Control 4.1.1: Inwieweit ist der Umgang mit Identifikationsmitteln gemanagt?

Auch wenn in den Punkten 4.1.2 bis 4.2.1 die Einhaltung des Minimalitätsprinzips ("Need-to-know") explizit nur für Zugriffe auf IT-Systeme (Authentifikation / Autorisierung) gefordert wird, muss es selbstverständlich sein, dass sinnvolle Regelungen auch für Zutritte zu physischen Bereichen am Standort gelten.

Diese eigentlich unkomplizierte Anforderung wird trotzdem von vielen Unternehmen oftmals nicht ausreichend betrachtet. Unternehmen sollten sich immer bewusst darüber sein, welchen Personen entsprechende Zutrittsrechte zu Räumen oder Gebäudeteilen gewährt sind. Aufschluss hierüber gibt der dokumentierte Schließplan für Schlüssel oder auch elektronische Schließung, wie beispielsweise Transponder oder Zutrittskarten.

Ein besonderes Augenmerk fällt auf organisationsfremde Personen, wie Reinigungskräfte, Sicherheitskräfte oder teilweise auch Hausverwaltungen. Reinigungskräfte sollten - wenn immer möglich - während der Arbeitszeit und unter Aufsicht reinigen. Eine Reinigung vor oder nach der Arbeitszeit ist möglich, soweit sichergestellt ist, dass im Unternehmen definierte Clean Desk Regelungen umgesetzt sind und die Umsetzung durch die Mitarbeiter auch ausreichend durch z.B. interne Audits überprüft wurde. Die Arbeitsplätze sollten also aufgeräumt und Medien mit vertraulichen Informationen (Papiere, Dokumente, mobile Datenträger etc.) in geeigneten Schränken verschlossen sein.

Häufig wird in Audits festgestellt, dass Generalschlüssel an Reinigungskräfte, die Hausverwaltung oder die Sicherheitsfirma ausgegeben wurden. Dem Unternehmen muss für diese Fälle bewusst sein, dass damit die Möglichkeit eines uneingeschränkten Zutritts Tag und Nacht besteht und somit ein physischer Zugriff auf Informationen (ggf. Server- oder Technik, Büros der Geschäftsführung, Entwicklungsbereiche, Maschinen etc.) möglich ist.

Bei der Ausgabe von Generalschlüsseln wird häufig als Argument die „Notwendigkeit in Notsituationen" begründet. I.d.R. kann eine Aushändigung jedoch oft zweckgebunden und versiegelt (z.B. als versiegelter Umschlag oder im Innenbereich, hinterlegt in einem „Einschlagkasten") erfolgen.

Der Abschluss einer Geheimhaltungsvereinbarung schützt nicht ausreichend vor Diebstahl und / oder Sabotage. Das externe Unternehmen sollte durch erweiterte Lieferantenbedingungen schriftlich verpflichtet sein, den Schlüssel niemals an Dritte weiterzugeben oder Kopien anzufertigen. Auch die "Versehrtheit" des Siegels sollte durch persönliche Sichtung ein fester Bestandteil der regelmäßigen Rechte-Prüfungen (Rechte-Inventur) sein. Restrisiken sind zu bewerten und schriftlich fixiert durch die Geschäftsleitung zu übernehmen, so dass die Sicherheitsverantwortlichen aus der Verantwortung entlastet sind.