WIKIPEDIA

Chief Information Security Officer

Ein **Chief Information Security Officer** (**CISO**) bezeichnet die Rolle des Gesamtverantwortlichen für Informationssicherheit in einer Organisation. Die Aufgaben variieren in der Praxis je nach Bedürfnis der Firma, die diese Rolle ausschreibt und besetzt, sie können aber auch von den einschlägigen Normen zur Informationssicherheit abgeleitet werden.

Aufgaben

Bei kleineren Organisationen oder für Verantwortliche von Teilbereichen innerhalb einer größeren Organisation entfällt ggf. das "Chief" und es wird die Bezeichnung **Information Security Officer** ("ISO", nicht zu verwechseln mit der Bezeichnung für Normen und Standards) oder **Informationssicherheitsverantwortlicher**, sowie **Informationssicherheitsbeauftragter** (**ISB**) verwendet. Mitunter kommt auch die irreführende Bezeichnung **Leiter IT-Sicherheit** vor. IT-Sicherheit ist aber nur ein Teilaspekt der **Informationssicherheit**.

Der CISO nimmt sich meist der folgenden Aufgaben an:

- Etablierung eines Managementsystems zur Informationssicherheit (ISMS – Information Security Management System)
- Erarbeitung von Schutzzielen für die unternehmenskritischen Werte (Assets), deren Bedrohungen und ihren Risiken und den aus der IS Strategie abgeleiteten Sicherheitszielen.
- Durchführung von Risikoassesments und Business Impact Analysen
- Aufbau und Betrieb einer Organisationseinheit zur Umsetzung der Sicherheitsziele abgeleitet von der IS Strategie
- Ausarbeitung, Anpassung von Sicherheitsrichtlinien und Sicherheitsvorgaben
- Auditierung der Funktionseinheiten zum Stand der Umsetzung und Weiterentwicklung der Sicherheitsvorschriften
- Bewusstsein der Mitarbeiter für Informationssicherheit durch Trainings und Kampagnen schaffen
- Aufstellen von Richtlinien, Vorgaben und Zielen für die Informationssicherheit
- Durchführung von Trainings und Awarenesskampagnen zur Informationssicherheit
- Sicherstellung der Einhaltung datenschutzrechtlicher Vorgaben
- Portfolio-Management der sicherheitsrelevanten Geschäftsprozesse
- Kontinuierliche Analyse und Optimierung der Informationssicherheit im Unternehmen
- Abstimmung mit und Etablierung der Informationssicherheit bei den Stakeholdern und der Konzern-/ Unternehmensleitung

Der **CISO ist meist nicht dem** Chief Information Officer (**CIO**) **unterstellt**, der Berichtsweg findet oft direkt zum Chief Executive Officer (CEO) statt, **da die IT-Sicherheit nur eine Untermenge der Aufgaben eines CISO darstellt**, und es um die Sicherung und das Risikomanagement *aller* Informationswerte (Assets) eines Unternehmens geht (also z. B. auch Aktenordner/Papier).

Idealerweise erfolgt die Funktionstrennung so, dass die IT-Abteilung bzw. der/die Leiter(in) der IT-Sicherheit eine Art interner Lieferant darstellen, während die Anforderungsseite durch den/die (C)ISO – im Auftrag der Geschäftsführung – dargestellt wird. Im Rahmen eines Information Security Management System (ISMS) auditiert der (C)ISO ggf. die IT-Lieferseite und berichtet über die Ergebnisse an die Geschäftsführung. In kleineren Unternehmen, aber auch in vielen größeren Unternehmen ohne ISMS bzw. mit geringem Reifegrad bzgl. der Informationssicherheit, werden all diese Funktionen aber möglicherweise abweichend definiert oder weniger streng getrennt.

Wesentliche Arbeitsgrundlagen für den CISO stellen im Regelfall die ISO/IEC 27000-Reihe sowie der IT-Grundschutz dar.

Weblinks

- eccouncil.org/... (https://www.eccouncil.org/ciso/about-us) – Aufgabenbeschreibung