Control 3.1.1 Inwieweit werden Sicherheitszonen für den Schutz von Informationswerten gemanagt?

Eine der SOLLTE-Anforderungen dieses Controls lautet:

„Verfahren zur Vergabe und zum Entzug von Zutrittsberechtigungen sind etabliert."

Viele Unternehmen erläutern in diesem Zusammenhang den Onboarding-Prozess von neuen Mitarbeitern. Oftmals existieren dafür Laufzettel, Checklisten in der Personalabteilung oder sogar ticketbasierte Workflows. Die Verantwortlichkeiten für die erstmalige Erteilung von Zutrittsrechten sind zumeist in Person des Fachvorgesetzten oder des Firmeninhabers bei kleineren Unternehmen definiert. Die Dokumentation der Zutrittsberechtigungen erfolgt oft in Schlüsselbüchern oder auch in der Software eines Zutrittsberechtigungssystems.

Werden erweiterte Zutrittsrechte benötigt, wird zumeist ein (Genehmigungs-) Prozess über den Vorgesetzten gestartet und die Rechte anschließend in einem Tool gesetzt bzw. ein entsprechender Schlüssel ausgegeben. Dieser Prozess funktioniert in den meisten Unternehmen sehr gut, denn erfolgt diese Erweiterung nicht, so könnte der Mitarbeiter unter Umständen nicht arbeiten. Ein Zustand, welcher in jedem Unternehmen zumeist schnell gelöst wird.

Wird das Thema Entzug von Zutrittsberechtigungen thematisiert, so wird in der Regel der Off-Boarding-Prozess erläutert. Auf Basis der Eintrittschecklisten, Schlüsselbücher etc. wird der Ausgabeprozess rückabgewickelt.

Soweit so gut. Und trotzdem hat der Auditor jetzt noch eine Frage…

Ein häufiger Kritikpunkt von Auditoren zu diesem Thema ist die mangelnde Durchführung (bzw. auch fehlende Dokumentation) von Inventuren der Zutrittsrechte. Und zwar Inventuren, die durch den Verantwortlichen für die entsprechende Sicherheitszone durchgeführt werden. Die umsetzenden Stellen (oft HR, IT oder Facility-Management) verwalten zwar die Zutrittsrechte, können aber deren Notwendigkeiten in der Regel gar nicht beurteilen.

Erfolgen diese Inventuren nicht und gibt es beispielsweise in elektronischen Systemen keinen Sperrautomatismus, behalten Mitarbeiter ihre einmal erteilten Zutrittsrechte. Projektwechsel, Wechsel in andere Abteilungen oder Jobrotation, wie oft bei Auszubildenen der Fall, werden unter Umständen nicht berücksichtigt.

Gehen Sie davon aus, dass ein guter Auditor nach Nachweisen für die regelmäßige Überprüfung von Zutrittsrechten fragt. Etablieren Sie einen entsprechenden Prozess und dokumentieren Sie die Durchführung! Erst dann sind die geforderten Verfahren zur Vergabe und zum Entzug von Zutrittsberechtigungen wirklich etabliert.