Technische und organisatorische Maßnahmen DIPF - TBA und Bildungsinformatik

Version: 1.0.2

Letzte Änderung: 03.07.2024

Erfasst durch: Paul Libbrecht mit Mithilfe von Roland Johannes, Björn Buchal, Helge Einspanier, Heiko Rölke, Julia Kreusch, Lisa-Marie Burgdorf und Daniel Schiffner.

Vertraulichkeit

1.1 Zutrittskontrolle

Maßnahmen, die den unbefugten Zutritt zu Datenverarbeitungsanlagen verhindern, die personenbezogene Daten verarbeiten. Der Zutritt zum Serverraum ist nur einem eingeschränkten Kreis von autorisierten Mitarbeitern möglich.

Organisatorische Maßnahmen

Empfang und Ausweispflicht Der Zutritt zum Gebäude wird tagsüber zu den normalen Geschäftszeiten durch Empfangspersonal überwacht. Interne Mitarbeiter/innen haben mit Hilfe ihrer elektronischen Schließberechtigung (Transponder) Zutritt zum Gebäude und den weiteren Geschäftsräumen.

Zutrittskontrollsystem und Überwachung Durch das elektronische Schließsystem werden den Mitarbeitenden individuelle, funktions- oder gruppenbezogene Schließberechtigungen erteilt. Alle Außenzugänge und die Bürobereiche sind mit digitalen Schließzylindern ausgerüstet. Schließvorgänge können nachvollzogen werden. Diese werden im Schloss gespeichert und auf die Mitarbeiterchips übertragen. Diese Daten werden zusätzlich zentral gespeichert.

Das elektronische Schließsystem ermöglicht nur Personen Zutritt zum TBA-Serverraum oder zur TBA-internen IT-Infrastruktur, die im Vorfeld Berechtigungen im Rahmen ihrer Aufgabenerfüllung erhalten haben.

Die Zutrittsberechtigungen werden zentral über ein Zutrittsrechtemanagement verwaltet. Hierfür existiert ein formaler Genehmigungsprozess. Bei Verlust der Zutrittskarte/Schlüssel wird diese/r sofort in dem Zugriffsrechtemanagement gesperrt. Die Sperrung ist in diesem Fall sofort auf kritischen Türen wirksam. Noch valide Berechtigungen in Zutrittskarten oder Schlüsseln verlieren automatisch nach spätestens zwei Tagen an allen Türen ihre Gültigkeit. Die Berechtigungen können unabhängig von der physischen Verfügbarkeit des Transponders geändert, gelöscht, oder gesperrt werden.

Wach- und Reinigungspersonal wird aus überprüften Firmen mit Sitz in Deutschland gestellt.

Technische Maßnahmen

Der TBA-Serverraum wird durch eine Video-Kamera überwacht.

1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungsanlagen von Unbefugten benutzt werden können. Hierzu sind technische und organisatorische Maßnahmen hinsichtlich der Benutzeridentifikation und Authentifizierung implementiert.

Organisatorische Maßnahmen

Benutzer- und Berechtigungsverfahren Benutzer, die im Rahmen ihrer Aufgabenerfüllung Zugangsrechte zu einem System erhalten sollen, müssen diese Berechtigungen über einen formalen Benutzer- und Zugangsberechtigungsprozess beantragen. Die Benutzerkennungen und -berechtigungen werden in einem Benutzerverwaltungssystem administriert. Die Vergabe von Zugriffsrechten wird über ein Ticketsystem organisiert, das den Vorgang dokumentiert. Im Benutzerverwaltungssystem werden Benutzerberechtigungen gesperrt, sobald die Zugehörigkeit einer Person zum Institut erlischt.

Externen Benutzern von Vertragspartnern ist der Umgang mit personenbezogenen Daten im Rahmen von Vertragsvereinbarungen erlaubt. Sie erhalten Zugang auf für sie speziell eingerichtete Systeme mit beschränktem Funktionsumfang, entsprechend der Vertragsvereinbarungen.

Einige Systeme sind allgemein zugänglich. Nutzer müssen sich hierzu mit einer aktiven Email Adresse anmelden und eine Aktivierung bestätigen. Dadurch erlauben Sie explizit die Verarbeitung ihrer Daten durch andere Benutzer des Systems (evtl. ohne Anmeldung, z.B. in kollaborativen Umgebungen). Vereinfachte Verfahren erlauben das automatisierte Verwalten von Zugangsdaten, solange die Benutzer über die Systeme ansprechbar bleiben. Reagieren Benutzer z.B. nicht mehr auf Reaktivierungsanfragen per Email, werden die Zugänge gesperrt.

Verträge oder Benutzerkonten können inaktiv werden, z.B. nach der Verweigerung neuer Benutzerbedingungen. Inaktive Konten sind nicht mehr benutzbar. Sie bleiben erhalten, damit das System keine Inkonsistenzen aufbaut (zum Beispiel um die Identität des Autors eines Kommentares noch sehen zu können).

Beim Ausscheiden von TBA-Mitarbeiter/-innen sind die Verfahrenshinweise zu den Ausscheidenden Benutzern von TBA maßgebend. Für den Zugang zu Systemen der DIPF-Haus-IT ist die IT-Nutzungsordnung des DIPFs anzuwenden.

Technische Maßnahmen

Authentisierungsverfahren Die Zugangsberechtigungen zu den Netzwerken (Kupfer- und Glasfasergeführtes LAN in Büros, TBA internes WLAN, und TBA-VPN) sind zentral verwaltet und nur für vertraute DIPF/TBA Systeme zugelassen. Auf technischer Ebene sind das: DHCP auf Basis der MAC-Adresse über Netzwerkkabel oder WLAN, und VPN-Server-Authentifizierung.

Zugangsberechtigungen sind so weit feingranular konfiguriert, damit Personen ihre Funktionen und Aufgaben erfüllen können. Die Berechtigungsverfahren gelten für alle Benutzer der DIPF/TBA-Systeme. Werden im Rahmen des Authentifizierungsverfahrens Passwörter eingesetzt, müssen diese den internen Passwortrichtlinien für Mitarbeiter/-innen und Systeme entsprechen.

Ein Fernzugriff auf interne Systeme ist nur in authentifizierter Form möglich, bei dem u.a. asymmetrische Authentisierungsverfahren (Public-/Private-Key-Verfahren) eingesetzt werden.

1.3 Zugriffskontrolle

Mit der Zugriffskontrolle werden unerlaubte Handlungen in den informationsverarbeitenden Systemen des DIPF mit Hilfe von Überwachung und Protokollierung der Zugriffe verhindert.

Berechtigungsvergabe

Die Systeme erlauben einen regulären Zugriff nur für interne, autorisierte Mitarbeiter/-innen aus gesicherten Netzsegmenten. Je nach Autorisierung werden differenzierte Berechtigungen für Benutzer/-innen eingerichtet, untergliedert nach Rollen und Profilen. Dabei stützt sich die Rechtevergabe darauf, dass die Benutzer/-innen dazu geschult sind, die Risiken von Passwörtern, MAC-IPs, oder private Keys einzuschätzen.

Auswertungen

Jede Art von Zugriff auf Authentifizierungssysteme wird an einen Protokollierungsserver übertragen. Bei auffälligen Zugriffsversuchen wird zusätzlich eine Alarmierung (Security Monitoring) an den/die zuständige/n Systemverantwortliche/n ausgelöst.

Veränderungen

Modifikationen an Zugriffsrechten werden ausschließlich durch Systemadministratoren/-innen des operativen Fachbereichs vorgenommen, die die Freigabe des/der Vorgesetzten erhalten haben. Veränderungen der Zugriffsrechte und Berechtigungen geschehen in der Regel innerhalb eines Arbeitstages, in dringenden Fällen

sofort. Im Produktivbereich dürfen nur Geräte eingesetzt werden, bei denen sichergestellt ist, dass vor der Nutzung eine Authentifizierung stattgefunden hat.

Löschung

Das Löschen von Nutzungsberechtigungen (z.B. nach dem Austritt einer/s Mitarbeiters/-in) erfolgt zeitnah. Im Verwaltungssystem werden Berechtigungen von Mitarbeitern/-innen gesperrt, sobald diese das Institut verlassen. Beim Ausscheiden von Mitarbeitern/-innen werden die Festplatten sicher gelöscht (z.B. multiple Rewrites). Siehe dafür die Verfahrensweise beim Ausscheiden eines Benutzers.

Integrität

2.1 Weitergabekontrolle

Im Rahmen der Weitergabekontrolle werden Maßnahmen beim Transport, der Übertragung und Übermittlung sowie bei der nachträglichen Überprüfung von personenbezogenen Daten definiert.

Organisatorische Maßnahmen

Vertrauliche Informationen Personenbezogene Daten, sowie andere Formen vertraulicher Informationen, werden nur über sichere Kommunikationswege übertragen. Dies geschieht durch verschlüsselte Kanäle (Cloud-Server via HTTPS, SSH, oder VPN). Beim Einsatz von üblicherweise unverschlüsselten Transportmechanismen, wie Emails oder USB-Sticks, werden Information zuvor verschlüsselt.

Adressaten, die den Personenbezog aus einer Datensammlung nicht benötigen, erhalten automatisch pseudonymisierte Daten.

Protokollierung Der Zugriff und die Aktivitäten von autorisierten Benutzern wird in Protokolldateien aufgezeichnet. Der Zugriff auf die Protokolle ist geschützt und nur autorisierten Administratoren/-innen gestattet. Auf den Protokollservern werden auch Verletzungen von Sicherheitsmaßnahmen protokolliert, wie z.B. nicht berechtigte Zugangsversuche oder signifikante Schutzverletzungen. Diese Protokolle, sowie alle Protokolle, sind maximal 30 Tage gelagert, wenn Sie personenbezogene Daten beinhalten oder beinhalten könnten. Danach sind sie anonymisiert oder gelöscht.

2.2 Eingabekontrolle

Um die Nachvollziehbarkeit der Datenverwaltung und -pflege zu verbessern, sind Maßnahmen zur nachträglichen Überprüfung, ob und von wem Daten eingegeben,

verändert oder gelöscht worden sind, implementiert.

Protokollauswertung

Protokollauswertungen werden stichprobenartig von den Systemadministratoren/-innen vorgenommen, insbesondere jedoch, wenn Auffälligkeiten oder der Verdacht auf eine Kompromittierung (z.B. durch eine Alarmierung / Triggering eines Events) aufgetreten ist. Die Protokollauswertungen sind als Informationen klassifiziert, die nur innerhalb des DIPF im Rahmen der Aufrechterhaltung und Sicherstellung der Systemstabilität und -sicherheit zu verwenden sind.

2.3 Auftragskontrolle (Auftragnehmer)

Das DIPF verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen. Zweck, Art und Umfang der Datenverarbeitung richten sich ausschließlich nach den Weisungen des Auftraggebers. Eine hiervon abweichende Verarbeitung erfolgt nur nach schriftlicher Einwilligung des Auftraggebers.

Das DIPF wird den Auftraggeber unverzüglich darüber informieren, wenn eine vom Auftraggeber erteilte Weisung gegen gesetzliche Regelungen verstößt. Jeder Verstoß gegen datenschutzrechtliche Vorschriften oder gegen die getroffenen vertraglichen Vereinbarungen wird dokumentiert und dem Auftraggeber unverzüglich mitgeteilt. Nicht mehr benötigte Unterlagen mit personenbezogenen Daten und Dateien werden erst nach vorheriger Zustimmung durch den Auftraggeber datenschutzgerecht vernichtet.

Personen am DIPF, die Daten im Auftrag verarbeiten, werden auf das Datengeheimnis verpflichtet.

---

3. Verfügbarkeit- und Belastbarkeitskontrolle

Organisatorische Maßnahmen

Monitoring und Notfälle Eine verteilte Monitoringinstallation erlaubt den Systemadministratoren/innen gravierende Zustandsänderungen (z.B. Festplatte bald voll, CPU-Last dauerhaft zu hoch) zu erkennen, und benachrichtigt diese redundant über unterschiedliche Kommunikationskanäle (z.B. Email, Signal-Messenger). Notfälle können damit schnell detektiert werden. Ein Notfallplan ist in Arbeit, indem der Ablauf (welche Personen werden benachrichtigt und nötige Aktionen) beschrieben sind. Siehe TBA-Notfallplan.md.

Backup-Verfahren Alle Daten werden in regelmäßigen Abständen gesichert, wobei die Sicherung physisch an einem anderen Ort aufbewahrt wird. Zum Schutz der Backups sind die zuvor genannten Zutrittskontrollen implementiert. Die

Administration der Backup-Software und der Zugriff auf die Daten sind limitiert auf dedizierte Backup-Administratoren. Die Häufigkeit von Datenbackups richtet sich nach der Wichtigkeit der Informationen und ist individuell anpassbar. Funktionalitätstests von Datenbackups werden stichprobenartig von den zuständigen Systemadministratoren/-innen vorgenommen. Siehe das Backup-Concept.

Technische Maßnahmen

Firewall und Virenschutz Die Netzwerke und IT-Systeme des DIPF sind mit einer Firewall geschützt, die regelmäßig von autorisierten Systemadministratoren/innen gewartet und aktualisiert wird. Die Firewallregeln sind so ausgelegt, dass nur benötigte Dienste erlaubt sind (etwa HTTPS zu den identifizierten Webservern oder OpenVPN zum VPN Server), und in der Grundeinstellung jeden anderen Netzwerkverkehr blockieren. Alle Internetverbindungen sind durch mindestens eine Firewall geschützt. Die Kontrolle sicherheitsrelevanter Konfigurationen erfolgt hierbei im Rahmen von Penetrationstests. Alle Netzwerkkomponenten werden regelmäßig durch automatische Scanner geprüft.

Durch Virenschutzprogramme existiert ein mehrstufiger Schutz vor Schadsoftware für Netzwerk- Gateways und IT-Systeme des DIPFs .

Hochverfügbarkeit und Stromversorgung Der Serverraum ist mit einer unterbrechungsfreien Stromversorgung (USV) ausgestattet, die auch gegen Überspannungen schützt. Kritische Systeme sind in Form einer Clusterlösung aufgesetzt.

Alle sensiblen und kritischen Systeme sind mit einem fehlertoleranten Festplattenverbund (i.d.R. RAID 5 oder Ceph) ausgestattet. Diese Infrastruktur erlaubt auch eine flexible Vergrößerung bei Bedarf. Der Serverraum ist mit einer Inertgas-Brandschutzanlage versehen. Alle kritischen Systeme sind dort untergebracht.

---

4. Überprüfungen

Gemäß DSGVO wird das TBA Zentrum von Datenschutzbeauftragten begleitet. Sie beraten die Leitung des Zentrums und des Instituts. Sie überprüfen datenschutzrelevante Prozesse sowie deren Dokumentation.

Schulungsmaßnahmen

Regelmäßige Schulungen zum Datenschutz und zur Informationssicherheit sind mindestens jährlich für die Mitarbeiter/innen des TBA-Zentrums verbindlich. Sie etablieren unter anderem die folgenden grundsätzlichen Konzepte:

- Datensparsamkeit wird zum Prinzip bei der Planung aller Datenerhebungen erklärt. Das verpflichtet die/den verantwortliche/n Mitarbeiter/in jedes erhobene Datenfragment zu begründen.
- Jedes Projekt, das personenbezogene Daten erhebt und jeder Vorgang, bei dem personenbezogene Daten verarbeitet werden, wird durch die Anlage eines Verzeichnisses der Verarbeitungstätigkeit (Art. 30 DSGVO) dokumentiert.
- Dieses Verzeichnis dokumentiert, welche Personen Zugriff auf personenbezogene Daten haben dürfen , damit Sicherheitsvorfälle erkannt, gemeldet und nachbearbeitet werden können.
- Jedes Projekt etabliert ein System zur Erledigung der Aufgaben, wie z.B. ein Ticketsystem, mit dem die Prioritäten der Tätigkeiten nach Dringlichkeit eingestuft werden können.
- Klarheit über die Implikationen bei der Wahl eines Passworts, die Verwendung von MAC-IPs oder Schlüsseln, insbesondere bei Einsatz auf nicht vertrauenswürdigen Systemen, und der damit verbundenen persönlichen Verantwortung.

Auftragskontrolle (Auftraggeber)

Das TBA Zentrum arbeitet regelmäßig mit externen Dienstleistern zusammen. Im Sinne der Informationssicherheit gibt es zwei Typen von Dienstleistern:

- Dienstleister, die personenbezogenen Daten verarbeiten. Das TBA Zentrum nutzt dafür ausschließlich Dienstleister mit Firmensitz in Deutschland und schließt mit diesen einen Vertrag zur Auftragsverarbeitung (AV) ab. Die Zusammenarbeit bleibt zeitlich auf die konkrete Aufgabenstellung beschränkt . Üblicherweise stellen diese Dienstleister einen Hostingservice oder eine Systemadministrationshilfe zur Verfügung.
- Dienstleister, die keine persönliche Daten verarbeiten, zum Beispiel Anbieter von Hardware oder Software, vor Inbetriebnahme wird die Sicherheit der gelieferten Leistung über die Reputation eingeschätzt. Nachträgliche Sicherheitsanpassungen, z.B. durch entdeckte Lücken, werden mit Hilfe aktiver Updateverfahren und automatisierten Audits vorgenommen.
