CISO und IT-SiBE sind das Gleiche. Oder doch nicht?

Aktuell suchen viele Firmen nach einem CISO. Doch was wird genau unter CISO verstanden? Und was macht ein IT-Sicherheitsbeauftragter (IT-SiBe)? Dieser Beitrag zeigt auf, was die Unterschiede zwischen einem CISO und einem IT-SiBe sind, warum es beide benötigt und wie diese Funktionen in ein Unternehmen integriert werden können.

Notwendige Rollen

In jedem Unternehmen gibt es Anforderungen an die Informationssicherheit. Diese müssen durch entsprechende (Fach-) Personen umgesetzt werden. Dabei wird klassisch zwischen CISO, IT-SiBe und allenfalls einem Schulungsverantwortlichen unterschieden. Auch wenn in der Literatur die Rollen CISO und IT-SiBe oft identisch behandelt werden, gibt es doch grosse Unterschiede, die es zu berücksichtigen gilt.

Die Funktion eines CISO wird benötigt, um die Aufsicht über alle Sicherheitsaspekte sicherzustellen. Die Funktion wird bewusst «Abteilungsneutral» positioniert, damit auf kurzen Kommunikationswegen bis hinauf zum VR zurückgegriffen werden kann. Je nach Struktur kann der CISO direkt dem VR oder der GL angehängt sein. Er ist in seinem Themengebiet weisungsbefugt. Der/Die CISO arbeitet dabei eng mit dem CIO zusammen, damit ICT- und Sicherheits-Strategie optimal aufeinander abgestimmt sind.

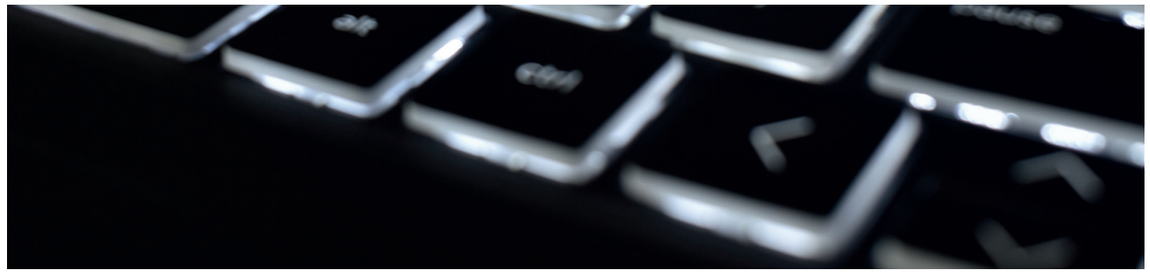
Ein IT-SiBe wird benötigt, um alle technischen Umsetzungen im Bereich Security zu koordinieren und zu begleiten. Während der IT-SiBe mitarbeitet, darf der CISO dies nicht tun (4-Augen-Prinzip, Seperation of Duties). Damit ist diese Rolle der verlängerte Arm der CISO-Funktion, ist aber ein Teil des ICT-Teams. Idealerweise wird die Funktion dem CIO unterstellt, damit auch hier die Kommunikationswege kurz sind.

Aufgaben

Damit die Rollen noch etwas klarer unterschieden werden können, kann auf die folgenden Aufgaben und Verantwortlichkeiten zurückgegriffen werden.

CISO

- Ist verantwortlich für die ICT-Sicherheit gegenüber der GL und VR
- Ist verantwortlich für die Aktualisierung des ISMS (InformationsSicherheitsManagementSystem) und den notwendigen Dokumenten
- Ist verantwortlich für alle Aufgaben und Termine, welche für die Aufrechterhaltung einer möglichen ISO 27001 Zertifizierung notwendig sind
- Erstellt und betreut selbstständig die Security-Strategie und daraus entstehende Konzepte (Genehmigung erfolgt durch GL / VR)
- Erstellt und aktualisiert selbstständig Security Policies und vertritt diese vor der GL / VR
- Leitet und überwacht die Umsetzung der Richtlinien (Policies)
- Begleitet das Risikomanagement bei den Themen Informationssicherheit, IT und teilweise Datenschutz
- Ist für die korrekte Behandlung von Informationssicherheits vorfällen zuständig
- Arbeitet eng mit der für den Datenschutz verantwortlichen Person (intern oder extern) zusammen
- Koordiniert, wo nötig, die Zusammenarbeit mit Externen (Lieferanten, Partner, etc.) und führt risikobasierte Lieferanten-Audits durch
- Überprüft die Einhaltung von Strategie, Konzepten, Richtlinien und Weisungen
- Entscheidet über Sicherheitsfragen
- Beurteilt Kontrollen auf andere Effektivität und Wirksamkeit
- Nimmt Einsitz in ICT-Projekten (Bewertung aus Sicht der Informationssicherheit)



IT-SiBe

- Arbeitet eng mit dem CISO zusammen und überwacht in seinem Auftrag die technische Umsetzung der Informationssicherheit
- Kennt die technische Infrastruktur sehr gut
- Berät in seiner Funktion das ICT-Team und unterstützt sie bei der Umsetzung von (technischen) Strategie und Konzepten
- Bringt Lösungsvorschläge für gefundene Schwachstellen
- Berät nach Bedarf die IT und die GL in ICT-Sicherheitsbelangen
- Führt (technische) Kontrollen durch
- Erstellt (im Auftrag) Konzepte und Weisungen (in der Regel auf Stufe ICT)
- Ist direkt dem CIO unterstellt

Schulungsverantwortlicher

- Deckt das gesamte Schulungsbedürfnis des Unternehmens im Bereich Informationssicherheit ab (evtl. ergänzt mit Datenschutzthemen)
- Klärt mit dem CISO und/oder IT-SiBe jährlich Themen und Bedürfnisse
- Sorgt für eine abwechslungsreiche und wirksame Schulungen für alle Mitarbeitenden
- Nutzt alle verfügbaren Kanäle für die Schulungen

Wie die obenstehende Aufzählung zeigt, ist der CISO mehrheitlich für die organisatorischen Themen, für Vorgaben und Beurteilungen zuständig, während der IT-SiBe sich um die technischen Aufgaben kümmert. Eine enge Zusammenarbeit ist wichtig, arbeiten die beiden doch Hand-in-Hand. Mit dieser Rollentrennung kann das gewünschte 4-Augen-Prinzip effektiv umgesetzt werden. Der IT-SiBe führt Kontrollen durch und hält die Resultate fest; der CISO beurteilt anschliessend die Resultate. Genügen die Informationen? Ist die Kontrolle effektiv und bringt dem Unternehmen auch einen Mehrwert? Kontrollen sind immer schnell und in einer grossen Anzahl eingerichtet, doch der Spruch «Wer misst, misst Mist» gilt auch hier. Die Auswahl geeigneter Kontrollen und damit abgeleitet sinnvolle KPIs ist die Aufgabe des CISO.

Fazit

Die Anforderungen an die Informationssicherheit werden immer aufwendiger umzusetzen. Systeme werden vernetzter, vermehrt werden Dienste aus der Cloud genutzt, die Mitarbeitenden sind mobiler, im Home-Office, unterwegs oder im Büro. Um diesen Bedürfnissen gerecht zu werden, benötigt es strategische Vorgaben. Diese werden durch den CISO definiert und von der Geschäftsleitung freigegeben. Der IT-SiBe kümmert sich um alle Belange der technischen Umsetzung, der Überwachung von Netzwerken und Systemen sowie deren Kontrolle. Nur einem eingespielten Team gelingt es, alles optimal abzudecken.

AndreasWisler
Inhaber, Dipl. Ing FH
CISA, CISSP, ISO 22301 + 27001 + 27701 Lead Auditor