Kreisverwaltung Mettmann

Technisch Organisatorische Maßnahmen Kreisverwaltung Mettmann

Kreis Mettmann

Inhalt

1 Einleitung

Ein sehr wichtiger Bereich des Datenschutzes und der IT-Sicherheit sind die technischen und organisatorischen Maßnahmen, die getroffen werden müssen, damit das Recht auf informationelle Selbstbestimmung gewährleistet ist und die personenbezogenen Daten vor Missbrauch, Fehlern und Unglücksfällen möglichst sicher sind. Im Folgenden werden die technischen und organisatorischen Maßnahmen des Kreises Mettmann dargestellt.

2 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Das Ziel einer Zutrittskontrolle ist es, Unbefugten den Zutritt (z.B. zu Datenverarbeitungsanlagen) zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden. Der Begriff des Zutritts ist dabei räumlich zu verstehen. Den vorschriftsgemäßen Zutritt zu IT-Bereichen stellen wir durch folgenden Maßnahmen sicher:

- Protokollierte Vergabe von Zutrittsberechtigungen
- Entzug der Zutrittsberechtigung nach Ausscheiden
- Türsicherungen (elektrische Türöffner) mit Chipkarte
- Elektronisches Zutrittskontrollsystem mit Protokollierung
- Dokumentierte Schlüsselvergabe an Mitarbeiter
- Richtlinien zur Begleitung von Gästen in IT-Räumen
- Zutritt im IT-Bereich nur nach Anmeldung mit Besucherkontrolle, Begleitung und Einweisung
- Alarmanlage für Außensicherung (Türen, Fensteröffnungskontakte)

Zugangskontrolle

Das Ziel einer Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte in Datenverarbeitungsanlagen und -systeme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, eindringen oder diese nutzen können. Um den Zugang zu unserem Netzwerk zu schützen, haben wir folgende Maßnahmen getroffen:

- Benutzerverwaltung zur Anmeldung
- Individueller Benutzername und Passwort

- Segmentierung von Netzwerken nach Schutzbedürftigkeit
- Einsatz von mehreren Virenscannern
- Einsatz einer mehrstufigen Firewall
- Einsatz sicherer Übertragungstechnik (VPN)
- Einsatz von 2-Faktor Authentisierung
- Passwortregelung (Technisch sichergestellte Anforderungen für Länge und Komplexität)
- Einsatz von Festplattenverschlüsselung
- Einsatz eines Web-Security-Gateways
- Authentifizierung von IT-Systemen im internen Netz

ZUGRIFFSKONTROLLE

Das Ziel einer Zugriffskontrolle ist zu gewährleisten, dass ausschließlich die zur Benutzung der Datenverarbeitungssysteme Berechtigten auf die ihrer Zugriffsberechtigung entsprechenden personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können. Um unerlaubte Tätigkeiten innerhalb der Systeme des Kreises Mettmann außerhalb der eingeräumten Berechtigungen zu verhindern, haben wir folgende Maßnahmen getroffen:

- Rechtevergabe nach Rollen / Organisationseinheiten
- Regelung für Einrichtung, Änderung und Entzug von Berechtigungen
- Verwaltung der Zugriffsrechte durch Administrator
- Datenschutzkonforme Entsorgung von Datenträgen und Papier
- Durch regelmäßige Sicherheitsupdates und Backups (nach dem jeweiligen Stand der Technik) wird sichergestellt, dass unberechtigte Zugriffe verhindert werden
- Revisionssicheres, verbindliches Berechtigungsvergabeverfahren
- Automatische Erzeugung von Protokolldateien, wo technisch möglich und sinnvoll, sowie die anlassbezogene Auswertung dieser Logs im berechtigten Verdachtsfall. Zyklische automatische Löschung durch Rotation

Trennungskontrolle

Das Ziel des Trennungsgebots ist zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten ebenfalls getrennt voneinander verarbeitet werden.

Um sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden, haben wir die folgenden Maßnahmen getroffen:

- Funktionstrennung durch mandantenfähige Systeme
- Erstellung eines Berechtigungskonzepts und Rechtevergabe nach Rollen
- Trennung von Netzen, insbesondere zwischen Internet (Außenwelt) und Intranet (Internes Netz)
- Umsetzung von Multi-Tier-Architekturen mit abgestuften Sicherheitsbereichen und Schutzmechanismen (z.B. Firewalls, Intrusion Detection Systems, o.a.)
- Verschlüsselungen und Tunnelverbindungen (SSL, VPN)
- Protokollierung von Übertragungsvorgängen

3 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Das Ziel einer Weitergabekontrolle ist zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, vervielfältigt, verändert oder entfernt werden können und dass überprüft sowie festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten zur Datenübertragung vorgesehen ist. Folgende Maßnahmen haben wir in Bezug auf die Weitergabe von personenbezogenen Daten getroffen:

- Sichere Aufstellung von Servern und SAN / NAS (Sicherheitsbereich)
- Unternehmenseigene Domain zur E-Mail-Kommunikation (intern)
- Weitergabe von (schützenswerten) Daten an Dritte nur nach Prüfung der Rechtsgrundlage
- Sichere Übertragung von Datenlieferungen (SFTP, VPN, HTTPS)
- Beschränkung des zur Übermittlung befugten Personenkreises

Eingabekontrolle

Das Ziel einer Eingabekontrolle ist, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Systeme und Anlagen zur Datenverarbeitung eingegeben, verändert oder entfernt worden sind. Die Nachvollziehbarkeit innerhalb der Datenverwaltung stellen wir wie folgt sicher:

- Protokollierung der Eingabe personenbezogener Daten
- Zweckfestlegung der Protokolldaten

4 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Das Ziel der Verfügbarkeitskontrolle ist zu gewährleisten, dass personenbezogene Daten gegen die Zerstörung oder Verlust physisch sowie auch logisch geschützt sind.

- Sicherungs- und Wiederherstellungskonzept
- Einsatz von Festplattenspiegelung
- Einsatz unterbrechungsfreier Stromversorgung
- Vermeidung von Single-Point-of-Failures als Grundgedanke aller Infrastruktur im Rechenzentrumsbetrieb, d.h. Sicherstellen von Verfügbarkeit durch Redundanz von Systemen und Komponenten
- Einsatz einer Netzersatzanlage
- Datensicherung, d.h. Backup wird räumlich getrennt vorgehalten
- Verwendung von Firewalls und Loadbalancern zur Zugangs- und Inhalts-Filterung
- Redundante Klimaversorgung
- Einsatz geeigneter Einbruchmeldeanlagen in allen IT-Räumlichkeiten
- Einsatz geeigneter Brandmeldeanlagen in allen IT-Räumlichkeiten
- Einsatz von Löschanlagen im Rechenzentrum
- 7x24h Monitoring aller Systeme der Rechenzentrumsinfrastruktur.

- Notfallpläne (BCM)
- Vertretungsregelungen für administrative Aufgaben und Verantwortlichkeiten

5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Allgemeine Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutz-Management
- Incident-Response-Management
- Einsatz eines Data-Leakage-Prevention Systems
- Regelmäßige Prüfungen durch den Datenschutzbeauftragten

Auftragskontrolle

Das Ziel einer Auftragskontrolle im Sinne von Art. 28 DS-GVO ist es zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend des Auftrags und den Weisungen des Auftragsgebers verarbeitet werden können.

- Vertragliche Regelungen zur Verarbeitung von personenbezogenen Daten im Auftrag
- Unteraufträge nur bei gleichwertigem Schutzniveau
- Prüfung und Dokumentation beim Auftragnehmer getroffener Maßnahmen
- Sicherung von Kontrollrechten vor Ort
- Verpflichtung der Mitarbeiter von Auftragnehmern auf das Datengeheimnis

6 Weitere Maßnahmen

Organisation

Es werden folgende weitere organisatorische Maßnahmen ergriffen um alle zu verarbeitenden Daten zu schützen:

- Ernennung eines IT-Sicherheitsbeauftragten und Vertreters
- Erstellung einer IT-Sicherheitsleitlinie
- Sensibilisierung der Mitarbeiter zur Informationssicherheit
- Regelung zur sicheren Entsorgung von Datenträgern
- Regelungen zum Einsatz von mobilen Endgeräten
- Regelungen zur Internetnutzung
- Regelung von Wartungsarbeiten
- Regelungen zur Einführung von Hard- und Software
- Regelungen für Wachschutz

KOMMUNIKATION

Folgende Maßnahmen werden zusätzlich ergriffen um die Kommunikation mit Vertragspartnern abzusichern:

- Fernwartungszugänge können immer nur von den lokalen Systemen aus initiiert werden
- Fernwartungen werden immer von geeignetem Fachpersonal beaufsichtigt

IT-BETRIEB

Es werden folgende weitere Maßnahmen ergriffen um einen sicheren IT-Betrieb zu gewährleiten:

- Restriktive Handhabung von Administrationskennungen
- Regelungen für Administrationstätigkeiten
- Regelmäßige Fortbildungen für Administratoren
- Protokollierung von administrativen Tätigkeiten
- Einsatz einer zentralen Softwareverteilung bzw. Patchverteilung
- Test- und Abnahmeverfahren für neue Hard- und Software
- Einsatz eines zentralen Log- und Monitoring-Systems
- Etablierte Vorgehensweise zur Behandlung von Sicherheitsvorfällen

- Gezielte Härtung der eingesetzten IT-Systeme
- Erstellung einer geeigneten IT-Betriebsdokumentation
- Geregelte Außerbetriebnahme und Entsorgung von IT-Komponenten
- Einsatz geeigneten Systemen zur Erkennung und Verhinderung von IT-Sicherheitsvorfällen
- Einsatz von Hochverfügbarkeitsarchitekturen
- Einsatz von virtuellen IT-Systemen
- Zentrale Verwaltung aller eingesetzten Clients

7 SCHLUSSBESTIMMUNG

Die IT-Sicherheit unterliegt beim Kreis Mettmann einem kontinuierlichen Verbesserungsprozess (PDCA-Zyklus) und wird ständig aktualisiert und angepasst. Eine Aktualisierung des Dokuments findet daher fortlaufend statt.

TECHNISCH ORGANISATORISCHE MAßNAHMEN

Kreis Mettmann

Herausgeber:

Kreis Mettmann
Der Landrat

März 2019