GESCHÄFTSKUNDENPORTAL – INFORMATIONSSICHERHEIT – ÜBERBLICK

August 2017

Agenda

- **Einleitung**
- Informationssicherheit
  - Vorgaben
  - Informationssicherheit Managementsystem
  - Sicherstellung Informationssicherheit
- Geschäftskundenportal
  - Beschreibung
  - Struktur-Überblick
  - Standorte der Server, Zutritts- und Zugriffssicherung bzw.-beschränkungen
  - Einhalten des BSI-Grundschutzes bzw. der entsprechenden ISO-Norm
  - IT-Sicherheitskonzept
  - Log-Files und Zugriffsrechte
  - Löschfristen
  - Zugriffsmöglichkeiten auf die gespeicherte Adress-DB des Kunden

Einleitung

Auszug aus dem Geschäftsbericht 2016:

- „Die Sicherheit unserer Informationssysteme hat für uns einen besonders hohen Stellenwert. Ziel ist es, die IT-Systeme konstant zu betreiben sowie unberechtigte Zugriffe auf unsere System- und Datenbestände zu vermeiden.“
- „Dafür hat das „Information Security Committee“ als Unterausschuss („subcommittee“) des IT-Boards Richtlinien, Standards und Verfahren entwickelt, die der internationalen Norm ISO 27002 für das Management von Informationssicherheit entsprechen.“
- „IT-Risiken werden zudem kontinuierlich von Konzernrisikomanagement, IT-Revision, Datenschutz und Konzernsicherheit überwacht und bewertet.“
- „Damit unsere Prozesse stets reibungslos funktionieren, müssen die dafür benötigten IT-Systeme dauerhaft verfügbar sein. Dies stellen wir dadurch sicher, dass wir die Systeme so gestalten, dass Komplettausfälle in der Regel vermieden werden.“
- „Wir beschränken den Zugang zu unseren Systemen und Daten so, dass die Mitarbeiter nur auf solche Daten zugreifen können, die sie für die ihnen übertragenen Aufgaben benötigen.“
- „Die Systeme und Daten werden regelmäßig gesichert, kritische Daten werden zudem in den Rechenzentren repliziert.“
- „Unsere gesamte Software wird regelmäßig aktualisiert, um mögliche Fehler zu beheben, Sicherheitslücken zu schließen und die Funktionalität zu erweitern.“
- „Risiken, die aus einer veralteten Software oder aus Software-Upgrades herrühren können, begegnen wir mit „Patch Management“ – einem definierten Prozess zur Aktualisierung von Software.“

Agenda

- Einleitung
- **Informationssicherheit**
  - **Vorgaben**
  - **Informationssicherheit Managementsystem**
  - **Sicherstellung Informationssicherheit**
- Geschäftskundenportal
  - Beschreibung
  - Struktur-Überblick
  - Standorte der Server, Zutritts- und Zugriffssicherung bzw.-beschränkungen
  - Einhalten des BSI-Grundschutzes bzw. der entsprechenden ISO-Norm
  - IT-Sicherheitskonzept
  - Log-Files und Zugriffsrechte
  - Löschfristen
  - Zugriffsmöglichkeiten auf die gespeicherte Adress-DB des Kunden

Informationssicherheit – Vorgaben – Überblick

DPDHL hat sich freiwillig verpflichtet (z.B. im veröffentlichten Jahresabschlussbericht), das Informationssicherheits-Managementsystem (ISMS) entsprechend den ISO-Informationssicherheits-Standards zu betreiben.

Dementsprechend sind die Vorgaben, d.h. das Rahmenwerk der Konzernstandards zur Informationssicherheit, gemäß der „International Standards Organization – Standard for Information Security Management“ (ISO27002:2013) aufgebaut.

Dokument	Ziel
Informationssicherheits-Richtlinie	▪ Spezifizierung Kontrollziele zum Management von Informationsrisiken sowie durch das „Cyber Space“ entstandene Risiken innerhalb von DPDHL.
Kontrollanforderungen für die Informationssicherheit	▪ Spezifizierung Kontrollanforderungen, d.h. die technischen Mindestschutzmaßnahmen, die auf Informationen, Informationssysteme und Daten der DPDHL angewendet werden müssen.
Prozesse für die Informationssicherheit	▪ Spezifizierung Prozessvorgaben zum Management von Informationsrisiken sowie durch „Cyber Space“ entstandene Risiken innerhalb von DPDHL.

Informationssicherheit – Vorgaben – Bereiche

Das Rahmenwerk der Konzernstandards zur Informationssicherheit deckt die nachfolgenden Bereichen ab:

- Informationssicherheits-Managementsystem, Compliance-Assessments und Governance sowie Berichtswesen
- Sicherheitsleitlinien
- Organisation der Informationssicherheit
- Personalsicherheit
- Management von organisationseigenen Werten
- Zugriffskontrolle
- Kryptographie
- Schutz vor physischem Zugang und Umwelteinflüssen
- Betriebssicherheit
- Sicherheit in der Kommunikation
- Anschaffung, Entwicklung und Instandhaltung von Systemen
- Lieferantenbeziehungen
- Management von Informationssicherheitsvorfällen
- Informationssicherheitsaspekte des Betriebskontinuitätsmanagements
- Richtlinienkonformität
- Sicherstellung des Geschäftsbetriebs („Business Continuity Management“)

Informationssicherheit – Managementsystem – Überblick

Entsprechend der Anforderungen des Rahmenwerk der Konzernstandards zur Informationssicherheit wird ein dokumentiertes, prozessorientiertes Informationssicherheits-Managementsystem (ISMS) betrieben, überwacht, überprüft, aufrechterhalten und verbessert.

Prozess	**Ziel**
Informationssicherheits-Managementsystem	▪ Sicherstellung Organisation, Betrieb und Überprüfung des Informationssicherheits-Managementsystem
Berichtswesen zur Informationssicherheit	▪ Sicherstellung Transparenz durch Erstellung und Verteilung von regelmäßigen Berichten zu der Informationssicherheit
Management von Informationssicherheits-Risiken	▪ Sicherstellung Vermeidung, Erkennung und Behandlung von Informationssicherheits-Risiken
Management von Informationssicherheits-Vorfällen	▪ Sicherstellung Vermeidung, Erkennung und Behandlung von Informationssicherheits-Vorfällen
Compliance-Assessment und Governance der Informationssicherheit	▪ Sicherstellung Einhaltung der Anforderungen des Rahmenwerk der Konzernstandards zur Informationssicherheit
Sensibilisierung für Informationssicherheit	▪ Sicherstellung Bewusstsein für Informationssicherheit bei Mitarbeitern durch entsprechende Sensibilisierungsmaßnahmen

Informationssicherheit – Sicherstellung Informationssicherheit – Überblick

Lebens-zyklus	Maßnahme	Inhalt der Maßnahme
Projekt	▪ Initiale Risikoidentifikation	▪ Ermittlung wahrscheinliches Risiko eines IT-Systems
	▪ IT-Sicherheitskonzept	▪ Identifizierung Schutzanforderungen, Informationsrisiken und -bedrohungen ▪ Beschreibung Abläufe und Maßnahmen zur Reduktion Risiken auf akzeptables Maß
	▪ Technische Konzepte, z.B. Berechtigung, Backup, Archivierung, Löschung, Protokollierung etc.	▪ Erstellung entsprechender Konzepte als Grundlage für Umsetzung in Projekt, Betriebseinführung, Betrieb und Entsorgung
	▪ „Information Security Self-Assessment“	▪ Überprüfung der Einhaltung der relevanten Vorgaben mittels Selbst-Einschätzung
Betriebs-einführung	▪ Fachliche/technische Abnahmetests	▪ Überprüfung fachliche und technische Umsetzung
	▪ Penetrationstest	▪ Überprüfung auf technische Schwachstellen (optional, bei Internetanwendungen verpflichtend)
Betrieb	▪ „Information Security Self-Assessment“, „Information Security Compliance Assessment“	▪ Wiederholung „Information Security Self-Assessment“ ▪ „Information Security Compliance Assessment“ entsprechend Prüfungsplan
Entsor-gung	▪ Abbau und Entsorgung entsprechend Vorgaben	▪ Löschung/Vernichtung von Daten etc.

Informationssicherheit – Sicherstellung Informationssicherheit – IT-Sicherheitskonzept

Das Sicherheitskonzept identifiziert Schutzanforderungen, Informationsrisiken und -bedrohungen und beschreibt Abläufe und Maßnahmen, um Risiken auf ein akzeptables Maß zu reduzieren. Es ist eine Erweiterung des generischen Ansatzes zum Risiko-Assessment und der generischen Risiko-Behandlung mit Spezifikationen für IT-Dienstleistungen, -Systeme und -Anwendungen.

Das Sicherheitskonzept enthält folgende Informationen:

- Ergebnis einer initialen Risikoidentifikation
- Ergebnis der Sicherheitsklassifizierung
  - Klassifizierung von Informationen und Daten
  - Klassifizierung von IT-Dienstleistungen, -Systemen, -Komponenten und –Anwendungen
- Identifizierte Informationssicherheits-Anforderungen (z.B. technische, regulatorische und fachliche)
- Ergebnis des Risiko-Assessments und der Risikobehandlung
  - Strukturanalyse
  - Identifizierung relevanter Bedrohungen
  - Risikoklassifizierung durch Eintrittswahrscheinlichkeit und Auswirkung
- Ergebnis der Risikobehandlung
  - Festgelegte Informationssicherheits-Maßnahmen
  - Umsetzungsstatus der Informationssicherheits-Maßnahmen
  - Spezifizierte verbleibende Risiken

Agenda

- Einleitung
- Informationssicherheit
  - Vorgaben
  - Informationssicherheit Managementsystem
  - Sicherstellung Informationssicherheit
- **Geschäftskundenportal**
  - **Beschreibung**
  - **Struktur-Überblick**
  - **Standorte der Server, Zutritts- und Zugriffssicherung bzw.-beschränkungen**
  - **Einhalten des BSI-Grundschutzes bzw. der entsprechenden ISO-Norm**
  - **IT-Sicherheitskonzept**
  - **Log-Files und Zugriffsrechte**
  - **Löschfristen**
  - **Zugriffsmöglichkeiten auf die gespeicherte Adress-DB des Kunden**

Geschäftskundenportal – Beschreibung

Komponente	Aufgabe	Funktion
Geschäfts-kundenportal	▪ Einstiegsportal für Paket Geschäftskunden	▪ Zentrales Portal für GK Anwendungen
VLS	▪ Online GK Versandsystem	▪ Bereitstellung von GK Labeln

Geschäftskundenportal – Struktur-Überblick

Das Geschäftskundenportal besteht aus den nachfolgenden Komponenten. Es konsolidiert diverse Prozesse und Services für Geschäftskunden von der Versandvorbereitung bis hin zur Sendungsverfolgung

Startseite

Versenden

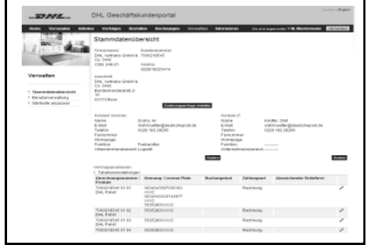
Abholen

Verfolgen

Bestellen

Abrechnen

Verwalten



Geschäftskundenportal – Standorte der Server, Zutritts- und Zugriffssicherung bzw.-beschränkungen

Komponente	Aspekt	Umsetzung
Geschäftskundenportal	Standort	▪ Frankfurt a.M.
	Betreiber	▪ „Equinix“
	Zutritts- und Zugriffssicherung bzw.-beschränkungen	▪ Standard nach ISO 27001
VLS	Standort	▪ Frankfurt a.M.
	Betreiber	▪ „Equinix“
	Zutritts- und Zugriffssicherung bzw.-beschränkungen	▪ Standard nach ISO 27001

Geschäftskundenportal – Einhalten des BSI-Grundschutzes bzw. der entsprechenden ISO-Norm

Lebens-zyklus	Maßnahme	Geschäftskundenportal	VLS
Projekt	▪ Initiale Risikoidentifikation	▪ Erfolgt	▪ Erfolgt
	▪ IT-Sicherheitskonzept	▪ Erfolgt	▪ Erfolgt
	▪ Technische Konzepte, z.B. Berechtigung, Backup, Archivierung, Löschung, Protokollierung etc.	▪ Erfolgt	▪ Erfolgt
	▪ „Information Security Self-Assessment“	▪ Erfolgt	▪ Erfolgt
Betriebs-einführung	▪ Fachliche/technische Abnahmetests	▪ Erfolgt	▪ Erfolgt
	▪ Penetrationstest	▪ Erfolgt	▪ Erfolgt
Betrieb	▪ „Information Security Self-Assessment“, „Information Security Compliance Assessment“	▪ Regelmäßig	▪ Regelmäßig
Entsorgung	▪ Abbau und Entsorgung entsprechend Vorgaben	▪ Vorgesehen	▪ Vorgesehen

Geschäftskundenportal – IT-Sicherheitskonzept

Komponente	IT-Sicherheitskonzept vorhanden?	Letzte Aktualisierung
Geschäftskundenportal	▪ Ja	▪ 2017
VLS	▪ Ja	▪ 2017

Geschäftskundenportal – Log-Files und Zugriffsrechte

Komponente	Aspekt	Umsetzung
Geschäftskundenportal	Inhalt der Log-Files	▪ Auditlogging ▪ Zugriffprotokolle
	Ablage der Log-Files	▪ TSI-Datenbank ▪ Verschlüsselung
	Zutritts- und Zugriffssicherung bzw.-beschränkungen	▪ Betriebsdienstleister „T-Systems“ ▪ Wartungsdienstleister „Materna GmbH“
VLS	Inhalt der Log-Files	▪ Fehlerzustände ▪ fachliche Transaktionen ▪ Aufruf externer Schnittstellen ▪ Aktionen von Administratoren
	Ablage der Log-Files	▪ VLS-Datenbank ▪ Verschlüsselt
	Zutritts- und Zugriffssicherung bzw.-beschränkungen	▪ Betriebsdienstleister „T-Systems“ ▪ Wartungsdienstleister „Micromata“

Geschäftskundenportal – Löschfristen

Komponente	Daten	Löschfristen	Kommentar
Geschäftskundenportal	Log-Files	▪ Täglich ▪ z.T. wöchentlich.	▪ Keine Sendungsdaten ▪ Keine Verhaltenskontrolle
VLS	Log-Files	▪ Löschen nach spätestens 90 Tagen	▪ n/a
	Sendungsdaten	▪ spätestens nach 11 Jahren	▪ GOBS-relevante Daten müssen mindestens 10 Jahre aufbewahrt werden
	Benutzerdaten (wie Adressen)	▪ spätestens 25 Monaten nach Kündigung des Kunden	▪ n/a

Geschäftskundenportal – Zugriffsmöglichkeiten auf die gespeicherte Adress-DB des Kunden

Komponente	Zugriffsmöglichkeit	Kommentar
Geschäftskundenportal	▪ N/A	▪ Speicherung von Adressdaten ausschließlich über eingebundene Anwendungen (z.B. VLS)
VLS	▪ Zugriff haben nur autorisierte Administratoren beim Wartungs- und Betriebsdienstleister	▪ n/a