Ihr Spezialist für Informationssicherheit

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Kennzahlen für die Informationssicherheit

Ziel eines Kennzahlensystems mit Key Performance Indikatoren (KPI) ist die Messbarkeit der Informationssicherheit. KPI sind deshalb ein wichtiger Aspekt zur Messung der Effizienz und Wirksamkeit von IT-Sicherheitsmaßnahmen. Dazu müssen Daten aus verschiedenen Bereichen der Informationssicherheit gesammelt und aggregiert werden. Diese Sammlung kann z.B. durch ein SIEM erfolgen, die Aufbereitung durch spezialisierte Tools wie Ampeg Security Lighthouse oder durch einfache Excel-Tabellen.

Ein weiteres Thema ist die Aussagefähigkeit von Kennzahlen. Ist zum Beispiel die Anzahl der auf dem Mailgateway blockierten E-Mails mit Schadcode ein sinnvoller KPI für den Virenschutz oder primär ein Indikator für die Anzahl der Mitarbeiter oder die Aktivitäten der Cyberkriminellen?
Gute Kennzahlen sind aussagekräftig aber einfach zu ermitteln. Schlechte Kennzahlen sind teuer und schwierig zu beschaffen und wenig aussagekräftig oder sogar irreführend.

ISO 27004

ISO/IEC 27004 ist ein Standard der ISO/IEC 27000 Familie. Ziel des Standards ist es, Institutionen zu helfen, die Effektivität ihres ISMS und der zugehörigen Controls zu messen und damit systematisch zu verbessern. ISO/IEC 27004 setzt für die Entwicklung von Kennzahlen ein fundiertes Verständnis sowie eine korrekte Bewertung der Risiken in der Informationssicherheit voraus.

Das Kennzahlensystem soll zuverlässige Informationen über die Risiken in der Informationssicherheit sowie den Status des implementierten ISMS bieten, um die Risiken bewerten zu können. Durch das Erheben von Sicherheitskennzahlen soll der aktuelle Informationssicherheitsgrad greifbar und darstellbar gemacht werden.

Des Weiteren sollen das Einhalten und Erreichen von Informationssicherheitszielen überprüft und eventueller Handlungsbedarf aufgezeigt werden. Der dazu entwickelte und in ISO/IEC 27004 beschriebene Messprozess beinhaltet die Festlegung der Kennzahlen und die Erfassung der Daten, die erforderlich sind, um die Effektivität des ISMS und der umgesetzten Controls beurteilen zu können.

Cobit

Der Einsatz eines geeigneten Steuerungsinstruments für die Aktivitäten der IT wird immer wichtiger, da die IT-Unterstützung für die Geschäftsprozesse ständig bedeutender und kritischer wird. Aus diesem Grund wurde Cobit („Control Objectives for Information and Related Technology") als Steuerungsmodell der gesamten IT entwickelt.
Cobit wird vom IT Governance Institut (ITGI) entwickelt und wurde ursprünglich von der Information Systems Audit and Control Association (ISACA) entworfen. Im Gegensatz zu ISO 27004 werden bei Cobit alle IT-Prozesse betrachtet.

Ziele und Kennzahlen werden in Cobit auf drei Ebenen definiert

- IT-Ziele und Kennzahlen, die definieren, was ein Unternehmen von der IT erwartet
- Prozessziele und Kennzahlen, die definieren, was ein Prozess für die Unterstützung der Ziele in der IT liefern muss
- Aktivitätsziele und Kennzahlen, die festlegen, was innerhalb eines Prozesses geschehen soll, um die erforderliche Leistung zu erzielen und wie diese Leistung gemessen wird

Dazu werden zwei Messgrößen definiert

- Outcome Measure: definieren Messgrößen, die dem Management aufzeigen, ob IT-Funktionen, -Prozesse, oder -Aktivitäten ihre Ziele erfüllt haben
- Performance Indicator: definieren Messgrößen, die bestimmen, wie gut die Performance von IT-Funktionen oder -Prozessen hinsichtlich der Unterstützung der Zielerreichung ist.

Wirksame Kennzahlen sollten laut Cobit folgende Eigenschaften aufweisen:

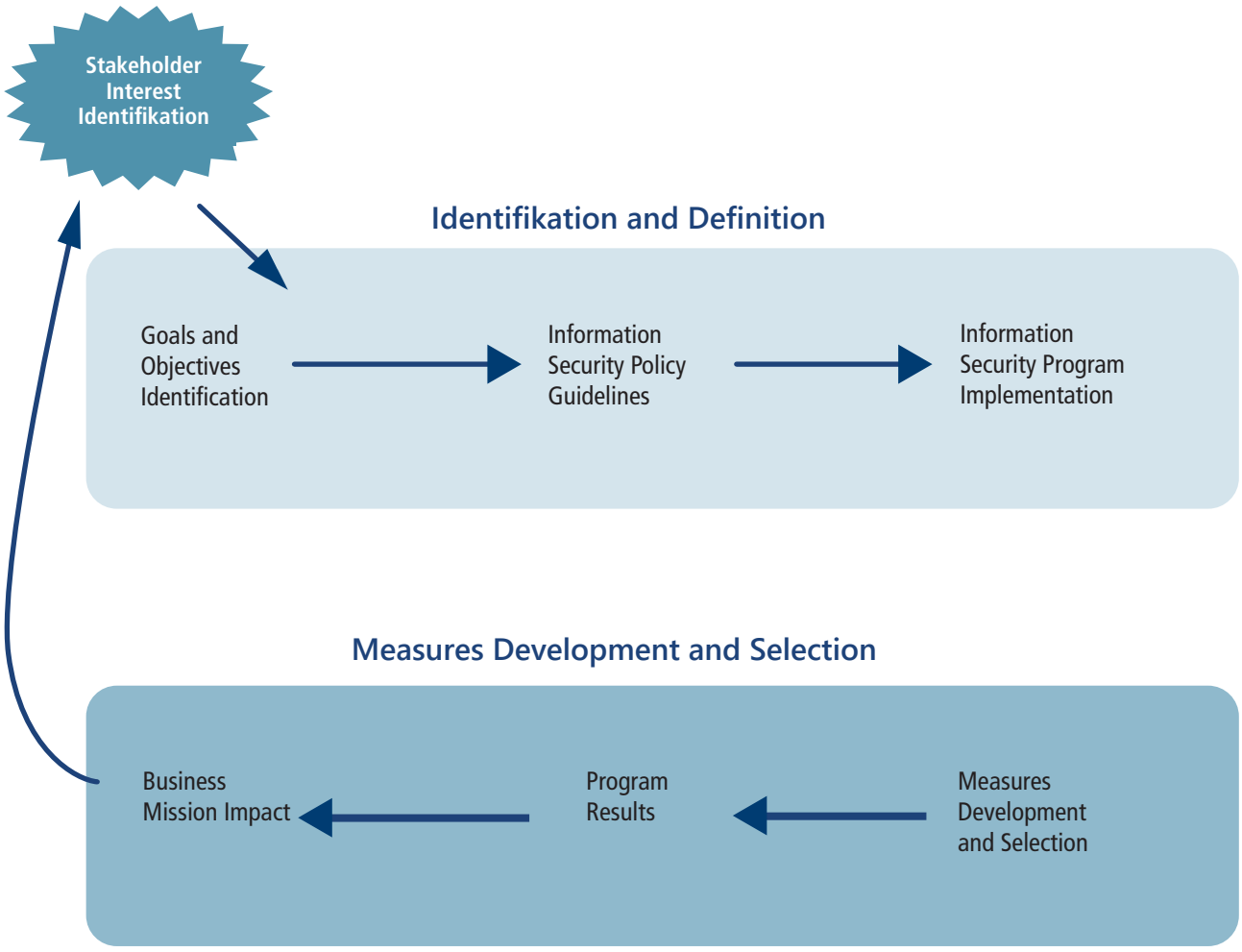
- Aufwand und Aussagekraft sollen in gleichem Verhältnis stehen
- Die Kennzahlen sollen intern vergleichbar sein (Zahlenwerte und Zeiträume)
- Die Kennzahlen sollen extern vergleichbar sein (unabhängig von der Unternehmensgröße oder Branche)
- Wenige aussagekräftige Kennzahlen sind besser als viele uneindeutige Kennzahlen
- Die Kennzahlen sollen einfach zu messen sein

Im Vergleich zu ISO 27004 ist Cobit komplexer, da ein größerer Bereich abgedeckt wird. Allerdings ist Cobit als Kennzahlensystem zur Bewertung der IT-Sicherheit auch weniger geeignet. Bei der Definition von Sicherheitskennzahlen könnte die Systematik von Cobit jedoch eine Hilfestellung sein.

NIST Special Publication 800-55

Das National Institute of Standards and Technology (NIST), genaugenommen deren Computer Security Division, hat im Rahmen ihrer Initiative „Measurements for Information Security" die Publikation SP 800-55 „Performance Measurement Guide for Information Security" veröffentlicht.

NIST SP 800-55 ist ein Leitfaden für die Entwicklung, Auswahl und Implementierung von Kennzahlen in der IT. Kapitel drei „Information Security Measures Background" beschreibt allgemeine Grundlagen über Kennzahlen. Kapitel fünf „Measures Development Process" beschreibt die Entwicklung von Kennzahlen in sieben Phasen. Im sechsten Kapitel wird auf die Implementierung der Kennzahlen eingegangen.



Die Implementierung besteht aus mehreren Phasen um die kontinuierliche Anwendung dieser Kennzahlen sicherzustellen und die zur Überwachung und Verbesserung der IT-Sicherheit dienen. Im Anhang des Standards finden sich eine Reihe von Beispielkennzahlen in Form von Kennzahlensteckbriefen.

Qualität von Kennzahlen

Kennzahlen können gut oder schlecht sein. Gute Kennzahlen sind aussagekräftig aber einfach zu ermitteln. Schlechte Kennzahlen sind teuer und schwierig zu beschaffen und wenig aussagekräftig oder sogar irreführend. Die folgenden Kriterien können zur Bewertung von Kennzahlen genutzt werden:

- **Einfach:** Die Kennzahl sollte einfach und schnell zu ermitteln sein. Viele Informationen können beispielsweise automatisiert durch ein SIEM oder aus Berichten erhalten werden. Grundsätzlich gilt, je einfacher die Daten einer Kennzahl ermittelt werden, desto effizienter sind diese Kennzahlen für eine Institution.
- **Aussagekräftig:** Die Aussagekraft beschreibt, ob aus der Kennzahl eine nützliche Information gewonnen werden kann. Wichtig sind Informationen, die der Verbesserung der IT-Sicherheit dienen.
- **Leicht verständlich:** Die Kennzahl sollte einen erkennbaren Aussagegehalt besitzen und klar verständlich sein. Dabei ist die Zielgruppe der Kennzahl zu berücksichtigen, da diese die Kennzahl verstehen und korrekt interpretieren muss.
- **Wiederholbar:** Es sollte möglich sein, die Erhebung der Daten in regelmäßigen Abständen wiederholen zu können. Nur so werden Abweichungen über längere Zeiträume hinweg erkannt und die Wirkung von Maßnahmen kann nachvollzogen werden.
- **Überprüfbar:** Eine regelmäßige Überprüfung der Kennzahlen muss durchgeführt werden, um die Aktualität der Kennzahlen zu gewährleisten.
- **Vergleichbar:** Viele Kennzahlen können nur in Relation zueinander ihre Aussagekraft entfalten. Aus diesem Grund ist es wichtig, dass bei den Erhebungen der Kennzahlen die gleichen Zahlenwerte bzw. Datenquelle verwendet werden. Innerhalb einer Organisation ist primär die Vergleichbarkeit über die Zeit und nicht die Vergleichbarkeit mit anderen Unternehmen relevant.
- **Zeitnah:** Für eine aussagekräftige Kennzahl sollten nur aktuelle Daten ermittelt werden, damit etwaige Abweichungen frühzeitig erkannt werden können und möglichst rasch darauf reagiert werden kann.
- **Zuverlässig:** Es dürfen keine fehlerhaften oder falschen Daten für die Kennzahlen ermittelt werden. Aus diesem Grund ist es von Vorteil, wenn Daten automatisiert erhoben werden.
- **Konkretisierbar:** Die Kennzahlen sollen an die Geschäftsziele, die Unternehmensgröße, den Reifegrad der IT und an die Art des Unternehmens angepasst werden können, damit ein individuelles Kennzahlensystem entwickelt werden kann.
- **Objektiv:** Kennzahlen sollten objektiv erhoben werden können, da subjektive Aspekte einer Kennzahl die Gefahr einer Beeinflussung enthalten. Damit wird möglicherweise die Aussage einer Kennzahl verfälscht.
- **Dokumentierbar:** Die Ergebnisse der Messung sowie allgemeine Informationen zur Messung und Darstellung einer Kennzahl, wie beispielsweise der Berechnungsweg oder die Darstellungsform, sollten dokumentiert werden.

Eine mögliche Darstellung dieser Parameter kann beispielsweise in einem sogenannten Kennzahlensteckbrief erfolgen. Dieser Kennzahlensteckbrief enthält alle Informationen die zur Ermittlung, Berechnung und Bewertung einer konkreten Kennzahl erforderlich sind.

Kennzahlensteckbrief

Kennzahlensteckbrief			
Bezeichnung			
Berechnung			
Beschreibung			
Adressat			
Zielwert			
Toleranzgrenzen			
Eskalationsregel			
Gültigkeit			
Verantwortlicher			
Datenermittlung		**Datenaufbereitung und Präsentation**	
Datenquellen		Verdichtung	
Erhebungsverfahren		Darstellung	

Unsere Leistung

Wir haben Erfahrung in der Ermittlung aussagekräftiger und brauchbarer Kennzahlen zur Messbarkeit der Informationssicherheit. Wir analysieren Ihre Infrastruktur und bewerten den Reifegrad Ihrer Informationssicherheit. Darauf aufbauend identifizieren wir für Sie sinnvolle Security KPIs.

Außerdem helfen wir Ihnen bei der Automatisierung der notwendigen Datensammlung und der Korrelation notwendiger Informationen.

Gerne helfen wir Ihnen bei der grafischen Aufbereitung und der Präsentation Ihrer Kennzahlen für Ihr Management.

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH

Fürholzener Straße 5a
85386 Eching
Telefon: 089 - 45217100
E-Mail: welcome@nesec.de
Internet: www.nesec.de

NESEC
Gesellschaft für angewandte Netzwerksicherheit mbH