Ein Produkt von congstar

congstar Services GmbH
Sicherheitsverfahren

Information über die Arten von Maßnahmen, mit denen die Telekom auf Sicherheits- oder Integritätsverletzungen sowie auf Bedrohungen und Schwachstellen reagieren kann

Die Sicherheit des Angebots unserer Telekommunikationsdienste ist der Deutschen Telekom ein wichtiges Anliegen. Um unseren Kunden sichere Services zur Verfügung stellen zu können, sehen wir eine Reihe von Maßnahmen vor. Das Fundament unserer Maßnahmen ist unsere Organisation, mit der wir die Sicherheitsgovernance im Konzern gewährleisten. Sie bietet die organisatorische Grundlage, um angemessen mit bestehenden oder potentiellen Schwachstellen und Bedrohungen umzugehen. Zu diesem Zweck entwickelt die Deutsche Telekom unter anderem das konzernweite Sicherheitsmanagementsystem ständig fort.

Wesentlicher Teil des Sicherheitsmanagementsystems ist neben dem Datenschutz der Bereich Zentrales Sicherheitsmanagement der Deutschen Telekom. Er regelt das Zusammenspiel aller Funktionen im Konzern, die Sicherheit gewährleisten. Das Zentrale Sicherheitsmanagement hat die Zertifizierung nach ISO 27001 erhalten und erfüllt damit die wichtigsten internationalen Standards. Das Sicherheitsmanagement wird kontinuierlich weiterentwickelt. Unter anderem wurde mit der Konzernrichtlinie Sicherheit ein konzernweit einheitliches, verpflichtendes Regelwerk geschaffen, das die sicherheitsrelevanten Grundsätze des Konzerns regelt und harmonisiert.

Die Deutsche Telekom als größter Anbieter von Kommunikationsdienstleistungen in Deutschland ist ein beliebtes Ziel von Hackerattacken, die immer wieder neue Herausforderungen mit sich bringen. Das Unternehmen reagiert auf diese Herausforderungen mit Hilfe eines Frühwarnsystems, das darauf abzielt, Informationen über Angreifer zu ermitteln, neue Angriffe zu erkennen und bessere Abwehrstrategien zu entwickeln. Grundsätzlich gilt, dass ein Frühwarnsystem umso besser ist, je mehr Datenquellen und Datenmaterial für die Analysen zur Verfügung stehen. Schon bei der Konzeption wurden die strengen rechtlichen Maßstäbe von Fernmeldegeheimnis und Datenschutz berücksichtigt. Mit dem Aufbau des Frühwarnsystems wird ein speziell an den Risiken und Bedürfnissen des Unternehmens orientiertes Bild der Sicherheitslage im Internet generiert. Ziel ist es, mit Hilfe der selbst gewonnenen Informationen und deren Zusammenführen mit den allgemein verfügbaren Herstellerinformationen die Kunden sowie vertrauliche Daten der Deutschen Telekom bestmöglich vor Gefahren im Internet zu schützen. Weiterhin wird es damit möglich, frühzeitig Anpassungsbedarfe der Sicherheitsmechanismen zu erkennen und diese zu implementieren.
Das Computer Emergency Response Team (CERT) der Deutschen Telekom betreibt ein international ausgerichtetes Management bei Sicherheitsvorfällen für alle Informations- und Netzwerktechnologien des Konzerns Deutsche Telekom. Es bildet eine zentrale Anlaufstelle für die Meldung von Vorfällen und etabliert Mechanismen zur Früherkennung von Angriffen auf intern und extern erreichbare Systeme.
Weitere Hinweise zum Thema Datenschutz und Datensicherheit finden Sie auch unter
https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit