G 59071
4,50 EUR*

RATING aktuell

Information für Unternehmen und Finanzdienstleister

01/2004
Februar/März

www.ratingaktuell-news.de
www.ratingaktuell-ticker.de

IT-Sicherheit als Rating-Faktor

Mit Themen-Special Fonds-Rating

UNTERNEHMEN
Bonitätsbewertungen bei Unternehmens-gründungen

MITTELSTAND
Businesspläne beim Rating-Verfahren

MANAGEMENT
Bonität und Rating sind Chefsache

BANKEN
Best Practice der Risiko-Limitierung

RATING
Lieferanten-Rating

FINANZWIRTSCHAFT
Banken-Ratings haben sich stabilisiert

INTERVIEW
Jaim Caruana, Vorsitzender des Baseler Ausschusses im Gespräch

* zzgl. Versand und 7 % MwSt.

IT-Sicherheit als Rating-Faktor

Stefan Hirschmann/Frank Romeike

Auf der einen Seite kann ein leistungsfähiges IT-Sicherheitsmanagement-System dazu beitragen, die von Kreditinstituten für operationelle Risiken zu hinterlegende Eigenkapitalmenge zu reduzieren. Auf der anderen Seite spielt IT-Sicherheit auch im Rating-Prozess eine nicht zu vernachlässigende Rolle. Ausschlaggebend hierfür ist zum einen die gezielte Vermeidung und Reduzierung operationeller Risiken, zum anderen aber auch die sich aus dem IT-Sicherheitsmanagement-System ergebenden Ansätze zur Messung der verbleibenden Rest-Risiken. Hierbei wird insbesondere auch auf die größte Schwachstelle in jedem IT-Sicherheitssystem eingegangen: den Menschen. Welche Bedeutung die IT-Sicherheit – auch und vor allem für Nicht-Banken – hat, zeigt Ihnen dieser Beitrag.

Die schnelle Ausbreitung von Computerattacken über das Internet legt nahe, dass das Sicherheitsbewusstsein im Umgang mit dem Internet häufig nur rudimentär vorhanden ist. Nutzer befallener Rechner bezahlen diese Arglosigkeit im günstigsten Fall mit Beeinträchtigung ihrer Arbeit durch Instabilität des Systems und gelegentlichen Abstürzen, viele Viren oder Würmer zerstören aber auch gezielt den Datenbestand und verursachen irreparable Schäden. Das schwächste Glied in der Kette der IT-Sicherheit ist jedoch in vielen Fällen der Risiko-Faktor Mensch. Einer der meist gesuchten Hacker der USA, Kevin Mitnick, überlistete praktisch jedes Sicherheitssystem, indem er Passwörter erschlich, die er einfach erfragte, oder in Mülltonnen (Dumster Diving) nach sicherheitsrelevanten Informationen suchte. IT-Sicherheit ist nur sekundär ein technologisches Problem, sondern vor allem ein menschliches und ein Management-Problem. So ist der größte Computerbetrug durch Stanley Mark Rifkin bei der Security Pacific National Bank in Los Angeles auf Social Engineering, also durch Techniken der Beeinflussung und Überredungskunst zur Manipulation oder zur Vortäuschung falscher Tatsachen, zurückzuführen.

Neue Generation von Viren

Erfolgreiche Social Engineers besitzen meist sehr gute soziale Kompetenzen, sind sympathisch und charmant und besitzen häufig nur ein eingeschränktes technisches Verständnis. Wenn sich ein Betrüger erst einmal in das Vertrauen eines Unternehmens eingenistet hat, wird damit die Zugbrücke heruntergelassen, und das Burgtor öffnet sich weit, so dass er die Festung betreten und alle gewünschten Informationen mitnehmen kann. Während sich die Mehrzahl der bisher bekannten Computer-Viren in der Regel über die an E-Mails angehängten Dateien verbreiteten, infiltriert eine neue Generation von Viren wie „Blaster“ und „Lovsan“ schon bei bloßer Internet-Verbindung, also ganz ohne Zutun des Anwenders, das System. PCs, mit denen ungesichert im Internet gesurft wird, sind über eine Sicherheitslücke im Betriebssystem aus dem Internet angreifbar. Dazu scannen bereits mit dem Virus infizierte Systeme zufällige Internet-Rechner-Kennungen (IP-Adressen). Kann eine Verbindung zu einem anderen Rechner hergestellt werden, verschickt der Wurm Daten an diesen und befällt ihn. So beginnt ein neuer Infektionszyklus und der angegriffene Rechner wird selbst zum Angreifer. Verbriefte Zahlen über das Gesamtausmaß einer Attacke sind zwar kaum zu erheben, doch ist die geschätzte Größenordnung von einzelnen Viren befallener Rechner (120.000 bis 1,4 Mio.) insbesondere dann eine beachtliche Anzahl, wenn man bedenkt, dass der Schwachpunkt im Betriebssystem, über den sich Würmer wie „Blaster“ und „Lovsan“ Zutritt verschaffen, bereits Wochen vor seinem Erscheinen bekannt war und von Sicherheitsexperten kommuniziert wurde. Dennoch fand der Wurm nicht nur in die Systeme der weniger versierten Privatnutzer seinen Weg, sondern auch in die der Professionals. Trotz zahlreicher Warnungen sparen Unternehmen auch heute noch an ihrer IT-Sicherheit, wie eine aktuelle Studie der Wirtschaftsprüfungsgesellschaft Ernst & Young belegt. Ein Drittel der 1.400 befragten Unternehmen aus 66 Ländern räumt demnach ein, im Fall eines Angriffs auf ihre Computersysteme nur unzureichend reagieren zu können. Rund 55 % gaben an, dass Budget-Beschränkungen der häufigste Grund für die Zurückhaltung bei IT-Investitionen seien. Auf große Katastrophen sind viele Unternehmen nach eigenem Bekunden vorbereitet, bei alltäglichen Risiken, wie z. B. dem Diebstahl geschützter Informationen oder einer Attacke durch Viren und Würmer, sind sie jedoch verwundbar. Andere Würmer, wie etwa Love Letter oder Anna Kournikova, haben sich alle bei der Verbreitung auf die Techniken des Social Engineering verlassen.

Operationelle Risiken und IT-Sicherheit in Banken

Kreditinstitute, die auf Grund der weltweiten Verknüpfung ihrer Systeme besonders anfällig für Attacken von Hackern sind, haben sich des Problems bereits vor Jahren angenommen. Die systemtechnischen Sicherheitsvorkehrungen bedürfen aber nicht zuletzt wegen der hohen Sensibilität der Daten einer permanenten Weiterentwicklung. Schon heute ergeben sich aus einer Reihe von gesetzlichen Regelungen (KonTraG, KWG, MaK usw.) Anforderungen an das Risiko-Management und die Sicherheit der Informationsverarbeitung in Kreditinstituten. Auch die neue Baseler Eigenkapitalübereinkunft (Basel II) verlangt explizit eine Hinterlegung so genannter operationeller Risiken mit Eigenkapital. Und Risiken, die sich aus der Nutzung moderner Informationstechnologien ergeben, gelten als zentraler Bestandteil der operationellen Risiken. „Da die Informationstechnologie heute in vielen Fällen die Geschäftsprozesse der Banken vollständig determiniert, sind Risiken in der IT-Sicherheit aus Sicht der operationellen Risiken wohl die größten Risiken überhaupt, denen sich ein Kreditinstitut ausgesetzt sieht“, sagt Detlef Kraus, IT-Sicherheitsexperte bei SRC Security Research & Consulting GmbH. Das Bonner Unternehmen unterstützt vorrangig Banken bei der Entwicklung und Implementierung sicherer Systeme, fungiert aber auch als

Bindeglied zwischen Forschung und innovativen IT-Dienstleistungen. Der Identifizierung bestehender Risiken im IT-Betrieb bzw. der Einrichtung entsprechender Schutzmaßnahmen komme allergrößte Bedeutung zu, so Kraus weiter, da Vertrauen und Glaubwürdigkeit – und damit letztlich die Reputation einer Bank – wesentlich von der Sicherheit und der Zuverlässigkeit der Prozesse im Kreditinstitut abhänge. Technische Schutzmaßnahmen, wie die Installation von Firewalls, seien dabei nur ein Element des ganzheitlichen IT-Sicherheitsmanagements. Besondere Bedeutung kommt nach Ansicht von SRC auch den organisatorischen und personellen Vorausetzungen zu. „Die Erreichung der IT-Sicherheitsziele einer Bank kann nur gewährleistet werden, wenn das IT-Sicherheitsmanagement als Prozess übergreifend über alle Geschäftsbereiche verankert ist", sagt Kraus. Mit Standards wie dem Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie ISO/IEC 17779 bzw. BS 7799-2 stünden hierfür allgemein anerkannte Methoden zur Verfügung, die es erlauben, gegenüber Aufsichtsbehörden und Kunden die Implementierung eines den Anforderungen entsprechenden IT-Sicherheitsmanagementsystems nachzuweisen. Neben der Identifikation erweist sich jedoch insbesondere die Quantifizierung operationeller Risiken als äußerst komplex. Operationelle Risiken und hier speziell IT-Risiken gelten als nicht vollständig quantifizierbar. Eine (ökonomische oder regulatorische) Eigenkapitalunterlegung setzt voraus, dass Risiken quantifiziert werden können. Die unterschiedlichen Methoden zur Quantifizierung operationeller Risiken befinden sich daher erst im Anfangsstadium. Einen ersten Schritt haben die meisten Banken in der Zwischenzeit jedoch gemacht: Sie sammeln gezielt operationelle Risiken und Verlustinformationen und versuchen daraus die Eintrittswahrscheinlichkeit und das Schadensausmaß für bestimmte Risiko-Kategorien abzuleiten. Ziel ist vor allem die Ableitung des erwarteten Verlustes („Expected Loss") sowie die Ermittlung des „Unexpected Loss". Allgemein können die verschiedenen Bewertungsansätze in quantitative und qualitative Methoden unterteilt werden (Abbildung 1).

Die meisten quantitativen Ansätze basieren auf der Wahrscheinlichkeitsrechnung, während qualitative Ansätze eher auf subjektiven erfahrungsbezogenen Werteinschätzungen beruhen. Die vom Baseler Komitee vorgeschlagenen Methoden zur Eigenkapitalunterlegung unterscheiden sich in Komplexität und Risiko-Sensitivität. Während bei den „einfachen" Ansätzen entweder ein einzelner Indikator oder ein Indikator pro Geschäftsbereich für die grobe Abschätzung der operationellen Risiken steht, wird bei den fortgeschrittenen Verfahren auf die internen Daten der Bank für Verlustereignisse abgestellt. Ein leistungsfähiges IT-Sicherheitsmanagement-System führt daher zu geringeren Schäden und in der Folge auch zu einer reduzierten (regulatorischen) Eigenkapitalunterlegung.

Sicherheitskonzepte kein exklusives Problem der Großen

Die aus operationellen Risiken entstehende Gefahr eines direkten oder indirekten Verlusts, der auf Grund einer fehlerhaften Geschäftsentwicklung, eines Systemfehlers, eines menschlichen Fehlverhaltens oder externer Einflüsse eintreten kann, ist aber kein genuines Problem von Banken oder anderen Großunternehmen. Jedes vierte mittelständische Unternehmen verfügt über keinerlei Notfallregelungen, falls die IT ausfällt oder durch Hackerangriffe lahm gelegt wird, so das Ergebnis einer SerCon-Studie. SerCon ist als Tochtergesellschaft der IBM Deutschland GmbH auf die Beratung des Mittelstandes spezialisiert. Auch kleine und mittlere Unternehmen, die sich keinen ausgewiesenen IT-Verantwortlichen leisten, sind gut beraten, einen IT-Sicherheitsprozess zu installieren – notfalls mit professioneller Unterstützung von außen. Über einen gesicherten Internet-Zugang, wie ihn beispielsweise der Nürnberger IT-Dienstleister Datev eG anbietet, wird der Zugang ins Internet über einen externen Provider realisiert, so dass der Anwender

Abbildung 1: Bewertungsmethoden für operationelle Risiken

	Quantitativ	Qualitativ
Bewertungsmethode	Ausgaben-/gewinnorientierte Ansätze	Key Performance Indicator (KPI)
	Zufallsverteilungen	Key Control Indicator (KCI)
	Economic Pricing-Modelle	Key Risk Indicator (KRI)
	Extremwert-Theorie (EVT)	Nutzwertanalyse
	Szenarioanalyse	Baumanalyse
	Simulationsmodelle	Szenarioanalyse (subjektiv)
	Ansatz der Zuverlässigkeitstheorie	Expertenbefragung/Interview Prozess-Risiko-Analyse

von einem Schutzmechanismus profitiert, der umfangreicher und wirkungsvoller ist als eine einfache Firewall. Ob beim Surfen im Internet, beim Download aus dem Web oder beim E-Mail-Verkehr: Geht der Anwender über einen gesicherten Internet-Zugang, so holt oder schickt er Daten niemals direkt aus dem Internet. Er nimmt den Datenaustausch immer über spezielle Serversysteme vor, die jeweils noch einmal abgesichert sind. Nur was während des Checks in der Sicherheitszone als ungefährlich eingestuft wird, gelangt auf den Rechner des Nutzers. Die Sicherheitszone des Providers sollte dabei nach einem mehrstufigen Konzept aufgebaut sein. Die Verbindung mit dem Internet läuft gewissermaßen durch einen Sicherheitsfilter in Form einer Internet Service Area (ISA). Diese ISA ist als zentrale Sicherheitsinfrastruktur mit einer Reihe von Firewalls und Virenscannern versehen, die von Sicherheitsexperten und -systemen rund um die Uhr überwacht und stets auf dem neuesten Stand gehalten werden. Aus Gründen der Ausfallsicherheit sind alle Systeme redundant an verschiedenen Standorten aufgebaut. In der internen Firewall zwischen ISA und den Anwendersystemen sind immer nur die wirklich benötigten Kommunikationswege (Ports) geöffnet, alle weiteren bleiben fest verschlossen. Mit Hilfe mehrerer Firewall-Systeme werden innerhalb der ISA verschiedene Sicherheitszonen gebildet. Der Datenverkehr zwischen diesen Zonen wird genauestens untersucht. Innerhalb der ISA übernehmen mehrere unabhängig voneinander arbeitende Systeme die Virenprüfung. Die übertragenen Daten werden hier zerlegt, die einzelnen Fragmente durch eine Reihe verschiedener Virenscanner geprüft. So lassen sich u. a. auch gepackte Archive durchsuchen. Damit die Systeme stets auf neuestem Stand sind, wird die Aktualität der verwendeten Virendaten mehrmals täglich geprüft beziehungsweise durch die einzelnen Hersteller automatisch aktualisiert. Für den Anbieter bedeutet das einen enormen Aufwand. Doch der ist nötig, um möglichst alle schädlichen Aktivitäten aufzudecken. Neben der zentral betreuten Sicherheitszone gehört im Falle der Datev-Lösung (DATEVnet) auch ein Virenschutzsystem auf dem Rechner des Nutzers zum Sicherheitskonzept. Ein lokal installierter Virenscanner erkennt auch Viren und

trojanische Pferde, die sich auf Datenträgern (wie z. B. Disketten oder CDs) verstecken oder auf Grund ihrer Verschlüsselung in den Viren-Komponenten der ISA nicht erkannt werden können. Hierbei muss jedoch beachtet werden, dass der technologische State-of-the-art-Schutz immer nur eine Seite der Medaille ist. Klare Anweisungen für Mitarbeiter zum Schutz von Informationen sind eine weitere fundamentale Grundlage bei der Entwicklung effizienter Kontrollen, um potenziellen Sicherheitsbedrohungen zu begegnen. So kann etwa eine klare Sicherheitsrichtlinie und eine gelebte Sicherheits- und Risikokultur das Risiko von Social-Engineering-Angriffen drastisch reduzieren.

Viren- oder Wurm-Attacken

Welches Ausmaß die Angriffswellen von Viren- oder Wurm-Attacken bereits angenommen haben, demonstriert ein monatlich erstellter Sicherheitsreport des Nürnberger IT-Dienstleisters. Hier sind jeweils die Ausmaße der Angriffe einzusehen, denen die nachgeschalteten Systeme ohne die Schutzfunktion ausgesetzt wären. Denn in der ISA wird der Datenverkehr kontinuierlich auf sicherheitsrelevante Vorkommnisse hin überprüft. Protokolliert werden u. a. die Anzahl der abgewehrten Eindringversuche, die als Kategorie der Informationssuche zur Vorbereitung eines Angriffs, dem Versuch eines unberechtigten Zugriffs, dem Versuch, durch hohe Last die Dienstverfügbarkeit zu behindern („Denial of Service"-Angriffe), sowie verdächtigen Aktivitäten, die von den Mustern des „normalen" Internet-Verkehrs abweichen, zugeordnet werden können. Gemäß dieser Abwehr-Statistik waren in den vergangenen Monaten des Jahres 2003 allein bei der Datev jeweils zwischen 1,6 und 4,7 Millionen Versuche unautorisierten Zugriffs zu verzeichnen. So registrierten und blockierten die Überwachungssysteme zur Spitzenverbreitungszeit der Grundversion des Wurms Blaster/Lovsan allein an einem einzigen Tag und nur auf dem betroffenen Port 135 über 1,5 Millionen Zugriffsversuche. Nach Hinzukommen weiterer Wurm-Varianten wurde an einem Tag sogar über 2,5 Millionen Mal verhindert, dass sich einer der Würmer Zutritt verschafft (Abb. 2). An den stark erhöhten Verbindungsversuchen auf Port 135 lässt sich die zunehmende Verbreitung des Computer-Wurms im Internet ablesen, deren Höhepunkt offensichtlich am 12. August 2003 erreicht war. Die Anzahl der geblockten Verbindungsversuche auf dem betroffenen Port waren danach zunächst rückläufig, aber immer noch auf sehr hohem Niveau. Am 19. August lässt sich ein signifikanter Anstieg der Aktivitäten konstatieren, was die Vermutung nahe legt, dass inzwischen neue Versionen des Wurms in Umlauf waren, die dieselben Einfallstore und Mechanismen nutzten.

Abb. 2: Aktivitäten der Blaster / Lovsan-Wurmfamilie

Datum	Geblockte Eindringversuche
07. August 2003	31.144
08. August 2003	49.573
09. August 2003	30.037
10. August 2003	42.054
11. August 2003	398.141
12. August 2003	1.528.710
13. August 2003	852.606
14. August 2003	763.033
15. August 2003	581.944
16. August 2003	573.972
17. August 2003	556.861
18. August 2003	579.324
19. August 2003	1.829.318
20. August 2003	2.571.012
21. August 2003	2.418.355

Anzahl der durch DATEVnet abgelehnten Verbindungsversuche aus dem Internet auf Port 135
Quelle: Datev

Um optimalen Schutz zu gewährleisten, muss der Anwender allerdings selbst darauf achten, dass auf seinem Rechner nicht parallel zum geschützten Zugang eine ungeschützte Verbindung mit dem Internet etabliert wird. Dies wiederum offenbart ein grundsätzliches Problem, dem sich in noch stärkerem Maße Kreditinstitute gegenüber sehen. Das teilweise oder vollständige Outsourcing der IT-Infrastruktur kann insbesondere für Banken und Sparkassen zu Kosten- und letztlich auch zu Wettbewerbsvorteilen führen. Gleichwohl ist aber auch ein Outsourcing nicht frei von operationellen Risiken. Wenn der Betrieb von IT-Systemen an Dienstleister ausgelagert wird, bleibt die letztendliche Verantwortung für die zuverlässige und sichere Abwicklung von Prozessen doch beim Kreditinstitut selbst. Ein Teufelskreis? Von entscheidender Bedeutung für das IT-Sicherheitsmanagement im Outsourcing sind die vereinbarten Service Level Agreements (SLA), in denen die vereinbarten Leistungen, ihr Niveau und die Rahmenbedingungen für ihre Erbringung festgelegt werden. Hierbei sollten auch die Forderungen der BaFin (Rundschreiben 11/2001) berück-

sichtigt werden. Eine gute Sammlung von „Best Practices“ im Outsourcing liefert die öffentlich zugängliche „IT Infrastructure Library“ (www.itil.org.uk). Danach wird IT-Sicherheitsmanagement als kontinuierlicher Regelkreis mit den folgenden Prozessen begriffen:

- Service Level Management,
- Availability Management,
- Performance and Capacity Management,
- Business Continuity Planning,
- Financial Management and Costing,
- Configuration and Asset Management,
- Incident Control/Helpdesk,
- Problem Management,
- Change Management,
- Release Management.

Durch einen solchen IT-Sicherheitskreislauf kann sowohl der Outsourcing-Anbieter als auch der Kunde die operationellen Risiken und in der Folge auch die Kosten reduzieren.

Notfallplanung in Kreditinstituten

Produkte, Prozesse und Technologien haben eine früher nicht gekannte Komplexität erreicht. Die durch den Einsatz neuer Technologien gestiegenen Abwicklungsgeschwindigkeiten führen dazu, dass im Falle eines Fehlers schnell große Schäden entstehen können. Vor allem in der Kreditwirtschaft hat das Management operationeller Risiken – auch unabhängig von Basel II – in den letzten Jahren deshalb einen stark gestiegenen Stellenwert erhalten. Internet-basierte Technologien sind zwischenzeitlich globaler Standard und ermöglichen übergreifende Koordination, Effizienz und Flexibilität. Aber was sind hierbei die Schlüsselfaktoren? „Eine hohe Systemverfügbarkeit und Benutzerfreundlichkeit, eine proaktive Notfallplanung inklusive einer sog. Disaster Recovery-Planung sowie die regelmäßige Überprüfung der festgelegten Sicherheitsstandards spielen eine besonders wichtige Rolle“, erklärt SRC-Sicherheitsexperte Kraus. Speziell für Kreditinstitute, bei denen das IT-Sicherheitsmanagement bekanntlich zentraler Bestandteil des Managements operationeller Risiken ist, hat das Unternehmen einen Katalog typischer Fragestellungen entworfen, die von den Bankmitarbeitern zu beantworten sind. Als Kernfelder sind hierbei etwa folgende Themen zu bearbeiten:

- Inwieweit ist der Schutz von Daten und Informationstechnologie Bestandteil der Unternehmenskultur eines Kreditinstituts?
- 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?
- In welchem Maße sind vernetzte Systeme durch Firewalls geschützt, die den Informationsfluss zur Außenwelt kontrollieren?
- Sind die Firewalls so konfiguriert, dass das Schutzziel auch erreicht wird?
- Inwieweit ist die Sicherheit von Prozessen von der Sicherheit verbundener Netze abhängig?
- Werden Software-Updates regelmäßig vorgenommen?
- Werden die IT-Systeme regelmäßig von IT-Spezialisten im Hinblick auf Möglichkeiten zum Umgehen von Sicherheitsmaßnahmen überprüft?
- Sind die im Notfall erforderlichen Maßnahmen klar dokumentiert?
- Sind die Zuständigkeiten für den Notfall klar und eindeutig geregelt?

Sicherheitsmaßnahmen können nie hundertprozentige Sicherheit gewährleisten. Bei der IT-Sicherheit geht es daher vor allem um die Vermeidung und Reduzierung von Risiken, die Entdeckung von Attacken, die Reduktion der Auswirkungen 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. „Je aufwändiger die Technik, umso vielfältiger sind auch ihre Einsatzmöglichkeiten für kriminelle Anwendungen“, erklärt Dr. Hans Daldrop, Geschäftsführer der Tintrup Computer GmbH, Lüdinghausen. „Wo ein Dietrich nur dem Einbrecher, ein Schneidbrenner allein dem Safeknacker nützen mag, sind Computer universelle Werkzeuge für Hacker – Einfallsreichtum und Elektronikkenntnisse vorausgesetzt“. Daldrop und seine Mitarbeiter entwerfen und realisieren Security-Konzepte mit Firewall-Systemen, um Daten vor Beschädigung, Diebstahl, Manipulation oder Verlust zu schützen. Aus seiner täglichen Arbeit mit mittelständischen Unternehmen weiß der Computerfachmann, dass die Dimension der Risiken, die von Sicherheitslücken in der IT-Infrastruktur ausgehen, in den meisten Unternehmen noch gar nicht in voller Schärfe erkannt ist. „Selbst stabilste und modernste EDV-Hardware ist ständig potenziellen Gefahren ausgesetzt. Wenn die Anlage plötzlich nicht mehr zur Verfügung steht und Mitarbeiter

nicht mehr auf die internen Anwendungen und Daten zurückgreifen können, ist die Firma blockiert", so Daldrop. Für jede Minute Betriebsausfall entstehen kaum zu unterschätzende Kosten. Bei Kreditinstituten kann der totale Systemzusammenbruch mitunter die Existenz gefährdende Konsequenzen nach sich ziehen. Deshalb ist eine klare und effiziente Notfallplanung erforderlich. Hierzu gehört neben der Sicherung betriebsnotwendiger Informationen vor allem eine praxistaugliche Struktur von Maßnahmen und Verantwortlichkeiten. Die Auslagerung des kompletten IT-Betriebs mag sich in diesem Zusammenhang als passende Lösung anbieten, ist jedoch auch mit wichtigen Auflagen verbunden, da Banken im Outsourcingfall gegenüber den Aufsichtsbehörden sicherstellen müssen, dass die Sicherheit der Informationssysteme gewährleistet bleibt. Dementsprechend schreibt das Kreditwesengesetz (§ 25 a Abs. 1 KWG Nr. 2) vor, dass Kreditinstitute über angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung verfügen müssen. Die Auslagerung von Bereichen auf ein anderes Unternehmen, die für die Durchführung der Bankgeschäfte oder Finanzdienstleistungen wesentlich sind, darf weder die Ordnungsmäßigkeit dieser Geschäfte oder Dienstleistungen, noch die Steuerungs- und Kontrollmöglichkeiten der Geschäftsleitung noch die Prüfungsrechte und Kontrollmöglichkeiten des Bundesaufsichtsamtes beeinträchtigen (§ 25 a Abs. 2 Satz 1 KWG). Dabei steht in der Regel die Sicherheit bei der Abwicklung von Finanztransaktionen 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 Hauptaugenmerk liegt dabei auf der Abdeckung sämtlicher Aspekte eines effizienten IT-Sicherheitsmanagement-Systems (Durchführung von Security Audits, Security Assessments, Penetrationstests und Risiko-Analysen; Erstellung von Sicherheitskonzepten und Sicherheitspolitiken; Aufbau firmeninterner Computer Emergency Response Teams u. a. m.). Im Rahmen der Implementierung eines solchen Systems werden die unternehmensinternen Sicherheitsziele und -maßnahmen überprüft und sowohl nach organisatorischen als nach wirtschaftlichen Gesichtspunkten angepasst bzw. optimiert. Die ergriffenen Schutzmaßnahmen sollen mögliche Schäden verhindern, ein einheitliches Schutzniveau für die Informationsverarbeitung in der Bank sicherstellen sowie den Stand der Technik überprüfen bzw. aktualisieren. Mit Blick auf Basel II kann ein IT-Sicherheitsmanagement-System dazu beitragen, die für operationelle Risiken zu hinterlegende Eigenkapitalmenge zu minimieren. 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 Rest-Risiken. Die Überprüfung des Systems durch externe Audits ermöglicht nachweisbare Sicherheit in den Geschäftsprozessen. „Vor allem bei Streit- und Regressfällen kann dies von großer Bedeutung sein", weiß Sicherheitsexperte Kraus, da die Zertifizierung des Systems einen unabhängigen Nachweis über ein dem aktuellen Stand der Technik entsprechendes Sicherheitsmanagement darstellt. Und: IT-Sicherheit ist auch immer eine Frage der richtigen Balance. Ein Übermaß an IT-Sicherheit hemmt den Erfolg des Unternehmens, während zu wenig Sicherheit angreifbar macht. Ziel muss ein Ausgleich zwischen Sicherheit und Produktivität sein. Vergessen werden sollte auch nicht das schwächste Glied in der Kette eines IT-Sicherheitssystems: der Mensch! Wie gut IT-Sicherheit funktioniert, hängt im Wesentlichen von den folgenden Faktoren ab:

- Hardware: alle technischen Faktoren, wie etwa Firewall/Brand- und Explosionsschutz
- Software: alle Prozesse und Methoden, d. h. alle organisatorischen Faktoren
- Lifeware: alle menschlichen Faktoren, vor allem die Sicherheitskultur im Unternehmen

Insbesondere die Lifeware, also die Risiko-Kultur im Unternehmen, wird sehr häufig vernachlässigt. Eine Studie der Management- und IT-Beratung Cap Gemini Ernst & Young in Zusammenarbeit mit dem Institut für Kapitalmarktforschung und Finanzierung der Ludwig-Maximilian-Universität München kam zu dem Ergebnis, dass „weiche Faktoren" die höchste Bedeutung für ein erfolgreiches Management operationeller Risiken bei Kreditinstituten (OR) haben.[1] Mehr als 80 % der Studienteilnehmer nannten die Etablierung einer offenen Risiko-Kultur als den wichtigsten Erfolgsfaktor, um operationelle Risiken effektiv zu steuern. Weitaus weniger erfolgskritisch schätzen die befragten Führungskräfte die Ausstattung der Abteilung mit Mitarbeitern und Budget ein.

1 Cap Gemini Ernst & Young Studie: Operationelle Risiken bei Kreditinstituten, Trends & Best Practice, Berlin, November 2002.