

Technische und organisatorische Maßnahmen (TOM)

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

Produktversion 2026.10.03 · Handbuch-Revision 2.1

Stand 03.10.2026 · Plattform .NET 10 / Windows Server

ID-55 TOM

Technische und organisatorische Maßnahmen (TOM)

Dieses Kapitel beschreibt die **technischen und organisatorischen Maßnahmen** von Ordavis IT nach **Art. 32 Abs. 1 lit. a bis d DSGVO**. Es richtet sich an **Datenschutzbeauftragte, Informationssicherheitsbeauftragte** und den **IT-Betrieb**. Sie können es als Herstellerbeitrag in Ihr Verzeichnis der Verarbeitungstätigkeiten übernehmen (Art. 30 Abs. 1 lit. g DSGVO); die Tätigkeiten selbst beschreibt ID-57.

Beschrieben ist der Stand der Fassung, mit der dieses Kapitel ausgeliefert wird. Jede Maßnahme sagt, ob das **Produkt** sie selbst leistet oder ob **Sie als Betreiber** sie treffen. Wo das Produkt hinter dem Wünschenswerten zurückbleibt, steht das in Abschnitt 8.

Verfahren und Schlüssel im Einzelnen stehen im Kryptokonzept (ID-54), Installation und Härtung in ID-50, Sicherheitsaktualisierungen in ID-53.

INHALT

1 Wer was leistet

2 Pseudonymisierung und Verschlüsselung (lit. a)

2.1 Verschlüsselung

2.2 Pseudonymisierung und Datensparsamkeit

3 Vertraulichkeit (lit. b)

3.1 Anmeldung

3.2 Zugriffskontrolle und Rollen

3.3 Mandantentrennung

4 Integrität (lit. b)

4.1 Protokollierung

4.2 Unverfälschte Daten und Programme

5 Verfügbarkeit, Belastbarkeit und Wiederherstellung (lit. b und c)

6 Regelmäßige Überprüfung (lit. d)

7 Was Sie als Betreiber ergänzen

8 Bekannte Grenzen

9 Häufige Fragen

Verwandte Themen

1 Wer was leistet

Ordavis IT läuft **auf Ihrem Server** in Ihrem Netz. Der Hersteller hat keinen Fernzugang zu Ihrer Anlage. Personenbezogene Daten erreichen ihn nur auf zwei Wegen:

- **Fehlerberichte**, die eine Anwenderin oder ein Anwender im Client selbst abschickt. Sie tragen Name und Mailadresse der meldenden Person, damit der Support antworten kann, dazu Lizenznehmer, Mandant, Serveradresse und Fassung. Protokoll und Bildschirmfoto gehen nur mit, wenn sie im Dialog ausgewählt bleiben. Der Bericht geht per HTTPS direkt an den Hersteller. Nur wenn dieser Weg nicht erreichbar ist, geht er als Mail über Ihren Mailserver; dann liegt er bis zum Versand und danach bis zum Ablauf der Frist der Mail-Warteschlange (ID-56, Abschnitt 3.3) auf Ihrem Server.

- **Push-Benachrichtigungen** an die App laufen in der Vorgabe über den Vermittler des Herstellers. Er sieht nur einen Platzhalter statt Betreff und Text (Abschnitt 2.1) und speichert Gerätetoken nur als Hashwert.

Die Prüfung auf Aktualisierungen und die Lizenzaktivierung übertragen Lizenzkennung, Lizenzdaten, Rechnerkennung und Fassung, keine Daten Ihrer Anwender. Daraus folgt die Aufteilung:

Bereich	Leistet das Produkt	Treffen Sie als Betreiber
Verschlüsselung	TLS für Client, Portal und App, Tresore für Zugangsdaten, verschlüsselte Sicherungen	HTTPS-Betriebsart und Zertifikat wählen, Sicherungskennwort vergeben und verwahren
Anmeldung	Kennwortschutz, Sperre nach Fehlversuchen, zweiter Faktor, Sitzungsfristen	Pflicht zum zweiten Faktor festlegen, Konten bei Austritt deaktivieren
Rechte	Rollen- und Rechtemodell, Prüfung jedes Zugriffs auf dem Server	Rollen nach minimaler Berechtigung zuweisen und regelmäßig prüfen
Protokollierung	Prüfprotokoll, Windows-Ereignisprotokoll, Betriebsprotokolle	Auswertung festlegen, SIEM anbinden
Verfügbarkeit	tägliche Sicherung aller Mandanten, Wiederherstellungsskript	Sicherungsziel außerhalb des Servers, Rücklauf regelmäßig erproben
Server und Netz	Betrieb ohne Datenbankzugang aus dem Client-Netz	Windows und PostgreSQL pflegen, Netz trennen, Zutritt zum Serverraum
Aktualisierung	signierte Aktualisierungen, Sicherheitsaktualisierungen bis 31.12.2032	Aktualisierungen zeitnah einspielen

2 Pseudonymisierung und Verschlüsselung (lit. a)

2.1 Verschlüsselung

- **Transport zwischen Client, Portal, App und Server.** Ist eine HTTPS-Betriebsart eingerichtet (eigenes Zertifikat oder Let's Encrypt), spricht der Server **TLS 1.2 oder 1.3**; TLS 1.2 lässt sich abschalten. In der Vorgabe-Betriebsart *Reverse-Proxy* übernimmt ein vorgelagerter Proxy des Betreibers die Verschlüsselung, der Dienst selbst spricht dann HTTP (ID-50, Abschnitt 7.1).
- **Transport zu Fremdsystemen.** LDAPS zum Verzeichnisdienst prüft das Zertifikat stets: gegen die hinterlegte Zertifizierungsstelle oder gegen den Zertifikatsspeicher von Windows samt eingetragenen Hostnamen. Postfächer (IMAP, POP3, SMTP) und Exchange prüfen in der Vorgabe ebenfalls; die Prüfung lässt sich auf einen hinterlegten Fingerabdruck umstellen oder für Notfälle ganz abschalten (*Ungültige akzeptieren*, jede Verbindung wird dann im Betriebsprotokoll vermerkt). Eine Verzeichnisanbindung ohne TLS (LDAP, Port 389) ist möglich. Die Verbindung zwischen Server und PostgreSQL erzwingt das Produkt **nicht** verschlüsselt (ID-54, Abschnitt 7).
- **Ruhende Daten.** Zugangsdaten zu Fremdsystemen (Verzeichnisdienst, OIDC, Postfächer, Scan-Konten, Messenger, Webhooks, Action1) und die Geheimnisse des zweiten Faktors liegen mit **AES-256-GCM**

verschlüsselt in der Datenbank. Token, die nur geprüft werden müssen, liegen nur als SHA-256-Hashwert vor; Kennwörter lokaler Konten als Argon2id-Hashwert.

- **Sicherungen.** Mit hinterlegtem Sicherungskennwort entsteht jede Sicherung als 7-Zip-Archiv mit **AES-256**, Dateinamen eingeschlossen (ID-50, Abschnitt 6.1).
- **Push-Benachrichtigungen** an die App sind Ende-zu-Ende verschlüsselt, sobald die App ihren Schlüssel gemeldet hat; Google und der Push-Vermittler sehen dann nur einen Platzhalter.
- **Schlüssel** auf dem Server sind überwiegend mit Windows-DPAPI geschützt; die Ausnahmen nennt ID-54, Abschnitt 7. Wo sie liegen, wie sie gewechselt werden und was eine Wiederherstellung braucht, steht ebenfalls in ID-54.

Die Datenbankdateien selbst verschlüsselt das Produkt nicht. Dafür ist die Laufwerksverschlüsselung des Servers zuständig, etwa BitLocker (Abschnitt 7).

2.2 Pseudonymisierung und Datensparsamkeit

- **Betriebsprotokolle** maskieren Mailadressen, IP-Adressen, Telefonnummern und Benutzernamen. Die Vorgabe kürzt sie (Domäne, Netz, Landeskennzahl bleiben), auf Wunsch werden sie durch ein Kürzel ersetzt (ID-50, Abschnitt 10.8). Push-Zustelltoken stehen in keinem Protokoll.
- **Anonymisierung auf Antrag.** Eine Person lässt sich mit dem Recht `privacy.manage` in allen Bereichen der Auskunft anonymisieren (Art. 17 DSGVO), erst nachdem die Auskunft zu ihr erstellt wurde; Inhalte ihrer Vorgänge nur auf ausdrückliche Wahl (ID-40, Abschnitt 19; ID-56, Abschnitt 5.1). Die Einträge des Prüfprotokolls bleiben dabei bewusst erhalten.
- **Fristenlöschung** gibt es für Alarmprotokolle, Rohereignisse des Monitorings, Laufdaten der Datensicherung, Protokolldateien, Sicherungen, Sitzungen, Anmeldeanfragen, Kennwort-Zurücksetzen, die Mail-, Push- und Messenger-Warteschlange und BCM-Offline-Kits. Fristen und Löschwege je Datenkategorie stehen im Löschkonzept (ID-56).

3 Vertraulichkeit (lit. b)

3.1 Anmeldung

Maßnahme	Umsetzung	Einstellbar
Kennwortschutz	Argon2id-Hashwert mit Salt; das Kennwort selbst wird nie gespeichert	—
Kennwortregel (lokale Konten)	mindestens 12 Zeichen mit Groß- und Kleinbuchstaben und Ziffer; gilt beim Einrichten, Ändern und Zurücksetzen	—
Sperre nach Fehlversuchen	fünf Fehlversuche in Folge sperren das Konto zehn Minuten; ein falscher Bestätigungscode zählt mit	<code>Identity:Jwt:BruteForceMaxAttempts</code> , <code>Identity:Jwt:BruteForceLockMinutes</code>

Maßnahme	Umsetzung	Einstellbar
Anfragegrenze	Anmeldung, Einrichtung und Kennwort-Zurücksetzen: zehn Anfragen je Minute und Absenderadresse	—
Keine Kontenaufzählung	die Anmeldung antwortet bei unbekanntem Konto und falschem Kennwort gleich und gleich schnell	—
Zweiter Faktor	Einmalcode nach RFC 6238 (Authenticator-App), Geheimnis verschlüsselt; Abschalten verlangt eine Bestätigung (ID-41, Abschnitt 6)	je Benutzer; Pflicht je Mandant (Abschnitt 8)
Eine Sitzung je Weg	eine neue Anmeldung beendet die vorherige Sitzung desselben Kontos am Arbeitsplatz (Client und Portal gemeinsam); jedes Mobilgerät hat eine eigene Sitzung (ID-41, Abschnitt 4.2)	—
Sitzungsende nach Ruhe	Client und App: 12 Stunden ohne Zugriff; Portal: 30 Minuten	<code>Identity:Jwt:RefreshTokenExpiryHours</code> , <code>Session:LifetimeMinutes</code>
Kurzlebige Zugriffstoken	15 Minuten (App: 10); die Rechte prüft der Server bei jedem Aufruf neu, gesperrte Konten erhalten spätestens danach keinen neuen Token	<code>Identity:Jwt:AccessTokenExpiryMinutes</code>
Zentrale Anmeldung	Windows-Anmeldung (Kerberos/NTLM) und OIDC; Konten und Gruppen aus dem Verzeichnisdienst werden nur gelesen	ID-41, ID-50
Geräteanmeldung der App	Schlüsselpaar im Android-Keystore; der private Schlüssel verlässt das Gerät nicht	—
Maschinen-Zugänge	Integrations-Token je Mandant, nur mit Einspeise-Rechten, einzeln widerrufbar, nur als Hashwert gespeichert (ID-50, Abschnitt 7.4)	Ablaufdatum je Token

Aktive Sitzungen lassen sich in der Benutzerverwaltung einsehen und gezielt beenden (ID-41).

3.2 Zugriffskontrolle und Rollen

- **Rechte statt Rollennamen.** Jede Rolle ist eine Sammlung einzelner Rechte nach dem Schema `<modul>.<objekt>.<aktion>`. Mehrere Rollen addieren sich (ID-44).
- **Durchsetzung auf dem Server.** Anmeldung und Recht prüft die Schnittstelle, nicht erst die Oberfläche; ohne Recht antwortet sie mit 403. Client und Portal blenden nur aus, was ohnehin abgewiesen würde.
- **Getrennte Rechte für das Lesen und das Ausgeben.** Wer das Prüfprotokoll lesen darf (`audit.read`), darf es noch nicht exportieren (`audit.export`). Berichte zeigen nur Daten, für die auch das jeweilige Modulrecht vorliegt. Freie SQL-Berichte laufen unter der eigenen, nur lesenden Datenbankrolle `ordvis_bericht` ohne Zugriff auf Zugangsdaten; fehlt die Rolle, laufen sie übergangsweise unter der Rolle der Anwendung, und der Systemstatus meldet das (ID-27a; ID-50, Abschnitt 7).
- **Zwei Ebenen.** Mandanten anlegen und löschen darf nur, wer die Plattform-Rechte `tenant.*` trägt; der gewöhnliche IT-Administrator hat sie nicht (ID-44, Abschnitt 1.1).
- **Verzeichnisdienst nur lesend.** Ordvis IT schreibt nie in das Active Directory.
- **Kein Datenbankzugang am Arbeitsplatz.** Clients sprechen ausschließlich mit der Schnittstelle und tragen keine Datenbank-Zugangsdaten. PostgreSQL muss aus dem Client-Netz nicht erreichbar sein; bei lokaler Datenbank lässt die Firewall Port 5432 nur vom Server selbst zu (ID-50, Abschnitt 7).

3.3 Mandantentrennung

- **Eigene Datenbank.** Jeder Mandant, den Sie in der Mandantenverwaltung anlegen, erhält eine eigene Datenbank (`infradesk_<Kürzel>`). Jede Anfrage wird nach der Anmeldung an die Datenbank ihres Mandanten geleitet. Der Mandant, der bei der Einrichtung entsteht, liegt in der Hauptdatenbank.
- **Mandantenkennung in jeder Zeile.** Zusätzlich trägt jede mandantenbezogene Tabelle die Kennung des Mandanten, und jede Abfrage im Rahmen einer Anmeldung filtert danach. Auch das Prüfprotokoll lässt sich nur für den eigenen Mandanten durchsuchen.
- **Übergreifender Zugriff** ist nur über ausdrücklich erteilte, befristete und entziehbare Freigaben möglich (ID-42, Abschnitt 6).

4 Integrität (lit. b)

4.1 Protokollierung

Protokoll	Was es festhält	Wo
Prüfprotokoll	Änderungen an Fachdaten und sicherheitsrelevante Vorgänge: Zeitpunkt, handelnde Person, Aktion, betroffenes Objekt, IP-Adresse, soweit vorhanden die geänderten Werte, dazu Zugangsweg (Client, Portal, App, Schnittstelle) und Gerätekennung	Datenbank; lesen mit <code>audit.read</code> , ausgeben mit <code>audit.export</code> (ID-40, Abschnitt 10)
Windows-Ereignisprotokoll	Anmeldungen und Fehlanmeldungen, Kontosperrungen, Kennwortänderungen, Änderungen an Konten, Rollen und Rechten, Dienst-, Aktualisierungs-, Sicherungs- und Lizenzereignisse; feste Ereigniskennungen	Protokoll <i>Anwendung</i> , Quelle <i>InfraDesk</i> ; für die Anbindung an ein SIEM (ID-40, Abschnitt 13)

Protokoll	Was es festhält	Wo
Betriebsprotokolle	technische Abläufe, Fehler, jede ein- und ausgehende Nachricht (Kommunikationsprotokoll); personenbezogene Felder maskiert	Protokollordner des Servers, auf Wunsch Syslog nach RFC 5424 (ID-50, Abschnitt 10)

Das Produkt bietet **keine Funktion**, einen Eintrag des Prüfprotokolls zu ändern oder zu löschen, und es löscht keine Einträge von selbst. **Lesende** Zugriffe stehen dort nur, wo besonders schutzbedürftige Daten das System verlassen oder eingesehen werden: die Ausgabe eines Alarmprotokolls, eines Berichts und des Prüfprotokolls selbst, die Datenauskunft und die Anonymisierung einer Person sowie das Ansehen von Datenpannen. Der Eintrag nennt Person, Zeitpunkt, Aktion und höchstens eine Anzahl, nie die gelesenen Daten und nie die Mailadresse der betroffenen Person.

Abbildung 1 zeigt, wie das Prüfprotokoll gegen nachträgliche Veränderung gesichert ist.

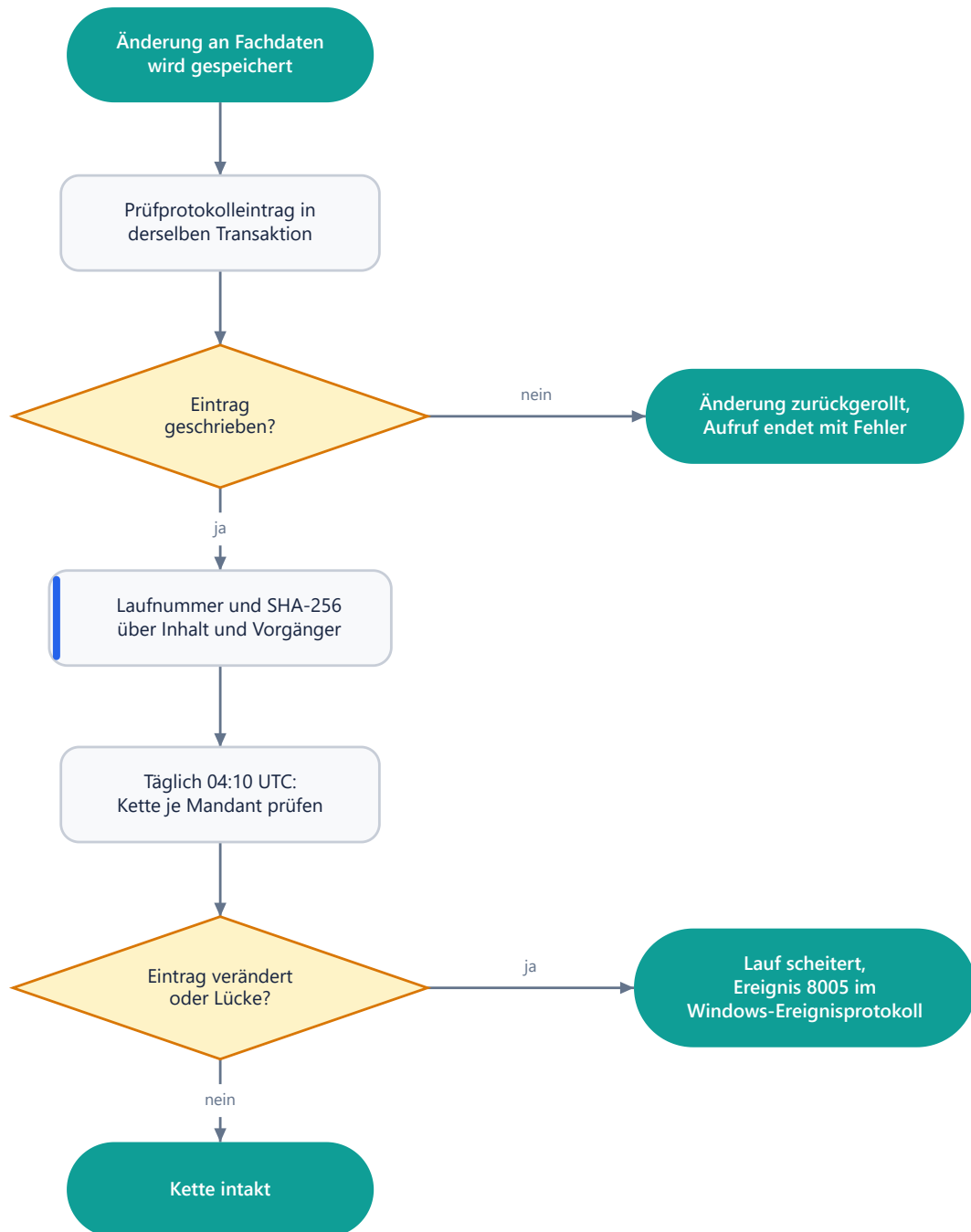


Abb. 1 – Eintrag in derselben Transaktion, Hashkette, tägliche Prüfung. Ein Bruch fällt außerhalb der Datenbank auf, im Windows-Ereignisprotokoll.

- **Kein Vorgang ohne Eintrag.** Der Eintrag entsteht in derselben Datenbanktransaktion wie die Änderung. Lässt er sich nicht schreiben, wird die Änderung zurückgerollt, und der Aufruf endet mit einem Fehler (Ausnahmen in Abschnitt 8).
- **Verkettet.** Jeder Eintrag trägt eine Laufnummer und einen SHA-256-Hash über seinen Inhalt und den Hash seines Vorgängers, je Mandant. Die geplante Aufgabe *Prüfprotokoll: Kette prüfen* prüft die Kette täglich um 04:10 UTC. Findet sie einen veränderten Eintrag oder eine Lücke, scheitert der Lauf. Der

Systemstatus zeigt das unter „Geplante Aufgaben“, und das Windows-Ereignisprotokoll meldet 8005 `AuditChainBroken`.

- **Ändern, Löschen und Leeren entzogen.** Dem Datenbankkonto der Anwendung sind diese Rechte an der Tabelle des Prüfprotokolls entzogen.

4.2 Unverfälschte Daten und Programme

- **Verschlüsselte Geheimnisse** tragen eine Prüfsumme (AES-GCM). Ein veränderter Wert fällt beim Lesen auf, statt still falsch entschlüsselt zu werden.
- **Aktualisierungen** tragen ein signiertes Manifest (ECDSA P-256). Server, Arbeitsplätze und App prüfen die Signatur und den SHA-256-Wert jeder Datei, bevor sie etwas einspielen, und brechen bei Abweichung ab (ID-53, Abschnitt 4).
- **Lizenzen** sind signiert (ECDSA P-256) und lassen sich nicht unbemerkt verändern.
- **Browser-Schutz.** Schnittstelle und Portal senden HSTS und Sicherheitskopfeilen (keine Einbettung in fremde Seiten, keine Typ-Umdeutung, Inhaltsrichtlinie).

5 Verfügbarkeit, Belastbarkeit und Wiederherstellung (lit. b und c)

- **Tägliche Sicherung.** Die geplante Windows-Aufgabe `InfraDesk-DailyBackup` sichert die Hauptdatenbank und **jede Mandanten-Datenbank**, auch die archivierter Mandanten. Fehlt ein Mandant oder scheitert einer, entsteht keine Sicherung, und der Lauf endet mit einem Fehler. Aufbewahrung in der Vorgabe 30 Tage, einstellbar unter *Einstellungen* ▶ *Backup* (ID-50, Abschnitt 6).
- **Prüfung nach jedem Lauf.** Jeder Dump wird vollständig gelesen, das verschlüsselte Archiv mit dem Sicherungskennwort geprüft (`7z t`). Scheitert eine Prüfung, wird die Sicherung verworfen. Das Ergebnis steht mit SHA-256-Prüfsumme im Sicherungsprotokoll, im Systemstatus („Datensicherung“) und als Ereignis 7001/7002 im Windows-Ereignisprotokoll (ID-50, Abschnitt 6).
- **Schlüssel reisen mit.** Die Tresorschlüssel liegen im verschlüsselten Sicherungsarchiv, damit eine Wiederherstellung auch auf anderer Hardware gelingt (ID-54, Abschnitt 5).
- **Wiederherstellung.** `restore.ps1` spielt eine Sicherung vollständig zurück oder mit `-Mandant` nur einen einzelnen Mandanten, ohne die übrigen zu berühren (ID-50, Abschnitt 6.2).
- **Aktualisieren ohne Datenverlust.** Datenbankänderungen laufen beim Aktualisieren des Servers; einen Rücksprung ermöglicht nur eine Sicherung von vorher (ID-53, Abschnitt 6).
- **Belastbarkeit.** Anfragegrenzen schützen die Schnittstelle vor Überlastung (ohne Anmeldung 120 Anfragen je Minute und Absenderadresse, angemeldet 1.500 je Konto; ID-60, Abschnitt 3.2). Eine kurze Störung beim Erneuern einer Anmeldung meldet niemanden ab (ID-41, Abschnitt 4.2).
- **Systemstatus.** Client und Portal zeigen unter *Systemstatus* den Zustand von Datenbank, Mailversand, Datensicherung und geplanten Aufgaben, dazu Sicherheitsvorgaben wie eine noch vorhandene Zugangsdatei der Einrichtung oder eine fehlende Berichtsrolle.
- **Notfall ohne Server.** Das BCM-Modul erzeugt jede Nacht je Mandant ein verschlüsseltes Offline-Notfall-Kit mit Notfallplänen und Alarmierungslisten, das sich ohne Ordavis öffnen lässt (ID-29, Abschnitt 6.1). Ohne hinterlegte Passphrase entsteht kein Kit.

6 Regelmäßige Überprüfung (lit. d)

Was das Produkt dafür mitbringt:

- **Zugriffsüberprüfung.** Ein Durchlauf friert alle Rollenzuweisungen eines Mandanten ein; jede wird einzeln bestätigt oder entzogen, mit Begründung und Namen der prüfenden Person. Abschließen lässt er sich erst, wenn nichts mehr offen ist (ID-40, Abschnitt 15).
- **Prüfprotokoll und Ereignisprotokoll** lassen sich nach Person, Objekt und Zeitraum auswerten oder an ein SIEM weitergeben (Abschnitt 4.1).
- **Systemstatus und Stückliste der Fremdbestandteile** (SBOM) zeigen, was auf der Anlage läuft (ID-53, Abschnitt 8).

Was der Hersteller tut:

- Schwachstellen nimmt security@ordavis.eu entgegen. Sicherheitsaktualisierungen erscheinen kostenlos bis einschließlich 31.12.2032; aktiv ausgenutzte Schwachstellen meldet der Hersteller nach der Cyberresilienz-Verordnung (ID-53).
- Vor jeder Fassung laufen die automatischen Tests des Produkts und eine Prüfung gegen einen Katalog von Datenschutz- und Sicherheitsvorgaben. Die Fremdbestandteile werden regelmäßig auf bekannte Schwachstellen und das Ende ihrer Pflege geprüft.
- Dieses Kapitel wird mit jeder Fassung ausgeliefert und beschreibt deren Stand.

Was Sie regelmäßig prüfen sollten steht in Abschnitt 7.

7 Was Sie als Betreiber ergänzen

Diese Maßnahmen kann das Produkt nicht selbst treffen. Nehmen Sie sie in Ihre TOM auf:

Maßnahme	Warum	Siehe
Zutritt zum Serverraum und Zugang zum Server beschränken	Wer Verwaltungsrechte auf dem Server hat, erreicht jeden Schlüssel	ID-54, Abschnitt 6
Laufwerk des Servers verschlüsseln (etwa BitLocker)	Datenbankdateien und Protokolle liegen sonst unverschlüsselt	Abschnitt 2.1
HTTPS für Schnittstelle und Portal einrichten	Im Auslieferungszustand erwartet der Server einen vorgelagerten Reverse-Proxy und spricht selbst HTTP	ID-50, Abschnitt 7.1; ID-53, Abschnitt 3
Verzeichnisdienst über LDAPS anbinden; die Zertifikatsprüfung der Postfächer nicht auf <i>Ungültige akzeptieren</i> stellen	Ohne TLS geht das Kennwort des Bind-Kontos im Klartext über das Netz; ohne Prüfung ist eine Verbindung nicht gegen Umleitung geschützt	Abschnitt 2.1; ID-41
PostgreSQL auf den Server beschränken oder <code>hostssl</code> erzwingen	Die Datenbankverbindung wird nicht erzwungen verschlüsselt	ID-54, Abschnitt 7
Sicherungskennwort vergeben, getrennt verwahren, Sicherungen auf ein zweites System kopieren	Ohne Kennwort bleibt die Sicherung unverschlüsselt; auf demselben Server schützt sie nicht vor dessen Verlust	ID-50, Abschnitt 6.1

Maßnahme	Warum	Siehe
Rücklauf einer Sicherung regelmäßig erproben	Das Produkt prüft nach jedem Lauf, dass die Sicherung vollständig lesbar ist, spielt sie aber nicht probeweise zurück	Abschnitt 8
Zweiten Faktor für alle Konten mit Verwaltungsrechten verlangen	Das Produkt verlangt ihn in der Vorgabe nicht	ID-41, Abschnitt 6.4
Rollen nach minimaler Berechtigung vergeben, mindestens jährlich eine Zugriffsüberprüfung	Rechte wachsen mit der Zeit	ID-40, Abschnitt 15
Konten beim Austritt deaktivieren; Verzeichnisabgleich einrichten	Ein aktives Konto ist ein offener Zugang	ID-41
Für Skripte und Fremdsysteme eigene Konten bzw. eigene Integrations-Token mit wenigen Rechten	Ein geteiltes Konto lässt sich keiner Person zuordnen	ID-60, Abschnitt 8
Prüfprotokoll und Ereignisprotokoll auswerten, Zuständigkeit festlegen	Ein Protokoll, das niemand liest, schützt nicht	Abschnitt 4.1
Aktualisierungen zeitnah einspielen, vorher sichern	Sicherheitsaktualisierungen wirken erst, wenn sie eingespielt sind	ID-53, Abschnitte 4 und 6
Zugangsdatei der Einrichtung nach sicherer Verwahrung löschen	Sie enthält Datenbankkennwort und Signaturgeheimnis	ID-54, Abschnitt 7
Ungenutzte Module abschalten	Jedes Modul ist Angriffsfläche	ID-53, Abschnitt 3
Swagger im Betrieb ausgeschaltet lassen	Eingeschaltet ist die Schnittstellenbeschreibung ohne Anmeldung lesbar	ID-60, Abschnitt 1
Löschfristen festlegen und umsetzen	Die Fristen bestimmen Sie als Verantwortlicher; für einen Teil der Bereiche löscht das Produkt noch nicht selbst	ID-56

8 Bekannte Grenzen

Offen gesagt, damit Sie sie in Ihrer Risikobewertung berücksichtigen können:

- **Das Prüfprotokoll ist gegen Datenbankverwalter nicht fälschungssicher, aber eine Änderung fällt auf.** Die Datenbank gehört dem Konto der Anwendung; als Eigentümer kann es sich die entzogenen Rechte zurückgeben, und ein PostgreSQL-Verwalter braucht sie ohnehin nicht. Wer einen Eintrag ändert oder aus der Mitte entfernt, bricht aber die Kette, und die tägliche Prüfung meldet das. Nicht erkennbar sind zwei Fälle: ein Entfernen der jüngsten Einträge am Ende der Kette und ein vollständiges Neuberechnen aller Hashwerte. Dagegen hilft ein Abgleich außerhalb der Datenbank, etwa das Windows-Ereignisprotokoll in einem SIEM.

- **Lesende Zugriffe werden nur ausgewählt protokolliert** (Abschnitt 4.1). Das Ansehen eines Vorgangs, eines Kontakts oder eines Alarms in der Oberfläche steht nicht im Prüfprotokoll, ebenso wenig die Vorschau eines Berichts. Nachvollziehbar ist dort, wer etwas **geändert** hat, nicht, wer es **gesehen** hat.
- **Scheitert das Schreiben eines Prüfprotokolleintrags**, wird die Änderung zurückgerollt. Das gilt für Änderungen, die über die Datenkontexte der Module gespeichert werden, und damit für den weit überwiegenden Teil. Ausgenommen sind Massenänderungen, die an diesem Weg vorbei direkt in die Datenbank schreiben, und Anlagen, deren neues Objekt beim Speichern nicht eindeutig feststeht. Dort entsteht der Eintrag unmittelbar nach der Änderung; scheitert er, bleibt die Änderung bestehen, und der Fehler steht im Betriebsprotokoll.
- **Das Prüfprotokoll hat keine Aufbewahrungsfrist**. Es wächst unbegrenzt und wird auch bei der Anonymisierung einer Person nicht bereinigt.
- **Fristenlöschung fehlt** für Vorgänge, Kontakte, deaktivierte Konten, Benachrichtigungen und das Prüfprotokoll. Bis dahin löschen oder anonymisieren Sie von Hand (ID-56).
- **Die Mandantentrennung ist eine Leistung der Anwendung**, keine der Datenbankrechte: Alle Mandanten-Datenbanken gehören derselben Datenbankrolle, und der Mandant aus der Einrichtung teilt sich die Hauptdatenbank mit der Mandantenverwaltung. Geplante Aufgaben arbeiten ohne angemeldete Person und damit über alle Mandanten.
- **Die Pflicht zum zweiten Faktor** gilt nur, wenn Sie sie festlegen (alle Konten, Konten mit Verwaltungsrechten oder ausgewählte Rollen, im Client und im Portal; Recht `identity.mfa.enforce`, ID-41, Abschnitt 6.4). Ohne Festlegung gilt keine Pflicht. Bei Anmeldungen über Verzeichnis, OIDC oder Windows entscheidet das fremde Verzeichnis.
- **Eine Sitzung je Weg** gilt für die Anmeldung über Client, Portal, App, Windows-Anmeldung und OIDC. Der zusätzliche Anmeldeweg `POST /api/v1/auth/central-login` der Schnittstelle beendet vorhandene Sitzungen nicht.
- **Kennwortregel** ohne Sonderzeichenpflicht, Wiederverwendungssperre oder Abgleich mit bekannten Kennwörtern. Konten aus dem Verzeichnisdienst folgen dessen Regeln.
- **Verbindungen zu Fremdsystemen** lassen sich unverschlüsselt (LDAP) oder ohne Zertifikatsprüfung (Postfächer, Exchange) betreiben, wenn der Betreiber das einstellt (Abschnitt 2.1).
- **Sicherungen werden nicht probeweise zurückgespielt**. Der Lauf liest jeden Dump vollständig und prüft das Archiv mit dem Kennwort; ob sich die Sicherung fehlerfrei in eine Datenbank zurückspielen lässt, belegt erst ein Rücklauf auf einem Testsystem. Das Informationssereignis 7001 erscheint im Windows-Ereignisprotokoll nur, wenn der Mindest-Schweregrad des Sicherheitsprotokolls auf *Information* steht (ID-40); ein Fehlschlag (7002) wird in der Vorgabe gemeldet.
- **Keine zentrale Vorgaberegeln für Zugriffe**. Jede Aktion der Schnittstelle trägt ihre eigene Zugriffsregel; eine zentrale Regel, die alles Unmarkierte abweist, fehlt noch.
- Die Grenzen der Verschlüsselung und Schlüsselablage stehen in ID-54, Abschnitt 7.

9 Häufige Fragen

Kann der Hersteller auf unsere Daten zugreifen? Nein. Es gibt keinen Fernzugang. Daten erreichen den Hersteller nur über Fehlerberichte, die jemand bei Ihnen ausdrücklich abschickt, und als Platzhalter bei Push-Benachrichtigungen (Abschnitt 1).

Wo liegen die Daten? In der PostgreSQL-Datenbank auf Ihrem Server, je Mandant in einer eigenen Datenbank (Abschnitt 3.3), dazu Sicherungen und Protokolle im Dateisystem des Servers.

Ist die Datenbank verschlüsselt? Zugangsdaten und Geheimnisse ja (AES-256-GCM), die übrigen Daten nicht. Verschlüsseln Sie das Laufwerk des Servers (Abschnitt 7).

Wer darf das Prüfprotokoll sehen und ausgeben? Lesen mit `audit.read`, ausgeben mit `audit.export` – getrennt vergebbar (Abschnitt 3.2).

Lässt sich ein Eintrag im Prüfprotokoll löschen? Nicht über das Produkt. Wer direkt in der Datenbank ändert, bricht die Kette, und die tägliche Prüfung meldet das (Abschnitt 4.1 und 8).

Wird protokolliert, wer einen Datensatz angesehen hat? Nur in ausgewählten Fällen (Abschnitt 4.1). Für gewöhnliche Ansichten nicht.

Wie lange bleiben Daten gespeichert? Das regelt das Löschkonzept je Datenkategorie (ID-56).

Wie gehen wir mit einem Löschantrag nach Art. 17 um? Auskunft erstellen, dann anonymisieren (ID-56, Abschnitt 5.1; ID-40, Abschnitt 19).

Welche Ereignisse kann unser SIEM empfangen? Die Ereignisse des Windows-Ereignisprotokolls (Quelle `InfraDesk`) und auf Wunsch die Betriebsprotokolle über Syslog (ID-40, Abschnitt 13; ID-50, Abschnitt 10.4).

Kann dieses Kapitel unverändert in unsere TOM? Ja, als Herstellerbeitrag. Ergänzen Sie die Maßnahmen aus Abschnitt 7 und Ihre Festlegungen zu Abschnitt 8.

Verwandte Themen

- ID-54 – Kryptokonzept
- ID-56 – Löschkonzept
- ID-57 – Verarbeitungstätigkeiten (VVT-Beitrag)
- ID-50 – Betriebshandbuch: Installation, Härtung, Sicherung, Protokolle
- ID-53 – Produktsicherheit & Meldewege
- ID-41 – Identität, Benutzer & Rollen
- ID-44 – Rollen- & Rechte-Matrix
- ID-42 – Mandantenfähigkeit
- ID-60 – API-Referenz
- ID-32 – Datenschutz (Verarbeitungsverzeichnis)