

## Network Security – Eine Einführung

Die grundsätzliche Herausforderung ist denkbar simpel: wie stellt man sicher, daß Unbefugte nicht in Kommunikationsnetze (im Sinne LAN, WAN oder Internet-basierend) eindringen und vertrauliche Informationen oder sonstige IT Ressourcen weder erspähen, manipulieren noch beschädigen.

Diese simple Herausforderung ist in der Praxis beliebig komplex und stellt nicht geringe Anforderungen an den Endkunden und an den Dienstleister. Ein typisches Security Projekt gliedert sich in folgende vier Phasen:

1. Analyse
2. Definition einer Security Policy
3. Implementierung
4. Laufende Überwachung (Audit) und Verfeinerung

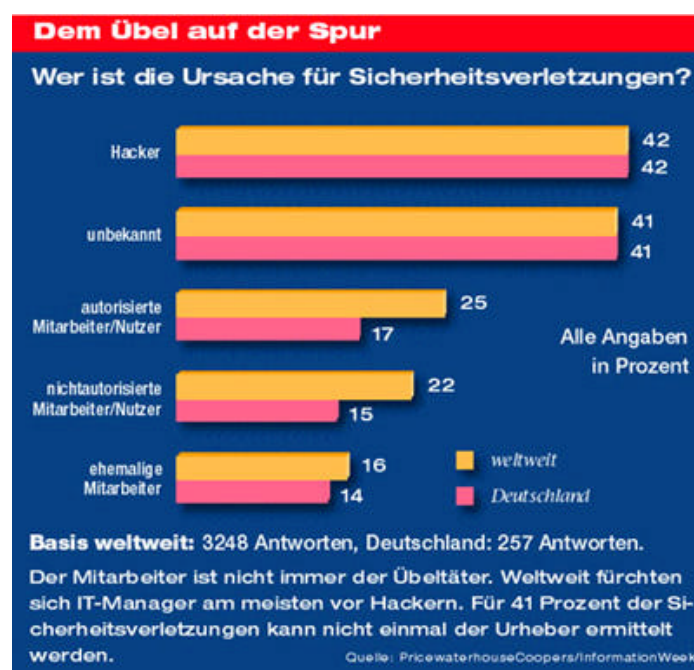
Aufgrund der massiven Publizierung von Sicherheitsvorfällen in den letzten Monaten hat die Attraktivität dieses Marketes erheblich zugenommen. Leider tummeln sich viele "Halbwissende" in diesem Markt. Eine professionelle Projektrealisierung bedingt nicht unerhebliche Vorinvestitionen im Aufbau von technischem, organisatorischem und rechtlichem Know-How.

### Analyse

Die meisten IT-Security Projekte leiden unter einem gewissen Aktionismus. D.h. ein Sicherheitsvorfall oder eine erkannte Sicherheitslücke erhöht die Motivation zu investieren und möglichst schnell zu handeln. Dieses ist verständlich und situationsbedingt oft sinnvoll, aber auf Dauer kontraproduktiv.

Sinnvoller ist es eine Bestandsaufnahme vorzunehmen und zu versuchen, Sicherheitslücken zu erkennen. Oftmals läßt sich durch einfaches Abschalten von nicht benötigten Diensten oder Verschärfen von Dateizugriffsrechten mehr erreichen, als durch übereilte Investitionen in Hard- und Software.

Eine sinnvolle Analyse richtet sich nach innen und nach außen. Interessant ist folgende Umfrage der Information Week Deutschland:



Eine qualitativ hochwertige Sicherheitsanalyse ist zeitintensiv und setzt ein hohes Maß an Erfahrung voraus. Der Analytiker muß sich laufend informieren und fortbilden.

Es gibt eine Vielzahl von Freeware und Shareware Tools und Ressourcen zum Thema Security Analyse. Zum weiteren Einlesen empfehlen wir das deutschsprachige IT-Audit Portal. Sehr nützlich ist die Roadmap to Network Security. Interessant ist das kostenlose Online Tool Security SnapShot der International Computer Security Association ICSA.

Das Center for Internet Security hat einen automatisierten Test zur Sicherheitsüberprüfung von Solaris freigegeben.

Als Literatur zu Härten von Betriebssystemen empfehlen wir die "Step-by-Step Guides" vom SANS Institute. In Sachen Anti-Virus Policy empfehlen wir das TruSecure Anti-Virus Policy Guide.

Lance Spitzner hat eine sehr informative Sammlung von Security Whitepapers publiziert.

Kommerzielle Security Scanner Produkte lassen laufend neue Erkenntnisse in ihre Produkte einfließen und ermöglichen eine Automatisierung der Überprüfung von Netzwerk- und Systemressourcen auf Sicherheitslücken.

### Definition einer Security Policy

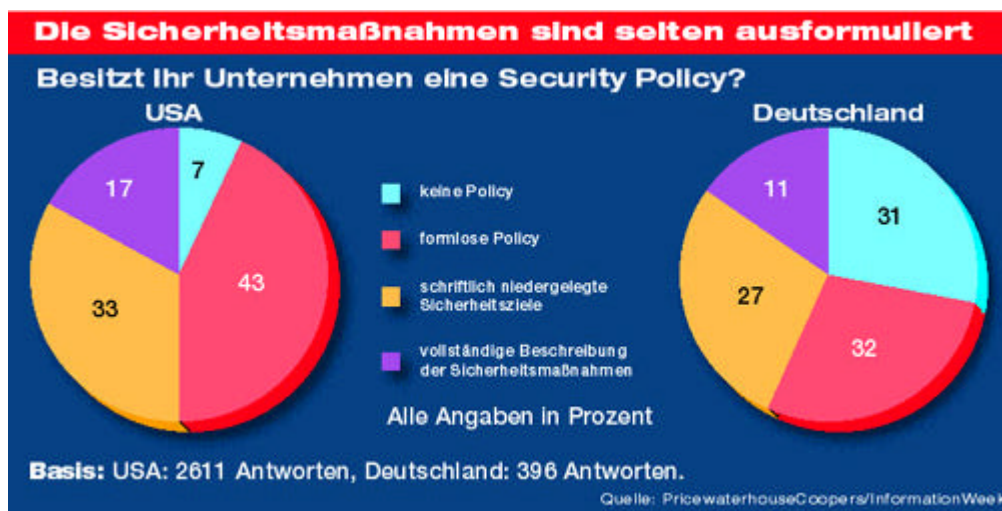
Eine sinnvolle Sicherheitspolitik kann nur in enger Abstimmung zwischen Unternehmensleitung und den IT Sicherheitsverantwortlichen erfolgen. Letztendlich müssen folgende zwei Fragen beantwortet werden:

Wer darf von wo kommend wann und wie auf welche Ressourcen zugreifen?

Wie detailliert (oder überhaupt) sollen diese Zugriffe protokolliert und ausgewertet werden?

Diese Antwort auf diese Fragen muß die Geschäftsprozesse des Unternehmens widerspiegeln. Um mögliche Mißverständnisse auszuräumen ist es unumgänglich, daß diese Politik schriftlich niedergelegt, abgesegnet und gepflegt wird.

Erstausnehmend ist wie wenig Unternehmen dies konsequent umsetzen:



Denn erst diese Security Policy erlaubt es sich sinnvolle Gedanken über die Implementation und der Auswahl von Produkten bzw. Herstellern zu machen.

## Implementation

Ausgehend von der Security Policy, sollte man versuchen abzuklären wie folgende Sicherheitsforderungen beantwortet werden können:

Grundlegende Sicherheitsforderungen		
Forderung	Beschreibung	Lösungsansätze
<b>Access Control</b>	Festlegen wer Zugriff auf welche Information eines Systems hat	Firewall Security Appliance
<b>Authentication</b>	Überprüfen der Identität der Kommunikationspartner	Authentisierung PKI
<b>Privacy</b>	Unterbindet das Lesen sensibler Informationen durch Unbefugte	VPN Security Appliance
<b>Integrity</b>	Sicherstellen, daß Systeme und Information nicht manipuliert oder verändert worden sind	Anti-Virus VPN PKI
<b>Non-Misuse</b>	Sicherstellen, daß Systeme und Information nicht unangemessen eingesetzt werden.	Accounting URL-Screening Anti-Virus
<b>Non-Repudiation</b>	Unterbinden, daß eine Transaktion zurückgewiesen wird	PKI
<b>Management Audit</b>	& Überprüfen und Administration von Sicherheitsmaßnahmen	Security Audit Intrusion Det. Accounting

Hieraus kann man sich an die Produktauswahl und -implementation heranwagen. Spätestens hier stellt sich die Kostenfrage. Grundsätzlich muß sich der Auftraggeber im Klaren sein, daß eine professionelle Sicherheitslösung nicht unerhebliche Kosten verursacht.

Nichts zu tun kann natürlich letztendlich ungleich teurer sein, wie diese Umfrage belegt:

### Sicherheitsverletzungen fordern ihren Tribut

Wie hoch ist der finanzielle Verlust, den Sicherheitsverletzungen im vergangenen Jahr hervorriefen?

	2000 weltweit	1999 weltweit	2000 USA	1999 USA	2000 Deutschland	1999 Deutschland
kein Verlust	24	24	22	20	31	44
bis zu 1000 Dollar	10	8	11	8	11	10
bis zu 10 000 Dollar	12	11	13	12	13	10
bis zu 500 000 Dollar	3	8	3	10	2	3
bis zu einer Million Dollar	1	1	1	1	1	1
nicht bekannt	41	47	38	48	36	33

Alle Angaben in Prozent.

Quelle: PricewaterhouseCoopers/InformationWeek

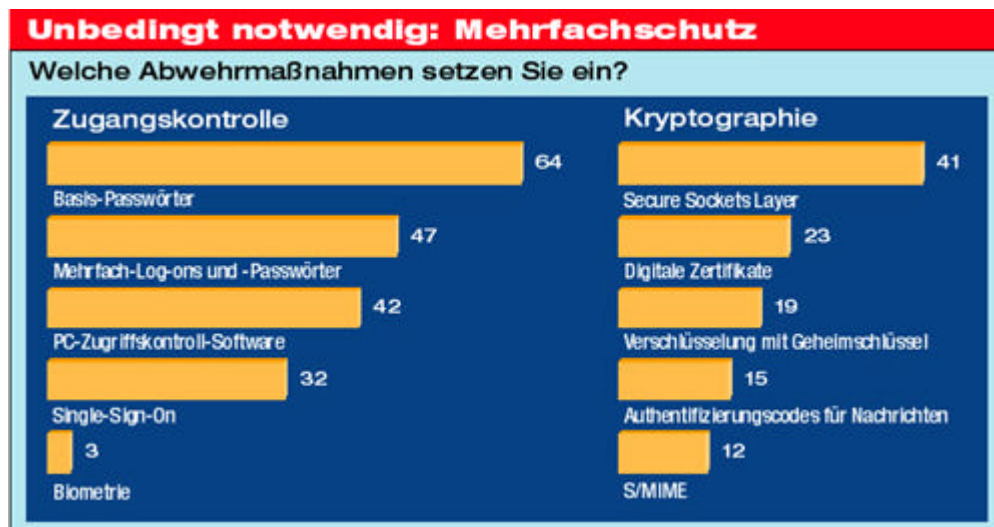
**Basis 2000:** weltweit: 3278 Antworten, USA: 1781 Antworten, Deutschland: 260 Antworten.

**Basis 1999:** weltweit: 1910 Antworten, USA: 1020 Antworten, Deutschland: 229 Antworten.

Besonders deutsche Unternehmen sind mit finanziellen Verlusten konfrontiert. Von ihnen geben 13 Prozent mehr als im Vorjahr an, durch Sicherheitsverletzungen Einbußen gehabt zu haben.

Oftmals macht man es sich sehr leicht und glaubt, daß mit der Installation und Konfiguration einer Firewall ein ausreichendes Maß an Sicherheit erreicht ist. Das ist in den wenigsten Fällen so.

Folgende Tabelle gibt einen Eindruck vom Stand der Dinge:



Als Minimum sollte man sich mit folgenden drei Produktthemen auseinandersetzen:

**Firewalls**

**Anti-Virus Lösungen**

**Strenge Authentisierung**

Die laufende Überwachung (Audit) und Verfeinerung bedingt den Einsatz weitergehender Werkzeuge wie z.B.:

**Intrusion Detection**

**Security Auditing**

**Accounting**

Eine Firewall ist ein "Single Point of Failure". D.h. bei einem Systemausfall ist das Firmennetz nicht mehr an das Internet angebunden. Für viele Geschäftsmodelle ist dies nicht tragbar.

Klassische 7x24 vor Ort Service Konzepte helfen hier kaum weiter, da trotzdem die Internet Anbindung für mehrere Stunden unterbrochen ist. Hier stellen Hochverfügbarkeitslösungen (HA) von StoneSoft, Check Point und Rainfinity eine maximale Unterbrechung von wenigen Sekunden sicher. Bei sehr hohen Netzwerkbandbreiten können diese HA-Lösungen um die Funktion der dynamischen Lastverteilung erweitert werden.

In größeren Netzen ist der Einsatz von URL-Screening Systemen inzwischen fast selbstverständlich, um der Mißbrauch des Internetzuganges zu reduzieren. URL-Screener haben zunächst wenig mit Netzwerk Sicherheit zu tun, lassen sich aber sehr gut an Firewalls, die sich ja am Flaschenhals Internet Gateway befinden, einbinden.

## **Laufende Überwachung (Audit) und Verfeinerung**

Netzwerke sind einem ständigen Wandel unterworfen. Neue Anwendungen, neue Betriebssysteme, Updates, neue Hardwarekomponenten usw. werden installiert. Diese Veränderungen bringen oftmals neue Sicherheitslücken mit sich. Gerade Updates verändern oftmals sicherheitsrelevante Parameter ohne dem Netzwerkadministrator zu informieren.

Für schon "gehärtete" Komponenten werden immer wieder neue Sicherheitslücken aufgespürt und umgehend publiziert.

Auch das Gefahrenpotential aus dem Internet verändert sich. Neue Applikationen und Protokolle, neue Hacker Tools und neue Generationen von Angreifern machen das Leben des Sicherheitsverantwortlichen spannend.

Firewalls können erkannte Angriffe in Log-Dateien protokollieren. Diese sollten täglich ausgewertet werden, um Trends zu erkennen und ggf. Gegenmaßnahmen zu treffen. Oftmals ist es schwierig und eine Herausforderung vor "lauter Wald" die "Bäume" zu sehen. In solchen Fällen ermöglichen es Accounting Tools wie z.B. Telemate.net oder das Reporting Module von Check Point eine schnelle graphische Auswertung vorzunehmen.

Firewall Systeme können so konfiguriert werden, daß registrierte Sicherheitsvorfälle z.B. ein SNMP Trap, eine eMail oder eine Pager Meldung auslösen, damit der System Administrator ggf. auch von unterwegs reagieren kann.

Eine Firewall kann zunächst nur Angriffe von außen abwehren. Viele Angriffe erfolgen allerdings von innerhalb des Netzes oder über authentifizierte VPN Verbindungen. Natürlich ist nicht sichergestellt, daß eine Firewall alle Angriffstypen erkennt und abwehrt.

Es ist deswegen sinnvoll hinter der Firewall in Netzwerksträngen bzw. auf Host Systemen sogenannte Intrusion Detection Systeme einzusetzen. Diese analysieren den Netzwerkverkehr bzw. Zugriffsversuche und vergleicht diese mit einer ständig aktualisierten Angriffsmuster Datei.

Im Falle eines Angriffs, egal ob von innen oder von außen, wird zunächst die Verbindung terminiert, ein Protokolleintrag vorgenommen, ggf. Alarm ausgelöst und ggf. die Firewall selbständig rekonfiguriert. Dies ist ein erster Schritt zu einer sich selbst regulierenden Sicherheitsinfrastruktur.

Online GmbH arbeitet mit dem Marktführer, dem REALsecure von ISS zusammen. Dieses Produkt ist besonders eng mit der Check Point FireWall-1 integriert und Bestandteil des Microsoft Internet Security und Acceleration Server, zu dem es spezielle umfangreiche Erweiterungen des Secure Sensor Server gibt.

Es ist sinnvoll in regelmäßigen Abständen die Netzwerksicherheit zu analysieren und die resultierenden Erkenntnisse in das Sicherheitskonzept einfließen zu lassen. Hier bieten sich die eingangs erwähnten und vorgestellten Analysewerkzeuge an.

*Thomas K.H. Bittner  
Senior Consultant, Online GmbH  
Microsoft Servers and Windows 2000 MVP  
Microsoft Windows 2000 Certified Professional  
[www.mvpatwork.de](http://www.mvpatwork.de)*