QMP 1.4-2 Datensicherheitsmaßnahmen

1. ZUSTÄNDIGKEITEN

Prozesseigner: GF/IT
Prozessüberwachung: GF QM
Prozessabwicklung: GF QM

2. ABLAUFBESCHREIBUNG

Organisatorische Sicherheitsmaßnahmen

Die aktuelle Sicherheitsleitlinie (Information Security Policy) minimiert das Risiko von Fehlverhalten der eigenen Mitarbeiter, da sie Vorgaben enthält, wie mit Daten, IT und Internet umzugehen ist.

Für die wichtigsten Notfallszenarien (z.B. Stromausfall, Malwarebefall, DoSAngriffe, Datenverlust usw.) sind Dokumente auszuarbeiten, die die zu treffenden Maßnahmen vorab festlegen.

Ein Informationssicherheits-Managementsystem kann, sowohl Gefahren für die Informationssicherheit als auch Bedrohungen des Datenschutzes im Unternehmen durch strukturiertes Vorgehen abwehren.

Eine Risikoanalyse in Bezug auf Datenschutz und den Einsatz von IT-Systemen wird gemäß „Chancen und Risikomanagement Verfahrensanweisung“ durchgeführt werden. Typische Bedrohungen sind technische Probleme, organisatorische Mängel, fahrlässiges Benutzerverhalten, vorsätzliche Handlungen sowie höhere Gewalt.

Voraussetzung für jede Notfallvorsorge sind die Planung und Durchführung regelmäßiger Datensicherungen. Im Datensicherungskonzept ist in schriftlicher Form festgelegt, welche Daten, von wem zu welchem Zeitpunkt gesichert werden müssen und welche Datensicherungsmethoden dabei eingesetzt werden.

Eine Klassifizierung der verwendeten und gespeicherten Daten in Bezug auf ihre Vertraulichkeit und die Datenschutzanforderungen ist eine wesentliche Voraussetzung für die Auswahl adäquater Sicherheitsmaßnahmen.

Die allgemeine Dokumentationspflicht über die getroffenen Datensicherheitsmaßnahmen stellt nicht nur im Anlassfall eine hilfreiche und notwendige Grundlage dar, sondern dient auch der Information der Mitarbeiterinnen und Mitarbeiter.

Eine Auslagerung soll verhindern, dass bei einem Vorfall im Serverraum auch die Sicherungen vernichtet werden. Sie werden idealerweise in einem Safe oder/und besser in einem eigenen Datenträgerarchiv, das räumlich vom Serverraum getrennt ist, oder überhaupt an einem anderen Standort sicher aufbewahrt.

Da wir (Auftraggeber) verpflichtet sind, nur Dienstleister in Anspruch zu nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten, trifft uns (ihn) eine Prüfpflicht. Dieser kann nachgekommen werden, indem wir uns vom Dienstleister dessen Sicherheitskonzept vorlegen lassen.

Standardsoftware oder im Auftrag entwickelte Programme werden einer geregelten Abnahme- und Freigabeprozedur unterzogen.

Eine Lizenzverwaltungs- und Versionskontrolle (IQSOFT) soll verhindern, dass es zum Einsatz nichtlizensierter Software sowie unterschiedlicher Software-Versionen kommt.

QMP 1.4-2 Datensicherheitsmaßnahmen

Personelle Sicherheitsmaßnahmen

Eine klare Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeiterinnen und Mitarbeitern ist ausdrücklich festgelegt.

Voraussetzung für eine Zuordnung von Daten zu den einzelnen Stellenbeschreibungen bzw. Arbeits- und Dienstverträgen, ist das Vorhandensein einer entsprechenden Dokumentation. Diese Forderung ist besonders bei Mitarbeiterinnen und Mitarbeiter mit speziellen Sicherheitsaufgaben beachtet (z.B. Datenschutzvantwortlich, IT-Sicherheitsbeauftragte, Ersthelfer etc.).

Neue Mitarbeiterinnen und Mitarbeiter sind nicht nur auf das Datengeheimnis zu verpflichten, sondern auch auf die Einhaltung der verschiedenen Richtlinien (wie z.B. PC-Benutzerregeln, Regeln für die Benutzung von Internet und E-Mail, Passwortrichtlinie, Bring Your Own Device-Richtlinie (Verboten!) usw.).

Bei Personalveränderungen, insbesondere beim Ausscheiden von Mitarbeiterinnen und Mitarbeitern, sind von diesen sämtliche Unterlagen, ausgehändigte Schlüssel, ausgeliehene IT-Geräte (mobile Geräte, Speichermedien usw.) sowie Dokumentationen und Bücher zurückzufordern. Des Weiteren sind sofort sämtliche Zugangsberechtigungen und Zugriffswege zu sperren bzw. zu löschen (Liste Austritt).

Betriebsfremde Personen (z.B. Reinigungspersonal, IT-Dienstleister) können Zugang zu vertraulichen Unternehmensdaten erhalten und stellen unter Umständen eine erhebliche Bedrohung dar. Sie sind jedenfalls schriftlich im Rahmen von Geheimhaltungsverpflichtungen auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen zu verpflichten (Auftragsverarbeiter-Vertrag).

Mitarbeiter sind über die nach dem DSG 2000 und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren. Die überwiegende Zahl von Schäden im IT-Bereich entsteht durch Nachlässigkeit oder Bequemlichkeit. Die Mitarbeiterinnen und Mitarbeiter werden daher in Bezug auf die möglichen Gefahren im Umgang mit Daten und IT-Geräten geschult.

Die Auswahl eines guten und sicheren Passwortes ist entscheidend für die Sicherheit und Vertraulichkeit der Daten. Gute Passwörter sind ausreichend lang (mindestens 8 Zeichen) und bestehen aus verschiedenen Arten von Zeichen (Groß- und Kleinbuchstaben, Zahlen, Sonder- und Satzzeichen), die zusammen kein sinnvolles Wort ergeben.

Alle Mitarbeiterinnen und Mitarbeiter sollten dazu angehalten werden, bei Abwesenheit vertrauliche Unterlagen zu verschließen und sich vom PC abzumelden.

Datenträger und Papierdokumente mit vertraulichen Inhalten müssen auf sichere Art entsorgt werden. So sind Papierdokumente mit einem handelsüblichen Shredder oder über ein Entsorgungsunternehmen zu vernichten. Bei Datenträgern muss sichergestellt sein, dass diese physisch vernichtet werden.

Neben arbeitsrechtlichen Punkten sind im Sinne des Datenschutzes und der Datensicherheit auch Vereinbarungen über die zu verwendenden Arbeitsmittel (Hardware, Software, Virenschutz, Durchführung von Datensicherungen, Datenkommunikation und Meldewege bei Sicherheitsproblemen) zu treffen. Es sollte auch schriftlich festgelegt werden, dass der Rechner ausschließlich für die berufliche Nutzung verwendet werden darf und andere Personen keinen Zugang erhalten dürfen.

Es ist ein verantwortlicher Ansprechpartner für den Datenschutz sowie für IT-Sicherheit festgelegt worden, der als direkte Kontaktperson für die Mitarbeiterinnen und Mitarbeiter bei auftretenden Fragen und Problemen fungiert.

QMP 1.4-2 Datensicherheitsmaßnahmen

Technische Sicherheitsmaßnahmen

Die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor Einsicht und Verwendung durch Unbefugte sind zu regeln. In Bezug auf die einzelnen Datenanwendungen muss die Zugriffskontrolle nach der Authentifikation des Nutzers den Zugriff auf die einzelnen Informationen über Berechtigungen wie z.B. Lesen, Schreiben, Löschen, Ausführen steuern.

Durch ein Nutzungsverbot (in Stellenbeschreibung) von nichtbetrieblicher Soft- und Hardware soll sichergestellt werden, dass durch die Verwendung privater Soft- und Hardware Schadprogramme eingeschleust werden, die die Stabilität der betrieblichen IT-Systeme negativ beeinträchtigen.

Es sollte sichergestellt sein, dass die Installation von Programmen nur durch befugte und fachkundige IT-Administratorinnen und IT-Administratoren vorgenommen werden.

Durch laufende und systematische Aktualisierungen sollen Fehler beseitigt, das System stabilisieren oder für mehr Sicherheit gesorgt werden. Ohne Updates kann jeder mit dem Internet verbundene PC zum Angriffsziel von Viren oder Spionagetools werden.

Die mobilen Geräte selber, sowie die Kanäle der Datenübertragung sollten verschlüsselt sein, um das Risiko von Verlust, Diebstahl und Einschleppen von Schadsoftware zu minimieren. Die Verschlüsselungspasswörter sind an einer gesicherten Stelle zu hinterlegen.

Es empfiehlt sich für verschiedene Anwendungen verschiedene Passwörter zu benutzen, damit ein gehacktes Passwort nicht Zugriff auf mehrere Bereiche gewährt.

Zur Abwehr von Schadprogrammen müssen alle IT-Systeme des Unternehmens mit Antivirus-Software ausgestattet sein.

Jede Kommunikation zwischen Firmennetz und Internet muss ausnahmslos über die Firewall geführt werden.

Die Verwendung von Wechselmedien (z.B. USB-Sticks, externe Festplatten, CD-ROMs) bringt einige Risiken, wie das Starten fremder Betriebssysteme, die unbefugte Installation unerwünschter Software oder Schadsoftware sowie das unberechtigte Kopieren von Unternehmensdaten mit sich und ist im Unternehmen entsprechend geregelt (lt. Stellenbeschreibung verboten!).

Sicherheitsmängel in Wireless-Netzwerken sind häufig die Ursache erfolgreicher Attacken und wird daher fachmännisch installiert und konfiguriert.

Marketing im Bereich sozialer Netzwerke wird nicht genutzt.

Laut Datenschutzgesetz besteht für Unternehmen eine Protokollierungspflicht über tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, damit diese im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Diese Protokolldaten sind mindestens drei Jahre aufzubewahren.

Für die rechtssichere Archivierung allgemeiner geschäftsrelevanter Geschäftsvorfälle sind die handels- und steuerrechtlichen Vorschriften, das österreichische Umsatzsteuergesetz sowie das Fachgutachten des Fachsenats Datenverarbeitung der österreichischen Kammer der Wirtschaftstreuhänder zu beachten.

Bauliche und infrastrukturelle Sicherheitsmaßnahmen

Besonders schützenswerte Räume (Serverräume, Datenträgerarchiv usw.) sind in nicht-exponierten, sicheren Bereichen unterzubringen und angemessene Schutzmaßnahmen zur Abwehr von Gefährdungen (z.B. Keller → Wasserschäden, Erdgeschoß → Einbruch, Sabotage) sind zu treffen.

Zusätzlich ist ein absolutes Rauchverbot in allen Räumen und die Zurverfügungstellung einer ausreichenden Anzahl von Handfeuerlöschern geregelt.

DSG 2000 verlangt, dass die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln ist. Die Überwachung des Zutritts zum Gebäude bzw. zu sensiblen Bereichen zählt zu den wichtigsten Schutzmaßnahmen. Die Zutrittskontrolle berücksichtigt daher die verschiedenen Bereiche, welche internen und externen Personen zum Gebäude und den sensiblen Bereichen Zutritt gewähren. An physischen Schutzmaßnahmen bieten sich mechanische und / oder elektronische Schließanlagen an.

Die Einrichtung eines Empfangsdienstes vermindert die Gefahr von unerlaubten Zutritten durch Dritte. So müssen sich unbekannte Personen beim Empfang anmelden und ausweisen; Besucherinnen und Besucher werden beim Empfang abgeholt und nach Beendigung des Besuches wieder hinausbegleitet. In diesem Zusammenhang empfiehlt sich die Führung eines Besucherlogbuches??? Abgrenzen ab wo gültig?

Alle Maßnahmen und Informationen, die im Zusammenhang mit der Schlüsselvergabe stehen, müssen in einem Schlüsselplan und in der „Eintritts-Checkliste“ dokumentiert werden. Die Herstellung, Aufbereitung, Verwaltung und Ausgabe und Rückgabe von Schlüsseln sollte zentral geregelt werden.

Die Stromversorgung muss entsprechend den Anforderungen dimensioniert werden, da eine unterdimensionierte Stromversorgung zu Abstürzen und Datenverlust führen kann. Die Überbrückung von Stromausfällen durch eine USV beugt Datenverlusten vor. Zumindest alle betriebswichtigen Server sowie die Sicherheitssysteme sollten über eine USV versorgt werden.

Da Server für den Betrieb innerhalb eines engen Temperaturbereichs ausgelegt sind und bei Überschreiten der max. Betriebstemperatur (meistens 30 bis 35°C), die Gefahr eines Rechnerausfalls besteht, ist – abhängig von der Beschaffenheit der Räumlichkeiten – die Installation einer Klimaanlage in den meisten Fällen vorgesehen.

3. WEITERE EXTERN MITGELTENDE UNTERLAGEN

Datenschutzgrundverordnung

4. ANLAGEN

Keine.