Critical Success Factors for the work of the information Security Personnel

Termpaper Research

Autoren:
Pascal Kiser
Maurin Thalmann

MANSEC / FS 2018

Inhaltsverzeichnis

Management Summary

Bei Critical Success Factors handelt es sich im Allgemeinen um einige wenige, für den Erfolg eines Unternehmens unabdingbare Faktoren. Diese Faktoren lassen sich aus fünf Bereichen herleiten: Industrie, Beziehungen zu Peers, Umgebungsfaktoren, zeitliche Faktoren und aus dem Gebiet der Managementsschicht. Demzufolge sind die Critical Success Factors auch für jede Managementsschicht sowie für die Organisation selbst separat zu definieren.
Die Informationssicherheit befasst sich mit der Planung, Umsetzung, Aufrechterhaltung und Optimierung der Informationssicherheit in einer Organisation, wobei die Gesamtheit all dieser Funktionen das per ISO-Norm definierte Informationssicherheits-Managementsystem (ISMS) bildet. Die ENISA setzt sich als Organisation für ein höheres Bewusstsein zu Sicherheitsthemen in den EU-Staaten ein und beschäftigt sich mit der Entwicklung von Cyber-Security-Strategien. Sie definieren den Begriff der CSF für die Informationssicherheit. Des Weiteren werden die einzelnen Faktoren beschrieben, wie CSFs die Sicherheit im Information Security Risk Management verbessern können. Zur Beurteilung der CSFs werden diese einer Erfolgsfaktorenanalyse unterzogen. Es steht jedoch in Frage, wie realitätsgetreu eine solche Analyse die Faktoren beurteilen kann. Deshalb werden CSFs vermehrt noch anhand von Key Performance Indikatoren gemessen.

Einleitung

Dieses Termpaper wurde im Rahmen des Moduls «Managementaspekte der Informationssicherheit (MANSEC)» von den Studierenden Pascal Kiser und Maurin Thalmann verfasst. Thema dieses Termpaper war die Recherche zur Frage nach kritischen Erfolgsfaktoren (Critical Success Factors) im Zusammenspiel mit der Arbeit von Informationssicherheitspersonal und wie diese gemessen werden. Dabei setzten sich die Studierenden mit dem Thema Critical Success Factors im Allgemeinen sowie den Aufgaben der Informationssicherheit auseinander. Im Anschluss darauf spezifizierte sich die Recherche auf die Anwendung der Critical Success Factors im Bereiche der Informationssicherheit und wie diese Faktoren gemessen werden können. Dieses Termpaper wurde als Testat für besagtes Modul erstellt und richtet sich diesbezüglich an die Dozenten, in deren Interesse die Recherche zu dieser Fragestellung angestellt wurde.

Definition des Begriffs CSF

Critical Success Factors - Definition

Der Begriff "Critical Success Factors" (CSF) wurde ursprünglich von dem amerikanischen Organisationstheoretiker John F. Rockart wie folgt definiert:

> *Critical success factors thus are, for any business, the limited number of areas in which results, if they are satisfactory, will ensure successful competitive performance for the organization. They are the few key areas where "things must go right" for the business to flourish. If results in these areas are not adequate, the organization's efforts for the period will be less than desired.*
> *(Rockart, 1979)*

Boynton und Zmud definierten Critical Success Factors in ihrem "Assessment of Critical Success Factors" wie folgt:

> *"Critical success factors are those few things that must go well to ensure success for a manager or an organization and, therefore, they represent those managerial or enterprise areas that must be given special and continual attention to bring about high performance. CSFs include issues vital to an organization's current operating activities and to its future success."*
> *(Boynton & Zmud, 1984)*

Beide Definitionen haben gemeinsam, dass es sich um einige wenige, für den Erfolg des Unternehmens unabdingbare Faktoren handelt. Die auf Deutsch auch als kritische Erfolgsfaktoren (KEF) bezeichneten CSFs beschreiben also eine beschränkte Anzahl Faktoren, die für den Erfolg des Unternehmens von existenzieller Bedeutung sind und deshalb auch besondere Aufmerksamkeit erhalten sollten.

Dabei gilt es zu beachten, dass mit CSFs nicht konkrete Kriterien zum Messen des Erfolgs wie beispielsweise die Anzahl verkaufter Einheiten oder die Anzahl dazugewonnener Kunden gemeint sind, sondern Elemente, dessen Vorhandensein für den Erfolg eines Unternehmens unabdingbar sind. Dies kann beispielsweise der Aufbau und Unterhalt eines Kundenbetreuungszentrums sein oder eine effektive Marketingstrategie.

Critical Success Factors nach Caralli & Wilson

Gemäss Caralli und Wilson des Carnegie-Mellon-Universität werden CSF folgendermassen definiert:

> *The limited number of areas in which satisfactory results will ensure competitive performance for the organization and enable it to achieve its mission.*
> *(Caralli & Wilson, 2004)*

Demnach definieren sich CSF als die Bereiche, in welchen eine Organisation klar definierte Ziele setzen muss, um im Ganzen erfolgreich zu sein bzw. zu bleiben.
Die Charakteristik eines CSF zeichnet sich durch die Herkunft, Dimension und Hierarchie eines CSF aus.

Charakteristik

Herkunft

Insgesamt gibt es fünf Quellen, aus welchen ein CSF definiert werden kann:

- Die **Industrie**, in welcher eine Organisation operiert
- Beziehungen der Organisation zu ihren **Peers**
- **Umweltbedingte Faktoren**, welche die Organisation nicht kontrollieren kann
- **Zeitliche** Barrieren, Herausforderungen und Probleme
- Das **Gebiet** jeder Schicht des Managements

In folgender Abbildung sind Beispiele von CSFs aus den verschiedenen Quellen einer Organisation aufgelistet.

Abbildung 1: Beispiele von CSFs aus den fünf Quellen (Caralli & Wilson, 2004)

Dimension

Die Dimension der CSF erstreckt sich über die internen und externen CSF sowie über die überwachenden und anpassenden CSF.
Interne CSF liefen innerhalb des Kontrollbereichs eines bestimmten Managers, wobei **externe** CSF mit grösster Wahrscheinlichkeit nicht vom Manager kontrolliert werden können.
Überwachende CSF sollen die kontinuierliche Überprüfung von existierenden Situationen hervorheben.
Anpassende CSF hingegen konzentrieren sich hauptsächlich auf das Verbessern und Wachstum einer Organisation.
Manager sind hauptsächlich Besitzer von überwachenden CSF. Dabei werden die anpassenden CSF meist mit den Zielen einer Organisation verwechselt.
(Caralli & Wilson, 2004)

Hierarchie

CSF existieren in einer Organisation in jeder Schicht des Managements, somit auch auf jeder einzelnen Stufe der Organisation, wie in folgender Abbildung ersichtlich ist:

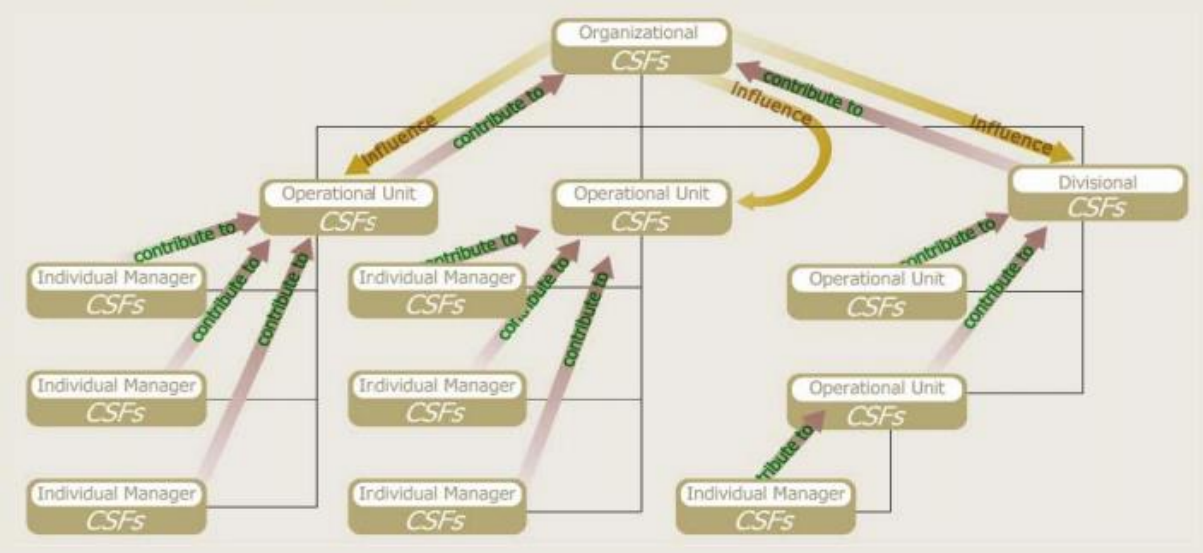

Abbildung 2: CSF Hierarchie in einer Organisation. (Caralli & Wilson, 2004)

Dies bedeutet, dass die CSF von unterstellten Managementschichten immer dazu beitragen, dass auch die CSF der ihnen übergeordneten Schichten erfüllt werden. Somit tragen alle Managementschichten im Grossen und Ganzen dazu bei, dass die CSF, welche organisationsweit gültig sind, erfüllt werden können.

CSF Methodik

Die CSF Methodik dient dazu, die CSF einer Schicht oder der Organisation zu definieren und im Betrieb umsetzen zu können. Diese Methode lässt sich in fünf Schlüsselpunkte aufteilen:

- Den Scope definieren
- Daten sammeln und zusammentragen
- Daten analysieren
- Daraus die CSFs ableiten
- Die CSFs analysieren

In diesem Prozess werden den Rollenträgern unterschiedliche Fragen gestellt, um aus der vorhandenen Strategie und den Zielen die CSF ableiten zu können. Aus den zusammengefassten Themen der jeweiligen Schichten werden daraufhin die CSF abgeleitet und ausgeführt. Caralli und Wilson geben einige Beispiele, wie an die Evaluation der CSF herangegangen werden soll bzw. mit welcher Einstellung die Manager an die Definition eines CSF herangehen sollen:

- Garantiere die Angleichung an organisatorische Einflussfaktoren
- Reduziere die organisatorische Doppeldeutigkeit
- Zuverlässige, führende Macht/Ziel für die Organisation
- Wiederspiegeln des aktuellen Betriebsumfelds der Organisation
- Wiederspiegeln der Risikoperspektive des Managements
- Ablaufskorrektur

(Caralli & Wilson, 2004)

CFS in der Information Security

Definition / Aufgaben der Information Security

Eines der Ziele dieses Dokuments ist es, kritische Erfolgsfaktoren für die Arbeit von Personen im Bereich Informationssicherheit zu definieren. Diese befasst sich mit der Planung, Umsetzung, Aufrechterhaltung und Optimierung der Informationssicherheit in einer Organisation. Die Gesamtheit der in diesem Zusammenhang definierten Massnahmen und Verfahren bilden das Informationssicherheits-Managementsystem (ISMS) im Sinne der ISO-Norm ISO/IEC 27001. (ISO, 2018)
Aus diesem Grund wird der Begriff ISMS in diesem Dokument verwendet, um die Gesamtheit der in der Aufgabenstellung als "the work of the information Security Personnel (Security Engineers, Security Architects, Security Officers)" genannten Tätigkeiten zu beschreiben.

CSF gemäss ENISA

Die ENISA (European Union Agency for Network and Information Security) ist ein von der EU im Jahr 2004 gegründetes Zentrum für Netzwerk- und Informationssicherheit mit dem Ziel, das Bewusstsein im Bezug auf Sicherheitsthemen in den Mitgliederstaaten zu erhöhen und übernimmt auch Beratungsaufgaben sowie die Organisation gesamteuropäischer Cyber Security Übungen. Sie beschäftigt sich mit der Entwicklung nationaler Cyber Security Strategien.

Die ENISA definiert Critical Success Factors für eine effektive ISMS wie folgt:

> *have the continuous, unshakeable and visible support and commitment of the organization's top management;*
>
> *be managed centrally, based on a common strategy and policy across the entire organization;*

be an integral part of the overall management of the organization related to and reflecting the organization's approach to Risk Management, the control objectives and controls and the degree of assurance required;

have security objectives and activities be based on business objectives and requirements and led by business management;

undertake only necessary tasks and avoiding over-control and waste of valuable resources;

fully comply with the organization philosophy and mindset by providing a system that instead of preventing people from doing what they are employed to do, it will enable them to do it in control and demonstrate their fulfilled accountabilities;

be based on continuous training and awareness of staff and avoid the use of disciplinary measures and "police" or "military" practices;

be a never ending process;

(ENISA, 2018)

Die Etablierung eines ISMS erfordert gemäss ENISA folgende Faktoren:

establishing the necessary Management Framework;

implementing selected controls;

documenting the system;

applying proper documentation control;

maintaining records demonstrating compliance.

(ENISA, 2018)

Zusammenfassend lässt sich also sagen, dass für den Erfolg eines ISMS einerseits eine klare und zentral verwaltete Strategie definiert sein muss, welche mittels geeigneter Massnahmen die definierten Ziele umsetzen und überwachen kann, ohne dabei unnötig Ressourcen zu verschwenden oder die Angestellten in ihrer Arbeit zu behindern. Dabei handelt es sich um einen sich immer wiederholenden Prozess, in welchem die Strategie immer wieder den Gegebenheiten angepasst wird.

Andererseits ist die Berücksichtigung gesamtbetrieblicher Ziele und Anforderungen sowie die Kompatibilität mit der Philosophie des Unternehmens von wesentlicher Bedeutung. Informationssicherheit muss, um effektiv zu sein, von der Geschäftsleitung bedingungslos unterstützt werden und soll dementsprechend nicht isoliert betrieben werden, sondern muss ins Gesamtmanagement der Unternehmung integriert und im Einklang mit dessen Zielen sein.

CSF für die Informationssicherheit

Die allgemeine Definition beschreibt CSF als wenige, für den Erfolg eines Unternehmens unabdingbare Faktoren. In Kontext einer Unternehmung wird Erfolg in erster Linie an der Ertragskraft gemessen. Damit CSF für den Bereich Informationssicherheit überhaupt bestimmt werden können, muss deshalb zunächst auf die Frage eingegangen werden, was Erfolg in diesem Zusammenhang bedeutet.

Der Duden definiert Erfolg als ein positives Ereignis oder das Eintreten einer beabsichtigten, erstrebten Wirkung. (Duden, 2018) Insbesondere die zweite Definition kann als das Erreichen von vorher definierten Zielen verstanden werden. Somit können die Kernziele der Informationssicherheit als Grundlage für die Formulierung von Critical Success Factors im Bereich Informationssicherheit genommen werden, da diese der allgemeinen Definition von CSFs entsprechen. Im Allgemeinen versteht man darunter einerseits **Datenschutz**, also den (rechtlichen) Schutz personenbezogener Daten vor Missbrauch und andererseits die **Datensicherheit**, also der (technische) Schutz von Daten gegen Verlust, Manipulation und unerlaubte Verwendung.

Zur Erreichung von Datenschutz wie auch Datensicherheit muss der Zugriff auf schützenswerte Daten eingeschränkt werden. Dazu werden allgemeine Schutzziele definiert (Eckert, 2012):

- **Confidentiality**: Zugriff auf gespeicherte und übertragene Daten darf nur durch autorisierte Benutzer geschehen.
- **Integrity**: Alle Veränderungen von Daten müssen nachvollziehbar sein.
- **Availability**: Der Datenzugriff muss innerhalb des definierten Zeitrahmens gewährleistet sein.

Messbarkeit: Key Performance Indikatoren

Diese Kernziele der Informationssicherheit können also als kritische Erfolgsfaktoren eines Informationssicherheits-Managementsystems verstanden werden. Dies Messbarkeit dieser Ziele ergibt sich in erster Linie aus der Summe der Key Performance Indikatoren, die zur Überwachung der operativen und organisatorischen Massnahmen und Regeln zur Erreichung dieser Ziele definiert werden.

Confidentiality

Als Kennzahlen für die Vertraulichkeit können die in ITIL V3 (Service Operation) im Access Management definierten Ziele und daraus abgeleitete KPIs verwendet werden:

- Anzahl fehlgeschlagener Anmeldungen
- Anzahl nicht angepasster Zugriffsrechte oder Gruppenzugehörigkeit bei geänderter Funktion eines Mitarbeiters
- Anzahl Abweichungen der definierten Security Policy

Integrity

Die Konsistenz kann durch eine Vielzahl von Ursachen gefährdet sein. Nebst Malware und Hackerangriffen können auch Fehler von Mensch und Software sowie defekte Hardware und Übertragungsfehler zu Inkonsistenzen in Datenbeständen führen. Einige Kennzahlen zur Überprüfung von Datenintegrität:

- Funktionstests Virenscanner
- Aktualität / Update-Stand eingesetzter Hardware
- Gesundheit und Alter verwendeter Festplatten
- Wiederherstellbarkeit und Wiederherstellungszeiten von Backups

Availability

Kennzahlen zum Messen der Availability sind:

- die Ausfallrate in Prozent
- die Reaktionszeit bei Ausfällen
- Redundanz der IT-Systeme
- Wiederherstellbarkeit und Wiederherstellungszeiten von Backups
- Einhaltung der im SLA / OLA definierten Betriebs- und Reaktionszeiten
- Zugriffszeiten und Datenübertragungsraten

Anhand dieser Kennzahlen kann der kritische Erfolgsfaktor der Verfügbarkeit getestet werden.

(WikiBooks, 2017)

Anwendung von CSFs in der Enterprise Security

CSF spielen heutzutage in der Enterprise- sowie auch der Information Security eine grosse Rolle. Hauptsächlich wird es als Werkzeug im Information Security Risk Management (ISRM) verwendet. Die CSF dienen einer Organisation auch als ein Prozess, um die Sicherheit im Betrieb regeln zu können.
Das ISRM kann durch die CSF laut Caralli und Wilson auch in vielerlei Hinsicht verbessert werden:

- Bestimmung eines realistischen Umfangs für eine Risikoanalyse
- Auswahl von kritischen Punkten für die Analyse
- Identifizierung und Validation von Sicherheitsanforderungen
- Identifizierung von Risiken zu kritischen Assets
- Setzen von Bewertungskriterien, um Risiken messen zu können
- Bedrohungen evaluieren und Risiken abschwächen

Umfang (Scope) mithilfe von CSFs festlegen

Den Scope mithilfe von CSFs festzulegen ist einer der wichtigsten und gleichzeitig einer der schwierigsten Aufgaben in der Risikoanalyse. CSFs spielen deshalb eine wichtige Rolle, da im Falle, dass der Fokus einer Risikoanalyse nicht auf die richtigen Bereiche gelegt wird, keine bedeutungsvollen Resultate erzielt werden. Durch eine Neigungsanalyse kann man sich auf die wichtigsten Bereiche fokussieren und so die Mission der Organisation weiterverfolgen.

CSF und kritische Assets

Ein risikobasierter Ansatz der Informationssicherheit, um Ressourcen zum Schutze der kritischsten Assets einer Organisation auszurichten. Dabei werden bestimmte Assets ausgewählt, um durch den Schutz dieser das grösste Risiko zu verhindern oder abzuschwächen. Welche Assets geschützt werden sollen, unterliegt meistens dem Urteilsvermögen der Manager oder bestimmten Werten.
CFSs können bei der Identifikation der kritischsten Assets einer Organisation, indem jene ausgewählt werden, welche am meisten dem Erfolg der Mission der Organisation beitragen.

CSF und Sicherheitsanforderungen

Sicherheitsanforderungen sind eine wichtige Komponente zum Schutz der kritischen Assets und bildet das Fundament zum Entwurf einer angemessenen Schutzstrategie für die Assets. CSF helfen hierbei bei der Priorisierung der Anforderungen. Die Priorität der Anforderungen bestimmt welche Anforderungen einen Einfluss auf den Besitzer des Assets und der Organisation hätte.

CSF und Risikoidentifikation

Die Risikoidentifikation stellt die Grundlage für den Ansatz zur Sicherheit eines Risikomanagements dar. Die Methoden der Risikoidentifikation dienen zur Übersicht von gewöhnlichen Risiken oder organisationsspezifischen Risiken. CSFs helfen dabei, den Fokus auf wichtige Risiken zu verschärfen bzw. die wichtigsten Risiken aus allen Risiken herauszufiltern. Risikoidentifikation sollte auf die wichtigen Bereiche fokussiert werden. So kann mithilfe der CSFs auch das Wissen oder der Input vom Personal geformt oder

angeleitet werden. Nach Identifikation der Risiken müssen diese validiert und priorisiert werden.

CSF und Risikomessung

Risikomessung benötigt ein Evaluationskriterium, welches einzigartige Einflussfaktoren wiederspiegeln kann, was aber nicht garantiert ist. Kriterien können deshalb mit CSFs der Organisation verglichen werden, um sicherzustellen, dass diese mit den Einflussfaktoren der Organisation übereinstimmen.

CSF und Risikoabschwächung

Risiken betreffen eine Organisation, wenn diese den normalen Betrieb einer Organisation erschweren oder behindern. Risiken mit CSFs zu vergleichen identifiziert Risikokandidaten für eine Abschwächung, da diese entweder das Erreichen des CSF behindern oder sie andere Faktoren der Organisation wie Ziele beeinflussen.

Enterprise Resiliency

Flexibilität (Resiliency oder Resilienz) eines Unternehmens ist die Fähigkeit, Unterbrüchen des Systems standzuhalten sowie sich an neue Risikoumgebungen anpassen zu können. Wie in der folgenden Abbildung 3 ersichtlich, steht die Sicherheit im Zentrum eines jeden Unternehmens. Ist diese gewährleistet, kann das Unternehmen in seinem Umfeld überleben. Somit ist dem Unternehmen eine gewisse Flexibilität gegeben, solange es seinen Kern sicher halten kann.

Abbildung 3: Enterprise Resiliency (Caralli & Wilson, 2004)

(Caralli & Wilson, 2004)

Messbarkeit von CSF

Key Performance Indicators

Als Key Performance Indikator (KPI) bezeichnet man in der Betriebswirtschaft eine Kennzahl, um den Erfüllungsgrad von kritischen Erfolgsfaktoren oder anderen Zielsetzungen zu messen. Um kritische Erfolgsfaktoren überhaupt messen zu können ist es notwendig, sinnvolle KPIs für den jeweiligen CSF zu definieren und die zur Berechnung der KPIs benötigten Daten zu erheben.

Erfolgsfaktorenanalyse

Die von Heinrich und Lehner beschriebene Erfolgsfaktorenanalyse ist eine Methode zur Beurteilung von Erfolsfaktoren und erfolgt in drei Schritten:

- Identifikation von Erfolgsfaktoren Auswahl von Erfolgsfaktoren mittels
- Datenerhebung, Auswertung der Daten

Die Identifikation von Erfolgsfaktoren geschieht in der Erfolgsfaktorenanalyse von Heinrich und Lehner aufgrund von Erfahrungswerten oder durch Diskussion. Die Auswahl der wichtigsten Erfolgsfaktoren geschieht mittels Fragebogen, wobei alle oder eine vorher ausgewählte Gruppe an Mitarbeitern befragt werden. Da sich die *kritischen* Erfolgsfaktoren definitionsgemäss auf einige wenige beschränken, ist dies für die Bewertung von CSFs aber nur bedingt relevant. Die Fragebogenmethode wird in der Erfolgsfaktorenanalyse jedoch auch verwendet, um weitere Kriterien zur Beurteilung von Erfolgsfaktoren zu ermitteln.

Bewertung und Berechnung des Erfolgs

Priorität

Für jeden zu untersuchenden Erfolgsfaktor K wird eine Priorität P(K) festgelegt gemäss der von Heinrich und Lehner vorgeschlagenen Skala:

P(K)=1 (irrelevant) bis P(K)=7 (sehr entscheidend)

Leistung

Analog zur Priorität wird mit der Leistung L(K) der Erfüllungsgrad gemessen.

L(K)=1 (sehr schlecht) bis L(K)=7 (ausgezeichnet)

Berechnung des Erfolgs

Der Erfolg E(K) eines Erfolgsfaktors K wird wie in der Formel in Abbildung 4 ersichtlich berechnet:

$$E(K) = \frac{\sum_{T=1}^{t} (P(K,T) * L(K,T))}{\sum_{T=1}^{t} P(K,T)}$$

Abbildung 4: Formel für die Berechnung des Erfolgs (Heinrich & Lehner, 2012)

Wobei T für die Teilnehmer des Fragebogens steht, beziehungsweise für die von diesem angegebenen Werte. Der Erfolg E(K) ist im Endeffekt eine Prozentzahl, welche aussagt, zu wieviel Prozent der Erfolg aller Faktoren gewährleistet werden kann.
(Heinrich & Lehner, 2012)

Relevanz für die Beurteilung von CFS in der Informationssicherheit

Die Erfolgsfaktorenanalyse von Heinrich und Lehner eignet sich besonders für die Bewertung von Faktoren, welche nicht direkt anhand messbarer Kennzahlen bewertet werden können. Ein Nachteil der Methode ist aber, dass die zur Berechnung verwendeten Werte durch Mitarbeiterbefragungen erhoben werden und es deshalb nur schwer abschätzbar ist, wie genau sie die reale Situation wiederspiegeln.
Die Erfolgsfaktorenanalyse kann ergänzend zu den KPIs eingesetzt werden oder in Fällen, in denen die Bestimmung oder Erhebung relevanter Leistungsindikatoren nicht möglich ist.

Fazit

Kritische Erfolgsfaktoren sind dadurch definiert, dass sie für den Erfolg einer Organisation zwingend vorhanden sein müssen. In Bezug auf die Informationssicherheit bedeutet das in erster Linie die Sicherstellung der Kernziele der Vertraulichkeit, der Konsistenz und der Verfügbarkeit von Daten.

Somit können die Key Performance Indikatoren zur Überwachung der im Sicherheitskonzept definierten technischen und organisatorischen Massnahmen verwendet werden, um den Erfüllungsgrad der kritischen Erfolgsfaktoren zu messen. Dies setzt jedoch voraus, dass diese Massnahmen sinnvoll und umfassend definiert, umgesetzt und überwacht werden.

Kritische Erfolgsfaktoren können als Grundlage für Risikoanalysen und die für Evaluierung von kritischen Assets dienen. Die permanente Überprüfung des Erreichungsgrad definierter Ziele ist die Grundlage zur Erkennung von Optimierungsbedarf.

Aus diesen Gründen sind die Bestimmung und Überprüfung von CSFs auch im Bereich der Informationssicherheit von grosser Bedeutung. Die Messbarkeit der kritischen Erfolgsfaktoren und deren Priorisierung sind von der Art und der Grösse der Organisation abhängig, da sie durch Key Performance Indikatoren realisiert werden, welche sich aus den konkreten Massnahmen ergeben, welche im Sicherheitskonzept der Organisation definiert werden.

Glossar

CSF: *Critical Success Factor*; Für den Erfolg eines Unternehmens zwingend notwendiger Faktor.

ENISA (*European Network and Information Security Agency*): Zentrum für Netzwerk- und Informationssicherheit der Europäischen Union. (ENISA, About ENISA, 2018)

ISMS (*Information Security Management System*): Regeln und Verfahren zur Definition, Umsetzung, Kontrolle, Aufrechterhaltung und Optimierung der Informationssicherheit in einem Unternehmen gemäss ISO/IEC 27001. (ISO, 2018)

ITIL (*Information Technology Infrastructure Library*): Framework für Prozesse und Funktionen sowie Best-Practice-Vorschlägen für IT-Infrastrukturen.

KEF (*kritischer Erfolgsfaktor*): Siehe *CSF*.

KPI (*Key Performance Indicator*): Kennzahl zur Messung der Erfüllungsgrad oder des Fortschritts eines kritischen Erfolgsfaktors oder eines anderen Ziels innerhalb einer Organisation.

OLA (*Operational Level Agreement*): Vereinbarung zwischen verschiedenen Organisationseinheiten innerhalb einer Organisation, vergleichbar mit *SLA*.

SLA (*Service Level Agreement*): Vereinbarung zwischen Dienstleister und Auftraggeber; beschreibt Qualität und Umfang der zu erbringenden Leistungen.

Abbildungsverzeichnis

Literaturverzeichnis

Boynton, A., & Zmud, R. (1984). An Assessment of Critical Success Factors. *Sloan Management Review*, 17-27.

Caralli, R. A., & Wilson, W. R. (2004). *Applying Critical Success Factors to Information Security Planning.* Retrieved from Carnegie Mellon Software Engineering Institute: https://resources.sei.cmu.edu/asset_files/Presentation/2004_017_001_51779.pdf

Critical Success Factor. (2018, Mai). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/Critical_success_factor

CSF - definition and meaning. (2018, Mai). Retrieved from BusinessDictionary: http://www.businessdictionary.com/definition/critical-success-factors-CSF.html

Duden. (2018, Mai). *Erfolg*. Retrieved from Duden: https://www.duden.de/rechtschreibung/Erfolg

Eckert, C. (2012). *IT-Sicherheit. Konzepte – Verfahren – Protokolle. 7., überarbeitete und erweiterte Auflage.* Oldenbourg.

ENISA. (2018, Mai). *About ENISA.* Retrieved from ENISA: https://www.enisa.europa.eu/about-enisa

ENISA. (2018, Mai). *Critical Success Factors.* Retrieved from ENISA: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/critical-success-factors

Heinrich, L., & Lehner, F. (2012). *Informationsmanagement, 8. Auflage*. Retrieved from Uni Saarland: http://iss.uni-saarland.de/workspace/documents/ifm-_uebungsstunde-3.pdf

ISO. (2018, Mai). *ISO/IEC 27001:2013.* Retrieved from International Organization for Standardization ISO: https://www.iso.org/standard/54534.html

Rockart, J. F. (1979). Chief Executives Define their Own Data Needs. *Sussex Business Review*.

WikiBooks. (2017, Mai 2). *ITIL V3 / Service Operation*. Retrieved from Wikibooks: https://en.wikibooks.org/wiki/ITIL_v3_(Information_Technology_Infrastructure_Library)/Service_Operation