Verbraucherhinweise Telekommunikation gemäß § 43a Absatz 1 Nr. 12 TKG

Reaktion auf Sicherheits- oder Integritätsverletzungen sowie auf Bedrohungen und Schwachstellen

Stand: 28.06.2021

1 Einleitung

Die Sicherheit des Telekommunikationsangebots ist der MAINGAU Energie GmbH (im Folgenden „MAINGAU“) ein wichtiges Anliegen. Um angemessen auf bestehende oder potenzielle Sicherheits- und Integritätsverletzungen bzw. auf Bedrohungen und Schwachstellen reagieren zu können, sieht die MAINGAU zahlreiche organisatorische und technische Maßnahmen vor.

Sofern Plattformen, Netzelemente und Systeme zur Abwicklung des Datenverkehrs von Telekommunikationsprodukten von der MAINGAU selbst betrieben werden, werden diese – im Rahmen der technischen Möglichkeiten – gemessen und kontrolliert. Diese Überwachung erfolgt unter Zuhilfenahme marktüblicher Netzwerküberwachungssysteme. Die eingesetzten Überwachungssysteme liefern regelmäßige Informationen zur Auslastung und Performance der beteiligten Netzelemente und Übertragungsstrecken. Anhand dieser Informationen kann die MAINGAU im Bedarfsfall geeignete Maßnahmen zur Vermeidung einer Kapazitätsauslastung oder Überlastung einer Netzwerkverbindung einleiten.

Soweit Plattformen, Netzelemente und Systeme zur Abwicklung des Datenverkehrs von Telekommunikationsprodukten von Dritten betrieben werden, wurden mit diesen Unternehmen Service Level Agreements vereinbart, die eine den von der MAINGAU vertriebenen Produkten entsprechende Dienstqualität des von diesem Drittunternehmen abgewickelten Datenverkehrs sicherstellen sollen. Um die Einhaltung dieser Service Level Agreements gewährleisten zu können, wurden die Drittunternehmen von der MAINGAU verpflichtet, durch geeignete technische und organisatorische Maßnahmen sicher zu stellen, dass die in den vereinbarten Service Level Agreements verankerte Dienstqualität erfüllt wird.

Weitere Hinweise zum Thema Datenschutz und Datensicherheit finden Sie auch unter www.maingau-energie.de/datenschutz.

2 Sicherheitsorganisation und Sicherheitsrichtlinien

Die Sicherheitsorganisation der MAINGAU folgt definierter Sicherheitsrichtlinien.

An der Spitze des Regelungsrahmens stehen bei der MAINGAU die internen IT-Sicherheitsrichtlinien. Der IT-Sicherheitsbeauftragte sowie der Datenschutzbeauftragte sind darüber hinaus feste Bestandteile der internen Sicherheitsorganisation.

Durch themenspezifische Richtlinien werden allgemeine Vorgaben konkretisiert, um ein angemessen hohes Sicherheits- und Datenschutzniveau zu gewährleisten.
Im Rahmen der Bearbeitung von Hinweisen und Beschwerden von Kunden und Mitarbeitern wird in regelmäßigen Abständen untersucht, ob Systeme, Prozesse und Organisationen tatsächlich die Anforderungen und Richtlinien erfüllen. Audits werden sowohl von internen als auch von externen Stellen, wie z. B. im Fall von Penetrationstests, durchgeführt.

Um Verbesserungspotentiale aufzudecken, prüft die MAINGAU ihren Sicherheits- und Datenschutzstandard regelmäßig.

3 Reaktionen auf Bedrohungen und Schwachstellen

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

1. Die Einführung von neuen Produkten und IT-Systemen wird hinsichtlich aktueller IT-Sicherheitsstandards bewertet.

2. Lieferanten, Dienstleister und Auftragnehmer werden zur Einhaltung von Sicherheitsstandards verpflichtet.

3. Die MAINGAU informiert sich laufend über veröffentlichte Sicherheitsschwachstellen und Missbrauchsfälle und sammelt solche Informationen selbst. Hierzu gehören beispielsweise der Erhalt/die Versendung ungewollter E-Mails (Spam), der Erhalt/die Versendung von E-Mails mit Malware (Viren/Würmer/Trojaner), Hackerattacken auf Computer und Fälle von Phishing. Diese Informationen verwendet die MAINGAU, um mögliche Sicherheitsprobleme rasch und frühzeitig zu beheben.

4. Zur Sicherstellung der Abwehr etwaiger Bedrohungen durch Eindringen unbefugter Dritter in die Geschäftsräume und zur Vermeidung von Angriffen auf die technischen Einrichtungen der MAINGAU sind diverse Zutrittsbeschränkungen und Sicherheitsmechanismen eingerichtet.

4 Reaktionen auf Sicherheits- und Integritätsverletzungen

Die MAINGAU Energie GmbH hat technische und organisatorische Maßnahmen umgesetzt, um auf Sicherheits- oder Integritätsverletzungen reagieren zu können. Beispiele für solche Maßnahmen sind:

1. Vorfälle mit Sicherheitsrelevanz oder mit Kundendatenbezug werden 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.

3. Die Systeme der MAINGAU werden rund um die Uhr, an 365 bzw. 366 Tagen im Jahr, beobachtet, damit eine rasche Reaktion auf akute Sicherheits- oder Integritätsverletzungen jederzeit möglich ist.

4. Für den Fall, dass die MAINGAU die Verletzung der Sicherheit oder Integrität von Kundendaten feststellt, werden diese Kunden gemäß den gesetzlichen Anforderungen informiert.

MAINGAU Energie GmbH, Postfach 1209, 63179 Obertshausen
Handelsregister: AG Offenbach/Main HRB 12523