Sicherheit für IT-Netzwerke

M. Nispel, Frankfurt/Main

Die Anzahl netzwerkgebundener IT-Anwendungen nimmt ebenso zu, wie die Angriffe durch Viren und Würmer aus dem Internet. Hinzu kommen viele Attacken von internen Zugängen, die durch den Anschluss infizierter mobiler Geräte möglich sind. Daher empfiehlt sich ein umfassendes Sicherheitskonzept, das sowohl auf interne als auch externe Bedrohungen reagieren kann.

1 Sicherheitsanforderungen

Zusammen mit den IT-Systemen hat auch das Internet Protokoll (IP) den Weg in nahezu alle Unternehmensbereiche gefunden. Die Abhängigkeit von einer sicheren und verfügbaren IT-Infrastruktur nimmt stetig zu. Dabei wird das Netzwerk als Herzstück dieser Infrastruktur zu einem entscheidenden Wettbewerbsfaktor. Konvergenzstrategien, die ein Zusammenführen von zuvor getrennt betriebenen Netzen und deren Anwendungen zum Inhalt haben, werden vermehrt umgesetzt – und das nicht nur bei Nutzung der Telefonie über IP-Netzwerke (Voice over IP – VoIP). Mittlerweile kommen immer mehr dynamische Lösungen aus den Bereichen Speichernetzwerke (Storage over IP), Sicherheits- und Überwachungstechnik (Video over IP) sowie der Gebäudekontrolle (z. B. Sensoren, Aufzugssteuerungen) zum Einsatz.

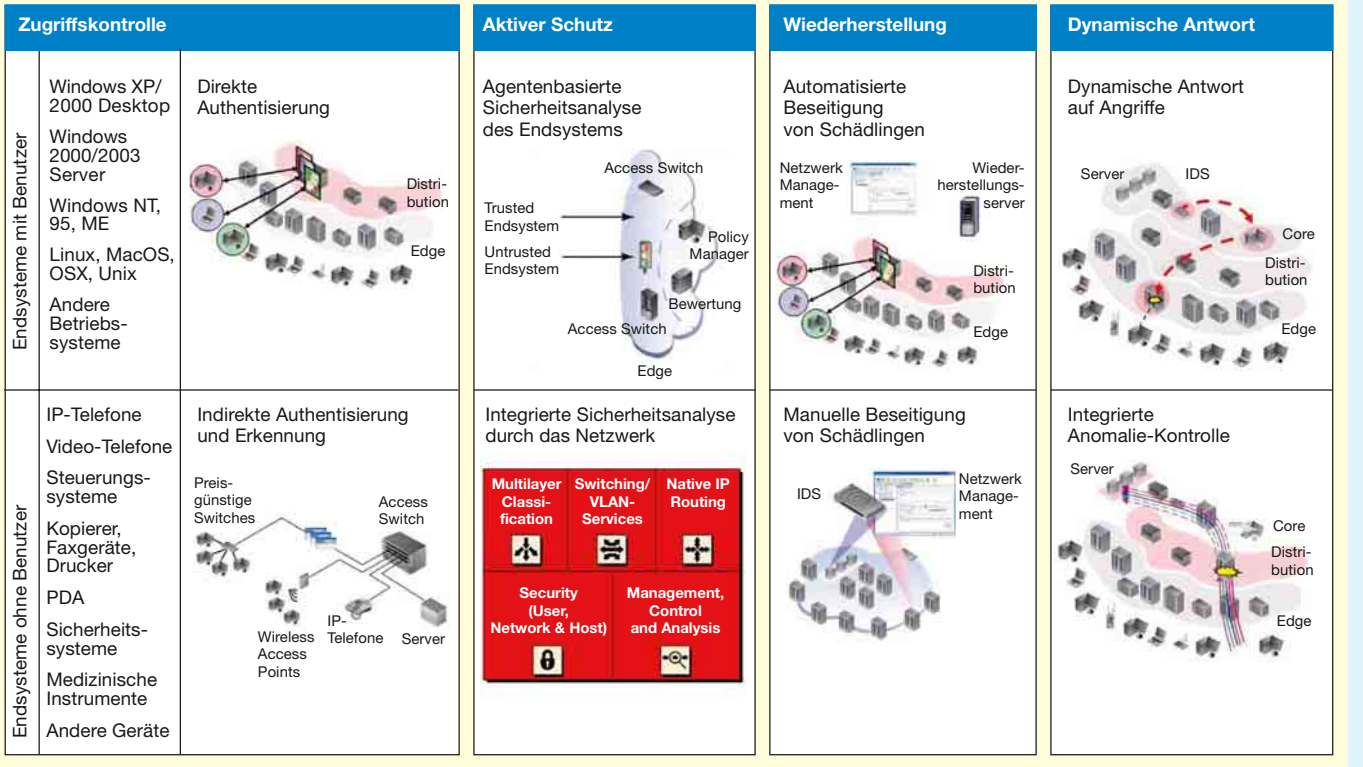
Autor
Dipl.-Ing. *Markus Nispel* ist technischer Direktor der Enterasys Networks GmbH, Frankfurt/Main.

Jedoch haben auch die Bedrohungen durch die Verbreitung des Internets und damit verfügbarer Mittel sowie das Know-how in gleichem Maße zugelegt. Insgesamt registrierten die Computersicherheits-Spezialisten von Sophos 15907 neue Schadprogramme im Jahr 2005 und damit 5183 Schädlinge mehr als im vorherigen Jahr. Vor allem die Zahl der Trojaner, deren Ziel es ist, geheime Daten der PC-Anwender auszuspionieren oder infizierte Rechner zum Versand von Spam-Mails zu missbrauchen, stieg in diesem Jahr drastisch an. Außerdem ergab schon eine Studie von Mummert und Partner im März 2003, dass 66 % aller Attacken von internen Systemen und Zugängen erfolgten. Dieser Trend hält weiter an. Zentrale Firewalls und Virenscanner werden durch Hereintragen von Viren und Würmern auf mobilen Systemen wie Laptops umgangen. Auch die Geschwindigkeit, mit der sich neue Generationen von Würmern und Viren ausbreiten, steigt rasant an. Der Wurm „Code Red“ brauchte im Jahr 2001 beispielsweise noch rund 37 Minuten, um die Anzahl der infizierten Systeme zu verdoppeln. 2003 benötigte sein Artgenosse „SQL Slammer“ dafür nur noch 8,5 Sekunden. Der finanzielle Schaden, den ein sicherheitsrelevanter Vorfall im Durchschnitt verursacht, wurde vom englischen Corporate IT Forum mit rund 240 000 Dollar beziffert – Tendenz steigend.

Sinnvolle Sicherheitskonzepte müssen daher sowohl auf interne als auch auf externe Angriffe vorbereitet sein. Ein ganzheitlicher und skalierbarer Ansatz dafür ist die Ergänzung der zentralen Sicherheitssysteme – meist nur Firewalls und Virenscanner sowie vereinzelt auch Funktionen zur Erkennung von Eindringlingen wie Viren und Würmern (Intrusion Detection System – IDS) – durch:

- verteilte Identitätsprüfung,
- automatisierte Regelvergabe und
- dynamische Antworten bei unbefugten Zugriffen an jedem Ort der Infrastruktur.

All diese Funktionen müssen direkt am Zugangspunkt (Access Switch) der einzelnen Netzwerke (z. B. vom Internet zum LAN)



❶ **Beispiel einer sicheren, offenen Netzwerk-Infrastruktur für den aktiven Schutz gegen typische Bedrohungen**

untergebracht werden, um Sicherheit zu garantieren. Gleiches gilt auch für Mechanismen zur Vergabe von Prioritäten der Anwendungen (Quality of Service – QoS) sowie für die Management- und Überwachungsmöglichkeiten (Monitoring). Ständige Verfügbarkeit mit Notfallvorsorge (Business Continuity) ist nur mit einem redundanten und sicheren Netzwerk zu erreichen, das einzelnen Anwendungen auch die benötigte Bandbreite zur Verfügung stellen kann.

2 Sicheres Telefonieren über IP-Netzwerke

In Systemen, die z. B. Sprach-/Datenintegration konsequent umsetzen, wird das Netzwerk immer mehr zum Kern der gesamten Unternehmenskommunikation und muss entsprechend verfügbar sein. Die Berechnung der Gesamtverfügbarkeit einer getrennten Sprach- und Datenwelt erfolgt wie bei einer Parallelschaltung beider Netze.

Im Gegensatz dazu lässt sich die Gesamtverfügbarkeit eines konvergenten Netzes, bei dem verschiedene Anwendungen das selbe Netzwerk für ihre Dienste verwenden, nur wie bei einer Reihenschaltung ermitteln. Das schwächste Glied der Reihe bestimmt demzufolge die Gesamtverfügbarkeit des Systems. Zusätzlich ist VoIP durch die Verwendung von IP wesentlich anfälliger für Angriffe als traditionelle Telefon-Netze. Diese sind zumeist mit herstellerspezifischer Betriebssystem- und Steuerungssoftware ausgestattet, funktionieren verbindungsorientiert und verwenden keine Broadcast-Mechanismen, bei denen Datenpakete gleichzeitig an alle Teilnehmer übertragen werden.

VoIP hingegen basiert auf einem IP-Netz, das durch das Protokoll selbst sowie durch die gleichzeitige Verwendung dieses Netzes für Datendienste den gängigen Angriffen (z. B. Würmern usw.) ausgesetzt ist. Schädigende Hacking-Tools können direkt angewendet werden, da alle VoIP-Server (Gateways, Communication Server) auf Standard-Betriebssystemen wie Windows und Linux aufsetzen. Die Sicherheitshinweise des CERT (Computer Emergency Response Team) in Bezug auf H.323, ein Protokoll für audiovisuelle Kommunikation in IP-Netzwerken, zeigen dies deutlich [1].

Wie auch im Datenbereich muss ein mehrstufiges Sicherheitskonzept umgesetzt werden, dass sowohl auf VoIP-Anwendungsebene agiert (Verschlüsselung, Authentifizierung und Autorisierung, Schutz der Integrität, Schutz gegen Man-in-the-Middle-Attacke) als auch das Netzwerk selbst sicher und verfügbar macht. Dazu sind einsetzbare Endgeräte und Server-Systeme genau zu analysieren. Im Bild ❶ ist ein Beispiel für eine sichere Netzwerk-Infrastruktur abgebildet, die sich aktiv gegen typische Angriffe (z. B. DHCP-Server-Spoofing, ARP-Spoofing und Source-IP-Spoofing) schützen kann. Ein solches Gesamtsystem sollte so offen gestaltet sein, dass es in Umgebungen mit unterschiedlicher Soft- und Hardware mehrerer Hersteller eingesetzt werden kann. Auch die Nutzung verschiedener Netzarten (LAN, WLAN, WAN, VPN) muss möglich sein. Zusätzlich sollte auf den Serverkomponenten einer VoIP-Lösung ein Überwachungsprogramm installiert sein, das Alarm schlägt, sobald es einen Angriff erkennt (Host IDS/IPS).

Am Backbone muss eine Firewall zusammen mit einem Gerät integriert sein, das einzelne Anwendungen abkapselt und Veränderungen daran vor einer Weitergabe prüft (Application Level Gateway – ALG). Als Backbone oder auch Core wird der zentrale Bereich eines Telekommunikations-Netzwerks bezeichnet, der über sehr hohe Bandbreiten verfügt und meist dazu dient, Netz-

Glossar verwendeter Fachbegriffe der Netzwerktechnik

Access Control Lists (ACL): Zugangskontrollliste, die beinhaltet welcher Benutzer zu welchen Diensten (Dateien, Netzwerkdiensten) Zugang hat

Access Switch: Gerät, das Netzwerkkarten mehrerer (eingebuchter) Endgeräte auf einen Datenbus schaltet und deren Datenaustausch ermöglicht

AES-Verschlüsselung: Standard für Datenverschlüsselung mit frei verfügbarem, lizenzfreien Algorithmus

Agent: Programm, das unabhängig von Benutzereingriffen arbeitet; es löst Aktionen aufgrund eigener Initiative aus (proaktiv); reagiert auf Veränderungen der Umgebung

Any-to-Any-Kommunikation: direkte Kommunikation zwischen verschiedenartigen Teilnehmern

Application Layer Gateway (ALG): Gateway, das einzelne Anwendungen abkapselt und Veränderungen vor der Weitergabe auf Zulässigkeit überprüft, (z. B. Schutz von Applikationen vor unbefugtem Zugriff aus dem Internet)

ARP: Netzwerkprotokoll, das eine Internetadresse zu einer Hardwareadresse zuordnet

ARP-Spoofing: Aussenden gefälschter ARP–Pakete

Authentication: „Authentifizierung"; „Identitätsprüfung"; eindeutige Identifikation gegenüber einem geschützten System durch bestimmte Merkmale; Authentisierung ist Identitätsnachweis

Authentication/Policy Management: Kontrollverfahren für Zugriff auf Netzwerke

Backbone: zentraler Bereich eines Telekommunikationsnetzes, der sehr hohe Bandbreiten besitzt; bezeichnet meist Gelände-Netz, das mehrere Gebäude oder Gebäudeteile verbindet

Backend: Bestandteil einer Software-Anwendung, der die eigentliche Arbeit übernimmt (für verteilte Anwendungen: Programm, das auf Server läuft und die Daten verwaltet)

Broadcast: „Rundruf"; Datenpakete werden von einem Punkt gleichzeitig an alle Netzteilnehmer übertragen

Client: Anwendung, die Dienst eines Servers im Netzwerk in Anspruch nimmt; oft wird Rechner auf dem Client-Anwendung läuft als Client bezeichnet

Core: anderer Begriff für Backbone

DHCP-Server: Server für dynamische Zuweisung von IP-Adressen und weiteren Kommunikationsparametern für Rechner in Netzwerken (z. B. Internet, LAN)

DHCP-Server-Spoofing: Vortäuschen eines falschen DHCP-Servers; durch Angabe falscher Gateway-Adresse zum Internet wird die Kommunikation durch den Rechner des Angreifers geleitet

Distribution: Zusammenstellung von Software die auf eine bestimmte Anwendung abgestimmt ist

DiffServ: „Differentiated Services"; Verfahren zur Priorisierung von IP-Datenpaketen, jedes IP-Paket wird zur Feststellung der Paketwichtigkeit geprüft, danach wird über bevorzugte Weiterleitung zum Empfänger entschieden

DSCP: „Differentiated Services Code Point"; Byte zur Signalisierung der Priorität, so wird jedes IP-Paket einer bestimmten Klasse (Class Selector) und in der Klasse einer Behandlungsstufe (Drop Precedence) zugeordnet

Dynamic Response: dynamische Reaktion bei Zugriff auf das Netzwerk

EAP-TLS, EAP-MD5, EAP-TTLS, PEAP: Authentifizierungsmechanismen für Zugriffskontrolle in Netzwerken

Edge: Netzwerkkomponente, in der mehrere Endsysteme einer Etage oder eines bestimmten Abschnitts zusammengefasst sind

Ethernet: rahmenbasierte Computervernetzungstechnik für lokale Netze

Expedite Forwarding (EF): Weiterleitungsverhalten eines IP-Pakets; bedeutet bevorzugte, unmittelbare Weiterleitung vor allen anderen Paketen

Firewall: System aus Soft- und Hardwarekomponenten, das den Zugriff zwischen verschiedenen Rechnernetzen beschränkt

Gateway/Communication Server: Gerät, das Verbindung und Kommunikation von Netzwerken ermöglicht, die auf verschiedenen Protokollen basieren

H.323: Protokoll zur audiovisuellen Kommunikation in Netzwerken, welche Pakete übertragen

Hacking Tools: Anwendungen, die zum Angriff auf Rechner verwendet werden

HTTP: „Hypertext Transfer Protocol"; Protokoll zur Übertragung von Daten über Netzwerke; zustandsloses Protokoll, d. h. nach der erfolgreichen Datenübertragung wird Verbindung zwischen beiden Kommunikationspartnern nicht aufrecht erhalten

Host IDS/IPS: „Intrusion Detection System"; System zur Erkennung von Angriffen auf ein Computernetz; hostbasiert bedeutet dabei, dass es direkt auf jedem Rechner, der es nutzen soll, installiert sein muss

Hotspot: Bezeichnung eines per Wireless LAN versorgten Bereichs

Hub: „Knotenpunkt" zur Verbindung mehrerer Netzkomponenten; arbeitet auf OSI-Schicht 1 (Bitübertragungsschicht); Signal eines Netzteilnehmers wird an alle anderen weitergeleitet

IEEE 802.1p: Standard zur Priorisierung in Netzwerken; Verwendung spezifizierter Header-Erweiterungen mit Prioritätskennung

IEEE 802.1x: Standard zur Authentisierung in Rechnernetzen; am Netzwerkzugang (physikalischem Port) erfolgt die Authentifizierung, übermittelte Authentizitätsinformationen werden geprüft und Zugriff auf angebotene Dienste gewährt bzw. abgewiesen

Intrusion Detection System (IDS): System zur Erkennung von Eindringlingen wie Viren oder Würmern

IP: „Internet-Protokoll"; Netzwerkprotokoll, das auf OSI-Schicht 3 arbeitet; es ermöglicht die logische Unterteilung von Netzen in Teilnetze und Adressierung einzelner Teilnehmer sowie den Verbindungsaufbau zu Teilnehmern

IT: Abkürzung für Informationstechnik

Jitter: Schwankung der Latenzzeit (Latency) von Datenpaketen

Latency: „Latenzzeit"; Zeitspanne, die Datenpaket im Netzwerk von Sender zu Empfänger benötigt; entsteht durch Laufzeit im Übertragungsmedium sowie Verarbeitungszeit aktiver Komponenten

MAC-Adresse: Hardware-Adresse eines Netzwerkgeräts; dient eindeutiger Identifikation im Netzwerk

Man-in-the-Middle-Attack: Angriff, bei dem der Datenverkehr zwischen mehreren Netzwerkteilnehmern eingesehen und manipuliert werden kann

OSI-Schicht: Schicht des OSI-Referenzmodells: 1. Bitübertragung; 2. Sicherung; 3. Vermittlung; 4. Transport; 5. Sitzung; 6. Darstellung; 7. Anwendung

Peer-to-Peer: Netzwerk-Kommunikation unter gleich berechtigten Teilnehmern; jeder kann gleichzeitig sowohl Client als auch Server sein

Policy: Richtlinie für Zugriffsrechte eines Computers in einem Netzwerk

Port: Anschlussbuchse an Netzwerkkomponenten zum Verbinden untereinander oder zum Anschluss von Endgeräten

Proxy: Dienstprogramm für Computernetze, das im Datenverkehr vermittelt; macht Datentransfer effizienter bzw. schneller und erhöht Sicherheit; aus Sicht des Servers verhält sich Proxy wie Client, Client gegenüber wie Server

Quality of Service (QoS): Dienstgüte; Festlegungen zu Prioritäten der Anwendungen

Quarantine: „Quarantäne"; Abschottung unerwünschter Programme und Dateien

RADIUS: „ Remote Authentication Dial-In User Service"; Client-Server-Protokoll zur Authentifizierung und Autorisierung von Benutzern bei Einwahlverbindungen in Computernetzwerke

Rate Limiting: Beschränken verfügbarer Bandbreite einzelner Anwendungen zur Regulierung des Datenverkehrs

Remediation: Wiederherstellung

Remote Procedure Call (RPC): Netzwerkprotokoll auf fünfter und teilweise sechster Schicht des OSI-Referenzmodells; ermöglicht Funktionsaufrufe auf entfernten Rechnern über Netzwerk

RTP: „Real-Time Transport Protocol"; Protokoll zur kontinuierlichen Übertragung audiovisueller Daten (Streams) über IP-basierte Netzwerke; wird normalerweise über UDP betrieben

Server: Anwendung, die nach Anfrage Kontakt mit Client aufnimmt und mit ihm Daten austauscht oder ihm einen Dienst bereitstellt; oft wird Rechner, auf dem Serverprogramm läuft auch als Server bzw. Host bezeichnet

SHA-1-Datenintegrität: Schutz vor Beeinträchtigungen und Manipulation von Daten beim Austausch großer Dateien, die für den Transport in kleinere Teilsequenzen unterteilt wurden

SIP-Registrierung: „Session Initiation Protocol"; Netzprotokoll zum Aufbau einer Kommunikationssitzung zwischen zwei und mehr Teilnehmern

Source-IP-Spoofing: Aussenden von Paketen mit gefälschter Quell-IP-Adresse

SRTP: „Secure Real-Time Transport Protocol"; paketbasiertes Protokoll zur sicheren, kontinuierlichen Übertragung von audiovisuellen Daten (Streams) über IP-basiertes Netzwerke; wird normalerweise über UDP betrieben; dient dazu, Multimedia-Datenströme über Netzwerk zu transportieren

Storage over IP: netzwerkgebundene Speicherlösung; Datentransport über IP

Subnet: Teilnetz; entsteht durch Unterteilung aller möglichen IP-Adressen; logische Unterteilung des Netzes in Subnetze; entspricht meist physischer Unterteilung in lokale Teilnetze

Switch: Gerät zur Verbindung mehrerer Computer oder Netzteilnehmer innerhalb von lokalem Netz (LAN); arbeitet auf OSI-Schicht 2 (Sicherungsschicht); wird als „intelligentes Hub" bezeichnet

Threat Assessment: Bedrohungs-Abschätzung; Beurteilung eines schädlichen Programms oder infizierter Datei

Trusted Endsystem: „vertauenswürdiges Endsystem"; das System verarbeitet nur Anwendungen und Daten, die für seine jeweilige Funktion nötig sind; Benutzer können mit Anwendungen bzw. Daten nicht beliebig verfahren

UDP: „User Datagram Protocol"; minimales, verbindungsloses Netzprotokoll; durch IP-Schicht hergestellte Endsystemverbindung wird um eine Anwendungsschnittstelle (Port) erweitert

URL: „Uniform Resource Locator"; identifiziert Ressource über primären Zugriffsmechanismus (oft HTTP) und Ort der Ressource im Computernetzwerk

VLAN: „Virtual Local Area Network"; virtuelles lokales Netzwerk innerhalb eines physikalischen Netzwerks

VPN: „Virtuelles Privates Netzwerk": Computernetz, das zum Transport von privaten Daten ein öffentliches Netz (z. B. Internet) nutzt

Wake-on-LAN: Standard, um einen ausgeschalteten Computer über seine eingebaute Netzwerkkarte zu starten

WAN: „Wide Area Network"; Netzwerk, das sich über großen geografischen Bereich erstreckt; Verbindung einzelner LAN auf OSI-Schicht 1

werke einzelner Gebäude oder Gebäudeteile zu verbinden.
Als weiterer Baustein für Sicherheit im Bereich VoIP ist zum Beispiel das Protokoll SRTP (Secure Real Time Protocol) zu nennen. Es dient der kontinuierlichen Übertragung audiovisueller Datenpakete über IP-Netzwerke und erhöht dabei die Datensicherheit durch verschiedene Verschlüsselungstechniken (AES-Verschlüsselung und SHA-1-Datenintegrität). Geräte für virtuelle Netzwerke (VPN) sollten Verschlüsselung in der Hardware unterstützen, damit kein zusätzlicher zeitlicher Verzug bei größeren Entfernungen (z. B. im WAN) entsteht. Ausführliche Tests haben gezeigt, dass VoIP so auf der Netzwerkseite ohne Qualitätsverlust verschlüsselt werden kann.

3 Elemente des Sicherheitskonzepts

3.1 Identitätsprüfung

Der Identitätsprüfung (Authentifizierung) aller am Netzwerk angeschlossenen Teilnehmer kommt eine zentrale Bedeutung zu. Da nie von einer Umgebung ausgegangen werden kann, in der alle Teilnehmer den Standard zur Authentisierung in Netzwerken (IEEE 802.1x) verwenden, sollte der Access Switch diverse Authentifizierungsmethoden gleichzeitig pro physikalischem Zugang (Port) unterstützen (z. B. Drucker, Sicherheitskameras, externe Personen, Besucher usw.). Ist dies nicht der Fall, wird die Umsetzung eines Zugriffskontrollverfahrens (Authentication/Policy-Management) nahezu unmöglich. Es sollten auch mehrere Nutzer pro Port unterstützt werden (z. B. Mini-Switches oder PC/Telefon-Kombinationen), denen sich dann unterschiedliche Richtlinien für Zugriffsrechte (Policy) zuordnen lassen. Einsetzbare Authentisierungsmethoden sind:

- portbasierte Authentisierung mit dem Standard IEEE 802.1x über digitale Zertifikate, biometrische Verfahren, Nutzer-Passwort bzw. einmaliges Passwort (One-Time-Password – OTP); Authentisierungsmechanismen sind z. B. EAP-TLS, PEAP, EAP-MD5, EAP-TTLS
- Authentisierung über die physikalische Hardware-Adresse (MAC-Adresse) des Endgeräts durch den Server für die Einwahl in das Netzwerk (RADIUS-Server)
- netzbasierte Authentisierung über Ortsangabe der Ressource im Netzwerk (URL redirect) auf lokalem HTTP-Server, der im Switch integriert ist und der Datenübertragung dient; danach via Einwahl-Server (RADIUS) ähnlich wie bei WLAN-Hotspot
- automatische Erkennung von Endsystemen wie IP-Telefonen (Convergence End-point Detection – CEP) mit dem Protokoll H.323 oder mit dem Protokoll zur Verwaltung von Kommunikationssitzungen (Session Initiation Protocol – SIP); es gibt herstellerspezifische Unterstützung
- Freischaltung einer Basisfunktionalität ohne Authentisierung (Default Authentication Role); z. B. zum Starten eines ausgeschalteten Computers über die eingebaute Netzwerkkarte (Wake-on-LAN) u. ä.

Die Authentisierung sollte vollkommen auf Standards beruhen, z. B. auf RADIUS, dem Protokoll zur Authentisierung bei Einwahl ins Netzwerk, das vom Datenverwaltungsprogramm auf dem Server, dem so genannten Backend, verwendet wird. Das ermöglicht den Einsatz beliebiger Serversysteme im Backend (z. B. Microsoft ADS, Novell NDS, Linux, Siemens DirX). Daraus ergibt sich nun wiederum die einfache Integration in Sicherheitssysteme für Einzelrechner wie ZoneLabs (jetzt Checkpoint) und Sygate (jetzt Symantec). Bei Einwahl in das Netzwerk wird dann nicht nur der Benutzer am zentralen RADIUS-Sever authentisiert, sondern auch die Hardwarekonfiguration des verwendeten Endsystems über einen Software-Agenten kontrolliert (Bild ❷). Es sollte aber auch eine Lösung ohne Agenten vorgesehen werden.

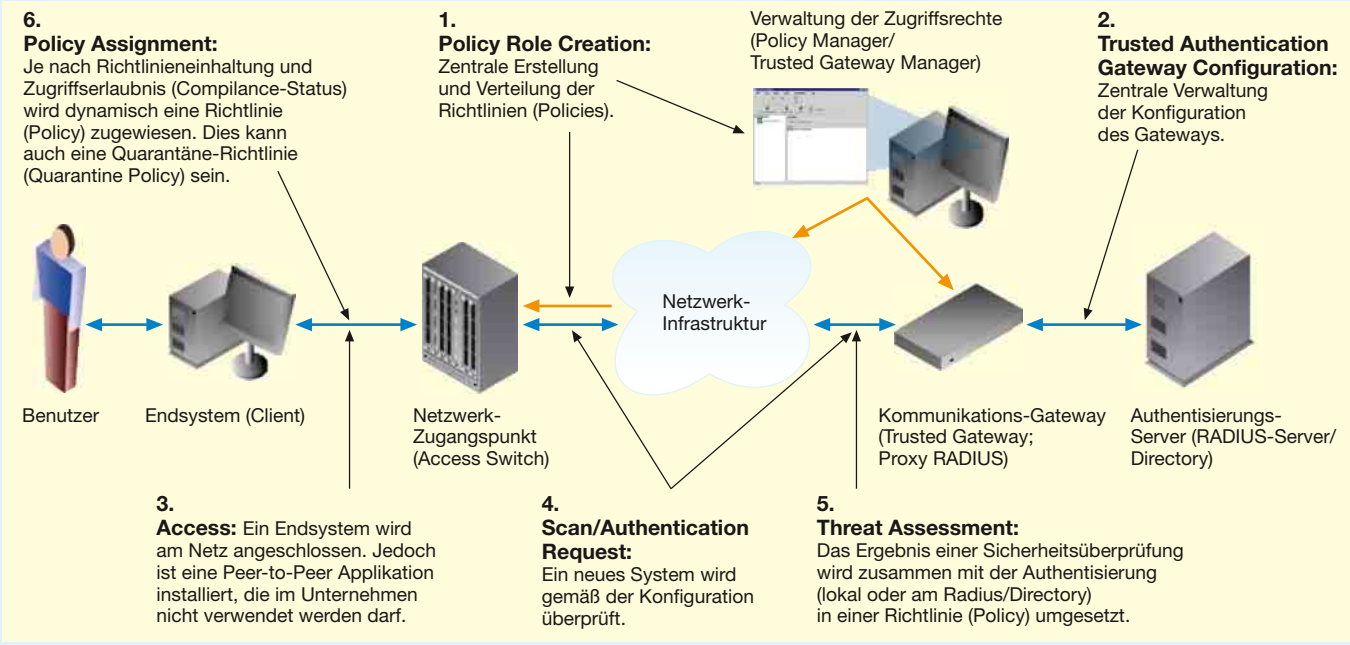
3.2 Verwaltung der Zugriffsrechte

Sicherheits- und QoS-Richtlinien (Policies) sollten den einzelnen Endsystemen nach der Authentisierung automatisch zugewiesen werden. Damit ist eine präzise, sicherheitsrelevante Einstufung der Endsysteme bzw. die Zuweisung von entsprechenden Service-Qualitäten möglich, ohne jedoch den Verwaltungsaufwand zu erhöhen. Die jeweiligen Policies pro Endsystem können bestehen aus:

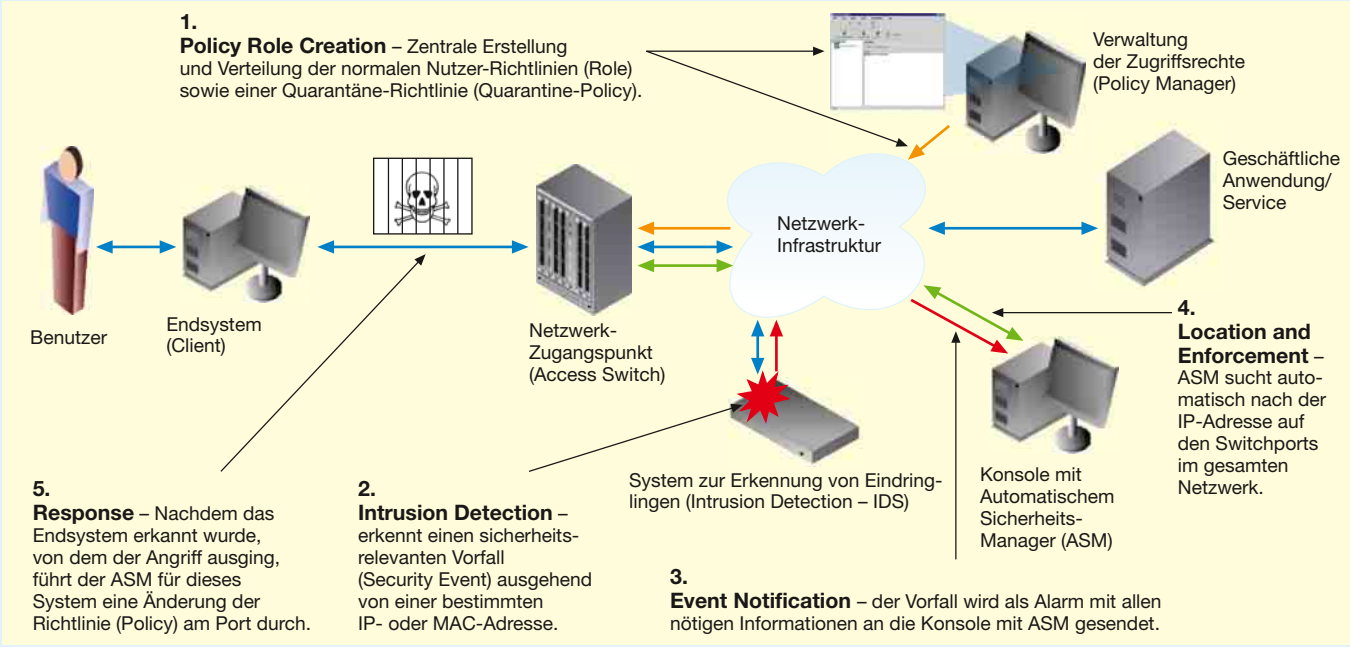
- Zuweisungen für ein virtuelles lokales Netzwerk (VLAN)
- Zuweisungen für die Zugangskontrollliste (Access Control Lists – ACL)
- Prioritätszuweisung (QoS)
- Beschränkung der verfügbaren Bandbreite (Rate Limiting)

Dazu kommt eine Zusatzklassifizierung auf den OSI-Schichten 2, 3 und 4 zur Unterscheidung von Protokollen, IP-Teilnetzen (Subnets), Prioritäts-Signalisierungen (DiffServ) und Anwendungen pro Benutzer.

Zugangskontrollliste (ALC). Diese Funktion bietet die Möglichkeit, Benutzergruppen im gleichen Teilnetz (Subnet) ohne den Aufbau virtueller Netzwerke (VLAN) zu trennen. Das Entfallen einer VLAN-Struktur bietet einen geringeren Verwaltungsaufwand und wesentliche Verbesserungen in der Netzstruktur, da keine OSI-Schicht-2- bzw. VLAN-Dienste über das gesamte Netz gebrückt werden müssen. Die Skalierbarkeit großer gebrückter Netze, die auf OSI-Schicht 2 basieren, ist begrenzt. Außerdem ist es durch die dynamische Natur der Zugangskontrolllisten möglich, die traditionellen, statischen Zugangslisten abzulösen. Dadurch entfällt der Verwaltungsaufwand bei Umzügen der Endsysteme innerhalb des Netzwerks (Change Management).



❷ **Schematische Darstellung zur Authentisierung mit Hilfe eines Software-Agenten**



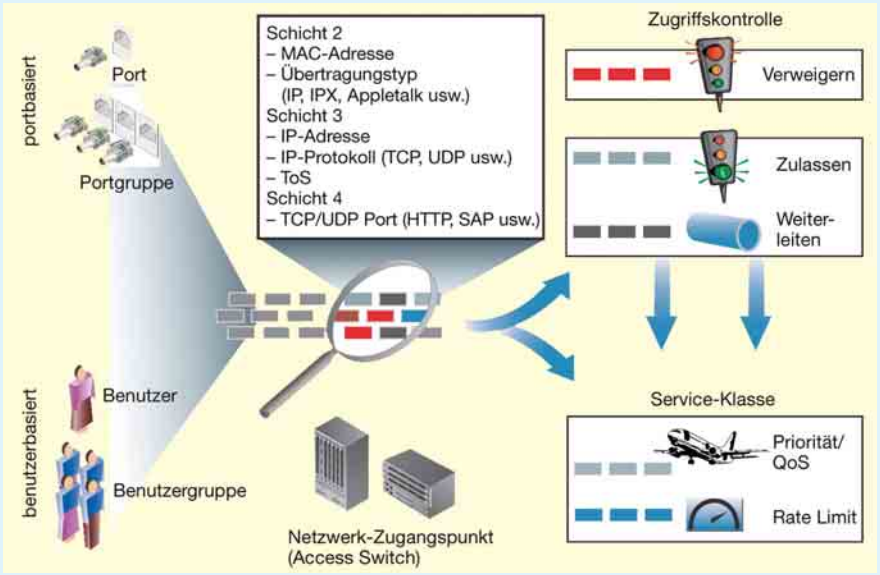
❸ **Schematische Darstellung eines Konzepts zum dynamischen Schutz vor unerwünschten Programmen, Dateien und unbefugten Benutzereingriffen**

3.3 Dynamische Reaktion auf Bedrohungen

Wie eingangs erwähnt, sollte das Netz am Access Switch in der Lage sein, aktiv auf neue Bedrohungen zu reagieren – direkt an jedem Eingangspunkt der Infrastruktur. Nur so kann z. B. die Ausbreitung von Würmern unterbunden werden. Andere Sicherheitsmechanismen wie zentrale Firewalls greifen hier nicht ausreichend. Als Beispiel dient die im Bild ❸ dargestellte Lösung von Enterasys. Das eingesetzte Zugriffskontrollverfahren (Authentication/Policy-Management) ist mit dem hauseigenen System zum Schutz vor Eindringlingen (IDS) verbunden. Dadurch sind am Access Switch nun Funktionen der OSI-Schichten 4 bis 7 verfügbar, und es ist möglich, auch auf komplexe Angriffe auf Anwendungsebene (z. B. Microsoft Remote Procedure Call) zu antworten. Die IT-Organisation ist so in der Lage, direkt sowie voll- oder halbautomatisch auf Angriffe zu reagieren.

3.4 Prioritäten der Anwendungen

Zur Sicherheit in konvergenten Netzen gehört auch die Bereitstellung von Bandbreite für die einzelnen Anwendungen. Einer reine OSI-Schicht-2-Funktionalität im Switch genügt den Anforderungen einer konvergenten Infrastruktur nicht. Beim gemeinsamen Einsatz von VoIP und anderen Anwendungen ist eine Priorisierung mit Hilfe eines virtuellen lokalen Netzwerks (VLAN) oder des Standards zur Priorisierung in Netzwerken (IEEE 802.1p) nicht ausreichend. Viele der möglichen Anwendungen können typischerweise nur aufgrund von Informationen aus OSI-Schicht 4 unterschieden werden – der Switch muss dies daher auch unterstützen.



❹ Automatische Erkennung eines Endgeräts und Zuweisung entsprechender Zugriffsrechte
Quellen: Enterasys

Bei VoIP und anderen Anwendungen auf Basis eines Echtzeit-Protokolls (RTP/UDP) ist dies noch etwas komplizierter. Die Ports der OSI-Schicht 4, die zur Sprachübertragung dienen, werden dynamisch ausgehandelt. Daher kann hier nur die Information aus OSI-Schicht 3 (Standard DiffServ – DSCP DiffServ Code Point, TOS Byte) ausgewertet werden. Hingegen sind Protokolle der OSI-Schicht 2 wie IEEE 802.1p nicht durchgängig nutzbar. Ein Beispiel dafür sind die als Softphones bezeichneten Programme, durch die der PC in Verbindung mit einem Mikrofon und einem Lautsprecher für VoIP nutzbar ist. Sie unterstützen Schicht-2-Protokolle typischerweise nicht. Daher ist ein Byte zur Signalisierung nötig, das mit jedem Paket mitgesendet wird (DSCP). Der Wert dieses Bytes wird jedoch vom Endsystem gesetzt.

Um zu garantieren, dass auch nur VoIP mit hoher Priorität (z. B. DSCP-Wert „EF“ = Expedite Forwarding = übergeordnete Weiterleitung) übertragen wird, kommt die Beschränkung der Bandbreite einzelner Anwendungen (Rate Limiting) zum Einsatz, um den Datenverkehr zu regulieren. Damit werden dann zwar geringe Latenzzeiten (Latency) mit nur kleinen Schwankungen (Jitter) für die Serviceklasse „EF“ garantiert, aber auch nur limitierte Bandbreite bereitgestellt. Dadurch hat eine absichtliche oder unabsichtliche Fehlkonfiguration auf einem Endsystem, die versucht einen Datentransfer über „EF“ abzuwickeln, keinen Einfluss auf die Servicequalität anderer VoIP-Verbindungen.

Vorteil und Fluch zugleich ist die Tatsache, dass Voice over IP die direkte Kommunikation verschiedenartiger Teilnehmer (Any-to-Any-Kommunikation) möglich macht und die Endsysteme beliebig umziehen können. Für ein effektives Management des Netzes sollte der Access Switch daher in der Lage sein, ein Endgerät automatisch zu erkennen und nachfolgend auch die Zuweisung der Zugriffsrechte durchzuführen.

Bei Enterasys ist diese Funktion unter CEP (Convergence Endpoint Detection) realisiert (Bild ❹). Dabei sollte auch z. B. herstellerspezifische Unterstützung vorhanden sein. Ein Switch muss in der Lage sein, nicht nur authentisierten Nutzer und Konvergenz-Endpunkte zu erkennen (CEP), sondern auch angeschlossene MAC-Adressen und deren (IP-) Adressen aus OSI-Schicht 3 dynamisch zu erlernen (Node and Alias Discovery).

Dadurch ist der Netzwerk-Verantwortliche (Administrator) in der Lage, jeden Nutzer anhand beliebiger Parameter zu lokalisieren. Im Fehlerfall also ein nützliches Werkzeug, das die Fehlerfindung erleichtert und die Zeit zur Wiederherstellung minimiert.

4 Fazit

Sicherheit in konvergenten Netzen bietet nur ein mehrstufiges Konzept. Dabei muss die Netzwerk-Infrastruktur redundant und sicher sein sowie den Anwendungen die jeweils benötigten Bandbreiten garantieren. Nur dann kann eine konvergente Lösung richtig funktionieren. Dies entbindet den Anwender jedoch nicht davon, auch auf Anwendungs- und Organisationsebene weitere Sicherheitsfunktionen vorzusehen.

Literatur

[1] CERT Advisory CA-2004-01 Multiple H.323 Message Vulnerabilities
[2] Wikipedia: Rechnernetz.
In: de.wikipedia.org/wiki/Rechnernetz
[3] Wikipedia: Netzwerksicherheit.
In: de.wikipedia.org/wiki/Netzwerksicherheit