www.jusletter-it.eu

Wolfgang Schnabl

Datenschutz und Informationssicherheit – ein natürlicher Gegensatz?

Information security and data protection are concepts that are generally hard to concile. The more monitoring is provided, the better the security. But, ideally, data protection implies no processing of personal data at all. A business security concept inevitably requires the processing of personal data, and the GDPR itself also demands security measures. ISO/IEC 27001 is an international standard describing a security management system. The GDPR describes an identical system. This standard allows common considerations of data protection and information security. (ah)

Category: Articles
Region: Austria
Field of law: Data Protection, IT Security

Citation: Wolfgang Schnabl, Datenschutz und Informationssicherheit – ein natürlicher Gegensatz?, in: Jusletter IT 24-Mai-2018

Inhaltsübersicht

1. Einführung

[Rz 1] Datenschutz ist ein Grundrecht, das sich bereits in der Konvention zum Schutze der Menschenrechte und Grundfreiheiten findet und sich aus dem Recht auf Achtung des Privat- und Familienlebens herleitet (Art. 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten [EMRK][1]). Gerade mit der zunehmenden Digitalisierung gewinnt auch Datenschutz immer mehr an Bedeutung. Jeder Mensch hinterlässt umfangreiche Spuren auf Rechnern, durch die Benutzung des Internets, ja selbst auf Internet-of-Things (IoT) Geräten. Wir alle sind inzwischen zu gläsernen Menschen geworden, vollkommen durchsichtig für den Staat und viele Unternehmen. Dadurch ist die freie Meinungsäußerung massiv beeinträchtigt und es besteht letztendlich Gefahr für unsere Demokratie.

[Rz 2] Dieser Entwicklung de«Abkehr vom Datenschutz» tritt die Datenschutzgrundverordnung (DSGVO)[2] entgegen. Diese gibt strenge Vorgaben hinsichtlich der Verarbeitung personenbezogener Daten vor. Grundsätzlich ist jede Verarbeitung verboten, außer eine solche ist nach Art. 6 DSGVO explizit erlaubt.

[Rz 3] Informationssicherheit auf der anderen Seite benötigt umfangreiches Wissen über Vorgänge im digitalen, aber auch analogen Umfeld, um effizient Gefahren von Unternehmen und Personen abwehren zu können. Im Idealfall «weiß» Informationssicherheit alles.

[Rz 4] Informationssicherheit und Datenschutz sind somit Konzepte, die sich grundsätzlich schlecht miteinander vereinbaren lassen. In der Praxis werden bei der Auswertung von Logfiles zur Fehlersuche etwa IP-Adressen analysiert, also personenbezogene Daten nach dem Verständnis der DSGVO (Erwägungsgrund #30). Troubleshooting im E-Mailbereich bringt es unvermeidbar mit sich, dass Administratoren auch Mailinhalte sehen. Datenschutz führt zu komplexen Zugangsstrukturen auf Fileservern und in Datenbanken.

[Rz 5] Aber nicht nur ein umfassendes Sicherheitskonzept eines Unternehmens erfordert zwangsläufig die Verarbeitung personenbezogener Daten, auch die DSGVO selbst fordert Nachvollziehbarkeit, Integrität und Vertraulichkeit. Eine gemeinsame Betrachtung von Datenschutz und Informationssicherheit ist daher zwingend notwendig.

---

1 Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten samt Zusatzprotokoll (BGBl. Nr. 210/1958, 210).

2 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG («Datenschutz-Grundverordnung», DSGVO), ABl. L 119 vom 4. Mai 2016, S. 1 f.

2. Informationssicherheit

[Rz 6] Daten und Informationen sind für Unternehmen heute wichtiger Bestandteil der Unternehmensstrategie. Dabei können Informationen sowohl auf Papier, in Rechnern als auch in Köpfen gespeichert sein. Die sichere Verarbeitung dieser Informationen ist daher für alle Unternehmen von existenzieller Bedeutung. Als Informationssicherheit bezeichnet man Eigenschaften von informationsverarbeitenden Systemen, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Der alte Begriff «IT-Sicherheit» bezeichnet Maßnahmen zur Absicherung von IT-Geräten und ist somit nur ein Teil der Informationssicherheit. Diese wird heute umfassend verstanden und beinhaltet neben der IT-Sicherheit auch die Sicherheitsorganisation, Compliance, interne Vorgaben, Mitarbeiter-Know-how und Security-Awareness, Kontrollmaßnahmen sowie Datenschutz.

[Rz 7] Die Bedrohungen für Informationen werden täglich mehr und ändern sich auch ständig. Ein umfassender Schutz von Informationen kann nur mit einem übergreifenden Konzept sichergestellt werden, das neben technischen Maßnahmen zur Risikominimierung auch organisatorische Maßnahmen sowie Unterstützung durch die Benutzer beinhaltet. Um neuen Bedrohungen entgegenzuwirken sowie Änderungen der IT-Infrastruktur mit einzubeziehen, muss ein solches Konzept regelmäßig überarbeitet und angepasst werden.

[Rz 8] Ein solch übergreifendes Konzept, das Security aktiv managt, wird Informationssicherheitsmanagementsystem (ISMS) genannt. Heute hat sich eine universell anwendbare, internationale Methodologie durchgesetzt, der ISO/IEC 27001 Standard[3]. Dieser Standard erlaubt es, Best-Practices zu implementieren und die korrekte Implementierung auch von einer unabhängigen Stelle zertifizieren zu lassen.

[Rz 9] Ein ISMS arbeitet nach dem Grundsatz des kontinuierlichen Verbesserungsprozesses, indem der Deming-Kreis angewendet wird. Dieser iterative Prozess besteht aus den Schritten Plan – Do – Check – Act und beschreibt in den einzelnen Phasen die Festlegung, den Betrieb, die Überwachung, die Überprüfung, die Instandhaltung sowie die Verbesserung eines ISMS.

[Rz 10] Ein ISMS legt den Fokus der Sicherheit auf Prävention, also Erkennen und Verhindern von Angriffen und Bedrohungen, bevor ein Schaden eintritt. Dazu müssen alle Systeme umfassend überwacht werden, sowie die aufgezeichneten Daten ausgewertet und korreliert werden.

[Rz 11] Ein umfassendes Wissen über alle Aktivitäten im System ist somit die nötige Voraussetzung und Grundlage einer guten Security. Dabei können sich Angriffe oft über Wochen oder Monate hinziehen, um so unter dem Radar von Intrusion Detection Systemen zu bleiben. Auch Advanced Persistent Threats (APT) stellen eine Herausforderung dar, da sich hier Angreifer bereits im Unternehmensnetzwerk befinden und nur schwer – etwa durch Analyse des «normalen» Benutzerverhaltens und dadurch Erkennen von Anomalien – aufgespürt werden können. Verschlüsselte Internetzugriffe stellen besondere Bedrohungen des Unternehmensnetzwerkes dar, da sie alle Sicherheitsmaßnahmen an der Grenze zum Internet umgehen.

[3] ISO/IEC 27001:2013 Information Technology – Security Techniques – Information Security Management Systems – Requirements (https://www.iso.org/isoiec-27001-information-security.html [alle Websites zuletzt aufgerufen am 6. Mai 2018]).

3. Datenschutz in der Informationssicherheit

[Rz 12] Logeinträge von Ereignissen sind die Grundbausteine der Informationssicherheit. Das Minimum an Information, die in einem Logeintrag gespeichert werden muss, sind der Zeitstempel des Ereignisses, die Fehlermeldung, der Erfolg oder Fehlschlag des Ereignisses, die Quell- und Ziel-IP-Adresse, die Benutzerkennung, die das Ereignis auslöst, sowie auf welche Ressourcen zugegriffen wird.

[Rz 13] Die für Security relevanten Daten sind, wie oben ersichtlich, sehr oft personenbezogene Daten. Verbindungsdaten, IP-Adresse, E-Mailadresse, Benutzerkonto müssen meist im Log mitprotokolliert, Mailinhalte analysiert sowie verschlüsselte Verbindungen aufgebrochen werden, um sinnvolle und aussagekräftige Feststellungen über Angriffe oder Regelverstöße zu ermöglichen. Die angeführten Beispiele stehen auf den ersten Blick im Widerspruch zu Grundprinzipien des Datenschutzes.

3.1. Aufbewahrungsdauer

[Rz 14] Logfiles können bei langsam durchgeführten, langdauernden Angriffen sinnvollerweise erst nach Monaten (und nicht wenigen Tagen, wie bei herkömmlichen Angriffen) gelöscht werden. Eine sich daraus ergebende Schwierigkeit besteht darin, den Zweck der Datenverwendung nach Art. 5 Abs. 1 lit. b DSGVO eindeutig festzulegen, und zwar mit einer Eindeutigkeit, aus der sich eine Löschfrist i.S.d. lit. e leg. cit. ergibt. Wie im obigen Beispiel gezeigt, sollte die Löschfrist viele Monate oder Jahre betragen, damit auch hochentwickelte und anspruchsvolle Angriffe erkannt werden können. 2008 ging die österreichische Datenschutzkommission von einer Aufbewahrungsfrist für Logfiles von wenigen Tagen bis max. zwei bis drei[4] Wochen aus. Eine so kurze Aufbewahrungsdauer ist auf Grund moderner Angriffsszenarien in der heutigen Internet-Welt aus Security-Sicht sicherlich fahrlässig.

3.2. Profiling

[Rz 15] Analyse und Vorhersagen von Benutzeraktivitäten sind klassische Profiling-Aktivitäten i.S.d. Art. 4 Z. 4 DSGVO, nämlich die automatisierte Verarbeitung personenbezogener Daten, um das Verhalten einer natürlichen Person zu analysieren oder vorherzusagen.

[Rz 16] In der Praxis verwenden moderne Sicherheitslösungen Anomalie-Erkennung. Splunk[5], ein verbreitetes Log-, Monitoring- und Reporting-Tool sammelt etwa mittels User Behavior Analytics Aktivitätsdaten und lernt typische Verhaltensweisen mit. Gute Intrusion Detection Systeme arbeiten ebenfalls mit Anomalieerkennung. Ebenso sind herkömmliche Virenscanner bei heutigen Angriffen weitgehend machtlos. Aus diesen drei Beispielen ist zu erkennen, dass moderne Sicherheits-Software nicht mehr ausschließlich mit Signaturdateien arbeitet, sondern Angriffe durch signaturlose Anomalieerkennung aufzuspüren versucht.

[Rz 17] Jede Anomalieerkennung basiert auf einer umfassenden Logfile-Analyse. Dabei werden zwangsläufig personenbezogene Daten in großem Umfang verarbeitet. Auch wenn das Ziel nicht

4 DSK 20. Juni 2008, Zl. K121.358/0009-DSK/2008.

5 https://de.wikipedia.org/wiki/Splunk.

das ausspionieren der Benutzer ist, wird das normale Benutzerverhalten als Referenz gespeichert und laufend analysiert.

3.3. Verschlüsselung

[Rz 18] Daten, die über Netzwerke übertragen werden, können grundsätzlich abgehört und auch verändert werden. Unverschlüsselte Internetverbindungen, auf denen kritische Daten übertragen werden (z.B. Logindaten zur Bank, Zahlungsdaten zum Online-Shop, Gesundheitsdaten zur Krankenkassa oder zur Versicherung), aber auch WLAN-Verbindungen werden heute ausnahmslos verschlüsselt. Durch eine verschlüsselte Internetverbindung wird sichergestellt, dass Informationen über den Inhalt des Datenaustausches nur zwischen den beiden Endgeräten, etwa dem PC des Benutzers und dem Server seiner Bank, sichtbar sind.

[Rz 19] Dadurch wird aber jegliche Sicherheitsmaßnahme, die ein Unternehmen an der Grenze zum Internet trifft, etwa Firewall, Virenschutz oder URL-Analyse, umgangen, da nun keine Sicherheitssoftware mehr den Datenverkehr analysieren kann. Was bei legitimen Transaktionen hingenommen werden kann, verleitet Hacker inzwischen dazu, ihre Phishing- oder Schadcode-Webseiten ebenfalls nur mehr verschlüsselt erreichbar zu machen. Die einzige Möglichkeit, sich solchen Bedrohungen zu stellen, ist, die verschlüsselte Verbindung aufzubrechen und somit die vertraulichen Daten des Benutzers einer Analyse zugänglich zu machen. Dies ist inzwischen Standard in der Informationssicherheit.

4. Informationssicherheit im Datenschutz

[Rz 20] Die DSGVO selbst legt großen Wert auf Informationssicherheit. Bereits in Art. 5 Abs. 1 lit. f DSGVO, den Grundsätzen für die Verarbeitung, wird festgelegt, dass personenbezogene Daten in einer Weise verarbeitet werden müssen, die eine angemessene Sicherheit dieser Daten gewährleistet.

[Rz 21] Moderne Bedrohungen und Angriffsvarianten auf Informationen vervielfachen heute die Menge an personenbezogenen Daten, die aus Security-Gründen verarbeitet werden müssen. In die Jahre gekommene Sicherheits- und Datenschutzkonzepte sind nicht mehr anwendbar und müssen sorgfältig und professionell überarbeitet werden.

4.1. Risikoanalyse

[Rz 22] Wie kann nun festgestellt werden, welche Sicherheit angemessen ist? In der Informationssicherheit wird dies durch eine Risikoanalyse ermöglicht. Gerade der ISO/IEC 27001 Standard verlangt zu jedem Unternehmenswert (Asset) eine solche, um Bedrohungen abschätzen und adäquate Maßnahmen treffen zu können. Bereits in der Planungsphase des ISMS muss eine Vorgehensweise erarbeitet werden, Risiken im ISMS-Prozess zu adressieren, zu analysieren und zu behandeln (Kapitel 6.1.1, 6.1.2 und 6.1.3 ISO/IEC 27001:2013). Und, wie es ein kontinuierlicher Verbesserungsprozess verlangt, ist diese Risikoanalyse und -behandlung regelmäßig zu wiederholen (Kapitel 8.2 und 8.3 ISO/IEC 27001:2013), um eine Verbesserung des Sicherheitsniveaus zu erreichen.

[Rz 23] Genau diese Vorgehensweise gibt auch die DSGVO vor. Vor allem im Art. 32 DSGVO werden geeignete technische und organisatorische Maßnahmen verlangt, um ein dem Risiko für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind. Dies entspricht den Vorgaben des ISO/IEC 27001 Standards.

4.2. Technische und organisatorische Maßnahmen

[Rz 24] Der ISO/IEC 27001 Standard gibt in seinem Anhang A 14 Kontrollbereiche (Domains) 114 Maßnahmen (Controls) vor, die in technische (Verschlüsselung, Access Control), organisatorische (Sicherheitsrichtlinien, Compliance) und personelle (Personalsicherheit, z.B. Schulungen) unterteilt werden. Dies entspricht den technischen und organisatorischen Maßnahmen der DSGVO. Aber auch die personellen Maßnahmen werden in der DSGVO gefordert, etwa bei den Aufgaben des Datenschutzbeauftragten, der für die Sensibilisierung und Schulung der Mitarbeiter gem. Art. 39 Abs. 1 lit. b DSGVO zuständig ist.

5. Ergebnis

[Rz 25] Moderne Sicherheitsmaßnahmen widersprechen in zunehmendem Maße der Datenschutzidee (Detailierungsgrad und Umfang von Logeinträgen, Profiling der Mitarbeiter, Aufbrechen von Verschlüsselung). Bestehende Sicherheitskonzepte müssen daher sorgfältig an die Vorgaben der DSGVO angepasst werden.

[Rz 26] Mit Hilfe eines Informationssicherheits-Managementsystems werden bereits grundlegende Vorgaben der DSGVO erfüllt. Insbesondere für Themen wie Privacy-Impact-Analysen, Risikoanalysen, technische/organisatorische Maßnahmen, Datenschutz-Zertifizierungen etc. erleichtert ein Informationssicherheits-Managementsystem nach ISO/IEC 27001 die Arbeit des Datenschutzbeauftragten erheblich.

Wolfgang Schnabl, Datenschutz- und IT-Security Consultant, ISO 27001 Lead Auditor, Business Protection – Schnabl GmbH.