Der Mensch im Fokus – Personalsicherheit

Im siebten Kapitel der ISO 27001 dreht sich alles um den Menschen. Dies beginnt für das Unternehmen bereits vor der Einstellung und endet, nachdem der Arbeitnehmende die Firma wieder verlassen hat.

Im ersten Schritt gilt es, bereits im Bewerbungsprozess Sicherheitsprüfungen vorzunehmen. Dies muss aber immer in Einklang mit geltenden Gesetzen, dem Datenschutz sowie der Privatsphäre erfolgen. Wichtig sind aber die Kontrolle des Leumunds, die Vollständig- und Richtigkeit des Lebenslaufs wie auch die unabhängige Identitätsprüfung. Aus langjähriger eigener Audit-Tätigkeit kenne ich mehrere Unternehmen, die beim ersten Vorstellungsgespräch die Original-Zeugnisse verlangen, gegen 50 Prozent Absagen für dieses Gespräch erhalten. Weiter sollten die Referenzen auch mal angerufen werden. Auch hier stelle ich erschreckend fest, wie wenig dies gemacht wird. Ich wurde schon sehr oft als Referenz angefragt, wurde aber noch nie angerufen. Doch in diesem ersten Schritt kann bereits sehr viel geklärt werden, ohne die bewerbende Person nachteilig zu behandeln.

In wie weit auch ein Strafregister- und Betreibungsauszug verlangt werden darf, ist umstritten. Nicht in allen Bereichen ist es angebracht, diese Unterlagen zu verlangen. In einigen ist es aber fast Pflicht, zum Beispiel bei Firmen im IT-Sicherheitsbereich oder Finanzumfeld. Bei einem Audit werden auch Lücken entdeckt, die für ein Unternehmen unangenehme Folgen haben können. Die Vertraulichkeit ist dabei ein Muss-Kriterium für alle involvierten Personen.

Immer wieder hört man von Personalverantwortlichen, die die Bewerbenden im Internet googlen. Dies ist rechtlich sehr heikel. Es ist unbestritten, dass Xing und Linkedin beigezogen werden dürfen, da diese als Business-Plattformen gelten. Jedoch gehören Facebook, Instagram und Co. nicht dazu. Jedes Unternehmen sollte weiter im Vorfeld die vertraglichen Vereinbarungen erstellen. Darin sind auch die Verantwortlichkeiten zu definieren. Oft erfolgt zweiteres in einer Stellenbeschreibung. In der Vereinbarung sollten mindestens folgende Punkte geregelt sein:

- Vertraulichkeits- und/oder Geheimhaltungsvereinbarung
- Gesetzliche Verantwortlichkeiten und Rechte bezüglich Urheberrecht und Datenschutz
- Einhaltung der Klassifizierungsvorschriften (mehr dazu in der nächsten Ausgabe)
- Umsetzen der Firmenrichtlinien und Weisungen
- Hinweis auf den Disziplinarprozess bei Missachtung dieser Regeln

Während der Beschäftigung

Die Norm fordert unmissverständlich, dass alle Mitarbeitenden die Informationssicherheit im Einklang mit den eingeführten Richtlinien und Verfahren der Organisation umzusetzen haben. Dazu gilt es entsprechende Rollen zu definieren, inklusive den gestellten Anforderungen, den Pflichten, wie auch den Rechten, die diese Rolle mit sich bringt. Ein Unternehmen sollte auch viel dafür tun, dass sich Mitarbeitende regelmässig in ihrem Bereich, wie auch in der Informationssicherheit weiterbilden. Dabei geht die Geschäftsleitung mit gutem Vorbild voraus. Weiter verlangt die Norm die Möglichkeit, anonym über Verletzungen der Informationssicherheit zu berichten («whistle blowing»). Dies ist aber in kleinen und mittleren Unternehmen nur schwierig umzusetzen. Ich bevorzuge eine offene Fehlerkultur. Fehler können auftreten. Aus diesen kann immer gelernt werden. Werden diese aber verschwiegen, kann nicht davon profitiert und entsprechende (Gegen-)Massnahmen ergriffen werden.

Der zweite Punkt im Kapitel 7.2 verlangt eine regelmässige Awareness in Bezug auf die Informationssicherheit. Das Unternehmen muss dazu ein Programm erarbeiten, wann, wie und warum alle sensibilisiert werden. Die Gefahren durch Phishing-Angriffe, Viren wie Ransomware, Datendiebstahl und weitere haben in den letzten Monaten stark zugenommen. Die Mitarbeitenden müssen wissen, wie sie solche Gefahren erkennen und richtig reagieren können. Auch müssen die Richtlinien und Weisungen im Unternehmen sowie der eigene Beitrag dazu bekannt sein. Darauf sollte regelmässig hingewiesen werden. Dies kann nicht nur durch (Frontal-)Schulungen erfolgen. Web Based Trainings (manchmal auch Computer Based Trainings genannt), Videos, Informationsseiten, Newsletter, Plakate, Quiz und andere Möglichkeiten sollten genutzt werden. Möchte man dies nicht selbst machen, da der Aufwand doch sehr gross ist, stehen im Internet verschiedene Firmen zur Auswahl, die dies auch im Abo anbieten (zum Beispiel mein Unternehmen, Infos sind unter www.goAware.ch zu finden).

Bild: Archiv

Zutritt- und Zugriffsrechte sind nach einem definierten Ablauf zu entziehen.

Der dritte Punkt hat den unschönen Namen «Massregelungsprozess» bekommen. Ich bevorzuge den Begriff Disziplinarwesen, wie er im Entwurf der Norm zu finden war. Das Unternehmen muss sich bereits vor dem ersten Vorfall überlegen und schriftlich definieren, wie mit Verstössen gegen die Richtlinien und Weisungen vorgegangen wird. Es gilt sicherzustellen, dass alle Betroffenen identisch behandelt werden. Ein solcher Prozess sollte nie ohne genaue Prüfung gestartet werden. Je nach Schweregrad kann folgendes Vorgehen sinnvoll sein:

- Mitarbeitergespräch: es wird auf das Fehlverhalten hingewiesen und Massnahmen definiert, dass dies nicht mehr vorkommt. Die Konsequenzen bei einem weiteren Fehlverhalten werden klar kommuniziert.
- Verwarnung: das Fehlverhalten sowie die getroffenen Massnahmen werden schriftlich festgehalten. Darin enthalten ist ein Zeitplan und klare Ziele. Alles wird im Personaldossier abgelegt.
- Abmahnung: letzte Chance für den Mitarbeitenden. Es wird nochmal darauf hingewiesen, dass das Verhalten so nicht akzeptiert wird und bei einem weiteren Verstoss die Kündigung erfolgt. Falls notwendig werden die Ziele und Massnahmen nochmals schriftlich definiert.
- Kündigung: haben die getroffenen Massnahmen keine Wirkung erzielt, muss gehandelt und die Kündigung ausgesprochen werden. Es empfiehlt sich, hier juristische Unterstützung beizuziehen.

Änderungen und Beendigung

Das dritte Kapitel (7.3) beschreibt Änderungen und Beendigung der Beschäftigung. Das Unternehmen muss dazu einen Prozess definieren, wie Stellenänderungen (zum Beispiel eine andere Abteilung, eine neue Funktion) gehandhabt werden. Zugriffsrechte müssen allenfalls angepasst werden: neue bekommen, alte entfernen. Ein negatives Beispiel sind oft Lernende. Am Ende ihrer Ausbildung waren sie in allen Abteilungen und verfügen über Rechte in allen Abteilungen, da neue zwar dazu gekommen sind, die alten aber nicht entfernt wurden. Es könnte ja sein, dass diese nochmals benötigt werden. In verschiedenen Audits habe ich Lernende gesehen, die über mehr Rechte verfügten als der Chef des Unternehmens.

Bei einem Austritt müssen alle übergebenen Werte (Schlüssel, Batch, Handy, Laptop usw.) zurückgegeben werden. Zutritt- und Zugriffsrechte sind nach einem definierten Ablauf zu entziehen. Weiter gilt es zu regeln, wie E-Mails und Anrufe zu behandeln sind. Ohne Rückfrage E-Mails an eine weitere Person weiterzuleiten kann rechtlich heikel sein. Ganz wichtig ist, beim Austritt nochmals auf die Vertraulichkeits- und Datenschutzbestimmungen hinzuweisen. Diese gelten auch nach Beendigung des Arbeitsverhältnisses weiter.

Das Kapitel A.7 der ISO-Norm beschäftigt sich mit der Sicherheit beim Personal. Dies beginnt bereits vor der Anstellung und dauert bis zur Beendigung. Mit den erwähnten Vorgaben kann die Informationssicherheit beim oft als schwächstes Glied der Informationssicherheitskette bezeichneten Menschen erhöht werden.

INFOS | KONTAKT

goSecurity GmbH
Schulstrasse 11
CH-8542 Wiesendangen

T +41 (0)52 511 37 37
www.goSecurity.ch
wisler@gosecurity.ch