohen Aufwand verbunden – auch über Mai 2018 hinaus. Organisation, Prozesse und Technologien gehen Hand in Hand und müssen über Unternehmensbereiche hinweg in Einklang gebracht und immer wieder von neuem überprüft werden. Gerade auch der „Stand der Technik" entwickelt sich in der heutigen Zeit rasant weiter – dies sollten Firmen unbedingt beachten. Daher gehen lediglich sehr wenige davon aus, dass externe Ausgaben nach dem Stichtag fallen werden. Dies verdeutlicht die Kontinuität des Themas. Gleichzeitig ist die Compliance Basis und Kernvoraussetzung für eine erfolgreiche Geschäftstätigkeit vor dem Hintergrund der digitalen Transformation.

IDC EMPFEHLUNGEN

Starten Sie mit einer Bestandsaufnahme. Bestimmen Sie Ihren GAP zwischen den alten und neuen Datenschutzbestimmungen
Einige DSGVO-Anforderungen sind nicht gänzlich neu und weichen nur etwas von dem aktuellen Bundesdatenschutzgesetz ab. Arbeiten Sie die Unterschiede heraus. Nur wenn Sie die Verordnung verstehen, können Sie beurteilen, welche Maßnahmen Sie bereits umgesetzt haben und welche zu überdenken oder neu einzuführen sind.

Stellen Sie ein Team zusammen, das aus IT-Entscheidern, Business Managern und Experten aus der Rechtsabteilung besteht
Bringen Sie Mitarbeiter zusammen, die unterschiedliche Schwerpunkte haben. Holen Sie auch einen Datenschutzbeauftragten mit ins Boot. Das Team sollte gemeinsam und regelmäßig an der Vorbereitung auf die Compliance arbeiten und die Umstellung der Prozesse und die Einführung von Technologie vorantreiben. Das Team sollte auch verantwortlich sein für die Dokumentation der Maßnahmen und diese regelmäßig überprüfen – auch nach dem Stichtag im Mai 2018. Holen Sie sich externe Hilfe, wenn interne Kapazitäten nicht ausreichen sollten.

Erfassen und bewerten Sie alle personenbezogenen Daten
Identifizieren und Klassifizieren Sie alle Ihre Daten, egal wo diese sich befinden – sei es auf Servern, in Rechenzentren, in Anwendungen, in der Cloud oder auf mobilen Endgeräten. Erfassen Sie den Datenfluss: Wo werden Daten erhoben, wohin werden sie übermittelt und wo werden sie gespeichert und welche Kopien werden erstellt. Sie müssen Ihre Daten kennen, um diese Compliance-konform managen zu können.

Definieren Sie, was der „Stand der Technik" für Ihr Unternehmen bedeutet und führen Sie entsprechende Technologien ein
Bewerten Sie immer wieder von neuem, was der „Stand der Technik" bedeutet, und berücksichtigen Sie dies bei der Auswahl von Technologien. Ziehen Sie verstärkt innovative Anbieter in Betracht, um das Risiko zu reduzieren, technologisch zurückzufallen. Moderne Technik ist für die Erreichung der DSGVO-Compliance erforderlich.

Überprüfen Sie die Verträge mit Ihren Auftragsverarbeitern
Der Gesetzgeber fordert, nur Auftragsverarbeiter zu wählen, die ausreichend Garantien für die Einhaltung der DSGVO bieten. Überprüfen Sie daher bestehende Verträge und bewerten Sie diese neu. Ziehen Sie im Zweifel auch einen Anbieterwechsel in Betracht.

EMPFEHLUNGEN VON ANWENDERN FÜR ANWENDER

Die Befragungsteilnehmer wurden gebeten, anderen Entscheidungsträgern Hinweise zu geben, worauf sie bei der Vorbereitung auf die DSGVO-Compliance achten sollten. Einige der Antworten sind nachfolgend ungefiltert wiedergegeben. Auf eine Kommentierung wird hier bewusst verzichtet, um einen authentischen Eindruck zu vermitteln.

„Das aktuelle System gemäß den Richtlinien für 2018 so früh wie möglich zu optimieren, damit keine Kostensteigerungen durch spätere notwendige Updates anfallen."

„Mit einem Sicherheits-Anbieter die genauen Richtlinien durchdenken."

„Höhere finanzielle Leistungen zur Umsetzung sind nötig."

„Ständige Weiterbildung, um auf dem aktuellen Stand zu bleiben und Risiken zu vermeiden."

„Immer auf die aktuelle Rechtslage achten und die größte Bedrohung nicht vergessen: die von innen heraus."

„Sich schlau machen und Gas geben ..."

„Genügend Angebote einholen und nur zertifizierte Unternehmen ins Boot holen."

„Sich absolut gründlich im Voraus informieren. Falls das Fachwissen nicht vorhanden ist, auf jeden Fall Experten hinzuziehen."

„Einen Experten beauftragen, da die Thematik sehr komplex ist."

„Über den Tellerrand schauen, ob man alle Prozesse im Unternehmen im Blick hat."

METHODIK

Ziel der im August 2017 unter IT- sowie Business-, Risk- und Compliance-Entscheidern durchgeführten Befragung war es, Einblicke in die aktuelle Situation, die Herausforderungen sowie die zu erwartenden Entwicklungen in Deutschland hinsichtlich der DSGVO-Compliance zu erhalten. Vor diesem Hintergrund hat IDC 254 Verantwortliche aus Unternehmen verschiedener Branchen mit mehr als 20 Mitarbeitern in Deutschland befragt. 22 Prozent der Unternehmen haben weniger als 100 Mitarbeiter, 35 Prozent zwischen 100 und 1000 Mitarbeiter und 43 Prozent haben mehr als 1000 Beschäftige.

Die nachfolgenden Informationen wurden von Microsoft zur Verfügung gestellt. Für diese Angaben übernimmt IDC keine Gewähr.

MICROSOFT
Unternehmensprofil

Microsoft

WWW.MICROSOFT.DE

INFORMATIONEN ZUM UNTERNEHMEN

Die Microsoft Deutschland GmbH ist die 1983 gegründete Tochtergesellschaft der Microsoft Corporation/Redmond, U.S.A., des weltweit agierenden Herstellers von Standardsoftware, Services und Lösungen mit 89,95 Mrd. US-Dollar Umsatz (Geschäftsjahr 2017; 30. Juni 2017). Der Netto-Gewinn im Fiskaljahr 2017 betrug nach eigenen Angaben 21,2 Mrd. US-Dollar. Neben der Firmenzentrale in München ist die Microsoft Deutschland GmbH bundesweit mit sechs Regionalbüros vertreten und beschäftigt rund 2.700 Mitarbeiterinnen und Mitarbeiter. Im Verbund mit rund 31.500 Partnerunternehmen betreut sie Firmen aller Branchen und Größen. Das Advanced Technology Labs Europe (ATLE) in München hat Forschungsschwerpunkte in IT-Sicherheit, Datenschutz, Mobilität, mobilen Anwendungen und Web-Services.

POSITIONIERUNG IM BEREICH DSGVO-COMPLIANCE

Für Microsoft ist das Einhalten der EU-Datenschutz-Grundverordnung weit mehr als eine Pflichtaufgabe: Das Unternehmen setzt sich seit vielen Jahren dafür ein, dass Kunden und Anwender möglichst viel Kontrolle über die eigenen Daten behalten. Daher ist die Regelung aus Sicht von Microsoft ein wichtiger Schritt, um die Rechte von Einzelpersonen in Bezug auf den Datenschutz zu verdeutlichen und umzusetzen. Microsoft gestaltet die eigenen Produkte und Cloud-Dienste konform zur neuen Regelung: Die Verordnung verlangt von Unternehmen, dass nur die Auftragsverarbeiter mit personenbezogenen Daten von EU-Bürgern arbeiten dürfen, die den Anforderungen rund um das Verarbeiten solcher Daten entsprechen. Im März 2017 hat Microsoft vertragliche Garantien mit derartigen Zusicherungen veröffentlicht.

Zudem will Microsoft seine Kunden dabei unterstützen, mit möglichst geringem Aufwand selbst konform zu werden zur DSGVO. Grundsätzlich sollten Unternehmen sich der Regelung aus Sicht von Microsoft in vier Schritten nähern: Ermitteln, Kontrollieren, Schützen, Berichten. Zuerst gilt es zu ermitteln, in welchem Umfang die eigene Organisation beziehungsweise die vorhandenen Daten von der Verordnung erfasst sind. Das Sicherstellen des rechtmäßigen Umgangs mit diesen Daten ist der zweite Schritt. Nur so können die Kunden durch die Verordnung eingeräumten Auskunfts- oder Löschansprüche erfüllt werden. Außerdem müssen die gespeicherten oder übertragenen Daten bestmöglich geschützt werden. Beispielsweise durch Verschlüsselung. Und zu guter Letzt müssen alle relevanten Prozesse und Transaktionen dokumentiert werden. Die verschiedenen Cloud-Angebote von Microsoft wie Azure, Dynamics 365, Enterprise Mobility + Security Suite (EMS) oder Office 365 unterstützen Anwender bei jedem der vier genannten Schritte.

DARSTELLUNG DES PORTFOLIOS ZUR UNTERSTÜTZUNG BEI DER ERREICHUNG DER DSGVO-COMPLIANCE

In den Microsoft-Produkten selbst stecken etliche Mechanismen, die Anwendern das Einhalten der DSGVO-Vorgaben erleichtern und den kompletten Datenlebenszyklus managen. So listet der Azure Data Catalog sämtliche Datenquellen in der Organisation auf. Office 365 Advanced Data Governance hilft durch Machine Learning, wichtige Daten schneller zu finden und zu sichern sowie veraltete oder irrelevante Datensätze automatisch zu identifizieren und zu entfernen. Dies senkt das Risiko von kompromittierten Unternehmensinhalten. Data Loss Prevention wiederum erkennt gängige Typen sensibler Daten in Dokumenten und schützt darüber hinaus vor unerlaubter oder versehentlicher Datenweitergabe. eDiscovery wiederum macht Daten auffindbar, die sowohl in der Cloud als auch lokal gespeichert sind.

Um die Zugriffsteuerung kümmern sich beispielsweise Azure Active Directory und die rollenbasierte Zugriffsteuerung von Microsoft Azure. Die Datenverwaltungsfunktionen von Office 365 helfen beim Archivieren und Verwalten von Daten in Exchange-Online-Postfächern, SharePoint-Online-Sites und OneDrive-for-Business-Speicherorten.

Den Schutz der Daten in Azure erhöhen beispielsweise eine Anti-Malware-Funktion oder Verschlüsselungstechniken für ruhende Daten mit oder ohne Anmeldeverfahren, die unberechtigte Zugriffe unterbinden. Auch beim Klassifizieren von Daten unterstützen Azure, Dynamics 365, EMS, Office 365 und Windows (Desktop und Server) die Anwender mit jeweils eigenen Tools.

Darüber hinaus bietet Microsoft noch eigenständige Hilfsmittel, wie den webbasierten GDPR Benchmark. Dieser hilft Unternehmen durch einen Fragenkatalog, die Techniken und Maßnahmen zu identifizieren, die in ihrer jeweiligen Situation beim Einhalten der DSGVO-Vorgaben helfen. Seine Partner unterstützt Microsoft mit noch detaillierteren Materialien wie dem GDPR Activity Hub oder Demos. Ziel: Partner und Endkunde ermitteln in Workshops den jeweils notwendigen Handlungsbedarf und die daraus resultierenden notwendigen Maßnahmen.

Interview mit Milad Aslaner, Microsoft

EU-DATENSCHUTZ-GRUNDVERORDNUNG IN DEUTSCHLAND

Anlässlich der Vorstellung der Ergebnisse der Studie „EU-Datenschutz-Grundverordnung in Deutschland“ sprach IDC mit Milad Aslaner, Senior Product Manager, Cyber Security bei Microsoft Deutschland.

IDC: Die neue EU-Datenschutz-Grundverordnung stellt viele Unternehmen vor große Herausforderungen. Mit welchen Angeboten unterstützen Sie Unternehmen, damit diese bis Ablauf der Frist im Mai 2018 den Anforderungen der DSGVO und dem BDSG-neu entsprechen und somit compliant sind?

Milad Aslaner: Als Anbieter von Cloud-Diensten wie Office 365, Dynamics 365, Microsoft Azure, SQL Server oder Enterprise Mobility und Security will Microsoft selbst natürlich bis Mai 2018 konform zur DSGVO sein. Für Microsoft-Kunden bedeutet dies, dass sie personenbezogene Daten ihrer Kunden aus der EU in Microsoft-Cloud-Diensten ablegen können, ohne sich um die Details der Datenschutz-Grundverordnung zu kümmern. Darüber hinaus bieten Microsoft-Produkte und -Cloud-Dienste etliche Funktionen, mit deren Hilfe Anwender ihre lokal oder in der Cloud betriebenen Infrastrukturen DSGVO-konform gestalten können.

IDC: Die Vorbereitungen auf die neue Datenschutz-Grundverordnung betreffen sowohl Prozesse und Organisationsstrukturen als auch Technologien. Anbieter aus verschiedenen Bereichen tummeln sich in diesem Marktumfeld. Wo ordnen Sie sich hier ein?

Aslaner: Microsoft hat sicherlich einen Schwerpunkt auf Technologien wie unseren Cloud-Angeboten. Mit diesen können Unternehmen ihren EU-DSGVO-Verpflichtungen in Bereichen wie dem Löschen, Richtigstellen, Verarbeiten oder Übertragen von personenbezogenen Daten nachkommen.

Wir stellen unseren Partnern – und damit den Endkunden – aber auch zahlreiche Hilfsmittel rund um Datenschutzprozesse, wie beispielsweise einen webbasierten Benchmark zur DSGVO, bereit. Darüber hinaus informiert Microsoft seine Kunden fortlaufend über die Maßnahmen rund um die DSGVO-Vorgaben, so dass Kunden von unseren Erfahrungen profieren können.

IDC: Warum ist der Background Ihres Unternehmens die richtige Wahl? Was konkret unterscheidet Sie von Ihren wichtigsten Mitbewerbern am Markt? Was machen Sie besonders gut, was ist in Ihren Augen Ihr USP?

Aslaner: Für Microsoft spielen Datenschutz und IT-Sicherheit schon seit sehr langer Zeit eine immens wichtige Rolle. Dies untermauern Investitionen in Milliardenhöhe, die im Lauf der Jahre in die Entwicklung von Mechanismen zum Schutz von Kundendaten geflossen sind. Außerdem ist Microsoft eines der ersten Unternehmen, das sich gegen Online-Kriminelle und Datendiebe nicht nur mit technischen Mitteln zur Wehr setzt. Vielmehr haben wir schon vor etlichen Jahren ausgefeilte rechtliche Methoden für Schläge gegen Cyber-Verbrecher entwickelt.

Davon abgesehen verfügen wir über das umfangreichste Compliance-Portfolio in der Branche und wir waren die Ersten, die wichtige Standards wie den ISO/IEC-27018-Datenschutz-Standard für Cloud-Dienste übernommen haben. Außerdem können wir wahrscheinlich aus mehr IT-Sicherheitsereignissen lernen als andere Anbieter: Der Microsoft Intelligence Security Graph sammelt Informationen von mehr als einer Milliarde Windows-Rechnern, von unseren weltweiten Rechenzentren und Cloud-Diensten. Diese Informationen bündelt der Security Graph und verwandelt sie dann per Machine Learning in verwertbare Informationen über bisher nicht gesehene Angriffsmuster, so dass aktive Gegenmaßnahmen zum Schutz der Daten unserer Kunden ergriffen werden können.

Den Zeiten, in denen erfolgreiche Angriffe für 200 oder mehr Tage unentdeckt blieben, bereitet der Security Graph ein Ende.

Und schon lange, bevor die Cloud überhaupt ein Thema war, haben wir mit der Trustworthy-Computing-Initiative, seinerzeit noch von Bill Gates ins Leben gerufen, etliche Sicherheitsprozesse eingeführt, die heute als Best Practices in der ganzen IT-Welt gelten. Darunter professionelle, verlässliche Prozesse für Sicherheitsupdates oder die Zusammenarbeit mit wohlmeinenden Hackern weltweit.

IDC: Die DSGVO verwendet den Begriff „Stand der Technik" in Bezug auf die Einführung von Technologie und Prozessen für den Datenschutz. Sind Ihre Lösungen und Ihr Angebot auf dem neusten Stand der Technik? Wie begründen Sie dies?

Aslaner: Um diese Frage zu beantworten, möchte ich ein wenig ausholen: Der Begriff „Stand der Technik" taucht im Artikel 25 der DSGVO auf. Also als Untermenge des Abschnitts zu „Datenschutz durch Technikgestaltung". Der englische Begriff hierfür lautet „Data protection by design". Microsoft hat schon im Jahr 2004 mit dem Security Development Lifecyle ein Rahmenwerk zum Entwickeln möglichst sicherer Software eingeführt. Seither ist der SDL zwingender Bestandteil sämtlicher Entwicklungsbemühungen und gilt auch für unsere Cloud-Angebote. Zwei Kernkomponenten des SDL sind „Privacy by Design" und „Privacy by default".

Letztlich fordert die EU-Datenschutz-Grundverordnung also das, was Microsoft schon seit mehr als einem Jahrzehnt lebt: Wir berücksichtigen Datenschutzbelange schon zur Planungsphase und wählen möglichst konservative Datenschutz-Standardeinstellungen. Von daher bin ich fest davon überzeugt, dass alle unsere Produkte dem Stand der Technik entsprechen.

IDC: Welches sind aus Ihrer Sicht die wichtigsten drei Erfolgsfaktoren, die Unternehmen unbedingt berücksichtigen müssen, um rechtzeitig compliant zu sein?

Aslaner: Es gibt an sich nur einen Erfolgsfaktor: Das Top-Management muss sich der DSGVO annehmen. Die Unternehmensführung muss dafür Sorge tragen, dass das Einhalten der Vorgaben nicht als reines IT- beziehungsweise Rechtsthema gesehen wird. Denn letztlich können diese beiden Fachbereiche nur gemeinsam für DSGVO-Konformität sorgen. Und auch der Aufruf zur Datensparsamkeit muss aus der Führungsetage kommen: Daten, die man als Organisation gar nicht erst sammelt, muss man auch nicht aufwändig schützen.

Milad Aslaner
Senior Product Manager, Cyber Security, Microsoft Deutschland

Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte:
Katja Schmalen, Marketing Director, +49 69 90502-115 oder kschmalen@idc.com.

IDC CENTRAL EUROPE GMBH

Hanauer Landstr. 182 D
60314 Frankfurt • Germany
T: +49 69 90502-0
F: +49 69 90502-100
E: info_ce@idc.com
www.idc.de

IDC
ANALYZE THE FUTURE