IT-Sicherheitskonzept

WOLLSCHLÄGER GBR
KANZLEIMARKETING imPuls

Technisch-organisatorische Maßnahmen (TOM) (Art. 32 DSGVO, §64 BSDG-neu)

Zielbeschreibung:
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 wurden folgende geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Verhältnismäßigkeit:
Durch das Verhältnismäßigkeitsprinzip, welches sich mittelbar in Art. 32 DSGVO wiederfindet, schränken sich die TOM-Vorgaben marginal wieder selbst ein. Art. 32 DSGVO spricht nämlich davon, dass die Implementierungskosten der Maßnahmen zu berücksichtigen sind.
Die wirtschaftliche Angemessenheit ist also zu berücksichtigen. Beispielsweise können die TOM eines Kleinbetriebs aus wirtschaftlichen Aspekten nicht in allen Bereichen die gleichen Standards haben wie die TOM eines Großkonzerns.

Zutrittskontrolle (Räume und Gebäude)

***Zielbeschreibung**:*
Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden bzw. in denen personenbezogene Daten gelagert werden.

Alle Anwendungen befinden sich auf angemieteten Servern der großen europäischen Hoster (Strato, Ionos oder Hosteurope). Anwendungen laufen grundsätzlich auf eigenen Servern und nicht auf einer Maschine des Hosters als eine Anwendung unter vielen.

Die Rechenzentren verfügen in der Regel mindestens über einen Sicherheitsbereich mit einer Eingangskontrolle. Meistens sind die Gelände eingezäunt und Video überwacht. Neben der Überwachung finden regelmäßige Kontrollgänge durch das Sicherheitspersonal statt. Der Zutritt wird durch ein elektronisches Zutrittskontroll-System ermöglicht und somit wird der Zugang zum Data-Center nur autorisierten Personen ermöglicht.

Zugangskontrolle (IT-Systeme, Anwendungen)

***Zielbeschreibung**:*
Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

Unsere Subunternehmerin, die EDV-Beratung Dölle, vermietet Anwendungen an den Kunden. Der Kunde entscheidet alleine und ausschließlich darüber, welche personenbezogenen Daten in welcher Weise verarbeitet werden (Herr der Daten).

Alle Anwendungen werden durch einen individuellen Zugang kontrolliert. Beim Anlegen der Benutzer müssen bestimmte Kriterien für das Passwort und den Benutzernamen erfüllt sein, um einen neuen Benutzer erfolgreich aufsetzen zu können. Innerhalb der Anwendungen ist durch ein Rollen- und Rechte-System der Zugang nur zu den Daten möglich, die die jeweilige Rolle vorsieht.

Im Weiteren werden beispielhaft 2 Szenarien beschrieben, die die Anwendungen automatisch abwehren können. Weitere Maßnahmen werden zum Schutz der Maßnahmen nicht genannt.

Hack-Versuche von außen werden erkannt und mit entsprechenden Maßnahmen abgeblockt. Um z. B. Brute-Force Angriffe abzuwehren wird ein Zugang vom System nach 3 falschen Passwort-Eingaben für mind. 30 Minuten gesperrt. Jeder weitere Versuch sperrt den Account um weitere 30 Minuten.

Auf allen Anwendungs-Servern ist ein Programm installiert, das erkennt ob versucht wird, eine Anwendung systematisch auf Schwachstellen von außen zu “testen”. Wird solch ein Versuch erkannt, wird die jeweilige IP-Adresse für 4 Stunden gesperrt.

Zugriffskontrolle (auf Daten)

***Zielbeschreibung**:*
Es ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und das personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

In allen Anwendungen wird der Zugriff auf die Daten mittels geeigneter Methoden kontrolliert. Vor fast jedem Datenbank-Zugriff wird kontrolliert, ob die selektierten Daten auch mit dem angemeldeten Benutzer eingesehen werden können. Auf Systemen mit besonders sensiblen Daten wird z.B. das sog. Session Hijacking dadurch verhindert, dass ein Benutzer nur ein einziges Mal zur gleichen Zeit angemeldet sein kann. Hierzu werden die Session-Daten mit der IP-Adresse verknüpft. Nach Abmeldung werden die aufgezeichneten Session-Daten direkt wieder gelöscht.

Weitergabekontrolle (von Daten)

***Zielbeschreibung**:*
Es ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Grundsätzlich erfolgt der Zugriff auf die Anwendungen über eine verschlüsselte Verbindung. So ist sichergestellt, dass während des Transports die Daten geschützt sind. Alle administrativen Zugriffe auf die Server erfolgen über eine SSL-verschlüsselte Session. Alle Backups werden verschlüsselt, bevor sie auf einen zentralen Backup-Server übertragen werden.

Eingabekontrolle (In Datenverarbeitungssystemen)

***Zielbeschreibung**:*
Es ist zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in die Anwendungen eingegeben, verändert oder gelöscht wurden.

Innerhalb der Anwendungen ist für sensible Bereiche immer zu sehen, wer den Datensatz als Letzter verändert hat. Außerhalb der Anwendungen läuft eine sog. Log-Datei mit, die jeden Zugriff mit Datum, Uhrzeit und IP-Adresse protokolliert. Mit Hilfe dieser Dateien kann die aufgeführte Zielbeschreibung umgesetzt werden.

Auftragskontrolle (des Auftragsnehmers)

Zielbeschreibung:
Es ist zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Mit den hier eingesetzten Hostern, Ionos und Hosteurope sind entsprechende AVs abgeschlossen. Es sei hier noch darauf hingewiesen, dass die angemieteten Server unter unserer Kontrolle stehen also eine Auftragsverarbeitung im klassischen Sinne nicht besteht.

Verfügbarkeitskontrolle (von Daten)

Zielbeschreibung*:*
Es ist zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

In den Rechenzentren der genutzten Hoster besteht i.d.R. mindestens eine unterbrechungsfreie Stromversorgung (USV) sowie ein Überspannungsschutz. Ebenso sind ein Branderkennungs- und Frühwarnsystem implementiert. Die Löschsysteme sind auf eine möglichst zerstörungsfreie Brandbekämpfung ausgelegt.
Zusätzlich werden die Sicherungen der einzelnen Server verschlüsselt auf weiteren Servern und lokalen NAS abgelegt. So ist sichergestellt, dass bei einem Defekt eines Servers keine Daten verloren gehen.

Datentrennungskontrolle (zweckbezogen)

Zielbeschreibung*:*
Es ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Innerhalb der Anwendungen werden die Daten immer nur zu einem Zweck erhoben. Die einzelnen Anwendungen sind vollkommen voneinander getrennt (teilweise sogar in unterschiedlichen Rechenzentren).

Pseudonymisierung (auf Daten)

Zielschreibung*:*
Es ist zu gewährleisten, dass Datenschutzgrundsätze, wie etwa Datenminimierung, wirksam umgesetzt und die notwendigen Garantien in die Verarbeitung aufgenommen werden, um den Anforderungen dieser Verordnung zu genügen.

In allen Anwendungen werden vom System nur der Benutzername sowie eine E-Mail Adresse zwangsweise benötigt und auch verarbeitet. Diese Daten können zu keinem Zeitpunkt pseudonymisiert werden, da ansonsten keine Anmeldung mehr erfolgen kann. Alle anderen Daten werden vom Kunden selber im System hinterlegt (Herr der Daten) und entziehen sich somit unserer Kontrolle. Wird ein Vertrag beendet, so werden am auf das Kündigungsdatum folgenden nächsten Werktag die kompletten Daten aus dem System gelöscht, sofern der Kunde seine eigenen Daten gelöscht hat. Solange noch Kunden-Daten auf dem Server vorliegen, wird der Vertrag weitergeführt und eine Löschung der Anmeldedaten erfolgt nicht.

Stand 05.06.23