IT-Sicherheitsleitlinie

Motivation

Diese Sicherheitsleitlinie beschreibt die Positionierung der Informationssicherheit (IT-Security) bei HOCHTIEF. Die Leitlinie bezieht sich auf eigene Tätigkeiten, macht aber auch deutlich, welchen Anspruch HOCHTIEF bei Geschäftspartnern ansetzt.

Die Konzernstrategie setzt auf ein umfassendes Risikomanagement. Für die Unterstützung der Geschäftsaufgaben von HOCHTIEF ist die Informationstechnik (IT) ein wesentlicher Bestandteil. Aus diesem Grund wird der Sicherheit der IT-Systeme und der Daten ein sehr hoher Stellenwert beigemessen.

1. Sicherheitsziele

Die Erzielung eines angemessenen Sicherheitsniveaus beim Einsatz der IT-Security durch technische und organisatorische **Sicherheitsmaßnahmen** ist nicht nur durch Rechtsvorschriften bestimmt, sondern auch Teil der Verpflichtungen gegenüber den Kunden und Geschäftspartnern von HOCHTIEF sowie dem Schutz der eigenen Interessen. Die Sicherheit beim Einsatz der Informationstechnik liegt somit im Interesse aller Parteien und wird damit zu einer wichtigen Zielvorgabe für HOCHTIEF.

Die zu erreichenden Ziele sind dabei insbesondere:
- Einhaltung gesetzlicher und vertraglicher Verpflichtungen
- Einhaltung interner und externer Vorgaben (Compliance)
- Schutz vor Zugriff durch nicht autorisierte Personen
- Schutz vor Manipulation der Daten
- Angemessene Verfügbarkeit der Daten und Systeme

Gesetzliche Vorgaben nach § 91 Abs. 2 AktG:
„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

2. Sicherheitsmaßnahmen

Zur Erreichung der definierten Sicherheitsziele werden folgende Maßnahmen umgesetzt:

- Etablierung und Aufrechterhaltung eines **IT-Sicherheitsmanagements**
- Definierte Vorgehensweise zur Konzeption, Implementierung und Aktualisierung einer risikogerechten und wirtschaftlich angemessenen **IT-Security-Policy**
- Kommunizierte Prozesse zu **Risiko-Evaluierungen bei Ausnahmeanträgen**

2.1. IT-Sicherheitsmanagement

Die Planung, Umsetzung und Aufrechterhaltung der IT-Sicherheit wird durch die IT-Sicherheitsorganisation sichergestellt, die den Vorstand unterstützt. Die IT-Sicherheitsorganisation besteht aus

- dem Chief Information Security Officer (CISO) der HOCHTIEF Aktiengesellschaft und
- den CISOs der Divisions (CISO Divisions).

Der IT-Sicherheitsorganisation werden ausreichende finanzielle Mittel und zeitliche Ressourcen zur Verfügung gestellt, um ihre Informationssicherheitsaufgaben ordnungsgemäß durchführen zu können.

Damit innerhalb der Organisation alle Stellen im Sinne des Vorstandes das Thema IT-Sicherheit vorantreiben, delegiert der Vorstand die Umsetzungsverantwortlichkeit an die Divisions (IT-Security-Policy als Teil der IT-Richtlinie).

Innerhalb der Divisions ist die IT-Security Teil der einzelnen IT-Steering-Committees. Die IT-Steering-Committees setzen sich aus Vertretern der Geschäftsleitungen und der operativen IT zusammen.

2.2. IT-Security-Policy

Der CISO erstellt eine IT-Security-Policy, welche angemessene und wirksame Sicherheitsmaßnahmen beschreibt. Anhand der gesetzlichen und geschäftlichen Rahmenbedingungen, der Bedrohungslage und der aktuell technischen Möglichkeiten aktualisiert der CISO die IT-Security-Policy bedarfsgerecht. Die in der IT-Security-Policy definierten **Maßnahmen** sind jeweils einer der beiden Schutzstufen „normal“ bzw. „hoch“ zugeordnet.

Die Divisions stellen sicher, dass die IT-Security-Policy innerhalb ihrer Division ggf. konkretisiert, kommuniziert und umgesetzt wird. Zudem sind **Sicherheitsvorfälle** dem CISO bzw. CISO Division zu melden.

Alle Mitarbeiter sind gemäß ihres Anstellungsvertrags auf die Einhaltung der Richtlinien bei HOCHTIEF verpflichtet. Die Führungskräfte stellen die Einhaltung und Umsetzung sicher.

Die Fachbereiche der HOCHTIEF Aktiengesellschaft und der Divisions ermitteln für die in ihrem Verantwortungsbereich befindlichen Informationen anhand eines Fragenkataloges den Schutzbedarf („normal“ oder „hoch“). Auf Basis des Schutzbedarfs setzen die Fachbereiche die Sicherheitsmaßnahmen aus der IT-Security-Policy um.

Beabsichtigte oder grob fahrlässige Handlungen, die die Sicherheit von Daten, Informationen, Anwendungen, IT-Systemen oder Netze gefährden, werden als Verstöße verfolgt und können durch disziplinarische oder arbeitsrechtliche Maßnahmen geahndet werden.

Sollten aus der betrieblichen Aufgabenstellung Anforderungen resultieren, welche der bestehenden IT-Security-Policy widersprechen, so dürfen diese nicht ohne vorherige Begutachtung umgesetzt werden und bedürfen einer **Risikoevaluierung** in Form eines Ausnahmeantrags.

2.2.1. Maßnahmen

Die aktuell gültigen Maßnahmen sind in der IT-Security-Policy detailliert beschrieben bzw. in einer Dokumentation der IT-Sicherheitskonzepte vereinfacht dargestellt.

2.2.2. Meldung von Sicherheitsvorfällen

Sicherheitsrelevante Vorfälle sind umgehend über die vorgesehenen Meldewege zu melden und umgehend zu untersuchen. Die daraus resultierenden Erkenntnisse werden ggf. in den Sicherheitszielen oder der IT-Security-Policy berücksichtigt.

2.2.3. Risikoevaluierung

Über einen Ausnahmeantrag kann die Fachabteilung Abweichungen von der IT-Security-Policy beantragen. Auf Basis der Angaben der Fachabteilung sowie einer technischen Beschreibung wird durch den CISO oder CISO Division eine Evaluierung von Risiko und Eintrittswahrscheinlichkeit durchgeführt. Nur nach positiver Genehmigung des Ausnahmeantrags durch den CISO oder CISO Division ist eine Umsetzung erlaubt.