Dr. Suppan International Institute

Der Netzwerk Insider

März 2002

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

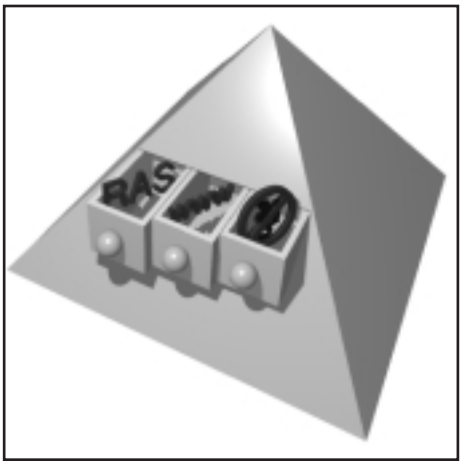
Schwerpunktthema

Vorgehensweise bei der Erstellung einer unternehmensweiten IT-Sicherheitspolitik

von Sven Schumann

Das Sicherheitsniveau einer IT-Infrastruktur unterliegt einem ständigen Wandel. Änderungen in den Geschäftsprozessen, technische Weiterentwicklungen und fehlerhafte Soft- und Hardwareprodukte erzwingen es, IT-Sicherheit als einen Prozess zu begreifen.

Im Rahmen dieses IT-Sicherheitsprozesses erfolgen die Anpassung vorhandener Sicherheitsverfahren an neue Anforderungen, die Beseitigung von Sicherheitslücken sowie die Einführung neuer Sicherheitsverfahren.



IT-Sicherheits-Pyramide

Ziel dieses Artikels ist es den IT-Sicherheitsprozess zu definieren sowie seine einzelnen Bestandteile zu erläutern:

- IT-Sicherheitspolitik,
- IT-Sicherheitsrichtlinien,
- Sicherheitskonzepte, wie Lösungen für
  - Internetzugang
  - Remote-Access
  - Virenschutz
  - Verschlüsselung
  - Netztopologie u. a.,
- Umsetzung der Sicherheitskonzepte

Anschließend soll die Vorgehensweise bei der Erstellung einer unternehmensweiten IT-Sicherheitspolitik beschrieben werden.

weiter Seite 14

Zum Geleit

Von SNMP zur Sicherheits-Realität

In der letzten Woche kam die Meldung durch CERT und NetworkWorld, dass die gängigen SNMP-Agenten in den Switch-Systemen, Routern, Servern, Datenbanken etc. einen gravierenden Sicherheits-Mangel enthalten.

Dieser drückt sich so aus, dass die Agenten, wenn sie mit illegalen SNMP-Paketen konfrontiert werden, das jeweilige System je nach Lastsituation und Art der Pakete komplett zum Absturz bringen können. Im schlimmsten Fall wird das System auch nicht wieder automatisch rebooten sondern muss manuell gestartet werden.

Eine sehr gute Zusammenfassung der denkbaren Störsituationen geben zwei von CISCO veröffentlichte Papiere*.

Da die im Markt vorhandenen SNMP-Agenten von nahezu allen Hestellern an der gleichen Stelle eingekauft werden, betreffen diese Fehler auch fast alle Netzwerk-Produkte von allen Herstellern. Entsprechende Erklärungen finden sich auf den Webseiten der Hersteller.

Als Gegenmaßnahme wird empfohlen, den Zugang zu der jeweiligen Netzwerk-Komponente mit einer IP-Access-Liste auf die erlaubten Systeme zu limitieren (sofern die Netzwerk-Komponente dies vorsieht). In einem Layer-3-strukturierten Netzwerk wird dies bei korrekter Konfiguration einen illegalen Zugang zumindest stark behindern, da Spoofing nur noch mit sehr konkreter Kenntnis der Netzwerk-Struktur und einem räumlichen Zugang zu den entsprechenden Netzwerk-Bereichen möglich ist. Weiterhin arbeiten alle Hersteller an einem neuen Code für die SNMP-Agenten, der zumindest den Absturz bei illegalen Paketen verhindert (ist auch ein relativ einfacher Programmierfehler im Parser, der schnell behoben werden können sollte). Von daher sollte man sich informieren, wenn ein entsprechender Patch verfügbar sein wird. Ein Problem wird dabei ggf. nur schwer lösbar sein. Dies ist die CPU-Belastung durch hohe SNMP-Lasten, auch wenn die SNMP-Pakete korrekt sind.

Im Moment gibt es keinen Grund zur Panik, da weder Angriffe noch Viren o.ä. in dieser Richtung bekannt sind.

weiter Seite 2

* http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-pub.shtml
http://www.cisco.com/warp/public/707/advisory.html

Von SNMP zur Sicherheits-Realität

Etwas anderes ist aber mit Amüsement bzw. Besorgnis (je nach Sichtweise) zu beobachten. Natürlich hört man jetzt aus jeder Ecke, dass SNMP eben unsicher ist und dies ja auch schon seit Jahren bekannt ist. Vornehmlich betrifft dieses Argument den nicht verschlüsselten Community-String als Passwort.

Genau hier liegt aber das Problem. Wir bieten als Unternehmen den potenziellen Angreifern zu viele Angriffsmöglichkeiten. In vielen Bereichen wissen wir dies, aber wir unternehmen nichts. In vielen anderen Bereichen denken wir zu wenig nach und sind zu lasch. Von daher ist diese SNMP-Gefahrenmeldung typisch für unsere Situation.

Impressum

Verlag:
Dr. Suppan
International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland
Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber
und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

Bezug:
Kostenlos
als PDF-Datei
über den eMail-
VIP-Service
der ComConsult Akademie

Für unverlangt
eingesandte Manuskripte
wird keine Haftung übernommen

Dabei sind die Angriffstools der Hacker längst nicht mehr auf genau eine Sicherheitslücke reduziert. Systematisch werden unsere Unternehmen nach Sicherheitsmängeln analysiert, um das Loch zum Angriff zu finden.

Das Problem?

Unter anderem ein organisatorisches:

In vielen Unternehmen ist die Zuständigkeit für Sicherheit nicht zentral gebündelt. Jede Fachabteilung betreibt Sicherheit für sich. Gelegentlich setzt man sich zusammen und versucht die Gesamtsituation zu koordinieren. Dieser Ansatz kann heute nicht mehr erfolgreich sein. Sicherheit muss als Stabsfunktion mit weit reichenden Handlungs-Vollmachten angelegt sein. Nur dann entspricht die Organisation dem Verhalten der Angreifer, die bewusst nach dem schwächsten Glied in der Kette suchen.

Wird dies dann ausreichen?

Nach unserer eigenen Erfahrung in der Akademie und Technologie Information: nein.

Wir waren immer stolz auf unseren Sicherheitsgrad. Nach dem üblichen Grundprinzip war kein direkter Zugriff auf ein internes System von Außen möglich. Auf einmal hatten wir trotz Scanner auf dem Mail-Server, trotz Scanner auf jedem Clienten einen Virus. Erfreulicherweise hat der Scanner auf dem Mailserver dann die Weiterleitung an Dritte unterbunden, der Virus hat auch intern keinen Schaden angerichtet und die ganze Sache war in Minuten ausgestanden. In der nachfolgenden Analyse wurde dann primär die Frage untersucht, wie der Virus denn über alle Hürden in das Unternehmen gekommen sein kann. Und schnell wurden Sicherheitslücken gefunden. Diese konzentrieren sich auf zwei Bereiche.

Zum einen die Notebooks der Mitarbeiter/innen, zum anderen den Datenaustausch mit anderen Unternehmen (hier gab es immer schon Schutz, dieser war aber nicht vollständig).

Letztere Lücke ist organisatorisch und technisch für uns leicht zu schließen gewesen.

Zur Schließung der Notebook-Lücke mussten wir allen Betroffenen den Internet-Zugang außerhalb der Firma mit einem firmeneigenen Notebook untersagen. Zudem wurde der Netzzugang für bestimmte Notebooks (Veranstaltungs-Notebooks) ganz untersagt. (Fremde Geräte durften noch nie ans Firmennetz angeschlossen werden). Im Moment bauen wir ein VPN auf, über das die Mitarbeiter/innen mit ihrem Notebook in die Firma kommen können, um dann von dort aus ins Internet zu gehen. Ein anderer Internet-Zugang wird für die Firmennotebooks nicht mehr erlaubt werden.

Dies ist ein durchaus spannendes Thema. In vielen Fällen sind in den Unternehmen davon primär die Top-Führungskräfte und die Projektleiter betroffen. Dürfen diese in Ihrem Unternehmen mit den Notebooks vom Hotel oder von zu Hause direkt ins Internet? Und dann in der Firma direkt ans Netz?

Aus diesem Beispiel möchte ich zwei Forderungen ableiten (auch an uns selber):

1.

> Wir brauchen Sicherheit als Stabsfunktion mit weitreichenden Befugnissen.

2.

> Wir brauchen umgehend eine anerkannte Sicherheits-Zertifizierung der deutschen Unternehmen.

Der Grad an Vernetzung zwischen den Unternehmen ist zu groß, um jede Lücke schließen zu können.

Mehr zu diesem Thema auf unserem Netzwerk Sicherheits-Forum 2002 vom 10. bis zum 13.06. in Königswinter.

Ihr

Dr. Jürgen Suppan

Aktueller Kongress

Security-Event des Jahres: Netzwerk Sicherheits-Forum 2002

Vom 10. bis zum 13. Juni 2002 veranstaltet die ComConsult Akademie zusammen mit der GAI NetConsult im Maritim Königswinter wieder das "Netzwerk Sicherheits-Forum". Geleitet und moderiert wird die Veranstaltung wie in den letzten Jahren von Dipl.-Inform. Detlef Weidenhammer, dem Geschäftsführer der GAI NetConsult.

Das diesjährige Netzwerk Sicherheits-Forum wird auf vielfachen Wunsch der Teilnehmer auf nunmehr vier Tage ausgedehnt, um am ersten Tag ein einführendes (optionales) Tutorium anbieten zu können. Hier soll neben dem notwendigen Basiswissen auch ein umfassender Überblick zum aktuellen Stand der IT-Security gegeben werden. Darauf aufbauend wird dann an den folgenden drei Tagen inhaltlich stärker in die Tiefe gegangen.

In Fachvorträgen werden namhafte Referenten zu ausgewählten Themen vortragen und diese in ihrer Bedeutung für die Praxis bewerten.

Die aktuellen Bedrohungen im Netzwerkumfeld

Techniken zum Aufbau sicherer IT-Umgebungen

Praktische Hinweise zum Alltagsbetrieb

Erfahrungsberichte und vergleichende Produktworkshops

Neue Themenfelder und Diskussionsrunden

Erfahrungsberichte von kompetenten Anwendern zeigen auf, mit welchen Problemen bei der Durchführung von Sicherheitsprojekten im Unternehmensumfeld auch heute noch zu rechnen ist.

Diskussionsrunden mit Herstellern und Referenten des Tages werden jeweils ein aktuelles Thema aufgreifen und den Teilnehmern so die Möglichkeit geben, gezielt Fragen zu stellen.

Ein ganzer Tag wird Workshops gewidmet sein, die in diesem Jahr auch erstmals in parallelen Sessions angeboten werden, um den Teilnehmern eine breite aber auch individuelle Auswahl zu ermöglichen. Neben Produktvergleichen nach festgelegtem Präsentationsmustern und Workshops zum Aufbau von Policies und Konzepten werden auch wieder interessante Life-Hacks vorgeführt.

Die überaus große Beteiligung und die positive Resonanz auf die letzten Foren zeigt, dass die Auswahl der Themen das Interesse der Teilnehmer gefunden hat. Damit ist das "Netzwerk Sicherheits-Forum" für jeden Sicherheitsverantwortlichen und -interessierten zu einer unverzichtbaren Plattform für aktuellste Informationen, Produktvergleiche und Fachdiskussionen geworden.

Die Themen

Bedrohungsszenarien für den Netzbereich
- Vorstellung aktueller Angriffsmethoden
- Einschätzung von Risiken und Schäden
- Quellen für Sicherheitshinweise

KonTraG
- Bedeutung von KonTraG für die IT-Verantwortlichen
- Abbildung des Risk Management Prozesses
- Durchführung von Bedrohungs- und Risikoanalysen
- Aufbau von Security-Policies und Sicherheitskonzepten

Security-Auditing
- Zielsetzung und Festlegung des Vorgehens
- Aufgaben von Review und Revision
- Durchführung von Scan, Penetration und Monitoring

Authentisierung und Autorisierung
- Multi- und One-Time Passwords
- Biometrische Verfahren
- Von einfacher Zugriffskontrolle bis SSO

Perimetersicherung
- Vergleich aktueller Firewallsysteme
- Aufbau einer sicheren DMZ
- Einsatz von VLANs in der DMZ

RAS und VPN
- Sicherung von RAS-Zugängen
- Integration in bestehende Nutzerverwaltungen
- Auswahl und Einsatz von VPN-Lösungen

Sichere Konfiguration einer Windows-Umgebung
- Bekannte Schwachstellen bei Windows
- Hardening von Windows-Servern
- Sichere Konfiguration von Webbrowsern

Sichere Konfiguration einer Unix-Umgebung
- Bekannte Schwachstellen bei Unix
- Hardening von Unix-Servern
- Sicherung der Administration

Sicherheit im eBusiness
- Privacy im Internet
- Aufbau sicherer Web-Applikationen
- Anforderungen an Clients und Server

PKI-Lösungen
- Komponenten einer PKI
- Zertifikate und Digitale Signaturen
- Erfahrungen mit PKI-Applikationen

Content-Security
- Umsetzung mehrstufiger Schutzkonzepte
- Vergleichende Vorstellung von Gateway-Scannern
- Aktuelle Probleme mit Java, JavaScript, ActiveX

Einsatz von IDS
- Arbeitsweise von IDS-Systemen
- Vergleich aktueller IDS-Produkte
- Integration von IDS in ein zentrales Alarmcenter

Anzeige

10 % Frühbucherrabatt bis 15.04.02

Netzwerk Sicherheits-Forum 2002

10.06. - 13.06.02 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir auch in diesem Jahr exklusiv eine Vorbuchungsphase für das Netzwerk Sicherheits-Forum 2002 bis zum 15.04.2002 für eine rabattierte Teilnahmegebühr an. In diesem Jahr besteht auch erstmals die Möglichkeit, die Veranstaltung 3-tägig oder 4-tägig (mit Tutorium am ersten Tag) zu buchen:

4 Tage Netzwerk Sicherheits-Forum 2002 vom 10.06. -13.06.02 mit Tutorium
zum Preis bei Buchung bis 15.04.02 von € 1.610,--
statt regulär € 1.790,-- zzgl. MwSt.

3 Tage Netzwerk Sicherheits-Forum 2002 vom 11.06. -13.06.02 ohne Tutorium
zum Preis bei Buchung bis 15.04.02 von € 1.430.--
statt regulär € 1.590,-- zzgl. MwSt.

Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk Sicherheits-Forum 2002

Ich melde mich an für das
Netzwerk Sicherheits-Forum 2002

☐ **vom 10.06. - 13.06.01 mit Tutorium**
zum Preis von € 1.610,-- zzgl. MwSt.*

☐ **vom 11.06. - 13.06.01 ohne Tutorium**
zum Preis von € 1.430,-- zzgl. MwSt.*

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Königswinter

von _____ bis _____

*Frühbucherpreise gültig bis 15.04.02

Vorname	Name
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Content Security – noch immer weit unterschätzt

Security-Audits im "Risk Management Process"

Die Verantwortung für die Bereitstellung einer sicheren IT-Umgebung ist längst nicht mehr allein der IT-Leitung zuzuordnen, neue gesetzliche Vorschriften wie KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) zwingen auch die Geschäftsleitung eines Unternehmens verstärkt sich dieser Problematik anzunehmen. Sicherheitsüberprüfungen, sog. Security-Audits, gehören dabei zum unverzichtbaren Bestandteil eines umfassenden Security-Managements und liefern für den KonTraG "Risk Management Process" die benötigten Informationen zur Risikoidentifikation.

Dipl.-Inform. Detlef Weidenhammer ist als Geschäftsführer der GAI NetConsult GmbH vorwiegend auf den Gebieten Internet/Intranet-Anwendungen und Netzwerk-Sicherheit tätig. Basierend auf langjähriger praktischer Tätigkeit bringt er seine Erfahrungen als Fachberater und auch als Referent bei Seminaren und Kongressen ein.

Einige der hierfür verwendeten Techniken werden nachstehend dagestellt.

Sicherheitsüberprüfungen: Ein Muss für jede Unternehmensführung

Ohne eine Risikoidentifikation und -bewertung kann kein sinnvolles Sicherheitskonzept erarbeitet und umgesetzt werden. Das KonTraG verpflichtet deshalb Vorstände von Aktiengesellschaften und nach aktueller Rechtsauffassung auch Geschäftsführer von GmbHs im Rahmen ihrer Sorgfaltspflichten zur Einführung und Umsetzung eines "Risk Management Process", ein Regelkreislauf mit insgesamt 4 Phasen.

Die Phase-1 "Strategisches Risk Management" umfasst die Festlegung der Unternehmensziele für die IT-Sicherheit durch Verabschiedung einer entsprechenden Security Policy.

Die Phase-2 "Risikoidentifikation" und die Phase-3 "Risikobewertung" umfassen die Sicherheitsüberprüfung einer IT-Umgebung.

Die Phase-4 "Risikosteuerung und -kontrolle" schließlich beinhaltet die Konzeption und Umsetzung von Maßnahmen zum sicheren Betrieb.

Nachstehend wird genauer auf die in der Phase-2 verwendeten Techniken zur Sicherheitsüberprüfung eingegangen.

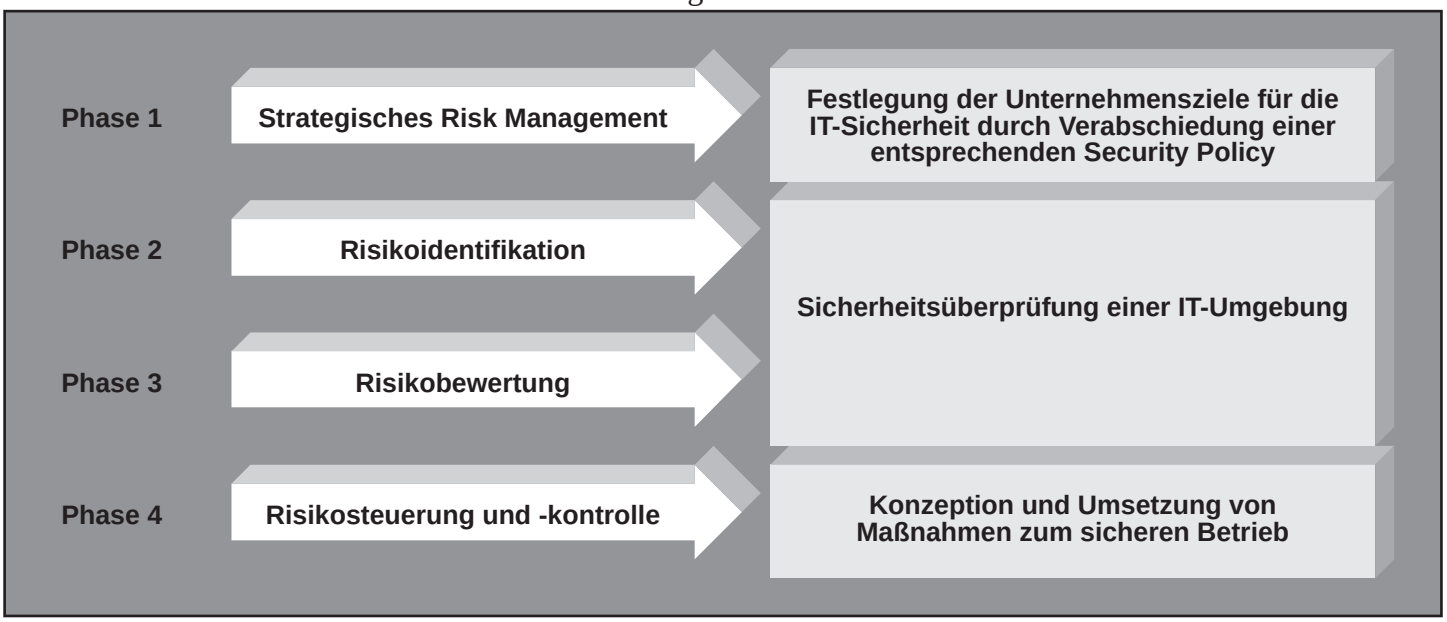
Notwendigkeit von Sicherheitsüberprüfungen

Auch bei den besten Sicherheitsmaßnahmen ist niemals von einer völligen Sicherheit auszugehen.

Fehler in der Administration oder in der verwendeten System- oder Anwendungssoftware können ebenso die Sicherheit bedrohen wie neue, bisher noch wenig bekannte Angriffsstrategien.

Die Bedrohungen kommen dabei sowohl aus internen, aber zunehmend auch aus externen Bereichen wie dem Internet.

Bild 1 Risk Management Process



Security-Audits im "Risk Management Process"

Eine unlängst vom Security Service Provider Riptech vorgelegte Studie über Angriffe aus dem Internet auf die von ihnen betreuten Kundennetze zeigt ähnliche Tendenzen wie die Zahlen des CERT. Nach Auswertung von 5.5 Milliarden Logeinträgen (Firewalls, IDS) aus den letzten beiden Quartalen 2001 konnten 128.678 Attacken identifiziert werden.

Wesentliche Ergebnisse waren:

- Starkes Ansteigen der Angriffe innerhalb der ausgewerteten 6 Monate (um 79%)
- Starkes Ansteigen von Wurm-basierten Attacken (Nimda, Code Red usw.)
- 43% der Unternehmen verzeichneten so gravierende Angriffe, dass eine sofortige Reaktion notwendig war
- 39% der Angriffe waren gezielt gerichtet, hierbei vorwiegend auf Unternehmen aus den Branchen Hochtechnologie, Finanzdienstleistungen, Unterhaltungsmedien und Energieversorger. Dies bedeutet aber auch, dass 61% wahllos innerhalb von globalen Aktionen das Ziel von Angriffen wurden, es kann sich also niemand in Sicherheit wiegen.

Wegen dieser ständig zunehmenden Bedrohungen ist die Überprüfung der Sicherheit aller eingesetzten IT-Systeme von besonderer Bedeutung.

Um fortlaufend eine sichere Umgebung zu gewährleisten, sind Maßnahmen auf unterschiedlichen Ebenen notwendig.

- Review zur Analyse und Bewertung von Sicherheitspolitik, Sicherheitskonzepten und allen eingesetzten technischen und organisatorischen Sicherheitsmaßnahmen
- Revision zur Überprüfung der korrekten Umsetzung von vorgegebener Sicherheitspolitik und Sicherheitskonzepten
- Schwachstellenanalyse in Form von Einbruchs- und Störversuchen durch Scan- und Penetration-Tests

Da es zumeist nicht sinnvoll ist, die eigenen Administratoren mit der Durchführung von Überprüfungsmaßnahmen zu betrauen (Gefahr der Betriebsblindheit, fehlende Fachkenntnis), empfiehlt sich der Einsatz externer Fachleute. Ebenfalls nicht trivial ist die Auswertung der erzielten Ergebnisse. Insbesondere Security-Scanner liefern häufig Fehlinterpretationen ("false positives"), die bei unsachgemäßer Prüfung zu unnötigen und aufwendigen Reaktionen führen können.

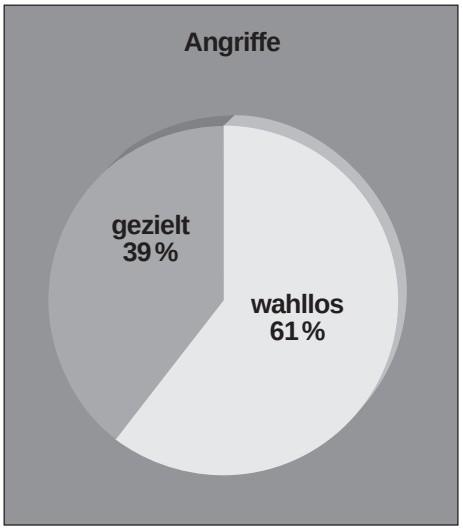


Bild 2

Sicherheits-Review der IT-Umgebung

Vor dem Einsatz von überprüfenden Security-Tools sollte immer ein Sicherheits-Review erfolgen. Nur durch diese Form der Analyse lässt sich ein umfassender Überblick auch über Schwachstellen gewinnen, die nicht toolgestützt zu ermitteln sind. Dies betrifft z.B. fast alle Formen der Sicherheitsorganisation und die Umsetzung von Maßnahmen, die bei Scan- und Penetration-Tests nicht untersucht werden.

Im Rahmen des Review wird zusammen mit den hierfür benannten Mitarbeitern des Unternehmens die vorhandene IT-Umgebung analysiert. Dies kann durch Workshops, Interviews und/oder durch Fragebögen realisiert werden. Soweit möglich wird auch auf vorhandene Unterlagen wie Security Policies und Fachkonzepte zurückgegriffen. Die Dokumentationen aller Sicherheitskomponenten, insbesondere die Netzpläne, werden bewertet, die gegenwärtigen und die geplanten Kommunikationsbeziehungen werden einer Risiko-Analyse unterzogen und die Auswirkungen auf Administratoren und Benutzer untersucht.

Ergebnis des Sicherheits-Reviews sind eine abschließende Bewertung der IT-Umgebung und die Empfehlung von Maßnahmen zur Verbesserung des Sicherheitsniveaus.

Die nachfolgend dargestellten Scan- und Penetration-Tests sollten immer begleitend durchgeführt werden, da sie wertvolle zusätzliche Erkenntnisse über vorhandene Schwachstellen liefern.

Revision - Prüfung der Sicherheitsorganisation

Die Revision sollte in Form einer Systemprüfung durchgeführt werden, bei der die korrekte Umsetzung der vorhandenen Sicherheitspolitik und Sicherheitskonzeption im Vordergrund steht.

Eine generelle Einzelfallprüfung, bei der jede konkrete Dienstenutzung nachvollzogen wird, ist hier nicht sinnvoll. Jedoch sollte stichprobenartig untersucht werden, ob die Sicherheitsvorkehrungen ausreichend sind.

Der erste Teil der Systemprüfung umfasst die Vollständigkeit und Aktualität der schriftlich fixierten Ordnung als Teil der Gesamtdokumentation.

In dieser Ordnung muss festgelegt sein, welche Art der Dienstenutzung für welche Personen erlaubt ist oder nicht. Neben der Security Policy als Basisdokument muss die Systemdokumentation auch Regelungen darüber enthalten, wie die Systemverwalter den sicheren Betrieb gewährleisten. Das Ergebnis des ersten Teils der Systemprüfung ist eine Aussage zur Aktualität und Angemessenheit der Security Policy und der Betriebsdokumentation.

Der zweite Teil der Systemprüfung besteht aus der Untersuchung der korrekten Einhaltung der Security Policy und der Vorgaben der Betriebsdokumentation.

Die Sicherheitskomponenten werden dahingehend geprüft, dass ihre Konfiguration mit der Dokumentation im Einklang ist. Diese Konfigurationsprüfung betrifft die Basiskonfiguration sowie die Konfiguration der speziell angebotenen Dienste wie Proxies, Filter oder auch dem Schlüsselmanagement.

Im dritten Teil der Systemprüfung wird die Wirksamkeit im Betrieb untersucht.

Anhand von Tests und der Sichtung von Protokolldaten wird stichprobenartig untersucht, ob die Sicherheitskomponenten entsprechend den Vorgaben korrekt arbeiten. Darüber hinaus werden alle weiteren Maßnahmen zur Sicherheitsadministration geprüft. Dazu gehört z.B. die regelmäßige Auswertung von Protokolldaten, die Auswertung von Alarmen und evtl. auch das Accounting.

Die Systemprüfung wird (wenn vorhanden) von der internen Revision übernommen, kann sich aber auch externer Fachleute bedienen.

Security-Audits im "Risk Management Process"

Schwachstellenanalyse mit Scan- und Penetration-Tests

Auch die besten technischen Sicherheitsmaßnahmen können nie von statischer Natur sein. Neu hinzukommende Anwendungen müssen genauso beachtet werden wie die korrekte Einhaltung der Security-Policy ("security health check"). Hierzu sind in regelmäßigen Abständen (und zusätzlich bei besonderem Anlass) technische Überprüfungen der Qualität der eingesetzten Schutzmaßnahmen vorzunehmen.

Zum Einsatz hierfür kommen üblicherweise Scan- und Penetration-Tests, die aber jeweils recht unterschiedliche Zielsetzungen haben:

Scan-Tests verfolgen einen breit angelegten Ansatz und versuchen durch umfangreiche Überprüfung der vorgegebenen Zielsysteme eine möglichst detaillierte Schwachstellenanalyse vorzunehmen. Die gefundenen Risiken werden zumeist klassifiziert, zumindest in die Kategorien gering-mittel-hoch, um den Verantwortlichen Prioritäten bei der nachfolgenden Bereinigung zu liefern. Risiken mit der Einstufung "hoch" sollten demnach sofort beseitigt werden, bei den anderen Schwachstellen kann je nach Einschätzung vielleicht sogar bis zum nächsten Update gewartet werden.

Der Einsatz von automatisierten Security-Scannern, die in Form einer Toolbox alle bekannten Schwachstellen "kennen" und einem Test unterziehen, ist hierzu unabdingbar. Es ist jeweils darauf zu achten, dass nicht nur altbekannte, sondern auch neue Sicherheitsbedrohungen berücksichtigt werden. Die Security-Scanner müssen also ständig aktuell gehalten werden, es gilt damit ähnliches wie für Virenscanner.

Als Startpunkt für das Aufkommen von Security-Scannern kann das Jahr 1994 mit der Freigabe und Verbreitung von SATAN (Security Administration Tool for Analyzing Networks) gelten. Damit stand erstmals ein System zur zentral veranlassten umfassenden Prüfung vernetzter Systeme zur Verfügung. Gute Report-Möglichkeiten verbunden mit Hinweisen zur Behebung der gefundenen Schwachstellen helfen dem Administrator bei der Überprüfung seines Sicherheitsstandes. Kommerzielle Systeme wie z.B. der Internet-Scanner von ISS (Internet Security Systems) kamen bald danach auf den Markt. Momentan befinden wir uns im Übergang zu einer neuen Generation von Security-Scannern. Diese zeichnen sich neben verbesserten Reports und Informations-Datenbanken vor allem durch die Kombination von Sicherheitstests aus. Idee dabei ist, das Verhalten von Eindringlingen nachzuahmen, deren Vorgehen zumeist durch das kombinierte Ausnutzen mehrerer Schwachstellen gekennzeichnet ist. Die ebenfalls neue Fähigkeit durch "Auto-Reaktion" gefundene Probleme automatisch beseitigen zu lassen ist jedoch noch vorsichtig und nur in eindeutig geklärten Fällen (z.B. File-Protections) einzusetzen.

Penetration-Tests haben anders als Scan-Tests nicht das primäre Ziel einen möglichst umfassenden Überblick zu Schwachstellen zu liefern, sondern sollen aufzeigen, wie tief ein Angreifer in vermeintlich geschützte Systembereiche eindringen kann. Im Gegensatz zum Scan-Test ist dabei das Vorgehen mehrstufig, d.h. es werden zwar ebenfalls Schwachstellen ermittelt, diese dann aber direkt ausgenutzt, um Systemzugang zu erhalten. Ist dieser Zugang nur mit wenigen Privilegien ausgestattet, wird die nächste Aktion das Erlangen von weiteren Privilegien sein bis man seine Zielsetzung erreicht hat.

Vorgehen bei einem BlackBox-Test

Nachfolgend wird der typische Ablauf der Sicherheitsüberprüfung bei einem sog. Black-Box-Tests gezeigt, wobei eine Kombination von Scan- und Penetration-Tests eingesetzt wird. Es soll die Angreifbarkeit eines Unternehmens demonstriert werden, wobei nur minimale Informationen zur Verfügung gestellt werden. Im Gegensatz zu einem WhiteBox-Test, bei dem die Ziele genau benannt werden, muss der BlackBox-Test allein mit der Benennung des zu untersuchenden Unternehmens auskommen. Dies simuliert genau den Fall des anonymen Angreifers, der nicht mehr Basisinformationen besitzt. Das weitere Vorgehen lässt sich dann in insgesamt vier Phasen von der reinen Informationsbeschaffung bis hin zur finalen Penetration gliedern.

Phase-1: InfoSeek

Die erste Phase dient der reinen Informationsbeschaffung unter Nutzung öffentlich zugänglicher Quellen. Mit dem Namen des Unternehmens können z.B. über Search-Engines (www.google.com) und den (wenn vorhandenen) Webserver des Unternehmens erste Informationen gesammelt werden. Besonders interessant sind Hinweise auf Unternehmensstrukturen, die sich z.B. aus Geschäftsberichten ergeben. Zur Ermittlung von Domain-Namen, IP-Adress-bereichen und Public-Servern stehen eine Vielzahl von weiteren Recherchemöglichkeiten zur Verfügung. Hierzu gehören öffentliche Server wie die RIPE-Datenbank (www.ripe.net), IP Index (www.ipindex.net) oder auch Tools wie nslookup, dig, whois, finger usw. Nette Hinweise liefert auch www.netcraft.com, wer selber sammelt schon wie dieser Server Statistiken über die Uptime seines eigenen Webservers? Interessant aber sind z.B. die verwendeten Webserver und Betriebssysteme.

Bild 3 Beispiel: Infos von Netcraft über Webserver des Bundes

Sites with longest running systems at Internet connection of the Federal Republic of Germany
Internet connection of the Federal Republic of Germany. The departments will offer public information. Bonn

Note: Uptime - the time since last reboot is explained in the FAQ					Generated on 20-Feb-2002 15:10:39	
Rank	**Site**	**Average**	**Max**	**Latest**	**OS**	**Server**
1	bund.de	170	174	174	Solaris 8	Apache/1.3.20 (UNIX) ServletExecAS/3.1
2	www.bund.de	133	183	176	Solaris 8	Apache/1.3.20 (UNIX) ServletExecAS/3.1
3	www.bva.bund.de	81	250	120	Linux	Apache/1.3.12 (UNIX) PHP/4.0.2
4	www.bsi.bund.de	44	70	70	Solaris 8	Apache/1.3.12 (UNIX)
5	www.bsi.de	30	68	69	Solaris 8	Apache/1.3.12 (UNIX)
6	www.bundesarchiv.de	5	10	11	Linux	Apache/1.3.20 (UNIX) PHP/4.0.6
7	www.bvvg.de	-	-	-	NT4/Windows 98	Lotus-Domino/5.0.9

```
domain:      bund.de
descr:       Bundesministerium des Inneren
descr:       Informationstechnik in der Bundesverwaltung (KBSt)
descr:       Graurheindorferstr. 198
descr:       53117 Bonn
descr:       Germany
nserver:     nserer.bund.de 194.95.179.193
nserver:     nuernberg.bund.de 194.95.179.196
nserver:     deneb.dfn.de
status:      connect
changed:     lastchange@denic.de 20011022
source:      DENIC

[admin-c] [tech-c] [zone-c]
Type:        PERSON
Name:        Egon Troles
Address:     Bundesministerium des Inneren
Address:     Graurheindorferstr. 198
City:        Bonn
Pcode:       53117
Country:     DE
Phone:       +49 1888 681 3394
Fax:         +49 1888 681 53394
Email:       troles@kbst.bund400.de
Email:       egon.troles@bmi.bund.de
Changed:     lastchange@denic.de 20011022
Source:      DENIC

[tech-c] [zone-c]
Type:        PERSON
Name:        Jens Claessens
Address:     Telekom
Address:     CC IVBB
Address:     Bonner Talweg 100
City:        Bonn
Pcode:       53113
Country:     DE
Phone:       +49 1888 9900 99
Fax:         +49 1888 9900 98
Email:       uhd@bund400.de
Changed:     lastchange@denic.de 20011022
Source:      DENIC
```

Bild 4 Öffentlich zugängige Informationen in der Ripe Whois Database

Nach diesen Recherchen sind die dem Unternehmen zuzurechnenden IP-Adressbereiche bestimmt, DNS-, Mail- und Webserver bekannt und zumeist auch noch die Namen (Adressen, Telefonnummern) der administrativen und technischen Ansprechpartner im Unternehmen.

Beim InfoSeek werden keinerlei inversive Methoden verwendet, so dass die Aktivitäten dieser Phase für das zu überprüfende Unternehmen nicht bemerkbar sind.

Phase-2: ConnectScan

Die Ergebnisse der ersten Phase liefern den Input für den sog. ConnectScan, bei dem die zuvor ermittelten IP-Adressbereiche auf wirklich erreichbare Zielsysteme untersucht werden.

Üblicherweise sind die IP-Ranges nur dünn belegt, so dass man zumeist nur mit einer geringen Zahl solcher Systeme rechnen kann. Häufig werden auch bestimmte Tastversuche wie Ping-Sweeps unterbunden, so dass auch andere Techniken wie TCP SYN Scans auf ausgewählte IP-Dienste oder Banner-Tests zum Einsatz kommen.

Beim ConnectScan werden einfache Tastversuche unternommen, die einem aufmerksamen Administrator nicht verborgen bleiben sollten. Es werden in dieser Phase aber noch keine Sicherheitsuntersuchungen durchgeführt.

Phase-3: SecurityScan

Die dritte Phase verwendet die Ergebnisse des ConnectScan, um gezielt nach Schwachstellen zu suchen.

Durch den Einsatz von Portscannern, CGI-Tests, OS-Detection, usw. werden genauere Informationen über die auf den Zielsystemen eingesetzte System- und Anwendungssoftware gesammelt. Versionen, bei denen bekannte Schwachstellen vorliegen und für die Programme zum Ausnutzen derselben verfügbar sind ("exploits"), werden je nach Gefährdung aufgelistet.

Dankbare Objekte hierfür sind zumeist ältere (ungepatchte) Betriebssysteme oder Dienste wie BIND, SSH, MS IIS, SMTP.

Häufig gelingt es aber auch schon durch einfaches Raten z.B. Router-Passwörter zu ermitteln oder mit ungeänderten Initial-Passwörtern wie bei SNMP (Community-String "public" oder "private") einen Schritt weiter zu kommen.

Häufig eingesetzte Tools hierbei sind:

kommerzielle Security-Scanner von ISS, NAI, Symantec usw., oder auch Open-Source Varianten wie Nessus, Nmap, WhatsRunning, Idistfp.

Beim SecurityScan sind typische Angriffsmuster erkennbar, die einem Administrator sofort auffallen sollten.

Bestimmte Tests können sogar zum Systemabsturz führen (insbesondere Denial-of-Service Attacken), weshalb diese vorher genau abzustimmen sind und bei Anwendung die ständige Erreichbarkeit des lokalen Administrators erforderlich machen.

Phase-4: Penetration

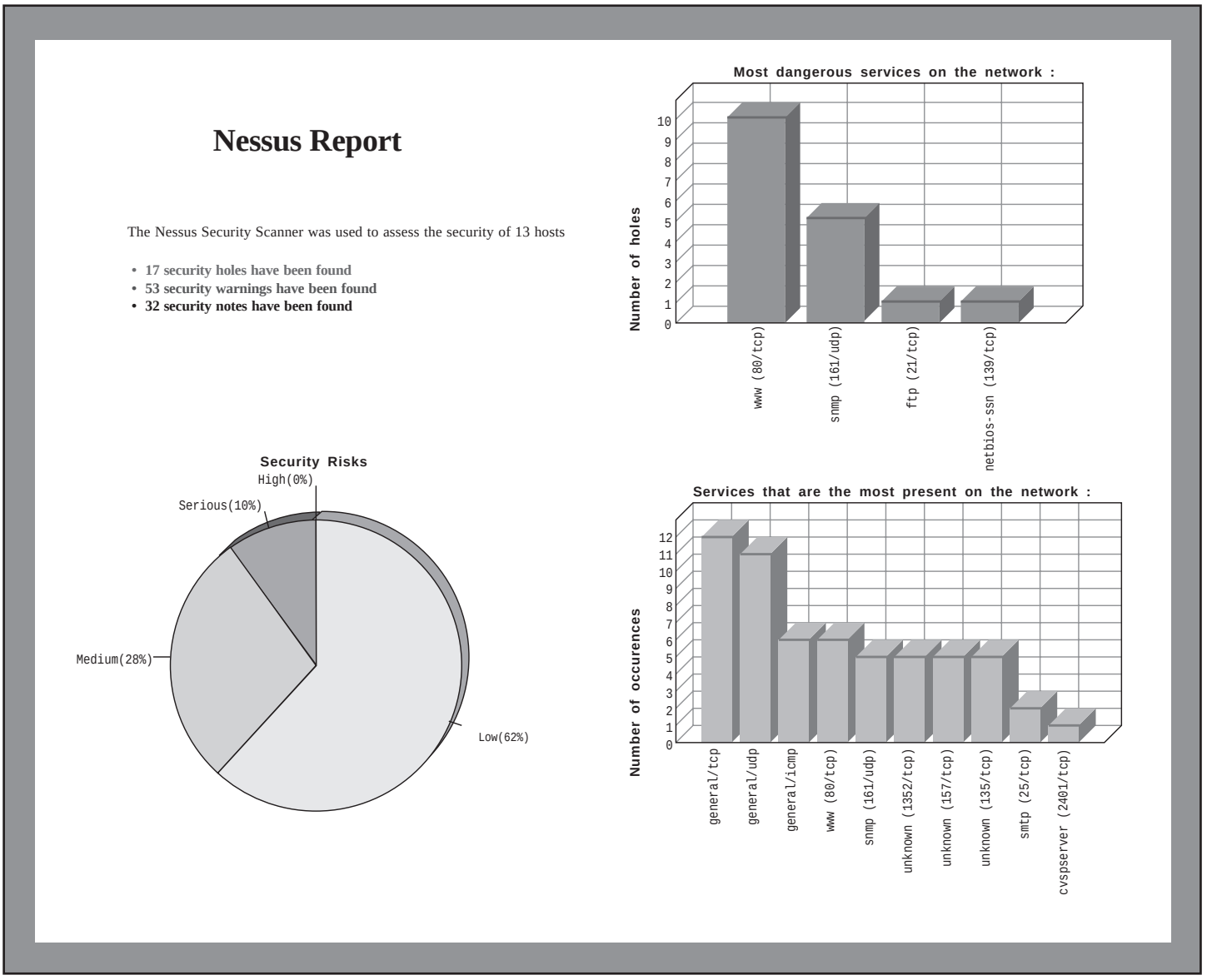
Soll die Überprüfung nicht mit den Ergebnissen des Security-Scans abgeschlossen werden, sondern Angriffe bis zum Erfolg (z.B. Eindringen in lokale System über Netzgrenzen hinweg) durchgeführt werden, kommt der Penetration-Test zum Einsatz. Dieser ist entgegen der Aussage einiger Hersteller von Security-Scannern nur bedingt automatisierbar und erfordert weitgehend manuelles Vorgehen von erfahrenen Fachleuten. Diese müssen insbesondere sehr gut über neue oder noch weitgehend unbekannte Schwachstellen Kenntnis haben, sind also angehalten sich zumindest beobachtend in Hackerkreisen zu bewegen.

Die aus der vorigen Phase ermittelten Schwachstellen liefern die ersten Ansatzpunkte für das weitere Vorgehen. Sind bekannte Schwachstellen ermittelt worden, werden die notwendigen Exploits eingesetzt, um diese auszunutzen. Je nach Art der Schwachstelle ist es möglich Dienste zu unterbinden (DoS-Attacke), Webinhalte zu verändern oder sich Zugang zum gewünschten Zielsystem zu verschaffen.

Eine "typische" Penetration läuft häufig wie folgt ab:

Step-1: Bei einem öffentlich erreichbaren System wurde eine ausnutzbare Schwachstelle festgestellt.

Bild 5 Ausgabe des Security-Scanners Nessus



Security-Audits im "Risk Management Process"

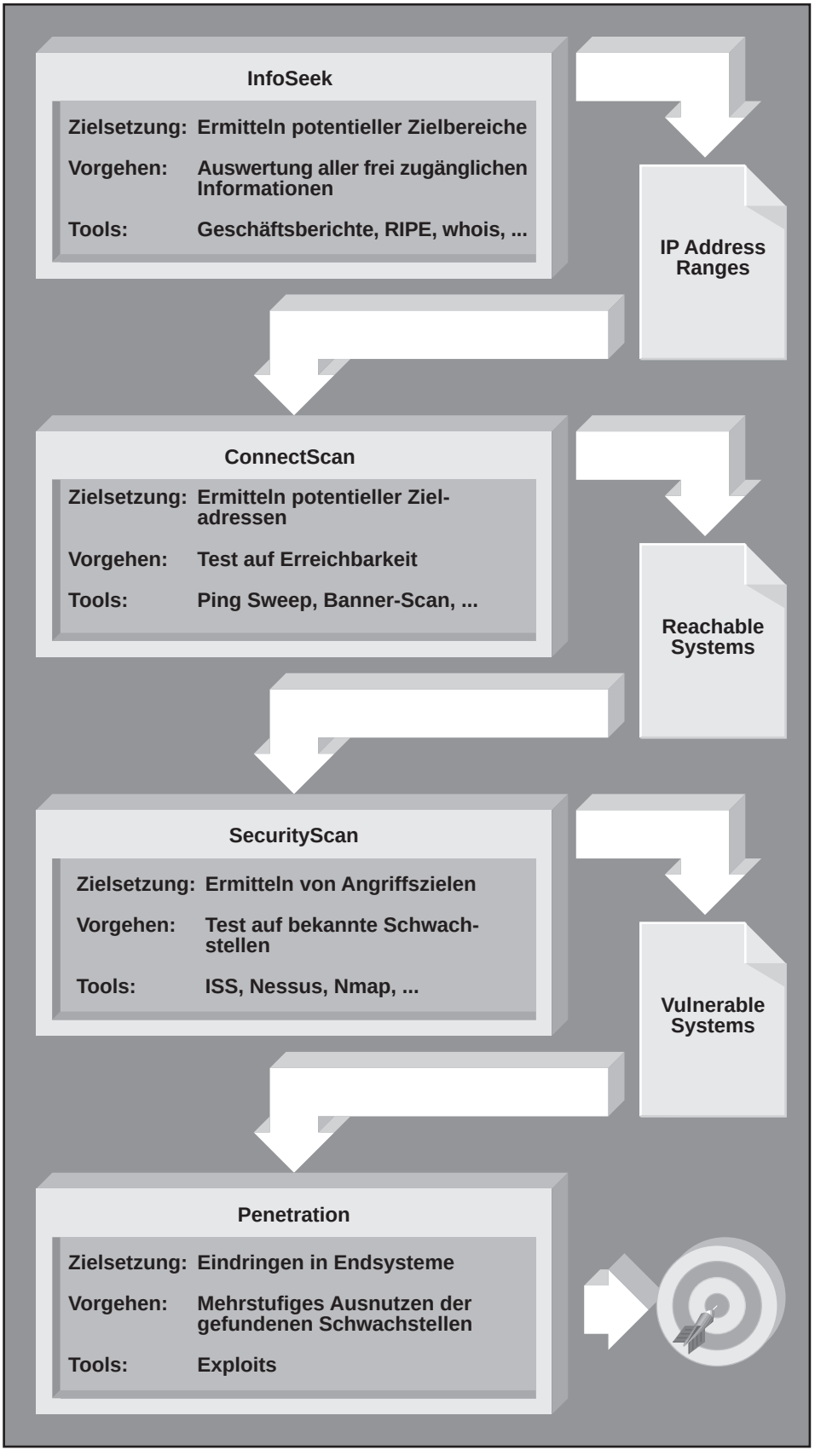


Bild 6 Vorgehensmodell BlackBox-Test

Anfällig hierfür sind besonders Web- und DNS-Server, natürlich auch gern gesehen sind vor der Schutzzone plazierte Server für ftp- oder telnet-Zugang.

Step-2: Entweder gelingt es gleich hohe Privilegien zu erlangen, oder es wird als einfacher User jetzt lokal nach weiteren Schwachstellen gesucht. Häufig gelingt es an die Passwort-Datei zu gelangen und diese dann einem Crack-Programm zuzuführen.

Step-3: Privilegiert lassen sich jetzt von diesem Ausgangssystem leicht weitere Aktivitäten starten. Zunächst werden sicherheitshalber Logeinträge gereinigt und evtl. Systemprogramme gegen manipulierte ausgetauscht. Hierüber oder durch Installation eines Sniffer-Programms lassen sich dann weitere Passwörter ablauschen.

Step-4: Mit etwas Glück findet der Angreifer Vertrauensbeziehungen zu anderen Rechnern oder er kann eine bestehende Session übernehmen ("hijacking"). Dagegen bietet selbst die Verwendung von Starker Authentisierung keinen Schutz. Ist diese Session von interner Seite aus initiiert, dann ist sogar ein Eindringen in das interne Netz möglich.

Fazit

Aus praktischer Erfahrung diverser Sicherheitsüberprüfungen lässt sich feststellen, dass man wohl in die meisten Unternehmensnetze eindringen kann, wenn diese zumindest über eine Internetanbindung mit den üblichen Standard-Diensten verfügen. Es sei darauf hingewiesen, dass in den vorstehend dargestellten Szenarien nicht einmal solche überaus Erfolg versprechenden Attacken wie Social-Engineering, Denial-of-Service oder das Einschleusen von manipulierten Email-Attachments berücksichtigt wurden. Je mehr Netzverbindungen zu unterschiedlichen Partnern ein Unternehmen betreibt, desto anfälliger wird es für Angriffe. Da diese internen Verbindungen häufig nur schwach gesichert sind, kann über nur ein einziges schlecht gesichertes Netz der gesamte Verbund attackiert werden. Gleiches gilt für die zunehmende Zahl von Tele-Arbeitsplätzen, die zumeist nur schlecht gesichert angebunden werden. Nur eine umfassende Überprüfung in der vorgestellten Form liefert aussagekräftige Informationen, um Maßnahmen für ein ausreichend gutes Sicherheitsniveau aufzusetzen.

Wireless LANs werden immer atraktiver

Neue erweiterte Fassung des Wireless LAN-Reports untersucht die neuesten Entwicklungen!

Wireless LANs zählen zu den wichtigsten Technologien der nächsten Jahre (siehe Intel-Ankündigung von Anfang März, die Funkfähigkeit demnächst in die meisten Chips zu integrieren).

Mit der Bedeutung steigt aber auch die Vielfalt und damit die Komplexität. Die Einsatz-Erfahrungen der letzten Monate zeigen: die Planung und Installation ist aufwändig, aber die angestrebten Vorteile werden erreicht. Gleichzeitig beinhaltet die im Moment dominierende IEEE 802.11b-Technik auch eine Reihe von Tücken, die nun durch neue Normen und Produkte ausgeglichen werden. Der Markt ist sehr stark in Bewegung.

Die neuen Standards bringen signifikante Vorteile für folgende Umgebungen:

- Abdeckung großer Flächen für viele Teilnehmer
- Abdeckung über mehrere Etagen hinweg (3-dimensional statt nur 2-dimensional)
- Umgebungen mit starken Funknachteilen (viel Beton, viel Wasser, starke Fading-Effekte)
- Bedarf nach mehr Bandbreite

Damit stellen sich die Fragen:

- auf der Basis welcher Norm soll ein Anwender arbeiten?
- beseitigen die neuen Normen die Schwächen der bisherigen 802.11b-Norm?
- sind die verschiedenen Normungsansätze kompatibel zueinander?
- was bedeutet dies für Planung und Installation?

Die Antwort auf diese Fragen gibt die in dieser Richtung erweiterte Fassung unseres Wireless LAN-Reports, die ab sofort verfügbar ist.

Dipl.-Math. Cornelius Höchel-Winter:
Wireless LANs: Arbeitsweise, Einsatzbedingungen, Produkte,
Umfang: 267 Seiten

Konkret haben wir über die schon bestehenden Inhalte hinaus für Sie untersucht:

- Welche Fortschritte wurden im Bereich der Sicherheit gemacht? Reichen die Ansätze der Arbeitsgruppe 802.11i aus, um Sicherheit zu gewährleisten? Welche Rolle spielen die schon auf dem Markt angebotenen Sicherheitserweiterungen wie das neue Verschlüsselungs-Verfahren von CISCO?
- Was bieten die neuen Übertragungsverfahren (802.11a/g), die auf einer anderen Funktechnik als bisher basieren, dem Orthogonal Frequency Division Multiplexing OFDM? Werden Planung und Installation einfacher, wann und wie steht mehr Bandbreite zur Verfügung? Gibt es weitere Vorteile neben der Bandbreite?

Schon jetzt muss betont werden, dass mit den neuen Normen die bestehenden Produkte und Technologien nicht ihren Sinn verlieren. Konkret hängt von der Art des Einsatzes ab, wann welche Wireless-Version Sinn macht. Dies wird in unserem Report an typischen Einsatz-Szenarien erklärt.

Antworten auf diese aktuellen Fragen finden Sie in unserer erweiterten neuen Fassung des Technologie-Report "Wireless LANs: Arbeitsweise, Einsatzbedingungen, Produkte". Nach einer detaillierten und anschaulichen Vorstellung des IEEE-Standards 802.11 und seiner Erweiterungen werden die Ergebnisse einer ausführlichen Untersuchung von typischen Produkten des Marktes vorgestellt und die Leistungsmerkmale dieser Geräte diskutiert. Ein weiteres Kapitel widmet sich konkreten Anwendungsbeispielen wie der Ein-Zellen- und Mehr-Zellen-Konfiguration, Lösungen für Konferenzräume und der Abdeckung eines größeren Gebäudekomplexes.

Fax-Antwort an ComConsult 02408/955-399

Reportbestellung

☐ Ich bestelle den Report
Wireless LANs: Arbeitsweise, Einsatzbedingungen, Produkte
zum Preis von € 349,--
zzgl. MwSt. und Versandkosten

Unterschrift

Name, Vorname

Firma, Abteilung

Straße

PLZ, Ort

Bedingungen:

Die Ware kann nicht umgetauscht oder zurückgegeben werden. Bei Versand berechnen wir eine Gebühr von 5,-- Euro zzgl. MwSt. für Porto und Verpackung, bei 2 und mehr Reports 10,-- Euro zzgl. MwSt. (Bei Versendungen ins Ausland 25,-- Euro bzw. bei 2 oder mehr Reports 30,-- Euro zzgl. MwSt.)

Neues Seminar

Redundanzverfahren und Design-Konzepte von LANs

Vom 8. bis 10. April 2002 veranstaltet die ComConsult Akademie im Hilton Bonn zum ersten Mal ihr neues Seminar "Redundanzverfahren und Design-Konzepte von LANs".

Zum Thema

Netzwerk-, Server- und Speicher-Architekturen wachsen zusammen. Gleichzeitig ergeben sich mit neuen Redundanz- und Steuerungs-Verfahren Lokaler Netzwerke sowie einem Preisverfall der Switch-Systeme funktional und wirtschaftlich wesentlich erweiterte LAN-Gestaltungsmöglichkeiten. Wirklich gute LAN-Design- und Redundanz-Lösungen basieren bisher auf Layer-3-Struktur-Konzepten und haben neben vielen Vorteilen einige gravierende Nachteile:

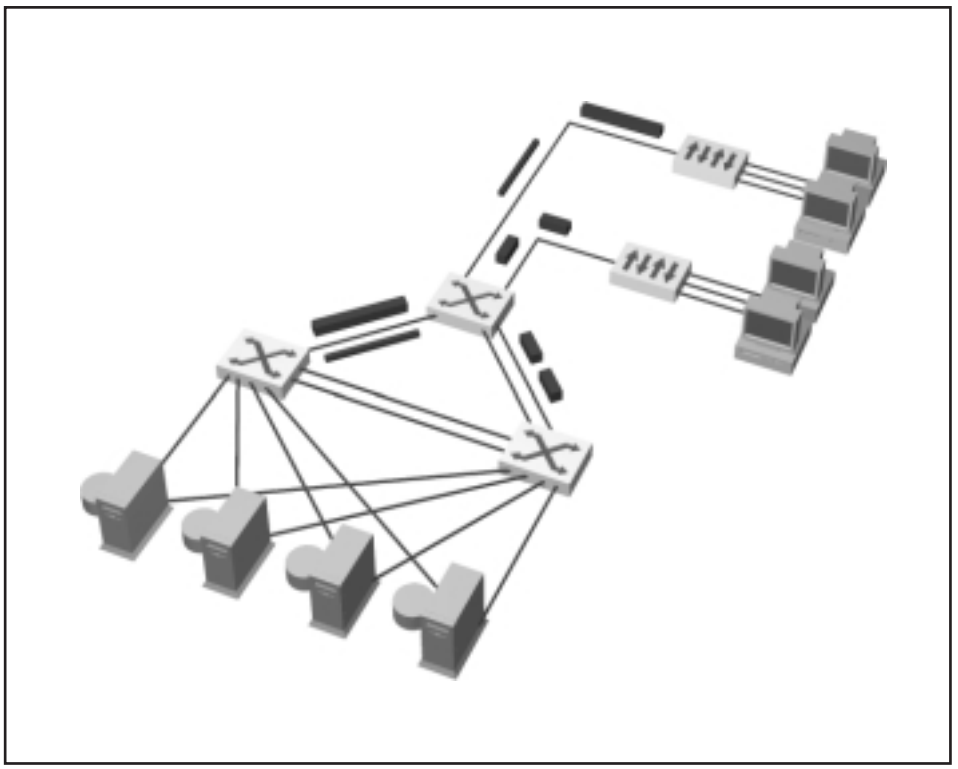
- sehr hohe Investitionskosten
- komplexer Betrieb
- für kleinere Netzwerke häufig oversized

Durch neue Redundanz- und Design-Standards speziell auf Layer-2-Niveau und günstigere Layer-3-Einstiegspreise hat sich diese Situation deutlich verändert. Heute steht dem LAN-Betreiber ein breites Spektrum an Lösungen mit folgenden Eigenschaften zur Verfügung:

- Skalierbare Redundanz-Qualität
- Skalierbare Investitions-Kosten
- Skalierbarer Betriebsaufwand
- Optimale Integration von Server- und Speicher-Architekturen

Damit werden Redundanz und Skalierbarkeit zu einer Standard-Architektur-Eigenschaft, die in jeder Netzwerk-Größe zum Einsatz kommen kann. Gute Einstiegslösungen sind bereits mit geringen Mehrkosten zu realisieren.

Gleichzeitig wachsen LAN- und System-/Speicher-Architekturen immer stärker zusammen. Damit gewinnen LAN-Design-Verfahren eine neue systemtechnische Bedeutung. Die Reduzierung auf triviale Netzwerk-Architekturen ohne Berücksichtigung der besonderen Anforderungen moderner Server-, Cluster- und Speicher-Systeme ist nicht mehr sinnvoll.



Das Seminar befasst sich sowohl mit dem Aufbau neuer als auch mit dem Redesign bestehender Netzwerke.

Dieses Seminar vermittelt, wie unter Nutzung der neuesten Redundanz- und Switching-Verfahren ein LAN optimal gestaltet werden kann und wie dabei die Anforderungen moderner Server- und Speicher-Systeme auch im Sinne von Verfügbarkeit, Loadbalancing und Verkehrsoptimierung architektonisch integriert werden können.

Die Teilnehmer lernen, welche LAN-Redundanz- und Design-Verfahren existieren, welche denkbaren Architektur-Alternativen daraus resultieren, was speziell die neuen Verfahren bringen, welchen Stellenwert die "alten" Verfahren haben und welche dominanten System-/Speicher-Architekturen zu beachten und wie diese konzeptionell abzugrenzen bzw. zu integrieren sind. Dazu gehören auch Tipps und Tricks, wann und wie welches Verfahren eingesetzt werden sollte, welche Verfügbarkeits-Werte mit welchen Verfahren erreicht werden können und wie bereits bestehende LANs durch geeignete Modifikation wirtschaftlich optimal in ihrer Leistung deutlich aufgewertet werden können.

Die Referentin Dipl.-Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie ist langjährige Referentin der ComConsult Akademie, ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen.

Redundanzverfahren und Design-Konzepte von LANs

Redundanzverfahren und Design-Konzepte von LANs – Der Inhalt

Motivation
Zukünftiger Struktur- und Leistungsbedarf im Umfeld vollvernetzter Systeme und Produktivitätssteigerung; typische Schwachstellen bei zentralen Switches und zentralen Servern; Verfügbarkeits-Stufen für Netzwerke und Server, Bildung von Gefahrenklassen; Positionierung von High Speed Techniken (Gigabit Ethernet, 10 Gbit Ethernet, DWDM) versus etablierte LAN-Techniken (10/100 Mbit Ethernet, Token Ring, ATM), Kombination und Integration mit neuen Diensten

Grundlagen neuer High Speed Techniken
Gbit Ethernet, 10 Gigabit Ethernet, DWDM; Konfigurationsmöglichkeiten und Kosten

Bedarf und Strategien zum stufenweisen Ausbau existierender Netzwerke
Typische LAN-Szenarien. Backbone-Design (LAN/ATM) und Redundanzproblematik, Design-Alternativen mit Layer-2, Layer-3 und Layer-4 Switching in aufsteigender Komplexität für unterschiedliche Leistungsklassen. Gebäude-/Etagen-Design, Server-Anbindung (Mainframes, Hosts, Unix- und PC-Server); strategische, netztechnische und betriebstechnische Bewertungs-Kriterien für eine Migration. Typische und angemessene Überbuchungs-Faktoren. Migrations-Szenarien an Projekt-Beispielen

Chancen und Risiken neuer Redundanzverfahren
IEEE 802.1w Rapid Spanning Tree, wesentliche Änderungen und Verbesserungen im Vergleich zu 802.1D, Einsatz-Beispiele, Kombination von RSTP mit Layer-3 Verfahren; IEEE 802.1s Multiple Spanning Tree und seine Verbindung zur VLAN-Technik; MSTP versus OSPF-Routing, VRRP, HSRP und kombinierter Betrieb: Wann und wo welches Verfahren?

NAS und SAN
Einsatz-Strategien und Aufbau von Speicher- und Backend-Netzen; wo eignet sich welche Lösung? Fibre Channel und Fibre Channel II. Storage über IP (FCIP, iFCP, iSCSI, iSNS), DAFS als neuer Direktzugriff auf vernetzte Plattensysteme, Stand der Standardisierung und Marktsituation

Tuning von Netzen mit Load Balancing, Layer-4 und Layer-7 Switching
Load Balancing mit Mehrfach-NIC's; Load Balalncing, Priorisierung, Zuschalten von Überlast-Servern und Failover mit separaten Layer-4 Switches in Ein-Standort- und Mehr-Standort-Konzepten; Kombination mit Layer-3 Switching in einem Gerät / in separaten Geräten; Was ist Layer-7 Switching? HTTP- und DNS Redirects und ihre Bedeutung für Mehrstandort-Konzepte; Einsatzszenarien, Vor- und Nachteile

Vom Best Effort zum Quality of Service LAN
Positionierung, Bedeutung und Einsatz der Standard-Ansätze IEEE 802.1D/p, 802.1Q/v, DiffServ, RSVP, sowie ihr Zusammenhang mit VLAN-Technik und Multicast-Applikationen; was bringt Priorisierung in LANs? Design-Hinweise zum effizienten Einsatz von Quality of Service-Strategien

Markttrends, Bewertungskriterien, Produktsituation:
"Heiße" und "kalte" Produktgruppen, Markttrends und Umsätze; Gegenüberstellung und Bewertung für die einzelnen Produkt-Kategorien, Produktübersichten

Der Veranstalter behält sich Änderungen im Programm vor.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Redundanzverfahren

Ich melde mich an für das Seminar
Redundanzverfahren und Design-Konzepte von LANs
☐ vom 08. - 10.04.02 Hilton Bonn
☐ vom 10. - 12.06.02 Hilton Bonn
☐ vom 16. - 18.09.02 Maritim Königswinter
☐ vom 11. - 13.11.02 Hilton Bonn
zum Preis von € 1.590,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Vorgehensweise bei der Erstellung einer unternehmensweiten IT-Sicherheitspolitik

1.1 Der IT-Sicherheitsprozess

Der IT-Sicherheitsprozess lässt sich als Pyramide mit vier aufeinander aufbauenden Ebenen darstellen. Die oberste Ebene und damit die Basis für alle Sicherheitsmaßnahmen ist die unternehmensweite IT-Sicherheitspolitik. Die zweite Ebene wird durch die IT-Sicherheitsrichtlinien gebildet. Diese definieren mittels Anforderungen und Maßnahmen die Schnittstelle zwischen den verschiedenen Sicherheitskonzepten und der Sicherheitspolitik. In der dritten Ebene sind die verschiedenen Sicherheitskonzepte angesiedelt und beschreiben detailliert die einzelnen Bausteine der IT-Sicherheitsarchitektur.

Dazu gehören unter anderem Lösungen für:

- Internetzugang;
- Remote-Access;
- Virenschutz;
- Verschlüsselung;
- Netztopologie;
- ....

In der vierten Ebene erfolgt die Umsetzung der Sicherheitskonzepte. Dies bedeutet, es werden die für die Sicherheitsverfahren notwendigen Sicherheitsmechanismen implementiert, konfiguriert und ausgeliefert. Der IT-Sicherheitsprozess ist in der nachfolgenden Skizze dargestellt.

Wandlungen in den Geschäftsprozessen, technischen Weiterentwicklungen sowie aufgedeckte Schwachstellen in Hard- oder Softwareprodukten resultieren in neuen Anforderungen an die IT-Infrastruktur. Sind diese Anforderungen bereits durch existente Sicherheitskonzepte (Ebene 3) abgedeckt, können sie direkt im Rahmen der Umsetzung (Ebene 4) erfüllt werden. Andernfalls müssen neue Sicherheitskonzepte entworfen werden, welche sowohl auf der Sicherheitspolitik (Ebene1) basieren als auch den Anforderungen der Sicherheitsrichtlinien (Ebene 2) gerecht werden. Sollten keine angemessenen Sicherheitsrichtlinien definiert sein, sind diese entsprechend neu zu erstellen.

Prinzipiell ist eine Änderung der Sicherheitspolitik zu vermeiden, da dies sich auf die gesamte Sicherheitsarchitektur auswirkt. Die Sicherheitspolitik sollte nur dann überarbeitet werden, wenn eine Änderung der IT-Infrastruktur eine Neubewertung der Risiken erfordert oder wenn sich die Sicherheitsziele der Unternehmung geändert haben.

Der Autor

Dipl.-Inform. Sven Schumann war bei der ComConsult Beratung und Planung GmbH als Berater für Netzwerk-Sicherheit und -Management beschäftigt. Er besitzt mehrjährige Erfahrung und umfassende praktische Kenntnisse insbesondere auf den Gebieten Internet-Security, Verschlüsselung und Firewalls.

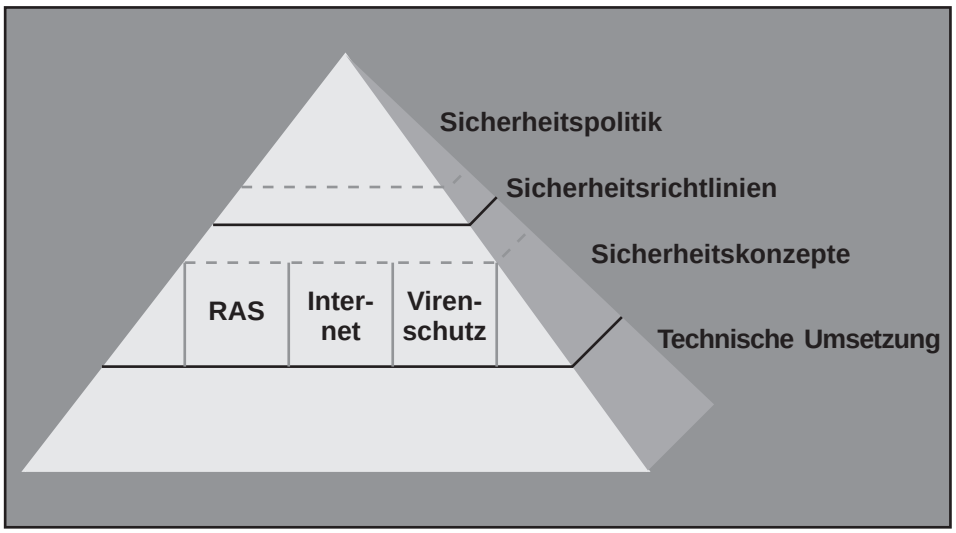
1.2 IT-Sicherheitspolitik

Im Rahmen einer unternehmensweiten IT-Sicherheitspolitik werden die Sicherheitsziele einer Unternehmung und die zur Erreichung dieser Ziele notwendigen Maßnahmen definiert. Die Sicherheitsziele sind in allgemeine und spezielle Sicherheitsziele untergliedert. Während sich die allgemeinen Sicherheitsziele auf die gesamte Unternehmung beziehen, richten sich die speziellen Ziele auf einzelne Arbeitsabteilungen, Projekte oder Datenbestände. Gleichzeitig werden innerhalb der Sicherheitspolitik Verantwortlichkeiten definiert und die Schnittstelle zwischen Management und IT beschrieben.

Im Abschnitt 1.1 wurden die verschiedenen Ebenen des IT-Sicherheitsprozesses dargestellt. Die IT-Sicherheitsrichtlinien nehmen hier eine eigene Ebene ein. Dies ist für eine klare und strukturierte Darstellung des IT-Sicherheitsprozesses sinnvoll und notwendig. Im Rahmen der Definition einer unternehmensweiten Sicherheitspolitik werden die Ebenen 1 (Sicherheitspolitik) und 2 (Sicherheitsrichtlinien) zu einer vollständigen Darstellung der IT-Sicherheitspolitik zusammengefasst.

Die durch die IT-Sicherheitspolitik definierten Maßnahmen bilden nur in der Gesamtheit einen wirksamen Schutz. Jede Sicherheitsmaßnahme für sich kann ausgehebelt werden. Nur durch den flankierenden Schutz anderer Sicherheitsmaßnahmen kann eine stabile Schutzfunktion erreicht werden. Deshalb ist eine Betrachtung des Zusammenwirkens aller im Unternehmen umgesetzten Sicherheitsmaßnahmen notwendig. Des weiteren muss eine unternehmensweite und bereichsübergreifende Kontrolle und Steuerung des IT-Sicherheitsprozesses erfolgen. Diese Aufgabe wird durch die Funktion des IT-Sicherheitsbeauftragten umgesetzt.

Bild 1 Der IT-Sicherheitsprozess als Pyramide



1.3 Der IT-Sicherheitsbeauftragte

Zur Koordination aller Maßnahmen sowie zur Kontrolle und Steuerung des IT-Sicherheitsprozesses sollte die Position eines IT-Sicherheitsbeauftragten (IT Security Officer) geschaffen werden.

Dieser muss über ein geeignetes Budget und hinreichende Personalressourcen zur Planung, Konzeption, Umsetzung und Kontrolle von Sicherheitsmaßnahmen verfügen.

Aufgrund der unternehmensweiten und bereichsübergreifenden Tätigkeit innerhalb einer Unternehmung ist zu empfehlen, dass eine solche Position als Stabsstelle des Vorstandes angesiedelt wird.

Folgende Aufgaben sind unter anderem durch den IT-Sicherheitsbeauftragten zu bewältigen:

- Aktualisierung der Sicherheitspolitik;
- Kontinuierliche Überwachung des IT-Sicherheitsniveaus der Unternehmung;
- Erstellen von Sicherheitskonzepten zur Erschließung von neuen Geschäftsfeldern;
- Erstellung oder Anpassung von Sicherheitskonzepten zur Realisierung des angestrebten Sicherheitsniveaus;
- Belehrung und Schulung der Benutzer.

Aufgrund der knappen personellen Ressourcen im IT Bereich ist es nicht realistisch, von einem ausschließlich dem Sicherheitsbereich zugeteilten Personal auszugehen. Statt dessen sollte in jedem Know-how Bereich (UNIX, NT, eMail, Firewall etc.) ein Ansprechpartner für den IT-Sicherheitsbeauftragten ernannt werden. Auf dieses spezialisierte Personal kann dann im Rahmen von Sicherheitsprojekten mittels Weisungsbefugnis durch den IT-Sicherheitsbeauftragten zugegriffen werden.

Basierend auf der Brisanz der Thematik Sicherheit sollte der IT-Sicherheitsbeauftragte dem Vorstand direkt Bericht erstatten.

Dabei sollte der IT-Sicherheitsbeauftragte über ein Einspruchsrecht mit aufschiebender Wirkung verfügen. Dieses erlaubt es, riskante Projekte solange zu stoppen, bis durch den Vorstand eine Entscheidung getroffen wurde.

1.4 Abgrenzung zur Notfallplanung

Die IT-Sicherheitspolitik befasst sich maßgeblich mit der Abwehr von Bedrohungen der IT-Infrastruktur, die durch externe oder interne Angreifer entstehen.

Bedrohungen, die aus nicht vorhersehbaren Ereignissen oder Naturkatastrophen resultieren, werden lediglich am Rande betrachtet. Eine Bewertung dieser Ereignisse sowie die Definition entsprechender Abwehrmaßnahmen sind im Rahmen der Notfallplanung zu berücksichtigen.

Gleichzeitig werden im Rahmen der IT-Sicherheitspolitik Anforderungen an Maßnahmen im Fehler- oder Katastrophenfall definiert. Auch diese Maßnahmen sind zu beschreiben und im Rahmen der Notfallplanung zu realisieren.

Bezogen auf den IT-Sicherheitsprozess ist die Notfallplanung sowohl auf Ebene 2 (Sicherheitsrichtlinien) als auch auf Ebene 3 (Sicherheitskonzepte) anzusiedeln.

Die IT-Sicherheitspolitik definiert damit die Notwendigkeit der Existenz der Notfallplanung, und die Notfallplanung ergänzt die IT-Sicherheitsrichtlinien und IT-Sicherheitskonzepte um die Komponente der Gefahrenabwehr im Fehler- oder Katastrophenfall.

1.5 Vorgehensweise

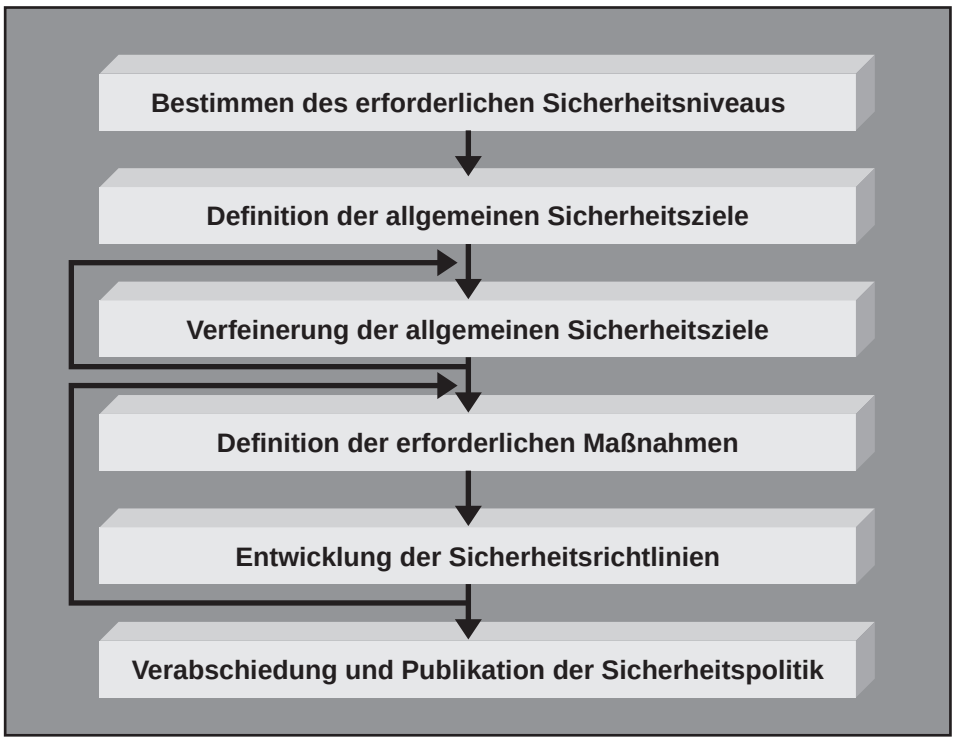
Die Entwicklung einer unternehmensweiten IT-Sicherheitspolitik umfasst die folgenden Phasen:

- Phase 1
  Bestimmung des erforderlichen IT-Sicherheitsniveaus;
- Phase 2
  Definition der allgemeinen Sicherheitsziele;
- Phase 3
  Verfeinerung der allgemeinen zu den speziellen Sicherheitszielen;
- Phase 4
  Ableiten der zum Erreichen der Sicherheitsziele notwendigen Maßnahmen;
- Phase 5
  Erstellen der IT-Sicherheitsrichtlinien;
- Phase 6
  Verabschiedung der IT-Sicherheitspolitik durch die Geschäftsführung.

Diese Vorgehensweise ist in Bild 2 dargestellt.

Die einzelnen Phasen werden im folgenden kurz vorgestellt.

Bild 2 Vorgehensweise



1.5.1 Bestimmen des erforderlichen IT-Sicherheitsniveaus

Im ersten Schritt werden die zu schützenden IT-Ressourcen definiert. Im Anschluss erfolgt die Bestimmung des Wertes dieser IT-Ressourcen.

Ein solcher ergibt sich aus folgenden Kriterien:

- Abhängigkeit der operativen Geschäftsprozesse von der IT-Ressource;
- Verarbeitung oder Speicherung von vertraulichen/geheimen Informationen durch diese IT-Ressource;
- Anforderungen an die Korrektheit der durch die IT-Ressource zu verarbeitenden Informationen;
- Anforderungen an die Verfügbarkeit der IT-Ressource.

Dabei muss berücksichtigt werden, dass die strategische/operative Bedeutung einer IT-Ressource meist deutlich höher ist als ihr reiner Materialwert.

Resultierend aus der IT-Infrastruktur und basierend auf den Datenbeständen der Unternehmung wird das erforderliche IT-Sicherheitsniveau bestimmt.

Damit ergibt sich zwangsläufig der notwendige Schutz für Hard- und Softwareressourcen aus den auf diesen Ressourcen gespeicherten oder verarbeiteten Datenbeständen.

1.5.2 Definition der Sicherheitsziele und Maßnahmen

Die allgemeinen Sicherheitsziele definieren den angestrebten Grundschutz für die IT-Infrastruktur der Unternehmung.

Spezielle Sicherheitsziele werden für alle Datenbestände definiert, welche vom Grundschutz abweichen und einen höheren oder niederen Schutzbedarf aufweisen.

Zum Erreichen des angestrebten Sicherheitsniveaus sind hierarchisch aufgebaute Maßnahmen zu definieren.

Das heißt, alle Maßnahmen für ein niederes Sicherheitsniveau sind Grundvoraussetzung für solche zum Erreichen eines höheren Sicherheitsniveaus.

1.5.3 Erstellen von Sicherheitsrichtlinien

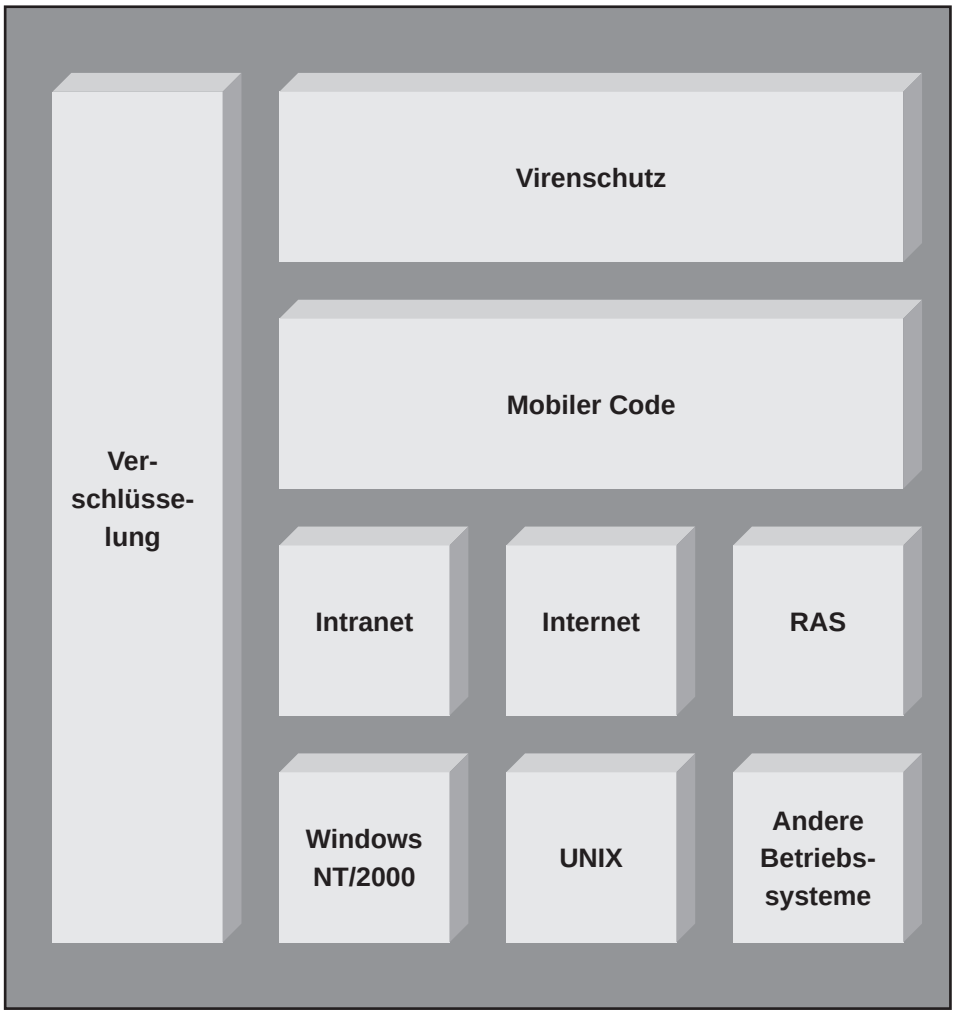
Nach der Erarbeitung der zum Erreichen der IT-Sicherheitsniveaus notwendigen Maßnahmen werden die für die Geschäftsprozesse kritischen Handlungsfelder bestimmt. Für diese erfolgt die Definition von Anforderungen und Maßnahmen im Rahmen von IT-Sicherheitsrichtlinien.

Üblicherweise sind die folgenden für die Geschäftsprozesse kritischen Handlungsfelder im Rahmen der IT-Sicherheitsrichtlinien zu behandeln:

- LAN und Windows NT/2000;
- Remote-Access und Telekommunikationsanlagen;
- Internetzugang und öffentliche Server;
- Abwehr von schadenstiftender Software;
- Kontrolle von mobilem Code;
- Einsatz von Verschlüsselungsverfahren.

Das Zusammenwirken der einzelnen Bestandteile der Sicherheitsrichlinien ist in Bild 3 dargestellt.

Bild 3 Zusammenwirken der einzelnen Bestandteile der Sicherheitsrichtlinien*



* Da eine Behandlung der Sicherheitsrichtlinien den Rahmen dieses Artikels sprengen würde, wird im folgenden nicht weiter darauf eingegangen. Vielmehr wird die Erstellung und Pflege der Sicherheitsrichtlinien innerhalb des IT-Sicherheitsprozesses in einem folgenden Artikel detailliert behandelt.

Vorgehensweise bei der Erstellung einer unternehmensweiten IT-Sicherheitspolitik

2.
Allgemeine Bedrohungsanalyse

Für die Erstellung einer unternehmensweiten Sicherheitspolitik ist es unumgänglich, eine Betrachtung der möglichen Bedrohungsklassen vorzunehmen. Im Rahmen dieses Kapitels wird eine allgemeine Bedrohungsanalyse für die IT-Infrastruktur, im weiteren ITI genannt, durchgeführt.

Die allgemeine Bedrohungsanalyse basiert auf den allgemeinen Sicherheitszielen Vertraulichkeit, Verfügbarkeit und Integrität. Diese sind wie folgt definiert:

Vertraulichkeit

Die Vertraulichkeit von sensitiven Daten muss gewährleistet sein.

Dies umfasst sowohl personenbezogene Daten, für die eine gesetzliche Schutzpflicht existiert, als auch unternehmenskritische Daten, welche die Marktposition der Unternehmung gegebenenfalls negativ beeinflussen und Geschäftsprozesse gefährden können.

Verfügbarkeit

Der Begriff "Verfügbarkeit" beschreibt den Zustand einer Ressource, vorhanden zu sein, wenn diese Ressource benötigt wird.

Dies umfasst neben der physikalischen Anwesenheit der Ressource auch die Möglichkeit des logischen Zugriffs. So kann es neben einer beispielsweise durch Kabelbruch hervorgerufenen physikalischen Unterbrechung einer Kommunikationsverbindung auch zu logischen Störungen durch Ausfall der Ressource oder Netzüberlastung kommen.

Integrität

Dieser Sicherheitsaspekt umfasst die Vollständigkeit und Korrektheit von gespeicherten und übermittelten Daten.

Dies bedeutet zum einen, dass Daten nur von Berechtigten verändert werden dürfen und zum anderen, dass zu gewährleisten ist, dass übermittelte Daten vollständig und unverändert beim Empfänger ankommen.

Daher muss sowohl der Zustand der Daten als auch die Authentizität einer Kommunikation prüfbar sein (mit dem Begriff Integrität wird auch die Verbindlichkeit definiert).

2.2
Unberechtigter externer Zugriff (Vertraulichkeitsverlust)

2.2.1
Hacking

Diese Bedrohungsvariante umfasst das Eindringen in das interne Netz einer Unternehmung über einen Internet- oder "Remote-Access"-Zugang.

Ziel eines solchen Angriffes ist es, über die externen Netzzugänge die Kontrolle über einen oder mehrere Rechner im Intranet zu übernehmen und somit Zugriff auf die IT-Infrastruktur (ITI) zu erlangen.

Diese Bedrohung tritt häufig in Verbindung mit den Bedrohungen "Trojanische Pferde" und "Social Engineering" auf (siehe die Abschnitte 2.2.2 und 2.2.3).

2.2.2
Trojanische Pferde

Im Rahmen dieser Bedrohung wird versucht, durch das Einschleusen eines Trojanischen Pferdes die Kontrolle über einen oder mehreren Rechner zu übernehmen. Unter einem Trojanischen Pferd wird in diesem Zusammenhang eine Software mit nicht dokumentierten und Schaden stiftenden Eigenschaften verstanden.

Ziel ist es hierbei in den meisten Fällen, die Fernsteuerung des angegriffenen Rechners zu erlauben.

Auf diesem Wege ist es dann unter anderem möglich, auf dem angegriffenen Rechner

- Dateien aufzuspielen,
- Dateien zu laden,
- Programme auszuführen sowie
- Tastatureingaben zu protokollieren und auf diese Weise Passwörter zu sammeln.

Dadurch ist es einem Angreifer möglich, Zugriff auf Informationen in der IT-Infrastruktur zu erlangen sowie die Verfügbarkeit und Integrität der Daten zu gefährden.

2.2.3
Social Engineering

Unter dem Begriff "Social Engineering" soll in diesem Zusammenhang das Beschaffen von Informationen unter Vorspiegelung einer falschen Identität verstanden werden.

Ein Angreifer versucht, Mitarbeiter der Unternehmung zur Preisgabe von sensitiven Informationen zu bewegen.

Dazu gehören unter anderem:

- Informationen über die ITI;
- Informationen über die Mitarbeiterstruktur (Namen, Telefonnummern, Anwesenheitsraster etc.);
- Passwörter und Rechtevergabe.

In bestimmten Situationen wird versucht, die Zielperson zum Freischalten von Accounts oder zu einer Vergabe von bestimmten Rechten zu bewegen. Ziel ist es, entweder direkten Zugriff auf die ITI zu erlangen oder einen anderen Angriff vorzubereiten.

2.2.4
Physikalischer Zugriff

Diese Bedrohung umfasst jeden unberechtigten direkten physikalischen Zugriff durch externe Personen und/oder Institutionen auf die ITI.

Hierunter fallen unter anderem:

- Server und Workstations;
- Verkabelung;
- Netzwerkkomponenten;
- Backupmedien;
- Telefonanlage.

Zusätzlich umfasst dies den Zugriff auf konventionelle Daten, wie zum Beispiel:

- Papierdokumente;
- Mikrofilme.

Durch einen direkten physikalischen Zugriff werden die Vertraulichkeit, die Integrität und vor allem die Verfügbarkeit der Informationen einer Unternehmung bedroht.

2.2.5
Kooperation mit Insidern

Ein Angreifer kann durch eine Kooperation mit einem Insider versuchen, die Sicherheitsmechanismen zu unterlaufen.

Dabei ist zwischen der wissentlichen und unwissentlichen Mithilfe durch einen Insider zu unterscheiden. Eine unwissentliche Hilfe wird häufig durch einen auf "Social Engineering" basierenden Angriff ausgelöst, siehe Abschnitt 2.2.3.

Eine Kooperation kann unter anderem umfassen:

- Öffnen von Netzwerkverbindungen nach außen;
- Freischalten von Accounts und Vergabe von Zugriffsrechten;
- Weitergabe von Know-how über die Sicherheitsarchitektur, die ITI und die Mitarbeiterstruktur;
- Einspielen von Software.

Basierend auf einer Kooperation mit einem Insider werden Vertraulichkeit, Integrität und Verfügbarkeit der Informationen bedroht.

2.3 Unberechtigter interner Zugriff (Vertraulichkeitsverlust)

2.3.1 Mithören

Diese Bedrohung umfasst das passive Mithören (Sniffing) im Intranet einer Unternehmung.

Ein interner Angreifer kann durch das Abfangen von Datenpaketen jede Kommunikation innerhalb des überwachten Netzwerksegmentes mithören. Dies betrifft alle Netzwerkdienste ab dem OSI Layer 3. Dazu muss der Angreifer in der Lage sein, die dafür notwendige Software in die ITI einspielen und installieren zu können.

Durch das Mithören wird die Vertraulichkeit der Informationen in der ITI bedroht.

2.3.2 Hacking

Diese Bedrohungsvariante umfasst das Eindringen in Bereiche der ITI über das Intranet.

Ziel dieses Angriffes ist es, über das interne Netz die Kontrolle über weitere Rechner im Intranet zu übernehmen und somit einen erweiterten Zugriff auf die ITI der betroffenen Unternehmung zu erlangen.

Oft handelt es sich hierbei um den zweiten Schritt nach erfolgreichem Eindringen eines externen Angreifers in das interne Netz, siehe Abschnitt 2.2.1.

Diese Bedrohung wird häufig mit der des "Mithörens", siehe Abschnitt 2.3.1, kombiniert und greift Vertraulichkeit, Integrität und Verfügbarkeit der Informationen an.

2.3 Physikalischer Zugriff

Diese Bedrohung umfasst jeden unberechtigten direkten physikalischen Zugriff einer internen Person auf die ITI.

Hierunter fallen unter anderem:

- Server und Workstations;
- Verkabelung;
- Netzwerkkomponenten;
- Backupmedien;
- Telefonanlage.

Zusätzlich umfasst dies den Zugriff auf konventionelle Daten, wie zum Beispiel:

- Papierdokumente;
- Mikrofilme.

Durch einen direkten physikalischen Zugriff werden die Vertraulichkeit, die Integrität und vor allem die Verfügbarkeit der Informationen bedroht.

2.4 Verfügbarkeitsverlust

2.4.1 Katastrophen

Diese Bedrohung umfasst menschliches Versagen oder höhere Gewalt, welche zu einem Verfügbarkeitsverlust der ITI führen.

Dazu gehören unter anderem:

- Brandschäden;
- Wasserschäden;
- Stromausfall.

2.4.2 Unberechtigter externer Zugriff

Wenn es einem externen Angreifer gelingt, in einer im Abschnitt 2.2 beschriebenen Art und Weise Zugriff auf das Intranet einer Unternehmung zu erlangen, wird dadurch die Verfügbarkeit der ITI bedroht.

Diese Bedrohung umfasst unter anderem:

- Vandalismus;
- Fehlbedienung;
- physikalische Verluste aufgrund von Brandstiftung, Diebstahl sowie EMP-Angriffen.

2.4.3 Unberechtigter interner Zugriff

Wenn es einem internen Angreifer gelingt, in einer im Abschnitt 2.3 beschriebenen Art und Weise Zugriff auf das Intranet einer Unternehmung zu erlangen, wird dadurch die Verfügbarkeit der ITI bedroht.

Diese Bedrohung umfasst unter anderem:

- Vandalismus;
- Fehlbedienung;
- physikalische Verluste aufgrund von Brandstiftung, Diebstahl sowie EMP-Angriffen.

2.4.4 Technisches Versagen

Diese Bedrohung umfasst alle Arten von nicht vorsätzlich ausgelöstem Hard- und Softwareausfall, die in einen Verfügbarkeitsverlust münden.

2.5 Integritätsverletzung

2.5.1 Unberechtigter externer Zugriff

Wenn es einem externen Angreifer gelingt, in einer im Abschnitt 2.2 beschriebenen Art und Weise Zugriff auf das Intranet zu erlangen, wird dadurch die Integrität des Informationsbestandes der Unternehmung bedroht.

2.5.2 Unberechtigter interner Zugriff

Wenn es einem internen Angreifer gelingt, in einer im Abschnitt 2.3 beschriebenen Art und Weise Zugriff auf das Intranet zu erlangen, ist dadurch die Integrität des Informationsbestandes der Unternehmung gefährdet.

2.5.3 Technisches Versagen

Diese Bedrohung umfasst alle Arten von nicht vorsätzlich ausgelöstem Hard- und Softwareausfall, die in einen Integritätsverlust münden.

2.5.4 Menschliches Versagen

Diese Bedrohung umfasst alle Arten eine nicht vorsätzlichen Fehlverhaltens beim Umgang mit der ITI, die in einen Verlust der Integrität des Informationsbestandes der Unternehmung münden.

Vorgehensweise bei der Erstellung einer unternehmensweiten IT-Sicherheitspolitik

3.
Bestimmung des IT-Sicherheitsniveaus

Zur Erstellung einer Sicherheitspolitik ist es notwendig, eine Definition von Schadens- und Informationsklassen sowie eine Strukturierung der Informationsbestände hinsichtlich der IT-Sicherheit durchzuführen.

Basierend auf dieser Definition erfolgt eine Zuordnung der Informationsbestände zu dem für jede Informationsklasse resultierenden Schaden. Diese Zuordnung erlaubt die Bestimmung des notwendigen Sicherheitsniveaus und die Ableitung der allgemeinen und speziellen Sicherheitsziele.

Im Rahmen dieses Kapitels wird eine mögliche Unterteilung von Schadens- und Informationsklassen sowie eine Strukturierung der verschiedenen Informationstypen vorgestellt.

3.1
Definition der Schadensklassen

Im Rahmen der Erstellung einer Sicherheitspolitik wird der Schaden, welcher durch eine Bedrohung entstehen kann, abgeschätzt.

Dabei wird von folgenden Schadensklassen ausgegangen:

Klasse 1
(Hoher Schaden)

In dieser Klasse werden alle Schäden zusammengefasst, welche aufgrund von Gesetzesverstößen, Image- oder finanziellem Verlust einen erheblichen Schaden für die Unternehmung bedeuten.

Klasse 2
(Mittlerer Schaden)

Zu dieser Klasse gehören alle Schäden, die einen finanziellen oder Imageverlust, welcher nicht existenzbedrohend ist, zur Folge haben. Innerhalb der Unternehmung werden finanzielle Verluste bis zu einer Höhe von x Mio. DM als mittlerer Schaden eingestuft.

Klasse 3
(Niedriger Schaden)

Dies umfasst kleinere Beeinträchtigungen des Erscheinungsbildes der Unternehmung in der öffentlichen Meinung, welche nicht oder nur in geringem Umfang in einen finanziellen Verlust münden. Innerhalb der Unternehmung werden finanzielle Verluste bis zu einer Höhe von y Mio. DM als mittlerer Schaden eingestuft.

Die Anzahl der Schadensklassen ist von der konkreten Risikosituation der Unternehmung abhängig.

Erfolgt eine zu feine Unterteilung erhöht sich die Anzahl der Sicherheitsziele drastisch und die IT-Sicherheitspolitik wird unübersichtlich. Eine zu grobe Unterteilung führt hingegen zu einer unverhältnismäßigen Anhäufung von einigen, wenigen Schadensklassen.

Ebenso wie die Klassifikation des Schadens ist auch die Definition der Geldbeträge als Indikatoren für die Schadensklassen von der wirtschaftlichen Situation der jeweiligen Unternehmung abhängig.

3.2
Allgemeine Informationsklassifikation

Im Rahmen der Informationsklassifikation wird von den drei Sicherheitszielen Vertraulichkeit, Verfügbarkeit und Integrität ausgegangen.

Da sowohl in den notwendigen Voraussetzungen als auch in den Schutzmaßnahmen die Sicherheitsziele Vertraulichkeit und Integrität eine hohe Ähnlichkeit aufweisen, werden diese hier zusammengefasst.

Beide Sicherheitsziele werden durch unberechtigten internen und/oder externen Zugriff bedroht und können daher durch ein Sicherheitsziel abgebildet werden.

Daher lässt sich folgende Einteilung des Informationsbestandes vornehmen:

Klasse 1
(Externer Zugriff)

Informationen, die vor einem unberechtigten externen Zugriff geschützt werden müssen, um einen Vertraulichkeitsverlust zu vermeiden.

Klasse 2
(Interner Zugriff)

Informationen, die vor einem unberechtigten internen Zugriff geschützt werden müssen, um einen Vertraulichkeitsverlust zu vermeiden.

Klasse 3
(Hohe Verfügbarkeit)

Informationen, welche eine hohe Verfügbarkeit aufweisen müssen und aus Gründen einer schnellen Reaktion auf Ereignisse nur kurzen Ausfallzeiten unterliegen dürfen.

Klasse 4
(Lange Verfügbarkeit)

Informationen, welche über einen langen Zeitraum hinweg verfügbar sein müssen; in dieser Klasse steht nicht die schnelle Reaktion im Vordergrund, sondern die grundsätzliche Verfügbarkeit des Informationsbestandes.

Klasse 5
(Gesetzliche Vorschriften)

Informationen, welche einem durch den Gesetzgeber vorgeschriebenen Schutzniveau unterliegen.

Die einzelnen Daten des Informationsbestandes einer Unternehmung sind in der Mehrzahl der Fälle durch mehr als eine Klasse zu beschreiben.

In diesen Fällen ist eine Priorisierung der Klassen aufstellen.

3.3
Allgemeine Sicherheitsziele

Aus der Informationsklassifikation resultieren die folgenden allgemeinen Sicherheitsziele:

Informationen der Klasse 1

Informationen der Klasse 1 sind so zu schützen, dass ein unberechtigter externer Zugriff durch Personen und/oder Institutionen verhindert wird.

Dies bedeutet:

– Der Aufwand für das Überwinden der Sicherheitsmechanismen durch einen externen Angreifer muss wesentlich größer sein, als der daraus resultierende Nutzen.

– Ein Angriff muss erkennbar, nachvollziehbar und analysierbar sein.

Informationen der Klasse 2

Informationen der Klasse 2 sind so zu schützen, dass der unberechtigte interne Zugriff auf diesen Informationsbestand verhindert wird.

Dies bedeutet:

– Der Aufwand für das Überwinden der Sicherheitsmechanismen durch einen internen Mitarbeiter muss größer sein, als der daraus resultierende Nutzen.

– Ein Angriff muss erkennbar, nachvollziehbar und analysierbar sein.

Informationen der Klasse 3

Informationen der Klasse 3 sind so zu schützen, dass die Verfügbarkeit im Rahmen der akzeptierten Ausfallzeiten gewährleistet ist.

Informationen der Klasse 4

Informationen der Klasse 4 sind so zu schützen, dass die Verfügbarkeit über einen definierten Zeitraum gewährleistet ist.

Informationen der Klasse 5

Informationen der Klasse 5 sind entsprechend der gesetzlichen Vorschriften zu schützen.

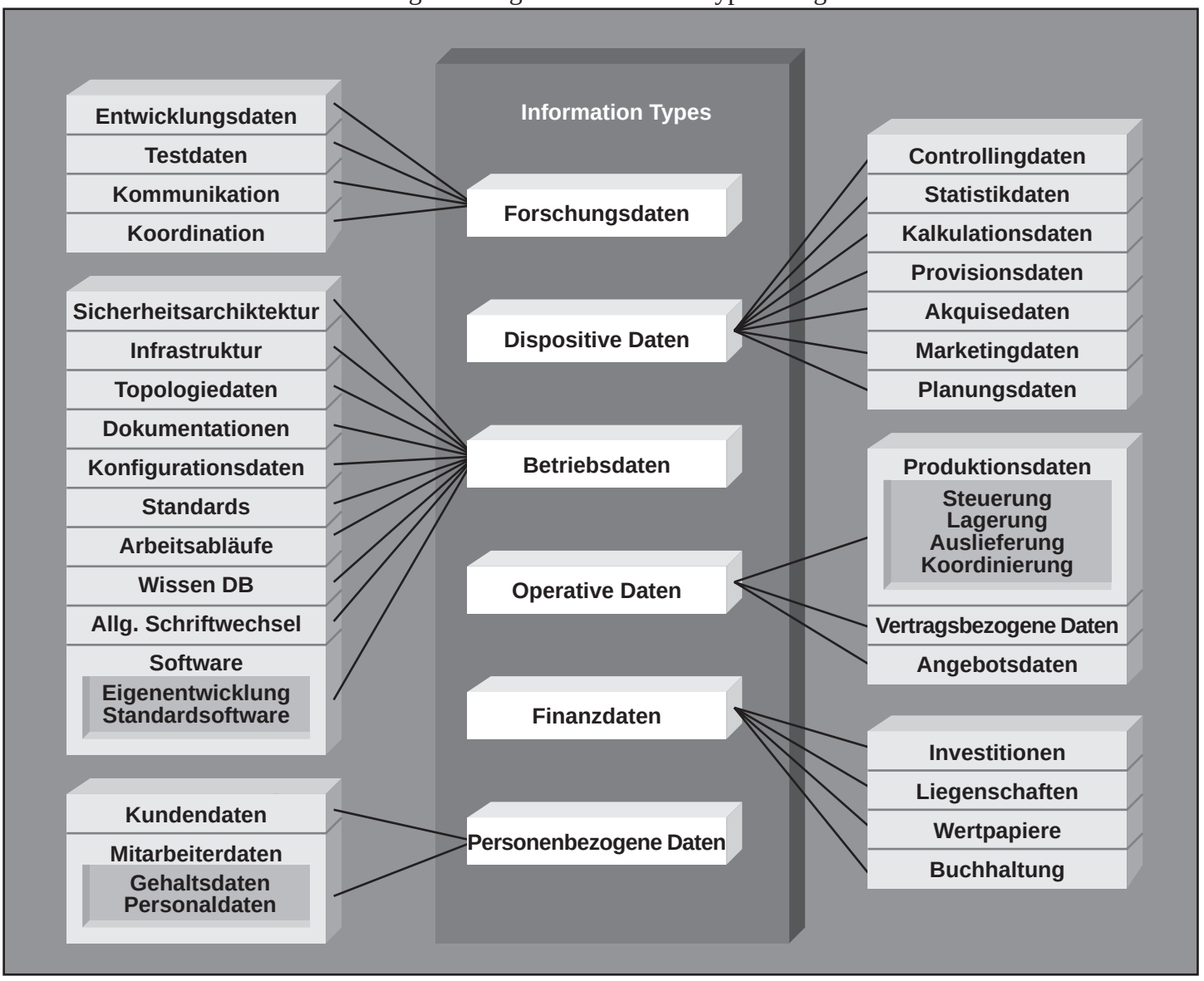
Diese offensichtlich noch sehr allgemeinen Sicherheitsziele werden im weiteren Verlauf der Erstellung einer unternehmensweiten IT-Sicherheitspolitik weiter verfeinert.

3.4 Informationstypen

Eine Aufgliederung der Informationstypisierung ist in Bild 4 dargestellt.

Die Strukturierung der Datenbestände einer Unternehmung und die damit verbundene Zerlegung in Informationstypen ist jedoch zwangsläufig von der IT-Infrastruktur einerseits und den konkreten Geschäftsprozessen andererseits abhängig.

Bild 4 Aufgliederung der Informationstypisierung



Daher wird im folgenden lediglich eine mögliche Strukturierung vorgestellt.

Operative Daten

- Produktionsdaten

Steuerung

Lagerung

Auslieferung

Koordinierung

- Vertragsbezogene Daten
- Angebotsdaten

Forschungsdaten

- Entwicklungsdaten
- Testdaten
- Kommunikation

Dispositive Daten

- Controllingdaten
- Statistikdaten
- ....

Betriebsdaten

- Sicherheitsarchitektur
- Topologiedaten
  (dies umfasst unter anderem Netzwerkpläne, IP-Strukturen, Domänen- und Benutzerkonzepte)
- Dokumentationen
  (darunter sind neben Betriebskonzepten auch Passwörter und Zugangscodes zu verstehen)
- ....

Finanzdaten

3.5 Zuordnung der Schadensklassen zu den Datenbeständen

Im folgenden wird für alle Kombinationen von Informationstypen und Informationsklassen die zugehörige Schadensklasse bestimmt. Aus diesem Tripel werden dann die Sicherheitsziele abgeleitet. Diese können nachfolgend auf Basis der Verfeinerung der Informationstypen weiter detailliert werden. In dem folgenden Beispiel wird für einige Informationstypen diese Zuordnung demonstriert.

Dabei zeigt die Tabelle welches Schadensklasse für welchen Informationstyp unter der Einwirkung bestimmter Bedrohungen relevant ist.

Die Tabelle sollte wie folgt gelesen werden:

> Erfolgt auf die Daten der Lagerhaltung ein unberechtigter externer Zugriff so tritt ein mittlerer Schaden auf.

> Kann auf die Daten der Lagerhaltung ein unberechtigter interner Zugriff erfolgen, so ist mit einem mittleren Schaden zu rechnen.

> Wird die hohe Verfügbarkeit der Lagerhaltungsdaten nicht gewährleistet, dann ist von einem hohen Schaden auszugehen.

Auf diese Weise kann für alle Informationsbestände der Unternehmung auf jeder gewünschten Abstraktionsebene das notwendige IT-Sicherheitsniveau bestimmt werden. Selbstverständlich muss diese Zuordnung in Abhängigkeit der konkreten Unternehmensstruktur erfolgen. Für die Strukturierung des Datenbestandes und der Zuordnung der Schadensklassen ist erfahrungsgemäß ein großer Anteil der gesamten Projektzeit zur Erstellung einer unternehmensweiten IT-Infrastruktur aufzuwenden.

Tabelle 1 Schadensklassenzuordnung

Informationstyp	Externer Zugriff	Interner Zugriff	Hohe Verfügbarkeit	Lange Verfügbarkeit	Gesetzliche Vorgaben
Lagerdaten	mittel	mittel	hoch	mittel	niedrig
Controlling-daten	hoch	mittel	mittel	mittel	niedrig
Kundendaten	hoch	mittel	mittel	hoch	mittel
Sicherheits-architektur	hoch	hoch	mittel	niedrig	niedrig

4.
Definition der Sicherheitsziele und Maßnahmen

Basierend auf dem notwendigen Sicherheitsniveau erfolgt die Definition der Sicherheitsziele. Die zu definierenden Sicherheitsziele berufen sich dabei auf umzusetzende Maßnahmen. Diese werden im Anschluss vorgestellt.

Für die Reduzierung der Sicherheitsziele und der Wahrung einer Übersichtlichkeit wird der notwendige IT-Grundschutz bestimmt. In unserem Beispiel sollen alle zur Abwehr von mittlerem Schaden notwendigen Maßnahmen als Grundschutz verstanden werden. Daher erfolgt nur noch die Definition der nach oben oder unten abweichenden Sicherheitsziele.

Als Beispiel wird sowohl die bereits vorgestellte Strukturierung der Informationsbestände als auch die Zuordnung der Schadensklassen verwendet. Dabei werden aus Platzgründen hier allerdings nur die Sicherheitsziele für die Abwehr von einem unberechtigten externen und internen Zugriff vorgestellt.

4.1
Definition der Sicherheitsziele

Die Sicherheitsziele sind basierend auf der Klassifizierung des vorhandenen Datenbestandes zu definieren und hierarchisch zu gliedern.

Z-1 Die Gesamtheit der Datenbestände der Unternehmung ist hinsichtlich der definierten Sicherheitsziele Vertraulichkeit, Verfügbarkeit und Integrität zu schützen. Dies umfasst außer den eigentlichen Datenbeständen auch die IT-Ressourcen, mit denen die Datenbestände ver- und bearbeitet werden.

4.1.1
Schutz vor unberechtigtem externen Zugriff

Alle Informationsbestände der Unternehmung sind gegen einen unberechtigten externen Zugriff zu schützen. Zu diesem Zweck sind alle der für die Abwehr eines Mittleren Schadens notwendigen Maßnahmen zu realisieren.

Für konkrete Datenbestände ergeben sich folgende verfeinerte Sicherheitsziele:

Z-2 Die dem Informationstyp Betriebsdaten zugeordneten Sicherheitsarchitekturdaten sind besonders gegen einen unberechtigten externen Zugriff zu schützen. Zu diesem Zweck sind alle, der für die Abwehr eines Hohen Schadens notwendigen Maßnahmen zu realisieren.

Z-3 Im Rahmen des Informationstypus Dispositive Daten sind die Controllingdaten durch Maßnahmen zur Abwehr eines Hohen Schadens vor einem unberechtigten externen Zugriff zu schützen.

Z-4 Innerhalb des Informationstypus Personenbezogene Daten sind die Kundendaten mit den entsprechend der zur Abwehr eines Hohen Schadens notwendigen Maßnahmen zu schützen.

4.1.2
Schutz vor unberechtigtem internen Zugriff

Alle Daten der Unternehmung sind gegen einen unberechtigten internen Zugriff zu schützen. Zu diesem Zweck sind in der Regel alle, der für die Abwehr eines Mittleren Schadens notwendigen Maßnahmen zu realisieren.

Für konkrete Datenbestände ergeben sich folgende verfeinerte Sicherheitsziele:

Z-5 Die dem Informationstyp Betriebsdaten zugeordneten Sicherheitsarchitekturdaten sind besonders gegen einen unberechtigten internen Zugriff zu schützen. Zu diesem Zweck sind alle der für die Abwehr eines Hohen Schadens notwendigen Maßnahmen zu realisieren.

4.2
Maßnahmen-Schadensklasse-Zuordnung

Die hier dargestellten Maßnahmen sind hierarchisch angeordnet. Das bedeutet, alle Maßnahmen zur Abwehr eines niedrigen Schadens sind Grundbedingungen für die Maßnahmen zur Abwehr eines mittleren Schadens. Letztere wiederum sind Bestandteil der Maßnahmen zur Abwehr eines hohen Schadens.

Diese Maßnahmen sind an die konkrete Unternehmenssituation anzupassen. Beispielhaft werden hier einige der notwendigen Maßnahmen vorgestellt. Dabei erfolgt nicht nur eine Untergliederung der Maßnahmen nach den Schadensklassen sondern auch nach dem Wirkungsbereich der Maßnahmen selbst.

Resultierend aus diesen Maßnahmen und den Sicherheitszielen folgt eine klare Zuordnung der notwendigen Sicherheitsmechanismen zu einzelnen Datenbeständen. Dies lässt sich sowohl in der Planungs- als auch in der Umsetzungsphase von IT-Projekten berücksichtigen und erlaubt somit eine fließende Implementierung der IT-Sicherheitspolitik.

5.
Fazit

Die Erstellung einer unternehmensweiten IT-Sicherheitspolitik ist einerseits notwendig und andererseits ein unter Umständen langwieriger Prozess. Bereits im Vorfeld eines solchen Projektes sind die einzubindenden Entscheidungsträger zu definieren und um Unterstützung zu bitten. Da es sich um die Definition von unternehmensweit gültigen politischen Regelungen handelt, sind neben dem Management sowohl der Datenschutzbeauftragte als auch der Betriebsrat einzubinden.

Erfahrungsgemäß birgt die Strukturierung der Datenbestände und die Zuordnung der Schadensklassen sehr viel Diskussionsstoff in sich und sollte daher auf einer Workshopbasis vorgestellt und weiterentwickelt werden. Eine Steuerung der aus der IT-Sicherheitspolitik resultierenden Kosten kann durch die Definition der Schadensklassen einerseits und die Schadenszuordnung andererseits erfolgen.

Im Anschluss an die Definition der Sicherheitsziele und der zur Umsetzung notwendigen Maßnahmen sollte ein Papier zur IT-Sicherheitspolitik erstellt werden, welches im Unternehmen publiziert wird und zur Schulung und Motivation der Mitarbeiter Verwendung findet. Es ist die Aufgabe des IT-Sicherheitsbeauftragten die Aktualität der IT-Sicherheitspolitik zu prüfen und diese gegebenenfalls zu ergänzen. Zur Erleichterung der Durchsetzung der beschriebenen Maßnahmen und Ziele sollte die IT-Sicherheitspolitik von der Geschäftsführung direkt verabschiedet werden.

Der hier vorgestellte und beispielhaft demonstrierte Ansatz ist pragmatischer Natur und hat sich in verschiedenen Projekten bewährt. Ziel ist es nicht ein abstraktes Papier zu verabschieden, welches zur Erhöhung der IT-Sicherheit nur wenig beiträgt. Vielmehr sollte die IT-Sicherheitspolitik sowohl vom Management als auch von der Technik mitgetragen werden. Denn nur eine gelebte IT-Sicherheitspolitik ist eine gute Sicherheitspolitik.

Vorgehensweise bei der Erstellung einer unternehmensweiten IT-Sicherheitspolitik

Tabelle 2 Maßnahmen

	Physikalischer Schutz	Logischer Schutz	Organisatorischer Schutz
Niedriger Schaden	Kontrolle des Zugangs zum Gelände der Unternehmung durch den Werkschutz	Die gesamte IT-Infrastruktur der Unternehmung wird als eine Schutzzone definiert Einsatz einer schwachen Authentifikation für den erfolgreichen Zugriff auf IT Ressourcen Einsatz von Virenschutzmaßnahmen	Belehrung der Benutzer über den ordnungsgemäßen Umgang mit IT Ressourcen ....
Mittlerer Schaden	Bildung von physikalischen Schutzzonen Zugangskontrolle für diese Schutzzonen mittels eines schwachen Authentifizierungsverfahrens	Bildung von logischen Schutzzonen Zugangskontrollen für diese Schutzzonen mittels Sicherheitsschleusen Definition von Benutzergruppen auf der Basis von Arbeitsbereichen Protokollierung von Zugriffsrechtsverletzung	Einrichtung der Position eines IT-Security-Officers als Verantwortlichem für den unternehmensweiten IT-Sicherheitsprozess Belehrung der Benutzer über den Umgang mit sensitiven IT Ressourcen Regelmäßige Revision ....
Hoher Schaden	Definition von Sicherheitsbereichen Zugangskontrolle zu diesen Sicherheitsbereichen durch eine starke Authentifizierung Absicherung dieser Sicherheitsbereiche durch eine Videoüberwachung und Alarmierungssysteme	Protokollierung von allen Zugriffen auf die IT Ressourcen Authentifizierung dieser Benutzergruppen durch eine starke Authentifizierung Verwendung von Verschlüsselungsverfahren zum Schutz der gespeicherten Daten ...	Definition von Arbeitsaufgaben und den zugeordneten Benutzergruppen Definition eines für die Sicherheit der jeweiligen Sicherheitszone Verantwortlichen Regelmäßige Katastrophenübungen ....

Neues Seminar

Optimale LAN-Anbindung von Servern, Server-Farmen und Speicher-Systemen

Vom 22. bis 24. April 2002 veranstaltet die ComConsult Akademie in Bonner Hilton Hotel zum ersten Mal ihr neues Seminar "Optimale LAN-Anbindung von Servern, Server-Farmen und Speicher-Systemen".

Zum Thema

Server-Systeme und Speicher-Technologien ändern sich in ihrer Bedeutung fürs Unternehmen massiv:

- immer mehr Benutzer pro Server
- immer leistungsstärkere Server
- zunehmender Grad an Zentralisierung
- neue und hoch-wirtschaftliche Formen von Speichern

Dies hat mindestens drei gravierende Konsequenzen:

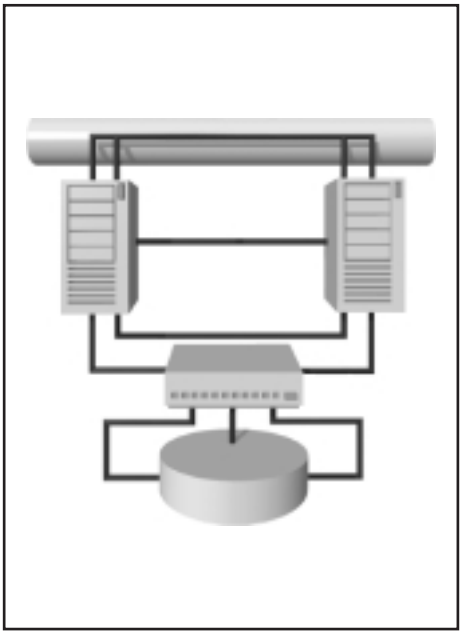
- Netzwerk, Server und Speicher wachsen zu einer architektonischen Einheit zusammen
- Die Anforderungen an Verfügbarkeit steigen
- Die Anforderungen an Betriebsfunktionalität und Gestaltbarkeit steigen

Tatsache ist, dass einerseits die Microsoft-Betriebssysteme Windows NT, Windows 2000 und künftig Windows XP eine zum Teil dominierende Präsenz in den Rechenzentren der meisten Firmen behaupten und andererseits immer wichtigere Arbeitsprozesse von der Verfügbarkeit dieser Serversysteme abhängig gemacht werden. Parallel werden neue Speicher-Technologien in immer höherer Zahl in den Unternehmen installiert.

Das Seminar richtet sich an Planer, Betreiber und Anwender von hochverfügbaren Server- und Speicherlösungen und deren Netzanbindungen sowie die Planer und Betreiber der umgebenden Netzwerke. Das Seminar diskutiert die bestehenden Alternativen in der Anbindung von Servern und Speicher an Netzwerke. Denkbare Architekturen werden speziell unter dem Blickwinkel Performance, Verfügbarkeit und Betrieb gegenüber gestellt und bewertet. Vor- und Nachteile der einzelnen Lösungsansätze werden aus der Sicht der Praxis diskutiert.

Das Seminar gibt Antworten auf die folgenden Fragen:

- Welche Alternativen bieten sich bei der Anbindung von Servern und Speicher-Systemen an Lokale Netzwerke? Welche Netzwerk-Technologie wird dabei vorausgesetzt?
- In welcher Form können Netzwerk-, Server und Speicher-Architekturen integriert werden? Welches Netzwerk-Design sollte gewählt werden? Ist eine Layer-2- oder eine Layer-3-Anbindung zu bevorzugen?
- Wie werden Windows Server Cluster aufgebaut und wie sollte die Netzanbindung aussehen?
- Wie Redundanzmechanismen funktionieren, welche Vor- und Nachteile die einzelnen Redundanzverfahren haben
- Welche DNS-Strukturen bei der Anbindung von Servern aufgebaut werden müssen, welche zusätzlichen Möglichkeiten DNS bietet
- Welche Rolle hochverfügbare Speicher-Technologien spielen
- Wie Storage Area Networks und Network Attached Storage-Lösungen aufgebaut werden
- Wie die Integration von Storage- und IP-Strukturen aussehen kann
- Was hinter IP Storage steckt
- Was bedeutet Mainframe-Integration in TCP/IP?
- Welche Lösungsmöglichkeiten bestehen für die ausfallsichere Anbindung von Servern auf der Basis der Betriebssysteme AIX, HP-UX und Solaris?
- Welche besonderen Eigenarten von TCP/IP müssen berücksichtigt werden?
- Wie sieht die Markt- und Produkt-Situation aus?
- Welche technischen Risiken bestehen? Welche typischen Fehler werden gemacht? Wie können Risiken und Fehler vermieden werden?
- Wie können Layer-4/7-Switching bzw. Content Networking beim Aufbau ausfallsicherer Serverfarmen angewandt werden?
- Was ist unter Web Switches zu verstehen und wie werden ausfallsichere und performante Intranets aufgebaut?



Die ersten beiden Tage des Seminars referiert Dr. Behrooz Moayeri während Dipl.-Ing Roland Moos den dritten Tag bestreitet.

Dr. Behrooz Moayeri ist Mitglied der Geschäftsleitung der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrungen zurück. In den letzten Jahren hat Dr. Moayeri zahlreiche führende deutsche Unternehmen bei der Migration von SNA und Token Ring u IP und Ethernet erfolgreich beraten.

Dipl.-Ing. Roland Moos hat in über 10 Jahren Berufspraxis bei verschiedenen Carriern umfassende Kenntnisse in der Sprach- und Datenkommunikation erworben. Heute arbeitet er als Senior-Trainer bei der ComConsult Akademie und im Produktforschungsbereich der ComConsult Technologie Information.

Optimale LAN-Anbindung von Servern, Server-Farmen und Speicher-Systemen

Optimale LAN-Anbindung von Servern, Server-Farmen und Speicher-Systemen – Der Inhalt

1. Tag

Empfohlene Netzstrukturen für Serverfarmen

Netzanbindung hochverfügbarer Serversysteme
- Layer-2 vs. Layer-3-Anbindung
- Redundanzmechanismen

Namensauflösung bei der Anbindung hochverfügbarer Systeme
- NetBIOS-Namensauflösung
- Unterschiede zwischen Windows NT und Windows 2000
- Geht es auch völlig ohne NetBIOS?
- DNS-Strukturen: statische und dynamische Konzepte
- Dynamic DNS Updates und Secure Dynamic DNS Updates

Redundanzkonzepte der Netzadapterhersteller

2. Tag

Netzanbindung von AIX-, HP-UX- und Solaris-Cluster-Systemen

Server Load Balancing

WLBS
Windows Cluster und Windows Loadbalancing Service

Netz-Design zur OS/390-Mainframe-Anbindung über TCP/IP

Alternativen für den physikalischen Netzzugang von OS/390-Mainframes
(der OSA-Express-Adapter, Cisco CIP)

Content Networking für Web Server

3. Tag

Ausfallsichere Datenhaltung

RAID-Konzepte

Parallele und serielle SCSI-Architekturen

SAN und NAS
Storage Area Network und Network Attached Storage
- Aufbau
- Technik
- Backuplösungen

IP Storage und was dahinter steckt

Konvergenz zwischen IP und SAN

iSCSI, FCIP, iFCP

Ausfallsicherheitskonzepte der SAN-/NAS-Hersteller

Der Veranstalter behält sich Änderungen im Programm vor.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Optimale LAN-Anbindung von Servern, Server-Farmen und Speicher-Systemen

Ich melde mich an für das Seminar
Optimale LAN-Anbindung von Servern, Server-Farmen und Speicher-Systemen
☐ vom 22. - 24.04.02 Bonn
☐ vom 09. - 11.07.02 Bonn
☐ vom 18. - 20.11.02 Bonn
zum Preis von € 1.590,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Hilton Bonn

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

ComConsult Certified Network Engineer

"Das Wissen erleichtert einem die Arbeit"

Oliver Zapp (28) arbeitet bei der Inducad GmbH. Der Insider sprach mit ihm nach seiner Prüfung zum ComConsult Certified Network Engineer.

Insider: Welche Ausbildung haben Sie?

Oliver Zapp: Ich bin Fachinformatiker für Systemintegration. Ich habe zuerst noch ein halbes Jahr im öffentlichen Dienst gearbeitet und weil es da langweilig war und das Vorankommen begrenzt war, hab ich dann zu Inducad in Kelkheim gewechselt.

Insider: Und was machen Sie da?

Oliver Zapp: Die Inducad GmbH ist eine Systemberatungsgesellschaft. Zur Zeit bin ich für die Betreuung unserer Mittelstandskunden zuständig. Erweitert wird das Aufgabengebiet mit SLAs und Projektmanagement.

Insider: Sind Sie in einem größeren Team?

Oliver Zapp: Zur Zeit bin ich alleine in meinem Bereich tätig. Der Bereich befindet sich noch im Aufbau, es ist angedacht, weitere Personen einzustellen.

ComConsult Certified Network Engineer Oliver Zapp

Insider: Wieso haben Sie den CCNE machen wollen?

Oliver Zapp: Angeboten wurde uns die Ausbildung von unserem Chef. Der wollte auch was in der Hand haben unseren Kunden gegenüber, damit er sagen kann "unsere Leute wissen, wovon sie reden".

Insider: Wie ist die Ausbildung dann abgelaufen?

Oliver Zapp: Angefangen habe ich letztes Jahr. Der Kurs "Lokale Netze für Einsteiger" mit Dr. Suppan hat mir am besten gefallen. Aber auch die anderen Seminare waren sehr lehrreich. Ich bin zufrieden. Wenn ich jetzt eine Arbeit erledige, weiß ich jetzt bewusst, warum ich das mache, was dahinter steckt. Vorher hab ich es einfach gemacht, ohne das richtige Wissen zu haben. Das Wissen erleichtert einem die Arbeit und das Tätigkeitsfeld erweitert sich.

Insider: Welche Bedeutung hat das Zertifikat für Sie?

Zapp: Weiß ich noch nicht. Das werden wir sehen.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Lokale Netze für Einsteiger, 18. - 22.03.02 in Aachen

Das Intensiv-Seminar vermittelt die grundsätzliche Funktionsweise, das Leistungsspektrum, aber auch die Defizitbereiche Lokaler Netze. Es bietet ein solides Fundament für den erfolgreichen Einstieg in den Netzwerk-Alltag.
Referenten: Dipl.-Ing. Roland Moos und Dr. Jürgen Suppan (ComConsult Akademie) Preis: € 1.990,-- zzgl. MwSt.

EMV in Anlagen und Systemen, 21. - 22.03.02 in Bonn

Das Seminar stellt das GHMT-Fünf-Säulen-Modell zur Planung der elektromagnetischen Verträglichkeit in Neubau- und- Umbauprojekten vor und zeigt geeignete Maßnahmen zur Umsetzung in der Praxis auf.
Referent: Dipl.-Ing. Dirk Wilhelm (GHMT) Preis: € 1.290,-- zzgl. MwS

Redundanzverfahren und Design-Konzepte von LANs, 08. - 09.04.02 in Bonn

Das Seminar befasst sich mit dem Aufbau neuer/Redesign bestehender Netzwerke und vermittelt, wie unter Nutzung der neuesten Redundanz- und Switching-Verfahren ein LAN optimal gestaltet werden kann und wie dabei die Anforderungen moderner Server- und Speicher-Systeme auch im Sinne von Verfügbarkeit, Loadbalancing und Verkehrsoptimierung architektonisch integriert werden können.
Referentin: Dipl.-Inform. Petra Borowka Preis: € 1.590,-- zzgl. MwSt.

DNS-/IP-Design für Windows 2000 Active Directory, 08. - 10.04.02 in Bonn

Dieses Seminar behandelt in konzentrierter Form die Implementierungsgrundlagen aus dem IP-Bereich für Windows 2000 bzw. für das Active Directory. Dabei spielt DNS die Hauptrolle, wobei auch insbesondere die dynamische Verbindung zum DHCP betrachtet wird.
Referenten: Markus Holländer, Lars Kuhl, Michael van Laak, Frank Neunzig Preis: € 1.590,-- zzgl. MwSt.

IP-VPNs erfolgreich einsetzen, 08. - 10.04.02 in Bonn

Das Seminar beschäftigt sich mit dem Home-Office-/Teleworker-Zugang, dem Unternehmens-WAN-Backbone, dem Filialnetzwerk und der Standort-Kopplung, denn VPNs stellen die wichtigste Weiterentwicklung im Bereich der Weitverkehrskommunikation dar.
Referenten: Dipl.-Inform. Andreas Meder, Dr. Behrooz Moayeri (ComConsult Beratung und Planung) Preis: EUR 1.590,--- zzgl. MwSt.

Cisco-Router erfolgreich einsetzen, 08. - 12.04.02 in Aachen

Das Seminar lehrt den Aufbau und die Arbeitsweise von Cisco-Routern an Cisco 2600 Routern, an denen die Teilnehmer aktiv arbeiten können.
Referent: Markus Schaub (ComConsult Akademie) Preis: € 2.590,-- zzgl. MwSt.

Neue Ethernet-Technologien, 08. - 12.04.02 in Aachen

Das Intensiv-Seminar beschäftigt sich mit dem Ausbau bzw. Umbau dieser Netze in Richtung Fast Ethernet und Frame Switching für alle Betreiber traditioneller Ethernet-Netzwerke. Referenten: Dipl.-Inform Oliver Flüs, Dipl.-Inform. Andreas Meder, Dipl.-Ing. Hartmut Kell, Dipl.-Ing. Harald Krause, Dr. Joachim Wetzlar (ComConsult Beratung und Planung) Preis: € 1.990,--zzgl. MwSt.

Exchange 2000 Server, Active Directory und Backoffice, 15. - 17.04.02 in München

Das Seminar befasst sich mit der Implemen-tierung von Exchange 2000 Server im Kontext des Windows 2000 - Active Directory Designs. Es werden Grundkenntnisse über Active Directory und Messaging vorausgesetzt.
Referenten: Hans-Willi Kremer (ComConsult Beratung und Planung) Preis: € 1.590,-- zzgl. MwSt.

Schirmung, Erdung, Potentialausgleich..., 15. - 16.04.02 in Bonn

Das Seminar behandelt die scheinbar unerklärbaren Störerscheinungen in Netzwerken und im Betrieb elektronischer Geräte, die durch Wechselwirkungen mit der Elektroinstallation entstehen.
Referenten: Dipl.-Ing. Karl-Heinz Otto und Hans-Günter Hergesell Preis: € 990,-- zzgl. MwSt.

Fast ausgebucht – Nur noch wenige Plätze:

Netzwerk-Redesign Forum 2002, 15. - 18.04.02 in Königswinter

Die Themen: Kosten Lokaler Netzwerke bis zu 50 % senken; Wo steht der Netzwerk-Markt? Netzwerk Architekturen im Wandel; Ethernet Überall; Verkabelung im Umbruch; Wireless LANs; Home Networking; Service-Level Management und Accounting im Netzwerk; Speicher-Netzwerke und neue Server-Architekturen. Moderation: Dr. Jürgen Suppan und Dr. Franz-Joachim Kauffels

Preis mit Tutorium (15. - 18.04.): € 1.790,-- zzgl. MwSt.
Preis ohne Tutorium (16. - 18.04.): € 1.590,-- zzgl. MwSt.

Lokale Netze für Einsteiger, 15. - 19.04.02 in Aachen

Das Intensiv-Seminar vermittelt die grundsätzliche Funktionsweise, das Leistungsspektrum, aber auch die Defizitbereiche Lokaler Netze. Es bietet ein solides Fundament für den erfolgreichen Einstieg in den Netzwerk-Alltag.
Referenten: Dipl.-Ing. Roland Moos und Dr. Jürgen Suppan (ComConsult Akademie) Preis: € 1.990,-- zzgl. MwSt.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Fehlersuche in lokalen Netzen für Einsteiger, 22. - 24.04.02 in Aachen

Das Praxis-Seminar stellt wesentliche Hilfsmittel für die Netzwerk-Überwachung und Fehlersuche über Vorträge und Übungen vor, typische Problemsituationen werden simuliert und systematisch deren Beseitigung erarbeeitet.
Referenten: 8 Mitarbeiter der ComConsult Beratung und Planung GmbH Preis: € 1.790,-- zzgl. MwSt.

Service Level Management Forum 2002, 22. - 26.04.02 in Düsseldorf

Die Themen: Technische Lösungsansätze für SLM; Infrastrukturen für SLM; Organisatorische Rahmenbedingungen für SLM; Unternehmens-Konzepte für SLM; Erfolgreiche Umsetzung von SLAs in der dezentralen Welt; Integration einer SLM-Lösung in eine bestehende System-Management-Lösung; Markt- und Produkt-Situation: Wer leistet was, wo stehen die traditionellen Produkte? Projekterfahrungen
Moderation: Dr. Jürgen Suppan (ComConsult Akademie) Preis: € 1.590,-- zzgl. MwSt.

Internetworking, 22. - 26.04.02 in Aachen

Das Seminar vermittelt die technischen und methodischen Kenntnisse zur erfolgreichen Strukturierung von Netzwerken mit Switching und Routing wobei Grundlagen-Kenntnisse Lokaler Netzwerk-Technologien erforderlich sind.
Referentin: Dipl.-Inform. Petra Borowka Preis: € 1.990,-- zzgl. MwSt.

TCP/IP und SNMP, 22. - 26.04.02 in Berlin

Das Intensiv-Seminar vermittelt einen praxis-orientierten Einblick in den Aufbau und den Betrieb von heterogenen Netzen, die den Kommunikationsstandard TCP/IP und den Netzmanagement-Standard SNMP benutzen.
Referent: Mathias Hein Preis: € 1.990,-- zzgl. MwSt.

Optimale LAN-Anbindung von Servern, ... 22. - 24.04.02 in Bonn

Das Seminar diskutiert die bestehenden Alternativen in der Anbindung von von Servern, Server-Farmen und Speicher-Systemen an Netzwerke. Denkbare Architekturen werden unter dem Blickwinkel Performance, Verfügbarkeit und Betrieb gegenüber gestellt und bewertet.
Referenten: Dr. Behrooz Moayeri, Dipl.-Ing. Roland Moos (ComConsult Akademie) Preis: € 1.590,-- zzgl. MwSt.

Wireless LAN: Technik, Planung und Betrieb 14. - 16.05.02 Bonn

Das 3-tägige Seminar beschäftigt sich mit Planung, Konfiguration und Betrieb von sicheren WLAN nach IEEE 802.11b, ergänzt und vertieft durch praktische Beispiele und Demonstrationen.
Referenten: Dr. Simon Hoff, Peter Mohn, Dr. Jochen Wetzlar (ComConsult Planung und Beratung) Preis: € 1.590,-- zzgl. MwSt.

Service Level Management in der Praxis 15. - 17.05.02 in Bonn

Das Seminar behandelt die Königsdisziplin des Netzwerk- und System-Managements: Service Level Management, wo die technischen und organisatorischen Fäden einer IT-Organisation zusammenlaufen und die zentrale Schnittstelle zwischen Betreibern und Anwendern innerhalb einer Firma oder zwischen externen Dienstleistern und Anwendern liegt.
Referenten: Martin Rother, Dr. Justus Meier (arxes NCC AG) Preis: € 1.590,-- zzgl. MwSt.

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

Titel des Seminars	Name	Vorname
Termin	Firma, Abteilung	Position, Funktion
☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel	Straße	PLZ, Ort
Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**	Telefon	Fax
	eMail	Unterschrift

Thema

Gebrauchte Netzwerkkomponenten

Die Spielregeln

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen. Die Spielregeln: Sie melden uns ihr Angebot oder Gesuch per Mail, mit dem Fax-Formular (unten) oder über den Web-Server. Wir veröffentlichen es unter einer Anzeigen-Nr. im Insider und auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her. Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Gebote

Adapter

BayNetworks Token-Ring-Hubs, Anzahl auf Anfrage, Preis auf Anfrage, verschieden Token-Ring-Hubs, BayStack, teilweise gemanaged. Anzeigen-Nr. B20205

Allied Telesyn , Anzahl auf Anfrage, Preis auf Anfrage, verschiedene 10-MBit/s-Hubs. Anzeigen-Nr. B20207

Hischmann 10-MBit/s-Hubs, Anzahl auf Anfrage, Preis auf Anfrage, verschiedene 10-MBit/s-Hubs, ASGE, inkl. diverser Module. Anzeigen-Nr. B20208

RAD Token-Ring-Hubs, Anzahl auf Anfrage, Preis auf Anfrage, verschiedene Token-Ring-Hubs/Teile, RAD-Ring, inkl. diverser Module. Anzeigen-Nr. B20206

Olicom ATM Fiber Adapter OC-6162-0010, Anzahl 28, Preis Euro 330,-, Fiber ATM Adpater, SC Anschluss, unbenutzt, Anzeigen-Nr. B20127

Hub

Bay Distributed 5000, Anzahl 10, Preis Gebot, 10 Stck. Rack 5000D, 6 Stk. MGT. Karte 5DN310, 20 Stk. 24xRJ45 Karte 308P, 7 Stk. 3x10Mbps FO Karte 304P, 1 Stk. 6xRJ45+1xFO Karte 378P-F, 3Stk. Stacking Kabel, Anzeigen-Nr. B20124

DEC-Hub, Anzahl 1, Preis VB , DEC-Hub 900 mit FDDI und Ethernet Modulen, LWL und Kupfer, Anzeigen-Nr. B20125

Gebote

Repeater

Alcatel Ethernet-Repeater, Anzahl auf Anfrage, Preis auf Anfrage, verschiedene Ethernet-Repeater, FibreCON, 10 und 100 MBit/s. Anzeigen-Nr. B20210

Router

Cisco Router 3600, Anzahl auf Anfrage, Preis auf Anfrage. Anzeigen-Nr. B20211

Switch/Brücke

Cabletron/Enterasys MMAC-M8FNB Chassis und Module, Anzahl 1 Stck., Preis VB sehr günstig, 1 x Chassis inkl. PS, 1 x EMM-E6, 5 x ESXMIM, 1 x ESXMIM-F2, 7 x BRIM-F6, Anzeigen-Nr. B20213

Cabletron/Enterasys 2E42.27R und ESX-1380, Anzahl je 1 Stck., Preis VB sehr günstig. Anzeigen-Nr. B20214

Cisco Catalyst 5000, Anzahl auf Anfrage, Preis auf Anfrage, verschiedene Switches/Teile, inkl. 10 MBit/s-Switching-Module. Anzeigen-Nr. B20202

BayStack 450-1SR-MDA, Anzahl auf Anfrage, Preis auf Anfrage ,stackable Switch. Anzeigen-Nr. B20209

BayNetworks Centilllion 100, Anzahl auf Anfrage, Preis auf Anfrage, verschiedene Switches/Teile, inkl. ATM-, Token- und Ethernet-Speed-Module. Anzeigen-Nr. B20203

Cabletron/Enterasys Div. SmartSwitch 9000 Module, Anzahl 11 Stck., Preis VB, div. Switch Module Ethernet und Fast Ethernet CU und FO. Alle Module 4. Generation 9E4xxx und 9H4xxx sowie PS. Anzeigen-Nr. B20212

BayNetworks System 5000, Anzahl auf Anfrage, Preis auf Anfrage,verschiedene Switches/Teile, inkl. ATM-, Token-Ring und Ethernet-Net-Module. Anzeigen-Nr. B20204

Bay Diverse, Anzahl 2, Preis Gebot , 1 Bay Stack 28200 mit 2x 28200-14 8xFO und 2x 28200-15 8xRJ45, 1 Bay Stack 304 12 und 1xRJ45, Anzeigen-Nr. B20123

Sonstige

Allied Telesyn Fast Ethernet Convertor MG 101XL 100 Base-Fx/100Base-Tx, Anzahl 2, Preis EUR 100,-- /Stck., Anzeigen-Nr. B20126

3Com und SK FDDI-Netzwerkkarten, Anzahl 8, Preis VB, Anzeigen-Nr. B20119

Lex Mark 4033-001 Druckerboxen, Anzahl 15, Preis FR. 200,--, Anzeigen-Nr. B20118

Gesuche

Sonstige

Madge Networks 57-35, Anzahl 1, Preis Erbitte Angebot , Madge 57-35 Collage 752, 5-port 155 Module SMF. Gerne gebraucht mit mindestens 30 Tagen Garantie. Anzeigen-Nr. S20103

Madge Networks 57-80, Anzahl 1, Preis Erbitte Angebot , Madge 57-80 Collage 765, 4-port 155 SMF/MMF. Gerne gebraucht mit mindestens 30 Tagen Garantie. Anzeigen-Nr. S20104

Madge Networks/Olicom OC-8660 0010, Anzahl 4, Preis Erbitte Angebot , Olicom OC-8660 0010 Translational Switxh UEM, Anzeigen-Nr. S20109

Netzwerk-Server gegen Spendenquittung, Anzeigen-Nr. S20120

TP Ethernet Cat 5 Kabel über 400Meter gegen Spendenquittung, Anzeigen-Nr. S20121

Switch/Brücke, Anzahl 5, gegen Spendenquittung, Anzeigen-Nr. S20122

Fax an ComConsult 02408/955-399

☐ **Ich suche**
☐ **Ich biete**
☐ **Antwort auf Anzeigen-Nr.** ☐ ☐☐☐☐

Produkt/Komponente/Release/Software

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon

Fax

eMail