

Ein Praxisbericht

Das IT-Grundschutz-Verfahren stellt eine effiziente Möglichkeit dar, IT-Sicherheit breit einzuführen und zu betreiben. Bei angemessenem Vorgehen erfolgen die Verbesserungen schrittweise, sodass die Mitarbeiter nicht überfordert werden. Das Software-Tool ISAT (Integrated Security Auditing Tool) unterstützt die Arbeiten optimal und vereinfacht die Einführung und den Betrieb durch vorgegebene Abläufe und die Erledigung von Routinearbeiten. Somit kann sich der IT-Sicherheitsbeauftragte auf die wesentlichen Arbeiten konzentrieren. Der folgende Bericht zeigt die wesentlichen Schritte der Einführung und des Betriebes auf und weist auf häufig gemachte Fehler hin.

VON CARLOS RIEDER

Gemäss dem BSI Deutschland soll mit Hilfe des IT-Grundschutzes das folgende Ziel erreicht werden: «Für typische Systeme mittels Anwendung von geeigneten organisatorischen, personellen, infrastrukturellen und technischen Standard-Sicherheitsmassnahmen ein für normalen Schutzbedarf angemessenes Sicherheitsniveau erreichen, welches für sensiblere Bereiche ausbaufähig ist.» Mit einfacheren Worten ausgedrückt bedeutet dies das Folgende: Ein vereinbartes Set von Massnahmen wird auf allen Objekten (Systemen und Anwendungen) eines Unternehmens angewendet. Bildlich gesprochen soll ein «einheitlich hoher Schutzwall» um die gesamte IT-Infrastruktur gebaut werden und nicht die häufig angetroffene Strohhütte mit Panzertür. Das dabei zur Anwendung gelangende Massnahmenpaket muss neben den technischen auch organisatorische Aspekte berücksichtigen.

Stärken und Schwächen dieses Verfahrens

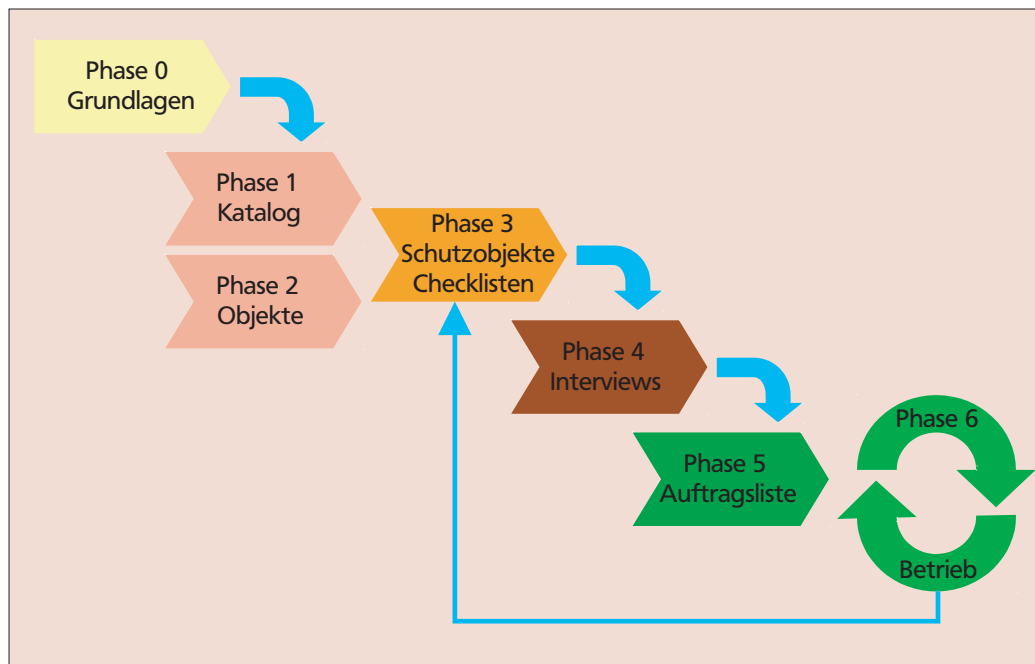
Worin liegen die Vorteile des IT-Grundschutz-Verfahrens? Es ist schnell anwendbar, bestehende Massnahmenkataloge stehen zur Verfügung und die wichtigsten (und heikelsten) Schutzobjekte sind meistens bekannt. Dies sind die Voraussetzungen für einen erfolgreichen Start. Gemäss Definition werden beim IT-Grundschutz «keine» Risiken beurteilt, somit ist der Initialaufwand sehr klein.

Entscheidend ist jedoch, dass der Massnahmenkatalog in das Unternehmen passt. Deshalb ist eine vertiefte Verifikation sehr wichtig. Die Gültigkeit der Massnahmen erstreckt sich üblicherweise



Carlos Rieder

Dipl. El.-Ing. FH, arbeitet bei der isec ag in Luzern und ist Leiter Competence Center IT-Security der Hochschule für Wirtschaft in Luzern.



Vorgehen Einführung und Betrieb IT-Grundschutz.

über mehrere Jahre, was den Aufwand bei der Verifikation rechtfertigt.

Die Strukturierung des Verfahrens führt zu einem klaren Vorgehen im Projekt, was wiederum die Effizienz des Gesamtprojekts steigert. Die kleinen Schritte erlauben den Takt individuell zu definieren und auch bei wenigen verfügbaren Ressourcen optimal zu nutzen.

Wie alles, hat auch das IT-Grundschutz-Verfahren seine Schwächen. Diese liegen vor allem im Über- oder Unterschutzes von gewissen Objekten. Eine wesentliche Eigenschaft des IT-Grundschutzes ist die gleiche Handhabung aller Objekte, unabhängig von Risikobetrachtungen. Dies führt dazu, dass die vorgeschlagenen Massnahmen nicht in jedem Fall optimal passen.

Eine andere Schwäche liegt in der Handhabung. Auf Grund der Menge der verlangten Massnahmen besteht die Gefahr, sich im Detail zu verlieren. Die vom BSI Deutschland vorgeschlagene Umsetzung des IT-Grundschutzes verlangt einen

sehr hohen Detailgrad, was auf Grund des vermuteten Umsetzungsaufwandes zum Projektabbruch vor dem effektiven Projektstart führen kann. Nur mit einem schlanken Massnahmenkatalog ist eine langfristige Umsetzung möglich.

Projektvorgehen/ Meilensteine

Sicher eine zentrale Voraussetzung für die Einführung von IT-Grundschutz ist das Commitment des Managements. Ohne dessen ausdrückliche Zustimmung kann die Umsetzung der Massnahmen langfristig nicht garantiert werden. Ebenfalls ist die Projektleitung klar festzulegen, idealerweise obliegt sie dem IT-Sicherheitsbeauftragten. Er sollte sich die Chance nicht entgehen lassen, die Bedürfnisse der Basis in Interviews vertieft kennen zu lernen und auch als kompetenter Ansprechpartner zum Thema IT-Sicherheit in Erscheinung zu treten. Wie bei jedem umfassenden Projekt, ist ein Zeitplan festzulegen und ein Projektteam zu bilden.

Abhängigkeitsmatrix (Beispiel)

Prozess	Applikationen (für Prozess)	VF	IN	VT	verantwortl.	Systeme (für Appl.)	SW	WI	VT	verantwortl.	Netze (für Appl.)	SW	WI	VT	verantwortl.	Infos (für Appl.)	VT	AR	DS	verantwortl.
				AR DS					AR DS VF IN					AR DS VF IN						
Auftragsbearbeitung	Navision-Software	x	x	v	Hubert Meier	Navision-Server	x	x	v	Hubert Meier	LAN	x	x	v	Ernst Gisler	Kunden-Daten	x	x	x	Sabine Räber
		Navision Client	x	x	v	Hubert Meier	WAN	x	x	v	Ernst Gisler	Artikelstamm	x	x	x	Pia Graf				
		SQL-Datenbank	x	x	v	John Hiller	Netzwerk-Dienste	x	x	v	Ernst Gisler	Lager	x	x	x	Ivo Blättler				
		ActiveDirectory	x	x	v	Rolf Beutler														
		W2k-Client	x	x	v	Rolf Beutler														
	Reuters	x	x	v	Rolf Beutler	Reuters-Server	x	x	v	Edi Sutter										
	E-Mail	x	x	v	Rolf Beutler	Mailservers	x	x	v	Rolf Beutler						E-Mails mit Attachments	x	x	x	jeder Ersteller
	WEB / Browser	x	x	v	Ruth Frey	Firewall	x	x	v	Ernst Gisler	Internetzugang	x	x	v	Ernst Gisler	allg. WEB-Infos	x	x	x	Fritz Glaser
	Office (Word)	x	x	v	Hans Tägler	Proxy	x	x	v	Ernst Gisler						Office-Dokumente	x	x	x	jeder Ersteller
						W2K Fileserver	x	x	v	Rolf Beutler										

Klassifizierungen:

VF Verfügbarkeit
IN Integrität

SW Systemwert
WI Wiederbeschaffung

VT Vertraulichkeit
AR Archivierung
DS Datenschutz

x eingesetzter Wert der Klassifizierung
v vererbter Wert der Klassifizierung

Beispiel einer Abhängigkeitsmatrix.

Auch macht es Sinn, die zukünftigen Ansprechpartner grob zu informieren, wie das Verfahren ablaufen soll, welcher Nutzen zu erwarten ist, sowie mit welchem Aufwand gerechnet werden muss.

Ausarbeiten der Grundlagen

Zu den Grundlagen gehören sicherlich die bekannten Standards Code of Practice of Information Security Management (ISO 17799) und das IT-Grundschutzhandbuch des BSI Deutschland. Der direkte Einsatz dieser Werke als Massnahmenkatalog führt jedoch in den meisten Fällen auf Grund des allzu hohen Detailgrades nicht zum Ziel. Es gilt daher die wesentlichen Aspekte herauszuschälen und so eine umsetzbare Variante zu erhalten. Mehr dazu im Kapitel Massnahmenkatalog.

Als Voraussetzung für die erfolgreiche Umsetzung des Grundschutzes muss eine

Übersicht der bestehenden Infrastruktur inklusive der gegenseitigen Abhängigkeiten bestehen. Erfahrungsgemäss ist ein solches Dokument, nennen wir es Abhängigkeitsmatrix, nur in wenigen Fällen in aktueller Form vorhanden. Dieser Umstand ist für uns immer wieder erstaunlich. Oft hört man Aussagen, dass auf Grund der grossen Komplexität dieses Grundlagendokument nicht erstellbar sei. Gerade aber bei grosser Komplexität ist es besonders wichtig, eine entsprechende Übersicht zur Verfügung zu haben, damit im Krisenfall schnell erkannt werden kann, welche gegenseitigen Abhängigkeiten bestehen.

Bei der Erstellung der Abhängigkeitsmatrix gehen wir von den Geschäftsprozessen aus. Falls diese nicht definiert sind, kann auch von den Applikationen ausgegangen werden. Die Zusammenhänge von Prozessen und zugehörigen Applikationen, Systemen, Netzwerken und Informationen werden tabellarisch erfasst. Weiter müssen die Verantwortlichen für die Objekte wie Systeme oder Applikationen bezeichnet werden. In diesem Stadium sind Vereinfachungen unumgänglich. Es gilt, sich auf das Wesentliche (für die Fortführung der Geschäftstätigkeit) zu konzentrieren.

Neben der Abhängigkeitsmatrix hat sich ein Netzonenplan sehr gut bewährt. Darin wird das Netzwerk in Zonen mit gleicher Bedrohung aufgeteilt. Im Zentrum ist die grüne Zone. Dies ist der vor Zutritt geschützte Bereich in eigenen Gebäuden. Bei der grünen Zone wird von einer geringen Bedrohung ausgegangen. Sie ist von der grauen Zone umgeben. Dies ist der Bereich des Mietleitungsnetzwerks. Die nächste Zone ist die gelbe. In ihr befinden sich Netzwerke mit demselben Sicherheitsstandard, wie zum Beispiel die der Mutter- oder Schwesterunternehmen. In der anschliessenden blauen Zone befinden sich Partnerunternehmen, zu denen ein vertraglich geregeltes Verhältnis besteht, auf deren Sicherheitsstandards jedoch kein Einfluss ge-

nommen werden kann. Ebenfalls im blauen Bereich ist die DMZ (Demilitarized Zone) angeordnet. Zum Schluss folgt die rote Zone. Hier befindet sich alles andere, vor allem auch das grosse «böse» Internet. Die rote Zone ist der Bereich mit der grössten Bedrohung. In einer zweiten Darstellung werden alle zulässigen Netzübergänge abschliessend dargestellt. Nach erfolgter Definition der Netzonen werden alle Systeme inklusive der Netzwerke einer dieser farbigen Zonen zugeordnet. So lassen sich einfach Gruppen von Objekten mit gleicher Bedrohung bilden. Als letzte Vorarbeit müssen die Klassifizierungen definiert werden. Wir unterscheiden zwischen sieben verschiedenen Klassen: Vertraulichkeit, Verfügbarkeit, Integrität, datenschutzrechtliche Relevanz, Archivierung, Systemwert sowie Wiederbeschaffungszeit. Die verschiedenen Klassen können beliebig fein unterteilt werden, jedoch gilt auch hier eine grobe Skala als realisierbarer. Da wir von einem IT-Grundschutzverfahren sprechen, welches per Definition eigentlich keine Klassifizierungen kennt, werden die Klassen vor allem zur Priorisierung verwendet. Das heisst, je höher klassiert ein Objekt ist, desto schneller sollten die entsprechenden Massnahmen umgesetzt werden.

Das Herzstück – der Massnahmenkatalog

Nicht umsonst nennen wir den Massnahmenkatalog das Herzstück. Schliesslich ist er der Massstab, an welchem wir unsere Schutzobjekte messen werden, und somit ist er von zentraler Bedeutung. Der Massnahmenkatalog sollte vom Management bestätigt werden. Nur so kann verhindert werden, dass bei «unliebsamen» Forderungen die Objektverantwortlichen sich an das Management wenden und so versuchen, die Umsetzung der Massnahmen zu umgehen. Im ISAT ist ein umfassender Katalog vorhanden, welcher die ganze Breite der IT-Sicherheit abdeckt und jährlich aktualisiert wird.

Wegweiser zur erfolgreichen Einführung des IT-Grundschutzes

- ▶ Commitment des Managements
- ▶ Massnahmenkatalog von höherer Instanz abgesegnet
- ▶ Nicht zu viele Objekte, nicht zu viele Schutzobjekte (Nach unserer Erfahrung müssten 40 bis 50 Schutzobjekte genügen)
- ▶ Interview mit den Schutzobjektverantwortlichen durch den IT-Sicherheitsbeauftragten oder seinen Stellvertreter
- ▶ Schnelle Reaktion auf erhobene Mängel, Statusbericht an den Interviewpartner
- ▶ Anpassen der Projektgeschwindigkeit an die Umsetzbarkeit im Unternehmen, IT-Sicherheit muss gelebt werden (können).
- ▶ Engagement des Projektleiters, Überzeugungskraft und Durchsetzungsvermögen
- ▶ Erfolge des Projekts kommunizieren

Auch kann ein bestehender, firmeninterner Katalog übernommen werden, um die Bedürfnisse des Unternehmens besser abzudecken. Der regelmässige Update-Aufwand für den eigenen Massnahmenkatalog ist bei dieser Entscheidung ebenfalls zu berücksichtigen. Kleinere Anpassungen können auch durch Sondermassnahmen im Standardkatalog abgedeckt werden, ohne die Möglichkeit des Updates zu verlieren. Jeder Massnahme werden Klassifizierungen zugeordnet. Sie geben an, wann die Massnahme umgesetzt werden sollte. Hier wird nur sehr grob unterschieden. Die meisten Massnahmen gelten ab der geringsten Klassifizierung.

Weiter werden Zuständigkeiten definiert. Wer ist wofür verantwortlich? Zuständigkeiten sind zum Beispiel:

- ▶ IT-Sicherheitsbeauftragter
- ▶ Technischer Produktverantwortlicher (Systembetreuer)
- ▶ Applikatorischer Produktverantwortlicher (Applikationsbetreuer)
- ▶ Telematiker
- ▶ Geschäftsleitung
- ▶ Verantwortlicher für die physische Sicherheit (Betreuer des Gebäudes und von dessen Infrastruktur)

Diese Liste ist beliebig erweiterbar. Die einzelnen Zuständigkeiten sind nach deren Aufgaben unterteilt: Durchführung, Entscheidung, Mitarbeit, Informieren.

Immer wieder zu Diskussionen Anlass gibt der Detaillierungsgrad der Massnahmen. Gehören systemspezifische Mass-

nahmen in einen Massnahmenkatalog oder nicht? Diese Frage wird vermutlich nie zu aller Zufriedenheit zu beantworten sein. Wir sind der Meinung nein. Die systemspezifischen Massnahmen sind sehr kurzlebig und müssen deshalb in kurzen Abständen überholt werden. Der Massnahmenkatalog soll jedoch längerfristig Bestand haben. Wir empfehlen systemspezifische Massnahmen in einem unabhängigen Dokument festzuhalten und im Massnahmenkatalog auf dieses Dokument zu verweisen.

Eine weitere Schlüsselerkenntnis betrifft den Katalogumfang. Wenn alle Varianten und Möglichkeiten abgedeckt werden sollen, wird der Katalog sehr gross und ist nicht mehr umsetzbar. Das richtige Mass zu finden, ist sehr schwierig. Wir haben zirka 250 Massnahmen definiert und decken mit diesen alle Kapitel des Code of Practice ab. Andere Anbieter haben den gesamten Code of Practice übernommen oder auch das gesamte IT-Grundschutzhandbuch des BSI. Nach unseren Erkenntnissen sind wir mit den 250 Massnahmen bereits am oberen Limit und können nur mutmassen, wie schwierig die Umsetzung wird, wenn noch mehr Massnahmen zu berücksichtigen sind. Auch hier zeigt es sich, dass weniger mehr ist.

Vom Objekt zum Schutzobjekt

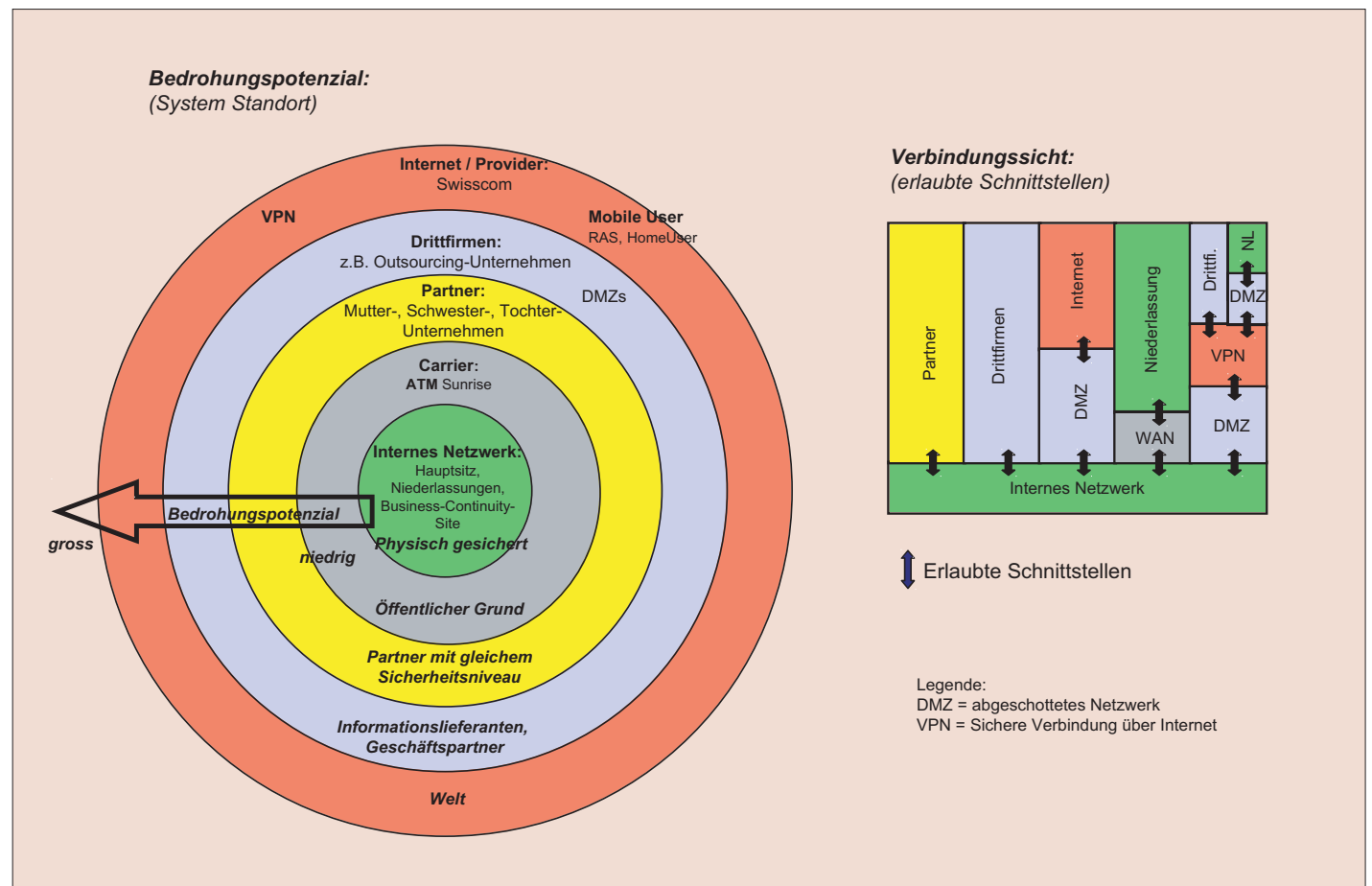
Nachdem die Abhängigkeitsmatrix erstellt worden ist, können daraus die nöti-

gen Objekte (Systeme und Netzwerke, Applikationen und Informationen) abgeleitet und entsprechend klassifiziert werden. Im Weiteren werden die Verantwortlichkeiten erfasst und – ganz wichtig – die gegenseitigen Abhängigkeiten. Um dem IT-Grundschutz gerecht zu werden, sollten alle Objekte erfasst sein. Dazu können die Inventardaten regelmässig eingelesen und den definierten Objekten zugeordnet werden. Somit erhält der IT-Sicherheitsbeauftragte eine weitere Möglichkeit, neu installierte oder weggefallene Objekte zu erkennen.

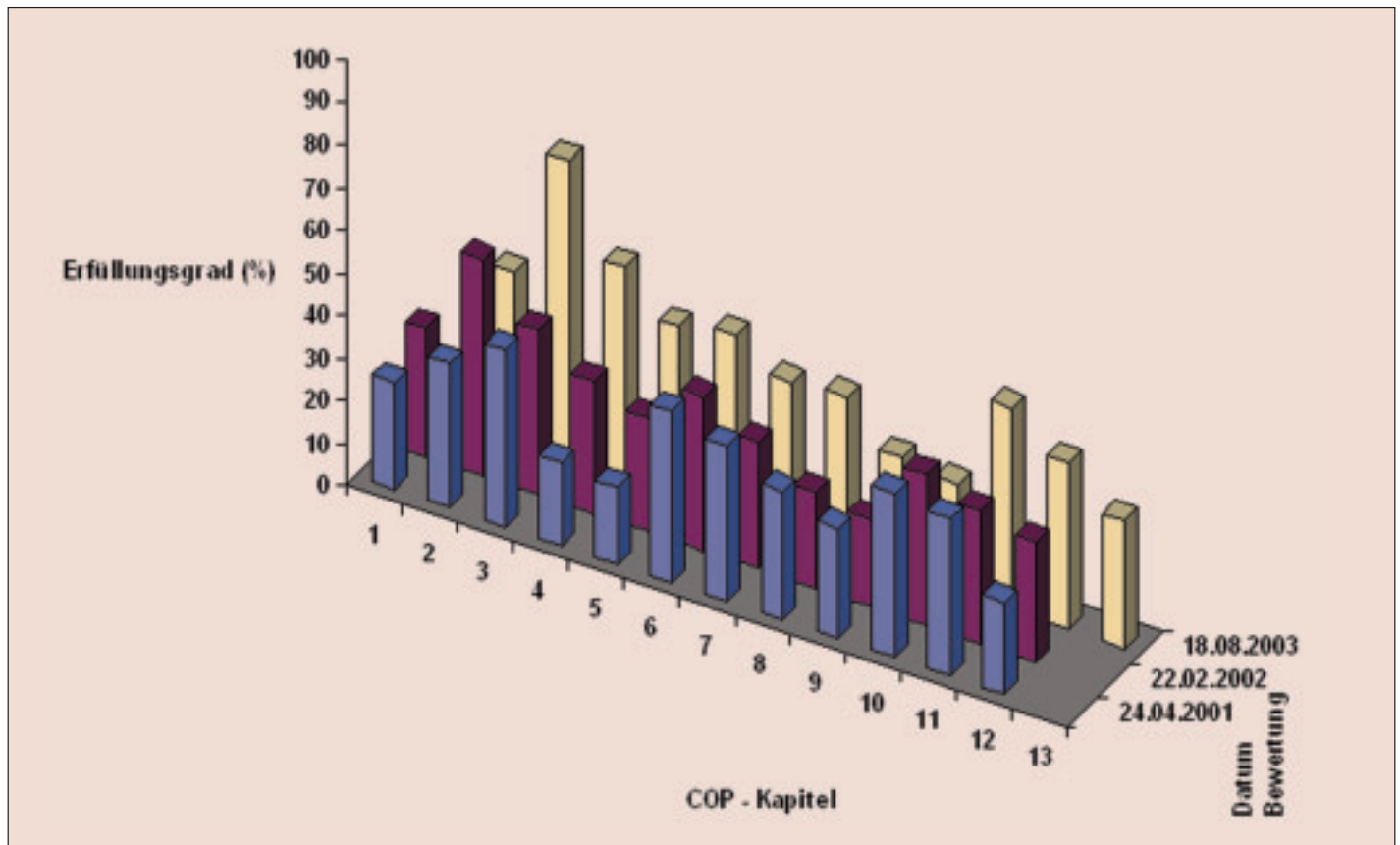
Aus den wichtigen Objekten werden Schutzobjekte erstellt. Voraussetzung dafür sind der gleiche Schutzbedarf und der gleiche Verantwortliche. Typische Schutzobjekte sind zum Beispiel «grüne Windows-Server». Sie erkennen daraus, wie grob zusammengefasst werden kann und auch soll. Wenn alle Server von demselben Team betrieben werden (Verantwortlichkeit) und der Schutzbedarf beinahe identisch ist, genügt diese Vereinfachung völlig. Ein besonders wichtiger Server kann ohne weiteres auch als einzelnes Schutzobjekt erfasst werden, um dadurch seiner Bedeutung gerecht zu werden.

IST-Analyse mit Interviews

Die im vorhergehenden Schritt definierten Schutzobjekte sind nun zu verifizieren. Dazu wird je Schutzobjekt eine Checkliste als Extrakt aus dem Massnahmenkatalog erstellt. Die Auswahlkrite-



Ein Netzwerkzonenkonzept.



Grafische Darstellung der bewerteten Erfüllungsgrade nach COP-Kapiteln

rien sind im Wesentlichen die Zuständigkeit, aber auch die Klassifizierung.

Mittels dieser Checklisten werden nun Interviews mit den Verantwortlichen durchgeführt, um den aktuellen IST-Zustand in Relation zu den festgelegten Massnahmen zu ermitteln. Allfälliger Handlungsbedarf kann direkt im Interview erfasst werden oder aber in einer nachträglichen Überarbeitung. Erfahrungsgemäss bewährt es sich, diese Interviews direkt am Notebook mit Beamer durchzuführen, um die Antworten durch den Verantwortlichen umgehend verifizieren zu lassen. Neben einem Prosa-

Kommentar wird auch der Erfüllungsgrad in Prozent erfasst.

Vielfach wird der Wunsch des IT-Sicherheitsbeauftragten geäussert, die Verantwortlichen die Interviews selbständig und direkt online machen zu lassen. Nach unserer Erfahrung sind Interviews der effizienteste Weg, um an die sicherheitsrelevanten Informationen zu kommen. Vielfach sind es gerade die etwas versteckten Angaben zwischen den Zeilen, welche auf die wesentlichen Schwächen hinweisen. Somit lohnt sich die Investition von zwei bis drei Stunden pro Interview garantiert.

Auftragsliste

Die erfassten Nachbesserungen werden in der Auftragsliste aufgeführt und können so bequem zur Verbesserung in Auftrag gegeben werden. Mit Hilfe von ISAT gestaltet sich die Verwaltung der Auftragsliste sehr einfach und ermöglicht die Konzentration auf die wesentlichen Arbeiten.

Wir empfehlen innerhalb eines Monats nach den Interviews die ersten Aufträge zur Reduktion des Handlungsbedarfes zu erteilen. Damit ist sichergestellt, dass es Ernst gilt und die in den Interviews erhaltenen Informationen auch wirklich etwas auslösen.

Ausgeführte Aufträge werden als Vollzug in der Auftragsliste erfasst inklusive Anpassung des Erfüllungsgrades und Löschen des Bedarfs nach Nachbesserungen.

Die Auftragsliste ist eine der grossen Stärken von ISAT und steigert die Effi-

zienz der Umsetzung spürbar. Dennoch müssen die Aufgaben entsprechend der Zuständigkeit verteilt werden. In vielen Fällen ist ein konsequentes Nachfassen unabdingbar. Gehen doch zu gerne solche Nebenaufgaben verloren. Hier ist Hartnäckigkeit angesagt, ohne diese passiert an der Basis vielfach nur wenig.

Prozess

Erfahrungsgemäss sollten die Schutzobjekte einmal jährlich verifiziert werden. In Ausnahmefällen, bei weniger wichtigen Schutzobjekten, kann auch ein zweijähriger Rhythmus genügen. Der Aufwand für die Interviews reduziert sich massiv, da oftmals nur noch wenig geändert werden muss. Somit dauern die Interviews auch nur noch eine halbe bis eine ganze Stunde.

Weiter ist es wichtig, dass die Vollständigkeit der Objekte und Schutzobjekte innert Jahresfrist überprüft wird. Dies kann durch die Verifikation der Abhängigkeitsmatrix und durch das Einlesen und Zuordnen der Inventardaten erfolgen.

Die erfassten Erfüllungsgrade können in Grafiken ausgewertet werden. Vergleiche dieser Auswertungen werden oftmals zum Aufzeigen der Entwicklung der IT-Sicherheit verwendet. Wir empfehlen zweimal jährlich schriftlich an die Geschäftsleitung zu rapportieren. Dadurch wird das Thema der IT-Sicherheit regelmässig ein Fenster in den Geschäftsleitungs-sitzungen erhalten.

Häufig gemachte Fehler

- ▶ Projekt überladen, zu hoch gesteckte Ziele
- ▶ Keine Unterstützung durch das Management, dieses will die Kosten für die Umsetzung nicht oder nur zu einem zu kleinen Teil mittragen
- ▶ Detaillierungsgrad zu gross, zu viele Objekte / Schutzobjekte
- ▶ Massnahmenkatalog zu umfassend
- ▶ Zu lange gewartet zwischen Erhebung und Beginn der Umsetzung, zu viele Veränderungen in der Zwischenzeit, kein Feedback aus dem Projekt, Verantwortliche haben ihren Glauben an das Projekt verloren
- ▶ Auf Grund fehlendem Reporting schwindet das Interesse (und die Mittel) der Geschäftsleitung