



Die Rüstungsspirale im Security-Umfeld dreht sich immer weiter.

# Vom Sicherheitskult zur Sicherheitskultur

Sicherheit ist kein statisches Thema, das sich durch Projekte verbessern lässt und dann wieder ad acta gelegt werden kann. Im Gegenteil: Sicherheit ist derselben Dynamik unterworfen wie die Organisation und Geschäftstätigkeit in vielen Unternehmen und erfordert einen kontinuierlichen Anpassungs- und Verbesserungsprozess. **VON ADRIAN MARTI\***

Die «Rüstungsspirale» im Security-Umfeld dreht sich immer weiter. Angreifer wie Hersteller von Sicherheitslösungen sind mit immer ausgefeilteren Methoden immer wieder für neue Entwicklungsschübe besorgt. Für den Sicherheitsverantwortlichen erschwert die zunehmende Komplexität der eingesetzten Systemlandschaften und Applikationen eine systematische Absicherung seines Unter-

nehmens. Lösungsansätze zur IT-Sicherheit erfordern eine Kombination verschiedener Hilfsmittel und Systeme, die auf Grund der sich ändernden Bedrohungslage immer wieder aufs Neue nachgebessert und angepasst werden müssen. Ein technikorientierter Sicherheitsansatz kann der aktuellen Bedrohungslage deshalb immer nur hinterherhinken. Sicherheit in einem Unternehmen entsteht durch das Zusammenspiel

verschiedener, miteinander in Beziehung stehender Elemente. Im Bereich der Informationssicherheit sind dabei die Organisation, die relevanten Prozesse, die unterstützende ICT-Infrastruktur aber auch Gebäude und Anlagen als wesentlichste Elemente zu

\* Adrian Marti ist als Senior Consultant bei der AWK Group tätig und zuständig für Security Management Solutions.

betrachten. Über diese vier Pfeiler kann ein systematisches Sicherheitsframework gelegt werden, die eine schnelle Beurteilung der Gesamtsituation und daraus abgeleitet ein strukturiertes Vorgehen zur Behebung identifizierter Lücken ermöglicht (siehe Grafik).

## Die Risikoanalyse

Die darauf basierende Risikoanalyse identifiziert sowohl die Bedrohungslage als auch den unternehmensspezifischen Schutzbedarf. Abgestützt auf diese Analyseresultate ist zu bestimmen, welche Restrisiken die Unternehmung zu tragen bereit ist und welche der identifizierten Risiken durch Massnahmen in welchem Ausmass reduziert werden sollen.

Basierend auf den Resultaten der Risikoanalyse ist das Sicherheits- und das Notfallkonzept auszuarbeiten. Ersteres beschreibt den Umgang mit dem Thema Sicherheit im Normalbetrieb und umfasst in erster Linie präventive Massnahmen zur Reduktion der Risiken sowie die Prozesse, welche sicherstellen, dass das Framework der sich verändernden Organisation und den sich ebenfalls verändernden Anforderungen an die Sicherheit laufend angepasst wird (Information Security Management System). Das Notfallkonzept hingegen umfasst die vorbereitenden Massnahmen, um eintretende Schadensfälle möglichst schnell und unter Minimierung des daraus entstehenden Impact bewältigen zu können und das Unternehmen geordnet in den Normalbetrieb zurückführen zu können. Es besteht aus dem Business Continuity Plan (BCP), der die Führung des Geschäftes in Krisen definiert (Krisenmanagement, Koordination der Disaster Recovery Arbeiten, Kommunikation) und aus den Disaster Recovery Plänen (DRP), die festlegen, wie die zentralen Prozesse und Systeme wieder in den Normalbetrieb zurückgeführt werden.

## Die Implementierungsphase

Von zentraler Bedeutung ist die anschliessende Implementierungsphase zur Umsetzung der erarbeiteten Konzepte und Massnahmen. Während dies im Bereich von Organisation oder Prozessen oftmals Prozessanpassungen und -einführungen, gezielte Schulungen, Übungen oder Awarenesskampagnen sind, handelt es sich im Bereich der Gebäude und Anlagen und der ICT-Infrastruktur um die Umsetzung der definierten Präventivmassnahmen zur ge-

### WEITERE INFORMATIONEN

## Notfallkonzept

Sicherheits- und Notfallkonzepte müssen auf einer eingehenden Risikoanalyse basieren. Während Ersteres präventive Massnahmen zur Reduktion von Risiken beschreibt, werden im Notfallkonzept jene Schritte abgehandelt, die ein Unternehmen im Schadensfall möglichst rasch wieder in den Normalbetrieb führen.

zielten Verminderung der Risikoexposition oder zur Vorbereitung der definierten DRP-Massnahmen. Zentral ist in dieser Phase aber auch die Etablierung eines eigentlichen Sicherheits-Management-Prozesses als Teil des Risikomanagements des Unternehmens, der dafür sorgt, dass die definierten Konzepte den sich dauernd

ändernden Rahmenbedingungen im Unternehmen angepasst werden, und dass die Geschäftsleitung und der Verwaltungsrat auf regelmässiger Basis entscheidungsrelevante Informationen über den Stand im Bereich Sicherheit erhalten. Angelehnt an BS7799-2 sprechen wir von der Etablierung eines Information Security Management System (ISMS).

## Regelmässige Überprüfungen

Da Sicherheit im Normalbetrieb – insbesondere bei längerem Ausbleiben von grösseren Störungen und Krisen – eher als zusätzlicher Aufwand betrachtet wird, ist die fortlaufende, systematische Überprüfung des Ist-Zustandes in Teilbereichen eine absolute Notwendigkeit. Die Mittel dazu sind Audits, Reviews oder Übungen (BCM) aber auch Inspektionen, Funktionskontrollen oder Penetration Tests oder Social Engineering. Diese Instrumente helfen bei der Identifikation von Schwachstellen und Änderungsbedarf, so dass einerseits Sicherheits- und Notfallkonzepte an die sich im Laufe der Zeit ändernden ICT-Systeme, Infrastrukturen und Prozesse angepasst werden können,

andererseits aber auch weitere Massnahmen für die Sensibilisierung und Verbesserung der Umsetzung im Unternehmen definiert und umgesetzt werden können. Die systematischen Überprüfungen müssen so ausgelegt sein, dass sie grundsätzlich von der internen Sicherheitsorganisation getragen werden können. Es macht aber gerade auch in diesem Bereich Sinn, immer wieder Externe mit einzubinden, um eine Aussen-sicht zu erhalten, neuestes Wissen einzubinden und damit sicher zu stellen, dass nicht auf Grund von «Betriebsblindheit» neue unerkannte Risiken entstehen.

Die Vorbereitung auf eine Zertifizierung nach BS7799 zeigt sowohl gegenüber den Mitarbeitenden wie auch gegenüber externen Partnern und Kunden, dass Sicherheit als eine zentrale Aufgabe angesehen wird. Obwohl es sehr empfehlenswert ist, die konzeptionellen Arbeiten BS7799-compliant auszurichten, empfehlen wir eine vollständige Umsetzung der Anforderungen im Standard oder gar eine Zertifizierung nur dann, wenn das explizit gefordert wird oder einen Mehrwert gegenüber den Kunden bringt.

Gefragt ist heute deshalb ein vermehrter Einbezug des Faktors Mensch in die IT-Sicherheit. Kulturelle Faktoren spielen bei der Schaffung von Sicherheit in IT-Systemen eine immer wieder unterschätzte Rolle. Es geht dabei um kollektive, bewusste und unbewusste Werte und Einstellungen, welche die Umsetzung der Sicherheitsanstrengungen im Unternehmen beeinflussen. Es ist die zentrale Aufgabe eines Sicherheitsverantwortlichen, die Anstrengungen von Mensch und Technik zu einem sinnvollen Ganzen zu kombinieren. ■

## Sicherheitsframework

	Organisation	Prozesse	Gebäude und Anlagen	IT-Infrastruktur
Risikopolitik	Sicherheitsleitbild			
Risikoanalyse	Bedrohungslage, Schutzbedarf, Restrisiko			
Sicherheitskonzept	Sicherheitsorganisation	Prozessanpassungen	Technische und organisatorische Massnahmen	
Notfallkonzept <small>Business Continuity Planning</small>	Notfallorganisation und -prozesse		Ersatzanlagen Ausweichstandorte	Ersatzsysteme Wiederherstellung
Implementierung	Umsetzung, Konzepte und Massnahmen, Training			
Überprüfung	Audits, Reviews, Übungen		Inspektionen	Funktionskontrollen Penetration, Testing
Zertifizierung	Vorbereitung auf Zertifizierung BS 7799			

QUELLE: ANKY GROUP; GRAFIK: CWT/HT