**FOKUS: SECURITY**

# Alles eine Frage der Organisation

Bei jedem Sicherheitsvorfall kommt es auf die schnelle und richtige Reaktion an. In der Praxis krankt es aber oft gar nicht an den Security-Massnahmen, sondern an deren Organisation.

→ **VON CHRISTOPH BAUMGARTNER**

Je komplexer und flexibler die IT-Infrastruktur eines Unternehmens, umso wichtiger werden klare Sicherheitsvorgaben und entsprechende Prozesse – oder auf Neudeutsch: ein Information Security Management System (ISMS). Ein ISMS muss jedoch nicht zwangsläufig Software-gestützt sein, es kann auch aus Dokumenten und gelebten Prozessen bestehen. Im Normen-Framework ISO/IEC 270xx wird ein solches ISMS definiert. Eine wichtige Anforderung des ISO-Frameworks hinsichtlich der Sicherheitsorganisation ist dabei die Gewaltenteilung (segregation of duties). Doch wie lässt sich dies im eigenen Unternehmen umsetzen?

## GEWALTENTEILUNG

Die sicherheitsbezogenen Aufgaben (Tasks) müssen auf unterschiedliche Rollen im Unternehmen aufgeteilt werden:

Die Geschäftsleitung zeichnet verantwortlich für alle Prozesse im Unternehmen. Somit ist sie auch für die Information Security zuständig. Aus Praktikabilitätsgründen delegiert die Geschäftsleitung oft die Betreuung der Information Security an den Chief Information Officer (CIO). Der IT-Sicherheitsbeauftragte oder Chief Information Security Officer (CISO) verfasst und pflegt im Auftrag der Geschäftsleitung die IT Security Policy und sichert deren Einhaltung im Unternehmen. Das Linienmanagement unterstützt bei der operativen Umsetzung.

**Christoph Baumgartner** ist CEO & Inhaber der auf IT Security Consulting spezialisierten OneConsult GmbH

Die Vertreter des Business aus den Produktionsabteilungen des Unternehmens (System, Application bzw. Process Owner) definieren die Vorgaben punkto Funktionalität, Leistungsanforderungen, Zugriffsberechtigungen etc. und führen die zugehörigen Risikoanalysen durch.

Die Security Engineers oder System Security Officers (SSO) wiederum implementieren Sicherheitskomponenten und -funktionalitäten, und die System Operator betreiben die IT-Systeme – jeweils nach den Vorgaben des IT-Sicherheitsbeauftragten und der Owner. Zu guter Letzt überprüft die interne Revision und/oder der Compliance Officer noch die Einhaltung der in der Security Policy definierten Vorgaben hinsichtlich Compliance und Governance.

«Ohne Weisungsrecht und Budget wird der Security-Beauftragte zur Farce»

**Christoph Baumgartner**

## KNACKPUNKTE

Eine solche IT-Sicherheitsorganisation wurde erst mit der flächendeckenden IT-Unterstützung nahezu aller Geschäftsprozesse zum Thema. Dies ist der Hauptgrund dafür, dass der IT-Sicherheitsbeauftragte meist kein Kästchen im Organigramm der übergeordneten Notfallorganisation belegt. Ausserdem wird er von den anderen Abteilungen oftmals als Verhinderer oder Verzögerer wahrgenommen, vor allem dann, wenn die Security Policy zuvor nicht ausreichend an die Mitarbeiter kommuniziert worden ist.

In manchen Unternehmen werden die Rollen des IT-Sicherheitsbeauftragten und des IT Security Engineers allerdings nicht getrennt. Das kann in zweifacher Hinsicht problematisch werden: Entweder entwickelt sich der kombinierte Security-Engineer-Beauftragte zum Halbgott, weil er sich selbst die umzusetzenden Vorgaben machen kann oder zur personifizierten Farce – falls er weder über ein Weisungsrecht noch über ein eigenes Budget verfügt. In beiden Fällen wird dies für die betroffenen Personen zu einer erheblichen Belastung und für das Unternehmen zu einem Sicherheitsproblem, das sich spätestens beim Eintritt eines Schadensereignisses rächt.

## LÖSUNGSANSÄTZE

An erster Stelle sollte sich ein Unternehmen überlegen, wie es die IT Security organisieren möchte. Macht es Sinn, eine Vollzeitstelle für den IT-Sicherheitsverantwortlichen zu schaffen? Könnte dies auch im Teilzeitpensum erledigt werden oder soll der komplette Bereich gar als Dienstleistung von extern bezogen werden?

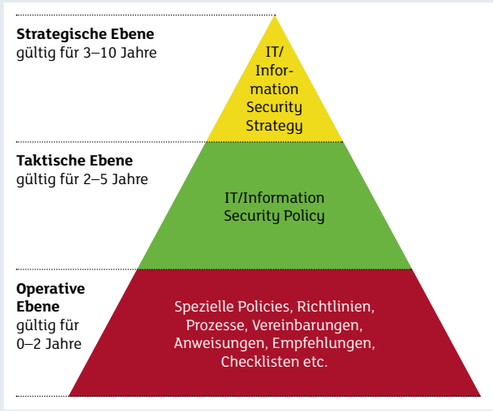
Zur Beantwortung dieser Fragen sind die Rechte und Pflichten dieser Rolle zu bedenken: Soll der IT-Sicherheitsbeauftragte lediglich die IT Security Policy pflegen oder diese auch durchsetzen? Muss er die Owner bei Risikoanalysen coachen? Wem soll er rapportieren und bekommt er ein eigenes Budget? Selbstredend müssen die Pflichten des IT-Sicherheitsbeauftragten auch mit seinen Kompetenzen korrelieren. Ohne vollumfängliches Weisungsrecht und entsprechender Rückendeckung von Top-Management und Linie kann der IT-Sicherheitsverantwortliche auch nicht die Einhaltung der Security Policy gewährleisten.

Sind diese Fragen geklärt, kann das Unternehmen entscheiden, in welcher Form die IT-Sicherheitsorganisation schriftlich definiert werden soll. Denn Strategie und Policy müssen zwingend und regelmässig kommuniziert, strikt durchgesetzt und periodisch auf ihre Aktualität hin überprüft werden. Die Sicherheitsvorgaben müssen in den Köpfen aller Mitarbeiter sitzen und über den gesamten Lifecycle eines Systems bzw. einer Applikation gewährleistet sein – vom Design über die Entwicklungs- und Betriebsphase bis zum geordneten Phase Out. Die dazu benötigte Security Awareness der Mitarbeiter kann mittels gezielter Schulungen gefördert werden. Leitet der IT-Sicherheitsbeauftragte diese Awareness-Massnahmen selbst, steigert dies zudem den Bekanntheitsgrad seiner Rolle und seiner Person.

Nur wer bereits während des Normalbetriebs eine solche IT-Sicherheitsorganisation aufgebaut und kommuniziert hat, kann auch im Notfall organisiert handeln. ←

## Hierarchie der IT/Information-Security-Dokumente

Diese Pyramide zeigt die Stufen einer durchgängigen Security-Dokumentation:
Die **IT/Information Security Strategy** ist ein 1 bis 1,5 A4-Seiten langes Dokument, in dem die Geschäftsleitung stichwortartig die wichtigsten Aspekte definiert.
Die **IT/Information Security Policy** weist einen wesentlich höheren Detaillierungsgrad auf, da sie alle im Strategiepapier nur kurz angeschnittenen Punkte in Prosa beschreibt und weitere aus der IT Security Strategy abgeleiteten Aspekte ausführt. Je nach Detaillierungsgrad kann diese von rund 15 bis über 100 A4 Seiten lang sein. Aus Praktikabilitätsgründen wird die IT Security Strategy meist zusätzlich integriert.




Die IT Security Policy ist gewissermassen das «Security-Gesetzbuch», es gilt für das gesamte Unternehmen und deren Stakeholder, wenn diese in irgendeiner Form Informationen und/oder IT-Mittel des Unternehmens nutzen.
**Alle weiteren für den operativen Betrieb benötigten Dokumente** zum Thema Sicherheit sind im Sockel der Pyramide positioniert. Anzahl und Umfang dieser Dokumente sind individuell.



BILD: FOTOLIA