Cassini GreenLab:
D!NG - Integrierte Sicherheitsarchitektur

Whitepaper:
Security Desk und Security Board

Version: 1.0

Status: final

Autoren: Onnen Godow,
Sven Malte Sopha

Stand: 28.08.2018

1. Ausgangssituation, Herausforderungen und Lösungsansatz

Die Umsetzung und Steuerung der Sicherheitsthemen einer Organisation wird durch steigende Anforderungen und Abhängigkeiten immer komplexer. Sicherheit in Organisationen setzt sich aus vier Dimensionen zusammen: Informationsschutz/Datenschutz, Informationssicherheit, Notfallmanagement und Geheimschutz. Aufgrund dieser Komplexität entsteht ein erheblicher organisatorischer und operativer Aufwand zur Gewährleistung und Aufrechterhaltung des erforderlichen Sicherheitsniveaus einer Organisation. Sicherheit in Organisationen wird mit herkömmlichen Mitteln zunehmend unbeherrschbar.

Der Informationssicherheitsbeauftragte, Datenschützer, Geheimschützer/Sicherheitsbevollmächtigte und Notfallbeauftragte stehen mittlerweile vor einem zunehmend unlösbaren Berg von Aufgaben und Fragestellungen. Die Verantwortlichen müssen jederzeit über den Zustand der Sicherheitsthemen gegenüber der Leitungsebene und Dritten, teilweise aufgrund gesetzlicher Vorgaben, auskunftsfähig sein. Berichtspflichten bei Sicherheitsvorfällen sind an der Tagesordnung und stellen nur einen kleinen Aspekt dar.

Bei technischen und organisatorischen Veränderungen, beispielsweise bei der Einführung von IT-Fachverfahren sind in der Regel die für die Sicherheit Verantwortlichen einzubeziehen. Häufig besteht zwischen den Verantwortlichen durch silohafte Verwaltungsstrukturen erhebliche Intransparenz bei der Umsetzung von sicherheitsrelevanten Veränderungen. Zur Informationsbereitstellung sind häufig zeit- und nervenraubende Verwaltungswege zu beschreiten. Es besteht daher die dringende Notwendigkeit zur Bereitstellung einer aktuellen und transparenten Informationsbasis über den Sicherheitszustand einer Organisation sowie zur Schaffung von effektiven Strukturen zur Steuerung und Entscheidung relevanter Fragestellungen.

Die Schaffung einer Anlaufstelle für alle Fragestellungen und Entscheidungsbedarfe rund um das Thema Sicherheit ist erforderlich. Diese Anlaufstelle kann ein Security Desk sein. Das Security Desk stellt auf Anfrage alle notwendigen Informationen bereit und steuert notwendige Entscheidungsbedarfe im Kontext Sicherheit ein. Umgesetzt wird dies durch die enge und institutionalisierte Zusammenarbeit von Informationssicherheitsbeauftragtem, Datenschützer, Geheimschützer und Notfallbeauftragtem. Der Auftrag der einzelnen Stakeholder in Bezug auf die gesetzlichen Regelwerke und die damit einhergehende Kontrollfunktion im Unternehmen werden dabei gewahrt.

2. Beschreibung des Lösungsansatzes

Die Erfahrungen aus der Praxis zeigen, dass es aus verschiedenen Gründen sinnvoll ist, alle strategischen und taktischen Sicherheitsthemen von den zuständigen Personen gemeinsam bearbeiten zu lassen und für die internen Kunden einen einheitlichen Ansprechpartner zu etablieren. Sicherheit wird dabei weit ausgelegt.

Alle Sicherheitsrollen müssen nicht nur eng und kontinuierlich zusammenarbeiten, sondern für die Organisation bedarf es einer einheitlichen Anlaufstelle für alle Fragestellungen und Entscheidungsbedarfe rund um das Thema Sicherheit. Diese einheitliche Anlaufstelle sollte und kann nicht eine Person sein, sondern vielmehr eine virtuelle Einheit: der Security Desk (SeD).

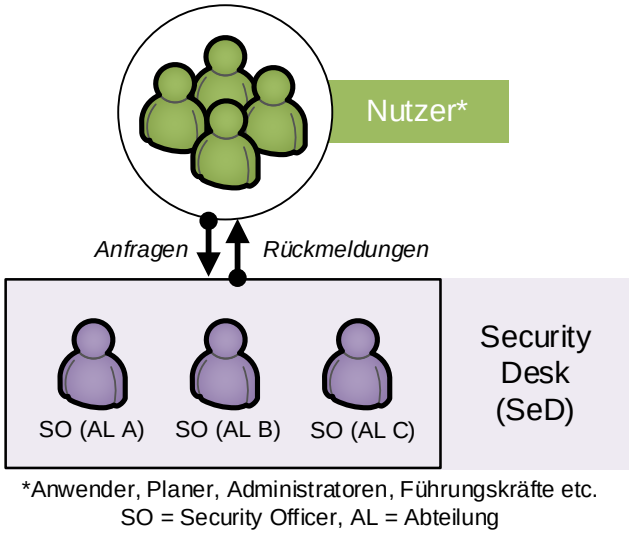
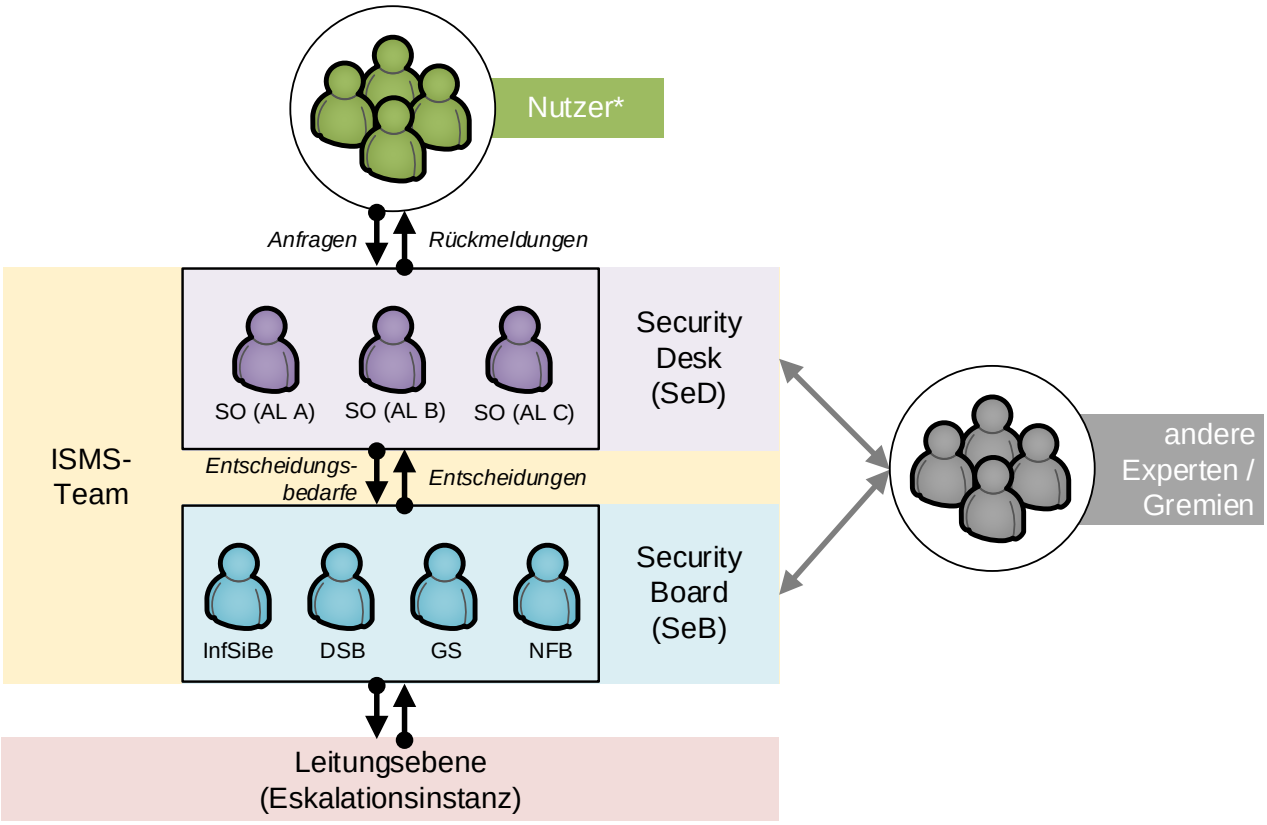


Abbildung 1: Security Desk (SeD)

Das Security Desk (SeD) wird besetzt von den Security Officer (SO), die jeweils in den Abteilungen als Koordinatoren für Sicherheitsthemen angesiedelt sind. Die Aufgaben des Security Desk teilt sich in zwei Dimensionen: Anfragenmanagement (reaktiv auf eingehende Anfragen und Entscheidungsbedarfe im Kontext Sicherheit) und Sicherheitsmanagement (proaktiv zur Steuerung der Sicherheitsthemen).

Die SO bearbeiten im Rahmen des SeD alle Anfragen mit Informationscharakter (ohne bindende Entscheidungen) im Sinne eines 1st-Level Supports. Anfragen, die über reine Auskunftsanfragen hinausgehen und Entscheidungsbedarfe haben, werden durch die SOs aufbereitet und dem Security Board (SeB) zur Entscheidung vorgelegt. Eine Geschäftsordnung regelt die Zusammenarbeit, Zuständigkeiten und Entscheidungsfindung im SeD und SeB. Das SeB arbeitet im Konsensprinzip. Das SeB und das SeD bilden den Kern des ISMS-Teams der Gesamtorganisation. Die Zusammenarbeit im SeD und SeB sowie im ISMS-Team erfolgt regelmäßig und ereignisgesteuert.



*Anwender, Planer, Administratoren, Führungskräfte etc.

Abbildung 2: Security Board (SeB)

Da die SOs nicht zwingend in einem Raum angesiedelt sind, sondern verteilt arbeiten, werden die SO durch ein Tool unterstützt. Das SeD hat jederzeit Zugriff auf alle relevanten Daten, um Hintergrundinfos für fundierte Entscheidungen zu erlangen . Dieser Zugriff erfolgt für definierte Schnittstellen zu Systemen mit wesentlichen Infos (Details siehe weiter unten).

Die Arbeiten und Entscheidungen im SeD/SeB erfolgen im Sinne eines Workflows und werden jederzeit toolgestützt (UCC) dokumentiert. Damit sind Anforderungen und Freigaben zu einem bestimmten Kontext nachvollziehbar und transparent für alle, auch für nicht direkt Beteiligte. Um eine schnelle Reaktion durch das SeD und SeB gewährleisten zu können, wird durch das SeD ein strukturiertes Antragswesen mit entsprechenden Formen festgelegt. Das SeD gibt der Gesamtorganisation ein Serviceversprechen durch festgelegte OLAs.

Der Security Desk als Anlaufstelle bildet die Basis für die Steuerung und Umsetzung Sicherheitsthemen der Organisation. Das SeB ist fest in die übergreifenden Geschäftsprozesse zu integrieren. Die Integration erfolgt im Sinne eines Veto-Rechts, insbesondere die Vorgänge die Sicherheitsthemen betreffen, sind zustimmungspflichtig durch das SeB. Die Geschäftsprozesse bzw. Freigabeprozesse der Gesamtorganisation müssen dies entsprechend abbilden, damit alle relevanten Rollen an den relevanten Entscheidungen beteiligt werden.

3. Schnittstellen und Toolunterstützung

Damit das SeD/SeB effizient arbeiten kann und damit Entscheidungen getroffen werden können, ist ein Zusammenspiel und Austausch mit anderen Bereichen in der Organisation notwendig. Nicht alle Informationen liegen den Kollegen immer vor, um Entscheidungen treffen zu können. Zu den relevanten Themen gehören u.a. Änderungsmanagement, Risikomanagement, Architekturmanagement/IT-Strategie, Beschaffungsvorhaben, Incident Management sowie IT-Betrieb und Konfiguration Management.

Neben der Notwendigkeit des direkten, bilateralen Austauschens, ist eine effiziente Zusammenarbeit mit benachbarten Bereichen nur mit Hilfe einer Toolunterstützung nachhaltig, um die notwendige Transparenz und Nachvollziehbarkeit sicherstellen zu können. Die Tool-Unterstützung sollte folgende Aspekte zum kollaborativen Arbeiten abbilden:

- Vorgangssteuerung und Nachverfolgbarkeit zu allen Vorgängen, egal ob Anfrage oder Entscheidung (Anforderungen, Freigaben etc.)
- Abbildung von Verantwortlichkeiten, Status und Reaktions-/Bearbeitungszeiten
- Kollaborationsfunktion für alle Beteiligten
- Dashboardfunktion zur Darstellung wesentlicher Ereignisse (Integration bestehender Systeme)
- Reportingmöglichkeit zur Steuerung und Nachvollziehbarkeit

Häufig treffen beim Sicherheitsbeauftragten oder dem User Help Desk Fragen zu aktuellen Ereignissen auf, die in der Regel nur den direkt in der Organisation beteiligten Mitarbeitern bekannt sind. Das Security Dashboard kann Abhilfe schaffen. Es soll eine kompakte Anzeige relevanter Security Informationen realisieren, um Transparenz über relevante Statusinformationen zu geben. Relevante Informationen sind: Laufende Vorgänge, Status von Diensten/Services sowie geplante Vorhaben. Zudem sollte über das Tool der Zugriff auf relevante Dokumentationen sichergestellt werden.

- Beispiel für Laufende Vorgänge:
  - Sicherheitsvorfälle (in Bearbeitung und abgeschlossen)
  - Änderungen an Systemen/Verfahren (in Bearbeitung und abgeschlossen)
  - Aktuelle TOP-Risiken

- Beispiel für Status von Diensten/Services:
  - Verfügbarkeit der relevanten Basisdienste/-services
  - Datenströme zu ungewöhnlichen Zeiten
  - Zugriff auf kritische Komponenten zu ungewöhnlichen Zeiten/Anomalien

- Beispiel Zeit- und Vorhabensplanung:
  - Geplante Tests und Übungen
  - Anstehende/laufende Notfallübungen
  - Relevante Ereignisse/Veranstaltungen
  - Ressourcen- /Vorhabenplanung

- Beispiel für relevante Dokumentationen:
  - Vorliegende Sicherheitskonzepte
  - Festgelegte Verfügbarkeiten zu den Verfahren/Diensten und Business Impact Ergebnisse
  - Eingesetzte Kryptoprodukte

4. Zusammenfassung

Das dargestellte Modell zeigt auf, dass Sicherheit in den Workflow der Gesamtorganisation fest integriert werden muss. Es darf keine Loslösung bzw. Parallelorganisation für Sicherheitsfragen geben. Die Lösung ist eine zentrale Anlaufstelle für alle Sicherheitsfragen. Festgelegte Entscheidungs- und Freigabeprozesse gestützt durch Tools zum kollaborativen Arbeiten ermöglichen eine koordinierte und transparente Bearbeitung der Sicherheitsthemen.

Im Mittelpunkt des Modells steht die Zusammenarbeit der vier Sicherheitsrollen (Datenschutz, Informationssicherheit, Geheimschutz und Informationssicherheit), die für jede Organisation zwingend sind. Für kleinere Organisationen können Rollen auch in Personalunion wahrgenommen werden.