Verbraucherhinweis gemäß § 43a Absatz 1 Nr. 12 TKG

Maßnahmen, mit denen die htp GmbH auf Sicherheits- und Integritätsverletzungen oder auf Bedrohungen oder Schwachstellen reagieren kann

Stand: 01.01.2013

I. Einleitung

Das Thema Sicherheit spielt bei der htp GmbH als Anbieter von Telekommunikationsdienstleistungen eine wichtige Rolle.

Um angemessen auf bestehende oder mögliche Sicherheits- und Integritätsverletzungen bzw. Bedrohungen und Schwachstellen reagieren zu können, sehen wir zahlreiche organisatorische und technische Maßnahmen vor.

II. Sicherheitsorganisation

Die einzelnen Maßnahmen sind Bestandteil einer Sicherheitsorganisation.
An der Spitze des Regelungsrahmens steht bei der htp die interne IT-Sicherheitsleitlinie, in der die Geschäftsführung den Stellenwert der IT-Sicherheit und des Datenschutzes, die Ziele und die Maßnahmen im Allgemeinen und das IT-Sicherheit- und Datenschutzmanagementsystem, welche das Zusammenspiel aller Geschäftsbereiche bei der htp regelt, definiert.

Der IT-Sicherheitsbeauftragte, das htp Sicherheitsteam und der Datenschutzbeauftragte sind feste Bestandteile der internen Sicherheitsorganisation.

Durch themenspezifische Richtlinien werden die allgemeinen Vorgaben konkretisiert, um ein angemessen hohes Sicherheits- und Datenschutzniveau zu gewährleisten.

Durch Audits oder im Rahmen der Bearbeitung von Hinweisen und Beschwerden von Kunden und Mitarbeitern wird in regelmäßigen Abständen untersucht, ob Systeme, Prozesse, Organisationen und Standorte tatsächlich die Anforderungen und Richtlinien erfüllen. Audits werden sowohl von internen als auch von externen Stellen, wie z. B. im Fall von Penetrationstes, durchgeführt.

III. Reaktionen auf Sicherheits- und Integritätsverletzungen im Einzelnen

Wir haben technische und organisatorische Maßnahmen umgesetzt, um auf Sicherheits- oder Integritätsverletzungen reagieren zu können, z. B.:

1. Vorfälle mit Sicherheitsrelevanz oder mit Kundendatenbezug werden von uns identifiziert, bewertet und behoben.
2. Die eingesetzte Hard- und Software wird von uns regelmäßig überprüft, so dass wir auf akute Sicherheits- oder Integritätsverletzungen schnell reagieren können. Es gibt ein dokumentiertes Changemanagement. Die damit verbundenen Prozesse sind auf Basis des internationalen Standards ITL beschrieben.
3. Für den Fall, dass wir die Verletzung der Sicherheit oder Integrität Ihrer Daten feststellen, werden wir Sie gemäß den gesetzlichen Anforderungen informieren.

VH-AK-Mb-1311-1

Verbraucherhinweis gemäß § 43a Absatz 1 Nr. 12 TKG

IV. Reaktionen auf Bedrohungen und Schwachstellen im Einzelnen

Als Telekommunikationsunternehmen steht die htp GmbH vor der Herausforderung, auf eine Vielzahl von Bedrohungen und Schwachstellen angemessen reagieren zu müssen. Um diesen Herausforderungen gerecht zu werden, haben wir eine Reihe von Maßnahmen umgesetzt. Beispiele für solche Maßnahmen sind:

1. Die Einführung von neuen Produkten und IT-Systemen wird von Anfang an durch IT-Sicherheitsexperten betreut.
2. Unsere Lieferanten, Dienstleister und Auftragnehmer werden zur Einhaltung unserer Sicherheitsstandards verpflichtet.
3. Wir informieren uns laufend über veröffentlichte Sicherheitsschwachstellen und Missbrauchsfälle und sammeln solche Informationen selbst. Hierzu gehören beispielsweise der Erhalt/die Versendung ungewollter E-Mails (Spam), der Erhalte/die Versendung von E-Mails mit Malware (Viren/Würmer/Trojaner), Hackerattacken auf Computer und Fälle von Phishing. Diese Informationen verwenden wir, um mögliche Sicherheitsprobleme rasch und frühzeitig zu beheben.
4. Wir lassen regelmäßig die von uns eingesetzte Hard- und Software von Dritten überprüfen und überprüfen diese auch regelmäßig selbst, um mögliche Bedrohungen oder Schwachstellen frühzeitig zu erkennen und beheben zu können.

Geschäftsführer:
Dipl.-Wirt.-Ing. Thomas Heitmann
Dipl.-Ök. Karsten Schmidt

Amtsgericht: Hannover
HRB 55735
St.-Nr. 25/202/40207

Sparkasse Hannover
Hannoversche Volksbank
Deutsche Bank

IBAN DE86 2505 0180 0000 7177 11
IBAN DE45 2519 0001 0609 6077 00
IBAN DE13 2507 0070 0011 8505 00

BIC-Code (SWIFT) SPKHDE2HXXX
BIC-Code (SWIFT) VOHADE2HXXX
BIC-Code (SWIFT) DEUTDE2HXXX