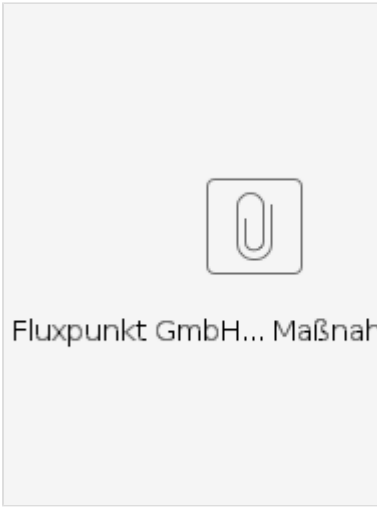
Technische und organisatorische Maßnahmen nach BDSG /DSGVO

Maßnahmen zur Umsetzung der Anforderungen des Bundesdatenschutzgesetzes und der DSGVO



Vorwort

Die Einhaltung datenschutzrechtlicher Vorschriften liegt uns sehr am Herzen. Wir sind kontinuierlich bestrebt, geeignete Maßnahmen zu implementieren, um dies zu gewährleisten.

Sofern keine gesetzlichen Normen entgegenstehen, verfolgen wir das Prinzip der Datensparsamkeit und beachten bei der Erhebung, Speicherung, Verarbeitung, Veränderung oder Übermittlung personenbezogener Daten die Zulässigkeitsvoraussetzungen und Interessensabwägungen des § 28 BDSG und Art. 6 DSGVO. Bei der Planung und Konzeption informationstechnischer Sicherungseinrichtungen orientieren wir uns an den Empfehlungen des BSI.

Um unnötige Redundanzen in der Aufzählung von Schutzmaßnahmen zu vermeiden, haben wir im vorliegenden Dokument die Kategorien der Anlage zu § 9 BDSG sowie die Umsetzungsmaßnahmen der Schutzziele aus Art. 32 DSGVO teilweise zusammengefasst. Technische Maßnahmen, wie der Einsatz von Verschlüsselungs- und Pseudonymisierungsverfahren sind in der Regel integraler Bestandteil verschiedenster Datenverarbeitungsvorgänge und Kontrollmechanismen, weshalb die konkrete Ausgestaltung innerhalb der jeweiligen Abschnitte beschrieben wird.

Bei der Beschreibung organisatorischer Maßnahmen, kennzeichnen die Begriffe „dürfen“ und „können“ optionale Mitarbeiterverhaltensweisen. Begriffe wie „sollen“ oder „sind aufgefordert“ kennzeichnen empfohlene Mitarbeiterverhaltensweisen, von denen nur nach einer Interessensabwägung abgewichen werden darf. Begriffe wie „müssen“ oder „dürfen nicht“ stellen verbindliche Anweisungen an unsere Mitarbeiter dar.

Das vorliegende Dokument beschreibt den aktuellen Zustand der implementierten technischen und organisatorischen Maßnahmen sowie interne Verhaltensrichtlinien und Mitarbeiteranweisungen. Technische Details entsprechen einem garantierten Mindestschutzumfang. Ein höheres Schutzniveau kann umgesetzt/implementiert sein, aus Sicherheitsgründen jedoch der Geheimhaltung unterliegen.

Zugangs- und Zutrittskontrolle

Wir unterhalten keine öffentlich zugänglichen Räume oder Ladenflächen.

Der Zutritt von betriebsfremden Personen (z.B. Gäste) ist nur in Begleitung eines autorisierten Mitarbeiters gestattet.

Der Aufenthalt externer Dienstleister in unseren Räumlichkeiten ist nicht unbeaufsichtigt gestattet.

Unsere Räumlichkeiten verfügen über ein elektronisches Schließsystem des Herstellers DOM Sicherheitstechnik und sind nur über nummerierte und auf einzelne Mitarbeiter ausgestellte Zutrittskarten bzw. -chips (RFID) zugänglich, wobei jeder Öffnen-/Schließen-Vorgang protokolliert wird. Die Protokollierung dient der Gefahrenabwehr, nicht der Zeiterfassung oder Mitarbeiterkontrolle. Zutrittskarten bzw. -chips können einzeln gesperrt oder im Zugangsumfang – zeitlich und/oder räumlich – eingeschränkt werden. Die Ausgabe von Zutrittskarten bzw. -chips an einzelne Mitarbeiter wird dokumentiert. Gleiches gilt für die Rückgabe und den Verlust. Verloren gegangene Zutrittskarten werden unverzüglich gesperrt.

Die Zugänge zu unseren Räumlichkeiten, sowie der Bereich vor dem Serverraum werden von einem Videoüberwachungssystem des Herstellers Axis 24 Stunden am Tag überwacht, wobei eine tatsächliche Aufzeichnung/Speicherung bei Bewegungen innerhalb definierter Bereiche stattfindet. Bei Dunkelheit wird automatisch eine Infrarotbeleuchtung aktiviert. Die Aufzeichnungen werden sowohl lokal, für die Dauer von vier Tagen, als auch an einem externen Standort, für eine Dauer von 21 Tagen aufbewahrt. Die Aufzeichnungen dienen der Gefahrenabwehr, nicht der Zeiterfassung oder Mitarbeiterkontrolle.

Unsere Server-, Speicher- und Netzwerksysteme befinden sich in einem separaten, abschließbaren Raum ohne Fenster (Serverraum), der sich örtlich zentral (Gebäudemitte) in unseren Räumlichkeiten befindet.

Unsere Server- und Speichersysteme des Herstellers HP verfügen über mechanisch abschließbare Blenden, die den physikalischen Zugriff auf Festplatten einschränken. Die Systeme befinden sich in einem Serverschrank mit seitlich verschraubten Wänden und abschließbaren Türen an Vorder- und Rückseite.

Die Mehrscheiben-Isolierglas-Fenster des Erdgeschosses sind mit zusätzlichen Fensterriegeln/-schlössern gegen Aufstemmen gesichert.

In den Büro- und Präsentationsräumen öffentlich zugängliche Netzwerkports sind mit RJ45-Port-Blockern gegen unberechtigte Nutzung physikalisch gesichert. Netzwerkkabel zwischen berechtigten nicht-mobilen Endgeräten und Netzwerkdosen sind mit RJ45-Secure-Clips gegen unberechtigtes Abziehen gesichert.
In den Büro- und Präsentationsräumen öffentlich zugängliche USB-A-Ports sind mit USB-Port-Blockern gegen unberechtigte Nutzung physikalisch gesichert.
Schlüssel zum Öffnen von Port-Blockern und Secure-Clips stehen berechtigtem Personal zur Anbringung an einen Schlüsselbund zur Verfügung.

Datenträgerkontrolle

Für Datenträger gelten die im Abschnitt *Zugriffskontrolle* aufgeführten Anforderungen an Verschlüsselung.

Ausgemusterte Datenträger werden mit Hilfe eines speziellen Kiosk-Systems vollständig und mehrfach mit Zufallszahlen überschrieben und anschließend formatiert. Sollte dies aufgrund eines Hardwaredefekts des Datenträgers nicht möglich sein, so wird dieser disassembliert und zerstört.

Wie im Abschnitt *Verfügbarkeitskontrolle* beschrieben, dürfen mobile Datenträger nicht mit Endgeräten verbunden werden. Entsprechend sind keine leicht zu entfernenden Datenträger vorhanden, die gelesen, kopiert, entfernt oder verändert werden könnten.

Speicherkontrolle

Die Kenntnisnahme personenbezogener Daten wird über die im Abschnitt *Zugriffskontrolle* beschriebenen Mechanismen gesteuert und unbefugte Kenntnisnahme verhindert.

Mitarbeiter sind auf den Umgang mit personenbezogenen Daten sensibilisiert und angewiesen, Unterstützungsleistungen gegenüber Dritten abzulehnen oder abzubrechen, wenn es hierdurch zu einer Übermittlung, unbefugten Kenntnisnahme oder sonstigen Verarbeitung personenbezogener Daten kommen sollte. Verantwortliche Dritte sind in diesem Zusammenhang aufgefordert, die Rechtmäßigkeit einer Verarbeitung glaubhaft zu machen, bevor Unterstützungsleistungen erbracht werden, bei denen personenbezogene Daten verarbeitet oder zur Kenntnis genommen werden.

Benutzerkontrolle

Die Benutzerkontrolle wird über die im Abschnitt *Zugriffskontrolle* beschriebenen Mechanismen durchgesetzt, unabhängig davon, ob es sich um einen Zugriff per Datenfernübertragung oder standortlokal handelt.

Zugriffskontrolle

Für die Zugriffssteuerung setzen wir ein differenziertes Berechtigungskonzept ein, das auf der Mitgliedschaft einzelner Mitarbeiter in verschiedenen Berechtigungsgruppen beruht (Role-Based Access Control (RBAC); Active Directory Benutzer und Gruppen). Die Standardrechte unterliegen hierbei maximalen Einschränkungen und werden nur bei Bedarf erweitert. Die Entscheidung über Vergabe und Entzug von Rechten obliegt der Geschäftsführung. Sofern Mitarbeiter das Unternehmen verlassen, werden unverzüglich alle Rechte entzogen – der zugehörige Active Directory Benutzer wird gesperrt.

Für jeden Kunden – und bei Bedarf auch für einzelne Projekte – wird eine eigene Active Directory Sicherheitsgruppe erstellt. Der Zugriff auf die Daten eines Kunden wird auf Mitarbeiter eingeschränkt, die Mitglied in dieser Sicherheitsgruppe sind.

Bei der Implementierung neuer Datenverarbeitungssysteme wird darauf geachtet, dass diese das zentralisierte Berechtigungskonzept unmittelbar für die jeweiligen Systemrechte umsetzen (Active Directory Anbindung) und Zugriffe protokolliert werden.

Für die Active Directory Benutzer-Authentifizierung werden individuelle Benutzerpasswörter mit mindestens 11 Zeichen verwendet, die Groß-/Kleinbuchstaben und Zahlen enthalten müssen. Die Verwendung von Sonderzeichen ist optional. Mitarbeiter sind aufgefordert, ihre individuellen Benutzerpasswörter nicht mehrfach zu verwenden. Für Windows-Anmeldungen darf Windows Hello (Anmeldung mittels biometrischer Merkmale, wie Fingerabdruck, Gesichts- oder Iriserkennung) verwendet werden. Zusätzlich ist für administrative Accounts ein weiterer Authentifizierungsfaktor (Microsoft Authenticator App) erforderlich. Für besonders sensible Bereiche werden zusätzlich Benutzerzertifikate und/oder DATEV mIDentity USB-Sticks des Herstellers KOBIL Systems zur Authentifizierung verwendet (Drei-Faktor Authentifizierung). Die Umsetzung dieser Anforderungen wird per Active Directory Gruppenrichtlinie durchgesetzt. Eine Drei-Faktor Authentifizierung stellt keinen garantierten Mindestschutzumfang dar – die Zwei-Faktor Authentifizierung hingegen schon.

Für mobile Geräte und Arbeitsplatz-PCs (Client-Systeme) zugelassene Hersteller sind: HP, Microsoft, Lenovo, Apple. Die Geräte müssen über ein Trusted Platform Module (TPM) zur Speicherung sensibler Schlüssel und Gewährleistung der Systemintegrität verfügen. Alle Windows Systeme müssen UEFI Secure Boot verwenden.

Client-Systeme sollen bei der Inbetriebnahme neu installiert werden. Hierfür soll ein Fluxpunkt-Basis-Image verwendet werden. Ziel ist ein sauberes System ohne Backdoors.

Client-Systeme müssen mit einer Laufwerksverschlüsselung (BitLocker oder FileVault) gesichert sein. Dies wird außerdem per Richtlinie beim Domänenbeitritt durchgesetzt. Die Schlüssel für die Laufwerksverschlüsselung werden zentral in Azure AD gespeichert.

Client-Systeme müssen bei Verlassen des Arbeitsplatzes gesperrt werden. Eine automatische Sperrung muß zudem nach längerer Inaktivität erfolgen.

Zugangsdaten für Fremdsysteme (Kundensysteme, Online-Portale, Lieferantenshops, etc.) werden in einem zentralen multi-plattform und multi-user Passwortserver des Herstellers Pleasant Solutions (zertifiziert nach FIPS, FOIP, FISMA, PCI DSS, HIPAA) gespeichert. Verbindungen zum Passwortserver sind SSL-verschlüsselt. Der Zugriff erfolgt entweder über eine interne Website oder über eine Client-Anwendung (KeePass). Zugangsdaten werden nur in der Serverdatenbank, FIPS 140-2 compliant (AES256-verschlüsselt), gespeichert – eine lokale Speicherung findet nicht statt. Das System verschlüsselt Passwörter im Arbeitsspeicher und löscht nach wenigen Sekunden automatisch die Zwischenablage, falls diese für eine Kennwortübergabe verwendet wurde. Der Passwortserver setzt die Rechtesteuerung des Active Directory um und erlaubt die gezielte Freigabe bestimmter Zugangsdaten mit Zeitsteuerung, Proxy-Funktionalität für Web und SSH (so dass Zugangsdaten ohne deren Preisgabe verwendet werden können), Protokollierung und Zugriffs-Reporting, Zwei-Faktor Authentifizierung, Lockout bei mehrfachen Authentifizierungsfehlern und automatischem Zeitablauf für Kennwörter. Je nach Benutzerrecht, dürfen einzelne Zugangsdaten verwendet (ohne Preisgabe), gelesen, verändert oder neu angelegt werden.

Die Erstellung von Zugangsdaten für Fremdsysteme unterliegt den folgenden Richtlinien:

1. Passwörter müssen zufallsgeneriert werden. Für die Erstellung soll der Passwort Generator des Passwortservers verwendet werden. Für die Verwaltung und Speicherung muß der Passwortserver verwendet werden. Passwörter sollen, wenn möglich, mit einem Verfallsdatum versehen werden.
2. Passwörter dürfen nicht mehrfach für verschiedene Dienste verwendet werden.
3. Falls der jeweilige Dienst dies unterstützt, sollen Passwörter mit mindestens 20 Zeichen, bestehend aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen generiert werden.
4. Zugriffsrechte müssen unmittelbar bei der Erstellung explizit gesetzt werden.

Die Anbindung unseres internen Netzwerks (vertrauenswürdiges Netz) an öffentliche Netzwerke (nicht-vertrauenswürdige Netze) erfolgt durch einen Multi-WAN-VPN-Router mit Paketfilter des Herstellers Viprinet in Kombination mit zweifach-redundant ausgelegten UTM Next Generation Firewall-Appliances des Herstellers Rohde & Schwarz. Jeder Host unseres internen Netzes ist darüberhinaus mit einem weiteren Paketfilter (z.B. Windows Firewall, Linux iptables,...) versehen, so dass – in Anlehnung an die Empfehlung des BSI – ein dreistufiger Aufbau aus Paketfilter, Application-Level-Gateway und Paketfilter (P-A-P) entsteht.

Die Basis der Firewall-Regelwerke sieht zunächst ein vollständiges Blockieren der gesamten Netzwerkkommunikation vor. Notwendige Kommunikation wird explizit freigegeben. Hierbei muß auf eine möglichst genaue Spezifikation der Kommunikationseigenschaften geachtet werden. Gewährende Firewall-Regeln sollen auf die zu erwartenden Nutzungszeiten eingeschränkt werden.

Unser internes Netzwerk ist durch VLAN-Separierung in mindestens die folgenden Segmente unterteilt:

1. Client-/Arbeitsplatznetzwerk
2. Scanner und Drucker
3. Voice
4. Videoüberwachung und Gebäudeautomatisierung
5. Server und IT-Infrastruktur
6. DMZ
7. Lab/Testing
8. Deployment
9. Datenschleuse

Die Netzwerkkommunikation von Geräten über eine VLAN-Grenze hinweg muß explizit in den UTM-Firewalls freigegeben werden. An dieser Stelle erfolgen inhaltliche Analysen des Traffics zur Angriffserkennung und -vermeidung. Freigaben erfolgen entweder für definierte Protokolle bestimmer Hosts und/oder aufgrund eines Identitätsnachweises durch Anmeldung eines Benutzers an einem Portal oder einer Client-Applikation der Firewall (auch im Rahmen eines Single-Sign-On-Prozesses bei der Anmeldung).

Serverdienste wie zum Beispiel Webservices oder Datenbanken müssen – je nachdem ob eine Nutzung von intern, extern oder intern/extern erfolgen soll – auf unterschiedlichen Container-Hosts (Docker) ausgeführt werden. Container-Hosts sind eigenständige virtuelle Maschinen, auf denen ein minimales Linux-System zur Container-Virtualisierung ausgeführt wird. Diese Trennung ermöglicht die Durchsetzung von Zugriffsbeschränkungen auf Netzwerkebene und verhindert Zugriffe auf interne Systeme durch Rechteeskalation eines öffentlich zugänglichen Systems.

Kundennetze, mobile Mitarbeiter und Home Offices werden per VPN angebunden. Für die Transportsicherung kommen IPsec oder TLS (SSL-VPN) zum Einsatz. VPN-Verbindungen mobiler Mitarbeiter und Home Offices müssen Perfect Forward Secrecy (PFS) sowie gegenseitige X.509-zertifikatsbasierte Authentifizierung verwenden. Für die Anbindung von Kundennetzen soll PFS sowie zertifikatsbasierte Authentifizierung, vor dem Einsatz von Preshared-Keys, verwendet werden. Beim Einsatz von Preshared-Keys gelten die Richtlinien für die Erstellung von Zugangsdaten für Fremdsysteme sinngemäß für die Erstellung des Preshared-Key. Konkrete Verschlüsselungsalgorithmen und Hashfunktionen werden unter Abwägung eines zu erreichenden Sicherheitslevels und des benötigten Rechenaufwands ausgewählt.

Kundennetze werden als nicht-vertrauenswürdige Netze betrachtet und entsprechend behandelt.

Weitergabekontrolle, Transportkontrolle und Übertragungskontrolle

Systeme, die zur Übertragung personenbezogener oder vertraulicher Daten eingesetzt werden, müssen mindestens eine Transportverschlüsselung einsetzen. Die damit zwingend einhergehenden Fehlererkennungs- und -korrekturverfahren sichern die Integrität der zu übermittelnden Daten. Mitarbeiter sollen Übertragungsweisen bevorzugen, die eine Ende-zu-Ende-Verschlüsselung unterstützen (z.B. Bereitstellung von Daten per Download über unsere flux.cloud-Plattform oder Microsoft OneDrive).

Protokolle ohne Transportsicherung dürfen nicht verwendet werden, wenn ein alternatives Protokoll mit Transportsicherung verfügbar ist (z.B für FTP, HTTP).

Für die Sicherung der Emailübertragung (IMAP und SMTP) setzen wir TLS ein. Für die Ende-zu-Ende-Sicherung von Übertragungen per flux.cloud setzen wir HTTPS (SSL) ein. Unsere Identität weisen wir dabei über ein, von einem vertrauenswürdigen Drittanbieter signiertes, RSA-Webserverzertifikat nach. Die Identität des Empfängers wird über die Kenntnis einer Zufallszeichenfolge innerhalb einer bereitgestellten URL sichergestellt. Bei der Bereitstellung soll ein Zeitablauf sowie ein zusätzliches Kennwort vergeben werden. Beim Zugriff auf unser öffentliches Wiki, sowie Dokumentations- und Ticketsystem, werden HTTP-Anfragen gezielt auf HTTPS umgeleitet (vorgeschalteter SSL-Reverse-Proxy).

Für die Übermittlung besonders sensibler oder vertraulicher Daten soll eine persönliche oder telefonische Kontaktaufnahme zur Verifikation der Empfängeridentität und Übermittlung einer Bereitstellungs-URL der zu übermittelnden Daten stattfinden. Bei telefonischer Übermittlung sensibler oder vertraulicher Daten muß die Telefonieverbindung mindestens bis zum Telefonieprovider verschlüsselt erfolgen (SIP-TLS/SRTP). Für verschlüsselte Telefonieverbindungen stehen uns die Provider STARFACE Connect und QSC zur Verfügung, die für ausgehende Gespräche explizit ausgewählt werden können. Für die Übermittlung besonders sensibler oder vertraulicher Daten sind Mitarbeiter außerdem angewiesen, für die per flux.cloud oder Microsoft OneDrive zum Download bereitgestellten Daten, eine Dokumentenverschlüsselung (verschlüsseltes PDF) zu verwenden. Das Dokumentenkennwort soll dabei im Rahmen der persönlichen oder telefonischen Kontaktaufnahme übermittelt werden.

~~Daten, bei denen ein Betroffener einen Löschungsanspruch hat und bei denen gesetzliche Aufzeichnungspflichten nicht entgegenstehen, müssen von Mitarbeitern per flux.cloud-Plattform oder Microsoft OneDrive (mit entsprechender Kategorisierung) übertragen werden, da nur so eine revisionssichere Email-Archivierung ausgeschlossen wird und einem Löschungsanspruch nachgekommen werden kann.~~

Aufgrund geänderter rechtlicher Rahmenbedingungen (DSGVO-Compliance) wird auf eine grundsätzliche revisionssichere Emailarchivierung verzichtet (da Löschpflichten ansonsten nicht nachgekommen werden kann). Stattdessen werden Dokumenten und Emails über Kategorisierungen /Labels entsprechende Aufbewahrungsrichtlinien (Retention-Policies) zugewiesen, die neben der Sicherstellung der Einhaltung einer Aufbewahrungsdauer auch eine automatische Löschung von Daten vorsehen.

Die Übermittlung von Daten per Email oder flux.cloud-Plattform wird protokolliert. Im Falle von aufbewahrungspflichtigen Emails, erfolgt eine revisionssichere Speicherung (Archivierung) der Emails für eine Dauer von 6 respektive 10 Jahren (zur Erfüllung gesetzlicher Anforderungen der GoBD aus HGB und AO). Diese Speicherung/Archivierung wird über Office 365 Retention-Policies umgesetzt.

Die Verwendung mobiler Datenträger (USB-Sticks, CDs/DVDs, mobile Festplatte, etc.) zum Transport personenbezogener Daten ist Mitarbeitern nicht gestattet. Die Annahme fremder mobiler Datenträger und deren Verwendung an unseren Datenverarbeitungssystemen ist Mitarbeitern ebenfalls untersagt.

Für Remote-Unterstützung/-Support beim Kunden setzen wir die Software TeamViewer, der TeamViewer GmbH aus Göppingen ein. Übertragungen sind hierbei durch Public-Key-Kryptographie (RSA 2048-Bit; Authentifizierung) und symmetrischer AES 256 Bit-Verschlüsselung (Transportsicherung) geschützt. Details unter: https://www.teamviewer.com/de/security/ und https://dl.tvcdn.de/docs/de/TeamViewer-Security-Statement-de.pdf.

Mitarbeiter sind im Rahmen ihres Arbeitsvertrags zur Geheimhaltung und auf das Datengeheimnis nach § 5 BDSG verpflichtet. Diese Verpflichtung überdauert das Arbeitsverhältnis und besteht auch nach dessen Beendigung fort.

Eingabekontrolle

Die von uns eingesetzten Systeme zur Erhebung, Verarbeitung, Speicherung und Nutzung von Daten bestehen hauptsächlich aus unserem Ticketsystem (Jira) und Wiki (Confluence) des Herstellers Atlassian sowie unserem Dokumentenmanagement- bzw. Enterprise Content Management System des Herstellers bitfarm Informationssysteme GmbH. Die Systeme protokollieren vollumfänglich jede Änderung an Daten sowie administrative Tätigkeiten inklusive des durchführenden Benutzers.

Daten (wie Dokumente, Emails oder allgemein Dateien), die im Dokumentenmanagementsystem abgelegt werden, werden mit Hilfe von Subversion (SVN) versioniert und mit Prüfsummen versehen. Eine Veränderung der Daten setzt voraus, dass ein berechtigter Mitarbeiter ein Dokument zur Bearbeitung auscheckt bzw. in einen Bearbeitungsmodus überführt und nach der Bearbeitung eincheckt bzw. die Änderung speichert und den Bearbeitungsmodus dadurch verlässt. Übergänge in den oder aus dem Bearbeitungsmodus werden protokolliert. Außerdem ist gewährleistet, dass ein Dokument zeitgleich nur durch einen Mitarbeiter verändert werden kann – im Bearbeitungsmodus ist das Dokument für andere Mitarbeiter gesperrt.

Die zur Erhebung, Verarbeitung, Speicherung und Nutzung von Daten verwendeten System werden mindestens zwei Mal pro Tag im Rahmen eines Backups gesichert und mindestens einmal am Tag an einen weiteren externen Ort zur Sicherung übermittelt, wodurch eine Sicherung der Protokolle gegen Verlust oder Veränderung umgesetzt wird. Hierfür verwenden wir eine Software des Herstellers Veeam. Für die Übermittlung und Speicherung der extern gesicherten Daten wird neben einer Transportverschlüsselung auch eine Datenverschlüsselung eingesetzt.

Auftragskontrolle

Wir setzen derzeit keine externen Auftragnehmer für die Betreuung unserer eigenen Datenverarbeitungsanlagen ein. Alle von uns eingesetzten Dienste und System werden – mit Ausnahme von Microsoft Office 365-Diensten (Exchange Online, Azure AD Verzeichnisdienst, Azure Virtualisierungsplattform für Hosting, OneDrive for Business, Skype for Business, SharePoint Online) – "on premise", auf unseren eigenen Servern an unserem Hauptstandort in Nürtingen betrieben. An einem weiteren eigenen Standort in Nürtingen, werden verschlüsselte Offsite-Backups aufbewahrt.

Unser externer Mailserver (Exchange Online) wird von Microsoft am Standort Wien (Österreich) betrieben. Weitere von uns genutzte Microsoft-Dienste, wie OneDrive for Business, SharePoint Online oder Skype for Business, werden in Rechenzentren in Irland oder den Niederlanden bereitgestellt. Die Datenschutzvereinbarung, Zertifizierungen und Compliance-Informationen befindet sich abrufbar unter: https://www.microsoft.com/de-de/trustcenter/about/transparency

Für den Betrieb unserer Hosting-/Monitoring- und Managed-Services-Plattformen nehmen wir Leistungen von Dritten, als Unterauftragnehmer, in Anspruch:

- Unsere Hosting-Plattform wird im Microsoft Azure Rechenzentrum in Amsterdam (Niederlande) von Microsoft Nederland, Evert van de Beekstraat 354, 1118 CZ Schiphol, betrieben.
  Die Hinweise zum Datenschutz befinden sich abrufbar unter: https://www.microsoft.com/de-de/TrustCenter/Compliance/EU-Model-Clauses
- Unsere Monitoring-Plattform Server-Eye wird im Rechenzentrum der INFOSERVE GmbH in Deutschland von Krämer IT Solutions GmbH, Koßmannstraße 7, 66571 Eppelborn, betrieben.
  Die Hinweise zum Datenschutz befinden sich abrufbar unter: https://www.server-eye.de/vorteile/datensicherheit/
- Für das Order-Management von Lizenzen aus dem Microsoft CSP-Programm bedienen wir uns der Distribution ALSO Deutschland GmbH, Lange Wende 43, 59494 Soest.
  Die Hinweise zum Datenschutz befinden sich abrufbar unter: https://www.also.com/ec/cms5/de_1010/1010/legal/datenschutzerklaerung

Nur auf ausdrücklichen Wunsch oder nach Zustimmung durch den Auftraggeber, werden Auftragsdaten zur Erbringung von Servicedienstleistungen (zum Beispiel für Support und Fehleranalysezwecke) an Soft- und Hardwareherstellers eines betroffenen Produkts übermittelt. Übermittelte Log-Dateien und Endkundeninformationen können als Nebenfolge hierbei personenbezogene Daten enthalten, die jedoch für keine anderen Zwecke als die Erbrigung der konkreten Servicedienstleistung verwendet werden dürfen. Mit diversen Herstellern haben wir zu diesem Zweck Auftrags(daten) verarbeitungsverträge (AV-Verträge) geschlossen. Im Rahmen der Prüfung der technischen und organisatorischen Maßnahmen (TOM) der Hersteller wurde uns jeweils ein ausreichendes Schutzniveu zugesichert, welches jedoch nicht notwendigerweise dem von uns in diesem Dokument aufgeführten Schutzniveu entsprechen muß.

Wie unter Weitergabekontrolle, Absatz 8 beschrieben, fallen beim Anbieter TeamViewer GmbH Verkehrsdaten an. Darüberhinaus hätte der Anbieter die Möglichkeit eines Man-in-the-Middle-Angriffs auf TeamViewer-Sitzungen. TeamViewer wurde einer sicherheitstechnischen Prüfung der FIDUCIA IT AG sowie einem BISG-Gutachten unterzogen. Darüberhinaus ist TeamViewer SOC 2 zertifiziert.

Weitere Kommunikationsverkehrsdaten fallen bei den Anbietern QSC, STARFACE Connect, HFO Telecom und sipgate an. Die Anbieter erbringen öffentlich zugängliche Telekommunikationsdieste und Telefondienste im Sinne des Telekommunikationsgesetzes (TKG) und unterliegen den besonderen Datenschutzanforderungen und dem Fernmeldegeheimnis des TKG.

Zum Zwecke der Buchführung und Erstellung von Jahresabschlüssen und deren Prüfung, ist nicht auszuschließen, dass personenbezogene Daten auf Belegen (Lieferscheine, Rechnungen, etc.) oder aus Fahrtenbüchern (Ansprechpartner eines Termins) an die Steuerberatungskanzlei Schlüter + Kollegen GmbH (Pfullingen) und die DATEV eG (Nürnberg) übermittelt werden. Die Datenschutzvereinbarung und das Verfahrensverzeichnis der DATEV eG befindet sich abrufbar unter: https://www.datev.de/web/de/m/ueber-datev/datenschutz/.
Mitarbeiter der Schlüter + Kollegen GmbH sind als Berufsgeheimnisträger zu besonderer Sorgfalt und Geheimhaltung verpflichtet. Das Unternehmen hat einen Datenschutzbeauftragten zur Prüfung und ordnungsgemäßen Umsetzung von Anforderungen aus Datenschutzgesetzen bestellt.

Verfügbarkeitskontrolle, Wiederherstellbarkeit, Zuverlässigkeit und Datenintegrität

Unsere Datenverarbeitungsanlagen sind vollständig mindestens zweifach-redundant ausgelegt. Jeweils zwei Online-USVs versorgen die redundanten Netzteile eines Servers oder PoE-Switches und sichern diese gegen Überspannung und Stromausfälle ab. Netzwerkverbindungen zu Servern sind durch Link-Aggregationen mindestens vierfach-redundant. Betriebssystemspeicher sind RAID-1 datengespiegelt. Alle weiteren Datenspeicher befinden sich auf RAID-5 Volumes mit einem Hotspare-Laufwerk oder auf RAID-6 Volumes.

Daten werden nach dem „3-2-1“-Prinzip gesichert: Mindestens 3 Kopien, auf mindestens zwei verschiedenen Medientypen, an mindestens einem weiteren Standort.

Das Backupkonzept sieht mindestens zwei Sicherungen pro Tag aller produktiven VMs vor und erlaubt die Wiederherstellung selbst einzelner Dateien innerhalb von VMs. Einmal pro Woche findet eine Vollsicherung statt. Die täglichen Differenzabbilder werden rückwärts-inkrementell erstellt um eine schnellstmöglich Wiederherstellung eines aktuellen Backups zu garantieren. Datenbanken auf Windows-Hosts unterstützen VSS und damit die Erstellung konsistenter Snapshots. Für Linux-basierte Datenbanken setzen wir individuelle pre-freeze- und post-thaw-Skripte ein, die die Konsistenz der Datenbank durch Anlegen eines Datenbanklocks vor dem Snapshot und Aufheben des Locks nach dem Snapshot sicherstellen.

Das Virenschutzkonzept sieht eine Perimetersicherung durch die UTM-Firewalls vor und setzt auf den in Windows integrierten Windows Defender. Die Mitarbeiter sind darüberhinaus sensibilisiert und geschult, auf den Umgang mit Daten unbekannter Herkunft, die Verifizierung von Datei-Prüfsummen und die Verwendung von Plattformen wie VirusTotal zur Prüfung fremder Dateien.

Für den Umgang mit mobilen Datenträgern (CD/DVD, USB-Sticks, SD-Karten, mobile Festplatten, etc.) kommt zur Perimetersicherung eine Datenschleuse PROVAIA des Herstellers PRESENSE zum Einsatz. Mobile Datenträger dürfen nicht mit Endgeräten verbunden werden (was darüberhinaus durch USB-Port-Locker verhindert wird), sondern müssen durch die Datenschleuse auf Viren, Skripte, Autostart-Funktionen geprüft und freigegeben werden. Dokumente werden von der Datenschleuse in portable und sichere Formate ohne Skripte und ohne eingebettete Schriften konvertiert. Der Inhalt freigegebener Datenträger wird anschließend auf ein spezielles Netzlaufwerk gespeichert.

Windows-Updates und Updates der Firewall (Firm-/Software, Signaturdateien, etc.) werden regelmäßig durchgeführt. Diverse Quellen für Zero-Day-Exploit-Informationen (Mailinglisten, Twitter, Websites) werden von uns überwacht, um schnellstmöglich auf mögliche Sicherheitslücken reagieren zu können.

Die externe Netzwerkanbindung wird über einen Multi-WAN-Router realisiert, der einen Kabelnetzanschluss, DSL und zwei LTE-Verbindungen bündelt.

Umsetzung des Trennungsgebots

Wie unter Zugriffskontrolle, Absatz 15 beschrieben, setzen wir auf eine hostbasierte Dienstetrennung (Trennung nach internen und externen Daten). Darüberhinaus sind einzelne Dienste innerhalb der Hosts jeweils containervirtualisiert (Docker) und ermöglichen so eine sehr differenzierte Trennung der Dienste (wie Ticketsystem, Wiki, Buchhaltung/Warenwirtschaft, Dokumentenmanagement, etc.).

Die containervirtualisierten Dienste bekommen individuellen Zugriff auf datenhaltende Docker-Volumes. Der Dienste-Container selbst enthält keine Daten und kann so leicht ausgetauscht, aktualisiert oder zurückgesetzt werden.

Mitarbeiter sind in Rechtegruppen unterteilt (z.B. Buchhaltung, Service/Support, Geschäftsführung, etc.), die mit unterschiedlichen Zugriffsrechten unterschiedlichem Funktionsumfang innerhalb einzelner Dienste einhergehen.

Zukunftsplanung

Wir planen die Einführung von 802.1x Authentifizierung und Autorisierung von Netzwerkgeräten und -benutzern (Network Access Control; NAC) zur Verbesserung der Zugriffskontrolle. Unsere Netzwerkhardware ist hierfür bereits vorbereitet.