DSGVO – DAS SCHRECKGESPENST IST DA

Am 25. Mai 2018 war es nach einer zweijährigen Übergangsfrist soweit und die Datenschutz-Grundverordnung der EU trat in Kraft. Dieser Artikel zeigt, welchen Einfluss diese Verordnung für die Informationssicherheit hat.

von Andreas Wisler

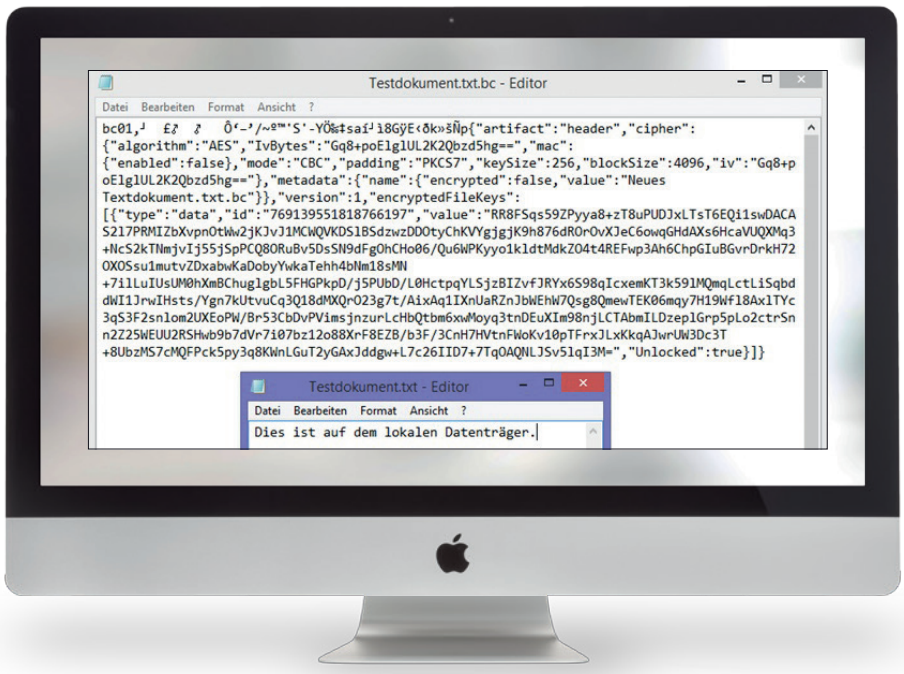
Die neue Datenschutz-Grundverordnung hat das Ziel, eine einheitliche, EU-weite Regelung in Bezug auf die Verarbeitung von personenbezogenen Daten sicherzustellen. Dies gilt für Unternehmen, die Dienstleistungen an EU-Bürgerinnen und Bürger anbieten, unabhängig davon, ob sie einen Sitz innerhalb oder ausserhalb der Europäischen Union haben.

ANWENDUNGSBEREICH

Die DSGVO gilt für die Verarbeitung personenbezogener Daten. Es spielt dabei keine Rolle, ob dies automatisiert oder nicht automatisiert erfolgt. Bei der Verarbeitung ist es auch unabhängig davon, ob die Daten elektronisch oder zum Beispiel auf Papier verarbeitet werden. Anfang Juli 2018 hat ein Gericht entschieden, dass dies auch für Notizen gilt, die bei Türverkäufen erstellt werden.

Was sind aber personenbezogene Daten? In Artikel 4, Nr. 1 steht: «alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden «betroffene Person») beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann». Beispiele dafür sind Name, Wohnort, Geburtsdatum, Personalnummer, Parteizugehörigkeit, etc.

Bei der Verarbeitung sind sowohl das Erheben (Daten beschaffen), Speichern, Ändern, Übermitteln, Verknüpfen (mit anderen Daten) oder auch Löschen gemeint. Das bedeutet, es spielt keine Rolle, wer was mit den Daten anstellt. Die Ausnahme bilden nur persönliche oder familiäre Bearbeitungen.



Das oben stehende Bild zeigt einmal die verschlüsselte Datei auf einem Cloud-Speicher und via der Software Boxcryptor geöffnet.

VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

In einem ersten Schritt sollte ein Verzeichnis von Verarbeitungstätigkeiten erstellt werden. In Artikel 30 ist ausführlich beschrieben, was darin zu erfassen ist. Es sind dies:

- Namen und Kontaktdaten des/r Verantwortlichen
- Zweck der Verarbeitung
- Erfasste Kategorien
- Empfänger der Daten, allenfalls Angabe der Drittländer
- Übermittlung der Daten, inkl. allfälliger Drittländer
- Fristen zur Löschung der Daten
- Beschreibung der technischen und organisatorischen Massnahmen (TOM)

GRUNDSÄTZE DER VERARBEITUNG VON PERSONENBEZOGENEN DATEN

Grundsätzlich ist es nicht erlaubt, mit personenbezogenen Daten zu arbeiten. Entweder existiert dazu eine Rechtsgrundlage oder es liegt eine Einwilligung für diese Datenbearbeitung vor. Diese Einwilligung muss freiwillig sein und wird für einen bestimmten Zweck abgegeben (Zweckbindung). Die betroffene Person muss klar und verständlich über den Verwendungszweck und über einen Widerruf informiert worden sein.

Werden die erhobenen Daten nicht mehr benötigt und es gibt auch keine Aufbewahrungsvorschriften mehr, müssen die Daten gelöscht oder so verändert werden, dass kein Personenbezug mehr möglich ist.

IT-SICHERHEIT

Der Artikel 32 DSGVO erwähnt die klassischen Schutzziele der Informationssicherheit: «Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.»

PSEUDONYMISIERUNG

Der Artikel 4 der DSGVO beschreibt dies wie folgt: «die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Massnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden».

Für eine Datenbank könnte dies beispielsweise ein Hash-Wert sein. Dieser ist nicht umkehrbar. Von Vorteil wird ein sicheres Verfahren wie SHA-2 oder SHA-3 verwendet. MD5 und SHA-1 gelten nicht mehr als sicher, da bereits erfolgreiche Angriffe darauf stattgefunden haben.

VERSCHLÜSSELUNG

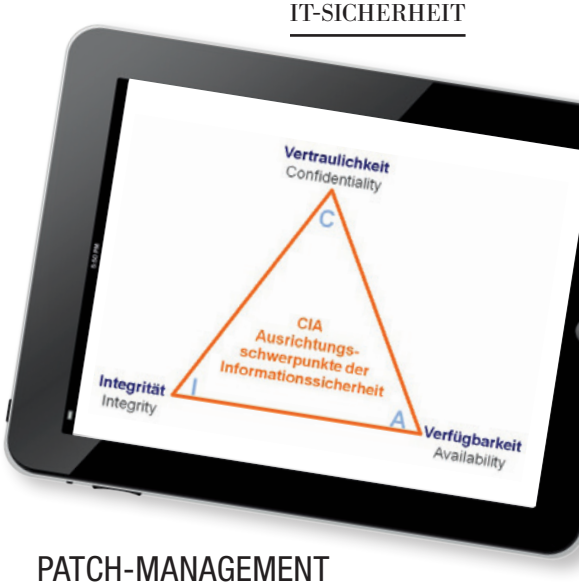
Die Verschlüsselung kann an verschiedenen Stellen genutzt werden:

- E-Mail-Server: Gemäss dem Bayrischen Landesamt für Datenschutzaufsicht genügt es bereits auf dem E-Mail-Server STARTTLS und Perfect Forward Secrecy zu verwenden. Dabei kommunizieren die Server untereinander verschlüsselt. Die Verbindung zwischen dem sendenden und empfangenden Server ist damit für einen Dritten nicht einsehbar, d. h. der Transport der Nachricht ist geschützt.
- Webseite: Auf einer Webseite muss zwingend HTTPS verwendet werden. Die Daten sind dabei für einen Dritten nicht einsehbar, der sich in die Verbindung einschleichen will. Auch für Kontaktformulare muss die sichere Variante verwendet werden.
- Dateien, Dokumente und Nachrichten: ein einfaches Verfahren, ist es, die Dateien / Dokumente direkt zu verschlüsseln. 7-ZIP wäre ein Programm, welches die Daten sicher verschlüsseln kann (beispielsweise mit AES-256). Bei E-Mails kommen S/MIME oder PGP zum Einsatz.
- Cloud: Daten in der Cloud sind nicht verschlüsselt, auch wenn der Transport der Daten in der Regel über HTTPS erfolgt. Der Cloud-Anbieter kann jederzeit auf die Daten zugreifen. Diesem Umstand gilt es grosse Beachtung zu schenken. Die Daten sollten daher immer verschlüsselt abgelegt werden, dies unabhängig, ob das Rechenzentrum in der Schweiz oder der EU liegt. Eine Variante ist die Software Boxcryptor. Sie stellt eine Mittelschicht zwischen lokalem Rechner und Cloud-Dienstleister zur Verfügung (unter Windows das Laufwerk X, auf einem Mac ein zusätzliches Laufwerk). Alle Daten, die via dieses Laufwerk abgespeichert werden, sind verschlüsselt.
- Mobile Geräte: egal ob es sich um Handys, Tablets oder Laptops handelt, alle diese Geräte sind zu verschlüsseln. Dabei genügt es bereits, die vom Hersteller
- implementieren Funktionen zu nutzen.

WIEDERHERSTELLUNG / BACKUP

Die DSGVO verlangt, dass die personenbezogenen Daten, inkl. Zugang bei physischen oder technischen Zwischenfällen rasch wiederhergestellt werden können. Dazu muss eine den Anforderungen angepasste Backup-Strategie erstellt werden. Auch ein Business Continuity sollte in Betracht gezogen werden. Das BCM kommt bei einem grösseren Ereignis zum Zuge und hilft, nach einem Vorfall schnell wieder produktiv arbeiten zu können.

Passwort	Als Hashwert (SHA512)
abcdef	cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e
abcdeg	ab32117f498c6f319c42ff67d7f005cba8f683626743c321d40cf7f3dfaaa49e558fb189610d78f18d6e06d3a6784840b3b5ce5fa6b0964666782e5fce7a2a83
abcdeh	7c2d1ccee8df211f043483b5c582362a6414be34b7ee4db5164359c39cbe5ea5240ce022e2f00fbb2f31dd5c0da7593b78b820cc8ebacf6f9dc2849e2b2ea2e1



PATCH-MANAGEMENT

Jede Software hat Schwachstellen. Daher ist es wichtig, wenn Schwachstellen erkannt werden, schnell und angepasst darauf reagieren zu können. In einem ersten Schritt sollte das Risiko dieser Schwachstelle bewertet werden. Sind Sofortmassnahmen notwendig? Oder kann dies im gewohnten Patch-Rhythmus (zum Beispiel monatlich) erfolgen? Entweder erfolgt ein ausserordentlicher Termin oder während des Wartungsfensters wird die Schwachstelle durch den Patch (Software, welche die Schwachstelle behebt) beseitigt.

REGELMÄSSIGE ÜBERPRÜFUNG

Weiter steht im Artikel 32, dass mittels eines zu definierenden Verfahrens regelmässige Überprüfungen, Bewertungen und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen erfolgen muss. Es genügt also nicht, einmal eine Massnahme umzusetzen und danach nichts mehr. Diese Kontrollen sind unbedingt schriftlich festzuhalten: Welches Resultat wurde erzielt? Welche Schwächen erkannt? Welche Schritte wurden eingeleitet?

Mit diesen Schritten kann der Datenschutz einfach und nachhaltig erhöht werden. Das einfachste ist aber immer noch, nur die Daten zu sammeln, die auch benötigt werden. Damit kann die Gefahr einer Busse massiv reduziert werden.

KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen
Telefon +41 (0)52 511 37 37

info@goSecurity.ch
www.goSecurity.ch