Technische und organisatorische Maßnahmen, Auswahl nach §32 DSGVO, §64 BDSG (neu)
Erstellt: 26.03.2018
Letzte Änderung: 06.07.2022

Maßnahmen	Beschreibung
1. Verschlüsselung und Pseudonymisierung personenbezogener Daten	
Verschlüsselung von Datensätzen	Daten, die nicht zwingend für die Dienstebereitstellung als Klartext vorliegen müssen, werden mit gängigen Verschlüsselungsverfahren unkenntlich gemacht. Insbesondere Mailinhalte (Spamfilter) und in der Cloud gespeicherte Daten (Hornetdrive) liegen nur verschlüsselt in Datenbanken vor. Core-Datenbank: Verschlüsselung von E-Mail-Header und -Body mit AES 128 bit, pro Kunde kommt ein anderer Schlüssel zum Einsatz. E-Mail-Adresse dient als Suchschlüssel und wird nicht pseudonymisiert oder verschlüsselt gespeichert, da dies eine nicht akzeptable Herabsetzung der Dienstefunktionalität herbeiführen würde. 365 Total Backup & 365 Total Protection Enterprise Backup: Backup-Daten werden mit einem individuellen AES 256 bit Schlüssel verschlüsselt. Hornetdrive: Alle in Hornetdrive abgelegten Dateien werden vor dem Hochladen auf dem Endgerät des Benutzers mit einem symmetrischen AES 256 bit Algorithmus verschlüsselt.
Pseudonymisierung von Datensätzen	Bei der Anzeige der Nutzer- und Nutzungsdaten des Webfilterservice werden auf Kundenwunsch die Benutzernamen/Mailadressen gegen ein in Intervallen wechselndes Pseudonym ersetzt.
2. Vertraulichkeit und Integrität	
2.1. Zugangskontrolle	

Maßnahmen	Beschreibung
Gebäudesicherheit (Rechenzentrum)	Die Grundstücksgrenze des Betreibers ist durch bauliche Maßnahmen wie Zaun, Tor, Pfähle gekennzeichnet. Der Zutritt zum kontrollierten Innenbereich ist nur durch Türen möglich, und muss durch Klingeln angefordert werden. Zugang zum internen Bereich wird durch zwei Mechanismen kontrolliert: an der ersten Tür durch eine Gegensprechanlage zum Kontrollraum mit elektrischem Türöffner, an der zweiten Tür mittels eines Schließsystems mit Magnetkarte. Im Sicherheitsbereich sind die verarbeitenden Systeme durch ein eigenes Schließsystem geschützt. Die Räumlichkeiten werden durch Videoüberwachung zusätzlich überwacht. Es existieren Alarmierungspläne für Szenarien wie z.Bsp. unautorisiertes Eindringen. Weitere Informationen sind den TOM des RZ-Betreibers zu entnehmen.
Akkreditierung (Rechenzentrum)	Es liegen den Betreibern Namenslisten der akkreditierten Personen vor (Positivliste). Berechtigtes Personal für den Zugang setzt sich zusammen aus mit der Hardwarewartung beauftragten Personen, Projektleiter, Geschäftsleitung und IT-Sicherheitsbeauftragter. Der Zutritt ist nach Feststellung der Personalien nur mit einem Ausweis des RZ-Betreibers erlaubt. Zutritt und Verlassen der Räumlichkeiten werden protokolliert. Besucher müssen durch eine akkreditierte Person angemeldet und von dieser begleitet werden. Weitere Informationen sind den TOM des RZ-Betreibers zu entnehmen.
Zutrittsprotokollierung (Rechenzentrum)	Zugang zum internen Bereich und Verlassen desselben werden mit Name, Firmenzugehörigkeit, Zeitstempel (Anfang & Ende des Zutritts) durch den Betreiber dokumentiert. Weitere Informationen sind den TOM des RZ-Betreibers zu entnehmen.
Videoüberwachung (Rechenzentrum)	Bei sämtlichen technischen Räumlichkeiten, den Zugangswegen sowie für den Perimeterschutz besteht eine zusätzliche Videoüberwachung. Diese ist in den Räumlichkeiten des Rechenzentrums vorhanden und wird durch zusätzliche Bewegungssensoren unterstützt. Weitere Informationen sind den TOM des RZ-Betreibers zu entnehmen.
Alarmanlage (Rechenzentrum)	Zugänge und Räumlichkeiten werden durch eine Alarmanlage überwacht. Es sind Prozessabläufe definiert, wie bei Auffälligkeiten zu verfahren ist. Weitere Informationen sind den TOM des RZ-Betreibers zu entnehmen.

Maßnahmen	Beschreibung
Gebäudesicherheit (Büro Hannover)	Die Grundstücksgrenze ist durch bauliche Maßnahmen gekennzeichnet. Der Zutritt zum Hausflur ist von 6-20 Uhr möglich, außerhalb der Zeiten nur mit Schlüssel. Zugang zum internen Bereich (Büroeingang, Empfangsbereich) ist durch einen persönlichen NFC-Chip möglich. Der Zugang zu den Büroräumen ist durch Türen geregelt, wofür ebenfalls der Zugang per NFC-Chip genutzt wird.
Akkreditierung (Büro Hannover)	Der Zugang zu den Räumlichkeiten per NFC-Chip ist nur namentlich erfasstem, autorisiertem Personal möglich, Zugänge werden protokolliert. Dritte erhalten ohne angemeldeten Besuch keinen Zutritt und können nur durch GL oder CISO autorisiert werden. Bei Eintritt werden Besucherausweise ausgegeben, die sichtbar getragen werden müssen, unberechtigte Personen im zu schützenden Bereich sind identifizierbar. Besucher werden auf den Datenschutz verpflichtet. Es werden Besucherlisten geführt, fremde Personen müssen sich ausweisen.
Zutrittsprotokollierung (Büro Hannover)	Der Zugang zu den Räumlichkeiten per NFC-Chip ist nur namentlich erfasstem, autorisiertem Personal möglich, Zugänge werden protokolliert. Dritte erhalten ohne angemeldeten Besuch keinen Zutritt und können nur durch ein Mitglied der Geschäftsleitung oder dem CISO autorisiert werden. Bei Eintritt werden Besucherausweise ausgegeben, die sichtbar getragen werden müssen, unberechtigte Personen im zu schützenden Bereich sind identifizierbar. Besucher werden auf den Datenschutz verpflichtet. Es werden Besucherlisten geführt, fremde Personen müssen sich ausweisen.
Alarmanlage (Büro Hannover)	Die Büroräume der Hornetsecurity GmbH in Hannover werden außerhalb der Bürozeiten durch Bewegungsmelder überwacht. Die Alarmierung erfolgt an einen definierten Personenkreis.
Gebäudesicherheit (Büro Berlin)	Die Grundstücksgrenze ist durch bauliche Maßnahmen gekennzeichnet. Der Zutritt zum Hausflur, der zusätzlich durch einen Portier bewacht wird, ist von 6-20 Uhr nur mit einem Tokenschlüssel möglich. Außerhalb dieser Zeiten ist der Eingang verschlossen. Zugang zum internen Bereich ist durch einen persönlichen NFC-Chip möglich.

Maßnahmen	Beschreibung
Akkreditierung (Büro Berlin)	Die ausgegebenen NFC-Chips wurden namentlich zugeordnet, Zugänge protokolliert. Dritte erhalten ohne angemeldeten Besuch keinen Zutritt. Bei Eintritt werden Besucherausweise ausgegeben, die sichtbar getragen werden müssen, unberechtigte Personen im zu schützenden Bereich sind identifizierbar. Besucher werden auf den Datenschutz verpflichtet. Es werden Besucherlisten geführt, fremde Personen müssen sich ausweisen.
Zutrittsprotokollierung (Büro Berlin)	Es ist durch das NFC-Log für den Hausflur und Besucherlisten für den Bürobereich nachvollziehbar, wann wer welchen Bereich betreten hat.
2.2. Datenträgerkontrolle	
Absicherung Laptops	Alle Windows-Rechner sind mit einem zentral verwalteten Antiviren-Client ausgestattet, der nicht deaktivierbar ist. Die betriebssystemeigene Firewall ist aktiviert, Updates werden selbstständig und zeitnah eingespielt. Internes Netzwerk: DIe WLAN-Anmeldung erfolgt per WPA2-Enterprise Authentifizierung. Ein Zugang für Gäste-Geräte erfolgt über das logisch getrennte Gäste-WLAN. Sofern nicht im eigenen Officegebäude gearbeitet wird, muss VPN zum Rechenzentrum genutzt werden, da Zugriffe auf die relevanten Systeme sonst nicht möglich sind (IP-Sperre). Der Webfilter-Service (Proxy) ist zu nutzen.
Verschlüsselung von Laptops	Laptops sind durch Einsatz in wechselnden Umgebungen naturgemäß einem höheren Diebstahlrisiko ausgesetzt. Hierdurch könnte Unbefugten schützenswerte Daten offengelegt werden. Zugriff auf Festplatten ist durch Verschlüsselung unterbunden, unterschiedliche Ansätze sind erlaubt: - per Aktivierung der hardwarebasierten SSD-Verschlüsselung im BIOS (OPAL SSC: AES-128/256bit Verschlüsselung) - per Festplattenverschlüsselung, z.B. Bitlocker mit AES-128/256bit, oder VeraCrypt mit AES, Twofish oder Serpent, oder dm-crypt/cryptsetup/LUKS mit AES, Twofish.

Maßnahmen	Beschreibung
Mobile Datenträger	Es existiert eine Richtlinie zum Umgang mit Wechseldatenträgern. Für den digitalen Datenaustausch sind nur Datenträger zu nutzen, die aus vertrauenswürdigen Quellen stammen (Beschaffung und Ausgabe durch System Engineering). Private Datenträgernutzung ist untersagt. Alle Windows-Rechner verfügen über einen Virenscanner, der bei Lese- und Schreibzugriffen die Daten vor dem Zugriff prüft. Für den externen digitalen Datenträgeraustausch ist auf eine hinreichend starke Verschlüsselung der Daten zu achten, z.B. mit VeraCrypt. Ein externer Datenaustausch darf nur mit expliziter, dokumentierter Erlaubnis des Dateninhabers erfolgen. Datenexport auf mobile Datenträger erfolgt nur bei dokumentierter Kundenanforderung. Datenexporte werden protokolliert und sind nachvollziehbar. Bei Versand muss der Versandweg permanent nachverfolgbar sein (Tracking-ID).
Verschlüsselung von Smartphones	Es existiert eine BYOD-Policy, für die Nutzung privater Geräte. Daten auf Mobilgeräten dürfen lokal nur im Hornetdrive (verschlüsselt) oder auf autorisierten Clouddiensten gespeichert werden. Die Authentifikation zu den Diensten erfolgt über personalisierte Zugänge.
2.3. Speicherkontrolle	
Rechtemanagement	Die Benutzerrechte sind eingeschränkt auf die Tätigkeitsbereiche (Berechtigungsmatrix) nach dem Minimalprinzip. Die Rechtevergabe erfolgt zentral gesteuert. Jeder Nutzer bzw. dessen Benutzerprofil ist einer abteilungsabhängigen Rolle zugewiesen, die die notwendigen Berechtigungen auf Systeme der für seine Aufgaben durchzuführenden Tätigkeiten (Lesen, Schreiben, Löschen) verfügbar macht. Die Auswahl der Systemadministratoren ist auf die für die Aufgabe qualifizierte Personen beschränkt. Zugriffe werden zentral protokolliert.

Maßnahmen	Beschreibung
Anti-Viren-Software	Für alle Windows-Clients ist ein zentral gesteuerter Virenscanner obligatorisch (GData Enterprise). Das Signatur-Updateintervall beträgt 60 Minuten, heuristische Erkennung ist aktiviert. Nutzer von Linux Betriebssystemen führen regelmäßig Offline-Scans aus. Mac-Rechner unterliegen aufgrund der Sicherheitsarchitektur des Betriebssystems keiner Pflicht zur Nutzung eines Antiviren-Scanners. Auf Linux-Servern wird die Integrität der Dateien durch ein host-basiertes Intrusion Detection System (HIDS) regelmäßig kontrolliert.
Firewall	Arbeitsplatz-Clients: Auf allen Arbeitsplatzrechnern ist eine betriebssystemseitige SW-Firewall aktiviert. Die Kommunikation zu Servern erfolgt über eine zentral administrierte Firewall, die die Erfordernisse des Datenaustauschs zwischen den Systemen abbildet und somit die Kommunikation auf die notwendigen Ports/Dienste und ggf. IP-Bereiche beschränkt. Server mit erhöhtem Schutzbedarf stehen in einem gesonderten Schutzring und sind nur über vorgeschaltete Proxys oder Loadbalancer mit eigener Firewall erreichbar. Es werden wöchentliche Pen-Tests durchgeführt, dass nur die vorgesehenen Services von außen erreichbar sind.
Netzwerktrennung	Server an einem Standort sind durch funktionsbasierte VLANs getrennt. Zweckähnliche Server sind im selben VLAN miteinander konnektiert. Die VLANs terminieren in zentralen Firewall-Gateways. Hier wird anhand der Konfiguration vorgegeben, ob und in welchem Umfang interne Netze untereinander Daten austauschen können.
2.4. Benutzerkontrolle	

Maßnahmen	Beschreibung
Erstellung von Benutzerprofilen und –rollen	Die Benutzerrechte sind eingeschränkt auf die Tätigkeitsbereiche (Berechtigungsmatrix) nach dem Minimalprinzip. Jeder Nutzer bzw. dessen Benutzerprofil ist einer abteilungsabhängigen Rolle zugewiesen, die die notwendigen Berechtigungen für seine Aufgaben widerspiegelt. Der Gruppen-/Abteilungsleiter arbeitet mit dem CISO die Berechtigungsmatrix aus und übermittelt sie an die Fachabteilung zur Vergabe der Berechtigungen. Bei Eintritt in eine Abteilung wird anhand der betreffenden Matrix die Rolle und damit die Berechtigung festgelegt, bei Austritt aus der Abteilung wird die Rechtezuweisung rückabgewickelt. Dasselbe gilt bei On-/Offboarding.
Externer Zugriff per VPN	Verbindungen zu sicherheits- oder datenschutzrelevanten Servern sind nur per VPN-Tunnel (IPSec) von außerhalb des Unternehmens möglich, so dass sichergestellt ist, dass auch in fremden WLANs etc. keine Zugriffe durch Unbefugte möglich sind. Einwahl-VPN-Zugänge sind personalisiert. Es werden die vom BSI empfohlenen Cipher für VPN verwendet.
2.5. Zugriffskontrolle (i. e. S.)	
Berechtigungskonzept	Zugangsberechtigungen werden rollenbasiert vergeben. Für Systeme, die keine Rollen verwalten können, werden Berechtigungsstufen vordefiniert, die für einen Benutzer angefordert, zugewiesen und ausgerollt werden. Rollenberechtigungen werden durch den Gruppen-/Abteilungsleiter anhand der Aufgabenstellung entworfen, getestet, in einer Matrix dokumentiert und vom CISO genehmigt. Einzelberechtigungen werden bei Vergabe pro System dokumentiert. Als Berechtigung wird die geringstmögliche Rechtevergabe gewählt, die die Erledigung einer Aufgabe mit diesem System noch ermöglicht. Aufgabenänderungen oder Berechtigungsanpassungen einer Rolle führen zu einem Review der entsprechenden Rechtematrix. Im Rahmen des Onboardingprozesses werden vom Gruppen-/Abteilungsleiter die Rechte angefordert und durch die Fachabteilung SE/IT gesetzt. Im Offboardingprozess werden diese Zuweisungen rückabgewickelt. Gemeldete zweifelhafte oder undokumentierte Zuweisungen führen zu einem Review der betreffenden Rechtematrix und -vergabe.

Maßnahmen	Beschreibung
Authentifizierung mit Name/Passwort	Es werden personenbezogene Anmeldecredentials, z.T. mit Zwei-Faktor-Authentifizierung durch Security-Token oder zusätzlichem One-Time-Password, eingesetzt.
Passwortrichtlinie	Passwörter sichern Systemzugänge ab und stehen somit im Zentrum von Sicherheitsvorgaben. Kennwortpolicy: mind. 10 Zeichen, mind. 3 von 4 Kriterien (Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen). Für verschiedene Systeme müssen unterschiedliche Kennwörter verwendet werden. Für Core-Systeme muss das Kennwort bei administativem Zugriff mindestens 12 Zeichen lang sein. Kritische Systeme (z.B. Jumpserver) verwenden eine Multi-Faktor-Authentifizierung. Die Verwendung von Passwort-Management-Programmen wird befürwortet.
Nachvollziehbarkeit	Ein Transaktionsprotokoll zeichnet jegliche Veränderung der Daten in einer Datenbank auf. Für das Control Panel wird eine Transaktionsprotokollierung jeglicher Systemänderungen durchgeführt. I.d.R. sind diese im Audit auslesbar.
2.6. Übertragungskontrolle	
E-Mail-Verschlüsselung	Hornetsecurity bietet allen Kommunikationspartnern opportunistische Transportverschlüsselung via STARTTLS in Verbindung mit Perfect Forward Secrecy (PFS) an. Es wird mindestens TLSv1.2 genutzt. Zur Vermeidung von Kommunikationsproblemen wird nicht grundsätzlich ein ClientCertificateRequest gestellt. Bei der TLS Verschlüsselung werden Algorithmen ausgeschlossen, die nach BSI mit "nicht empfohlen" gekennzeichnet sind. Bei erzwungenem TLS werden nur "high grade" Cypher zugelassen. Beim Service "Archiving" werden die Daten unveränderbar verschlüsselt gespeichert. Es wird optional E-Mail-Verschlüsselung per PGP und S/MIME unterstützt. Die hierfür bei S/MIME Zertifikaten verwendeten Signaturalgorithmen und Hashverfahren orientieren sich an den BSI Empfehlungen. Für PGP werden DSA & Elgamal mit 2048 Bit Schlüssellänge als Verschlüsselungsverfahren verwendet.

Maßnahmen	Beschreibung
VPN Zugriff	Verbindungen zu sicherheits- oder datenschutzrelevanten Servern sind nur per VPN-Tunnel (IPSec) von außerhalb des Unternehmens möglich, so dass sichergestellt ist, dass auch in fremden WLANs etc. keine Zugriffe durch Unbefugte möglich sind. Einwahl-VPN-Zugänge sind personalisiert. IPsec ermöglicht eine sichere Übertragung von Informationen in IP-basierten Datennetzwerken, wobei insbesondere die Vertraulichkeit, die Integrität und die Authentizität der mittels des IP-Protokolls übertragenen Informationen gewährleistet werden können.
Dokumentation der Empfänger von Daten	Es ist nachvollziehbar, wohin personenbezogene Daten automatisiert übermittelt wurden. E-Mail-Übertragung: Die Ziel-Adresse wird eingehend aus der Kundenkonfiguration ausgelesen, ausgehend per DNS-Auflösung für die Zieldomain ermittelt. Die elektronische Datenübermittlung wird protokolliert mit Datum, Uhrzeit, Message-ID, Absender, Empfänger, versendende und empfangende IP, sofern vorhanden reverse-DNS-Name und SMTP-Error-Code. Eine Löschung der Protokolle erfolgt gemäß Löschmatrix.
2.7. Eingabekontrolle	
Dokumentation von Eingaben, Änderungen und Löschung von Daten	Es ist nachvollziehbar, wer wann welche Daten manipuliert hat. Über das Control Panel (Frontend) erfolgte Dateneingabe, -veränderung oder -löschung wird transaktionsorientiert mit Datum, Uhrzeit, Kundenname, IP-Adresse und Anmeldename protokolliert. Kunden können nur die ihnen zugehörigen Daten verändern. Mitarbeiter der Hornetsecurity können alle Kundendaten einsehen und ändern. Es gilt die Anweisung, Änderungen nur auf Kundenwunsch oder nach Rücksprache mit dem Kunden einzugeben oder durchzuführen. Eine Löschung der Protokolle erfolgt gemäß Löschmatrix.
Nachvollziehbarkeit von Datenverarbeitungen	Es ist nachvollziehbar, welcher Dienst in welcher Weise welche Daten manipuliert hat. Es erfolgt eine zentrale Speicherung der Protokolle der Auswertung und ggf. Manipulation der Daten für Spam- und Webfilterservices. Im Bedarfsfall erfolgt der Zugriff zur Nachvollziehbarkeit der DV. Eine Löschung der Protokolle erfolgt gemäß Löschmatrix.

Maßnahmen	Beschreibung
2.8. Transportkontrolle	
Sorgfältige Auswahl von Transportpersonal	Gewährleistung, dass beim Transport personenbezogener Daten die Vertraulichkeit und Integrität des Transportgutes geschützt wird. Personenbezogene Daten werden nur verschlüsselt versendet. Es wird sichergestellt, dass der Versand nachverfolgt werden kann (Tracking Nummer des Frachtführers). Es sind vertrauenswürdige, ortsübliche Spediteure für den Transport zu beauftragen. Bei überregionalen oder internationalen Aufträgen muss ein permanentes Tracking der Sendung auch bei Übergang auf Folge- oder Subspediteure gewährleistet sein. Datenträger werden in geeigneten Umverpackungen versendet, die gegen mechanische Einwirkungen schützen. Daten werden vor Ort so lange als Backup vorgehalten, bis der korrekte Empfang sichergestellt / quittiert worden ist.
Verschlüsselung von Datenträgern	Gewährleistung, dass beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt wird. Für den externen digitalen Datenträgeraustausch wird eine hinreichend starke Verschlüsselung der Daten genutzt, z.B. VeraCrypt oder 7zip. Ein externer Austausch erfolgt nur mit expliziter, dokumentierter Erlaubnis des Dateninhabers.
2.9. Wiederherstellbarkeit	

Maßnahmen	Beschreibung
Art und Umfang der Datensicherung/ Backups	Verantwortlich für den korrekten Betrieb, die Nachverfolgung von Systemmeldungen und die Konfiguration der Datensicherung ist die Abteilung SE/IT. Die Durchführung erfolgt mit Open Source Software. Das Backup ist eine Kombination von Voll- und inkrementeller Datensicherung. Die Systeme werden automatisiert alle 24 Stunden gesichert. Es stehen mindestens die Datenstände der letzten 30 Tage zur Verfügung. Die Sicherung erfolgt pro Rechenzentrum mit lokalen Agents über das interne Gigabit-Netzwerk zentral auf einem Sicherungssystem mit Festplatten-RAID. Dadurch kann ein Restore innerhalb weniger Minuten gestartet werden. Die Backup-Systeme selber sichern sich untereinander RZ-übergreifend. Die gesicherten bzw. zu sichernden Server werden im Wiki dokumentiert. Löschfristen können der Löschmatrix entnommen werden.
Recoverykonzept	Verantwortlich für den korrekten Betrieb, die Nachverfolgung von Systemmeldungen und die Konfiguration der Datensicherung ist die Abteilung SE/IT. Die Durchführung erfolgt mit Open Source Software. Im Störungsfall können Betriebssystem, Konfiguration und Daten auf ein bestehendes oder neu assembliertes System durch teil- oder vollautomatisierte Installation (Datenrestore und/oder automatisiertes Deploy) aufgespielt werden (inkl. des Backup-Systems selbst). Es finden regelmäßige, dokumentierte Test-Restores statt. Unterschreitet die gewünschte Wiederherstellungszeit bestimmte Triggerwerte, werden zusätzlich folgende Maßnahmen zur Verfügbarkeit der Systeme ergriffen: - < 24 Stunden: es wird zusätzlich ein zweites System für Failover-Betrieb bereitgestellt, - <4 Stunden: es wird ein Cluster betrieben.
2.10. Datenintegrität	

Maßnahmen	Beschreibung
Funktionstests von neuen Verfahren	- Spezifikation funktionaler und nichtfunktionaler neuer Projekte unter Verwendung einer angepassten Version des Volere Templates. - Code Reviews aller Änderungen vor Go-Live zur Qualitätssicherung - 4-Augen-Prinzip bei allen Änderungen an Livesystemen - Unit-Tests für automatisierte Prüfung atomarer Funktionen und zur Verbesserung der Wartbarkeit von Quellcode - Automatisierte, standardisierte Integrationstests bei jedem Release (Selenium Web Driver Toolkit unter Verwendung von Browserstack, ggf. Docker-Container, CI-Pipeline) - Erweiterung der Testfälle nach Implementieren neuer Funktionen gegen die Spezifikation, Finden und Beheben von Bugs - Nach jedem Release noch einmal Gegenlaufen der Autotests.
Einsatz von Maßnahmen zum Schutz der Integrität personenbezogener Daten	Änderungen an Berechtigungs- und Konfigurationsobjekten und personenbezogenen Daten sind über das Control Panel möglich. Jede Aktion - inkl. (fehlgeschlagener) Anmeldung - wird im Audit-Log mit Datum, Zeit, Anmeldename, Aktion, Objekt und originärer IP-Adresse gespeichert. Für die Berechtigungsverwaltung sind drei Standardberechtigungsrollen vorgegeben (Benutzer, Kundenadministrator, Partner). Individuell definierbare Berechtigungen, die ebenfalls als Rollen verfügbar gemacht werden, sind möglich. Benutzer werden diesen Rollen zugeordnet. Datenübermittlung erfolgt ausschließlich über verschlüsselte Verbindungen (VPN oder TLS; vgl. Ziffer 2.6). Datenübertragungen von Tier 1 (Front End) zu 2 bzw. Tier 2 zu 3 (Back End) sind durch Firewallregeln nur für definierte Endpunkte möglich.
2.11. Auftragskontrolle	
Auftragsdurchführung	- Die Mitarbeiter des Auftragnehmers werden regelmäßig geschult, die Leistung im Sinne des mit dem Auftraggeber geschlossenen Leistungsvertrags (unter Berücksichtigung der zugehörigen AVV) auszuführen. - Für neue Mitarbeiter existieren Einarbeitungsprozesse und Boot Camps. - Weisungsgeber und -empfänger werden explizit benannt. - Weisungen werden nur nach schriftlicher Erteilung / schriftlicher Bestätigung (per Ticketsystem) durchgeführt. - Prozesse, insbesondere für datenschutzrelevante Vorgänge, sind inklusive Eskalationsweg im Wiki beschrieben. Es existiert ein eindeutiger Kommunikationskanal für Datenschutzanfragen.

Maßnahmen	Beschreibung
Auswahl von Auftragsverarbeitern, die die Anforderungen der DSGVO gewährleisten	In ihrem Kern soll die Auftragskontrolle die weisungsgemäße Durchführung der Auftragsdatenverarbeitung sicherstellen. Auftragsverarbeiter werden nach Qualifikationen und bestehenden Referenzkunden, Zertifikaten und Sicherheitskonzepten bewertet und ausgewählt. Bei der Auftragserteilung an Auftragnehmer werden die nach DSGVO notwendigen Punkte vertraglich fixiert. Ist der Auftragnehmer nicht in der Lage, dies sicherzustellen, wird von einem Vertragsabschluss Abstand genommen.
Abschluss DSGVO-konformer AV-Vereinbarungen	Eine AV-Vereinbarung muss alle wesentlichen Aspekte enthalten. Hornetsecurity als Auftraggeber schließt mit Auftragnehmern nur DSGVO-konforme AV-Vereinbarungen ab. Ggf. wird der DSB in die Prüfung von AV-Vereinbarung einbezogen.
Sicherstellung der Löschung von Daten nach Auftragsbeendigung	Mit dem Inkrafttreten der DS-GVO erfährt die Löschung personenbezogener Daten gegenüber der bisherigen Rechtslage insofern eine Aufwertung, als die diesbezüglichen Bestimmungen detaillierter ausformuliert worden sind und zum Teil auch darüber hinausgehen. Sofern keine sonstige Rechtsgrundlage besteht, gelten die in der Löschmatrix genannten Fristen für die Löschung persönlicher Daten. Es existiert ein entsprechender Prozess für Löschanforderungen.
Laufende Prüfung der Auftragnehmer	Hornetsecurity legt bei Auftragnehmern größten Wert auf dokumentierte und gelebte Datenschutz- und IT-Sicherheitsprozesse und prüft die Dokumentation als auch stichprobenartig durch Vor-Ort-Besichtigungen. Verträge mit Auftragnehmern werden nur geschlossen, wenn diese sich vertraglich eindeutig zur Einhaltung von Vertraulichkeit und Datenschutz verpflichten.
3. Verfügbarkeitskontrolle	

Maßnahmen	Beschreibung
Katastrophenvorsorge	Die Katastrophenvorsorge gliedert sich in 3 Bereiche: Maßnahmen zur Minderung der Risiken, der Auswirkungen und dem Eintritt eines Schadens. 1. Hornetsecurity nutzt für den Betrieb mindestens zwei weit voneinander entfernte Rechenzentrumsstandorte in Deutschland, die von zertifizierten Betreibern unterhalten werden. Jedes dieser Rechenzentren verfügt für sich allein über redundante Stromversorgung, Netzwerkversorgung, Klimatisierung und Löschanlagen. Die Datenverarbeitung wird vollständig bereits mit dem Betrieb eines einzelnen RZ gewährleistet. Das zweite und weitere RZ werden zur Erhöhung der Redundanz eingesetzt. Zentrale Datensysteme sind zusätzlich gedoppelt mit automatischer Replikation sowie Hot-Fail-Over-Funktionalitäten ausgestattet. Daten werden georedundant gespeichert. Kommunikation und Datenaustausch erfolgt grundsätzlich verschlüsselt. 2. Daten werden grundsätzlich auf gespiegelten Datenträgern durch geeignete RAID-Verfahren gespeichert. Daten werden nach einem Backupplan regelmäßig gesichert, um ältere Datenstände wiederherstellen zu können. Wichtige Services werden durch geclusterte Server bereitgestellt. Für alle Server wird ein Wiki mit aktuellen Konfigurationen und Einsatzzweck geführt. Es finden regelmäßig dokumentierte K-Fall-Simulationen statt. 3. Die Kritikalität der Server und Services ist dokumentiert mit der erwarteten maximalen Wiederherstellungszeit, woraus sich die Priorität bei einem Desaster-Recovery ergibt.

Maßnahmen	Beschreibung
Notfall/K-Fall	Im Rahmen der IT-Sicherheitsstrategie hat das IT-Notfallmanagement die Aufgabe, die Kontinuität des Geschäftsbetriebs sicherzustellen. Die Kritikalität der Server und Services ist dokumentiert. Hieraus leitet sich die Reihenfolge für eine Wiederherstellung ab. Es existiert ein umfangreiches Monitoring von Diensten und Hardware. Für unterschiedliche Ereignisse (Warnung, Störungen, Ausfall) gibt es zugehörige Eskalationspläne mit zu benachrichtigenden Rollen und Personen. Es werden bei Komplettausfall für verschiedene Verwendungszwecke Hardwareausstattungen und Einzelteile in unterschiedlichen Konfigurationen vorgehalten. Eingesetzte Konfigurationen werden zentral dokumentiert. Im Störungsfall können Betriebssystem und Konfiguration auf ein neues assembliertes System durch teil- oder vollautomatisierte Installation (Datenrestore und/oder automatisiertes Deploy) aufgespielt werden. Es finden K-Fall-Übungen statt und mögliche K-Fall Szenarien werden erfasst. Die Ergebnisse werden dokumentiert und dienen als Grundlage für regelmäßige Verbesserungen.
4. Trennbarkeit	
Trennung von Produkt- und Testsystemen	Für interne Zwecke (z.B. Entwicklung, Test und Backup) werden logisch und physikalisch getrennte Systeme mit eigener Datenbank und Datenstruktur genutzt. Neue Versionierungen unterliegen einem mehrstufigen Qualitätssicherungsprozess. Automatisierte Software-Tests führen Standardtests durch und garantieren die korrekte Funktionsweise aller Kernfunktionalitäten. Nach diesen automatisch durchgeführten Standardtests erfolgt der Betrieb in einem Testsystem, auf das nur interne Mitarbeiter und auf den Datenschutz verpflichtete externe Betatester Zugriff erhalten. Die Testdauer im Testsystem beträgt mindestens 1 Woche. Ein Feedbackprozess passt die automatisierten Standardtests bei Fehlern für zukünftige Standard-Testverfahren an. Nach fehlerfreier Testphase wird die neue Version im Produktivsystem ausgerollt.

Maßnahmen	Beschreibung
Festlegung von Datenbankrechten	Anwender erhalten nach einem vordefinierten Rollenkonzept Zugriff auf unterschiedlichen Umfang von Daten und Abfragemöglichkeiten. Angefangen bei der Benutzer-Rolle, die nur eigene Daten entsprechend dem angemeldeten Benutzeraccount sehen darf, bis hin zur Partner-Rolle, die Zugriff auf Informationen der ihr zugeordneten Kunden und Nutzer erhält und deren Rollen auch konfigurieren, anlegen oder löschen darf, stehen Standardrollen für die Zuweisung zur Verfügung. Individuelle Rollen mit differenzierten Zugriffsrechten sind ebenfalls möglich, diese können einem beliebigen Benutzeraccount zugewiesen werden.
Logische Mandantentrennung	Eine Mandantentrennung ist eingerichtet, damit ein Mandant (Cloud-Anwender) nicht unberechtigt Informationen von anderen Mandanten (Cloud-Anwendern) einsehen kann. Es wird gewährleistet, dass kein Mandant auf die Ressourcen eines anderen Mandanten zugreifen kann, beispielsweise auf virtuelle Maschinen, Netze oder Cloud Storage. Im Control Panel erfolgt eine logische Mandantentrennung auf Datenbank-Ebene.
5. Organisationskontrolle	
Benennung eines geeigneten DSB	Lukas Wagner LL.M. Zert. Datenschutzbeauftragter (TÜV) HK2 Comtection GmbH Hausvogteiplatz 11 A 10117 Berlin Telefon: +49 30 278900180 https://www.comtection.de Als externer Datenschutzbeauftragter nimmt Herr Wagner dessen Pflichten und Rechte wahr, z.B. Überwachung der Verarbeitungsvorgänge, Prüfung der Vereinbarkeit mit den Datenschutzgesetzen, Vertretung vor den Aufsichtsbehörden. Er verfügt über langjährige Erfahrung im Datenschutz. Die nach dem Gesetz erforderliche Fachkunde und Zuverlässigkeit ist selbstverständlich und kann Dritten gegenüber dokumentiert werden.

Maßnahmen	Beschreibung
Implementierung regelmäßiger Überprüfungs- und Evaluierungszyklen	Ein innerbetrieblicher Meldeprozess animiert alle Mitarbeiter, erkannte Unregelmäßigkeiten zu eskalieren. Der IT-Sicherheitsbeauftragte (CISO) nimmt die Informationen entgegen und passt unter Einbeziehung der relevanten Gruppenleiter bestehende Prozesse an. Mitarbeiter erhalten Rückmeldung zu gemeldeten Sachverhalten. Stichprobenartige Kontrollen des CISO bei Berechtigungskonzepten und Sicherheitsmaßnahmen decken Optimierungsmöglichkeiten auf. Es finden regelmäßige Kontrollen und ggf. Anpassungen der Maßnahmen statt, ob diese noch dem Stand der Technik entsprechen. Regelmäßige Netzwerkscans prüfen auf Vorkommen von unautorisierten Dienstebereitstellungen. Änderungen im Betriebsablauf oder in relevanten Prozessen werden firmenweit kommuniziert. Ein aktives Incident-Management mit regelmäßigen Treffen der Gruppenleiter arbeitet Mängel, die zu Störungen geführt haben, auf und leitet (Sicherheits)Maßnahmen ab, um Authentizität, Integrität, Vertraulichkeit Verfügbarkeit und Verbindlichkeit aller Systeme nachhaltig sicherzustellen.
Erstellung eines Löschkonzeptes	Hornetsecurity unterscheidet verschiedene personenbezogene Daten pro Service. Eine ausführliche Matrix der Regellöschfristen findet sich in der Löschmatrix, die separat angefordert werden kann. Löschen in Sondersituationen, was nicht durch die Regellöschfristen abgedeckt ist, wird fallabhängig mit der für die Datenspeicherung verantwortlichen Fachabteilung durchgeführt. Federführend ist der IT-Sicherheitsbeauftragte, hilfsweise der Datenschutzbeauftragte. Aussetzung der Löschung - insbesondere bei archivierten E-Mails - ist auf Antrag des Kunden oder einer berechtigten Stelle möglich. Um Löschanfragen Betroffener umsetzen zu können, ist eine vorzeitige Löschung von Daten im Archiv möglich. Dieser Prozess kann im Self-Service durch autorisiertes Kundenpersonal im 4-Augen-Prinzip ausgelöst werden. Die Löschaktionen werden protokolliert. Werden Daten über die in der Matrix für Regellöschfristen genannten Zeiten gespeichert, erfolgt dies anonymisiert durch Kumulation der Datenbestände.

Maßnahmen	Beschreibung
Belehrungen/Schulungen	Mitarbeiter (inkl. Praktikanten, studentische Hilfskräfte) werden regelmäßig schriftlich über Datenschutz belehrt und müssen dies per Unterschrift bestätigen (1x pro Halbjahr). Zur verpflichtenden Awarenessschulung werden pro Abteilung in unregelmäßigen Abständen Test-Phishing-Mails versendet. Schulungsvideos und Awareness-Übungen werden zu verschiedenen Themenbereichen ausgerollt. Ein firmenweiter Awareness-Score liefert Auskunft über den Erfolg.
Zuständigkeiten und Verantwortungsbereiche	Zuweisung der Verantwortung für Informationen, Anwendungen und IT-Komponenten - Servicebereitstellung gegenüber dem Kunden: SD (Service Desk) - Servicebereitstellung intern: SE/IT (Systems Engineering/Infrastructure Team) - Monitoring: SE/CM (Systems Engineering/Cloud Management) - Programme & Scripte: SE/SL (Systems Engineering/Security Labs) - Front-/Backend, Datenspeicherung: PDC (Programming and Developing Center) - Koordination Prozesse & IT-Sicherheit: CISO (Chief Information Security Officer) - Störungen und nachhaltige Behebung: IM (Incident Manager)
Betroffenenanfragen	Die DSGVO sieht ein Auskunftsrecht für betroffene Personen vor (Art. 15 DSGVO) Auskunftsersuchen sind per E-Mail an datenschutz@hornetsecurity.com bzw. privacy@hornetsecurity.com zu senden. Die Anfrage wird im Ticketsystem erfasst, der Eingang umgehend bestätigt. Die Auskunft ist kostenfrei. In Fällen von unbegründeten oder exzessiven Anträgen durch eine betroffene Person kann die Auskunftserteilung verweigert werden. Es existiert ein ausführlicher Prozess zu Anfragen (zusammengefasst): 1. Überprüfung, ob es sich überhaupt um ein Auskunftsverlangen handelt. 2. Prüfung der Identität des Antragsstellers. 3. Prüfung, ob personenbezogene Daten der betroffenen Person verarbeitet wurden. 4. Wenn keine Daten vorhanden sind: Negativmitteilung an den Betroffenen. 5. Wenn Daten vorhanden sind: Zusammenstellung und unverzügliche Beantwortung innerhalb eines Monats ab Eingang. In Fällen der Fristverlängerung wird der Antragsteller umgehend hierüber informiert.

Maßnahmen	Beschreibung
	Darüber hinaus sieht die DSGVO die Rechte auf Information (Art. 13 + 14 DSGVO), Berichtigung (Art. 16 DSGVO), Löschung (Art. 17 DSGVO), Einschränkung der Verarbeitung (Art. 18 DSGVO) und Datenübertragbarkeit (Art. 20) vor.
Entsorgungskonzept Datenträger	Datenträger, auf denen einmal Kundendaten abgespeichert wurden, werden im Defektfall nicht reklamiert, sondern direkt der Datenträgervernichtung zugeführt. Auch eine Wiederverwendung eines einmal mit Kundendaten versehenen Datenträgers ist ausgeschlossen. Zu vernichtende Datenträger werden im SE unter Verschluss gesammelt. Datenträger werden durch einen zertifizierten Anbieter, der durch die Hornetsecurity bedarfsgerecht beauftragt wird, professionell vernichtet. Die Datenträgervernichtung wird kontrolliert und protokolliert. Handelt es sich bei zu löschenden Datenträgern um im Ausland eingesetzte Server mit eingebauten Datenträgern, gilt folgende Regelung: - Löschen aller personenbezogenen Daten, Konfigurationen und Scripten für die Dienste - Installieren und Ausführen eines Wipe Programms - Kunde soll den Server für Hornetsecurity vor Ort entsorgen.

Dokumentenversionen	Datum
0.1	26.03.2018
0.2	25.05.2018
0.3	08.08.2018
1.0	14.08.2018
1.0.1	13.01.2020
1.1	06.01.2021
1.2	01.05.2022
1.2.1	06.07.2022