Kilchenmann AG – Massnahmen zur Informationssicherheit

Inhaltsverzeichnis

1. Rechtliche Bestimmungen

Der Datenumgang bei der Kilchenmann AG richtet sich nach den rechtlichen Vorgaben. Seit dem 01.09.2023 nach dem nDSG.

Ergänzend zu den bestehenden Massnahmen, wurde ein Verarbeitungsverzeichnis eingeführt, die Prozesse überarbeitet und die Mitarbeiter geschult.

2. Verpflichtung der Mitarbeiter auf das Datengeheimnis

Die Mitarbeiter der Kilchenmann AG unterliegen vertraglichen geregelten Geheimhaltungsvereinbarungen und werden regelmässig zu Sicherheits-, Notfall- und Geheimhaltungsthemen geschult.

3. Technische und Organisatorische Massnahmen

3.1. Technische Massnahmen

3.1.1. Rechenzentrumssicherheit

Die Kilchenmann AG betreibt am Hauptsitz in Kehrsatz-Bern zwei Rechenzentrumsräume.

Der Zutritt in den Rechenzentrumsraum ist nur autorisierten Personen gestattet und mittels Überwachungsanlage geschützt. Der Zutritt zum Gebäude ist mittels Alarmsystem und Sicherheitsdienst 24/7 überwacht.

Die Unterbrechungsfreie Stromversorgung wird mittels USV-Anlage (kurzfristig) und Notstromaggregat (mittelfristig) sichergestellt und in monatlichen Abständen getestet.

3.1.2. Patch-Management

Sämtliche Komponenten der IT Infrastruktur werden im monatlichen Wartungsfenster mit sicherheitsrelevanten Aktualisierungen versorgt. Kritische Sicherheitslücken werden unmittelbar nach Bekanntwerden geschlossen.

3.1.3. Netzwerksicherheit

Die Kilchenmann AG betreibt eine redundante Firewall-Infrastruktur mit Zonenkonzept zur Sicherung der einzelnen Standorte. Der Zugriff durch Partner erfolgt mittels gesicherter VPN Verbindung. Datenübertragungen erfolgen über VPN Verbindungen oder verschlüsselte TLS/SSL Verbindungen zur manipulationsfreien Kommunikation.

Darüber hinaus sind Schutzkonzepte implementiert zur Angriffserkennung und Verhinderung, unautorisierten Datentransfers und Protokollierung der Sicherheitsereignisse.

3.1.4. Datensicherung

Die Datensicherung wird durch ein Backup & Recovery Konzept sichergestellt. Das Konzept legt die Intervalle und Aufbewahrungsfristen für die verschieden Datentypen in Abhängigkeit ihrer Sensibilität fest. Die Backupinfrastruktur und Datensicherung unterliegen einer ständigen Überwachung. Kritische Daten werden an einem sicheren Ort gegen zufällige Zerstörung oder Verlust aufbewahrt.

3.1.5. Viren- und Spamschutz

Kilchenmann setzt zur Vermeidung von Funktionsstörungen und Missbräuchen seiner Informatikmittel primär technische Schutzmassnahmen (z.B. Antivirenprogramme, Filter gegen Spamming, Spyware oder unerwünschte Websites) ein.

3.2. Organisatorische Massnahmen

3.2.1. Personal

Alle Mitarbeiter der Kilchenmann AG unterliegen vertraglich geregelten Geheimhaltungspflichten. Der Umgang mit Informationen/Daten wird regelhaft geschult, wodurch eine hohe Sensibilisierung zur Nutzung der Kommunikationsmittel besteht. Zusätzlich ist die Teilnahme am kontinuierlichem Cyber-Security Awareness Training verpflichtend. Für die jeden Mitarbeitenden mit administrativen Rechten besteht eine gesonderte Administratorenvereinbarungen.

3.2.2. Authentisierung

Der Zugriff auf die Arbeitsplatzrechner sowie der einzelnen Applikationen erfolgt ausschliesslich mittels persönlichem Benutzernamen und Kennwort. Dies ermöglicht mittels Protokollierung die Nachvollziehbarkeit bei Zugriff und Änderungen der Daten. Zur Absicherung der Online-Ressourcen und der Einwahl mittels VPN wird eine Multi-Faktor-Authentifizierung eingesetzt.

3.2.3. Autorisierung

Der Zugriff ist mittels eines Rechte- und Rollenkonzepts definiert. Demnach haben die Mitarbeiter nur Zugriff auf Systeme und Verzeichnisse, welche Sie unmittelbar für ihre Arbeitsaufgabe benötigen. Die Definition sowie Änderungsanträge erfolgen auf Ebene der Abteilungsleitung und nach dem Prinzip der Gewaltenteilung.

Administrative Tätigkeiten auf Domänenebene erfolgen im Vier-Augen Prinzip und werden zur Nachvollziehbarkeit unveränderlich protokolliert.

3.2.4. Partner und Subunternehmen

Zur Einhaltung dieser Standards verpflichten wir vertraglich unsere Partner und Subunternehmen, welche mit dem Umgang von personenbezogenen Daten autorisiert sind.

3.2.5. Zertifizierung und Audits

Der Hauptsitz sowie die Niederlassungen der Kilchenmann AG sind durch die Schweizerische Vereinigung für Qualitäts- und Management-Systeme (SQS) nach ISO 9001:2015 zertifiziert.

Zusätzlich erfolgt zur Erhöhung der Qualität und zur Prüfung auf die Einhaltung unserer Prozesse und Richtlinien einmal jährlich ein internes Audit durch geschulte Auditoren unter Leitung der Abteilung Qualitätsmanagement.

Für die Umfassende Prüfung der IT-Systeme und Netzwerke findet in regelhaften Abständen ein Penetrationstest durch spezialisierte Anbieter statt.

3.2.6. Schulung der Mitarbeiter

Im Rahmen einer kontinuierlichen Awareness-Kampagne, die jährlich durchgeführt wird, werden alle Mitarbeiter umfassend zu verschiedenen Aspekten der Cybersicherheit geschult und getestet. Ergänzend dazu findet eine Phishing-Mail-Kampagne statt, um die Sensibilisierung der Mitarbeiter weiter zu erhöhen.