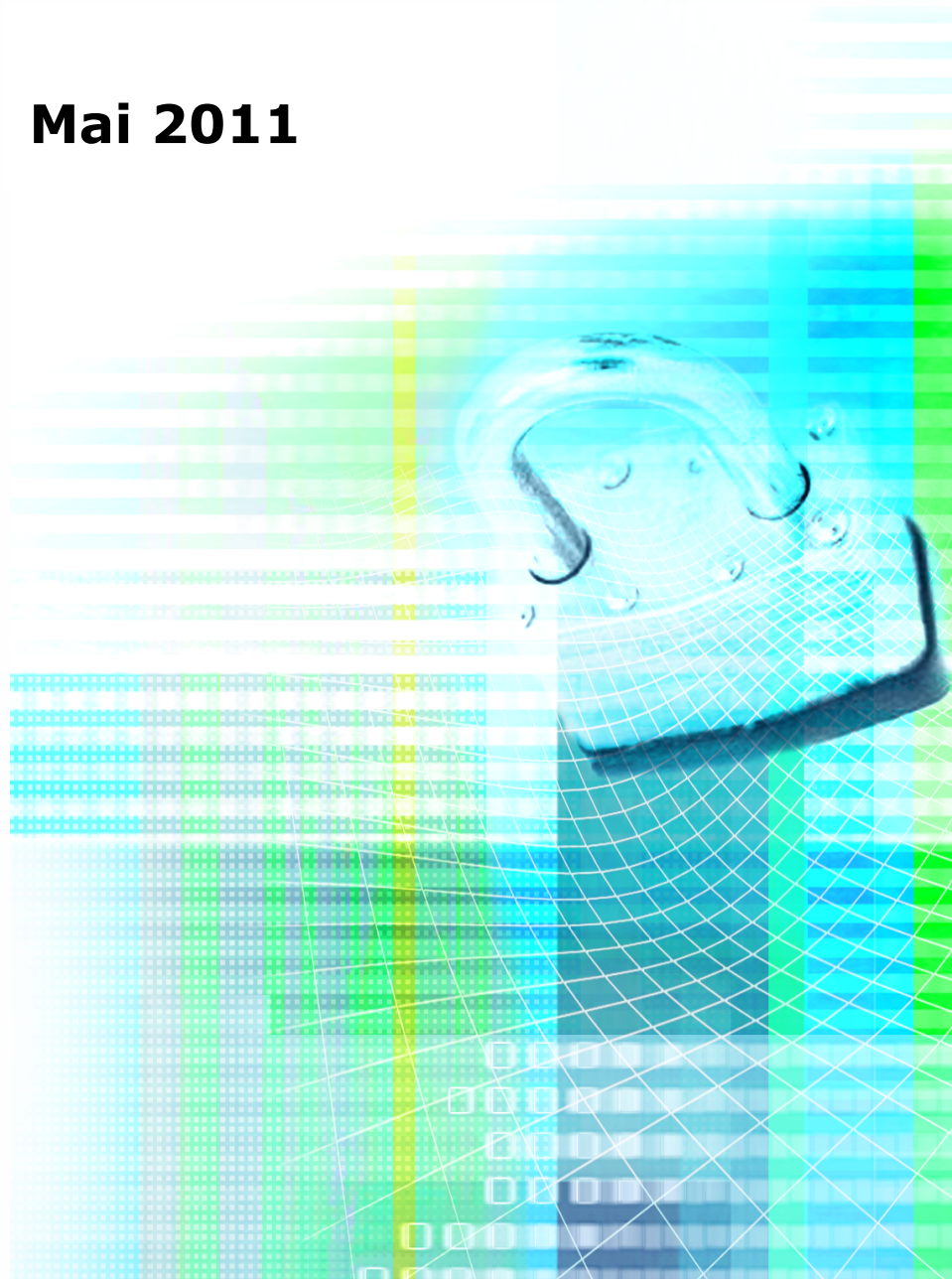


Risikoanalyse mit OCTAVE

Angebote DFN-CERT

Mai 2011



Inhaltsverzeichnis

1 Angebote des DFN-CERT.....	3
1.1 Einführung / Arbeitsunterlagen.....	3
1.2 OCTAVE-Tutorium.....	3
1.3 Begleitung der Analyse durch das DFN-CERT.....	4
1.3.1 Leistungspaket 1: Unterstützung bei der Qualitätssicherung.....	4
1.3.2 Leistungspaket 2: Begleitung bei der Risikoanalyse.....	5
1.3.3 Leistungspaket 3: Technische Analyse.....	6
2 Zukünftige Weiterentwicklungen.....	8

1 Angebote des DFN-CERT

1.1 Einführung / Arbeitsunterlagen

Die OCTAVE¹-Risikoanalysemethode wurde von der Carnegie Mellon Universität in Pittsburgh (USA) entwickelt und durch das DFN-CERT überarbeitet. OCTAVE beschreibt einen grundsätzlich selbst gesteuerten Ansatz, durch den die eigenen Mitarbeiterinnen und Mitarbeiter einer Organisation die konkreten Bedürfnisse und Lücken bei der Informationssicherheit richtig einschätzen können. Checklisten und Arbeitsblätter helfen bei dieser Analyse, die auf Basis des Wissens der beteiligten Mitarbeiterinnen und Mitarbeiter im Team durchgeführt wird. Konkret stellt das DFN-CERT für die Durchführung einer Risikoanalyse nach der OCTAVE-Methode registrierten Nutzern folgende Unterlagen zur Verfügung:

- Arbeitsblätter
- Checklisten
- Leitfaden zur Umsetzung

Bei den Unterlagen handelt es sich um eine den heutigen Ansprüchen angepasste Übertragung des ursprünglichen Konzepts. Insbesondere werden ausschließlich die in Deutschland gebräuchlichen Fachbegriffe verwendet, um dem OCTAVE-Nutzer den Einstieg in das Thema zu erleichtern und einen fließenden Übergang zu den BSI-Standards aufzuzeigen. Im Hinblick auf eine mögliche ISO27001-Zertifizierung wurden ebenso die Themenbereiche neu strukturiert und dieser internationalen Norm angepasst, die auch in Deutschland immer mehr Bedeutung erlangt. Insgesamt wird dadurch vermieden, dass die Erkenntnisse aus dem OCTAVE-Prozess später noch einmal neu strukturiert oder erhoben werden müssen, wenn z.B. externe Berater eingebunden werden sollen oder tatsächlich eine Zertifizierung nach ISO27001 erwogen wird.

1.2 OCTAVE-Tutorium

Derzeit ist geplant, zweimal im Jahr ein eintägiges Tutorium „Risiko- und Bedrohungsanalyse mit der OCTAVE-Methode“ anzubieten. Primäre Zielgruppe sind die Verantwortlichen für das Risiko- und IT-Sicherheitsmanagement einer Institution, die entweder selbst oder mit Unterstützung eine solche Analyse durchführen wollen und sich hierbei für die Verwendung von OCTAVE interessieren.

Darüber hinaus besteht die Möglichkeit, individuelle Termine in Hamburg oder vor Ort zu vereinbaren, um die Mitglieder von Analyseteams und insbesondere die Leitungspersonen eines solchen Teams mit der Vorgehensweise vertraut zu machen und bei der Aufnahme der Tätigkeiten zu unterstützen.

¹ OCTAVE steht für „Operationally Critical Threat and Vulnerability Evaluation“

1.3 Begleitung der Analyse durch das DFN-CERT

Die Vorbereitung und Moderation von Workshops vor Ort, Begleitung des Prozesses und die Aufbereitung von Ergebnissen kann durch das DFN-CERT alleine oder im Verbund mit Partnern unterstützt werden. Bei der Begleitung einer Risikoanalyse durch das DFN-CERT ist es uns besonders wichtig, die langfristige und nachhaltige Etablierung von Schlüsselprozessen zu fördern. Hierzu engagieren wir uns nachdrücklich in der Kommunikation mit den Verantwortlichen, so dass die für Informationssicherheit zuständigen Administratoren eine Stärkung ihrer Rolle sowie ein größeres Bewusstsein bei den Entscheidern erfahren. Wie die Erfahrung zeigt, ist dies für eine vertrauenswürdige, externe Stelle oft leichter möglich. Natürlich bleiben begrenzende Faktoren – zum Beispiel Ressourcen und Budgets – weiterhin bestehen.

Der Ansatz des DFN-CERT ist wie immer auf die „Hilfe zur Selbsthilfe“ ausgerichtet und konzentriert sich daher auf die Begleitung des eingesetzten Teams und die Zuarbeit in den Bereichen, in denen seine Expertise gefragt ist. Daraus ergibt sich als Konsequenz, dass die beauftragende Einrichtung intensiv das Thema bearbeitet und entsprechendes Knowhow aufbaut. Für die Planung und Durchführung einer Risikoanalyse nach OCTAVE wird ein Zeitraum von mindestens 12 Wochen angesetzt.

Auf Grundlage der im Pilotprojekt gemachten Erfahrungen haben wir drei Dienstleistungspakete zusammengestellt, um den unterschiedlichen Anforderungen der Institutionen gerecht zu werden. Darüber hinaus gibt es die Möglichkeit, die Erarbeitung spezieller Inhalte auf individueller Basis zu vereinbaren. Dies ist jedoch nicht Gegenstand der weiteren Darstellung.

1.3.1 Leistungspaket 1: Unterstützung bei der Qualitätssicherung

Im Rahmen dieses Leistungspakets wird das Analyseteam bei der Planung und Vorbereitung des Projekts, sowie bei der Aufbereitung der Ergebnisse durch einen Mitarbeiter vom DFN-CERT vor Ort unterstützt. Die Durchführung der Risikoanalyse erfolgt in Eigenregie durch das Analyseteam. Das DFN-CERT übernimmt das Review der in den einzelnen Arbeitsschritten erstellten Dokumente und trägt durch eine Kommentierung, Klärung von offenen Fragestellungen und Bearbeitung von Teilaspekten zu einem erfolgreichen Projektergebnis bei. Darüber hinaus stehen die Mitarbeiter während der Projektlaufzeit telefonisch oder per E-Mail für Rückfragen zur Verfügung.

Leistungsbeschreibung Paket 1	
Vorhaben	Beschreibung
Vorbereitungsphase	Initiale Projektbesprechung <ul style="list-style-type: none"> • Sign-Off mit dem Management • Abstimmung der Sicherheitsziele • Bestimmung des OCTAVE Teams • Projektplanung vor Ort beim Anwender
Analysephase	Review der erstellten Unterlagen in fünf Bearbeitungsschritten:

Leistungsbeschreibung Paket 1	
Vorhaben	Beschreibung
	<ul style="list-style-type: none"> • Identifizierung der organisationsspezifischen Informationen • Definition von Bedrohungsprofilen • Erfassung der IT-Infrastruktur in Bezug auf die kritischen Werte • Identifizierung und Analyse der Risiken • Entwicklung einer Schutzstrategie • Vorbereitung der Workshops beim Anwender
Projektabschluss	Auswahl und Priorisierung angemessener Sicherheitsmaßnahmen <ul style="list-style-type: none"> • Kostenabschätzung • Aufbereitung der Abschlusspräsentation, • Abschlusspräsentation vor Ort beim Anwender

1.3.2 Leistungspaket 2: Begleitung bei der Risikoanalyse

Dieses Leistungspaket entspricht hinsichtlich der Vorbereitungsphase, Projektabschluss und Support dem Vorgehen beim Leistungspaket 1. Jedoch führt ein Mitarbeiter vom DFN-CERT die eigentliche Risikoanalyse gemeinsam mit den Mitgliedern des Analyseteams in fünf Workshops vor Ort durch.

Leistungsbeschreibung Paket 2	
Vorhaben	Beschreibung
Vorbereitungsphase	Initiale Projektbesprechung <ul style="list-style-type: none"> • Sign-Off mit dem Management • Abstimmung der Sicherheitsziele • Bestimmung des OCTAVE Teams • Projektplanung
Workshop 1	Identifizierung der organisationsspezifischen Informationen <ul style="list-style-type: none"> • Aufstellung der Bewertungskriterien • Ermitteln der kritischen Werte • Bewertung der Sicherheitsmaßnahmen der Organisation • Kontrolle der Dokumente und Vorbereitung des folgenden Workshops
Workshop 2	Definition von Bedrohungsprofilen <ul style="list-style-type: none"> • Auswahl kritischer Werte • Identifizierung der Sicherheitsanforderungen für kritische Werte • Identifizierung der Bedrohungen

Leistungsbeschreibung Paket 2	
Vorhaben	Beschreibung
	<ul style="list-style-type: none"> • Kontrolle der Dokumente und Vorbereitung des folgenden Workshops
Workshop 3	<p>Erfassung der IT-Infrastruktur in Bezug auf die kritischen Werte</p> <ul style="list-style-type: none"> • Ermittlung der relevanten IT-Systeme und deren Vernetzung • Analyse der technischen Prozesse • Kontrolle der Dokumente • Vorbereitung des folgenden Workshops
Workshop 4	<p>Identifizierung und Analyse der Risiken</p> <ul style="list-style-type: none"> • Bewertung der Schadenswirkung von Bedrohungen • Aufstellen von Kriterien zur Abschätzung von Eintrittswahrscheinlichkeiten • Abschätzung der Eintrittswahrscheinlichkeiten • Kontrolle der Dokumente • Vorbereitung des folgenden Workshops
Workshop 5	<p>Entwicklung einer Schutzstrategie</p> <ul style="list-style-type: none"> • Beschreibung der vorhandenen Schutzstrategie • Auswahl der Möglichkeiten zur Risikominimierung • Entwicklung eines Plans zur Risikominimierung • Identifizierung von notwendigen Änderungen der aktuellen Schutzstrategie • Festlegung weiterer Schritte • Kontrolle der Dokumente
Projektabschluss	<p>Auswahl und Priorisierung angemessener Sicherheitsmaßnahmen</p> <ul style="list-style-type: none"> • Kostenabschätzung • Aufbereitung der Abschlusspräsentation, • Abschlusspräsentation

1.3.3 Leistungspaket 3: Technische Analyse

In vielen Fällen ist es sinnvoll, die Evaluation und Verbesserung der eigenen Informationssicherheit in einer Organisation durch standardisierte, technische Prüfverfahren zu erweitern. Das DFN-CERT setzt neben der Hilfe bei der Reaktion auf Sicherheitsvorfälle gerade auf die vorbeugende Unterstützung bei der Durchführung und Verbesserung von Sicherheitsmaßnahmen, bietet aber auch individuelle Beratung und Unterstützung an. Dieses OCTAVE-Leistungspaket beinhaltet eine individuelle Systemanalyse vor Ort inklusive eines lokalen Penetrations-Tests (nur Standard-Systeme, d.h. Laptops, Clients, Server, keine SAP-Systeme, Hosts oder TK-Anlagen). Die dabei gewonnenen Erkenntnisse und Bewertungen

ermöglichen es, die OCTAVE-Schritte S2.3 (Identifizierung von Bedrohungen) sowie S3.1 (Ermittlung der Zugangswege zu den kritischen Werten) und insbesondere S3.2 (Analyse der technischen Prozesse) mit fundierten und aktuellen Informationen zu füllen.

Zusätzlich wird eine Liste von Adhoc-Maßnahmen erstellt, die von der Organisation zur Aufrechterhaltung der IT-Sicherheit direkt umgesetzt werden muss bzw. es wird ermittelt, ob neue, zusätzliche Sicherheitsmaßnahmen eingesetzt werden müssen, um die Ausnutzung von existierenden und bisher nicht ausreichend abgedeckten Schwachstellen zu verhindern.

Außerdem wird auf systematische Fehler beim Betrieb der Systeme, soweit diese erkennbar sind, besonders eingegangen, um eine Anpassung der Prozesse vor Ort zu unterstützen. Die technische Analyse beinhaltet ein Kick-Off-Meeting zum Festlegen des Umfangs und der weiteren Vorgehensweise und wird mit einer Ergebnispräsentation und einem Bericht abgeschlossen.

Dieses Paket bietet sich vor allem in der Ergänzung zum Paket 2 an, zumal in diesem Fall die Präsentation im Rahmen des Workshops 4 erfolgen kann und hierdurch Aufwände eingespart werden.

Der OCTAVE-Anwender erhält somit detaillierte Informationen über den aktuellen Sicherheitszustand seiner IT-Systeme, ohne das hierfür das Expertenwissen über Prüfung und Bewertung vor Ort verfügbar sein müsste. Dadurch kann, abgesehen davon, dass die Informationen an sich wertvoll für die Organisation sind, sich das OCTAVE-Team auf die anderen Phasen und Schritte konzentrieren und somit effektiver arbeiten.

Leistungsbeschreibung Paket 3	
Dienst / Vorhaben	Beschreibung
Kick-Off-Meeting	<ul style="list-style-type: none"> • Festlegen des Umfangs und des Zeitplans der Analyse
Durchführung der Analyse	<ul style="list-style-type: none"> • Schwachstellenprüfung, Anwendung des Netzwerkprüfers und kleiner lokaler Penetrations-Test • Im Rahmen der Analyse wird eine Liste von Adhoc-Maßnahmen erstellt, die von der Organisation zur Aufrechterhaltung der IT-Sicherheit direkt umgesetzt werden muss bzw. es wird ermittelt, ob andere Sicherheitsmaßnahmen ergänzend eingesetzt werden müssen, um die Nutzung der Schwachstelle zu verhindern. • Außerdem wird auf systematische Fehler beim Betrieb der Systeme, soweit diese erkennbar sind, besonders eingegangen, um eine Anpassung der Prozesse vor Ort zu unterstützen.
Abschlussmeeting	<ul style="list-style-type: none"> ▪ Präsentation und Besprechung der Evaluationsergebnisse

Durch die Kombination von Paket 2 und 3 ergibt sich die Möglichkeit, Aufwände einzusparen und insbesondere die Anzahl der Meetings insgesamt zu reduzieren.

2 Zukünftige Weiterentwicklungen

Das DFN-CERT wird die Arbeitsblätter und den Leitfaden sowie die Leistungspakete aufgrund von Rückmeldungen der Nutzer sowie sich ändernder Rahmenbedingungen permanent aktualisieren. Es ist außerdem geplant, die Arbeitsblätter durch ein Software-Tool zu ersetzen, das den Anwendern eine prozessgesteuerte und komfortable Dateneingabe und -speicherung ermöglichen wird.

Des Weiteren wird es zukünftig regelmäßige OCTAVE-Anwendertreffen geben, auf denen über aktuelle Entwicklungen informiert wird und bei denen sich die Nutzer untereinander und mit dem DFN-CERT austauschen können.