Risikoanalyse mit der OCTAVE-Methode

Dr. Christian Paulsen, DFN-CERT

In diesem Vortrag wird die Risikoanalyse-Methode OCTAVE vorgestellt, die ursprünglich an der amerikanischen Carnegie Mellon Universität in Zusammenarbeit mit dem CERT/CC entwickelt wurde. OCTAVE steht für „Operationally Critical Threat, Asset, and Vulnerability Evaluation“, was man auf Deutsch frei als „Bewertung operativ kritischer Werte, Bedrohungen und Schwachstellen“ übersetzen kann.

Das DFN-CERT hat diese Methode ins Deutsche übersetzt, den Umfang der Originaldokumente erheblich verkleinert und an ISO 27001 angepasst. ISO 27001 ist ein international anerkannter Standard für den Aufbau und Betrieb eines Informationssicherheitsmanagementsystems.

OCTAVE liefert als Ergebnis eine strategische Beurteilung der Informationssicherheit einer Organisation auf Basis einer Risikoanalyse.

Die gesamte Analyse wird dabei von einem internen Team durchgeführt, das anhand von Checklisten, Fragen und Übersichtsgrafiken durch den gesamten Evaluationsprozess geführt wird. Dadurch verbleibt zum einen das dabei erworbene Know-How innerhalb der Organisation und zum anderen wird damit ein größeres Bewusstsein für Informationssicherheit auf allen Organisationsebenen geschaffen.

Der OCTAVE-Analyseprozess konzentriert sich dabei nicht nur auf technische Aspekte, wie es sehr oft bei anderen Risikoanalysemethoden der Fall ist, sondern beinhaltet auch die betriebswirtschaftliche Sicht auf die Prozesse zur Informationsverarbeitung. Somit ist es einfacher, die Leitungsebene einer Organisation in den Entscheidungsprozess zu integrieren und von der Notwendigkeit von Investitionen in die Informationssicherheit zu überzeugen.

Auch Hochschulen finden so einen vereinfachten Einstieg ins Informationssicherheitsmanagement.