

IT-Sicherheitsmanagement für Kreditinstitute

Begrenzung operationeller Risiken durch wirksames IT-Sicherheitsmanagement

15.05.2002

SRC Security Research & Consulting GmbH

1	Einleitung	1
2	Was sind operationelle Risiken?	1
3	IT-Risiken - ein wesentlicher Bestandteil operationeller Risiken	2
3.1	IT-Risiken beim Outsourcing der IT-Infrastruktur	3
3.2	IT-Risiken bei technischen Migrationen	4
4	IT-Risikomanagement	5
4.1	Risikomanagement	5
4.2	IT-Risikomanagement	8
4.3	Standards und Methoden	10
4.4	Beratungs- und Unterstützungsangebote von SRC	10
5	Der Nutzen eines übergreifenden IT-Sicherheitsmanagement-Systems für ein Kreditinstitut	11

1 Einleitung

Der Baseler Ausschuss für Bankenaufsicht hat in seinen derzeit in Abstimmung befindlichen Konsultationspapieren für die Entwicklung einer neuen Eigenkapitalrichtlinie für Kreditinstitute erstmals explizit eine Hinterlegung sog. operationeller Risiken mit Eigenkapital vorgeschlagen. Bereits heute ergeben sich aus gesetzlichen Regelungen (KonTraG, KWG) Anforderungen an das Risikomanagement und die Sicherheit der Informationsverarbeitung in Kreditinstituten. Durch den Vorschlag des Baseler Ausschusses für Bankenaufsicht mit der Thematik ist allerdings der explizite Beitrag einer Reduzierung operationeller Risiken zum wirtschaftlichen Erfolg eines Kreditinstitutes deutlich geworden.

Die Risiken, die sich bei Nutzung der modernen Informationstechnologie ergeben, sind zentraler Bestandteil der operationellen Risiken. Da die Informationstechnologie mittlerweile in vielen Fällen die Geschäftsprozesse in Kreditinstituten vollständig determiniert, sind Risiken in der IT-Sicherheit aus Sicht der operationellen Risiken möglicherweise die größten Risiken überhaupt, denen ein Kreditinstitut ausgesetzt sein kann. Es ist daher notwendig, bestehende Risiken im IT-Betrieb zu identifizieren und geeignete Schutzmaßnahmen vorzusehen.

Sicherheit und Zuverlässigkeit sind dabei die aus Sicht des Risikomanagements zu stellenden zentralen Anforderungen an die Informationsverarbeitung. Vertrauen und Glaubwürdigkeit – und damit letztlich die Reputation eines Kreditinstituts – hängen wesentlich von der Sicherheit und der Zuverlässigkeit der Prozesse im Kreditinstitut ab. Schäden, die aus schwerwiegenden Zuverlässigkeitsproblemen oder Sicherheitsverletzungen z.B. bei Internet-basierten Diensten eines Kreditinstituts auftreten, haben immer auch negative Imagewirkungen auf die übrigen Geschäftsfelder und Vertriebswege eines Kreditinstituts. Es kommt daher darauf an, die Sicherheitsstandards übergreifend für Produkte und Vertriebswege festzulegen und umzusetzen. Technische Schutzmaßnahmen, wie die Installation von Firewalls, sind dabei nur ein Element des IT-Sicherheitsmanagements. IT-Sicherheit hängt immer auch von den organisatorischen und personellen Voraussetzungen ab, so dass ein IT-Sicherheitsmanagement auch diese Bereiche umfassen muss. Die Erreichung der IT-Sicherheitsziele eines Kreditinstituts kann nur gewährleistet werden, wenn das IT-Sicherheitsmanagement als Prozess übergreifend über alle Geschäftsbereiche verankert ist.

Mit Standards, wie dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie ISO/IEC 17799:2000 bzw. BS 7799-2:1999 stehen hierfür allgemein anerkannte Methoden zur Verfügung. Diese Standards erlauben es, gegenüber Geschäftspartnern und Aufsichtsbehörden die Implementierung eines den Anforderungen des Standards entsprechenden IT-Sicherheitsmanagementsystems nachzuweisen.

2 Was sind operationelle Risiken?

Die zu operationellen Risiken veröffentlichten Konsultationspapiere des Baseler Ausschusses für Bankenaufsicht basieren auf einer klaren Abgrenzung operationeller Risiken. Operationelle Risiken werden demnach als Gefahr eines direkten oder indirekten Verlustes, der

aufgrund einer fehlerhaften Geschäftsabwicklung, eines Systemfehlers, eines menschlichen Fehlverhaltens oder externer Einflüsse eintreten kann, definiert.

Das erste Konsultationspapier des Baseler Ausschusses für Bankenaufsicht zur Neuregelung der Eigenkapitalausstattung der Banken vom Juni 1999 forderte erstmalig eine Eigenkapitalunterlegung für "other risks, principally operational risk". Im Zuge des sich anschließenden Dialogs zwischen Bankenaufsicht und Banken wurde die Eigenkapitalunterlegung im zweiten Konsultationspapier vom Januar 2001 und dessen Ergänzungspapier für Operationelle Risiken explizit auf operationelle Risiken als wichtigste und am ehesten messbare Komponente der "other risks" eingeschränkt. Im September 2001 wurde ein Arbeitspapier mit neuen Vorschlägen hierzu veröffentlicht. Im Dezember 2001 wurden aufbauend hierauf die "Sound Practices for Operational Risk Management" veröffentlicht.

Unabhängig von den Konsultationspapieren des Baseler Ausschusses für Bankenaufsicht hat das Management operationeller Risiken in den letzten Jahren einen stark gestiegenen Stellenwert in der Kreditwirtschaft erfahren. Ausschlaggebend hierfür sind folgende Gründe:

- Produkte, Prozesse und Technologien in der Kreditwirtschaft haben eine früher nicht gekannte Komplexität erreicht. Dies führt zu einer gestiegenen Zahl von Möglichkeiten für eine fehlerhafte Geschäftsabwicklung, Systemfehler oder menschliches Fehlverhalten. Die durch den Einsatz neuer Technologien gestiegenen Abwicklungsgeschwindigkeiten führen dazu, dass im Falle eines Fehlers sehr schnell große Schäden entstehen können.
- Besonders spektakuläre Fälle der Vergangenheit haben dafür gesorgt, dass die operationellen Risiken allgemein stärker in das Bewusstsein gerückt wurden. Bestes Beispiel hierfür ist der Fall eines Kreditinstituts, für dessen Homebanking-System im Fernsehen technische Angriffsmöglichkeiten vor laufender Kamera demonstriert wurden. Anschließende Presseberichte stellten einen unmittelbaren Zusammenhang zwischen dem durch die Fernsehsendung verbundenen Vertrauensverlust und einem Kursrückgang der Aktie des Kreditinstituts her. Bei anderen Instituten gingen vertrauliche Daten verloren oder es kam zu Manipulationen, die zu hohen Verlusten führten.

In der Vergangenheit bekannt gewordene Fälle haben gezeigt, dass das Eintreten von operationellen Risiken unmittelbar oder mittelbar zu erheblichen Schäden für ein Kreditinstitut führen kann.

3 IT-Risiken - ein wesentlicher Bestandteil operationeller Risiken

Die Notwendigkeit zur permanenten Verbesserung von Geschäftsprozessen und zur Erzielung von Effizienzgewinnen führt zu einem ständigen Ausbau der Informationstechnologie in Kreditinstituten und der permanenten Orientierung an neuesten technischen Entwicklungen. Internet-basierte Technologien sind zwischenzeitlich Standard und ermöglichen in früher nicht gekanntem Ausmaß übergreifende Koordination, Globalisierung, Effizienz und Flexibilität.

Sicherheit und Zuverlässigkeit sind dabei die aus Sicht des Risikomanagements zu stellenden Anforderungen an die Informationsverarbeitung. Hohe Systemverfügbarkeit, Benutzerfreundlichkeit, eine proaktive Notfallplanung einschließlich einer Disaster Recovery Planung sind dabei ebenso wichtig, wie die regelmäßige Überprüfung der festgelegten Sicherheitsstandards.

IT-Sicherheitsmanagement ist daher zentraler Bestandteil des Managements operationeller Risiken. Typische Fragestellungen, die in diesem Zusammenhang zu bearbeiten sind, betreffen z.B. die folgenden Felder:

- Der Schutz von Daten und der Informationstechnologie sollte Bestandteil der Unternehmenskultur eines Kreditinstituts sein. Wird in diesem Zusammenhang darauf geachtet, dass Reaktionszeiten bei Fehlern und die Häufigkeit von Fehlern minimiert werden? Können Daten und Dateien verloren gehen oder angreifbar werden durch unklare Sicherungskonzepte für Netzlaufwerke? Gibt es klare und systematische Regeln für den Zugriff und die Speicherung von Daten?
- Vernetzte Systeme müssen durch Firewalls geschützt werden, die den Informationsfluss zur Außenwelt kontrollieren. Dies schließt häufig Internet-Kommunikation, die Kommunikation mit Außendienstmitarbeitern und die Kommunikation über E-Commerce-Plattformen ein. Eine Sicherheitsverletzung an einer Stelle kann bereits zu Schäden führen. Sind die Firewalls so konfiguriert, dass das Schutzziel auch erreicht wird? Inwieweit ist die Sicherheit von Prozessen von der Sicherheit verbundener Netze abhängig?
- Sicherheitsmaßnahmen können keine 100%-ige Sicherheit gewährleisten. Bei der IT-Sicherheit geht es daher vor allem um die Minimierung von Risiken, die Entdeckung von Attacken und die Verfolgung von Eindringlingen. Mit dem raschen Technologiewandel entwickeln sich auch die Möglichkeiten zur Umgehung von Sicherheitsmaßnahmen, so dass diese permanent angepasst werden müssen. Werden Software-Updates regelmäßig vorgenommen? Werden die IT-Systeme regelmäßig von IT-Spezialisten im Hinblick auf Möglichkeiten zum Umgehen von Sicherheitsmaßnahmen überprüft?
- Eine klare und effiziente Notfallplanung ist notwendig. Hierzu gehört neben der Sicherung betriebsnotwendiger Informationen vor allem eine praxistaugliche Struktur von Maßnahmen und Verantwortlichkeiten. Sind die im Notfall erforderlichen Maßnahmen klar dokumentiert? Sind die Zuständigkeiten für den Notfall klar und eindeutig geregelt?

3.1 IT-Risiken beim Outsourcing der IT-Infrastruktur

Das teilweise oder vollständige Outsourcing der IT-Infrastruktur kann für Kreditinstitute zu Kosten- und letztlich auch zu Wettbewerbsvorteilen führen. Gleichwohl ist auch ein Outsourcing nicht frei von operationellen Risiken, die beachtet werden müssen. Auch wenn der Be-

trieb von IT-Systemen an Dienstleister ausgelagert wird, bleibt die letztendliche Verantwortung für die zuverlässige und sichere Abwicklung von Prozessen doch beim Kreditinstitut selbst.

Dementsprechend schreibt § 25 a Abs. 1 KWG Nr. 2 vor, dass Kreditinstitute über angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung verfügen müssen. Gemäß § 25 a Abs. 2 Satz 1 KWG darf die Auslagerung von Bereichen auf ein anderes Unternehmen, die für die Durchführung der Bankgeschäfte oder Finanzdienstleistungen wesentlich sind, weder die Ordnungsmäßigkeit dieser Geschäfte oder Dienstleistungen, noch die Steuerungs- und Kontrollmöglichkeiten der Geschäftsleitung, noch die Prüfungsrechte und Kontrollmöglichkeiten des Bundesaufsichtsamtes beeinträchtigen. Entsprechend § 25 a Abs. 2 Satz 2 KWG hat sich jedes Institut die erforderlichen Weisungsbefugnisse zu sichern und die ausgelagerten Bereiche in seine internen Kontrollverfahren einzu beziehen.

Ein Kreditinstitut behält daher auch bei Auslagerung des IT-Betriebs an einen Dienstleister die Verpflichtung, gegenüber Kunden und Aufsichtsbehörden sicherzustellen, dass die Sicherheit der Informationssysteme gewährleistet bleibt. Klare Vereinbarungen über die zu erbringenden Service Levels können dazu beitragen, eventuelle Risiken zu vermeiden.

Risiken können sich in diesem Zusammenhang nicht nur beim Outsourcing-Partner, sondern auch beim Kreditinstitut selbst ergeben. Gerade aus den Schnittstellen des Kreditinstituts zu der ausgelagerten Datenverarbeitung können sich neue operationelle Risiken ergeben.

Häufig wird z.B. der Betrieb des eigentlichen Buchungssystems auf Service-Rechenzentren übertragen. Der Zugriff auf diese Systeme erfolgt aber i.d.R. nicht über „unintelligente“ Terminals, sondern über in LANs eingebundene PCs, die es erlauben, Daten auch vor Ort zu verarbeiten und vom Bankensystem unabhängige Software zu nutzen.

Den sich hierdurch ergebenden Möglichkeiten einer flexiblen Datenverarbeitung in der Bank stehen oft zusätzlichen Risiken z.B. aus dem Einsatz nicht lizenzierter Software, dem Diebstahl oder der Zerstörung von DV-Komponenten, Möglichkeiten zur Manipulation von Eingabedaten für die Bankanwendung oder der Verletzung von Datenschutzbestimmungen gegenüber.

3.2 IT-Risiken bei technischen Migrationen

Unter Migration wird im IT-Bereich der Prozess des Wechsels oder der Anpassung der aktuellen IT-Plattform eines Unternehmens zur Unterstützung neuer Produkte, Dienstleistungen oder regulatoriver Anforderungen. Da IT-Migration i.d.R. mit der Einführung neuer Methoden und Systeme verbunden ist, ergeben sich vielfältige operationelle Risiken.

Ein schlecht abgestimmter Migrationsprozess kann weitreichende Auswirkungen auf die Geschäftstätigkeit und Betriebsfähigkeit eines Kreditinstituts haben. Voraussetzungen für einen erfolgreichen Migrationsprozess sind eine umfassende Projektplanung mit klar definierten

Teilprojekten und Verantwortlichkeiten. Ein an den Projektzielen orientiertes Projektcontrolling sowie die Durchführung ausführlicher Tests vor Inbetriebnahme sind ebenfalls unverzichtbar, um die Risiken einer IT-Migration zu begrenzen.

4 IT-Risikomanagement

Informationssicherheits-Managementsysteme (ISMS) sind in der Lage, die IT-Risiken von Unternehmen umfassend zu steuern und zu kontrollieren. Hierbei können sich Unternehmen an dem international anerkannten Standard ISO 17799 „Management von Informationssicherheit“ orientieren und die Konformität zum Standard durch eine unabhängige Zertifizierungsstelle bestätigen lassen.

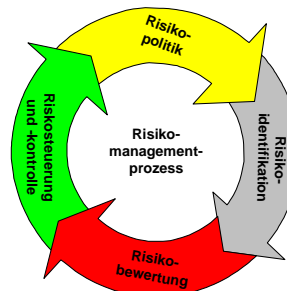
Im anschließenden Abschnitt werden in die grundlegenden Elemente eines Risikomanagementsystems dargestellt. Der darauf folgende Abschnitt stellt eine Umsetzung der Elemente bezogen auf den IT-Bereich dar, die nachfolgend als IT-Risikomanagement bezeichnet werden.

4.1 Risikomanagement

Risikomanagement ist keine einmalige Maßnahme, sondern muss als strategisch bedeutsamer Prozess in den Geschäftsprozessen eines Unternehmens verankert werden.

Risikomanagement ist demnach als Regelkreis bzw. Prozess zu sehen, der sich aus vier unabhängigen Komponenten zusammensetzt:

1. Festlegung der Risikopolitik,
2. Risikoidentifikation,
3. Risikoanalyse sowie
4. Risikosteuerung bzw. -kontrolle.



4.1.1.1 Risikopolitik

Der Risikomanagementprozess, der auch als Risikocontrolling bezeichnet wird, beginnt mit der Festlegung der strategischen und von der Geschäftsleitung vorgegebenen Risikopolitik.

Im Rahmen der Risikopolitik gilt es insbesondere festzulegen, welche risikopolitischen Ziele das Unternehmen verfolgt (risikoneutral, risikofreudig, risikoscheu) und wie der Risikomanagement-Mix gestaltet werden soll. Diese sind mit den übrigen Zielen des Unternehmens, wie z.B.

- Sicherung der Existenz des Unternehmens,
- Sicherung des Unternehmenserfolges,

- Senkung der Risikokosten,
- Qualität,
- Shareholder Value etc.

abzustimmen.

Risiken können

- Geschäftsrisiken, wie z.B. bedingt durch Konjunktur, Wettbewerbsverhalten, Technologierisiken,
- Finanzrisiken, wie z.B. bedingt durch Währungsrisiken, Finanzierungsrisiken, Kreditrisiken, Länderrisiken,
- Personalrisiken, wie z.B. bedingt durch Besetzung von Schlüsselpositionen, Fluktuation, Arbeitsmarkt,
- Rechtliche Risiken, wie z.B. bedingt durch Vertragsrisiken, Patentrisiken, Kartellrecht, Umweltrisiken, Gesetze,
- Projektrisiken, wie z.B. bedingt durch Lieferantennisiken, Verzugsstrafen, oder
- IT-Risiken, wie z.B. bedingt durch Datenverlust, IT-Stillstand, Datendiebstahl

sein.

Während die Risikopolitik als Bestandteil der Unternehmensstrategie zu bewerten ist, sind die weiteren Schritte als Teil des operativen Risikomanagements zu sehen.

4.1.1.2 Risikoidentifikation

Der erste Schritt des operativen Risikomanagements ist die Risikoidentifikation. Nur wenn Risiken erkannt sind, können diese in den nachfolgenden Schritten durch entsprechende Maßnahmen gesteuert werden. Im Rahmen der Risikoidentifikation werden die wesentlichen Bedrohungen, d.h. sowohl externe als auch internen Bedrohungen, die auf ein Unternehmen einwirken, systematisch und vollständig erfasst.

Die Beurteilung, ob ein Risiko eine Bedrohung für das Unternehmen darstellt, erfolgt anhand der in der Risikopolitik vorgegebenen Ziele.

Zur systematischen und konsistenten Erfassung bietet sich eine Kategorisierung der Risiken an, wie z.B. eine Einteilung nach

- Wirkung (Ertrags- Vermögens- Finanzwirksam),
- Herkunft (intern/extern) oder

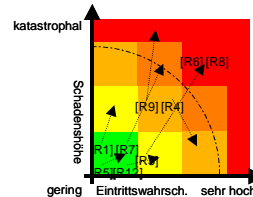
- Ursachen.

4.1.1.3 Risikoanalyse

Im zweiten Schritt des operativen Risikomanagementprozesses werden die Risiken bzw. Bedrohungen bewertet.

Ziel der Risikoanalyse ist die Bewertung eines jeden zuvor identifizierten und erfassten Risikos anhand seiner

- möglichen Schadenshöhe sowie der
- Eintrittswahrscheinlichkeit.



Die Risikoanalyse bewertet also den Schadenserwartungswert für jede identifizierte Bedrohung, der das Gefährdungspotential einer Bedrohung darstellt. Anhand des Gefährdungspotentials wird eine Priorisierung der Risiken vorgenommen, die die Reihenfolge für die nachfolgend einzuleitenden Maßnahmen bildet.

Die Gesamtheit der erfassten Risiken bildet das sog. Risikoportfolio, das die Risikoexposition eines Teilbereiches oder aggregiert für das gesamte Unternehmen darstellt.

4.1.1.4 Risikosteuerung

Die Ergebnisse der Risikoanalyse werden in der Risikosteuerung in Entscheidungen und geeignete Maßnahme umgesetzt. Maßnahmen sind

- Risikovermeidung,
- Risikoverminderung durch Reduktion der Eintrittswahrscheinlichkeit oder der Schadenshöhe,
- Risikoübertragung auf Dritte, wie z.B. Versicherung oder
- Risikoübernahme durch das Unternehmen selbst (Restrisiko).

Es ist festzuhalten, dass auf der einen Seite jeder Maßnahme mindestens eine Bedrohung zugrunde liegt, und auf der anderen Seite jede Bedrohung durch mindestens eine Maßnahme kontrolliert wird.

Die Risikosteuerung bzw. –kontrolle liefert somit die Begründung, wie die Bedrohungen auf Basis der durch die Geschäftleitung vorgegebene Risikopolitik durch die gewählten Maßnahmen kontrolliert werden.

4.2 IT-Risikomanagement

Entsprechend dem oben aufgeführten Risikomanagementprozess sind die Risiken zu berücksichtigen, die aufgrund der Nutzung von IT-Systemen in Unternehmen entstehen.

Die Bedrohungen der IT-Systeme lassen sich in

- Verlust der Vertraulichkeit,
- Verlust der Integrität,
- Verlust der Verfügbarkeit

einteilen.

IT-Sicherheitspolitik

Ausgangspunkt für ein ganzheitliches IT-Risikomanagement ist die IT-Sicherheitspolitik (Security Policy), welche die Sicherheitsziele eines Unternehmens auf abstrakter Ebene beschreibt. Diese sind, wie auch die Qualitäts- oder auch die Risikopolitik, von der Geschäftsleitung zu formulieren und als Teil der Unternehmensziele zu verankern.

IT-Risikoanalyse

Im Rahmen der Risikoanalyse, der eine Bedrohungs- und Schwachstellenanalysen vorangeht, werden die Bedrohungen identifiziert, die auf die IT-Systeme des Unternehmen einwirken. Diese Bedrohungen entstehen häufig aufgrund von Schwachstellen in IT-Systemen, die z.B. durch den Einsatz nicht aktueller Software, und auch nicht technischer Schwachstellen im Management der IT-Systeme, z.B. durch fehlende Regelungen.

Der Identifikation folgt die quantitative und qualitative Bewertung des Risikos, die den Erwartungswert eines möglichen Schadens darstellt.

IT-Sicherheitskonzept

Im Rahmen der Risikokontrolle bzw. -steuerung wird entschieden, wie mit den IT-Risiken umgegangen wird (Vermeidung, Verminderung, Übertragung auf Dritte, Tragen des Restrisikos).

Entscheidet sich ein Unternehmen für die Vermeidung bzw. die Verminderung so sind Maßnahmen zu ergreifen, die diese Ziele umsetzen. Das IT-Sicherheitskonzept formuliert anhand der Bedrohungen die Maßnahmen, die unternehmensweit bei der Konzeption, der Konfigura-

tion und dem Betrieb der IT-Systemen zu berücksichtigen sind. Darüber hinaus begründet das Sicherheitskonzept die Wirksamkeit der Maßnahmen, also warum die Sicherheitsziele des Unternehmens durch die eingeleiteten Maßnahmen erreicht werden.

Security Audits/Security Assessments

Security Audits und Security Assessments überprüfen, ob vorhandene organisatorischen und technischen Maßnahmen zur Erfüllung der Sicherheitsziele geeignet sind und können so die Aufgaben der Revision unterstützen. Ein Bestandteil von Security Audits bzw. eines Security Assessment sind die Penetrationstests, die entweder die Wirksamkeit von technischen Maßnahmen z.B. auf einer Firewall nachweisen, oder Schwachstellen bei der Umsetzung aufdecken.

Informationssicherheits-Managementsysteme

Kernfunktion eines Informationssicherheits-Managementsystems (ISMS) ist die Handhabung der IT-Risiken. Hierbei können die international anerkannten Normen ISO 17799 bzw. BS 7799, die einen Leitfadens für das Management der Informationssicherheit beschreiben, als Orientierungshilfe verwendet werden. Kernanforderung der Normen ist die Formulierung der unternehmensweiten Sicherheitsziele, die die Basis für die Umsetzung, Einhaltung und Erhaltung des Sicherheitsniveaus bilden.

Aus den Sicherheitszielen werden im Anschluss technische, personelle, infrastrukturelle oder organisatorische operative Maßnahmen abgeleitet, die die operative und technische Umsetzung der Sicherheitsziele beschreiben.

Es ist zu beachten, dass das Sicherheitsniveau eines Unternehmens sowohl durch technische als auch durch organisatorische Maßnahmen bestimmt wird.

Computer Emergency Response Team CERT

Damit ein Unternehmen Bedrohungen frühzeitig und effizient begegnen kann, ist eine schnelle und effiziente Reaktion notwendig. Dazu dient die Einrichtung eines sog. Computer Emergency Response Team (CERT), das schnell Gegenmaßnahmen ergreift, um größeren Schaden vom Unternehmen abzuwenden.

CERT können somit als Maßnahme zur schnellen Abwehr oder Kontrolle von Bedrohungen verstanden werden. Typische Bedrohungen sind Viren, Trojaner, Würmer oder Hacker-Angriffe aus dem Internet.

Security Awareness

Die Verankerung der Sicherheit im Unternehmen setzt die Sensibilisierung der Mitarbeiter und die Schaffung eines Sicherheitsbewusstseins voraus („Security Awareness“). Hierzu müssen zeitlich lang angelegte Programme für die Vermittlung von sicherheitsrelevanten Themen angesetzt werden, die zu einer entsprechenden Sensibilisierung der Mitarbeiter für Sicherheitsthemen führen.

4.3 Standards und Methoden

Im Umfeld des IT-Sicherheitsmanagement existieren unterschiedliche Normen und Standards, an denen sich ein Unternehmen orientieren kann. Neben den zertifizierbaren Normen BS 7799 (ISO 17799) und dem IT-Grundschutzhandbuch des BSI existieren verschiedene Normen mit hauptsächlich nationaler Bedeutung (z.B. AZN 4360:1999 aus Australien). Darüber hinaus ist derzeit eine Norm (ISO 13569) in der Entwicklung, welche speziell auf die Bedürfnisse im Bankenumfeld eingeht und zukünftig für Kreditinstitute von Bedeutung sein kann.

4.4 Beratungs- und Unterstützungsangebote von SRC

Als Gemeinschaftsunternehmen der kreditwirtschaftlichen Verlage in Deutschland bündelt SRC umfassendes Know-how zur IT-Sicherheit von der Netzwerksicherheit bis hin zum Einsatz moderner Authentifikationsverfahren an einer Stelle mit einem klaren Fokus auf kreditwirtschaftliche Anwendungen. Die Sicherheit bei der Abwicklung von Finanztransaktionen steht bei unterschiedlichsten von SRC begleiteten Projekten im Mittelpunkt. Diese reichen von der engen Einbindung in die Weiterentwicklung und Implementierung von Sicherheitssystemen im Bereich des kartengestützten Zahlungsverkehrs in Deutschland sowie in internationalen Zahlungssystemen über die Unterstützung einzelner Hersteller und Netzbetreiber bei der Implementierung sicherer Zahlungssysteme bis hin zur Zusammenarbeit mit einzelnen Kreditinstituten im Rahmen individueller Projekte.

Das Beratungsprogramm von SRC im Bereich Netzwerksicherheit deckt sämtliche Aspekte effizienten IT-Sicherheitsmanagement-Systems ab. Hierzu gehören:

- Erstellung von zertifizierbaren IT-Sicherheitsmanagement-Systemen nach BS 7799 (ISO 17799), IT-Grundschutzhandbuch oder weiterer Normen.
- Durchführung von Security Audits, Security Assessments, Penetrationstests und Risikoanalysen.
- Erstellung von Sicherheitskonzepten und Sicherheitspolitiken.
- Aufbau firmeninterner Computer Emergency Response Teams (CERT).
- Durchführung von Security Awareness Programmen.

- Beratung zu Public Key Infrastrukturen (PKI) und dem Einsatz elektronischer Signaturen mit der Signaturkarte der deutschen Kreditwirtschaft.
- Sicherheitsbegutachtungen und Evaluierungen von IT-Produkten und IT-Systemen nach Common Criteria, ZKA-Kriterien u.a.

5 Der Nutzen eines übergreifenden IT-Sicherheitsmanagement-Systems für ein Kreditinstitut

Die Einführung eines IT-Sicherheitsmanagement-Systems bietet einem Kreditinstitut eine Reihe von Vorteilen:

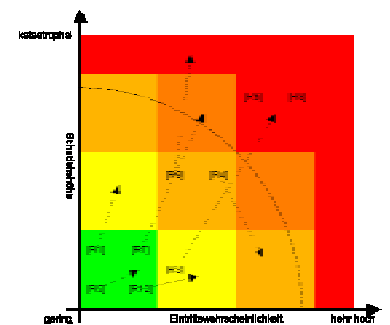
- Im Rahmen der Implementierung des IT-Sicherheitsmanagements-Systems werden die unternehmensinternen Sicherheitsziele und -maßnahmen überprüft und sowohl nach organisatorischen wie nach wirtschaftlichen Gesichtspunkten angepasst und optimiert.
- Die auf der Basis eines unternehmensweiten IT-Sicherheitsmanagement-Systems eingerichteten Schutzmaßnahmen verhindern mögliche Schäden und stellen ein einheitliches Schutzniveau für die Informationsverarbeitung im Kreditinstitut sicher.
- Das IT-Sicherheitsmanagement-System gewährleistet, dass die Schutzmaßnahmen jeweils vor dem Hintergrund des Stands der Technik überprüft und aktualisiert werden.
- Die Implementierung eines IT-Sicherheitsmanagement-Systems führt dazu, dass Risiken identifiziert und verringert werden. Mit Blick auf die in Abstimmung befindliche neue Baseler Eigenkapitalvereinbarung kann ein IT-Sicherheitsmanagement-System daher dazu beitragen, dass die für operationelle Risiken zu hinterlegende Eigenkapitalmenge minimiert werden kann. Ausschlaggebend hierfür ist zum einen die gezielte Vermeidung operationeller Risiken, zum anderen aber auch die sich aus dem IT-Sicherheitsmanagement-System ergebenden Ansätze zur Messung der verbleibenden Restrisiken.
- Die Überprüfung des IT-Sicherheitsmanagement-Systems durch externe Audits ermöglicht nachweisbare Sicherheit in den Geschäftsprozessen, was bei Streit- und Regressfällen von großer Bedeutung sein kann.
- Die Zertifizierung des IT-Sicherheitsmanagement-Systems stellt einen unabhängigen Nachweis über ein dem aktuellen Stand der Technik entsprechendes Sicherheitsmanagement dar und kann im Wettbewerb mit anderen Instituten einen Vorteil bedeuten.

Security Audits, Security Assessments Penetrationstests, Risikoanalysen

Security Audits von SRC zeigen, wo Unternehmen Schwachstellen in ihrer Informationsverarbeitung in Bezug auf Vertraulichkeit und Integrität besitzen. Hierbei werden organisatorische Aspekte (z. B. Eskalationsprozeduren, Zuständigkeiten, Sicherheitspolitiken, Regelungen) bis hin zu detaillierten technischen Aspekten (z. B. Firewall Access Listen, Systemkonfigurationen) in die Untersuchung einbezogen. Als Bestandteil solcher Untersuchungen können Begehungen (z.B. des Rechenzentrums) durchgeführt werden, bei denen Aspekte der baulichen Sicherheit und des Zugangs- und Zutrittsschutz sowie das allgemeine Sicherheitsniveau beurteilt werden können.

Einen Teilbereich der Security Audits bilden die **Penetrationstest**. Hierbei wird ausschließlich die technische Sicherheit der Systeme untersucht, wobei sich SRC Methoden bedient, die aus der Hacker-Szene stammen, um die im Unternehmen vorhandenen Systeme auf technische Schwachstellen hin zu untersuchen. Durch unterschiedliche Szenarien kann ermittelt werden, welche Möglichkeiten z. B. ein Angreifer aus dem Internet besitzt, um in Unternehmenssysteme einzudringen, oder sich einem Innentäter (z. B. Reinigungs- oder Servicepersonal) bieten.

Eine umfassendere Untersuchung stellen **Risikoanalysen** dar, bei denen die Auswirkungen von Schwachstellen auf bestimmte Geschäftsprozesse betrachtet werden. Ausgehend von der im IT-Sicherheitshandbuch des BSI beschriebenen Vorgehensweise führt SRC, beginnend mit der Feststellung des Schutzbedarfs (Schutzbedarfsfeststellung) über die Analyse von Bedrohungsszenarien (Bedrohungsanalyse) Risikoanalysen durch. Nach der Durchführung der Bedrohungsanalyse sind die Eintrittswahrscheinlichkeit und die Dauer bestimmter Schadensereignisse bekannt. Anschließend werden die Auswirkungen der Schäden an den IT-Systemen auf die Geschäftsprozesse untersucht und die Höhe der potenziellen Schäden abgeschätzt.



Die so gewonnenen Informationen werden genutzt, um eine Bewertung der Risiken vorzunehmen und diese in tragbare bis untragbare Risiken aufzuteilen.

Unsere Dienstleistungen

SRC führt Sicherheitsuntersuchungen nach einer Vorgehensweise durch, die mit dem Kunden individuell auf seine Bedürfnisse hin abgestimmt ist. Durch die Einbeziehung der Auswirkungen vorhandener Schwächen auf die Geschäftsprozesse ergibt sich hierbei ein Spektrum von sehr technischen Ergebnissen aus den Penetrationstests bis hin zu Ergebnissen im Rahmen von Risikoanalysen. Als Teil der Ergebnisse schlägt SRC kurz-, mittel- und langfristige Maßnahmen vor, mit denen die Schwächen beseitigt und das Sicherheitsniveau dauerhaft erhöht werden kann.

Ihr Nutzen

Die Ergebnisse der von SRC durchgeführten Security Audits werden genutzt, um das aktuelle Sicherheitsniveau der Systemlandschaft unserer Kunden zu beurteilen und erforderliche Maßnahmen abzuleiten. Regelmäßig durchgeführte Sicherheitsuntersuchungen sind fester Bestandteil eines Sicherheitsmanagements und sorgen dafür, dass die Sicherheit betriebskritischer IT-Prozesse unserer Kunden kontinuierlich auf einem hohen Niveau gehalten wird.

SRC Security Research & Consulting GmbH

SRC Security Research & Consulting GmbH wurde im Herbst 2000 von den vier kreditwirtschaftlichen Verlagen Bank-Verlag, Deutscher Genossenschafts-Verlag, Deutscher Sparkassenverlag, und VÖB-ZVD Bank für Zahlungsverkehrsdienstleistungen als unabhängiges Beratungsunternehmen gegründet. SRC bündelt aktuelles Know-how zur Sicherheit in der Informationstechnik und berät und unterstützt seine Kunden bei der Konzeption, der Spezifikation, der Implementierung, dem Betrieb und der Begutachtung sicherer Systeme.

Zur Zeit sind 37 Mitarbeiter an den Standorten Bonn und Wiesbaden beschäftigt. SRC ist ein noch junges Unternehmen mit erfahrenen Mitarbeitern, die zum Teil seit über zehn Jahren im Bereich der IT Sicherheit tätig sind.

Referenzen

Mitarbeiter von SRC haben eine Vielzahl von Sicherheitsuntersuchungen und Risikoanalysen bei Kunden aus unterschiedlichen Bereichen durchgeführt. Hierzu zählen auch Kunden aus dem Banken- und Versicherungsumfeld.

Für weitere Informationen und ein persönliches Gespräch stehen wir Ihnen gerne zur Verfügung.



 Herr Randolf-Heiko Skerka
: randolf.skerka@src-gmbh.de
: +49-(0)228-2806-0
: +49-(0)228-2806-199
 <http://www.src-gmbh.de>

**SRC Security Research &
Consulting GmbH**

Graurheindorfer Straße 149a
53117 Bonn

Sicherheitskonzepte Sicherheitsmanagement Sicherheitspolitik

Im Informationszeitalter haben Informationen und deren Verarbeitung einen besonders hohen Stellenwert für ein Unternehmen. Die Erreichung eines angemessenen Sicherheitsniveaus setzt das Vorhandensein eines funktionierenden Sicherheitsmanagements voraus und ist dabei weit mehr als das Zusammenspiel technischer Sicherheitsmaßnahmen. Die wesentlichen Bestandteile eines Sicherheitsmanagements sind die Sicherheitspolitik, in der die Sicherheitsziele des Unternehmens beschrieben sind und welche von der Geschäftsführung getragen wird.

Die Art und Weise, wie die Sicherheitsziele erreicht werden, wird in Sicherheitskonzepten dokumentiert. Das Sicherheitskonzept ist das zentrale Dokument im Sicherheitsprozess. Jede konkrete Maßnahme muss sich letztlich darauf zurückführen lassen. Es umfasst insbesondere eine Schutzbedarfsfeststellung und, ausgehend von einer Risikoanalyse, Maßnahmen, mit denen das definierte Sicherheitsniveau und damit die Sicherheitsziele erreicht werden können.

Die Steigerung des Sicherheitsbewusstseins bei den Mitarbeitern im Unternehmen ist ein wesentlicher Faktor, um das Sicherheitsniveau langfristig aufrecht erhalten zu können. Die Durchführung von Sicherheitsschulungen ist dabei ein wichtiger Bestandteil der Aufklärung von Mitarbeitern.

Unsere Dienstleistungen

SRC unterstützt Sie bei der Implementierung eines zertifizierbaren (z.B. nach BS 7799 oder IT-Grundschutzhandbuch) Sicherheitsmanagements. Hierzu gehören beispielsweise die Formulierung von Sicherheitspolitiken, die Erstellung von Sicherheitskonzepten und Schwachstellenanalysen, die Schulung von Mitarbeitern sowie die Unterstützung bei der Auswahl von Produkten.

Ihr Nutzen

Wir integrieren Ihr Sicherheitsmanagement in Ihre bestehenden Managementsysteme und nutzen bereits existierende Ansätze, wie sie z.B. aus dem Qualitätsmanagement kommen. Vielfach besitzen Unternehmen bereits Managementsysteme, insbesondere ein ISO-9000-fähiges Qualitätsmanagement, welches effektiv genutzt werden kann, um ein individuelles und auf die Geschäftsziele des Unternehmens abgestimmtes Sicherheitsmanagement zu implementieren.

SRC Security Research & Consulting GmbH

SRC Security Research & Consulting GmbH wurde im Herbst 2000 von den vier kreditwirtschaftlichen Verlagen Bank-Verlag, Deutscher Genossenschafts-Verlag, Deutscher Sparkassenverlag und VÖB-ZVD Bank für Zahlungsverkehrsdienstleistungen als unabhängiges Beratungsunternehmen gegründet. SRC bündelt aktuelles Know-how zur Sicherheit in der Informationstechnik und berät und unterstützt seine Kunden bei der Konzeption, der Spezifikation, der Implementierung, dem Betrieb und der Begutachtung sicherer Systeme.

Zur Zeit sind 37 Mitarbeiter an den Standorten Bonn und Wiesbaden beschäftigt. SRC ist ein noch junges Unternehmen mit erfahrenen Mitarbeitern, die zum Teil seit über zehn Jahren im Bereich der IT Sicherheit tätig sind.

Referenzen

Mitarbeiter von SRC haben in vielen Projekten an der Erstellung von Sicherheitspolitiken und -konzepten mitgewirkt und waren an der Implementierung normkonformer Informationssicherheits-Managementsysteme beteiligt.

Für weitere Informationen und ein persönliches Gespräch stehen wir Ihnen gerne zur Verfügung.



: Herr Randolph-Heiko Skerka
: randolf.skerka@src-gmbh.de
: +49-(0)228-2806-0
: +49-(0)228-2806-199
: <http://www.src-gmbh.de>

**SRC Security Research &
Consulting GmbH**

Graurheindorfer Straße 149a
53117 Bonn

Computer Emergency Response Team (CERT)

Unternehmen müssen zu jeder Zeit in der Lage sein, das vorhandene Sicherheitsniveau einschätzen und ggf. ad-hoc Maßnahmen ergreifen können. Um bei auftretenden Sicherheitsvorfällen schnell zu reagieren und Gegenmaßnahmen frühzeitig zu entwickeln, ist es erforderlich, dass Informationen über Schwächen der eingesetzten Systeme qualifiziert und Maßnahmen erarbeitet werden.

Die Kenntnis aktueller Sicherheitsschwächen und entsprechender Gegenmaßnahmen ist insbesondere bei Systemen von Bedeutung, die über das Internet erreichbar sind. Hierzu ist eine Auswertung von Sicherheitsmeldungen notwendig, die aus unterschiedlichen Quellen, wie z.B. Herstellern, frei verfügbaren Newsletter oder Internet-Seiten stammen. Werden solche Meldungen effizient behandelt und ausgewertet, können sich Unternehmen einen entscheidenden Zeitvorteil bei der Abwehr von Hacker-Angriffen verschaffen.

Ein Computer Emergency Response Team (CERT) ist eine Sammelstelle für die Meldung von Sicherheitsmeldungen und Sicherheitsverstößen. Da ein CERT schnell und einfach für jeden Mitarbeiter im Unternehmen erreichbar sein muss, ist eine spezielle Informationsplattform erforderlich.

Ein CERT muss grundsätzlich drei Eigenschaften erfüllen:

1. Eine zentrale Organisation innerhalb des Unternehmens einnehmen,
2. eine pädagogische Rolle hinsichtlich der Computersicherheit spielen,
3. eine reaktive Rolle bei Sicherheitsverstößen wahrnehmen.

Unsere Dienstleistungen

SRC unterstützt Sie beim Aufbau eines internen CERTs, welches eine zentrale Organisation innerhalb des Unternehmens wahrnimmt, Sicherheitsinformationen analysiert und hieraus spezifische Maßnahmen entwickelt. Ziele unseres Services sind:

- die Konzeption und der Aufbau einer CERT Organisationsstruktur und der geeigneten Informationsplattformen,
- die Entwicklung einer Vorgehensweise für die Auswahl und Weiterverarbeitung relevanter Sicherheitsinformationen aus unterschiedlichen Quellen,
- die Ausbildung der CERT Mitarbeiter und Überführung des CERT in den Betrieb.

Ihr Nutzen

Die Beratungsdienstleistung auf diesem Gebiet berücksichtigt die individuellen Anforderungen der Kunden, wie z.B.

- heterogene Systemlandschaften mit unterschiedlichen Hard- und Softwarekomponenten,
- Bereitstellung von Ressourcen für die Auswertung verschiedener Quellen für Sicherheitsmeldungen,
- unterschiedliche Sicherheitsanforderungen an die eingesetzten Systeme.

Durch den Aufbau einer geeigneten Informationsplattform werden Sicherheitsmeldungen aus unterschiedlichen Quellen bewertet und Maßnahmen schnell und effizient ergriffen. Durch die Auswertung vorhandener Sicherheitsmeldungen kann zu jedem Zeitpunkt das aktuelle Sicherheitsniveau der eigenen Systemlandschaft beurteilt werden. Erforderliche Maßnahmen können eingeleitet und ad-hoc Maßnahmen umgehend getestet und umgesetzt werden. Hierdurch wird die Sicherheit kontinuierlich auf einem hohen Niveau gehalten.

SRC Security Research & Consulting GmbH

SRC Security Research & Consulting GmbH wurde im Herbst 2000 von den vier kreditwirtschaftlichen Verlagen Bank-Verlag, Deutscher Genossenschafts-Verlag, Deutscher Sparkassenverlag, und VÖB-ZVD Bank für Zahlungsverkehrsdienstleistungen als unabhängiges Beratungsunternehmen gegründet. SRC bündelt aktuelles Know-how zur Sicherheit in der Informationstechnik und berät und unterstützt seine Kunden bei der Konzeption, der Spezifikation, der Implementierung, dem Betrieb und der Begutachtung sicherer Systeme.

Zur Zeit sind 37 Mitarbeiter an den Standorten Bonn und Wiesbaden beschäftigt. SRC ist ein noch junges Unternehmen mit erfahrenen Mitarbeitern, die zum Teil seit über zehn Jahren im Bereich der IT Sicherheit tätig sind.

Referenzen

Mitarbeiter von SRC waren maßgeblich am Aufbau und Betrieb des ersten kommerziellen deutschen Computer Emergency Response Teams (CERT) beteiligt.

Für weitere Informationen und ein persönliches Gespräch stehen wir Ihnen gerne zur Verfügung.



 Herr Randolf-Heiko Skerka
: randolf.skerka@src-gmbh.de
: +49-(0)228-2806-0
: +49-(0)228-2806-199
 <http://www.src-gmbh.de>

**SRC Security Research &
Consulting GmbH**

Graurheindorfer Straße 149a
53117 Bonn