T O M Technisch organisatorische Maßnahmen

Jan Steffens und Rainer Steffens (Feb 14, 2017)

ZUTRITTSKONTROLLE

Maßnahmen, damit Unbefugten der Zutritt zu den Datenverarbeitungsanlagen verwehrt wird, mit denen personenbezogene Daten verarbeitet werden:

Der Zutritt zu Arbeitsplatzrechnern und Servern ist über eine kontrollierte protokollierte Schlüsselvergabe gewährleistet. Die Räume sind grundsätzlich verschlossen. Der Zutritt für Besucher wird durch eigenes Personal kontrolliert.

Die Räume des Auftragnehmers sind mit Bewegungsmeldern ausgestattet. Im Falle eines unbefugten Betretens der Räume erfolgt automatisch eine Signalisierung per Alarmaufschaltung bei einem externen Sicherheitsdienstleister zur Auswertung. Im Falle eines unbefugten Zutritts erfolgt die Aktivierung eines Alarms und Alarmierung der örtlichen Polizei sowie der Geschäftsleitung. Die Bewegungssequenzen werden zusätzlich auf einem räumlich abgesetzten Speicher abgelegt.

Das Rechenzentrum des Auftragnehmers ist zusätzlich mit einem elektronischen Zugangssystem ausgestattet. Im Falle eines Zutritts wird der Zutritt als Bewegungssequenz aufgezeichnet. Die Bewegungssequenzen werden 30 Tage in einem abgesetzten Speicher aufbewahrt.

ZUGANGSKONTROLLE

Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -verfahren benutzen:

Der Zugang zu Endgeräten von Mitarbeitern wird durch ein persönliches Passwort geschützt.

Die Änderung der Passwörter wird alle 6 Monate systemseitig erzwungen. Die Passwortkomplexität gemäß BSI Empfehlung wird ebenfalls systemseitig erzwungen.

Der Zugang von außen auf das Netz des Auftragnehmers wird durch verschlüsselte Verbindungen sichergestellt. Externe Zugriffe auf sensible Daten werden zusätzlich mit einer Zwei-Faktor-Authentifizierung mit einmal Passwörtern abgesichert.

Firewall Systeme schirmen das Netzwerk gegen unerlaubten Zugriff aus dem Internet ab. Verbindungen zu Kunden werden über VPN Gateways oder gesicherte Fernadministrationstools hergestellt. Zugriffe werden dokumentiert.

Mitarbeiter erhalten nur im Rahmen Ihrer Tätigkeit Zugriff auf die zur Vertragserfüllung notwendigen Systeme und Daten.

Die vom Auftraggeber zur Authentifizierung eingerichteten und an den Auftragnehmer übergebenen Zugangskennungen und Passwörter aus Systemen des Auftraggebers, verlassen den Personenkreis der Berechtigten nicht. Sie werden in gesicherten Bereichen auf IT-Systeme des Auftragnehmers hinterlegt und sind nur dem Personenkreis zugänglich, der diese für die Erbringung der vereinbarten Dienstleistung zwingend benötigen.

Vom Auftragnehmer generierte Passwörter haben eine Länge von mindestens 8 Zeichen und enthalten mindestens eine Ziffer und ein Sonderzeichen sowie Groß- und Kleinbuchstaben. Die Weitergabe an den Auftraggeber erfolgt grundsätzlich mit einem Passwortverschlüsselten Dokument. Das Passwort für die Entschlüsselung wird ausschließlich telefonisch mitgeteilt.

Im Falle eines Betriebs außerhalb der Räume des Auftragnehmers ist die Verbindung zum Zugangssystem des Auftraggebers ist mit einer 256Bit SSL Verschlüsselung gegen eine „man in the middle attack“ geschützt.

ZUGRIFFSKONTROLLE

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Befugten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können:

Soweit technisch machbar, werden An- und Abmeldungen der Benutzer an den DV-Arbeitsstationen und den Anwendungen protokolliert. Internetzugriffe und Mailverkehr werden datenschutzkonform protokolliert.

Eine Auswertung erfolgt zur technischen Fehleranalyse oder Verdacht eines Richtlinienverstoßes im Rahmen des technisch und organisatorisch Machbaren sind angemessene Abstufungen der Zugriffsberechtigten aufgebaut.

Diese Erlauben das Eingeben, Lesen, Kopieren, Verändern oder Entfernen von Auftraggeber-Daten bei der Verarbeitung, Nutzung und nach der Speicherung nur in dem für die jeweilige Aufgabe erforderlichen Umfang.

Die Zugriffsberechtigten werden durch eine begrenzte Anzahl an System- und Anwendungsadministratoren verwaltet.

Die Aufbewahrung von Sicherungsdatenträgern erfolgt in gesicherten Bereichen, zu denen nur das betroffene Betriebspersonal und die Geschäftsleitung Zutritt haben.

Ausgemusterte Datenträger werden datenschutzgerecht entsorgt. Vorzugsweise sind Einmalsicherungscodes zu verwenden.

WEITERGABEKONTROLLE

Maßnahmen, die 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.

Personenbezogene Daten werden nur zweckgebunden und vertraulich an Geschäftspartner übermittelt. Die Verschlüsselung erfolgt entsprechend dem Stand der Technik. Personenbezogene Daten werden derzeit nur falls erforderlich und nur an Unterauftragnehmer übermittelt.

Aus betriebserforderlichen Gründen sind Büro- und Produktionsräume des Auftragnehmers auf verschiedene Standorte verteilt. Personenbezogene Daten des Auftraggebers werden im Rahmen betriebsüblicher und betriebsnotwendiger Prozesse zwischen den Standorten übermittelt.

Die Übertragung erfolgt über gesicherte Internet-Infrastrukturen über das Internet. In diesem Fall wird grundsätzlich VPN-Technik nach aktuellem Stand angewendet.

Der Transport von Sicherungsdatenträgern, die personenbezogene Daten enthalten, erfolgt ausschließlich durch besonders ausgewählte und eingewiesene Mitarbeiter des Auftragnehmers. Die Daten sind grundsätzlich verschlüsselt auf den Datenträgern gespeichert.

EINGABEKONTROLLE

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind.

Die Eingabekontrolle wird über technische und organisatorische Maßnahmen dokumentiert. Bei Servicezugriffen werden Mitarbeiter, Partner, Kunde sowie Datum, Beginn und Ende mit Kurzbeschreibung der erbrachten Dienstleistung dokumentiert. Zusätzlich wird die Eingabekontrolle über Systemprotokolle dokumentiert.

AUFTRAGSKONTROLLE

Maßnahmen die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

Voraussetzung für eine Auftragsdatenverarbeitung ist ein schriftlicher Vertrag.

Der Auftragnehmer setzt zur Steuerung der Aufträge ein Transaktionssystem ein in dem die Anforderungen, die Arbeitsanweisungen und die Umsetzung dokumentiert werden. Die Qualität der Dokumentation wird laufend durch das Qualitätsmanagement des Auftragnehmers kontrolliert.

VERFÜGBARKEITSKONTROLLE

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

Der Auftragnehmer rüstet die relevanten DV-Systeme mit einem geeigneten Schutz gegen Viren, Trojaner, Würmer und sonstige Malware aus und gewährleistet dadurch einen hinreichenden Schutz gegen Verletzung der Systemintegrität durch die vorgenannten Gefahren.

Die Ausführung arbeitsplatzfremder Software wird, soweit technisch möglich, durch technische Maßnahmen und durch organisatorische Regelung verhindert. Betriebssysteme und Schutzsoftware werden in angemessenen Zeitabständen aktualisiert. Dafür betreibt der Auftragnehmer ein zentrales Patchmanagement in dem alle relevanten DV-Systeme integriert sind.

In den Produktionsräumen stehen zum Schutz der Produktionseinrichtungen unterbrechungsfreie Stromversorgungen, Rauchmeldeanlagen, Feuerlöschgeräte und doppelt ausgeführte Klimaanlagen zur Verfügung. Die Produktionsräume werden zusätzlich auf Abweichungen des Raumklimas und Kohlenmonoxid-Dichte überwacht.

Der Datenbestand wird einmal täglich vollständig auf externen Speichermedien gesichert. Diese Speichermedien werden täglich an einen entfernten gesicherten Standort verbracht. Die Daten sind auf den mobilen Sicherungsmedien verschlüsselt gespeichert.

Es werden regelmäßige testweise Rücksicherungen auf eine produktionsnahe Testumgebung durchgeführt. Das Datensicherungskonzept sieht das Auslagern von Sicherungsmedien aus den Sicherungszyklen vor. Dies geschieht alle vier Wochen. Für die anzunehmenden Notfallarten wurde existieren Notfallpläne, die regelmäßig validiert und aktualisiert werden.

TRENNUNGSKONTROLLE

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Der Auftragnehmer nutzt personenbezogene Daten nur für interne Zwecke im Rahmen des Auftrages oder der Kundenbeziehung. Die Daten werden entsprechend des Auftrages getrennt gespeichert. Alle Mitarbeiter sind angewiesen und geschult, Daten nur im Rahmen der Dienstleistungserbringung und zur Wahrung der Zweckbindung zu erheben, zu verarbeiten und zu nutzen.