ComConsult Technologie Information

Der Netzwerk Insider

Januar 2000

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

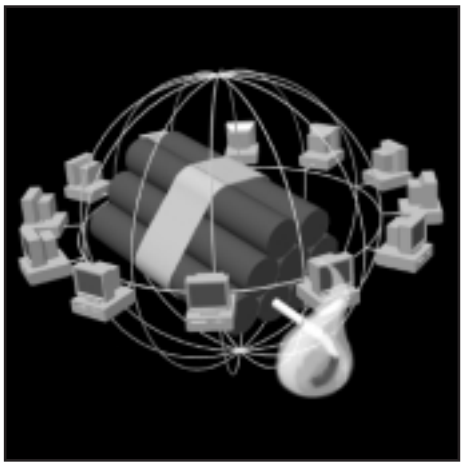
Schwerpunktthema

IT-Sicherheit – Der Schlüssel zum erfolgreichen E-Business

von Dipl.-Inform. Detlef Weidenhammer

Die allgemeine Internet-Euphorie bringt neben vielen Übertreibungen auch absehbar umwälzende Entwicklungen hervor. Hierzu gehört insbesondere die Abwicklung geschäftlicher Aktivitäten aller Art über das "Netz der Netze". Als größtes Hindernis für die weitere Ausbreitung werden aber immer noch die damit verbundenen Sicherheitsrisiken angesehen.

Obwohl nun auch die Internet-Nutzung durch Unternehmen aller Art schon seit mehreren Jahren geübte Praxis ist, sind die kritisch betrachteten Themen noch immer die gleichen. Neben den üblichen Klagen zur (schwachen) Performance entwickelt sich auch das Thema IT-Sicherheit immer mehr zu einem Dauerbrenner.



Sicherheitsrisiken durchs Internet

Ging es in den ersten Jahren, und natürlich auch heute noch bei Neueinsteigern in erster Linie um die Absicherung der Netzgrenzen (Perimeter-Schutz), so sehen sich die meisten Unternehmen heute neuen Problemen gegenüber. Die zunehmende Öffnung durch Erweiterung der Kommunikation mit Geschäftspartnern und Serviceunternehmen im Rahmen einer Business-to-Business Beziehung (B2B) bringt neben großen Vorteilen auch erhebliche Sicherheitsprobleme.

Sind hierbei zumeist die Partner bekannt und lassen sich in eine übergreifende Sicherheitskonzeption einbeziehen, so ist ein Aufbau von Kundenbeziehungen und -geschäften (Business-to-Customer) über das Internet noch kritischer zu sehen.

weiter auf Seite 6

Zum Geleit

Gigabit-Ethernet über Kupfer ist uninteressant!

Die Ankündigungen zu Gigabit-Ethernet überschlagen sich. 3Com kündigt einen neuen Switch und Uplink-Einschübe für die bestehenden an, Alteon kündigt eine Adapter-Karte für 1000 Base-T zum Preis von 500 US-Dollar an, nahezu alle Hersteller von Adapterkarten wollen bis Mitte 2000 mit neuen Produkten für 1000 Base-T auf dem Markt sein. Der Tenor ist einhellig und wird dankbar von allen aufgegriffen: Twisted Pair reduziert den Preis von Gigabit-Ethernet gegenüber einer Glasfaser-Lösung um 50%. Es muss festgestellt und deutlich herausgestellt werden, dass diese Botschaft kompletter Unsinn ist und den Entscheider in eine gefährliche Richtung führen kann.

Es ist die falsche Antwort auf eine richtige Frage.

Die Frage heißt: Welche Netzwerk-Infrastrukturen braucht ein Unternehmen, um für die Zukunft gerüstet zu sein?

Eine Unterfrage ist: Welchen Stellenwert hat Gigabit-Ethernet dabei?

Auf jeden Fall ist es zweitrangig, den scheinbar niedrigsten Port-Preis für Gigabit zu bezahlen. Außerdem ist die Botschaft gelogen. Wer Gigabit-Ports durch einen niedrigen Portpreis in großer Stückzahl einführt, der benötigt auch ein Backbone-Netz und eine Gesamtinfrastruktur, die diese Datenströme tragen kann. Diese Gesamt-Infrastruktur wird mit Redundanzmechanismen zu versehen sein, die Frage nach Layer-2 kontra Layer-3-Switching beantworten müssen. Betrachtet man die damit verbundenen Kosten, so stellt man schnell fest, dass von dem Low-Cost-Sonderangebot für 500 US-Dollar nicht viel übrig bleibt (mal abgesehen davon, dass Nortel bereits seit Monaten einen LWL-NIC zum selben Preis anbietet).

Kommen wir zurück zur Kern-Frage, welche Infrastrukturen ein Unternehmen benötigt, um für die Zukunft gerüstet zu sein.

weiter auf Seite 2

Gigabit-Ethernet über Kupfer ist uninteressant!

Fotsetzung von Seite 1

Es muss in der Planung und im Design mindestens eine Antwort auf folgende Fragen geben:

- Wie verfügbar soll das Netzwerk an welcher Stelle sein?
- Welche Laufzeiten im Gesamtnetzwerk werden angestrebt?
- Wie soll Skalierbarkeit von Leistung und Qualität realisiert werden?
- Werden hochgradig interaktive Anwendungen (Ping-Pong-Applikationen) im Netzwerk betrieben?
- Soll ein Hochleistungs-Cluster eingebunden werden?

Impressum

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

Telefon 02408/14907
Telefax 02408/149233

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

- Soll eine hochskalierbare und ausfallsichere Web-Hosting Lösung geschaffen werden?
- Wird innerhalb der nächsten 4 Jahre eine Voice-over-IP-Lösung angestrebt, um die vorhandene Nebenstellenanlage stufenweise durch eine Netzwerk-basierte Lösung zu ersetzen?
- Soll zukünftig eine Video-Konferenz-Lösung zum Einsatz kommen?
- Wie sicher muss das Netzwerk-Design gegenüber Fehlkonfigurationen am Endgerät sein (IP-Adresse des R3-Servers usw.)?
- Wie hoch soll der angestrebte Betriebsaufwand sein, wie qualifiziert ist das Betriebspersonal, wer führt die meisten Changes aus, was ist dafür an Kenntnissen erforderlich?

Die Antwort wird in vielen Fällen im Bereich der ausgewählten Technologie ein Backbone-Netzwerk mit Gigabit-Technologie sein. Die bisherigen Projekt- und Betriebserfahrungen von ComConsult belegen: dies ist hochgradig rentabel und erfolgreich.

Aber natürlich müssen eine Reihe von Fragen beantwortet werden:

- Welcher Redundanz-Mechanismus wird eingesetzt: Link-Aggregation, Spanning, Tree, OSPF, EIGRP, HSRP, VRRP?
- Welche Verfahren werden eingesetzt, um die neuen Sprach- und Video-Anwendungen zu unterstützen (Beispiel: Multicast-Steuerung)?
- Soll skalierbares Web-Hosting mit Layer-4/7-Switching eingesetzt werden?

Nehmen wir das Beispiel Voice-over-IP. Neben den diversen damit verbundenen Fragen sind die simplen Frage zu beantworten:

- Woher kommt die Stromversorgung des Telefons? Vom Switch? Dann ist für diesen Switch diese Eigenschaft viel wichtiger als 1000 Base-T.
- Wie komme ich an eine zusätzliche Anschlussdose, wenn jedes Telefon, jedes Fax-Gerät jetzt einen Ethernet-Anschluss benötigt, aber nach der Regel 1,5 bis 2 Anschlüsse pro Arbeitsplatz geplant worden ist und bereits ein PC und ein Drucker angeschlossen sind?
- Welche Port-Dichten müssen entsprechende Switch-Systeme aufweisen?
- Mit welchen Mechanismen stelle ich die notwendige Verfügbarkeit am Endgerät her? Bisherige Netzwerk-Designs planen Verfügbarkeit überwiegend im Backbone, seit einigen Monaten sind redundante Server-Anschlüsse im Kommen, was aber bedeutet Verfügbarkeit von Datennetzen im Umfeld von Voice-over-IP?

An dieser Stelle soll kein Grundsatzartikel über Netzwerk-Design stehen. Dies ist ein Geleitwort, dass meine subjektive Einschätzung von Markt- und Technologie-Entwicklungen wiedergibt. Trotzdem belegen die vielen dargestellten Fragen m.E., dass es wichtigere Fragen zu beantworten gilt als die Frage, ob ich Gigabit mit Twisted Pair mache oder nicht. Mal ganz abgesehen davon, dass auch im Glasfaser-Bereich erhebliche Preisreduktionen zu erwarten sind und die bisherigen Twisted Pair Chips noch erhebliche Abwäre generieren. Ich habe nichts gegen 1000-Base-T, doch die Frage, ob diese Technik für den Markt zum jetzigen Zeitpunkt wirklich wichtig ist, muss mit einem klaren Nein beantwortet werden. Der Gigabit-Zug rollt so oder so, ein modernes Netzwerk-Design ohne Gigabit ist eine klare Fehlentscheidung. Ob mit oder ohne Twisted Pair ist, solange es nicht vorrangig um den Anschluss von Endgeräten mit Gigabit geht, unwichtig. Und unsere Endgeräte - unser Dank gilt den jeweiligen Herstellern - können auf Grund ihres Hardware-Architektur / Betriebssystem-bedingten Kommunikations-Brems-Designs vorläufig nichts mit Gigabit anfangen. Lassen Sie uns auf die wirklich wichtigen Fragen konzentrieren. Diese sind kompliziert genug. Wir werden dies in den nächsten Ausgaben des Insiders und natürlich auf unserem Netzwerk Redesign-Forum 2000 im April machen.

Ihr
Dr. Jürgen Suppan

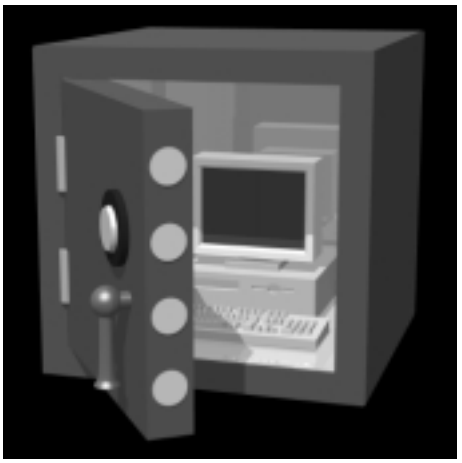
Sonder-Seminar

Sicherheit für Datenschutzbeauftragte und Revisoren

Das Sonder-Seminar "Sicherheit für Datenschutzbeauftragte" ist speziell auf die im Rahmen der Tätigkeit eines Datenschutzbeauftragten oder Revisoren auftretenden technischen Fragestellungen ausgerichtet, denn Datenschutzbeauftragte, Revisoren und Führungskräfte im IT Bereich werden heute mehr denn je mit technischen Details konfrontiert. Im Rahmen ihrer Tätigkeit müssen sie in der Lage sein technische und organisatorische Zusammenhänge zu beurteilen.

Der Referent Dipl.-Inform. Sven Schumann von der ComConsult Beratung und Planung GmbH besitzt als Berater für Netzwerk-Sicherheit und -Management mehrjährige Erfahrung und umfassende praktische Kenntnisse insbesondere auf den Gebieten Internet-Security und Verschlüsselung.

Das Seminar stellt die verschiedenen Teilgebiete der Datensicherheit vor und vermittelt den Teilnehmern ein technisches Grundverständnis über die Datensicherheit beim Einsatz von Personalcomputern. Im Rahmen der Veranstaltung wird Bezug auf das Betriebssystem Windows-NT genommen.



Sonder-Seminar: Maßnahmen für sicheren PC-Betrieb

Das vermittelte Verständnis über die technischen und organisatorischen Zusammenhänge in der Datensicherheit lässt sich auch auf andere Betriebssysteme anwenden.

Ziel ist es, sowohl dem Datenschutzbeauftragten als auch dem Revisor das für die tägliche Arbeit notwendige grundlegende technische Know-how zu vermitteln.

Die Teilnehmer lernen auf diesem Seminar welche Teilgebiete die Datensicherheit umfasst, wie der IT-Sicherheitsprozess im Unternehmen zu verankern ist, welche Grundlagen die Basis für die Sicherheit beim PC-Betrieb bilden und wodurch sie bedroht wird: Welche Angriffe möglich sind, wie schwerwiegend sie sein können und welche Risiken sich daraus ergeben.

Sie lernen Maßnahmen für einen sicheren PC-Betrieb kennen, z.B. welche Verschlüsselungsverfahren heute "State of the Art" sind, wie man sie einsetzt und wie Aufwendig ihr Einsatz ist. was für eine sichere Internetnutzungnotwendig ist und Richtlinien für einen ordnungsgemäßen PC-Betrieb.

Um das Seminar praxisbezogen abzurunden, bieten wir Ihnen eine kleine Vorführung von aktuellen "Hackertools" und/oder Sicherheitssoftware, um eine PC-Landschaft auf Schwachstellen in der Konzeption und Konfiguration zu überprüfen.

Fax-Antwort an ComConsult 02408/149233

Anmeldung Sonder-Seminar

☐ Ich buche das Sonder-Seminar
Sicherheit für Datenschutzbeauftragte
vom 21.02.-22.02.00 in Bonn
zum Preis von DM 2.480,-- (EUR 1.268,--)
zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Holiday Inn Crowne Plaza, Bonn
(Übernachtung/Frühstück DM 199,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/149233** oder schicken Sie eine eMail an **akademie@comconsult.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

Zusatz-Termin

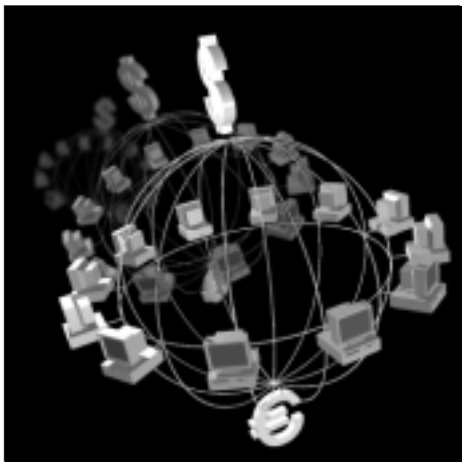
Internet und E-Business für Führungskräfte

Das Seminar "Internet und E-Business: Durchblick für Manager" findet in diesem Jahr zusätzlich am 20. - 21. März im Maritim Hotel in Bonn statt. Der Referent Dr. Franz-Joachim Kauffels ist einer der erfahrensten und bekanntesten Referenten der geasamten Netzwerkszene. Für die kommenden Jahre stellt er folgende lineare Prognose für die Zahl der deutschen Online-Benutzer auf:

2000: 16 - 17 Millionen
2001: 22 Millionen
2002: 27 Millionen

Damit sind die Technologien des Internet die größte Herausforderung seit Beginn der vernetzten Informationsverarbeitung. Riesige Chancen und enorme Risiken liegen eng beieinander. Im Zuge der Globalisierung können vor allem Schwellenländer und die neuerstarkten Tigerstaaten das Internet nutzen. Auch wenn E-Business hierzulande zuerst langsam angelaufen ist, der Durchbruch ist für viele Branchen weltweit erfolgt, wer weiter wartet, gefährdet möglicherweise sein Unternehmen. Kaum ein Wirtschaftszweig kann sich den modernen Marketingparadigmen und weiteren Möglichkeiten entziehen.

Teilnehmer, die in Unternehmen, Organisationen und Behörden zu Entscheidungen



E-Business: RiesigeWachstumsraten

beitragen, die die technologische und strategische Entwicklung im Übergang zum interaktiven Zeitalter beeinflussen, werden durch dieses Seminar in die Lage versetzt, die neuen Technologien kennen- und schätzen zu lernen. Techniken und Verfahren, Möglichkeiten und Gefahren, Kosten und Nutzen, Chancen und Risiken werden in kleinem Kreis diskutiert.

Lernen Sie die Antworten auf folgende Fragen kennen :

- Wie betrifft der Wandel zur Informationsgesellschaft mein Unternehmen?
- Welche Herausforderungen bedeutet das "Interaktive Zeitalter"?
- Wie kann ich Internet, Intranets und Extranets im Unternehmen einsetzen?
- Wie erhalte ich Wettbewerbsvorteile durch die Internet-Technologie?
- Wie bringe ich mein Unternehmen ins Internet?
- Welche Nutzungs- und Kommunikationsmöglichkeiten gibt es?
- Wie ändern sich die Marketing-Paradigmen durch das Internet?
- Wie nutze ich die modernen Möglichkeiten effizient?
- Internet und E-Business: Riesenchance für den Mittelstand?
- Wie wende ich Gefahren durch Internet-Technologien ab?
- Was ist die Rolle der großen Hersteller (Microsoft, IBM,...)?

Fax-Antwort an ComConsult 02408/149233

Anmeldung Internet und E-Business

☐ Ich melde mich an für das Seminar
Internet und E-Business: Durchblick für Manager
vom 20.03.-21.03.00 in Bonn
zum Preis von DM 2.480,-- (EUR 1.268,--) zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Hotel, Bonn
(Übernachtung/Frühstück DM 230,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/149233** oder schicken Sie eine eMail an **akademie@comconsult.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 _____

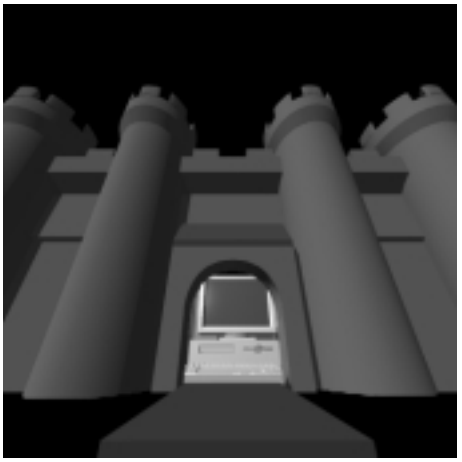
Netzwerk Sicherheits-Forum 2000

Das Security-Event im Jahr 2000

Vom 22.bis zum 24. Mai veranstaltet die ComConsult Akademie zusammen mit der GAI NetConsult im Maritim Königswinter das "Netzwerk Sicherheits-Forum 2000".

Sicherheitsrisiken für den Netzbetrieb haben in den letzten Monaten massiv zugenommen. Hochautomatisierte und öffentlich verfügbare Angriffstools ermöglichen immer mehr unerfahrenen Angreifern erfolgreiche interne und externe Angriffe.

Auch dieses Jahr wird den Teilnehmern mit dem Netzwerk Sicherheits-Forum ein herausragendes Event präsentiert, das für jeden Sicherheitsverantwortlichen und Netzwerkadmininstrator eine unverzichtbare Plattform für aktuelle Informationen, Produktvergleiche und Fachdiskussionen darstellt.



Öffnet seine Tore im Mai:
Das Sicherheits-Forum 2000

Das Forum geht auf die bestehenden Sicherheitsrisiken in modernen, heterogenen, offenen Netzwerken ein und konzentriert sich auf:

- Benennung praxisrelevanter Sicherheitsrisiken
- Methoden zur Vermeidung von Sicherheitsrisiken
- Praxiserprobte Ansätze zur Umsetzung von Sicherheitskonzepten
- Produkte und bestehende Einsatzerfahrungen.

Die Teilnehmer lernen nicht nur die Bedrohungen richtig einzuschätzen sondern erhalten auch Lösungsvorschläge und konkrete Produktempfehlungen.

Fax-Antwort an ComConsult 02408/149233

10 % Frühbucher-Rabatt bis zum 15.03.00

Netzwerk Sicherheits-Forum 2000

22.05. - 24.05.00 in Königswinter

Für Besucher der bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir in diesem Jahr exklusiv eine Frühbuchungsphase für das Netzwerk Sicherheits-Forum 2000 bis zum 15.03.00 für die rabattierte Teilnahmegebühr von DM 2.600,-- (EUR 1.329,36) für die Basis-Anmeldung und DM 2.980,-- (EUR 1.523,65) für die Bündel-Anmeldung (Sie erhalten zusätzlich den Technologie Report "Netzwerk Sicherheit: Konzepte, Produktauswahl, Realisierung") statt regulär DM 3.588,--. Die Buchung ist verbindlich, kann aber jederzeit auf andere Mitarbeiter Ihres Unternehmens übertragen werden.

Ich melde mich an für den Kongress
Netzwerk Sicherheits-Forum 2000
vom 22.05.-24.05.00 in Königswinter zu den unten angekreuzten Leistungen:

☐ **Basis-Anmeldung** zum Preis von DM 2.600,-- (EUR 1.329,36) zzgl. MwSt.

☐ **Bündel-Anmeldung** zum Preis von DM 2.980,-- (EUR 1.523,65) zzgl. MwSt.

Bitte buchen Sie für mich ein Zimmer im Maritim Hotel, Königswinter (Übernachtung/Frühstück DM 211,--)

Faxen Sie uns einfach diesen Abschnitt an **02408/149233** oder schicken Sie eine eMail an **akademie@comconsult.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

IT-Sicherheit – Der Schlüssel zum erfolgreichen E-Business

Fortsetzung von Seite 1

In einer unlängst erschienenen Studie des "Secure Computing Magazines" (www.check-mark.com/survey) zeigten die Ergebnisse einer weltweiten Befragung von Unternehmen zum Thema E-Business sehr deutlich die Defizite im Bereich der IT-Sicherheit auf. Diese decken sich nahezu mit unseren Erfahrungen aus mehrjähriger Praxis, wobei gerade beim Einsatz von neuartigen Sicherheitsmaßnahmen in Deutschland eher eine noch größere Zurückhaltung festzustellen ist.

Security Policy

Obwohl die Mehrheit der Unternehmen Policy und Konzeption aufzuweisen hatte, waren diese zumeist veraltet und deckten selten den gesamten in Frage kommenden Bereich ab. Besonders schlecht sah es im allgemeinen mit Schulungsmaßnahmen aus. Unter Berücksichtigung der häufig anzutreffenden Personalknappheit muss dies als ein zusätzlicher großer Unsicherheitsfaktor bewertet werden.

Schutzmaßnahmen

Am häufigsten eingesetzt werden Tools zur Zugriffskontrolle (71%) und zum Virenschutz (97%). Firewalls zur Netzsicherung setzten weniger als 2/3 der Befragten ein. Dies ist um so erstaunlicher, als die Gefahr von Hackerangriffen allgemein als sehr hoch empfunden wird. Verschlüsselung wird bei ca. 40% eingesetzt, wobei hier zumeist Unternehmen aus der Finanzbranche vertreten sind.

PKI

Obwohl bei den meisten Unternehmen als besonders wichtig angesehen, werden noch kaum Lösungen zur Bereitstellung von "Public Key Infrastructures" angegangen. Zumindest mehr als 40% haben dies jedoch in ihrer Planung für die nächsten 12 Monate. In Deutschland ist die Zahl vermutlich noch deutlich geringer anzusetzen.

Verfügbarkeit

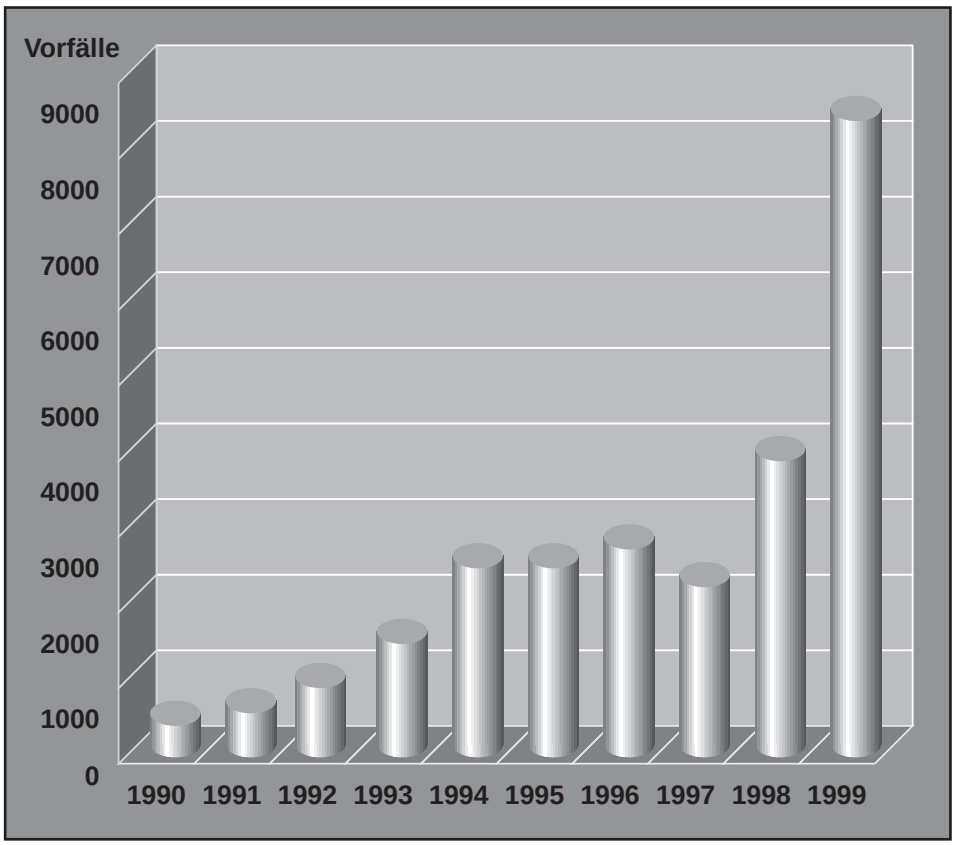
Immerhin 38% der Befragten setzen Maßnahmen zur erhöhten Verfügbarkeit ein. Dies bezieht sich jedoch meistens auf das Aufrechterhalten der Stromversorgung (USV) und weniger auf die 24x7 Sicherung aller E-Business Komponenten.

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.

Die Befragung nach Sicherheitsverletzungen ergab wie erwartet die größte Gefahr durch Vireninfektion (73%). Daneben wurden besonders auffällig: eMail-Attachments mit Nebenwirkungen (61%), eMail Spam (49%) und Stören der Netzverfügbarkeit (31%). Die zumeist gefürchteten Webattacken wurden in der Praxis nur bei 8% registriert. Weniger als 6% berichteten über Industriespionage oder das Verbreiten geheimer Informationen.

Man kann bei all diesen Befragungen von einer hohen Dunkelziffer ausgehen, denn wer gibt schon gerne zu, dass er auf Grund von unzureichenden Schutzmaßnahmen Opfer eines Angriffes geworden ist. Aufschluss zumindest über die ständig ansteigende Zahl von Sicherheitsverletzungen geben die Statistiken, die das CERT (Computer Emergency Response Team) in jedem Jahr veröffentlicht.

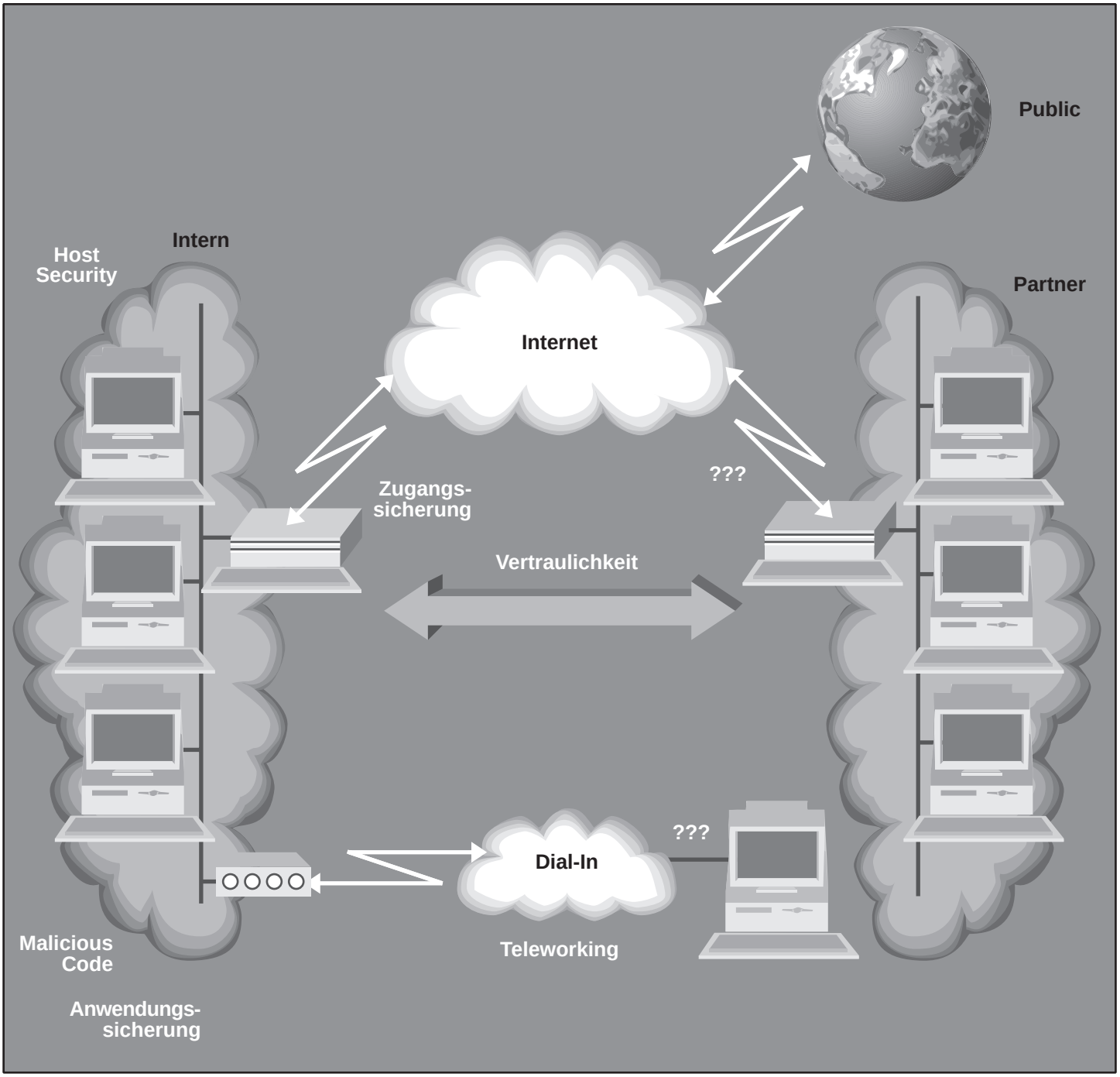
Bild 1 Sicherheitsverletzungen 1990 - 1999 (Quelle: US-CERT)



IT-Sicherheit – Der Schlüssel zum erfolgreichen E-Business

Die globale Vernetzung wird für eine immer größere Anzahl von Unternehmen zu einem wichtigen Erfolgsfaktor bei dem Erhalt alter und der Erschließung neuer Geschäftsfelder. Dabei nimmt der Anschluss an das Internet eine zentrale Position ein und löst bei der Anbindung von Zweigstellen oder Geschäftspartnern auch zunehmend die bisher als "halbwegs" sicher anzusehenden Verbindungen über Stand- oder Wählleitungen ab. Viele Unternehmen verkennen jedoch noch immer die nun verstärkt auftretenden Gefahren für die Sicherheit des lokalen Netzes und die Integrität der transportierten Daten. Neben altbekannten Gefahren wie dem Ausspähen von sensiblen Informationen oder dem Password-Cracking tauchen im Zusammenhang mit der Internet-Nutzung ganz neue Gefährdungen auf: Datenimporte enthalten unerwünschte Nebenwirkungen, die Identität von autorisierten Nutzern wird gefälscht oder es werden gar gesicherte Kommunikationskanäle übernommen (hijacking). Die Problembereiche der IT-Sicherheit werden insbesondere bei allen Arten von Netzanbindungen immer umfangreicher:

Bild 2 Typische Problembereiche der Netzwerk-Sicherheit

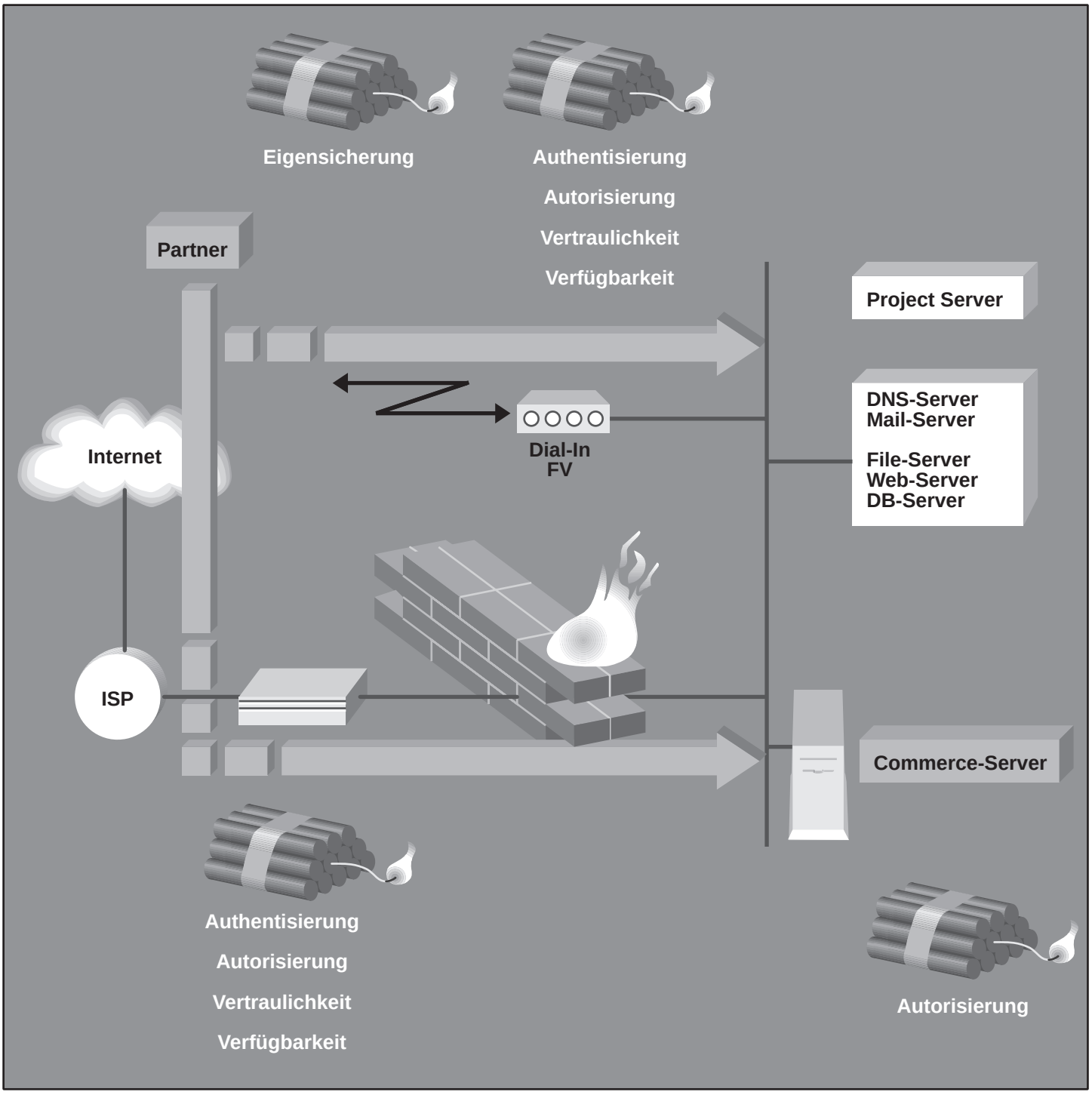


Intranet

Aber auch beim Aufbau eines Intranet bekommen die vorher zumeist vernachlässigten Sicherheitsbedürfnisse einen völlig neuen Stellenwert. Zugriffsschutz, Authentisierung oder auch die Vertraulichkeit müssen unbedingt gewährleistet sein, wenn der Übergang zu einer sicheren, voll integrierten Unternehmenslösung gelingen soll.

Bei der Kopplung von Unternehmensnetzen im Rahmen einer B2B-Kommunikation werden die auftretenden Gefährdungen zumeist unterschätzt. Ein Verbund ist aus Sicherheitssicht nur so gut geschützt wie sein schwächstes Glied. Alle Probleme, die ein Partner hat, können ohne gute Schutzmaßnahmen an den Netzgrenzen auch alle anderen Partner stark gefährden.

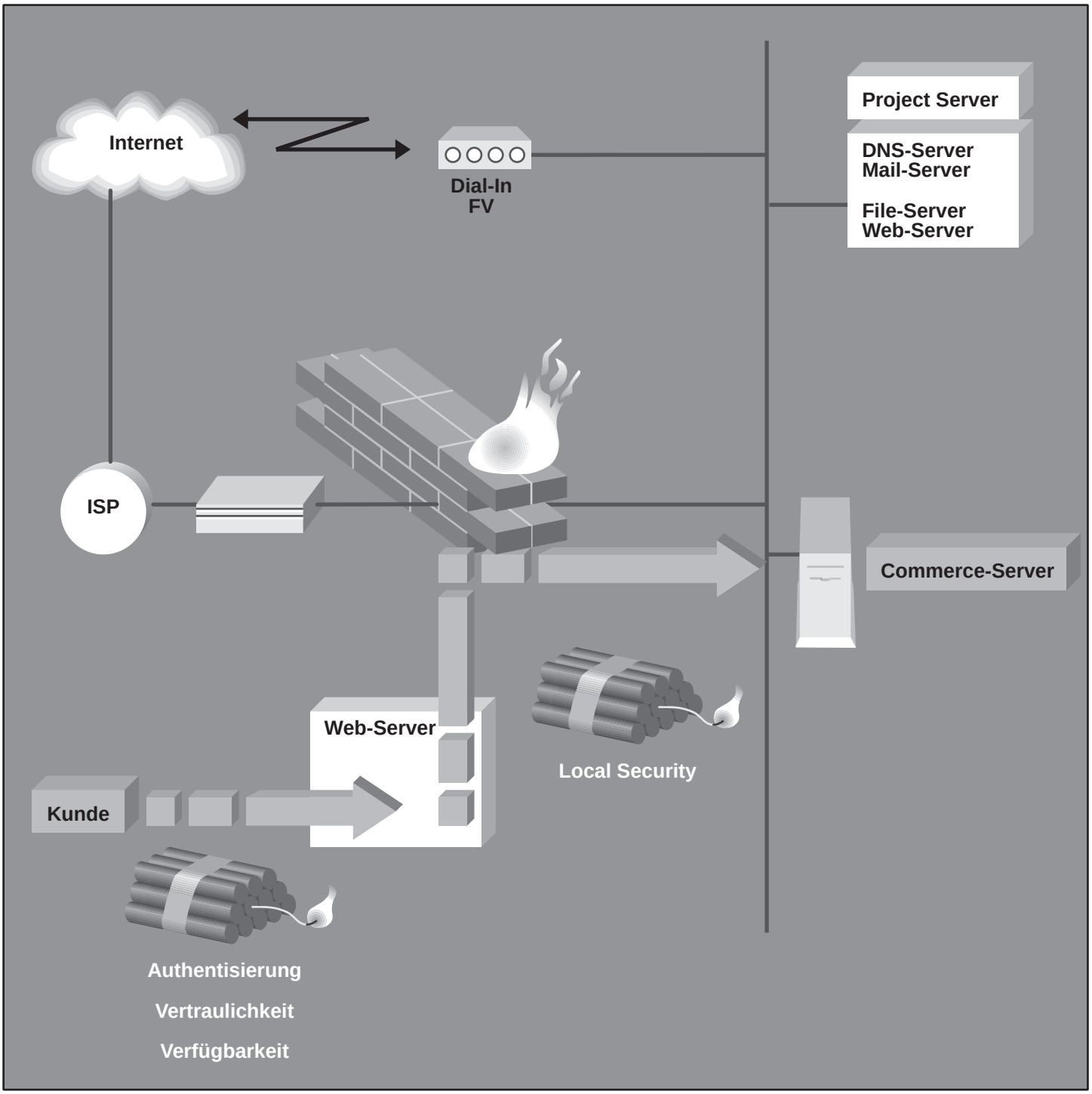
Bild 3 Gefährdungen einer Business-to-Business Kommunikation



Noch problematischer ist die Integration von Kundenzugriffen im Rahmen einer Business-to-Customer Kommunikation. Diese Art von E-Business erfordert die Bereitstellung von netzverteilten Anwendungen mit Zugriffen bis tief hinein in die Unternehmensnetze. Kunden, die zumindest zu Beginn einer Geschäftsbeziehung noch unbekannt sind, müssen auf Daten zugreifen können, die zumeist auf internen Main- und Datenbankservern liegen. Natürlich wird man keinem Fremden den direkten Zugriff gestatten, d.h. aber dass die indirekte Kommunikation über vermittelnde Web- oder Applikationsserver sehr sorgfältig konzipiert werden muss.

Nur Unternehmen, die von Anfang an viel Sorgfalt auf die strukturierte Konzeption aller Netzübergänge gelegt haben, sind in der Lage die neuen Anforderungen sauber zu integrieren.

Bild 4 Gefährdungen einer Business-to-Customer Kommunikation



Sicherheit kann jedoch nicht allein durch den bloßen Einsatz verschiedener Produkte erzielt werden. Sicherheit ist ein fortwährender Prozess, der mit einer fundierten Risikoanalyse und Konzeption beginnt, mit der Produktauswahl und Realisierung von Schutzmaßnahmen umgesetzt und durch eine gute Betriebsorganisation und Überwachung ständig begleitet wird. Es ergibt sich ein Sicherheitszyklus, der aus den folgenden Hauptkomponenten besteht:

Analyse

Diese sollte immer vor der übereilten Realisierung von Schutzmaßnahmen durchgeführt werden. Beinhaltet die Erfassung und Bewertung des IST-Standes. Das Vorgehen sollte alle Problembereiche schnell identifizieren und ist durch Tools zur Schwachstellenanalyse abzusichern.

Konzeption

Eine sichere und wartbare IT-Umgebung ist ohne die Grundlage eines Sicherheitskonzeptes undenkbar. Dieses erarbeitet und manifestiert alle organisatorischen und technischen Schutzmaßnahmen und legt das Vorgehen bei neu auftretenden Sicherheitsfragen fest. Es wird ergänzt durch eine umfassende Security Policy und ein Sicherheitsmanagement.

Realisierung

Umsetzung der Vorgaben des Sicherheitskonzeptes. Neben globalen Maßnahmen wie Firewalls, RA-Servern oder zentralen Virenscannern sind auch lokal installierte Systeme zur Authentisierung, Autorisierung, Verschlüsselung oder Einbruchserkennung einzusetzen.

Betrieb

Die besten Schutzmaßnahmen erweisen sich als sinnlos, wenn sie nicht fachgerecht angewendet und betreut werden. Deshalb kommt der guten Organisation des Tagesbetriebs eine erhöhte Bedeutung zu. Besonders wichtig sind Hinweise, Checklisten usw. für die Bewältigung von Ausnahmesituationen wie z.B. einem gerade stattfindenden Angriffsversuch

Überprüfung

Vollständige Sicherheit ist eine Illusion. Neue Bedrohungen, anfällige Software und eigene Konfigurationsfehler unterlaufen auch die besten Schutzmaßnahmen. Nur die gründliche Überprüfung durch Revision, externe und interne Einbruchstests und ein ständiges Online-Monitoring verbessern das Sicherheitsniveau.

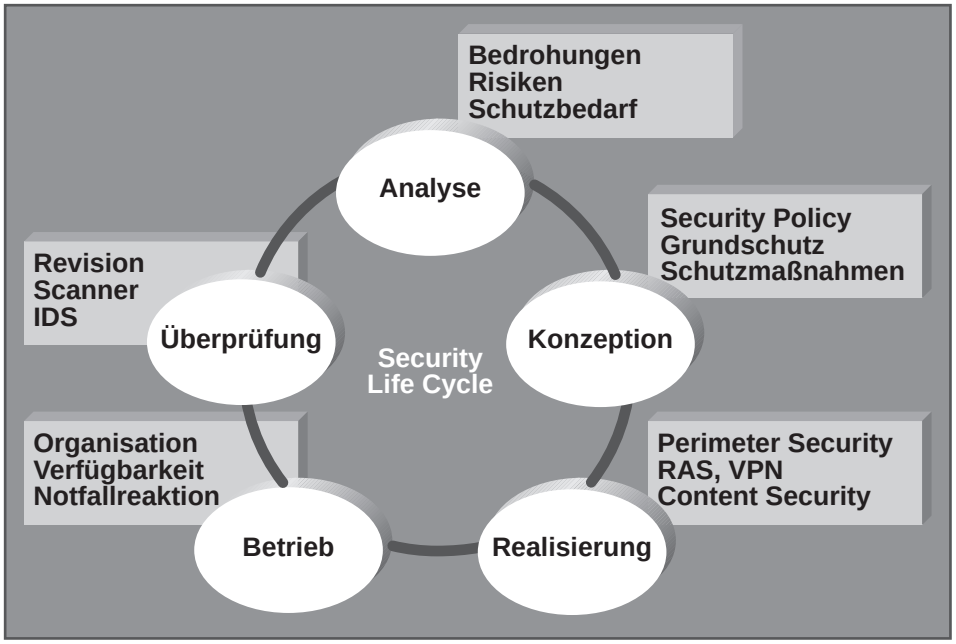


Bild 5 Sicherheit als ständiger Prozess

Firewall-Systeme

Aus der Erkenntnis heraus, dass beim Anschluss eines lokalen Netzwerkes an das Internet große Sicherheitsprobleme entstehen, hat sich in den letzten Jahren die Absicherung durch Firewall-Systeme durchgesetzt. Da gerade in größeren, komplexen Netzwerken die vollständige Sicherung der einzelnen Systeme kaum zu realisieren ist, wird dieser zentralen Lösung der Vorzug gegeben. Das Firewall-System kontrolliert dabei den Zugang zu dem zu schützenden Netz. Es verhindert sowohl unautorisierten Zugang von der Außenwelt zu lokalen Ressourcen als auch unberechtigte Nutzung externer Dienste durch Anwender aus dem lokalen Netz.

Mit Hilfe eines Firewalls lässt sich die Nutzung von internen Diensten auch ausschließlich auf das interne Netz beschränken und somit direkter Missbrauch von Diensten durch die Außenwelt verhindern. Dennoch kann man die Verfügbarkeit von Anwendungen mit sensiblen Daten gar nicht stark genug einschränken, so sollten hochschutzbedürftige verteilte Anwendungen grundsätzlich in einem eigenen physikalischen Netzwerk mit nur wenigen, gut kontrollierten Zugängen angesiedelt werden. Damit wird eine optimale Überwachung der kritischen Anwendungen möglich, da zusätzliche spezifische Kontrollsysteme den Zugang zu den Anwendungen sichern und die Zugänge vom normalen Datenfluss des Internet-Zuganges gegebenenfalls separiert werden können.

Der externe Zugriff auf sensible Daten sollte möglichst vermieden werden. Bei weniger schutzbedürftigen verteilten Anwendungen sollten alle Möglichkeiten zur Prüfung der Identität z.B. durch starke Authentisierungsverfahren genutzt werden. Hierzu werden in erster Linie Token-Verfahren zur Generierung von One-Time Passwörtern eingesetzt. Auch biometrische Verfahren, die z.B. durch Vergleich von Fingerabdrücken unverfälschbare Identifikationsmerkmale prüfen, sind stark im Kommen.

Die allgemeinen Anforderungen an Sicherungsmaßnahmen gelten in aller Regel auch für die interne Kommunikation im Intranet. Im Einzelfall kann der Schutzbedarf bei der Kopplung jedoch geringer sein als bei der Absicherung von Internet-Zugängen, z. B. weil Benutzer im Intranet als vertrauenswürdiger angesehen werden können. In diesen Fällen kann der Übergang auch mit schwächeren Maßnahmen wie z.B. filternden Routern abgesichert werden.

Das "beste Firewall-System" existiert nicht, obwohl fast jeder Hersteller genau dies von seinem Produkt behauptet. Um aus der Vielzahl der unterschiedlichen Firewall-Systeme die für ein Unternehmen bestgeeignete Lösung herauszufinden, sollte zunächst ein Kriterienkatalog aufgestellt werden. Unterstützung bei der Auswahl findet man am ehesten in Evaluierungen von Fachzeitschriften oder durch externe Berater.

Zertifizierungen durch neutrale Institutionen bieten hier leider nur Hinweise, aber keine echte Empfehlung. Sicherheitsüberprüfungen werden z.B. nach ITSEC (Information Technology Security Evaluation Criteria) vorgenommen, bisher haben aber nur wenige Hersteller diesen zumeist zeit- und kostenintensiven Weg gewählt. Zertifizierungen können immer nur Hinweise für eine Auswahl geben, ersetzen diese jedoch nicht. Insbesondere fehlen Bewertungen der Funktionalität, die aus einem einfachen Firewall erst ein effizientes Security-Gateway im täglichen Betrieb machen.

Ein Firewall sollte bereits im Grundumfang eine hohe Funktionsvielfalt bieten. Hierzu gehören unbedingt vielfältige Kontrollmöglichkeiten, Address Translation, Integritätskontrolle und natürlich Erweiterungsmöglichkeiten. Zum Content-Scanning (auf Viren, Trojaner usw.) sollte die Möglichkeit bestehen, Datenpakete zur Inspektion an einen dedizierten Server weiterzuleiten.

Virtual Private Networks (VPN)

Dem Einsatz von sicheren Verschlüsselungsverfahren kommt eine immer größere Bedeutung zu. Insbesondere bei vertraulicher Datenkommunikation über das Internet müssen kryptographische Methoden eingesetzt werden. Für den Aufbau solcher Virtual Private Networks (VPN) bieten die meisten Hersteller Lösungen an, die jedoch oft nur zwischen Systemen des gleichen Herstellers eingesetzt werden können. Die Nutzung des Internet-Standards IPSEC stellt eine gute Lösung dar, wie diverse Interoperabilitätstest bereits gezeigt haben. Besondere Aufmerksamkeit ist der Schlüsselverwaltung (manuell, dynamisch) zu widmen. Die lange Jahre sehr ärgerliche Exportbeschränkung seitens der US-Regierung für hinreichend sichere Verschlüsselung scheint nun endlich vom Tisch zu sein, so dass man wieder unter ausreichend vielen Produkten auswählen kann.

Firewalls gibt es heute in nahezu jeder Ausbaustufe und für jeden Geldbeutel. Neben aufwendigen Enterprise-Firewalls, die als zentrales Sicherheitsgateway über eine immense Funktionsvielfalt verfügen, gehört der breite Markt den günstigen NT-basierten Systemen. Obwohl NT als Betriebsgrundlage sicher nicht allererste Wahl ist, haben es einige Hersteller doch geschafft, hierauf verlässliche Firewalls aufzusetzen. Im Kommen sind auch sog. Firewall-Appliances, weitgehend vorkonfigurierte Systeme auf dedizierter Hard/Software, und Linux-Firewalls, die so langsam ebenfalls ernst zu nehmen sind.

Administration

Der fachgerechten Administration einer Firewall Schutzzone bestehend aus unterschiedlicher Hard- und Software, kommt eine hohe Bedeutung zu, da davon die Sicherheit aller mit dieser Zone direkt oder indirekt verbundenen Systeme abhängt. Durch die Integration in die zumeist schon bestehende Umgebung des System- und Netzwerk-Managements und die damit verbundene fachgerechte Überwachung kann ein gewisses Maß an Sicherheit gewährleistet werden. Erst die penible Sorgfalt, ständige Kontrolle und Berücksichtigung aktueller Hinweise und Anforderungen im Umgang mit den zentralen Sicherungsmaßnahmen jedoch wird in den meisten Fällen einen zufriedenstellenden Schutz bewirken.

Aufbau von Schutzzonen

Neben der Auswahl geeigneter Schutzmaßnahmen kommt dem Aufbau von Schutzzonen zwischen Netzen unterschiedlichen Sicherheitsniveaus eine hohe Bedeutung zu. Dies umfasst den Aufbau genauso wie den Tagesbetrieb im Normal- aber auch im Ausnahmefall (erfolgter Angriff). Gerade die Gestaltung des Übergangs zwischen lokalem Netz und Internet umfasst nicht nur die Auswahl und Anordnung der beteiligten Komponenten (Router, Firewall, Server), sondern auch die sichere Abwicklung der immer benötigten Internet-Dienste wie z.B. DNS oder Routing.

Grundprinzip jeder Sicherheitskonzeption ist der Aufbau einer mehrstufigen Schutzkonfiguration. Damit werden Angriffe deutlich erschwert, da es nicht ausreicht, z.B. nur eine bestimmte Schwachstelle zu kennen und auszunutzen. Auch der Ausfall oder die Fehlkonfiguration einzelner Komponenten führt damit nicht zwingend zum Verlust der Sicherheit des Gesamtsystems. Den Ausgangspunkt für die folgende Betrachtung soll eine zumeist in hochschutzbedürftigen Umgebungen eingesetzte Konfiguration aus zwei Routern und einem Firewall bilden. Diese bietet Schutz sowohl vor äußeren als auch vor inneren Angriffen und bedingt auch vor dem Ausfall einzelner Komponenten. Bei geringerem Schutzbedarf kann dann abgestuft auf einzelne Systeme verzichtet werden.

Aus Sicherheitsgründen sollten die Netzkomponenten möglichst auf bekannt unsichere Funktionalität wie z.B. dynamisches Routing, ungesicherte Fern-Administration und Management mit SNMP verzichten. In Ausnahmefällen muss eine unter den Komponenten abgestimmte Einschränkung der geforderten Funktionalität durch Paketfilter, Firewallregeln, strenge Authentisierung sowie Verschlüsselung für eine angemessenes Maß an Sicherheit sorgen. In jedem Fall aber sollten sämtliche Komponenten untereinander mit statischen Routen kommunizieren.

Neben dem Firewall mit seinen ausgewiesenen Sicherheitsfunktionen bieten die Router zusätzliche Möglichkeiten. Der externe Router dient als erste Hürde gegen potentielle Angreifer aus dem Internet. Er sollte über die Möglichkeit eines konfigurierbaren Paketfilters verfügen und ist so zu konfigurieren, dass er Zugriffe abweist, die ohne weitere Prüfung durch den Firewall als unberechtigt erkannt werden können. Auf diese Art können einfache Attacken (z.B. IP-Spoofing) und bekannt unsichere Dienste (z.B. die Berkeley r-Dienste) schon frühzeitig abgewiesen werden. Da die Administration von Routern in der Regel wenig komfortabel und daher recht fehleranfällig ist, sollten nur wenige, einfache Filterregeln implementiert werden. Mit den Sicherheitsfunktionen des externen Routers wird der Firewall entlastet und das interne Netz ist auch bei Fehlfunktionen des Firewalls geschützt.

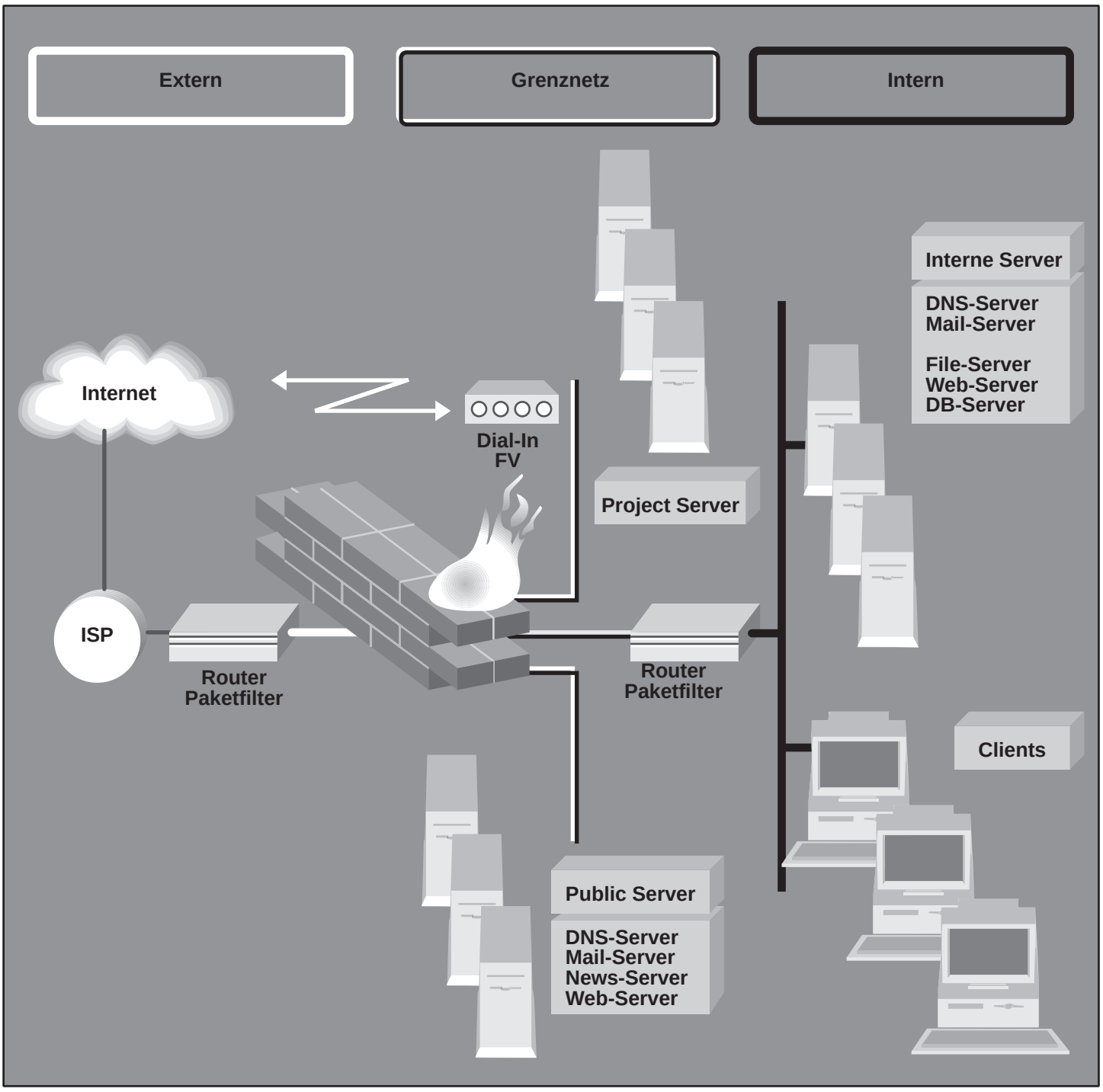
Der interne Router dient der Absicherung des Firewalls vor Angriffen aus dem internen LAN, z.B. durch IP-Spoofing. Diese Möglichkeit besteht insbesondere bei fehlerhafter Konfiguration der Schutzzone oder aber bei weiteren externen Zugängen ins interne Netz. Für die Realisierung der Funktion des internen Routers bietet sich die Ergänzung eines bestehenden lokalen Routers um Regeln zur Paketfilterung an.

Server, die für die Bereitstellung von Informationen an externe Benutzer dienen (z.B. Webserver), sollten nicht im lokalen Netz plaziert werden. Auch die früher häufig empfohlene Positionierung zwischen Firewall und externem Router in einer DMZ (demilitarized zone) wirft Sicherheitsprobleme auf und entspricht nicht mehr dem heute Machbaren. Bei der immer möglichen Kompromittierung eines öffentlichen Servers hat ein Angreifer beste Möglichkeiten den gesamten Datenverkehr, der den Netzübergang passiert, zu beeinflussen. Es empfiehlt sich die Installation eines separaten Netzes an einem zusätzlichen Interface des Firewalls, unter anderem um den Datentransfer überwachen und gegebenenfalls protokollieren zu können. Hier sollten auch als Split-Server Lösung die extern sichtbaren Server für DNS und Mail plaziert werden. Sie erfüllen nur die Minimalanforderungen an die externe Kommunikation und kommunizieren nach innen nur mit den dafür vorgesehenen Servern.

Verfügbarkeit

Die zu definierende Verfügbarkeit eines Netzübergangs entscheidet darüber, ob ein oder mehrere Backup-Systeme im Falle von Hardware-Ausfällen vorzusehen sind. Hierbei ist zwischen Hot-Standby- und Cold-Standby-Systemen zu unterscheiden. Cold-Standby-Systeme werden in der Regel eine Wiederverfügbarkeit innerhalb von wenigen Stunden garantieren, dies in Abhängigkeit der Verfügbarkeit des Bedienungspersonals. Sollte sich herausstellen, dass der Internet-Anschluss rund um die Uhr innerhalb eines kurzen Ausfallzeitraumes (im Sekunden bzw. Minutenbereich) automatisch wieder gesichert verfügbar sein muss, so wird ein wesentlich aufwendigeres Hot-Standby-System realisiert werden müssen. Neben dem ständigen Abgleich von Konfigurations- und Sitzungsdaten gehört auch die automatische Anpassung von Routen und IP-Adressen zum erforderlichen Leistungsumfang solch einer Lösung.

Bild 6 Typischer Aufbau eines gesicherten Netzübergangs



Deutlich zunehmend ist die Anforderung nach der gesicherten Bereitstellung von Heimarbeitsplätzen, oder ganz allgemein gesprochen von Fernzugriffen (Remote Access). Die Vielzahl der möglichen Nutzergruppen und unterschiedlichen Verbindungen macht es unabdingbar, ein umfassendes Gesamtkonzept zu entwickeln. Es sollte flexibel bei der Hinzunahme neuer Anforderungen sein und leicht ableitbare Schnittstellen incl. der benötigten technischen Ausstattung liefern. Zunächst müssen dazu die grundsätzlichen Risiken bewertet werden, die mit der Nutzung unterschiedlicher Zugangsmedien (Internet, ISDN, GSM ...) verbunden sind. Hierauf aufsetzend werden Empfehlungen zu unverzichtbaren Sicherheitsmaßnahmen festgelegt und in einem jeweils medienspezifischen Profil zusammengefasst. Im nächsten Schritt werden dann für jede Nutzergruppe (Mitarbeiter, Kunden,...) Sicherheitsanforderungen definiert. So wird im allgemeinen bei Mitarbeitern generell ein höheres Vertrauensverhältnis unterstellt, als bei einem zumeist unbekannten Techniker der Fernwartung. Bildet man jetzt die konkrete Kombination aus Nutzer und Zugangsmedium, z.B. Heimzugriff eines Mitarbeiters über ISDN, dann ergeben sich zumeist Abweichungen zwischen den Anforderungen und den vorhandenen Sicherheitsvorkehrungen. Durch Erweiterung der Sicherheitsmaßnahmen können entweder die Anforderungen erfüllt werden, oder der Zugang wird nicht erlaubt.

Malicious Code

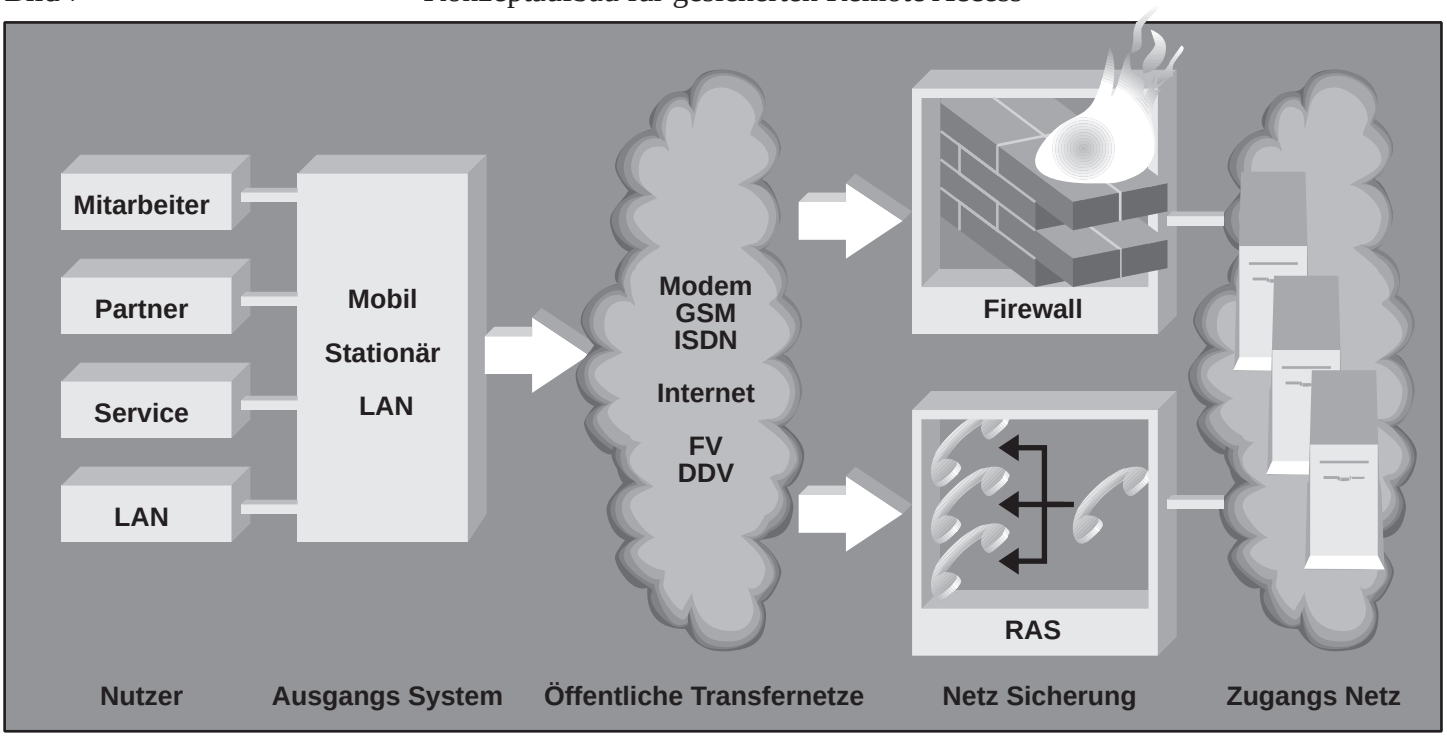
Die momentan wohl größte Gefahr für Unternehmen geht von datenimportierenden Diensten aus. Da aber genau dies die heute wichtigsten Anwendungen wie Mail, Web und Filetransfer betrifft, kann das Unterbinden dieser Dienste keine Lösung sein. Zumeist wird in diesem Zusammenhang nur von Viren gesprochen, die stellen aber mittlerweile nicht mehr die alleinige Gefahrenquelle dar. Alle Arten von sog. Malicious Code (Viren, Trojaner, Vandals) müssen in die Sicherheitsbetrachtungen einbezogen werden.

Viren zeichnen sich dadurch aus, dass sie andere Programme infizieren (den Code erweitern) und sich dann weiter verbreiten. Sie haben die unterschiedlichsten Auswirkungen, nicht immer bösartige, und sind wegen typischer Codemuster durch gute Virenscanner zumeist zu erkennen. Mindestens 20.000 Viren sind heute bekannt, die größten Probleme bereiten zumeist Macro-Viren, die sich z.B. in Office-Dokumenten verbergen. Durch die geschätzte Praxis des Dokumentenaustauschs auch über das Internet (per Mail oder ftp) ist damit der Verbreitung solcher Viren Tür und Tor geöffnet. Nur durch eine gute Nutzerschulung und ein mehrstufiges Virenschutzkonzept (Gateway, Server, Endsystem) lässt sich das Problem in den Griff bekommen.

Wie gefährlich diese Viren sind, zeigt das Beispiel des berüchtigten Melissa-Virus im letzten Jahr. Selbst eine mit diesen Themen doch vertraute Firma wie Microsoft musste einen ganzen Tag lang den gesamten Mailverkehr unterbinden, um der weiteren Verbreitung des Virus Herr zu werden.

Noch weitaus gefährlicher als Viren, insbesondere für den aufkommenden E-Business Bereich sind Nebenwirkungen, die sich im Code von Java, ActiveX oder auch beliebigen Anwendungsprogrammen aus unsicherer Quelle verbergen. Diese Manipulationen lassen sich durch herkömmliche Virenscanner nicht entdecken und sind in ihren Möglichkeiten nahezu unbegrenzt. Je nach Intention des Erzeugers können sie alle möglichen Manipulationen auf einem Zielsystem starten: Homebanking-Transaktionen vornehmen, lokale Passwörter knacken oder abgelegte Keys für Business-Kommunikation auslesen. Alle diese Fälle sind bereits vorgekommen und zeigen die Grundproblematik der heutigen Sicherheitstechnologien auf. Durchaus sehr sichere Basistechniken können ausgehebelt werden, wenn sie auf schlecht administrierten unsicheren Grundsystemen aufsetzen. Hierzu muss leider die gesamte Windows-Familie und damit 90% aller weltweit eingesetzten Endsysteme gezählt werden.

Bild 7 Konzeptaufbau für gesicherten Remote Access



IT-Sicherheit – Der Schlüssel zum erfolgreichen E-Business

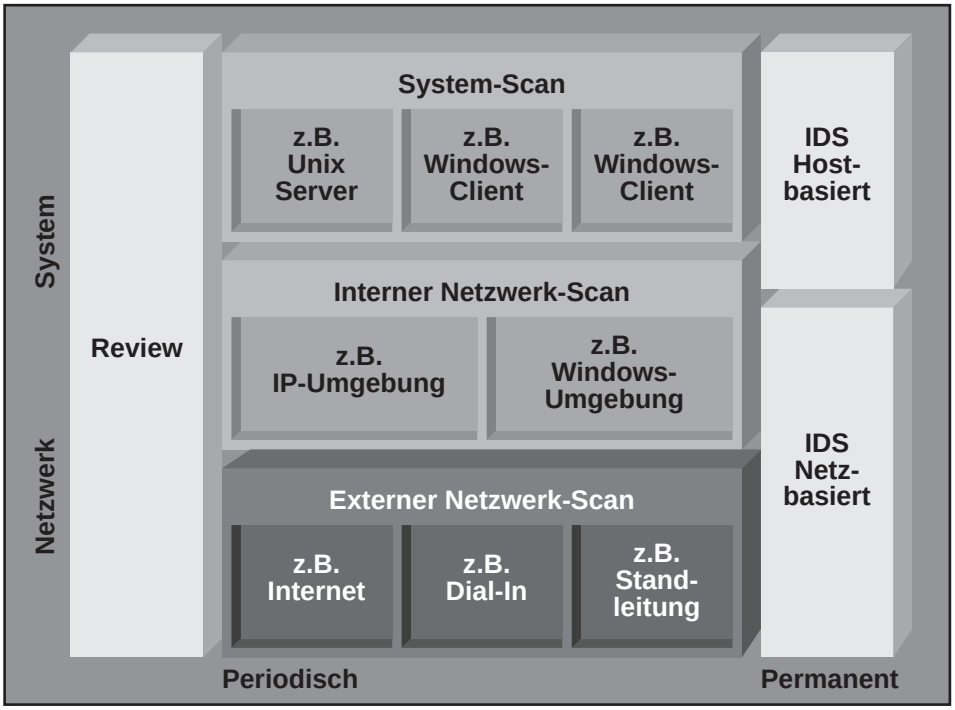


Bild 8 Baukasten für Sicherheitsprüfungen

Überwachung der Sicherheit

Auch bei den besten Sicherheitsmaßnahmen ist niemals von einer 100%-igen Sicherheit auszugehen. Fehler in der Administration oder in der verwendeten Software können ebenso die Sicherheit bedrohen wie neue, bisher noch wenig bekannte Angriffsstrategien. Deshalb kommt einer ständigen Überwachung der Sicherheit des Gesamtsystems eine große Bedeutung zu. Um fortlaufend eine sichere Netzumgebung zu gewährleisten, sind Maßnahmen auf unterschiedlichen Ebenen notwendig. Als proaktive (vorbeugende) Maßnahmen sollten in festen Intervallen, aber dazwischen auch unangemeldet durchgeführt werden:

- Organisatorische Prüfung in Form einer Revision
- Technische Prüfung in Form einer Einbruchs- und Störsimulation (Einsatz von Security-Scannern)

Als ständige aktive Maßnahme empfiehlt sich:

- Überwachung des laufenden Betriebs auf aktuell durchgeführte Angriffe (Einsatz von Intrusion-Detection-Systemen)

Die Durchführung der Überprüfungsmaßnahmen erfordert insbesondere bei der Auswertung ein hohes Maß an Fachkenntnis. Da es zumeist nicht sinnvoll ist, die eigenen Administratoren mit dieser Aufgabe zu betrauen (Gefahr der Betriebsblindheit), empfiehlt sich der Einsatz externer Firmen. Ein sinnvolles Angebot an Sicherheitsprüfungen sollte wie in Bild 8 aussehen.

Insbesondere die zunehmende Abwicklung von Geschäftsvorgängen im Umfeld des E-Business macht eine neue Art der Vertrauensbildung zwischen Unternehmen dringend notwendig. Innerhalb der Business-to-Business Kommunikation wird notwendigerweise eine enge Beziehung zu einem Partner eingegangen, zumeist ohne dessen Sicherheitsvorkehrungen zu kennen oder darauf Einfluss nehmen zu können. Eine Sicherheitsüberprüfung und die anschließende Zertifizierung durch eine neutrale Instanz dienen als vertrauensbildende Maßnahmen.

Das Vorgehen zu dem von uns vergebenen Zertifikat "Secured E-Business" sei nachstehend kurz dargestellt: Die Sicherheitsvorkehrungen eines Unternehmens werden nach einem umfassenden Kriterienkatalog überprüft. Hat das Unternehmen die Tests erfolgreich durchlaufen, erhält es das Zertifikat "Secured E-Business". Dieses Zertifikat bescheinigt der geprüften Institution einen verantwortungsvollen Umgang mit der IT-Sicherheit. Damit die streng definierten Richtlinien stets aktuell bleiben, gilt das Zertifikat für den begrenzten Zeitraum von 90 Tagen und muss dann durch gezielte Nachprüfungen erneuert werden. Die Sicherheitsinformationen werden zwischen den einzelnen Testzyklen ständig aktualisiert. Intrusion Detection Tools bieten darüber hinaus ein zusätzliches Maß an Netzwerksicherheit während des laufenden Betriebs. Im Rahmen der Zertifizierung wird ein 10-Punkte Plan umgesetzt:

Phase-1: Analyse	1. Vorbereitender Review mit Sicherheits-Checkliste
	2. Internet Perimeter Check mit Security Scanner
	3. Dial-In Check mit Telephony Scanner (Option)
Phase-2: Report	4. Empfehlungen zur Verbesserung des Sicherheitsniveaus
	5. Abschlussbericht mit Management Summary
	6. Abstimmung der Ergebnisse
Phase-3: Überwachung	7. Aufbau eines Intrusion Detection Systems
	8. Kontinuierliche Hinweise auf aktuelle Sicherheitsrisiken
	9. Periodisch erscheinendes Sicherheits-Bulletin
Abschluss*	10. Zertifikat "Secured E-Business"

* nur nach erfolgreichem Durchlaufen aller Tests

Fazit

Die Möglichkeiten der globalen Kommunikation sind zu phantastisch, als dass man die Nutzung wegen der durchaus vorhandenen Risiken stark einschränken sollte. Aus geschäftlicher Sicht wird dies zumeist auch gar nicht möglich sein. Ausgeklügelte Gegenmaßnahmen verbunden mit einer guten Konzeption und Organisation aller Aktivitäten können die Probleme beherrschbar machen. Jeder muss sich aber darüber im Klaren sein, dass der Kampf gerade erst begonnen hat. Immer neue "Interessenten" und Angriffsziele werden auftauchen und den oben dargestellten "Security Life-Cycle" wohl nie zu einem Ende kommen lassen.