

ware in den kommenden zwölf Monaten vermehrt Angriffe auf das iPhone und das Android-Betriebssystem für Mobiltelefone. Die ersten Schadprogramme für diese Plattformen wurden bereits im Jahr 2009 entdeckt. Im Gegensatz zu iPhone-Benutzern, die nur bei infizierten Geräten gefährdet sind, laufen Android-Anwender ständig Gefahr, sich mit Malware zu infizieren, weil Fremdsoftware auf diesen mobilen Endgeräten in der Regel nicht adäquat geschützt ist. So genannte „App-Stores“ haben im Moment Hochkonjunktur, ob Nokia oder Research-in-Motion - alle wollen es Apple nachmachen. Doch trotz umfassender Sicherheitstests der Hersteller sind die Apps längst nicht so sicher, wie sie scheinen. Anfang des Jahres wurde eine Trojaner-verseuchte Banking-Anwendung für Android gefunden, andere werden

folgen. Das ist eine Sache, solange das Telefon nur privat zum Einsatz kommt. Doch Smartphones und ganz besonders das iPhone breiten sich auch in der Unternehmenswelt massiv aus.

Heiter oder wolkig?

Bei einem Thema war sich wirklich jeder Hersteller im Sicherheitsbereich einig: Cloud Computing wird der Megatrend 2010. Für den BITKOM hat das mit der Wirtschaftslage zu tun. „Cloud Computing ist kostengünstiger, weil Unternehmen nicht sämtliche IT-Ressourcen vorhalten müssen, sondern je nach Bedarf online darauf zugreifen können“, sagte Scheer. Zusätzlich werden die Unternehmen flexibler. Bei Reorganisationen oder Fusionen können sie ihre betrieblichen

Abläufe mit Cloud Computing schnell anpassen. Dass viele Entscheider und Techniker gleichermaßen wegen der ungeklärten Sicherheitsfragen beim Cloud-Prinzip große Bauchschmerzen haben, ist dem BITKOM auch aufgefallen. So müsste gerade beim Outsourcing von betrieblichen Prozessen oder dem Zugriff auf externe Anwendungen und Datenspeicher in einer Cloud, ein möglichst wirkungsvoller Schutz gewährleistet sein.

Wie der auszusehen hat, wenn ein fremder Dienstleister über die Daten nicht nur im Transit, sondern auch an der Destination sowie während der Bearbeitung durch die Applikationen verfügt, ist allerdings offen. Der Infodienst IT-Grundschutz wird das Thema in einer der nächsten Ausgaben rechtlich und vom organisatorischen Standpunkt her beleuchten.

Das richtige Werkzeug für den Job

Anforderungen an ein modernes ISMS

Lars Rudolff, Management Consultant, Secaron AG

Das richtige Tool kann sowohl das Information Security Management als auch das Business Continuity Management erleichtern. Wichtig für die Auswahl sind eine gründliche Planung im Vorfeld und die Kenntnis der eigenen Stärken und Schwächen.

Sicherheitsmanager und Notfallmanager haben zahlreiche Aufgaben im Unternehmen. Sie müssen unter anderem Risiken identifizieren, bewerten und steuern, regulatorische Anforderungen erfüllen und die Organisation optimal auf alle Eventualitäten vorbereiten. Je größer die Organisation ist, desto komplexer sind diese Aufgaben und

desto mehr Daten fallen dabei an, die verwaltet und vor allem ausgewertet werden müssen

Die Herausforderung für Sicherheitsmanager und Notfallmanager ist es, die wirklich kritischen Informationen und Geschäftsprozesse zu identifizieren und den Risiken angemessene Maßnahmen zu

ergreifen. Alles in gleichem Maße zu betrachten und zu schützen, wäre weder hinsichtlich der benötigten Ressourcen noch aus rein finanzieller Sicht vertretbar. Es geht darum, genug Überblick und Kenntnis über alle wesentlichen Geschäftsprozesse und Informationen zu erlangen und in einem geordneten und transparenten Verfahren eine Priorisierung

im Hinblick auf deren Kritikalität vorzunehmen. Durch die Konzentration auf das Wesentliche können die Ressourcen und das Budget des Sicherheits- und Business Continuity-Managements gezielt zur Senkung von kritischen Risiken eingesetzt werden. Gleichzeitig werden zwei Wirtschaftlichkeitsaspekte berücksichtigt: die Wirtschaftlichkeit der Managementsysteme und die der Maßnahmen.

Prozessorientierung im Trend

Darüber hinaus müssen Sicherheitsmanager und Notfallmanager in regelmäßigen Abständen Berichte für das Management, einzelne Fachbereiche und das operationelle Risikomanagement der betreffenden Organisation erstellen, um die notwendige Transparenz und damit Aufmerksamkeit für diese beiden wichtigen Themen zu schaffen. In Organisationen mit mehreren

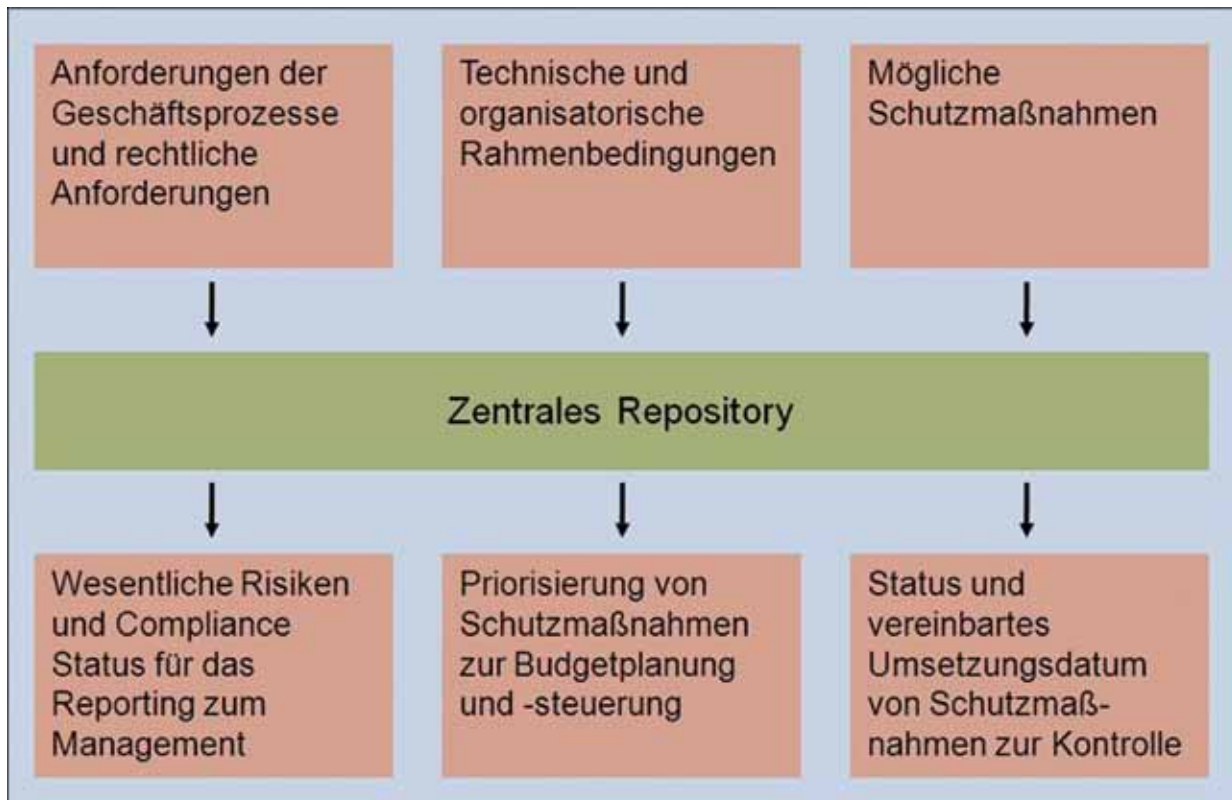
hundert IT-Anwendungen und Geschäftsprozessen ist dies eine komplexe Aufgabe. Die Erstellung eines einzigen Berichts kann unter Umständen mehrere Wochen in Anspruch nehmen.

In den letzten Jahren zeichnet sich bei vielen Organisationen in Deutschland und Europa ein Trend zur prozessorientierten Vorgehensweise in der Informationssicherheit und im Business Continuity Management ab. Ziel ist es, Bewertungen, Analysen und Konzepte in einem transparenten und reproduzierbaren Verfahren zu erstellen und aktuell zu halten. Beispiele hierfür sind die Identifikation und Bewertung von Risiken, die Prüfung gegen interne oder externe Vorgaben sowie die Erstellung, Pflege und der Test von Notfallplänen. Oft werden Elemente des Information Security Management wie auch des Business Continuity Management in der Projektvorgehensweise und anderen Prozessen der Organisati-

on verankert. Wichtig ist auch das Einbinden der Verantwortlichen für die Informationen und Geschäftsprozesse.

Dies hat einerseits rein operative Gründe. Eine zentrale Stelle kann viele Aspekte - wie zum Beispiel den Schaden beim Ausfall eines einzelnen Geschäftsprozesses - nur schwer oder gar nicht bewerten. Andererseits gibt es dafür interne und externe Vorgaben, beispielsweise von Wirtschaftsprüfern, der internen Revision und von den jeweiligen Standards BS ISO/IEC 27001 für die Informationssicherheit und BS 25999 für das Business Continuity Management. Alle fordern die Nachvollziehbarkeit aller wesentlichen Tätigkeiten. Und die ist ohne einen geregelten Prozess kaum zu erreichen.

Ein weiterer wichtiger Trend ist ein ganzheitliches, integriertes Managementsystem, das neben Informationssicherheit und Busi-



Arbeitsweise moderner ISMS oder BCMS Tools

ness Continuity Management auch Dinge wie Qualitätsmanagement und Umweltmanagement umfassen kann. Dabei werden insbesondere:

- Anforderungen übergreifend erfasst. Zum Beispiel indem eine Business Impact Analyse aus dem Business Continuity Management um Aspekte der Informationssicherheit ergänzt wird,
- Maßnahmen zwischen den unterschiedlichen Bereichen priorisiert und koordiniert oder
- Informationen zu einem übergreifenden Berichtswesen zusammengefasst.

Diese Trends sind aus fachlicher Sicht sinnvoll und eine konsequente Weiterentwicklung. Sie bringen jedoch eine Erhöhung der Komplexität mit sich sowie eine steigende Menge der zu verarbeitenden Informationen. Dabei besteht die Gefahr, dass Sicherheitsmanager und Notfallmanager oder deren Teams aufgrund der Masse an Informationen den Blick für das Wesentliche verlieren oder mit Routine-tätigkeiten unverhältnismäßig viel Zeit verbringen. Damit würden sich viele der Vorteile eines modernen BCMS und ISMS relativieren.

Anforderungen an ein Softwarewerkzeug

Um die oben beschriebenen Entwicklungen optimal umsetzen zu können, ist ein Softwarewerkzeug unerlässlich. Ein gutes Tool erlaubt es, Informationen dezentral zu erfassen, aber zentral zu sammeln, zu konsolidieren und unter unterschiedlichen Gesichtspunkten auszuwerten.

Mögliche Tools reichen von Textverarbeitungs- und Tabellenkalkulationsprogrammen über individuelle Datenbanklösungen bis hin zu umfangreichen Softwarelösungen, die speziell zu diesem Zweck ent-

wickelt wurden. Wichtig sind für den Sicherheitsmanager wie auch den Notfallmanager in erster Linie die folgenden Aspekte:

- Eine einfach zu bedienende Oberfläche, in der sich auch Mitarbeiter zurechtfinden, die das Tool nur selten nutzen, zum Beispiel um einmal pro Jahr die Business Impact Analyse zu aktualisieren.
- Ausreichend Flexibilität, um die zur Organisation passenden Prozesse und Methoden optimal abbilden zu können.
- Ein flexibles Berechtigungskonzept, um die unterschiedlichen Rollen in den Prozessen abzubilden.
- Umfassende und individuelle Auswertungsmöglichkeiten, um schnell und einfach die wichtigen Informationen herauszufiltern.
- Notwendige Schnittstellen, um vorhandene Datenbestände zu nutzen und Redundanzen zu vermeiden.
- Problemlose Erweiterbarkeit, um auch künftige Anforderungen erfüllen zu können.

Bei Auswahl und Einführung eines Tools zur Unterstützung eines ISMS oder BCMS gibt es grundsätzlich zwei unterschiedliche Herangehensweisen:

- 1) Wenn sich eine Organisation in der Phase befindet, in der die Methoden und Prozesse erst noch definiert und etabliert werden müssen, kann der Einsatz einer Standardlösung wertvolle Hilfestellung leisten. Voraussetzung ist aber, dass sich die Lösung an Best-Practice-Ansätzen und anerkannten Standards orientiert.
- 2) Wenn eine Organisation bereits Methoden und Prozesse etabliert hat, zählt in erster Linie die Flexi-



Lars Rudloff, ist bei der Secaron AG als Management Consultant für den Bereich IT-Risikomanagement und die integrierte Sicherheits- und Notfallmanagementplattform »Iscale« verantwortlich.

bilität der Softwarelösung. Denn die Softwarelösung muss sich an die Organisation anpassen und nicht umgekehrt. Nur so kann ein Tool den Erfolg eines ISMS oder BCMS langfristig unterstützen.

Das Management von Informationssicherheit und das Business Continuity Management entwickeln sich hin zu einem strukturierten, prozessorientierten und integrierten Vorgehen. Die Verantwortlichen müssen mit einer wachsenden Menge an Informationen umgehen, ohne dabei den Blick für das Wesentliche zu verlieren. Ein Softwarewerkzeug ist dafür im Grunde unerlässlich, wobei die angebotenen Optionen sehr vielschichtig sind. Das Tool muss zur Organisation, zu deren Methoden und Prozessen, aber auch zu ihrem Reifegrad passen. Bei der Auswahl des Werkzeugs sollte eine Organisation stets ihre Ziele und ihre Strategie in der Informationssicherheit und im Business Continuity Management im Blick behalten. Nur so können beide Managementsysteme langfristig erfolgreich sein.