35. Jahrgang / Nr. 1, Februar 2019

<kes>

Die Zeitschrift für Informations-Sicherheit

ISSN 1611-440X

BSI Forum

offizielles Organ des BSI

Bundesamt für Sicherheit in der Informationstechnik

Windows 10:
Stand der Dinge in Sachen Security

S. 44

Kryptografie:
Warum wichtige Algorithmen von Quantencomputern bedroht sind

S. 24

DSGVO
Unterschätzte Aufgaben und aktuelle Urteile

ab S. 54

DATAKONTEXT

Brandherd Office & Co.

Unstrukturierte Daten – die wahre Herausforderung bei der Pflicht zum Löschen personenbezogener Daten

Datensparsamkeit endet nicht bei der Erhebung und Verarbeitung, sondern fordert auch ein regelmäßiges Löschen nicht länger benötigter personenbezogener Daten. Wo solche Informationen in unstrukturierten Daten (bzw. Dateien) vorliegen, ist das eine besondere Herausforderung. Der vorliegende Beitrag zeigt, welche Herausforderungen bei der Umsetzung eines Datenschutz-Löschkonzepts für unstrukturierte Daten existieren und was man dabei dringend beachten sollte.

Von Stefan Van, Hamburg

Die vielleicht größte und häufig unterschätzte Herausforderung in Sachen EU-Datenschutzgrundverordnung (DSGVO) ist die unternehmensseitige Pflicht zur Löschung personenbezogener Daten. Diese sind zeitnah zu löschen oder zu anonymisieren, nachdem der zugrunde liegende Verarbeitungszweck (inkl. Aufbewahrungsplicht), für den die Daten ursprünglich erhoben wurden, erfüllt ist (Art. 5 Abs. 1 lit. e DSGVO). Dass sich hinter der Erfüllung dieser einzelnen Anforderung ein Projekt- und Umsetzungsaufwand von bis zu mehreren Millionen Euro verbergen kann, ahnen nur die wenigsten.

Dabei ist die Anforderung zur Löschung von personenbezogenen Daten nicht neu und existierte bereits nach altem BDSG. Viele Unternehmen sahen in der Vergangenheit jedoch über die Umsetzung hinweg und akzeptierten das Risiko einer Non-Compliance. Verstärkt wurde diese Haltung durch den scheinbar unverhältnismäßig hohen antizipierten Aufwand und die dem gegenüberstehenden geringen möglichen Geldbußen. Mit dem Inkrafttreten der DSGVO und den nunmehr sehr hohen potenziellen Geldbußen hat das Thema der Datenlöschung wieder an Aufmerksamkeit und Prominenz gewonnen.

Besondere Aufmerksamkeit sollte man dabei personenbezogenen Daten widmen, die in unstrukturierter Form vorliegen. Hierzu gehören zum Beispiel Formate wie PDF, Excel, Word, aber auch Scans und Hardcopies sowie E-Mails.

Anders als bei personenbezogenen Daten, die in den Datenbanken einschlägiger Applikationen gespeichert und somit an einem zentral definierten Ort zu finden sind, werden unstrukturierte Daten häufig an undefinierten Speicherorten auf dem Netzlaufwerk mehrfach abgelegt. Erschwerend kommt hinzu, dass selbst erstellte Datenobjekte oft zusätzlich im Entwurfsstand und/oder auf lokalen Festplatten vorliegen.

Herausforderungen

Selbst wo sich Unternehmen bereits mit der Definition und Umsetzung eines Datenschutz-Löschkonzepts beschäftigen, widmen sie sich häufig lediglich den strukturierten Daten in Applikationen. Dies ist aus Sicht des Datenschutzes ungenügend, da personenbezogene Daten, die vor und nach diesen Applikationen verarbeitet werden, ebenfalls vom Löschkonzept abzudecken sind. Sechs Herausforderungen der Datenlöschung bei unstrukturiert gespeicherten Daten werden im Folgenden näher erläutert.

Übersicht über Existenz und Speicherorte relevanter Datenobjekte

Im Hinblick auf strukturierte Daten haben Unternehmen in der Regel einen guten Überblick darüber, in welchen genutzten Applikationen personenbezogene Daten verarbeitet werden. Hinsichtlich unstrukturierter Daten fehlt es den Verant-

wortlichen jedoch meist an Transparenz: In welchen Unternehmensbereichen welche personenbezogenen Daten verarbeitet und wo diese gespeichert werden, ist nur rudimentär bekannt. Man benötigt jedoch genaue Kenntnis darüber, unter welchem exakten Pfad welche relevanten Datenobjekte abgelegt sind.

Häufig kommen noch erschwerende Faktoren hinzu, zum Beispiel Entwurfsstände oder die multiple Ablage von vereinzelten Dokumenten. Grundsätzlich ist davon auszugehen, dass eine Löschung des richtigen Dokuments nutzlos ist, solange noch Entwurfsstände oder Kopien davon existieren.

Netzlaufwerke als Speicherort

In vielen Unternehmen herrscht die gängige Praxis, elektronische Datenobjekte auf dem eigenen Netzlaufwerk abzuspeichern. Häufig existieren dort abteilungsspezifische Ordnerstrukturen, die sich weiter nach Themen oder zuständigen Mitarbeitern untergliedern lassen. Grundsätzlich ist gegen diese Praktik nichts einzuwenden, doch hinsichtlich der Pflicht zur Datenlöschung liegen wesentliche Schwachpunkte vor: Ein Netzlaufwerk stellt „by Design" keine Information zur Verfügung, ob beziehungsweise wann ein definiertes Trigger-Event (s. u.) stattgefunden hat.

Auch die Informationen zum Erstellungsdatum und dem letzten Änderungszeitpunkt sind kein geeigneter Anhaltspunkt zur Identifikation von zu löschenden Datenobjekten: Das Erstellungsdatum sagt lediglich aus, wann ein Datenobjekt erstellt wurde, nicht aber, ob es noch gültig beziehungsweise der zugehörige Vorgang noch in Kraft ist (z. B. rechtlich gültiger Vertrag). Und die technische Information des letzten Änderungsdatums wird häufig durch den Zugriff der Backupläufe aktualisiert. So wird ein Datenobjektzugriff propagiert, der von keinem realen Benutzer durchgeführt wurde.

Das größte Defizit besteht jedoch in der fehlenden technischen Unterstützung einer automatisierten Löschung von Datenobjekten – jede Löschung muss der Benutzer daher manuell durchführen.

Existenz definierter Verarbeitungszwecke

Voraussetzung für die Festlegung von Löschregeln (s. u.) sind zugrundeliegende Verarbeitungszwecke: Grundsätzlich muss jedes Unternehmen dazu in der Lage sein, ein Datenobjekt, das personenbezogene Daten enthält, einem legitimen, definierten Verarbeitungszweck zuzuordnen.

In der Praxis lässt sich jedoch branchenübergreifend beobachten, dass es oft zu Schwierigkeiten bei der Definition von Löschregeln kommt, weil die zugrunde liegenden Verarbeitungszwecke noch gar nicht definiert waren. In der Konsequenz kommen langwierige Diskussionen mit Fachbereichen auf, die sich ungern von ihren angesammelten personenbezogenen Daten trennen möchten.

Definition von Löschregeln auf Ebene unstrukturierter Daten

Eine Löschregel besteht aus einem festzulegenden Trigger-Event und einer Aufbewahrungsdauer: Unter einem Trigger-Event versteht man dasjenige auslösende Ereignis, in dem oder durch das der definierte Verarbeitungszweck erfüllt wird und eine festzulegende Aufbewahrungsdauer zu laufen beginnt. Die Aufbewahrungsdauer bestimmt also, wie lange ein Datenobjekt nach dem Eintreten des Trigger-Events noch aufzubewahren ist.

In Verbindung mit der Schwierigkeit, überhaupt alle relevanten Datenobjekte und ihre Speicherorte zu kennen, besteht die große Herausforderung darin, eine spezifische Löschregel je Datenobjekt zu definieren: Je nach Unternehmensgröße kann das bis zu mehrere hundert Datenobjekte umfassen. Zu dem großen Arbeitsaufwand, der sich dahinter verbirgt, kommen noch fachliche

Herausforderungen, die ebenfalls nicht zu unterschätzen sind.

Die Festlegung der **Trigger-Events** ist in der Praxis meist viel wichtiger als die datenschutzrechtliche Aufbewahrungsdauer und wird häufig unterschätzt. Es kann sich dabei zum Beispiel um ein Erstellungsdatum (z. B. Zeugniserstellung), Fristende (z. B. Vertragsende), das Ende eines Vorgangs (z. B. erfolgreiche Plausibilitätsprüfung) oder ein Ereignis (z. B. Kündigung) handeln.

Diese Beispiele verdeutlichen, dass die Festlegung von Trigger-Events einen großen Einfluss auf den Lebenszyklus personenbezogener Daten haben kann. Eine ungeeignete Festlegung kann einerseits dazu führen, dass personenbezogene Daten zu früh gelöscht werden, obwohl sie für den Verarbeitungszweck noch erforderlich sind – andererseits kann dies auch eine zu späte Löschung bewirken, sodass personenbezogene Daten ohne weiteren legitimen Zweck verarbeitet beziehungsweise gespeichert werden (Datenschutzverstoß!).

Eine weitere große Herausforderung besteht darin, zu identifizieren, wann der jeweilige Trigger-Event eingetreten ist. Zudem lassen sich nicht immer eindeutige Trigger-Events definieren: Das trifft beispielweise auf Kontaktinformationen zu, die über eine zur Verfügung gestellte Visitenkarte erhoben wurden. In diesem Fall liegt eine implizite (nicht dokumentierte) Einwilligung der betroffenen Person vor, was eine legitime Verarbeitung beziehungsweise Speicherung ermöglicht. Beispielsweise nach mehrfach erfolglosen Kontaktversuchen über einen längeren Zeitraum stellt sich aber die Frage, ob die gespeicherten Kontaktinformationen weiterhin legitim verarbeitet beziehungsweise gespeichert werden dürfen.

Die vormalige Unternehmenssicht beschränkte sich häufig auf die gesetzlichen Aufbewahrungspflichten mit dem Fokus, wie lange Daten (einschließlich Datenobjekte) *mindestens* aufzubewahren sind. Die DSGVO fordert nun eine neue Sicht, die sich um die Kernfrage dreht, wie lange man personenbezogene Daten *maximal* aufbewahren darf. Bei der **datenschutzrechtlichen Aufbewahrungsdauer** ist es besonders heikel, wenn dieselbe Art von Daten aus Datenschutzsicht zu unterschiedlichen Zeitpunkten gelöscht werden muss – dies erscheint zunächst sehr irritierend.

Anhand des Beispiels eines (akzeptierten bzw. abgelehnten) Antrags für eine private Krankenversicherung, für die grundsätzlich identische personenbezogene Daten eingereicht wurden, soll diese Schwierigkeit näher veranschaulicht werden: Obwohl es sich in beiden Fällen bei den Antragsdaten um gleichartige Datenobjekte handelt, muss der private Krankenversicherer die personenbezogenen Daten von akzeptierten und abgelehnten Anträgen zu unterschiedlichen Zeitpunkten löschen. Der wesentliche Unterschied ist das Vorhandensein des legitimen Verarbeitungszwecks: Ein akzeptierter Antrag wird aller Voraussicht nach zu einem rechtskräftigen Versicherungsvertrag führen – ergo einer Legitimierung zur Vertragserfüllung (Art. 6 Abs. 1 lit. b i. V. m. Art. 9 Abs. 2 lit. a DSGVO): Alle bis dahin erhobenen personenbezogenen Daten werden für die Erfüllung und die laufende Abwicklung des Vertrags benötigt und dürfen beziehungsweise müssen bis zum Vertragsende verarbeitet werden.

Im Fall eines abgelehnten Antrags kommt jedoch kein Versicherungsvertrag zustande – ein Verarbeitungszweck liegt somit nicht (länger) vor, die erhobenen personenbezogenen Daten sind zeitnah zu löschen. Der private Krankenversicherer muss daher eine entsprechende Löschregel definieren, die zwei unterschiedliche Aufbewahrungsdauern berücksichtigt, um beiden Szenarien gerecht zu werden. Da im Versicherungsumfeld langjährige Verträge nichts Ungewöhnliches sind, könnte ein Fehler hierbei dazu führen, dass personenbezogene Daten über mehrere Jahrzehnte hinweg ohne legitimen Verarbeitungszweck gespeichert bleiben.

Berücksichtigung von Abhängigkeiten

Eine weitere, vielen Unternehmen unbekannte Herausforderung ist die Identifikation und Berücksichtigung von Abhängigkeiten zwischen verschiedenen Geschäftsvorfällen. Eine ungenügende Berücksichtigung solcher Abhängigkeiten kann dazu führen, dass Datenobjekte mit personenbezogenen Daten zu früh gelöscht werden, obwohl man sie grundsätzlich noch legitim verarbeiten dürfte. In der Konsequenz könnten Geschäftsvorfälle nicht mehr nachvollzogen werden, da Datenobjekte und Informationen zum erforderlichen Zeitpunkt nicht mehr zur Verfügung stehen.

Zur Verdeutlichung soll das fiktive Beispiel einer langjährigen Herstellergarantie (15 Jahre) für ein Produkt (Maschine) dienen: Basierend auf einer bilateralen Abstimmung mit dem Rechnungswesen hat der Datenschutzbeauftragte eines Unternehmens die Löschregel definiert, alle Datenobjekte, die personenbezogene Daten enthalten und im Zusammenhang mit dem Verkauf von Maschinen stehen, 10 Jahre nach erfolgreicher Verkaufsabwicklung zu löschen (das erfasst z. B. Anfrage, Kaufvertrag und Lieferschein). Ausgangspunkt und Grundlage zur Festlegung dieser Löschregel war die Orientierung an den handelsrechtlichen Aufbewahrungspflichten von Geschäfts- und Handelsbriefen. Sollten sich nun Kunden im letzten Drittel ihrer Garantiezeit in der Serviceabteilung melden, um Garantieansprüche geltend zu machen, lässt sich aufgrund der bereits gelöschten Datenobjekte im Unternehmen nicht mehr feststellen, wann die einzelnen Maschinen tatsächlich verkauft worden sind.

Hätte sich der Datenschutzbeauftrage vorab mit der Serviceabteilung abgestimmt und Kenntnis von Garantiefällen nach über 10 Jahren gehabt, dann würde die Löschregel höchstwahrscheinlich anders definiert worden sein (Trigger-Event: Ablauf Garantieanspruch – datenschutzrechtliche Aufbewahrung: 10 Jahre).

Praxistipps

Grundsätzlich ist das Thema Datenlöschung inklusive der dazugehörigen Löschregeln sehr branchen- und unternehmensspezifisch zu betrachten. Dennoch lassen sich aufgrund der Projekterfahrung des Autors hilfreiche Ratschläge ableiten, die universell berücksichtigt werden können und im Folgenden dargestellt sind.

Datenobjekt-orientiere Perspektive

Dokumentieren Sie, in welchen unstrukturierten Datenobjekten personenbezogene Daten enthalten und wo diese auf dem Netzlaufwerk gespeichert sind – legen Sie hierzu am besten ein Register an. Im Zuge der Registererstellung empfiehlt es sich, einzelne Abteilungs-Workshops durchzuführen.

Bei Bedarf bietet es sich an, zu jedem Datenobjekt noch folgende Informationen (Auszug) hinzuzufügen:

- welcher Verarbeitungszweck zugrunde liegt,
- was die rechtliche Verarbeitungsgrundlage ist,
- welcher Abteilung der Nutzer/Ersteller angehört,
- in welchen Prozessen das Datenobjekt verwendet wird,
- wo das Datenobjekt abgespeichert (z. B. Pfad) wird,
- welche gesetzlichen oder aufsichtsrechtlichen Pflichten neben dem Datenschutz zu berücksichtigen sind und
- die zugehörige Löschregel, bestehend aus Trigger-Event und datenschutzrechtlicher Aufbewahrungsdauer.

Dokumentierte Argumentation der Löschregel

Diverse Male konnte in der Praxis bereits beobachtet werden, dass man den Hintergrund selbst dokumentierter Löschregeln später nicht mehr nachvollziehen konnte. Folglich ist zu empfehlen, für jedes unstrukturierte Datenobjekt auch festzuhalten, aus welchen Gründen die jeweilige Löschregel so festgelegt wurde. Damit gewinnen die Löschregeln deutlich an Substanz, Aussagekraft und Nachvollziehbarkeit und man ist im Fall eines internen oder externen Audits deutlich sicherer aufgestellt.

Anhaltspunkte zur Löschung überfälliger Datenobjekte

Da eine Lösung zur automatisierten Löschung auf Netzlaufwerken noch nicht absehbar ist, muss man sich anderweitig behelfen: Halten Sie folglich Ausschau nach praktikablen Anhaltspunkten, die Ihnen eine solche Datenlöschung erleichtern. Im Idealfall können Sie auf bestehende Quellen oder Medien zurückgreifen, mit denen schnell zu erkennen ist, welche Fälle zu löschen sind. Hierbei kann es sich beispielsweise um eine systemgenerierte Liste aller inaktiven Verträge handeln, mit deren Hilfe man die im Zusammenhang stehenden Datenobjekte auf einem Netzlaufwerk identifizieren und löschen kann.

Verarbeitungszwecke

Machen Sie sich bewusst, dass identische Arten personenbezogener Daten für verschiedene Verarbeitungszwecke verarbeitet werden können, die unterschiedliche Löschregeln nach sich ziehen. Es empfiehlt

sich dann, betroffene Datenobjekte zu duplizieren und separat abzuspeichern: Somit ist sichergestellt, dass die Datenlöschung aufgrund des einen Verarbeitungszwecks den anderen Verarbeitungszweck nicht tangiert.

Haftung berücksichtigen

Alle relevanten Datenobjekte, die in einem Zusammenhang mit Vorfällen einer existierenden oder möglichen Haftung stehen, sollten mindestens so lange aufbewahrt werden (ohne Berücksichtigung der handels- und steuerrechtlichen Aufbewahrungspflichten), bis dieses Haftungsverhältnis nicht mehr besteht.

Vererbung von Löschregeln

Gibt es eine Abhängigkeit zwischen zwei vermeintlich unterschiedlichen Datenobjekten, so ist es mit hoher Wahrscheinlichkeit legitim, die zeitlich kürzere datenschutzrechtliche Aufbewahrungsdauer durch die längere des anderen Datenobjektes zu ersetzen (Vererbung).

Dies ist für alle Fälle anwendbar, in denen eine vorzeitige Löschung des Datenobjekts mit der zeitlich kürzeren datenschutzrechtlichen Aufbewahrungsdauer die Nachvollziehbarkeit des anderen Datenobjekts beeinträchtigen würde. Durch die Vererbung erhalten beide Datenobjekte zumindest dieselbe Aufbewahrungsdauer – in vielen Fällen dürfte es auch sinnvoll sein, die komplette Löschregel (inkl. Trigger-Event) zu vererben.

Deklaration von Datenobjekten als interne Kontrollen

Sofern unstrukturierte Datenobjekte, die personenbezogene Daten enthalten, im Rahmen einer Kontrollhandlung (Überwachung, Abstimmung, Abgleich etc.) genutzt werden, lassen sich diese als interne Kontrollen im Sinne des internen Kontrollsystems (IKS) erachten. Solche Datenobjekte können (gemäß Handelsgesetzbuch) mit einer Aufbewahrungsdauer von 10 Jahren versehen werden. Diese Deklaration bietet sich besonders gut für Situationen an, in denen ansonsten kein legitimer Verarbeitungszweck vorläge.

Fazit & Ausblick

Der vorliegende Beitrag hat ausgewählte Herausforderungen und Lösungsansätze erörtert, die im Zuge eines einjährigen Umsetzungsprojekts zur Datenlöschung identifiziert beziehungsweise umgesetzt wurden – es handelt sich dabei um Erkenntnisse aus vielen Diskussionen, Meetings und getroffenen Entscheidungen. Die in letzter Zeit oft erwähnte Norm DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten" stellt zwar an vielen Stellen hilfreiche Leitfäden zur Verfügung, doch fehlt es ihr oftmals am Praxisbezug.

Zwei weitere, hier nicht thematisierte Herausforderungen sind die Datenlöschung von/in E-Mails sowie strukturierten Daten in Applikationen – beide bringen jeweils ihre eigenen Schwierigkeiten mit sich: Während es bei der Löschung von E-Mails zu einem emotionalen Widerstand der Belegschaft kommen kann, die E-Mails gerne als Archivierungssystem nutzt, bedeutet das Sicherstellen einer Datenlöschung in Applikationen größeren technischen Umsetzungsaufwand.

Wer glaubt, mit der Umsetzung der Datenlöschung noch hinreichend Zeit zu haben, irrt sich übrigens: Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat beispielsweise bereits in einer Pressemitteilung vom 7. November 2018 verkündet, drei Großkonzernen einen Fragenbogen mit 50 Punkten zugeschickt zu haben, um die datenschutzrechtliche Rechenschaftspflicht (Accountability) zu prüfen. Mit sehr hoher Wahrscheinlichkeit wurden die Angeschriebenen unter anderem auch dazu aufgefordert darzulegen, wie sie die Löschung personenbezogener Daten in den Bereichen „strukturiert", „unstrukturiert" und „E-Mail" sichergestellt haben. Es dürfte nur eine Frage der Zeit sein, bis andere Aufsichtsbehörden nachziehen oder/und auch KMU bezüglich der Datenlöschung auditiert werden. ■

Stefan Van (www.xing.com/profile/Stefan_Van) ist freiberuflicher Unternehmensberater für Datenschutz mit dem Schwerpunkt Data-Retention and -Deletion.