E. Detaillierte Ergebnisse zum Assessment (Detailed Assessment Results)

1 IS Policies and Organization

1.1 Information Security Policies

1.1.1 Inwieweit sind Richtlinien zur Informationssicherheit vorhanden?
Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)
Betrachtete Dokumente/Nachweise/Prüfungshandlung: • X-VA-76-10000012648-IT-Sicherheitsrichtlinie, • X-VA-76-10000790945_Leitlinie zur Informationssicherheit • Q Boards *Statement Hydac:* *"Es existiert eine Leitlinie zur Informationssicherheit sowie eine Informationssicherheitsrichtlinie (IT-SRL) für den HYDAC Firmenverbund.* *Diese sind von der Geschäftsführung frei geben und im Intranet veröffentlicht.* *Die Leitlinie und Richtlinie sind Verfahrensanweisungen und somit verpflichtend für alle Mitarbeiter.* *Die Kontrolle der Dokumente wird über das Dokumentenmanagement System (SAP basierend) durchgeführt."* Die Anforderungen an die Informationssicherheit sind in der Leitlinie zur Informationssicherheit definiert. Die Leitlinie enthält Ziele und den Stellenwert der Informationssicherheit in der Organisation. Richtlinien sind im Intranet für alle Mitarbeiter verfügbar. Mitarbeiter ohne Intranet Zugriff erhalten Zugang über deren Boards/Vorgesetzten.
Feststellung
Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.2 Organization of Information Security

1.2.1 Inwieweit wird in der Organisation Informationssicherheit gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- P1-Anwendungsbereich-Scope-ISMS.pdf,
- P2 - Organisation und Verantwortlichkeiten ISMS.pdf,
- Auszug Monatsbericht Mai&Juni 2021 mit Feedback Management zu ISMS.png,
- VA interne Audits

Statement Hydac:

"Das Statement Hydac: Informationssicherheitsmanagementsystem befindet sich für die zu prüfenden Standorte in Umsetzung und wird fortlaufend ergänzt und aktualisiert.

Es gibt ein monatliches GF-Meeting (Jourfix) indem aktuelle Themen besprochen werden. Zyklisch findet ein Meeting mit der Geschäftsführung, dem Informationssicherheits- / IT-Sicherheitsbeauftragten und der IT-Leitung statt.

Alle zwei Monate erfolgt ein Monatsbericht an die Geschäftsleitung indem durchgeführte Aktionen und Themen beschrieben werden. Die Geschäftsleitung kommentiert den Monatsbericht.

Einmal im Jahr wird der Geschäftsleitung ein IT-Sicherheitsbericht mit dem Stand des ISMS, aktuellen Projekten und Umsetzungsgraden in den Gesellschaften vorgelegt."

Der Geltungsbereich (Scope) des ISMS (die vom ISMS gemanagte Organisation) ist festgelegt. Die Anforderungen der Organisation an das ISMS sind ermittelt.
Die Organisationsleitung hat das ISMS beauftragt und freigegeben.

Feststellung

Es konnte nicht nachgewiesen werden, dass die Wirksamkeit des ISMS durch das Management regelmäßig überprüft wird.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Informationssicherheit ist in der Organisation angemessen zu managen. Hierzu ist ein Informationssicherheitsmanagementsystem (ISMS-Prozess) aufzubauen, einzuführen und von der Organisationsleitung freizugeben. Die Wirksamkeit des ISMS ist regelmäßig durch die Organisationsleitung zu überprüfen. Folgende Dokumentation ist zu erstellen: - Management-Review-Protokolle, Auditberichte und andere anwendbare Kontrollen zur regelmäßigen Wirksamkeitsprüfung in den letzten 2 Jahren Nachweis(e): - Nachweis regelmäßiger Kontrollen, Management-Reviews, interne und externe Auditberichte oder weitere Kontrollen der letzten 2 Jahren Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

1.2.2 Inwieweit sind die Verantwortlichkeiten für Informationssicherheit organisiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- P2 - Organisation und Verantwortlichkeiten ISMS.pdf,
- Bestellung IT-CISO&SiBe.pdf,
- interne Teammatrix mit Aufgabengebieten.pdf
- Organigramm ORG0021_02_c_HV_ZA Informatik.pdf
- Organigramm ORG0009_01_e_HYDAC Accessories GmbH_GB AM und BT.pdf
- TNB Kloß – Lead Auditor 27001.pdf
- GIAC Reverse Engineering Malware Schnur.pdf
- GIAC Certified Forensic Analyst Schnur.pdf

Statement Hydac:

"Die Zuweisung der Verantwortung für das ISMS und für die Informationssicherheit sind geklärt und durch die Geschäftsführung frei gegeben und die Bestellung im Intranet veröffentlicht."

Die Verantwortlichkeiten für die Informationssicherheit sind im Unternehmen definiert.

Die notwendigen Ressourcen stehen zur Verfügung.

Die Ansprechpartner sind innerhalb der Organisation und relevanten Geschäftspartnern bekannt.

Die weiterführenden Aufgaben sind klar definiert.

Feststellung

Es konnte nicht nachgewiesen werden, dass der Chief Information Security Officer (Herr Schnur) ein Qualifikationsnachweis im Bereich Informationssicherheit (z.B. CISM, CISA, ISO 27001 Lead Implementer, ISO 27001 Lead Auditor) besitzt.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Die Verantwortlichkeiten für die Informationssicherheit in der Organisation sind zu definieren, zu dokumentieren und zuzuweisen. Die verantwortlichen Mitarbeiter sind für ihre Aufgabe zu qualifizieren. Nachweis(e): - Qualifikationsnachweis (z.B. Schulungszertifikate) Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

1.2.3 Inwieweit werden Informationssicherheitsanforderungen in Projekten berücksichtigt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Demand Prozess,
- Nachweise IDEAS Projekt,
- Sicherheitsrichtlinie Klassifizierung von Dokumenten und Informationen

Statement Hydac:

" Projekte werden in Service Now erstellt und gesteuert. Projekte sind über ein Feld klassifiziert. Grundsätzlich werden Demands angelegt aus denen Projekte hervorgehen. In der Prüfungsphase wird der Datenschutz, der Betriebsrat und die Personalabteilung automatisch per Mail informiert. Das IT-Sicherheitsteam muss dem Projekt über einen Freigabetask aktiv zustimmen. Erst nach Genehmigung IT-Sicherheitsteam und GL wird das Projekt angelegt.

HYDAC Accessories:
Projekte werden im SAP Projektmanagement verwaltet."

Feststellung

Es konnte nicht nachgewiesen werden, dass nicht alle Projekte unter Berücksichtigung ihrer Anforderungen an die Informationssicherheit klassifiziert sind.

Die Vorgehensweise und Kriterien zur Klassifizierung von Projekten sind nicht dokumentiert.

Eine Risikobewertung von Projekten konnte nicht nachgewiesen werden.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Projekte sind unter Berücksichtigung ihrer Anforderungen an die Informationssicherheit zu klassifizieren. Die Vorgehensweise und die Kriterien zur Klassifizierung von Projekten sind zu dokumentieren. In einer frühen Phase des Projektes ist eine Risikobewertung auf Basis einer definierten Vorgehensweise durchzuführen und bei Änderungen des Projektes zu wiederholen. Für identifizierte Informationssicherheitsrisiken sind Maßnahmen abzuleiten und im Projekt zu berücksichtigen. Es ist eine Prozessbeschreibung zu erstellen, welche die Vorgehensweise zur Klassifizierung sowie zur Durchführung einer Risikobewertung von Projekten beschreibt. Abgeleitete Maßnahmen sind im Verlauf des Projektes regelmäßig zu überprüfen und bei Änderungen der Bewertungskriterien neu zu bewerten. Nachweis(e): - Prozessbeschreibung zur Klassifizierung von Projekten - Nachweis zur Einstufung / Klassifizierung von Projekten (Beispiel-Projekte) - Prozessbeschreibung zur Risikobewertung von Projekten - Nachweis zur Risikobewertung von Projekten Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

1.2.4 Inwieweit sind die Verantwortlichkeiten zwischen Organisations-fremden IT-Service-Anbietern und der eigenen Organisation definiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- X-VA-76-10000012648-IT-Sicherheitsrichtlinie,
- IT-SRL externe Dienstleister,
- Cloud-Sicherheitsrichtlinie,
- Servicevereinbarungen für Cloud-Dienste im Scope (Umantis)
- AVV
- Verinice Asset Übersicht

Statement Hydac:

"Cloudanwendungen bzw. Clouddienste sind nur nach Freigabe durch die IT gestattet. Für die Einführung eines Cloud-Dienstes gibt es eine Cloud-Sicherheitsrichtlinie. Des Weiteren gilt die IT-Sicherheitsrichtlinie sowie die IT-SRL für externe Dienstleister."

Eingesetzte betroffene IT-Dienste und IT-Dienstleistungen sind identifiziert.

Eine Prozessbeschreibung zur Bewertung eingesetzter Dienste ist vorhanden.

Die Bewertung wird durch die IT-Security Abteilung durchgeführt.

Für IT-Dienste werden die Konfigurationseinstellungen durch die IT-Security Abteilung bewertet.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.3 Asset Management

1.3.1 Inwieweit werden Informationswerte (Assets) identifiziert und erfasst?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- ISMS Asset-Modell,
- Screenshot Verinice

Statement Hydac:

"Die relevanten Serviceleistungen der Zentralabteilung Informatik sind in dem genutzten ISMS Tool „Verinice“ abgebildet und werden fortlaufend aktualisiert."

Die für die Organisation kritischen Informationswerte sind in der Schutzbedarfsanalyse identifiziert und bewertet worden.
Diesen Informationswerten ist eine verantwortliche Stelle zugeordnet.
Informationsträger, welche die Informationswerte verarbeiten, sind in einer Assetliste (Verinice) erfasst.
Diesen Informationsträgern ist ein Verantwortlicher zugeordnet.

Feststellung

Der Prozess wurde im bestehenden IMS neu initialisiert.

☐ Hauptabweichung ☐ Nebenabweichung ☒ Beobachtung ☐ Identifiziertes Verbesserungspotential

1.3.2 Inwieweit werden Informationswerte hinsichtlich ihres Schutzbedarfs klassifiziert und gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

• Klassifizierung von Dokumenten und Informationen

Statement Hydac:

"Dokumente und Informationen werden anhand eines, vom Zentralbereich Informatik entwickelten, Dokumentes in verschiedene Kategorien klassifiziert. Dies geschieht mit Hilfe einer Klassifizierungsmatrix. Die Anforderungen an den Umgang mit Dokumenten einer Kategorie sind in dem Dokument erläutert."

Feststellung

Es konnte nicht nachgewiesen werden, dass eine Bewertung der identifizierten Informationswerte nach den definierten Kriterien durchgeführt und dem vorhandenen Schema zur Klassifizierung zugeordnet wird. Die Schutzziele Integrität und Verfügbarkeit werden in der Richtlinie Klassifizierung von Dokumenten und Informationen nicht berücksichtigt. Des Weiteren sind die definierten Schutzziele abweichend zwischen der Richtlinie und dem eingesetzten Tool Verinice.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Ein einheitliches Schema zur Klassifizierung von Informationen hinsichtlich Vertraulichkeit ist zu definieren, zu dokumentieren und freizugeben. Dabei sind die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität zu berücksichtigen. Alle Mitarbeiter sind über das Klassifizierungsschema zu informieren. Die Informationseigentümer sind zu verpflichten, ihre Informationen gemäß Klassifikationsschema einzustufen. Es sind Maßnahmen für den gesamten Lebenszyklus abzuleiten (mind. Kennzeichnung, korrekte Handhabung, Transport, Speicherung, Rückgabe, Löschung / Entsorgung), z.B. in Form einer "Schutzmatrix". Es sind alle relevanten Formen der Verarbeitung zu beachten, wie z.B. Dokumente, E-Mails, Dateien, Ausdrucke usw. Es sind Regeln festzulegen, wie unklassifizierte Dokumente zu behandeln sind. Ggf. sind spezifische Anforderungen des Auftraggebers zu berücksichtigen. Nachweis(e): - Klassifizierungsschema - Handlungsanweisungen ("Schutzmatrix") zum Umgang mit Informationen - Prozessbeschreibung Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

1.3.3 Inwieweit wird sichergestellt, dass nur evaluierte und freigegebene organisationsfremde IT-Dienste zum Verarbeiten von Informationswerten der Organisation eingesetzt werden?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Schulungskonzept_Awareness,
- X-VA-76-1000012648-IT-Sicherheitsrichtlinie,
- IT-SRL externe Dienstleister.pdf,
- IT Standards,
- Softwarepaketierung Prozess,
- Vorlage Servicevereinbarungen für Cloud-Dienste
- Verinice

Statement Hydac:

"Es werden Webfilter eingesetzt um potenziell schädliche Seiten zu blockieren. In Verdachtsfällen werden diese Webfilterlogs geprüft und ausgewertet. Zusätzlich werden Mitarbeiter durch Schulungen sensibilisiert und sind sich durch die IT-Sicherheitsrichtlinie ihrer Verantwortung an eine ordnungsgemäße Nutzung bewusst. Siehe ebenfalls VDA Version 5.1 Punkt 1.2.3"

Es werden keine organisationsfremden IT-Dienste ohne explizite Bewertung und Umsetzung der Informationssicherheitsanforderungen eingesetzt.

Die Mitarbeiter werden entsprechend sensibilisiert. Die Freigabe neuer Dienste erfolgt durch den ISB und DSB.

Feststellung

Es konnte nicht nachgewiesen werden, dass die organisationsfremden IT-Dienste mit dem Schutzbedarf der verarbeiteten Informationswerte abgeglichen sind.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Es ist sicherzustellen, dass organisationsfremde IT-Dienste nur mit expliziter Bewertung und Umsetzung der Informationssicherheitsanforderungen eingesetzt werden. Es ist je organisationsfremdem IT-Dienst eine Risikobewertung durchzuführen und zu dokumentieren. Gesetzliche, regulatorische und vertragliche Anforderungen sind zu betrachten und bei Anwendbarkeit zu dokumentieren. Die organisationsfremden IT-Dienste sind mit dem Schutzbedarf der verarbeiteten Informationswerte abzugleichen. Die Bewertung ist zu dokumentieren. Organisationsfremde IT-Dienste und deren Freigabe je nach Schutzbedarf sind zu dokumentieren. Nachweis(e): - Risikobewertung je eingesetzten organisationsfremden IT-Dienst - Überprüfungsprotokolle der Umsetzung der Sicherheitsanforderungen - Übersicht aller (freigegebener) org.-fremden IT-Dienste mit jeweiligem Schutzbedarf Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

1.4 IS Risk Management

1.4.1 Inwieweit werden Informationssicherheitsrisiken gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- P8-P9 Risikoanalyse Risikobewertung,
- Change Management Prozess,
- Verinice Asset und Verknüpfungen
- Verinice Risikoanalyse

Statement Hydac:

"Ein Referenzdokument zur Risikoanalyse ist vorhanden. Darauf aufbauend werden die Risikowerte im ISMS-Tool „Verinice“ abgebildet."

Risiken werden in Form eines Risikoverzeichnisses erfasst und hinsichtlich ihrer Eintrittswahrscheinlichkeit und Schadenshöhe bewertet und dokumentiert.
Jedem Risiko ist ein Risikoeigner zugeordnet.
Die Risiken werden in regelmäßigen Intervallen und anlassbezogen (neu-)bewertet.
Jedem Risiko ist eine Maßnahme zur Behandlung des Risikos zugeordnet.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.5 Assessments

1.5.1 Inwieweit wird die Einhaltung der Informationssicherheit in Verfahren und Prozessen sichergestellt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Auditprogramm Informationssicherheitsaudits,
- Informationssicherheitsauditbericht RT-Filtertechnik Standort Kromsdorf (wird im Audit vorgelegt),
- TISAX Ergebnisbericht.pdf – ISMS Audit 2021/2022
- Auditplan DS IT RT Filter Kromsdorf.pdf
- Auditplanung Datenschutz Hydac-2022_Freigabe GL.pdf
- Auditplanung DS IT HYDAC-2023.pdf
- interner Auditbericht 2018 ISO9001.pdf
- interner Auditbericht 2021 ISO9001.pdf
- interner Auditbericht 2022 ISO9001.pdf

Statement Hydac:

"Jährlich werden alle ISMS Dokumente einer Dokumentenprüfung unterzogen. Zur Überprüfung der Einhaltung der Informationssicherheit werden interne Audits (Datenschutz- und Informationssicherheitsaudit) mittels VDA ISA im HYDAC Firmenverbund durchgeführt."

Im Zuge der regelmäßigen internen Audits wird die Konformität der Informationssicherheit und die Einhaltung organisatorischer und technischer Vorgaben überprüft.

Jährlich wird das ISMS durch eine externe Beratungsgesellschaft (Controlware) geprüft.

Der Auditbericht für das Jahr 2021/2022 wurde vorgestellt.

Das Auditprogram wurde für 2023, 2024 und 2025 präsentiert.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.5.2 Inwieweit wird das ISMS von einer unabhängigen Instanz überprüft?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- iso_9001_hydac_technology_hydac_firmenverbund_2024-07-19_de.pdf
- TISAX Ergebnisbericht 2021.pdf

Statement Hydac:

"Die Prüfung des ISMS findet in Rahmen von Audits statt. Eine regelmäßige externe Überprüfung findet im Rahmen der TISAX Überprüfung statt. Weitere interne Audits werden durch den Zentralbereich ZQW im Rahmen der ISO 9001 Audits durchgeführt. Als weitere unabhängige Überprüfung werden Audits durch einen externen Diesntleister sowie Auskunfstanfragen durch Kunden durchgeführt.

HYDAC Accessories:

Es findet eine regelmäßige Prüfung im Rahmen des ISO 9001 Audits durch ZQW statt."

Im Rahmen der TISAX Zertifizierung durch die operational services wurde das ISMS durch eine unabhängige Instanz überprüft.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

1.6 Incident Management

1.6.1 Inwieweit werden Informationssicherheitsereignisse verarbeitet?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Behandlung von IT-Sicherheitsvorfällen,
- Notfallhandbuch,
- SOC Report Dashboard in Service Now,
- Incident Verlust Endgerät,
- Lessons Learned Vorlage

Statement Hydac:

"Informationssicherheitsvorfälle werden anhand einer etablierten Richtlinie bearbeitet. Der Meldeweg von Sicherheitsvorfällen ist bekannt, etabliert und im Intranet veröffentlicht. Die genaue Beschreibung der Behebung von solchen Problemen ist detailliert in der dafür vorgesehenen Richtlinie beschrieben und wird durch das IT-Sicherheitsteam praktiziert. Das Notfallhandbuch ergänzt die Behandlung von IT-Sicherheitsvorfällen."

Im Unternehmen existiert eine Definition von Informationssicherheitsvorfällen.

Eine Vorgehensweise zur Meldung und Erfassung von Informationssicherheitsvorfällen ist definiert und umgesetzt.

Die relevanten Aspekte werden berücksichtigt. Verfahren zur Sicherstellung der Nachweisbarkeit bei Informationssicherheitsvorfällen sind etabliert und dokumentiert.

Die Vorfälle werden bewertet und zur Sicherstellung der Nachweisbarkeit dokumentiert.

Es ist eine angemessene Reaktion auf Informationssicherheitsvorfälle im Rahmen des Prozesses definiert.

Feststellung

Es konnte nicht nachgewiesen werden, dass Anforderungen aus Geschäftsbeziehungen ermittelt und umgesetzt sind.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Es existiert keine angemessene Definition von Informationssicherheitsereignissen.

☐ Hauptabweichung ☐ Nebenabweichung ☒ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Die Vorgehensweisen zur angemessenen Reaktion auf Informationssicherheitsereignisse sind zu definieren. Die Art und Weise der Auswertung der Ereignisse ist zu definieren. Bei Bedarf sind Maßnahmen zur Verhinderung des erneuten Auftretens umzusetzen. Die Anforderungen aus Geschäftsbeziehungen sind zu ermitteln und umzusetzen (z.B. Bericht an Auftraggeber). Nachweis(e): - Prozess zur regelmäßigen Erhebung vertraglicher Anforderungen - Verfahren zur Verhinderung des erneuten Auftretens ähnlich gearteter Ereignisse Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

2 Human Ressources

2.1.1 Inwieweit wird die Eignung von Mitarbeitern für sensible Tätigkeitsbereiche sichergestellt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- BPMN Einstellungsprozess,
- Stellenausschreibung SOC
- Umantis

Statement Hydac:

"Mitarbeiter werden aufgrund ihrer Qualifikationen und Zertifizierungen ausgewählt. Werden weitere Nachweise oder Schulungen für Tätigkeiten benötigt, so werden diese angefragt bzw. durchgeführt.

Als sensible Tätigsbereich ist Human Ressources definiert.

Identitätsprüfung findet über Sozialversicherungsnummer in SAP statt."

Die Identität von potenziellen neuen Mitarbeitern wird überprüft.

Es werden Einstellungsgespräche mit Bewerbern durchgeführt.

Es findet eine erweiterte Prüfung der Eignung abhängig vom Tätigkeitsbereich und Stelle statt.

Feststellung

Es konnte nicht nachgewiesen werden, dass sensible Tätigkeitsbereiche und Stellen ermittelt sind.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Sensible Tätigkeitsbereiche und Stellen sind zu ermitteln. Hierzu sind die Anforderungen für relevante Positionen zu definieren und bei Bewerbern zu prüfen. Im Prozess ist die Überprüfung der Identität vorzusehen (z. B. Prüfung von Ausweisdokumenten). Zur Überprüfung der Eignung der Mitarbeiter sind einfache Methoden zu beschreiben und zu implementieren (z.B. durch Einstellungsgespräche). Abhängig vom Tätigkeitsbereich und der Stelle sind erweiterte Prüfmethoden zu etablieren (z. B. Assessment-Center, psychologische Analyse, Prüfung von Referenzen, Zeugnissen und Diplomen, Einsichtnahme in Führungszeugnisse, Prüfung des beruflichen und privaten Hintergrunds). Nachweis(e): - Liste sensibler Tätigkeitsbereiche - Kriterien für Positionen mit erhöhten Anforderungen an die Informationssicherheit Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

2.1.2 Inwieweit werden alle Mitarbeiter zur Einhaltung der Informationssicherheit verpflichtet?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Datengeheimnis Arbeitsvertrag,
- IT-SRL, Vorlagen
- Datenschutz

Statement Hydac:

"Im Arbeitsvertrag wird auf die Einhaltung von Verfahrensanweisungen und im Unternehmen geltendene Richtlinien sowie Geheimhaltung verpflichtet. Mit Abschluss des Arbeitsvertrages erhält der Mitarbeiter eine Erklärung zum Datengeheimnis, die er mit dem Unterzeichnen einwilligt. Weitere Verpflichtungen zur Geheimhaltung können je nach Berufsgruppe bestehen und werden durch den Zentralbereich Datenschutz ausgegeben. Die IT-SRL ist eine Verfahrensanweisung und somit für alle Mitarbeiter bindend."

Mitarbeiter werden zur Geheimhaltung und auf das Regelwerk zur Informationssicherheit verpflichtet.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

2.1.3 Inwieweit werden Mitarbeiter über die Risiken beim Umgang mit Informationen geschult und sensibilisiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

• Schulungskonzept Awareness,

• Sicherheitstipp / -warnung, IT-Sicherheitsrichtlinie

Statement Hydac:

"Es finden mehrere Formen der Sensibilisierung der Mitarbeiter statt. Diese wären:

- Eine regelmäßige Online-Unterweisung für den Themenbereich IT-Sicherheit für alle Mitarbeiter wird durchgeführt. Nach Abschluss der Unterweisung kann ein entsprechendes Teilnahmezertifikat als PDF heruntergeladen werden.

- Es finden regelmäßige Phishing-Kampagnen statt, die die Awareness der Mitarbeiter verbessern soll.

- Jeder Mitarbeiter erhält zudem eine Unterweisung durch den Zentralbereich Datenschutz, um alle für Ihn notwendigen Informationen bezüglich des Datenschutzes zu erhalten.

- Anlassbezogene Information der Mitarbeiter als Sicherheitstipp oder Sicherheitswarnung per Mail oder Ticker (Laufband-Meldung), zum Beispiel bei aktuellen Phishing-Mailwellen

HYDAC Verwaltung – Zentralbereich Informatik:

- Im Zentralbereich Informatik finden regelmäßig Pentests statt, mit deren Ergebnisse der jeweilige Bereich sensibilisiert wird."

Feststellung

Es konnte nicht nachgewiesen werden, dass Mitarbeiter geschult und sensibilisiert sind.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)

Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft):
Mitarbeiter sind gemäß den Anforderungen der Informationssicherheit zu unterweisen.
Bei Einstellung sind Mitarbeiter initial auf die Sicherheitsanforderungen zu belehren und zu verpflichten.
 	
Teilnehmerlisten sind zu erstellen und regelmäßig (z.B. einmal jährlich) auf Vollständigkeit zu prüfen.
 	
Nachweis(e):
- Schulungsinhalt (z.B. Folien) mit mindestens folgendem Inhalt:
  - Richtlinie zur Informationssicherheit
  - Meldungen von Informationssicherheitsereignissen
  - Verhalten bei Auftreten von Schadsoftware
  - Richtlinien zu Benutzerkonten und Anmeldeinformationen (z. B. Passwortrichtlinie)
  - Compliance-Themen der Informationssicherheit (rechtliche und vertragliche Anforderungen zur Informationssicherheit (z.B. kundenspez. Anforderungen, etc.))
  - Anforderungen und Verfahren zum Einsatz von Geheimhaltungsvereinbarungen bei der Weitergabe von schutzbedürftigen Informationen
  - Einsatz organisationsfremder IT-Dienste
- Teilnehmerlisten
 	
Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.

Bewertung nach Follow-Up

2.1.4 Inwieweit ist mobiles Arbeiten geregelt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Sicherheitsrichtline mobiles Arbeiten,
- Sicherheitstipps,
- IT-SRL mit „Klassifizierung von Dokumenten und Daten“ und „Endgeräteschutz“
- BV HomeOffice.pdf

Statement Hydac:

"Das mobile Arbeiten ist mit der Richtlinie mobiles Arbeiten geregelt. Zusätzlich wurden IT-Sicherheitstipps per E-Mail versendet. Diese Sicherheitstipps stehen allen Beschäftigten im Intranet zur Verfügung. Der Zugang außerhalb des HYDAC Netzwerks erfolgt über einen VPN-Client."

Die Schutzmaßnahmen in Bezug auf mobiles Arbeiten außerhalb der definierten Schutzzonen sind bei Dienstreisen und Home-Office geregelt.

Der Umgang auf Dienstreisen ist dokumentiert und wurde vorgestellt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

3 Physical Security and Business Continuity

3.1.1 Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- X-VA-73-10000315021-Unternehmenssicherheit-Zugangsmanagement-Besucher,
- X-VA-73-10000216051-Unternehmenssicherheit-Zugangsmanagement-Beschäftigte,
- Sicherheitsrichtlinie Zutrittssicherungen und Sicherheitszonen,
- Grundriss mit Sicherheitszonen der jeweiligen Standorte
- Mechatronische Schließanlage +CLIQ der Fa. Ikon ASSA ABLOY

Statement Hydac:

"Der Zugang zu Gebäuden ist in einer Verfahrensanweisung sowohl für Besucher als auch für Beschäftigte geregelt. Zusätzlich gibt es ein internes Dokument zu Bestimmungen der Zutrittssicherung und der Sicherheitszonen. Pläne des Grundrisses mit eingezeichneten Sicherheitszonen sind erstellt."

Sicherheitszonen sind unter Berücksichtigung von Geländen/Gebäuden/Räumen definiert und dokumentiert.

Verfahren zur Vergabe und zum Entzug von Zutrittsberechtigungen sind etabliert.

Feststellung

Es konnte nicht nachgewiesen werden, dass Maßnahmen zum Schutz gegen einfaches Mithören und Einsichtnahme definiert und umgesetzt sind.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Erstellung eines Sicherheitszonenkonzept inkl. Darstellung der Schutzmaßnahmen (z.B. Zutritt, Alarm, Brandmelder, etc.). Die Kennzeichnung und Beschreibung der Zonen sind in das Zonenkonzept aufzunehmen (inkl. Anlieferungs- und Versandbereich). Die Verhaltensregeln für die jeweiligen Sicherheitszonen sind bekanntzugeben. Eine Richtlinie für die Einbringung und Nutzung von mobilen IT-Geräten und mobilen Datenträgern ist einzuführen. Netzwerk- und Infrastrukturkomponenten sind vor unautorisierten Zugang zu schützen. Maßnahmen zum Schutz gegen einfaches Mithören und Einsichtnahme sind umzusetzen. Nachweis(e): - Sicherheitszonenkonzept inkl. Beschreibung der zugehörigen Schutzmaßnahmen je Zone - Fotodokumentation der Schutzmaßnahmen - Darstellung der Schutzmaßnahmen gegen einfaches Mithören und Einsichtnahme Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

3.1.2 Inwieweit ist in Ausnahmesituationen die Informationssicherheit sichergestellt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Notfallhandbuch,
- Backup-Konzept,
- Nachweise Brandschutzübung,
- Behandlung von Datenschutz- und IT-Sicherheit relevanten Störungen,
- Nachweise Security Exercises,
- X-VA-63-10000000658_Notfallmanagement.pdf – Verfahrensanweisung - IMS
- RANCID
- Service Request SCTAK0011089

Statement Hydac:

"Zentralbereich Informatik:

Die Anforderungen zur Weiterführung der Informationssicherheit ist für den Krisenfall identifiziert und beschrieben. In einem Notfallhandbuch sind mehrere Szenarien beschrieben, die für potentielle Krisenfälle das weitere Vorgehen beschreiben und als Hilfestellung dienen. Regelmäßige Notfallübungen werden in Planspielen im IT-Sicherheitsteam durchgeführt.

Allgemein:
Zentrale Konzepte für Ausnahmesituationen und BCM werden vom Zentralbereich ZQW erstellt."

Potenziell betroffene IT-Systeme und Software sind identifiziert.

Die Informationssicherheit wird im BCM (Business Continuity Management) bzw. im Desaster Recovery Prozess berücksichtigt.

Ein Krisenstab ist eingeführt und die Verantwortlichen für Informationssicherheit sind in den Krisenstab integriert. Notfallübungen werden durchgeführt.

Backupkonzepte sind vorhanden. Ein redundanter Serverraum für die Produktivsysteme ist vorhanden. Backups werden in separaten Brandabschnitten gesichert.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

3.1.3 Inwieweit ist der Umgang mit Informationsträgern gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- X-VA-76-1000012648-IT-Sicherheitsrichtlinie,
- Sicherheitsstrategie mobile Datenträger,
- Klassifizierung von Dokumenten,
- Verschrotten von IT-Equipment,
- Nachweise Documentus / Reisswolf,
- DIN-66399-Zertifikat-bis-2023-V3.pdf

Statement Hydac:

"Die Verwendung und der Umgang mit Betriebsmitteln ist in verschiedenen Richtlinien geregelt. Der allgemeine Umgang ist in der IT-Sicherheitsrichtlinie beschrieben. Der Umgang mit Dokumenten und Daten ist in der Klassifizierungsrichtlinie geregelt und ist ergänzend zu der Sicherheitsstrategie für mobile Datenträger. Aktenvernichter einer niedrigeren Schutzklasse als P4 sind im internen Bestellsystem (HeP) nicht auswählbar. Mit dem Dienstleister zur sicheren Daten- /Datenträgervernichtung Documentus, der die Datentonnen verarbeitet, besteht ein Rahmen- und Geheimhaltungsvertrag."

In den Richtlinien und den Verfahrensanweisungen für den Gebrauch und der Mitnahme von Assets sind die Sicherheitsanforderungen definiert und in der Praxis umgesetzt. Dazu zählen:

- IT-Geräte mit sensiblen Daten werden so gelöscht, dass die Daten nicht wiederhergestellt werden können.
- Es sind Shredder der Sicherheitsstufe P-4 vorhanden.
- Es sind Datentonnen vorhanden und werden durch den Dienstleister Reisswolf entsorgt.
- Die Entsorgung von Datenträgern durch den Dienstleister Reisswolf erfolgt gemäß eines der gängigen Standards (z.B. DIN 66399 Sicherheitsstufe 4).

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

3.1.4 Inwieweit ist der Umgang mit mobilen IT-Geräten und mobilen Datenträgern gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- X-VA-76-10000012648-IT-Sicherheitsrichtlinie,
- Sicherheitsrichtlinie Endgeräteschutz,
- Sicherheitsstrategie mobile Datenträger,
- Übergabeprotokoll Smartphone
- McAffee Endpoint Security
- McAffee Endpoint Encryption
- MDM Mobile IRON

Statement Hydac:

"Die Anforderungen mit dem Umgang von mobilen Endgeräten sind in mehreren Richtlinien und Dokumenten beschrieben und dokumentiert. Eine Verpflichtungserklärung wird bei Übergabe des mobilen Endgerätes unterschrieben. "

Die Anforderungen bzgl. Verschlüsselung, Zugriffsschutz, Registrierung, Datensicherung für mobile Datenträger sind ermittelt und dokumentiert.

Festplattenverschlüsselung mittels McAffee ist auf allen Clients aktiviert.

Mobiltelefone/Tablets werden durch ein MDM zentral verwaltet.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

4 Identity and Access Management

4.1 Identity Management

4.1.1 Inwieweit ist der Umgang mit Identifikationsmitteln gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- X-VA-73-10000216051 Unternehmenssicherheit-Zugangsmanagement-Beschäftigte,
- Onboarding BEST PRACTICE Checkliste,
- Offboarding Laufzettel, Schlüssellisten
- 5768_Oazimi_Malsore.pdf
- BV_Schliessanlage.pdf

Statement Hydac:
"Erstellung, Übergabe, Rückgabe, Gültigkeitszeiträume sowie Umgang mit Verlust werden in Protokollen festgehalten. "

Die Zuweisung von Identifikationsmitteln erfolgt gemäß definierter Eintritts-/Wechsel-/Austrittsworkflows bzw. Prozessen nach dem 4-Augenprinzip.
Die Ausgabe und Rückgabe von Identifikationsmitteln unterliegt einem geordneten Verfahren und wird protokolliert.
Der Prozess zur Vergabe und Entzug von Identifikationsmitteln wurde während des Audits vorgestellt.
Der Umgang bei Verlust von Identifikationsmitteln ist beschrieben.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

4.1.2 Inwieweit wird der Zugang von Benutzern zu Netzwerkdiensten, IT-Systemen und IT-Anwendungen gesichert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Sicherheitsrichtlinie Vergabe von IT-Berechtigungen,
- Sicherheitsrichtlinie kryptographische Verfahren,
- Screenshot Onlineformular, Screenshot Service Request
- Ticket SCTASK0027696
- Service Now Konsole

Statement Hydac:

"Für jeden Mitarbeiter gibt es ein AD-Konto mit entsprechendem Benutzernamen. Dieser ist eindeutig und kann somit einem einzelnen User zugewiesen werden. Der Umfang der Berechtigungen des jeweiligen Users wird durch eine interne Richtlinie geregelt. Ausnahme bilden Sammelkennungen, welche für den Schichtbetrieb in der Produktion genutzt werden. Benutzer in der Produktion haben keinen Zugang zum Internet. Berechtigungen werden über Intranetformular bzw. ServiceNow nach dem Minimalprinzip beantragt. "

Die eingesetzten Verfahren zur Benutzerauthentifizierung entsprechen dem aktuellen Stand der Technik.

Benutzer werden vor dem Zugriff auf Daten mit hohem Schutzbedarf mindestens durch starke Passwörter nach Stand der Technik authentifiziert.

Feststellung

Es konnte nicht nachgewiesen werden, dass höherwertige Verfahren zur Authentifizierung von privilegierten Benutzerkonten verwendet werden (z. B. Privileged Access Management, 2-Faktor-Authentifizierung).

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Anforderungen für die Benutzerauthentifizierung sind in einer Richtlinie zu beschreiben. Die möglichen Angriffsszenarien sind zu berücksichtigen und einer Risiko-Bewertung zu unterziehen (z. B. direkte Zugriffsmöglichkeit aus dem Internet). Maßnahmen aus der Risikobewertung sind umzusetzen (z. B. dauerhaftes Monitoring der Zugriffe auf Unregelmäßigkeiten oder Einsatz einer starken Authentifizierung). Es sind starke Passwörter einzusetzen. Es sind höherwertige Verfahren zur Authentifizierung von privilegierten Benutzerkonten zu verwenden Nachweis(e): - Richtlinie inkl. Beschreibung der Authentifizierungsverfahren - Nachweis über Passwort-Stärke (Screenshot Domain-GPO) - Nachweise für starke Authentifizierung (techn. Beschreibung und Screenshots) Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

4.1.3 Inwieweit werden Benutzerkonten und Anmeldeinformationen sicher verwaltet und angewandt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Sicherheitsrichtlinie Vergabe von IT-Berechtigungen,
- Screenshots Formulare,
- Nachweise Service Request Benutzeranlage,
- Sicherheitsrichtlinie Passwortsicherheit,
- Screenshots GPO

Statement Hydac:

"Für die Benutzerregestierung exisitert ein Prozess, der durch ein Onlineformular im Intranet gestartet wird. Daraufhin wird der besagte Prozess abgearbeitet. Das Intranet-formular wird auch für den Offboarding-Prozess verwendet. Externe Accounts laufen ab, erhalten einen Ansprechpartner der Firma und einen internen. Ein Passwortmanager ist etabliert."

Die Anlage, Änderung und Löschung (Life-Cycle) von Benutzerkonten ist definiert.

Rechte werden durch den zuständigen Abteilungsleiter beantragt.

Es werden eindeutige und personalisierte Benutzerkonten verwendet.

Initiale Anmeldeinformationen müssen nach dem 1. Login geändert werden.

Feststellung

Es konnte nicht nachgewiesen werden, dass die Anmeldeinformationen (z. B. Passwörter) eines personalisierten Benutzerkontos nur dem zugeordneten Benutzer bekannt sind.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Für alle Informationssysteme und Dienste ist eine formale Benutzerregistrierung zur Vergabe und Rücknahme von Zugangs- und Zugriffsberechtigungen einzuführen. Die Einrichtung von Benutzerkonten unterliegt einem Genehmigungsprozess (4-Augen-Grundsatz). Die Anträge zur Rechtevergabe sind zu archivieren. Anmeldeinformationen (Benutzername und Passwort / PIN) sind dem Benutzer so zuzustellen, dass die Kenntnisnahme Unbefugter ausgeschlossen ist. Initialpasswörter sind nach der Erstanmeldung zu ändern. Der Prozess ist in einer Richtlinie zu beschreiben. Nachweis(e): - Prozessbeschreibung für Vergabe und Entzug von Benutzerrechten je Dienst bzw. Anwendung - Beispiel Umgang mit neuen Anmeldeinformationen für einen Benutzer Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

4.2 Access Management

4.2.1 Inwieweit werden Zugriffsberechtigungen vergeben und gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Sicherheitsrichtlinie Vergabe von IT-Berechtigungen,
- Screenshots Formulare,
- Nachweise Service Request Benutzeranlage
- Ticket SCTASK0029326

Statement Hydac:

"Die Vergabe bzw. Änderung von Berechtigungen werden durch einen Prozess gesteuert. Berechtigungen im SAP-Umfeld werden künftig durch ein konzipiertes Rollenkonzept bearbeitet und verteilt. "

Die Anforderungen an das Management von Zugriffsberechtigungen sind ermittelt und erfüllt.

Gemäß Regelwerk findet eine regelmäßige Überprüfung der gewährten Zugriffsberechtigungen von normalen und privilegierten Benutzerkonten sowie technischen Konten statt, auch in IT-Systemen von Kunden. Es werden Berechtigungs-Rollen verwendet.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5 IT Security / Cyber Security

5.1 Cryptography

5.1.1 Inwieweit wird die Nutzung kryptografischer Verfahren gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Sicherheitsrichtlinie kryptographische Verfahren,
- Sicherheitsrichtlinie Klassifizierung von Dokumenten und Informationen,
- Schulungsunterlage Arbeiten mit verschlüsselten Daten,
- Schulungsunterlagen USB Verschlüsselung

Statement Hydac:

"Es existiert ein Dokument zur Regelung für Einsatz von Verschlüsselungstechnologien, in diesem sind neben den einzusetzenden Verfahren auch Erläuterungen zu diesen Verfahren beschrieben."

Ein eingesetztes kryptographischen Verfahren bietet nach dem Stand der Technik die notwendige Sicherheit für das Einsatzgebiet.

Rechtliche Rahmenbedingungen für den Einsatz von Kryptographie sind berücksichtigt.

Ein Nutzungskonzept für Kryptographie ist definiert und umgesetzt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.1.2 Inwieweit werden Informationen während der Übertragung geschützt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

• Sicherheitsrichtlinie kryptographische Verfahren,

• Sicherheitsstandards kryptographische Verfahren,

• Sicherheitsrichtlinie Klassifizierung von Dokumenten und Informationen

Statement Hydac:

"Der Austausch von Informationen erfolgt stets gesichert. Dafür geeignete Verfahren sind in dem Kryptokonzept beschrieben. Zudem sind Informationen nach der internen Richtlinie zu klassifizieren. Diese stellt ebenfalls Anforderungen an die Art der Sicherung.

HYDAC Accessories:
Der Datenaustausch mit VW läuft über das VW Business Portal."

Der Schwerpunkt zum Datenaustausch erfolgt über Kundensysteme. Daher erfolgt der elektronische Datenaustausch abhängig von der Klassifizierung durch Inhalts- und oder Transportverschlüsselung. Informationen ab hohem Schutzbedarf sollten ausschließlich verschlüsselt übertragen werden.

Feststellung

Es konnte nicht nachgewiesen werden, dass alle verwendeten Netzwerkdienste zur Übertragung von Informationen identifiziert und dokumentiert sind.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Netzwerkdienste zur Übertragung von Informationen sind vollständig zu dokumentieren. Ein Regelwerk mit Vorgaben zur Nutzung der Netzwerkdienste auf Basis der Klassifizierung von Informationen ist zu definieren und umzusetzen. Maßnahmen sind umzusetzen für: - Schutz vor unberechtigtem Zugriff - Sicherstellung der korrekten Adressen - Sicherstellung korrekten Transports - Verschlüsselung in Abhängigkeit der Klassifizierung (hoher Schutzbedarf) Nachweis(e): - Liste der genutzten Netzwerkdienste - Regelung zur Nutzung von Netzwerkdiensten - Technische Beschreibung und Screenshots der eingesetzten Maßnahmen Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

5.2 Operations Security

5.2.1 Inwieweit werden Änderungen gesteuert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Change Management Prozess,
- Patch Management Prozess,
- Softwarepaketierung Prozess,
- Änderungsabläufe,
- Screenshot Unterschriften Freigabeprozess VA
- ServiceNow CHG0030871 – Normal Change

Statement Hydac:

"Änderungen an eingesetzter Software werden durch Client Management und IT-Sicherheit geprüft und freigegeben. Anschließen werden diese über ein genutztes Software-verteilungssystem verteilt. Patchstände werden im Patchmanagement dokumentiert. Änderungen durch Projekte werden in Control Punkt 1.2.3 beschrieben.

organisatorisches Änderungsmanagement (ZQW):

Es gibt die X-VA Änderungsabläufe produktorientiert

Änderungen allgemein: Es gibt grundsätzlich unsere Vorgabedokumente, z.B. X-VA, X-FBL oder IMS-HBU bzw. bereichsspezifische Vorgabedokumente in denen alle relevanten Abläufe aktuell beschrieben sind. Ist eine Änderung geplant, muss geprüft werden, ob die Änderung okay ist und auch die Vorgabedokumente müssen angepasst werden. In den Änderungsprozess, z.B. bereichsübergreifende Prozesse des IMS, sind verschiedene Mitarbeiter/Abteilungen und die Geschäftsleitung involviert

- Unterschriftsprozess, z.B. X-VA: Ersteller, Prüfer, QM-Freigabe, GL-Freigabe"

Changes werden über ServiceNow eingesteuert sowie verwaltet.

Regelmäßig tagt für das Change-Management eine Gremienrunde (Change Advisory Board).

Danach erfolgt die Genehmigung/Ablehnung für einen Change.

ServiceNow dokumentiert den Fortgang des Change.

Der Prozess wurde innerhalb des Audits präsentiert.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.2.2 Inwieweit sind die Entwicklungs- und Testumgebungen von den Produktivumgebungen getrennt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

• Sicherheitsrichtlinie Entwicklung und DevOps

Statement Hydac:

"Im SAP und Service Now Umfeld ist eine strikte Trennung umgesetzt. Für jedes Produktivsystem gibt es ein zugehöriges Test- und Entwicklungssystem. Zusätzlich wird ein Testnetz für allgemeine Tests bereitgestellt.

Der jeweilige Solutionowner ist für den Betrieb der entsprechenden Systeme und deren Kritikalität verantwortlich. Basis ist hierbei Trennung Entwicklungs- und Testumgebungen von den Produktivumgebungen."

Auf Basis einer entsprechenden Bewertung erfolgt für die Systeme eine Trennung zwischen Entwicklungs-, Test- und Produktivumgebung.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.2.3 Inwieweit werden IT-Systeme vor Schadsoftware geschützt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- X-VA-76-1000012648-IT-Sicherheitsrichtlinie,
- Sicherheitsrichtlinie Endgeräteschutz,
- Sicherheitsstandards Endgeräteschutz,
- Patchmanagement Prozess

Statement Hydac:

"In der Richtlinie wird sowohl auf die Gefahr von Schadsoftware sowie auf mögliche Schutzmaßnahmen hingewiesen. Für den Schutz von Schadsoftware gibt es eine Dokumentation über Sicherheitsmaßnahmen für Endgeräte. Des Weiteren enthält das Dokument eine Matrix die aufzeigt, welche (Schutz-)Software auf den verschiedenen Endgeräten installiert sein muss. "

Ein umfangreiches Konzept zum Schutz vor Schadsoftware ist implementiert.

Anforderungen an den Schutz vor Schadsoftware sind ermittelt.

Technische und organisatorische Maßnahmen zum Schutz vor Schadsoftware sind definiert und umgesetzt.

Eine Software zum Schutz vor Schadsoftware ist installiert und wird regelmäßig automatisch aktualisiert.

Eine automatische Überprüfung auf Schadsoftware erfolgt von empfangenen Dateien und Programmen vor deren Ausführung.

Eine regelmäßige Untersuchung des gesamten Datenbestandes aller Systeme auf Schadsoftware wird durchgeführt.

Maßnahmen zur Sicherstellung, dass Schutzsoftware nicht durch Benutzer deaktiviert oder verändert werden kann, sind definiert und umgesetzt.

Es werden nur IT-Systeme mit Software zum Schutz vor Schadsoftware betrieben.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.2.4 Inwieweit werden Ereignisprotokolle aufgezeichnet und analysiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Sicherheitsrichtlinie Systemüberwachung,
- Screenshot Knowledge Base Eintrag Service Now für Use Case,
- Screenshot Incident,
- Screenshot ELK
- SIEM Management Konsole

Statement Hydac:

"Die Auswertung und Ansammlung von Logs wird in der Sicherheitsrichtlinie Sicherheitsprotokollierung und Monitoring geregelt. Des Weiteren ist ein eigener Logserver in Betrieb, der Logs von verschiedenen Systemen verarbeiten und bei potentiellen Verdachtsmomenten die Auswertung vereinfachen kann. Für verdächtige Aktivitäten sind entsprechende Use Cases definiert, die im Service Now bearbeitet werden. "

Fortinet Firewalls werden über den Fortinet Manager verwaltet und geloggt.

Auf Basis von Events werden Tickets eröffnet und durch die Sicherheitsorganisation bearbeitet.

Logdateien und Ereignisprotokolle werden regelmäßig sowie fallbezogen analysiert und ausgewertet.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.2.5 Inwieweit werden Schwachstellen erkannt und behandelt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Patch Management Prozess,
- Sicherheitsrichtlinie Endgeräteschutz,
- Infoserve Scanreport,
- BPMN Prozess für Sicherheitslücken,
- Screenshot Problem Sicherheitslücke Service Now
- Matrix42
- WSUS

Statement Hydac:

"Software-Patches werden anhand eines konzipierten und etablierten Patch Management umgesetzt. Dabei werden Patches vor dem Verteilen, geprüft und getestet. Schwachstellen in der eingesetzten Software werden durch die CVE von Mitre, der National Vulnerability Database und durch Pulse Dive gesucht und über den CVE-Score bewertet."

Informationen über technische Schwachstellen werden gesammelt und bewertet.

Ein angemessenes Patch-Management ist definiert und umgesetzt.

Es wird überwiegend die automatische Update-Funktion eingesetzt. Windows-Server-Updates werden per WSUS verteilt.

Client Updates und Drittsoftware-Patches werden über die zentrale Softwareverteilung Matrix42 ausgerollt.

Scans werden regelmäßig durchgeführt. Die Systeme werden entsprechend überwacht und bei Auffälligkeiten wird eingegriffen.

Risikominimierende Maßnahmen sind im Regelwerk definiert. Die Installation von Patches wird im Rahmen der regelmäßigen Prüfungen kontrolliert.

Feststellung

Es konnte nicht nachgewiesen werden, dass technische Schwachstellen (HyDac-Training - 212.X88.XXX.XXX) bewertet werden.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Informationen über neue Schwachstellen sind regelmäßig einzuholen. Patches für Betriebssysteme und Standard-Software sind schnellstmöglich zu installieren. Die erfolgreiche Patchinstallation ist mit geeigneten Verfahren zu überprüfen (Auswertung von Reports oder Schwachstellenscans). Nachweis(e): - Schwachstellen-Report (Quellenangabe) - Technische Beschreibung der Update-Verfahren und ggf. Ersatzmaßnahmen Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

5.2.6 Inwieweit werden IT-Systeme technisch überprüft (Systemaudit)?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Sicherheitsrichtlinie Auditanforderungen,
- Nachweis Monitoring,
- Infoserve Scanreport,
- Pentest-Report,
- Permission to attack von Sec Consult,
- Problem Sicherheitslücke Scan Report

Statement Hydac:

"Die Anforderungen an ein Audit sind erfasst und entsprechend intern dokumentiert. Zudem werden anlassbezogene Pentests durchgeführt um mögliche Schwachstellen frühzeitig zu finden und um die umgesetzten Sicherheitsmaßnahmen zu prüfen. Kritische Systeme werden über Monitoringsysteme überwacht.

Externe IP-Adressen werden monatlich durch einen externen Dienstleister gescannt und ein Report zur Verfügung gestellt. "

Es werden regelmäßig (jährlich) entsprechend Penetrationstests durch ein externes Unternehmen vorgenommen.

Auf Basis der Reports findet eine protokollierte Maßnahmenverfolgung der Findings statt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.2.7 Inwieweit wird das Netzwerk der Organisation gemanagt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- IT-Sicherheitsrichtlinie,
- Netzwerkmanagement & -strukturierung,
- Screenshot Projekt AB Migration,
- IT Standards

Statement Hydac:

"Der Umgang und die Nutzung des Netzwerkes ist in der Verfahrensanweisung IT-Sicherheitsrichtlinie geregelt und für jeden Mitarbeiter verpflichtend. Zudem gibt es ein Netzwerksegmentierungskonzept, das die Verwaltung des Netzwerkes regelt."

Feststellung

Es konnte nicht nachgewiesen werden, dass Anforderungen an die Steuerung und Verwaltung von Netzwerken ermittelt und umgesetzt sind.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): Anforderungen an die Steuerung und Verwaltung sind ausgehend von den Sicherheitsanforderungen zu definieren und in der Arbeitsanweisung zu dokumentieren, dazu gehören: - Verfahren zur Verwaltung und Steuerung der Netzwerke - Authentifizierung von Systemen im Netzwerk - Der Zugriff auf die Managementschnittstellen von IT-Systemen ist eingeschränkt Anforderungen an die Segmentierung von Netzwerken sind ausgehend von den Sicherheitsanforderungen zu definieren, dazu gehören: - Beschränkungen bei der Anbindung von IT-Systemen an das Netzwerk - Einsatz von Sicherheitstechnologien - Das erhöhte Risiko durch aus dem Internet erreichbare Netzwerkdienste (z.B. Nutzung von DMZ-Netzwerken) - Technologie-spezifische Trennungsmöglichkeiten (z. B. durch eine Firewall) bei Nutzung von organisationsfremden IT-Diensten - Geeignete Trennung von eigenen Netzwerken und Kundennetzwerken unter Berücksichtigung von Kundenanforderungen Nachweis(e): - Liste der Anforderungen an die Steuerung und Verwaltung, ermittelt aus den Sicherheitsanforderungen - Liste der Anforderungen an die Segmentierung der Netzwerke, ermittelt aus den Sicherheitsanforderungen - Umsetzungsnachweis der sicherheitsrelevanten Verfahren zur Steuerung und Verwaltung der Netzwerke (technische Beschreibung, Screenshots der laufenden Systeme) - Liste der eingesetzten Verfahren zur Verwaltung und Steuerung der Netzwerke - Screenshots der Netzwerksegmentierung - Technische / organisatorische Maßnahmen, um den Zugriff auf die von Managementschnittstellen von IT-Systemen einzuschränken Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

5.3. System acquisitions, requirement management and development

5.3.1 Inwieweit wird Informationssicherheit bei neuen oder weiterentwickelten IT-Systemen berücksichtigt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- IT Standards, Formblatt Standard Notebook,
- Generelle IT Mindestanforderungen im Umfeld der HYDAC Produktion,
- Demand Prozess,
- Change Management Prozess,
- Nachweise Abnahme VXrail ELK
- SCTAK0027889

Statement Hydac:

"Es dürfen nur Standard-PCs und Standard-IPCs beschafft werden. Der Standard ist in einem jeweiligen Dokument beschrieben. Modifikationen dürfen nur nach Absprache mit der IT getroffen werden. Weitere Anforderungen werden in entsprechenden Wartungsverträgen festgehalten und beschrieben. "

Die Anforderungen an die Informationssicherheit bei der Planung von IT-Systemen sind definiert.

Die Anforderungen an die Informationssicherheit bei der Beschaffung von IT-Systemen und IT-Komponenten werden berücksichtigt.

Neue Systeme werden zentral beschafft und durch die Informationssicherheitsorganisation bewertet.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.3.2 Inwieweit sind Anforderungen an Netzwerkdienste definiert?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- SLA_Connect_DE_V3.02_CI,
- PD_Connect Ethernet-DE_V3.01_CI,
- Netzwerkmanagement & -strukturierung
- Cacti Konsole
- Icinga Konsole

Statement Hydac:

"Die Anforderungen an die Informationssicherheit sind ermittelt und umgesetzt. Zudem gibt es redundante Rechenzentren, die eine Ausfallsicherung gewähren. "

Verfahren zur Absicherung, Nutzung und Überwachung von Netzwerkdiensten sind vertraglich vereinbart und die Leistungsumfänge mittels SLAs beschrieben."

Verschiedene Leistungsbeschreibungen der genutzten IT-Services wurden präsentiert.

Die Überwachung des Netzwerkverkehrs erfolgt über Icinga und Cacti.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.3.3 Inwieweit ist die Rückgabe und das sichere Entfernen von Informationswerten aus Organisationsfremden IT-Diensten geregelt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- IT-Sicherheitsrichtlinie,
- Cloud-Sicherheitsrichtlinie,
- IT-SRL externe Dienstleister,
- Servicevereinbarung Cloud-Dienst,
- Vorlage Servicevereinbarungen für Cloud-Dienste

Statement Hydac:

"Nach Möglichkeit wird auf externe Cloud-Dienste verzichtet. Des Weiteren gelten die etablierte IT-Sicherheitsrichtlinie, IT-Sicherheitsrichtlinie für externe Dienstleister sowie die Cloud-Sicherheitsrichtlinie. "

Bei der Vertragsgestaltung ist eine Rückgabe und sichere Entfernung von Informationswerten aus organisationsfremden IT-Diensten obligatorischer Bestandteil der extern vergebenen Leistung.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

5.3.4 Inwieweit sind Informationen in gemeinsam genutzten organisationsfremden IT-Diensten geschützt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- IT-Sicherheitsrichtlinie,
- Cloud-Sicherheitsrichtlinie,
- IT-SRL externe Dienstleister,
- Servicevereinbarung Cloud-Dienst,
- Vorlage Servicevereinbarungen für Cloud-Dienste

Statement Hydac:

"Nach Möglichkeit wird auf externe Cloud-Dienste verzichtet. Des Weiteren gelten die etablierte IT-Sicherheitsrichtlinie, IT-Sicherheitsrichtlinie für externe Dienstleister sowie die Cloud-Sicherheitsrichtlinie. "

Vor Selektierung eines Clouddienstes wird das Vorhandsein einer Mandantentrennung überprüft.

Es werden nur Dienstleister eingesetzt, welche ein entsprechendes Trennungskonzept besitzen.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

6 Supplier Relationships

6.1.1 Inwieweit wird die Informationssicherheit bei Auftragnehmern und Kooperationspartnern sichergestellt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- IT-Sicherheitsrichtlinie,
- IT-SRL externe Dienstleister,
- Lieferantenselbstauskunft,
- Checkliste Bewertung potentieller Lieferant,
- SAP Ariba Fragenliste

Statement Hydac:

"Potenzielle Lieferanten müssen vorab eine Lieferantenselbstauskunft einreichen, die durch die Fachabteilungen geprüft wird. Bei erfolgreicher Überprüfung gelten die vertraglichen Bestimmungen einschließlich der IT-Sicherheitsrichtlinie für externe Dienstleister und der Kenntnisnahme der IT-Sicherheitsrichtlinie.

Zukünftig sollen Lieferanten über SAP Ariba verwaltet werden. Innerhalb Ariba muss das IT-Sicherheitsteam den Lieferanten anhand von Antworten spezifischer Fragebögen bewerten und freigeben."

Feststellung

Es konnte nicht nachgewiesen werden, dass Auftragnehmer und Kooperationspartner einer Risikobewertung bzgl. der Informationssicherheit unterzogen werden.

☐ Hauptabweichung ☒ Nebenabweichung ☐ Beobachtung ☐ Identifiziertes Verbesserungspotential

Geplante Maßnahmen (incl. Umsetzungszeitraum)
Das geprüfte Unternehmen hat die Umsetzung der folgenden mitigierenden Maßnahmen geplant (dauerhaft): In den Lieferantenprozess ist aufzunehmen: Auftragnehmer und Kooperationspartner müssen einer Risikobewertung bzgl. der Informationssicherheit unterzogen werden. Lieferanten sind hinsichtlich Informationssicherheit zu klassifizieren und entsprechende Maßnahmen sind zu definieren (z.B. Self Assessment, Lieferanten-Audit). Die identifizierten Anforderungen an die Informationssicherheit sind vertraglich mit den Auftragnehmern zu vereinbaren. Die Auftragnehmer sind zu verpflichten, dass die Anforderungen an deren Unterauftragnehmer weiterzugeben sind. Eine Überprüfung der Informationssicherheit ist für Lieferanten durchzuführen. Ein Nachweis für ein dem Schutzbedarf der Informationen angemessenes Level der Informationssicherheit (z. B. Zertifikat, Testat, eigene Auditierung) ist einzuholen. Nachweise: - SAP Ariba Lieferanten Übersicht - Prozess-Beschreibung Lieferanten-Management - Risikobewertung Lieferanten - Bericht Lieferanten-Audit Die Umsetzung wird gemäß Planung spätestens am 15.06.2023 abgeschlossen sein.
Bewertung nach Follow-Up

6.1.2 Inwieweit ist Geheimhaltung beim Austausch von Informationen vertraglich vereinbart?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- IT-SRL externe Dienstleister,
- X-VA-Behandlung von Kundenanfragen und Angebotserstellung,
- X-VA-Vertragsprüfung und Auftragsabwicklung,
- X-FBL-Checkliste für Kundenaufträge,
- X-FBL-Checkliste für Angebote,
- X-FBL-Laufkarte Kundenanfrage und Kundenauftrag,
- X-VA-Rechtskonformität,
- Schulungsunterlage „Sensibilisierung Preisgabe vertraulicher Informationen“,
- Geheimhaltungsverträge
- NDA Template

Statement Hydac:

"Der jeweilige Bereich ist für die vertragliche Einhaltung verantwortlich.

Lieferantenseitig ist dies der Einkauf und in der Verfahrenansweisung Lieferantenmanagement beschrieben. Wenn vom Kunden eine Geheimhaltungsvereinbarung gefordert wird, dann arbeitet der Vertrieb mit der Rechtsabteilung zusammen.

Vorlagen zu Geheimhaltungsverträgen liegen im Intranet bereit."

NDAs werden als Vorlagendokument zentral durch die Abteilung Legal verfasst und der Abteilung Einkauf bereitgestellt.

Durch die Abteilung Legal findet eine stetige Vertragsprüfung und ggf. Anpassung des Vorlagendokuments (z. B. aufgrund geänderter gesetzlicher Lage oder innerbetrieblicher Anforderungen) statt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

7 Compliance

7.1.1 Inwieweit wird die Einhaltung regulatorischer und vertraglicher Bestimmungen sichergestellt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- P1-Anwendungsbereich-Scope-ISMS,
- P2-Organisation-Verantwortlichkeiten-ISMS,
- ISO Nachweise,
- Rechtskonformität,
- E-Mailverlauf Zentralbereiche
- Rechtskataster Umwelt Online inkl. IS & DS
- Sensibilisierung über Preisgabe von vertraulichen Informationen / Geschäftsgeheimnissen

Statement Hydac:

"Die gesetzlichen Bestimmungen für die Informationssicherheit und für das ISMS sind erfasst und dokumentiert. Zentralabteilungen für Datenschutz, Recht und Qualitätswesen sind umgesetzt."

Interne Vorgaben und Gesetze werden regelmäßig überprüft.

Sensibilisierungsmaßnahmen zu Compliance-Themen der Informationssicherheit für Mitarbeiter werden regelmäßig durchgeführt.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.

7.1.2 Inwieweit wird der Schutz von personenbezogenen Daten bei der Umsetzung der Informationssicherheit berücksichtigt?

Detaillierte Sachverhaltsdarstellung (inkl. Beurteilungsverfahren)

Betrachtete Dokumente/Nachweise/Prüfungshandlung:

- Interne Mitteilung 02/2019: DS Erklärung ISMS,
- Change und Demand Prozess,
- Gesprächsprotokoll Datenaustausch ISMS und DS,
- Datenschutzhandbuch
- Zertifikat IAPP CIPPE.pdf
- Datenschutzauditor.pdf
- Datenschutz Schulungskonzept
- NEUTRAL Datenschutzeinführung Mitarbeiter_DSGVO neues Design.pptx
- DSMS – otis privacy
- Meldeformular Datenschutzbeauftragte_unabhängiges Datenschutzzentrum_Saarland.pdf
- Benennung zum gemeinsamen Datenschutzbeauftragten.pdf
- Bestellung H Verwaltung HV.pdf
- Bestellung HAC.pdf

Statement Hydac:

"Die Anforderungen an den Datenschutz sind mit Absprache des Fachbereich Datenschutz erfasst und werden in einem separaten Datenschutzmanagementsystem verwaltet. Genauere Informationen sind dem Datenschutzhandbuch zu entnehmen, dass der Datenschutz zur Verfügung stellt.

Zusätzlich findet ein regelmäßiger Informationsaustausch mit dem Zentralbereich Datenschutz statt."

Herr Nils Ulrich ist seit 2015 als Datenschutzbeauftragter bestellt. Eine Bestellurkunde wurde präsentiert und eingesehen.

Ein Verfahrensverzeichnis gem. Art. 30, Abs. 1 DSGVO wird vom DSB geführt und gepflegt. Der Abschluss von AV-Verträgen ist obligatorisch.

Feststellung

Auf Basis der Beobachtungen wurde keine Abweichung festgestellt.