Audit/Prüfprotokoll Auftragsdatenverarbeitung gemäß § 11 Abs. 2 BDSG

Geprüfter Auftragsdatenverarbeiter:

The unbelievable Machine Company GmbH
Grolmanstr. 40
D-10623 Berlin

Datum der Prüfung:

11. März 2014

Art der Prüfung:

Erstprüfung, Einhaltung der vom Auftraggeber zugesicherten technischen und organisatorischen Maßnahmen nach § 9 BDSG und Anlage, Kontrolle der ordnungsgemäßen Datenverarbeitung

Ort der Prüfung:

- Büro der The unbelievable Machine Company GmbH (im Folgenden *um genannt), Grolmanstr. 40, D-10623 Berlin
- von *um genutztes Rechenzentrum der e-shelter facility services GmbH, Datacenter Berlin, Nonnendammallee 15, D-13599 Berlin

Anwesende Personen:

Für *um:

- Thorleif Wiik, Vertrieb/Technik,
- Dana Gleisberg, Assistenz der Geschäftsleitung (Auditteil *um)
- Peter Lampe, Manager Kundenprojekte der e-shelter facility services GmbH (Auditteil: e-shelter)

sowie für mailingwork:

- Jörg Arnold, Geschäftsführer
- Torsten Gneuß, Geschäftsführer
- Steve Seypt, Software Entwickler
- Thorsten Ulrich, Software Entwickler
- Markus Haubold, Datenschutzbeauftragter

Gesprächs-/Prüfungsthemen:

1 Büroräume *um

Im Rahmen der Erstprüfung wurden die Geschäftsräume von *um besichtigt. Im Vorfeld fand ein umfangreicher Austausch mit Sven Meyzis, Datenschutzbeauftragter von *um statt.
Es wurden folgende Dokumente vorgelegt, die einen ersten Eindruck vom hohen Niveau der Datenverarbeitung bei *um gestatteten:

- Dokumentation: „Technische und organisatorische Maßnahmen des Datenschutzes, *um Office"
- Dokumentation: „Technische und organisatorische Maßnahmen des Datenschutzes, *um Hosting"

- gültiges Zertifikat „Payment Card Industry Data Security Standard (PCI DSS)"
- gültiges Zertifikat „ZERTIFIKAT für das Managementsystem nach DIN ISO/IEC 27001:2005", ausgefertigt vom TÜV Austria Deutschland
- gültiges Zertifikat des Datenschutzbeauftragten über die interne Überprüfung des Datenschutzniveaus bzw. die Einhaltung der einschlägigen datenschutzrechtlichen Bestimmungen bei *um
- Muster der Verpflichtungserklärungen auf das Datengeheimnis (§ 5 BDSG) und Fernmeldegeheimnis (§ 88 TKG)
- Zuarbeiten zu Passwort-Policy und Strukturierung der Serverzugriffe von René Beiler, Information Security Manager bei *um

Im Hinblick auf die nachgewiesenen Zertifizierungen bezog sich die Auditierung auf folgende, ausgewählte Sachverhalte:

- stichprobenartige Überprüfung ausgewählter Maßnahmen zur Zutrittskontrolle
- stichprobenartige Überprüfung ausgewählter Maßnahmen zur Zugangs- und Zugriffskontrolle
- Überprüfung des Umfangs der Verpflichtung von Mitarbeitern auf Daten- und Fernmeldegeheimnis

1.1 Überprüfung der Maßnahmen zur Zutrittskontrolle:

Bei den Büroräumen handelt es sich um Mietflächen in einem renovierten, vorrangig gewerblich genutztem Gebäude in Berlin Charlottenburg. Die Umgebung ist mit ebenfalls renovierten Gebäuden bebaut und unterliegt einer gemischten Nutzung (Wohn-, Büro- und Gewerbeflächen). Bausubstanz und Ambiente vermitteln einen ordentlichen Eindruck. Die *um Büroräume befinden sich in den Stockwerken S5, 5 und S6 des Gebäudes Grolmanstraße 40. Baulich bedingt verfügt das Gebäude über Zwischenstockwerke.

- Die Eingangstür zum Gebäude (Straßen-/Haupteingang) ist verschlossen. Eine Wechselsprecheinrichtung mit elektrischem Türöffner ist installiert.
- Der Zutritt zu dem Büroräumen erfolgt lt. Dienstanweisung ausschließlich über die 5. Etage. Der Eingangsbereich ist durch eine geschlossen gehaltene, verglaste Stahltür gesichert. Unmittelbar hinter der Eingangstür befindet sich ein großzügiger Empfangsbereich mit Sekretariat und Arbeitsplätzen.
- Die Eingangstüren sind mit einem zentralem, codierten Sicherheits-Schließsystem ausgestattet.
- Die *um Büroflächen wurden in den vergangenen Jahren kontinuierlich im Gebäude erweitert. Hierfür wurden sicherheitsorientierte, bauliche Veränderungen geschaffen: bürointerne Treppen und Übergangsbereiche, Erweiterung des Schließsystems, Strukturierung der Office-Bereiche.

1.2 Überprüfung der Maßnahmen zur Zugangs- bzw. Zugriffskontrolle:

- Die *um-Arbeitsplätze sind mit Desktop-PC oder Notebooks ausgestattet. Sämtliche Notebooks sind nach Angaben von *um mit einer verschlüsselten Festplatte ausgestattet.
- Personenbezogene Daten der Auftraggeber werden nicht lokal, sondern ausschließlich im Rechenzentrum gespeichert. Es gibt im *um-Office keine lokalen Serverlösungen.
- Es existiert eine dokumentierte Passwort-Policy. Diese umfasst u.a. folgende Regelungen:
  - Admin-Passworte verfügen über mindestens 12 Zeichen, sonstige Passworte über 8 Zeichen
  - Mix aus Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen

    - Passworte werden alle 90 Tage gewechselt, nicht wiederverwendet/rotiert
    - Passworte dürfen nicht bei automatischen Login-Prozessen genutzt werden
    - keine Trivialpassworte (Geburtstage, Telefonnummern, Wörter)
- Bei der Bürobesichtigung erfolgte eine Sichtkontrolle aller unbenutzten Workstations. An nicht besetzten Arbeitsplätzen waren die PC ausgeschaltet. Bildschirme von vorübergehend nicht besetzten (temporär verlassenen) Arbeitsplätzen waren gesperrt.
- Im Rahmen des 24/7-Supports und der definierten Eskalationsszenarien können mobile Arbeitsgeräte auch unterwegs eingesetzt werden. Insgesamt sind die hierfür definierten Zugangswege ebenso wie die Netzwerke im *um Office in die PCI-Zertifizierung inkludiert.
- Verschlissene Hardware wird über einen zertifizierten Entsorger vernichtet.
- Für ein spezielles Kundenprojekt (Webentwicklung) arbeitet *um z.Zt. mit Freelancern. Diese verfügen über einen separaten Bürobereich. Auch hier setzt *um auf langfristige Zusammenarbeit.
- *um setzt ein nach PCI-DSS Standard zertifiziertes Berechtigungssystem ein, welches im Rahmen des kontinuierlichen Verbesserungsprozesses implementiert wurde.
- Zugang auf die mailingwork-Server erhalten ausschließlich Administratoren. Der Zugriff erfolgt verschlüsselt über VPN-Tunnel und eine Zwei-Faktor-Authentifizierung.

1.3 Überprüfung der Maßnahmen zur Einhaltung von Datengeheimnis bzw. Fernmeldegeheimnis

- es erfolgen monatliche Schulungen zu den Themen IT-Security und Datenschutz
- die Mitarbeiter werden auf die Einhaltung von Datengeheimnis (§ 5 BDSG) und Fernmeldegeheimnis (§ 88 TKG) verpflichtet.
- Als Nachweis für die Verpflichtungen und regelmäßigen Weiterbildungen werden Schulungslisten geführt.
- Zur Vereinfachung der Weiterbildungen für die derzeit 50 Mitarbeiter ist die Umsetzung einer E-Learning Plattform in Planung.
- Eine Verpflichtung auf allgemeine Geheimhaltung (Dienstgeheimnis) findet arbeitsvertraglich statt.

Zusammenfassung Auditteil Büro *um

*um ist ein leistungsstarker Partner auf dem Gebiet Hosting/Managed Server und Beratung zu Serverachitektur. Der vor Ort gewonnene Eindruck deckt sich mit den vorgelegten Zertifikaten und Nachweisen: Bei *um wurden strukturelle Rahmenbedingungen geschaffen, um qualitativ hochwertiges Arbeiten zu ermöglichen und die besonderen Anforderungen an IT-Sicherheit und Datenschutz zu erfüllen. An Hand der vorliegenden Unterlagen und gewonnenen Eindrücke besteht kein Zweifel an einer sicheren Datenverarbeitung im Auftrag.

2 Rechenzentrum e-Shelter

Zusammen mit *um wurde eine Besichtigung des Rechenzentrums der e-shelter facility services GmbH / Datacenter Berlin vorgenommen. In diesen Auditteil wurden folgende Bereiche einbezogen:

- Eingangsbereich mit Maßnahmen zur Zutrittskontrolle
- Außenanlagen mit Notstromaggregaten und Klimatechnik
- Innenbereich mit Klimatechnik, Brandschutzanlagen und Cages mit Servertechnik von *um.

2.1 Überprüfung Eingangsbereich/ allgemeine Zutrittskontrolle

- Absicherung des Rechenzentrum-Geländes mit folgenden sichtbaren Maßnahmen: doppelte Zaunanlagen, Videoüberwachung, Schrankenanlagen bzw. Drehkreuzen mit Sicherung durch berührungslose Chipkarte und teilweise Scramble-Tastatur (PIN-Code).
- Zutritt erfolgte nach Voranmeldung und Legitimierung durch Personalausweis (Umtausch des Personalausweises in eine Besucher-Chipkarte, Rückgabe des Personalausweises bei Check-Out).
- e-shelter verfügt über eine eigene Security-Abteilung, ein Mitarbeiter dieser Security-Abteilung war während des gesamten Aufenthaltes als Begleitperson zugegen.
- Bauliche Aufteilung des Außenbereichs in mehrere Schalen (im Außenbereich z.B. Separierung der Klima- und Notstromtechnik mit getrennten Zaun- und Toranlagen; im Innenbereich z.B. bauliche Abtrennung der Klimaspange von dem Gebäudebereich mit den Cages).
- Die Korridore, Anlagen und Räume innerhalb des Rechenzentrums unterliegen umfassender Videoüberwachung. Die einzelnen Sicherheitsbereiche sind durch Stahltüren mit Sicherung durch berührungslose Chipkarte und teilweise Scramble-Tastatur (PIN-Code) gesichert.
- Die Cages mit der Servertechnik verfügen weiterhin über Stahlgitter-Trennwände und Türen mit Sicherung durch berührungslose Chipkarte.
- Laut Auskunft von *um werden alle sieben Cages ausschließlich von *um genutzt (keine Mischflächen).
- Alle Server sind in Serverschränken untergebracht, die Serverschränke sind zusätzlich mit Profilzylinderschloss oder Zahlenschloss gesichert; im doppelten Boden sind die Käfige mit Stahlgitter abgetrennt.

2.2 Überprüfung Brandschutz- und Löschanlagen

- Das Rechenzentrum verfügt über eine Argon-Löschanlage. Im Brandfall wird das Argon in die vom Brand betroffenen Bereiche eingeleitet und das Feuer erstickt, indem der Sauerstoffgehalt der Luft auf unter 14 % gesenkt wird.
- Die vom Brand nicht betroffene Rechentechnik kann während eines Löschvorgangs weiterbetrieben werden, da keine Stromabschaltung erforderlich ist.
- Neben der Kameraüberwachung verfügen die Käfige mit der Servertechnik über eine Raumluftüberwachung, die sensorisch die Luft auf Rußpartikel untersucht.
- Eine davon unabhängige Rauchmeldeanlage über Rauchmelder an der Decke ist ebenfalls installiert. Zudem sind Handauslöseknöpfe für die Brandmeldung/-löschung vorhanden.
- Im Rechenzentrum wird auf peinlichste Sauberkeit geachtet, um Fehlalarmierungen durch Stäube oder andere Partikel-Emissionen (z.B. beim Zerlegen von Verpackungskartons etc.) zu vermeiden.
- CO2-Feuerlöscher sind vorhanden, die Rettungswege sind ausgeschildert.

2.3 Überprüfung USV-Anlagen

- Das Rechenzentrum befindet sich zwischen den beiden Energiegürteln der ehemaligen Stadtteile Ost- und West-Berlin. Dadurch stehen zwei separate Energieeinspeisungen von getrennten Umspannwerken zur Verfügung. Jeder Käfig besitzt daher zwei getrennte Verteilerschränke (getrennte Stromeinspeisungen bis zum Rack).
- Fallen beide Energieeinspeisungen aus, stehen Generatoren zur Verfügung. Besichtigt werden konnte der Anlagenteil außerhalb des Gebäudes (Generatoren in Containern, Tankanlagen).
- Nach Auskunft von e-shelter kann die Generator-Anlage mit dem vorgehaltenen Treibstoff den Rechenzentrums-Betrieb unter Volllast für mindestens 72 Stunden aufrecht erhalten

(Erfüllung der Anforderungen an Tier IV Klassifikation).
- Es erfolgen monatliche Tests der Anlagen unter Last sowie jährlich ein Black-Building-Test.
- Der Treibstoff der Dieselaggregate wird im Winter konditioniert, um ein Gelieren des Treibstoffs zu vermeiden.

2.4 Überprüfung Klimaanlagen

- Im Außenbereich des Rechenzentrums befinden sich die Kühlaggregate, die über zwei Kühlschleifen die Cages mit Kaltluft versorgen.
- Je Aggregateblock sind zwei Kompressoren vorhanden (redundante Ausführung).
- Bei Außentemperaturen unter 15°C kommen zudem Umgebungsfrischlüfter zum Einsatz.
- Bei hohen Außentemperaturen kann durch eine adiabatische Zusatzkühlung erreicht werden, dass die Kältemaschinen bis 46°C Außentemperatur einsatzbereit sind.
- Im Außenbereich sind Erweiterungsflächen für Kühlaggregate bereits baulich erschlossen (abgetrennter Bereich, Fundamente).
- Im Innenbereich sind die Klimageräte baulich von den Cages getrennt; Wartungspersonal hat somit keinen Zutritt zur Rechentechnik.
- Alle Geräte waren sichtbar mit Prüfprotokollen ausgestattet, Wartungsintervalle werden laut Datierung auf den Protokollen eingehalten.

Zusammenfassung Auditteil Rechenzentrum e-shelter

Die Begehung des Rechenzentrums zeigte, dass sich die Infrastruktur auf einem sehr hohen Niveau befindet. In Verbindung mit den vorgelegten und gültigen Zertifikaten ISO 27001 auf Basis von IT-Grundschutz, VdS Anerkennung als Wach- und Sicherheitsunternehmen, VdS Qualitätsmanagementsysteme/Technisches Facility Management für Hochverfügbare Data Center und VdS Anerkennung als Errichterfirma für Einbruchmeldeanlagen bestehen keine Zweifel an der Ordnungsmäßigkeit der Datenverarbeitung.

Datum: 08.04.2014

Markus Haubold,
Datenschutzbeauftragter