Die OCTAVE-Risikoanalysemethode als selbstgesteuerter Einstieg ins Informationssicherheitsmanagement

Christian Paulsen
DFN-CERT Services GmbH
Sachsenstraße 5
20097 Hamburg
paulsen@dfn-cert.de

Abstract: In diesem Beitrag wird die Risikoanalysemethode OCTAVE vorgestellt, die einen einfachen Einstieg in das komplexe Thema Informationssicherheitsmanagement ermöglicht. Dieser selbstgesteuerte Analyseansatz konzentriert sich auf die kritischen Werte einer Organisation und auf eine Auswahl von geeigneten Schutzmaßnahmen. Die Methode ist vollständig kompatibel zum Informationssicherheitsstandard ISO 27001.

1 Einleitung

Grundlage für jede aktive und angemessene Sicherheitsstrategie ist eine Risiko- und Bedrohungsanalyse, in der systematisch die betriebswirtschaftlichen Risiken mit Schwachstellen und Gefährdungen in Beziehung gesetzt werden, um daraus Maßnahmen zur Risikoverminderung bzw. -vermeidung abzuleiten. Dies gilt ganz besonders für den Teilaspekt der Informationssicherheit[1], der heute immer stärker Einfluss – direkt und indirekt – auf alle anderen Risiken einer Organisation nimmt. Viele Unternehmen, Hochschulen und andere Organisationen stehen jedoch vor dem Problem, den Einstieg in dieses komplexe Thema mit begrenzten zeitlichen und finanziellen Ressourcen zu bewältigen. Die für eine Bewertung der Informationssicherheit zur Verfügung stehenden Standards bieten wenig Unterstützung bei der Fragestellung, wie eine Risikoanalyse sinnvoll und angemessen durchgeführt werden kann, da die Umsetzung von Maßnahmen nicht Gegenstand von Normen ist. Mit dem Ziel, diese Lücke zu schließen, bietet das DFN-CERT die Risikoanalysemethode OCTAVE an, die in diesem Beitrag zusammenfassend und praxisorientiert vorgestellt wird.

[1] In der Fachliteratur wird zunehmend der Begriff IT-Sicherheit durch Informationssicherheit ersetzt, um den ganzheitlichen Ansatz hervorzuheben.

2 Nachteile gängiger Risikoanalyseverfahren und -standards

Jede Organisation bzw. jedes Unternehmen, das eine IT-Infrastruktur besitzt, setzt bereits mehr oder weniger umfangreiche Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der verwendeten Daten und Systeme ein. Es ist jedoch für die verantwortlichen Mitarbeiter und deren Vorgesetzte in der Regel sehr schwierig zu evaluieren, ob die gewählten Maßnahmen ausreichend sind oder nicht. Dies kann erst durch eine individuelle Risikoanalyse in Erfahrung gebracht werden. Gängige Standards zur Informationssicherheit bieten jedoch wenig Unterstützung bei der Fragestellung, wie eine Risikoanalyse sinnvoll und angemessen durchgeführt werden kann. Lediglich das BSI bietet eine Methode zur Risikoanalyse an. Diese kann jedoch nur dann zur Anwendung kommen, wenn eine Organisation bereits den IT-Grundschutz (weitgehend) umgesetzt hat.

Inzwischen haben viele IT-Sicherheitsdienstleister die Durchführung einer Risiko- und Bedrohungsanalyse in ihrem Angebot. Die angewandten Methoden sind jedoch häufig nicht transparent und die zur Anwendung kommenden Maßstäbe unterscheiden sich in der Praxis sehr. Somit ist eine Reproduzierbarkeit oder auch nur Vergleichbarkeit in der Regel nicht gegeben. Des weiteren ist es häufig so, dass Unternehmen / Organisationen auf die Einbeziehung einer externen Expertise angewiesen sind und somit das Know-How – dabei vor allem der Erfahrungsschatz aus der praktischen Arbeit in anderen, vergleichbaren Organisationen – herein geholt werden soll. Die Vergleichbarkeit ist auch dann ausschlaggebend, wenn intern die Ergebnisse verschiedener eigener Risikoanalysen (z. B. aus den Vorjahren) mit einem aktuellen Ergebnis verglichen werden sollen.

Damit für eine Organisation durch die Risikoanalyse und Sicherheitsbewertung ein qualifiziertes Ergebnis erzielt werden kann, müssen alle Beteiligten ihre Stärken in den Sicherheitsprozess mit einbringen. Erwartet wird ja gerade die zielgerichtete Umsetzung von Maßnahmen zur Absicherung kritischer Geschäftsprozesse, Vermeidung von Fehlinvestitionen und insgesamt eine tragfähige Umsetzung einschließlich Budgetplanung. Dies kann nicht allein durch die IT-Sicherheitsverantwortlichen und technischen Administratoren geleistet werden. In manchen Fällen führen die Diskussionen vor und während der Risikoanalyse auch zu einem grundlegenden Wandel in der Einschätzung von Informationssicherheit (Stichwort „Awareness“). Ausgelöst wird dann gewissermaßen ein Paradigmenwechsel, durch den die Verantwortung für Informationssicherheit insgesamt neu geregelt wird. Der Fokus der Analyse darf also nicht nur auf technische Aspekte beschränkt sein.

Ein weiterer wichtiger Punkt, der oft unterschätzt wird, ist die Nachhaltigkeit. Die reine Erfassung der aktuellen Situation oder die einmalige Durchführung einer Risikoanalyse ist nicht zielführend. Stattdessen müssen Ergebnisse kontinuierlich umgesetzt und Maßnahmen überwacht oder angepasst werden. Informationssicherheit ist kein statischer Zustand, sondern ein Prozess, der auch als solcher verstanden sein muss.

3 Erfolgsfaktoren für nachhaltige Risikoanalysen

Aus den im vorigen Abschnitt genannten Aspekten resultieren die folgenden Erfolgsfaktoren für die Durchführung einer nachhaltigen Risikoanalyse:

- Anwendung einer einheitlichen und transparenten Methode, mit der durch ein Team Risiken und Bedrohungen analysiert werden können, um zu reproduzierbaren und vergleichbaren Ergebnissen zu gelangen.
- Maßgebliche Beteiligung durch Einforderung einer konkreten inhaltlichen Mitarbeit (Eigenanteil) aller Verantwortlichen, ihren jeweiligen Rollen entsprechend, um Kosten zu senken und die Akzeptanz der Ergebnisse zu erhöhen.
- Beteiligung aller Entscheidungsebenen in einer Organisation (Management, Vertreter der Fachabteilungen, IT-Sicherheitsverantwortliche und Administratoren).
- Einbeziehung externer Expertise mit den Schwerpunkten Technologie, Qualitätssicherung und Moderation, falls dies notwendig ist.
- Pragmatische Umsetzung der Ergebnisse, nicht nur ein Festhalten an der erfolgten Dokumentation des Ist-Zustands. Hierbei sollte klar zwischen Ad-hoc-Maßnahmen, die sofort umgesetzt werden müssen, wenn ein kritischer Punkt identifiziert wurde, und den kontinuierlichen Maßnahmen unterschieden werden.
- Etablierung von kontinuierlichen Prozessen zur Sicherstellung der Informationssicherheit, d. h. Informationssicherheit als Prozess.

4 Die OCTAVE-Methode

Die Risikoanalysemethode OCTAVE vereint die eben aufgeführten Merkmale in sich. OCTAVE steht für „Operationally Critical Threat, Asset, and Vulnerability Evaluation“, was man am besten frei als „Bewertung operativ kritischer Werte, Bedrohungen und Schwachstellen“ übersetzen kann. Dieses Verfahren wurde an der Carnegie Mellon Universität in Zusammenarbeit mit dem CERT/CC entwickelt und unterstützt den Anwender mit Formblättern, Checklisten und Moderationsplänen bei der Durchführung einer Sicherheitsevaluation. Das DFN-CERT hat die umfangreichen Arbeitsblätter ins Deutsche übersetzt, gekürzt, an ISO 27001[2] angepasst und ein Software-Tool entwickelt.

Die OCTAVE Methode liefert als Ergebnis eine strategische Beurteilung und Planung für Informationssicherheit auf Basis einer Risikoanalyse. Dabei wird der Schwerpunkt auf eine betriebswirtschaftliche Analyse der Risiken und Sicherheitsprozesse gelegt, nicht auf eine technologische Basis.

OCTAVE ist grundsätzlich ein selbst gesteuerter Ansatz, mit dem die eigenen Mitarbeiter einer Organisation den Bedürfnissen für Informationssicherheit Rechnung tragen können.

[2] Internationaler Standard für die Etablierung eines Informationssicherheitsmanagementsystems (ISMS).

Die Umsetzung erfolgt durch ein bereichsübergreifendes Team, das allerdings überschaubar bleiben soll. Um eine wirksame Umsetzung zu realisieren, muss das Team eine gute Kenntnis von den Geschäfts- und Sicherheitsprozessen der Organisation besitzen. Das Team ist für die Durchführung verantwortlich und erhält hierfür ein explizites Mandat des Managements. Letztendlich wird basierend auf den spezifischen betriebswirtschaftlichen Risiken der Organisation eine Sicherheitsstrategie entwickelt.

5 Vorgehensweise bei der OCTAVE Methode

Bei der OCTAVE Methode werden die folgenden Phasen unterschieden (siehe auch Abbildung 1):

1. Vorbereitungsphase für die Teambildung und Zeitplanung
2. Ermittlung von Bedrohungsprofilen für Werte, die an Informationsverarbeitung und IT festzumachen sind
3. Identifizierung von Schwachstellen in der IT-Infrastruktur
4. Entwicklung der IT-Sicherheitsstrategie und deren Umsetzung

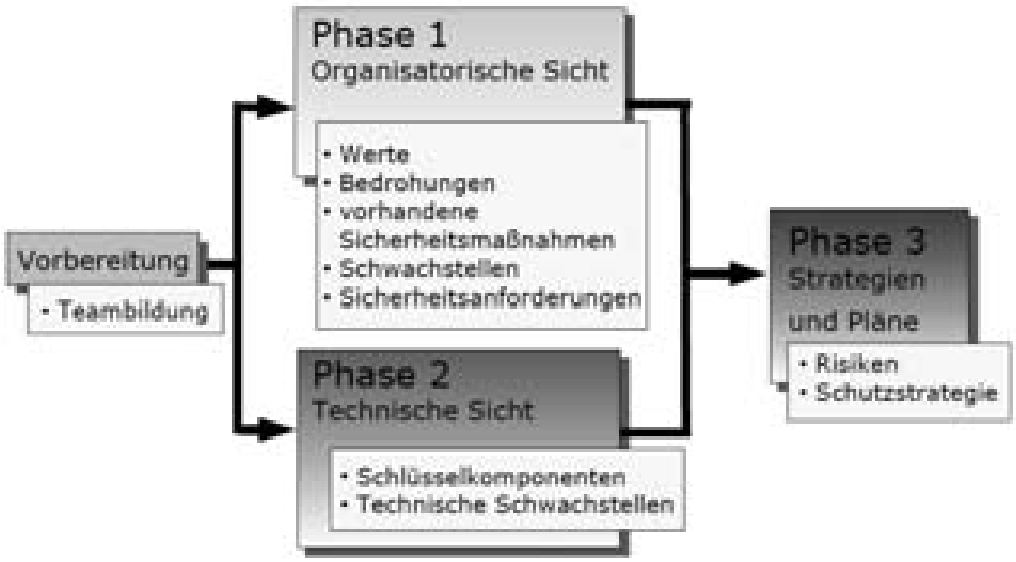

Abbildung 1: Überblick über die Phasen einer OCTAVE-Analyse

Diese Prozesse untergliedern sich, je nach Größe der Organisation, in fünf bis acht Schritte und weitere, nachgeordnete Aktivitäten. Dabei werden wichtige Werte[3] zu Objekten zu-

[3]Unter Werte werden hier nicht nur materielle Werte wie z. B. das Anlagevermögen verstanden, sondern ebenso immaterielle Werte wie Informationen und das Know-How der Mitarbeiter, welche neben den Produktionsmitteln ebenso Voraussetzung zur Erzeugung von Produkten oder zur Erbringung von Dienstleistungen sind.

sammengefasst. Ein Objekt kann dabei ein komplexes IT-System sein, wobei die technischen Einzelheiten (u. a. Server, Netzwerk, Arbeitsplätze) zunächst nicht im Vordergrund stehen. Allerdings werden auch Geschäftsprozesse, Verfahren oder Anweisungen als Objekte angesehen und behandelt, es geht also insgesamt um eine ganzheitliche Betrachtung.

5.1 Phase 1: Ermittlung von Bedrohungsprofilen für Werte, die an Informationsverarbeitung und IT festzumachen sind

Der Schwerpunkt der ersten Phase liegt in der Auswertung der organisatorischen Aspekte. Zunächst definiert das Team die Bewertungskriterien, die später verwendet werden, um Risiken zu beurteilen. Anschließend werden die wichtigen Werte identifiziert, in Objekten zusammengefasst und die aktuellen Sicherheitsmaßnahmen evaluiert.

Die Aufgaben werden allein vom Analyseteam durchgeführt, zusätzliche Informationen werden nur eingeholt, wenn es erforderlich ist. Aus den wichtigen Werten bzw. Geschäftsprozessen werden dann hinsichtlich ihrer Bedeutung für die Organisation drei bis fünf ausgewählt und dann im Detail analysiert. Zuletzt definiert das Team die Sicherheitsanforderungen und definiert ein Bedrohungsprofil für jeden kritischen Wert.

Die OCTAVE Methode wurde entwickelt, um den Einstieg in eine strategische Beurteilung und Planung von Informationssicherheit zu unterstützen. Dabei wird bewusst darauf verzichtet, bei der ersten Anwendung von OCTAVE alle Werte zu analysieren, dies muss im Rahmen des kontinuierlichen Sicherheitsprozesses nachgezogen werden. Wichtige Fragestellungen in dieser Phase sind:

- Welches sind die kritischen Werte?
- In welcher Beziehung stehen die Werte zueinander?
- Was sind die spezifischen Bedrohungen?
- Was wird bereits unternommen, um diese Werte zu schützen?

5.2 Phase 2: Identifizierung von Schwachstellen in der IT-Infrastruktur

Während dieser Phase erfasst das Analyseteam die IT-Infrastruktur, die in Bezug zu den kritischen Werten steht. Der Schwerpunkt liegt dabei auf den Sicherheitsmaßnahmen, die durch die Betreiber der Infrastruktur getroffen worden sind.

Das Analyseteam ermittelt zuerst, wie die Mitarbeiter die IT-Infrastruktur nutzen, wenn auf kritische Werte zugegriffen wird. Dies beinhaltet die Identifizierung der Schlüsselkomponenten und die für die Konfiguration und Betrieb verantwortlichen Personen. Abschließend wird analysiert, ob durch die verantwortlichen Personen Sicherheitsmaßnahmen technisch umgesetzt wurden.

- Wichtige Fragestellungen in dieser Phase sind:
- Wie greifen die Mitarbeiter auf die kritischen Werte zu?
- Welche Komponenten der technischen Infrastruktur sind den kritischen Werten zuzuordnen?
- Was sind die technischen Schwachstellen?

5.3 Phase 3: Entwicklung der Sicherheitsstrategie und deren Umsetzung

In der dritten Phase erfolgt eine Risikoanalyse auf Grundlage der vorangegangen Phase. Es werden die Schadenswirkungen und Eintrittswahrscheinlichkeiten der identifizierten Bedrohungen abgeschätzt. Darauf aufbauend wird eine Schutzstrategie für die kritischen Werte entwickelt. Anschließend werden geeignete Sicherheitsmaßnahmen ausgewählt und ein Umsetzungsplan erstellt. Wichtige Fragestellungen in dieser Phase sind:

- Was sind die Auswirkungen im Schadensfall?
- Welche Maßnahmen werden benötigt, um den Bedrohungen entgegenzuwirken?
- Welche Maßnahmen müssen unverzüglich / mittelfristig / langfristig ergriffen werden?
- Welche Veränderungen sind im Sicherheitsmanagement erforderlich, um die Informationssicherheit kontinuierlich sicher zu stellen?

Auch wenn OCTAVE lediglich zum Zweck der Risikoanalyse eingesetzt wird, erhält man durch die ermittelten und bewerteten Risiken eine übersichtliche Informationsbasis, mit der Fehlinvestitionen vermieden und Maßnahmen zielgerichtet umgesetzt werden können. In der letzten OCTAVE Phase wird zudem eine Strategie zur Unterstützung des zukünftigen Risikomanagements ausgearbeitet. Hiermit wird die wichtigste Grundlage für die Etablierung eines strategisch ausgerichteten Informationssicherheitsmanagements bereitgestellt.