Datenschutzbegutachtung nach §11 Abs. 2 Satz 4 Bundesdatenschutzgesetz (BDSG) zur Überzeugung über die Einhaltung der getroffen technischen und organisatorischen Maßnahmen nach §9 BDSG der Firma mailingwork/w3work, im Auftrag der Firma TS&C durch Joachim Kohnle, extern bestellter Datenschutzbeauftragter.

w3work

Gesellschaft für Kommunikation und Medien

Gneuß & Arnold GbR

Birkenweg 6

09569 Oederan

mailingwork GmbH

Birkenweg 7

09569 Oederan

am Mittwoch, dem 30 Januar 2013 in den Räumen von mailingwork/w3work in Oederran

Teilnehmer:

Herr Mühlich (TS&C) - teilweise

Herr Arnold (Geschäftsführer mailingwork GmbH / w3work GbR) – teilweise

Herr Gneuß (Geschäftsführer mailingwork GmbH / w3work GbR) – teilweise

Herr Haubold (w3work GBR)

Herr Mentzner (mailingwork GmbH)

Herr Kohnle (KOHNLE-IT)

Einleitung:

Als extern bestellter Datenschutzbeauftragter der Firma Toedt, Dr. Selk & Coll. GmbH, habe ich im Auftrag von Herr Michael Toedt, eine angekündigte Datenschutz Audit nach §11 Abs. 2 Satz 4 BDSG in den Räumen von mailingwork/w3work in Oederan durchgeführt, um zur Überzeugung zu gelangen, dass alle in dem Dokument „Technische und organisatorische Maßnahmen“ der Firma mailingwork/w3work genannten Vorkehrungen und Prozesse auch eingehalten werden.

Zutrittskontrolle:

Ist: (ist zustand bei der vor Ort Begehung)

Die Zugänge zu den Büroräumen von mailingwork/w3work sind durch Alarmgesicherte Sicherheitscodeschlösser und Schlüsselschließsysteme gesichert. Durch die Ortslage ist ein unbeobachteter Zugang zudem schwer möglich. Ferner ist auch ein Wohnbereich des Eigentümers direkt angeschlossen.

Die Zugänge zum Rechenzentrum (nicht persönlich gesichtet) von e-shelter (Serverstandort für die Aktuelle Version mailingwork 3, siehe Anlage) in Berlin sind gesichert und geschützt durch

- doppelte Zaunanlage
- Videoüberwachung außen
- Schrankenanlagen / Drehkreuze mit Sicherung durch Chipkarte
- Der Zutritt ist nur nach Voranmeldung und er Abgabe von Ausweisdokumenten und in Begleitung vom Rechenzentrumsmitarbeitern möglich
- Video Überwachung im Gebäude
- Zugang zu den individuellen einzelnen Käfigen ist durch Code-/Chipkartenschlössern vor unberechtigten zugriffen geschützt
- Die Käfige selbst mit Stahlgitterabtrennungen im Zwischenboden
- Die Serverschränke mit PZ-Schloss bzw. mit Codeschloss
- Ebenso ist ein 24/7 Wachschutz vorhanden

Das Rechenzentrum für die ältere Version, mailingwork 2, ist im Rechenzentrum der Colt Telecom, Berlin untergebracht. Dieses ist nicht ganz so modern eingerichtet, bietet aber einen sehr hohen und ausreichenden Sicherheitsstandard. Das Colt Telecom Rechenzentrum wird in einem absehbaren Zeitraum verlassen.

Zugangskontrolle:

Die eingesetzte Benutzerverwaltung der Server und der Arbeitsplatzrechner garantiert einen umfangreichen Zugang Kontrolle, welche auch entsprechend Dokumentiert wird. Die Bildschirmschoner / Bildschirmsperren sind auch mit Password Eingaben geschützt. Die Passworte sind in Regeln so gestaltet, dass Sonderzeichen, Zahlen und Buchstaben in ausreichender Länge eingesetzt werden. Logins von Mitarbeitern die das Unternehmen verlassen, werden umgehend gelöscht. Entsprechende Listen wurden mir vorgelegt.

Zugriffskontrolle:

Es ist auf den Linux Rechnern mit der systemspezifischen Benutzerverwaltung und den damit einhergehender Vergabe von Benutzerrechten ausreichen gewährleistet, dass der mailingwork/w3work Mitarbeiter nur auf die Bereiche Zugriff erlangt, für die er berechtigt ist. Das Führen eines Berichts über die Vergabe von Benutzerrechte wurde mir gezeigt und ich kann bestätigen, dass dieser regelmäßig geführt wird.

Es wurde mir bestätigt, dass eine Trennung der Test- und Produktionsumgebung zu jedem Zeitpunkt gewährleistet ist. Die Absicherung der Bereiche, in denen Datenträger aufbewahrt werden, ist mit einem Schlüsselsystem ausreichend gewährleistet. Es ist den Mitarbeitern die private Nutzung vom Internet und Email verboten, welche Zugriff auf Daten des Auftraggebers haben.

Weitergabe Kontrolle:

An das Versandlösung mailingwork werden „nur“ die Emailadresse und Vor und Zuname, sowie der „salutation Code“ übermittelt. Die Übermittlung wird via TSL/SSL Verschlüsslung realisiert. Auch ist eine Weitergabe als verschlüsselte Datei via Email möglich, wobei das Password auf einem getrennten Weg übertragen wird.

Eingabekontrolle:

Es wurde bestätigt, dass alle Modifikationen am Datensatz (Anlage, Veränderung, Löschung), der Zeitpunkt und der Benutzername protokoliert werden.

Auftragskontrolle:

Aufträge werden schriftlich erteilt. Die Details sind in der jeweiligen Vereinbarung zur Datenverarbeitung geregelt. Es finden regelmäßige innerbetriebliche Schulungen und Unterweisungen zum Thema Datengeheimisse und Datenschutz statt. Eine regelmäßig geführte Teilnehmerliste wurde mir vorgelegt.

Verfügbarkeit:

- Die Sicherung besteht aus einem räumlich getrennten Filesystembackup, welcher täglich durchgeführt und 30 Tage aufbewahrt wird.
- Das Rechenzentrum ist mit Argon-Löschanlagen ausgestattet
- Im RZ ist eine Rußpartikel-Raumüberwachungsanlage installiert
- Die Kameras dienen auch der Überwachung von z.B. von thermischer Störungen
- Es sind zwei USV - Energiegürtel installiert und zusätzlich ein 72 Stunden Notstrom-Dieselgenerator
- Wartungsarbeiten im RZ werden 72 Stunden im Voraus angekündigt

Trennungskontrolle:

Es wurde bestätigt, dass durch die Zugriffsberechtigungen nur berechtigte Nutzer auf die benötigten Daten zugreifen können. Die Trennung erfolgt durch den Einsatz von logisch getrennten Datenbanken und Verzeichnissen.

Vergleich mit per ADV-Vereinbarung vereinbarten TOM's:

- **Zutrittskontrolle: keine Defizite festgestellt**
- **Zugangskontrolle: keine Defizite festgestellt**
- **Zugriffskontrolle: keine Defizite festgestellt**
- **Weitergabe Kontrolle: keine Defizite festgestellt**
- **Eingabekontrolle: keine Defizite festgestellt**
- **Auftragskontrolle: keine Defizite festgestellt**
- **Verfügbarkeit: keine Defizite festgestellt**
- **Trennungskontrolle: keine Defizite festgestellt**

Fazit:

Zum Schluss kann ich nun meine absolute Überzeugung zum Ausdruck bringen, dass bei der Firma mailingwork/w3work alles unternommen wird, um den heutigen Datenschutzansprüchen nach BDSG gerecht zu werden und auch zukünftige Anforderungen schnell erfüllen zu können. Die vorgelegten Protokolle und Listen sind ordentlich und allem Anschein nach auch regelmäßig geführt. Die Offices sind nach Aufgaben und Funktionen räumlich getrennt. Die Mitarbeiter werden regelmäßig in einen innerbetrieblichen Seminar vom bestellten Datenschützer, Herrn Haubold, über den Datenschutz und seinen rechtlichen Begründungen geschult und entsprechend sensibilisiert.

Poing, 25. Februar 2013

Joachim Kohnle

Anlage

Gebäudeinfrastruktur für höchste Anforderungen

e-shelter hat mit seinem Datacenter in Berlin eine hochverfügbare Umgebung geschaffen, die durch ihre redundant ausgelegten Systeme und integrierte Facility-Management-Infrastruktur höchsten Anforderungen an physischer Sicherheit und technischer Verfügbarkeit gerecht wird.

Das e-shelter Datacenter in Berlin besteht aus 18.000 m² Rechenzentrums- und 2.000 m² Bürofläche, die nach den jeweils individuellen Anforderungen der Mieter ausgebaut werden.

Bauliche Ausführung

Die Gebäude auf dem Berliner Campus sind Umbauten, die ausschließlich für die Nutzung als Datacenter entworfen und realisiert wurden. Alle externen und internen Ein- und Ausbauten sind mit hochwertigen Materialien nach Industriestandard gebaut:

- Regenentwässerung der Gebäude generell über Satteldächer und außen liegende Regenfallrohre
- Maximale Flächennutzung durch ein Stützenraster von 19 x 10 m
- Brandschutzwände mit einer Feuerwiderstandsdauer von 90 Minuten
- Höhe des Doppelbodens beträgt 90 cm und hat eine Punktlast der Lastklasse 4 bzw. 5 (4 - 4,5 kN)
- Die lichte Geschosshöhe des Rohbaus beträgt 3,40 m
- Gemauerte Außenwände mit fensterloser, abschirmender und gedämmter, vorgehängter Fassade im Bereich RZ und Technik

Für die technischen Bereiche des Mieters wird ein hoher Grad an kundenspezifischer Anpassung realisiert. Die jeweilige Mieteinheit wird erst vor dem Einzug nach den Erfordernissen des Kunden ausgebaut. Die Raumgestaltung kann somit individuell angepasst und die Flächen nach dem Bedarf des Mieters skaliert werden.

Die Beschaffenheit des Grundstücks und die Gebäudeanlagen sind ausgelegt, um mögliche Schäden durch Elementarrisiken (z.B. Überflutung, Feuer, Blitzeinschlag) oder Terrorattacken zu minimieren.

Stromversorgung

Die gesamte Stromversorgung auf dem e-shelter Campus in Berlin wird als duale Strom- und Notstromversorgung mit einer unterbrechungsfreien A- und B-Versorgung für die IT-Systeme der Mieter und mit einer zusätzlichen redundanten Versorgung für alle kritischen technischen Gebäudeanlagen wie Klima-, Kälte-, Lüftungs- und Sicherheitsanlagen ausgeführt. Darüber hinaus verfügt e-shelter auf dem Campus über zwei Einspeisungen auf der 10 kV-Ebene.

Die Notstromversorgung wird durch redundante Netzersatzaggregate und die Unterbrechungsfreie Stromversorgung (USV) bereitgestellt. Die USV-Anlagen versorgen die Mieteinheiten über Batteriestrom bis die Dieselgeneratoren die Versorgung übernehmen. USV-Anlagen und zugehörige Batterieanlagen sind je A- und B-Versorgung redundant aufgebaut und können auf A- oder B-Versorgung für mindestens 15 Minuten die Stromversorgung bei 100 % Maximallast überbrücken.

Die Steuerung der Generatoren erfolgt automatisch, so dass bei einem Ausfall der Stromversorgung durch einen Stromlieferanten die Generatoren selbsttätig starten. Der am Campus vorgehaltene Kraftstoff reicht aus, um die gesamte Stromversorgung des Standortes für 72 Stunden ununterbrochen sicherzustellen.

Das gesamte Strom- und Notstromversorgungssystem von e-shelter erfüllt alle Anforderungen an Hochverfügbarkeit:

- Redundante 10 kV-Einspeisung
- Separate USV-Systeme (getrennte, vollredundante A- und B-Versorgung)
- Redundant ausgelegte Netzersatzanlagen mit Dieselgeneratoren

Klimatisierung und Lüftung

Die Klima- und Kälteanlagen auf dem e-shelter Campus sind nach den Sonderanforderungen für hochverfügbare Systeme ausgeführt, um Ausfallsicherheit und Redundanz zu gewährleisten:

- Energieeffiziente, redundante Umluftkühlungssysteme in Klimaspangen
- Redundante Klimaschränke und Pumpen der Kälteversorgung
- Kältemaschinen mit integrierter Freier Kühlung und übergeordneter Gruppensteuerung
- Redundante, USV-gestützte Gebäudeleitsysteme (GLT) zur Überwachung aller technischen Anlagen und Systeme
- Raumlufttechnische Anlagen mit zentraler Be- und Entlüftung und Be- und Entfeuchtung

Anlage

Sicherheit

Das integrierte Sicherheitskonzept von Objekt- und Gebäudeschutz bei e-shelter ist angelegt, um den bestmöglichen physischen Schutz für IT- und Netzwerksysteme der Mieter sicherzustellen.

Physische, technische und personelle Sicherheit gewährleistet e-shelter durch ein 6-stufiges Sicherheitssystem, das mit der Überwachung des Campusgeländes und der jeweiligen Gebäude beginnt und mit der Kontrolle der Mietbereiche und der einzelnen Systeme abschließt:

- Videoüberwachungsanlage für das Gelände und die Gebäude in Kombination mit einer Gefahrenmeldeanlage
- Gesicherte Grundstücksgrenzen durch Sicherheitszaunanlage mit Übersteig- und Unterkriechschutz
- Zufahrt durch Schrankenanlage mit Sicherheitstoren und Durchfahrsperren
- 24/7 zertifizierte Notruf- und Betriebs-Leitstelle (NSL und BSL)
- Zugangskontrollen per berührungsloser Chipkarte und Scramble-Tastatur
- Geschlossene Videoüberwachung von Türen und Zugängen mit automatischem Intrusionsalarm
- Diverse Sensoren innerhalb und außerhalb der Gebäude zur Intrusionserfassung

Die Steuerung der technischen Sicherheit wird durch ein Gefahrenmelde- und Gebäudemanagementsystem geleistet, das den Zustand aller Sicherheits- und Infrastruktursysteme anzeigt und den Regelbetrieb überwacht.

Die Meldungen werden in der e-shelter Notruf- und Service-Leitstelle vor Ort rund um die Uhr erfasst und die gegebenenfalls erforderlichen Maßnahmen eingeleitet.

Geschultes Personal stellt den Regelbetrieb sicher und sorgt auch bei Störungen und Notfällen für die Aufrechterhaltung der Prozesse.

Brandschutz und Löschanlagen

Für den Innenausbau der Mietflächen werden ausschließlich spezielle, nichtbrennbare oder nur schwer entflammbare Materialien verwendet. Die einzelnen RZ-Flächen sind in separate Brandschutzzonen unterteilt. Innerhalb jedes Mietbereiches sind umfassende Brandbekämpfungs- und Brandschutzsysteme installiert. Rauchmelder mit Brandfrühesterkennung (VESDA = Very Early Smoke Detection Apparatus), die in ein Brandmeldesystem (BMS) eingebunden sind, gewährleisten die frühestmögliche Warnung bei einem potenziellen Feuer. Die Brandbekämpfung erfolgt durch ein Feuerlöschsystem mit Löschgas (Argon).

- Gebäudebrandabschnitte der Feuerwiderstandsklasse F90 A und alle Technik- und Hardwareräume als F90 A-Brandbekämpfungsabschnitte
- Gesicherte Trassen mit F30/90 A Brandschotts
- Flächendeckende Überwachung aller Räume und Ebenen mit automatischen, digitalen Brandmeldern und -anlagen
- Brandfrühesterkennung mit VESDA Systemen
- Automatische Gaslöschanlage zur Flutung der Rechnerräume

Netzwerk-Anbindung

e-shelter ist ein Carrier-neutraler Anbieter und ermöglicht freien Zugang zu verschiedenen Netzwerkanbietern. Der Mieter verfügt somit über die Flexibilität, aus mehreren Netzwerkanbietern auszuwählen und mit den Anbietern seiner Wahl einen Vertrag abzuschließen.

Das e-shelter Datacenter in Berlin bietet zwei unabhängige Netzwerk-Einspeisungspunkte und zwei separate Carrier-Meet-Me-Räume sowie separate Versorgungsnetze, um eine komplett redundante Netzanbindung zu gewährleisten.