Firewall-Grundlagen

› Sobald zwischen dem lokalen Netz und dem Internet eine Verbindung besteht, können Angreifer versuchen, Daten zu stehlen oder das Netz lahm zu legen. Verschiedene Firewall-Konzepte sorgen für Sicherheit.

› VON PETER KLAU

Die Sicherheit steht an erster Stelle, wenn das private Netzwerk eines Unternehmens (LAN) mit dem Internet verbunden ist. Eine zunehmende Anzahl von Mitarbeitern braucht Zugang zu Internet-Diensten wie dem WWW, E-Mail, FTP und Remote-Verbindungen (Telnet, SSH). Unternehmen wollen zudem für ihre Webseiten und FTP-Server den öffentlichen Zugang über das Internet ermöglichen. Dabei muss die Sicherheit der privaten Netze gegenüber unautorisierten Zugriffen von außen gewährleistet sein. Der Administrator muss das lokale Netzwerk gegen das große Chaos "Internet" abschirmen, damit Daten nicht in unbefugte Hände geraten oder gar verändert werden. Für Firmen, die vom Internetzugang abhängig sind, stellen auch die sogenannten DoS-Attacken eine große Gefahr dar.

Mit Firewalls lassen sich Netzwerke gegen unbefugte Zugriffe von außen absichern. Die verfügbaren Lösungen reichen von der Zusatzsoftware bis hin zu speziellen Geräten, die ausschließlich auf diese Aufgabe ausgelegt sind. In ihrer grundlegenden Funktionsweise unterscheiden sich die Systeme allerdings nur wenig.

› Definition einer Firewall

Eine Firewall besteht aus einer Gruppe von Netzwerkkomponenten (Hard- und Software) an der Schnittstelle zweier Netze. Sie gewährleistet die Einhaltung von Sicherheitsrichtlinien zwischen einem privaten und einem öffentlichen (nicht sicheren) Netz, wie zum Beispiel dem Internet. An dieser "Brandschutzmauer" entscheidet sich, auf welche Dienste innerhalb des privaten Netzes zugegriffen werden kann und welche Dienste des nicht sicheren Netzes aus dem privaten Netz heraus nutzbar sind. Damit eine Firewall effektiv arbeiten kann muss entsprechend der gesamte Datenverkehr zwischen dem privaten Netz und dem Internet über diese Station laufen. Die Firewall untersucht alle Pakete und lässt nur die unverdächtigen passieren.

Dabei muss die Firewall ihrerseits immun gegen Eindringlinge sein. Was würde eine Firewall nutzen, wenn Hacker sie nach Belieben anpassen könnten? Daraus lässt sich eine "Schwäche" von Firewalls ableiten: Diese Systeme bieten leider keinen Schutz, sobald es einem Angreifer gelungen ist, sie zu überwinden. Daher ist auf die eigene Sicherheit der Firewall ebenso viel Augenmerk zu legen wie auf die Sicherheit des privaten Netzes selbst, die durch die Firewall gewährleistet werden soll.

Eine Firewall ist nicht wie ein Router, ein Bastion-Host oder ein anderes Gerät Teil des Netzes. Sie ist lediglich eine logische Komponente, die ein privates Netz vor einem öffentlichen Netz schützt. Ohne eine Firewall wäre jeder Host im privaten Netz den Attacken von außen schutzlos ausgeliefert. Das bedeutet: Die Sicherheit in einem privaten Netz wäre von der Unverwundbarkeit der einzelnen Rechner abhängig und somit nur so gut wie das schwächste Glied im Netz.

› Zentraler Sicherheitsknoten

Der Vorteil einer zentralen Firewall ist, dass sie das Sicherheitsmanagement vereinfacht. Damit gilt die von ihr hergestellte Sicherheit für das gesamte Netz und muss nicht für jeden Rechner einzeln definiert werden. Die Überwachung geschieht ebenfalls zentral über die Firewall. So kann sie gegebenenfalls auch einen Alarm auslösen, da Angriffe von außen nur über diese definierte Schnittstelle zwischen den Netzen erfolgen können.

Das Erkennen eines Angriffs ist der erste Schritt zur Abwehr des Angreifers.

Als in den letzten Jahren die Internet-Adressen knapp wurden, trat auch in Unternehmen eine Verknappung von IP-Adressen (http://www.tecchannel.de/internet/209/index.html) ein. Eine Internet-Firewall ist in diesem Zusammenhang die geeignete Stelle zur Installation eines Network Address Translators (NAT), der die Adressenknappheit lindern kann. Und schließlich eignen sich Firewalls auch, um den gesamten Datenverkehr von und zum Internet zu überwachen. Hier kann ein Netzwerk-Administrator auch Schwachstellen und Flaschenhälse erkennen.

› Nachteile und Begrenzungen

Eine Firewall kann keine Angriffe abwehren, wenn die Pakete nicht durch sie hindurch geleitet werden. Wenn zum Beispiel eine Einwählverbindung via Modem oder ISDN aus dem geschützten Netzwerk besteht, können interne Benutzer eine direkte PPP-Verbindung zum Internet aufbauen. Benutzer, welche die zusätzliche Authentifizierung am Proxy-Server scheuen, werden schnell diesen Weg nehmen. Durch die Umgehung der Firewall erzeugen sie jedoch ein großes Risiko für eine Backdoor-Attacke.

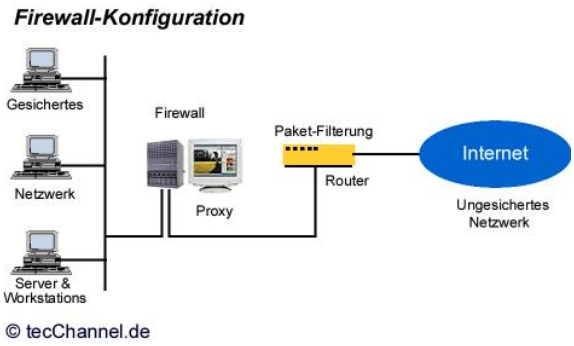
Firewalls nützen nichts bei Angriffen aus den eigenen Reihen. Sie hindern niemanden daran, sensitive Daten auf eine Diskette zu kopieren und sie außer Haus zu schaffen. Erst recht nicht, wenn diese Person weit reichende Rechte hat oder durch Diebstahl an Passwörter gelangt ist. Firewalls schützen auch nicht vor Computerviren oder Trojanern, da sie nicht jedes Datenpaket nach potenziellen Viren durchsuchen können. Auch sogenannte Data-driven Attacks können Firewalls nicht verhindern. Dabei handelt es sich um scheinbar harmlose Daten mit verstecktem Code zur Änderung von Sicherheitseinstellungen.

Zudem muss die Firewall leistungsfähig genug sein, um den Datenstrom analysieren zu können. Je schneller die Internetanbindung, desto mehr Pakete fließen pro Sekunde in und aus dem Netzwerk. Soll die Firewall zudem noch die Datenströme - also nicht nur die einzelnen Pakete, sondern auch den logischen Datenfluss - überwachen, ist ein umso leistungsfähigeres System erforderlich.

› Komponenten einer Firewall

Ein Firewall-System kann aus ein bis drei Komponenten bestehen:

- › Paketfilterungs-Router
- › Proxy-Server (Application Level Gateway)
- › Verbindungs-Gateway (Circuit Level Gateway)



Firewall-Konfiguration: Hier mit Paketfilterungs-Router und einem Proxy-Server.

Grundsätzlich konkurrieren zwei Firewall-Konzepte: die "passive" Paketfiltertechnologie und die "aktiven" Application Level Gateways. Alle anderen Firewall-Systeme sind Varianten und Weiterentwicklungen dieser beiden Konzepte oder werden damit kombiniert. Dazu gehören etwa das Stateful Packet Filtering, Circuit Level Gateways oder

sogenannte Hybrid-Firewalls. Diese neueste Variante stellt eine Kombination aus Paketfilter und Application Level Gateway dar.

› Paketfilterungs-Router

Ein Paketfilterungs-Router entscheidet bei jedem Datenpaket anhand festgelegter Filterregeln, ob er es weiterleitet oder nicht. Überprüft werden Header-Informationen wie:

- › IP-Ursprungsadresse
- › IP-Zieladresse
- › das eingebettete Protokoll (TCP, UDP, ICMP, oder IP Tunnel)
- › TCP/UDP-Absender-Port
- › TCP/UDP-Ziel-Port
- › ICMP message type
- › Eingangsnetzwerkschnittstelle (Ethernetkarte, Modem, etc.)
- › Ausgangsnetzwerkschnittstelle

Falls das Datenpaket die Filter passiert sorgt der Router für die Weiterleitung des Pakets, andernfalls verwirft er es. Wenn keine Regel greift, verfährt der Paketfilterungs-Router nach den Default-Einstellungen.

Anhand der Filterregeln kann ein Router auch eine reine Service-Filterung durchführen. Auch hier muss der Systemadministrator die Filterregeln vorher definieren. Service-Prozesse benutzen bestimmte Ports (Well Known Ports), wie zum Beispiel FTP den Port 21 oder SMTP den Port 25. Um beispielsweise den SMTP-Service abzublocken, sondert der Router alle Pakete aus, die im Header den Ziel-Port 25 eingetragen haben oder die nicht die Ziel-IP-Adresse eines zugelassenen Hosts besitzen.

Einige typische Filterrestriktionen sind:

- › Nach außen gehende Telnet-Verbindungen sind nicht erlaubt.
- › Telnet-Verbindungen sind nur zu einem bestimmten internen Host erlaubt.
- › Nach außen gehende FTP-Verbindungen sind nicht erlaubt.
- › Pakete von bestimmten externen Netzwerken sind nicht erlaubt.

› Abwehr von Angriffen

Bestimmte Angriffstypen verlangen eine vom Service unabhängige Filterung. Diese ist jedoch schwierig umzusetzen, da die dazu erforderlichen Header-Informationen Service-unabhängig sind. Die Konfiguration von Paketfilterungs-Routern kann auch gegen diese Art von Angriffen erfolgen, für die Filterregeln sind jedoch zusätzliche Informationen notwendig. Beispiele für diese Angriffe sind:

Source IP Address Spoofing Attacke

Bei einer Spoofing-Attacke fälscht der Angreifer die IP-Absenderadresse eines Datenpakets und verwendet stattdessen die Adresse eines Rechners im internen Netz. Die Firewall kann einen solchen Angriff erkennen, indem sie überprüft, ob ein von außen kommendes Paket eine interne Adresse nutzt. Um den Angriff abzuwehren, sind solche Pakete entsprechend herauszufiltern.

Source Routing Attacke

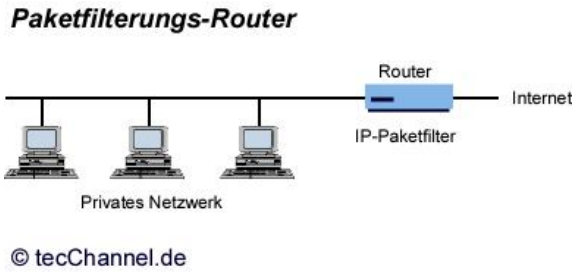
Bei einer Source Routing Attacke gibt der Angreifer die konkrete Route vor, die ein Datenpaket nehmen soll, um Sicherheitsmaßnahmen zu umgehen. Das Verfahren zum Source Routing ist zwar im TCP/IP-Standard vorgesehen, kommt jedoch kaum noch zum Einsatz. Deshalb kann die Firewall die Pakete mit diesem Flag bedenkenlos verwerfen.

Tiny Fragment Attacke

Bei dieser Angriffsform erzeugt der Hacker extrem kleine Datenpakete, von denen nur das erste den TCP-Header enthält. Das soll den Router veranlassen, nur das erste Fragment zu prüfen und die restlichen ungeprüft durchzulassen. Dies erlaubt dem Hacker, die gewünschten Befehle ins Netz zu schmuggeln. Als Abwehr kann die Firewall alle Pakete verwerfen, bei denen das Feld Fragment-Offset (http://www.tecchannel.de/internet/209/4.html) auf eins gesetzt ist.

› Vorteile von Paketfilterungs-Routern

Die Mehrzahl der Firewall-Systeme setzen nur einen Paketfilterungs-Router ein. Außer der Zeit, die für die Planung der Konfiguration des Routers erforderlich ist, entstehen keine weiteren Kosten, denn die Filtersoftware ist Bestandteil der Router-Software. Um den Datenverkehr zwischen privatem und öffentlichem Netz nicht zu stark einzuschränken, sind von Haus aus nur sehr moderate und wenige Filter definiert. Die Paketfilterung ist im Allgemeinen durchlässig für Benutzer und Applikationen. Sie erfordert zudem kein spezielles Training und keine zusätzliche, auf den einzelnen Rechnern installierte Software.



Einfache Sicherung: Hier schützt nur ein Paketfilterungs-Router das Netzwerk.

Nachteile

Doch die Paketfilterung hat auch Nachteile. So ist neben detaillierten Protokollkenntnissen für eine komplexe Filterung auch eine lange Regelliste notwendig. Derartige Listen sind sehr aufwändig und daher schwer zu verwalten. Es ist zudem schwierig, die Filter auf Wirksamkeit zu testen. Auch sinkt der Router-Durchsatz, wenn zu viele Filter definiert sind.

Daneben können Hacker die Firewall durch Tunneln der Pakete überwinden, wobei ein Paket vorübergehend in einem anderen gekapselt wird. Und schließlich: Data-driven-Attacken kann der Router nicht erkennen.

› Proxy-Server

Ein Proxy-Server (engl. Proxy: Stellvertreter, Bevollmächtigter), auch Application Level Gateway genannt, erlaubt dem Netzwerk-Administrator die Installation von strengeren Sicherheitsregeln als dies bei einem Paketfilterungs-Router möglich ist. Der Server dient als sicheres Gateway zwischen einem privaten und einem öffentlichen (ungesicherten) Netz. Als Gateway bezeichnet man entweder die Software, die eine Verbindung zwischen zwei Netzwerken herstellt, oder den Computer, auf dem diese Software ausgeführt wird.

Ein Proxy-Server dient nebenbei zur Zwischenspeicherung von Web-Inhalten und kann als erweiterbare Firewall verwendet werden. Das ermöglicht gleichzeitig Datensicherheit und einen schnelleren Zugriff auf Internetinhalte. Der Proxy hat dabei zwei Gesichter: Für den lokalen Client operiert er beim Abruf eines Web-Dokuments wie ein Webserver. Gegenüber dem entfernten Internet-Server tritt er wie ein Webclient auf. Proxy-Server sprechen aber nicht nur HTTP, sondern beherrschen auch Dienste wie FTP, POP3 oder IRC - allerdings abhängig vom jeweiligen Produkt. Da sie als einziger Knotenpunkt zwischen lokalem und globalem Netz geschaltet sind, schützen sie zudem die lokalen Clients. Denn nur der Proxy-Server ist Angriffen von außen ausgesetzt. Die Clients liegen "unsichtbar" hinter ihm.

Vorteile eines Proxy-Servers

Das Betriebssystem auf Client-Seite spielt prinzipiell keine Rolle. Nur spezielle Funktionen wie beispielsweise eine automatische Konfiguration der Clients oder das Trennen einer Internet-Verbindung vom Client funktionieren lediglich von Windows-Clients aus.

Daneben lässt sich für jeden Dienst wie FTP oder HTTP ein separater Proxy einrichten. Unerwünschte Dienste filtert der Proxy heraus. Zudem findet kein direkter Paketfluss zwischen internen und externen Rechnern statt.

› Bastion-Host

Unter einem Bastion-Host versteht man einen besonders gesicherten Rechner, der wie eine Festung wirken soll. Er schützt die Rechner im privaten Netz vor Angriffen von Außen. Wie bei einer Festung gibt es nur einen Ein- und Ausgang, der ständig bewacht ist und bei Bedarf sofort geschlossen werden kann. Die Überwachung des Aus- und Eingangs übernimmt meist ein Router als Paketfilter. Bastion-Hosts sind von ihrer Art her damit die gefährdetsten Rechner in einer Firewall. Auch wenn sie in der Regel mit allen Mitteln geschützt sind, sind sie häufigstes Ziel eines Angriffs, da ein Bastion-Host als einziges System Kontakt zur Außenwelt unterhält.

Die Rechner im privaten Netz sind aus dem Internet nicht direkt erreichbar und dadurch unsichtbar. Andersherum ist auch das Internet nur über den Bastion-Host zugänglich. Deshalb ergibt sich für diesen Rechner die logische Grundhaltung: je einfacher der Bastion-Host aufgebaut ist, desto leichter ist er zu schützen. Denn jeder auf dem Bastion-Host angebotene Dienst kann Software- oder Konfigurationsfehler enthalten. Bei minimalen Zugriffsrechten sollte der Bastion-Host gerade so viele Dienste anbieten, wie er für die Rolle als Firewall unbedingt braucht.

Bastion-Hosts werden in unterschiedlichen Architekturen installiert, wie zum Beispiel als Dual-Homed-Host, in Kombination mit einem Überwachungs-Router.

› Vorteile eines Bastion-Hosts

Ein Bastion-Host lässt sich so einrichten, dass Dienste nur über eine Authentifizierung abrufbar sind. Zudem kann der Administrator spezielle Bestandteile dieser Dienste komplett abschalten, etwa den PUT-Befehl für FTP-Server. Die voneinander unabhängigen Proxy-Dienste laufen unter einer unprivilegierten Benutzerkennung in separaten, gesicherten Verzeichnissen, so dass ein Angriff über diese Dienste nur schwer möglich ist. Alle anderen Dienste wie SMTP oder HTTP sind auf diesem Rechner komplett abgeschaltet und stellen somit keine Sicherheitslücke dar. Im Bedarfsfall kann der Administrator auch den kompletten Datenverkehr überwachen, um Angreifer zu erkennen.

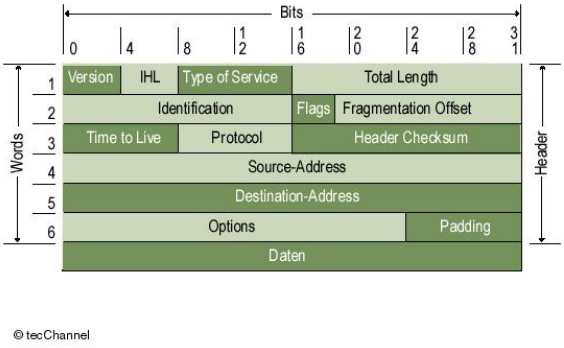
Nachteile von Bastion-Hosts

Bei bestimmten Diensten, wie etwa Telnet oder FTP müssen sich die Benutzer zweimal einloggen: Einmal auf dem Proxy des Bastion-Hosts und danach auf dem eigentlichen Server. Zudem muss die Client-Software speziell an den Proxy angepasst werden.

› Verbindungs-Gateways

Verbindungs-Gateways (Circuit Level Gateways) sind Proxy-Server mit Zusatzfunktionen. Sie beschränken sich, ähnlich wie Application Level Gateways, nicht nur auf die Kontrolle der IP- und Transportschicht-Header. Statt dessen bauen Sie die Datagramme der Transportschicht aus den IP-Paketen, die unter Umständen fragmentiert sind, zusammen. Wie bei Application Level Gateways gibt es auch hier keine direkten Verbindungen zwischen der Innen- und Außenwelt. Vielmehr findet automatisch eine Adressübersetzung statt. So lässt sich eine Benutzerauthentifizierung erzwingen. Auf der anderen Seite verstehen die Circuit Level Gateways das Anwendungsprotokoll nicht und können deshalb keine Inhaltskontrolle durchführen. Beide Gateway-Varianten verfügen

zwar über gemeinsame Merkmale; aber die Fähigkeit, das Anwendungsprotokoll zu verstehen, besitzt nur das Application Level Gateway.



© tecChannel

IP-Pakete: Ein Verbindungs-Gateway muss aus den Daten im IP-Header ersehen, welche Pakete zu einem Datenstrom gehören.

Verbindungs-Gateways vertrauen den internen Benutzern. In der Praxis werden Proxy-Server daher für die Verbindungen nach innen benutzt, während man Verbindungs-Gateways für den Datenverkehr von innen nach außen einsetzt.

› Hybrid-Firewalls

Hybrid-Firewalls bestehen aus Paketfilter und Application Level Gateway, wobei das Gateway die Filterregeln des Paketfilters dynamisch ändern kann. Als "Stateful Inspection" bezeichnet man einen Paketfilter "mit Gedächtnis". Dieser speichert allerdings nur die Informationen aus den Paket-Headern.

Der Vorteil einer Hybrid-Firewall gegenüber einem alleinigen Application Level Gateway liegt in der höheren Performance. Allerdings bedingt dies auch einen gewissen Sicherheitsverlust. Der Grund liegt darin, dass bei den meisten Protokollen der Proxy keinerlei Kontrolle mehr über die Verbindung besitzt, nachdem er den Paketfilter geöffnet hat. Deshalb muss ein Angreifer den Proxy nur eine Zeit lang in Sicherheit wiegen, um anschließend durch den (für ihn geöffneten) Paketfilter freies Spiel zu haben.

Grundlage des Paketfilters mit Stateful Inspection ist die sogenannte "Stateful Inspection Engine". Diese analysiert die Datenpakete während der Übertragung auf Netzwerkebene. Im gleichen Arbeitsgang erstellt die Engine dynamische Zustandstabellen, welche die Betrachtung mehrerer Pakete erlauben. Die Korrelationen zwischen zusammengehörenden ein- und ausgehenden Paketen ermöglichen ausgefeilte Analysen.

› Hochsicherheits-Firewalls

Hochsicherheits-Firewalls können aus einem Firewall-Subnetz mit zwei Paketfilterungs-Routern und einem Proxy (Bastion Host) bestehen. Ein solches Firewall-System sichert auf der Netzwerk- und Applikationsebene durch die Definition einer "entmilitarisierten Zone" (Englisch: demilitarized zone, kurz DMZ). Dabei befinden sich Bastion-Host, Informationsserver, Modem-Pools und andere Server im DMZ-Netz. Das DMZ-Netz agiert so als kleines isoliertes Netzwerk zwischen dem privaten Netz und dem Internet.

Dabei ist das DMZ so konfiguriert, dass Zugriffe aus dem privaten Netz und dem Internet nur auf Server im DMZ erfolgen können. Direkter Verkehr durch das DMZ-Netz hindurch ist nicht möglich - egal in welcher Richtung.

Bei den hereinkommenden Datenpaketen schützt der äußere Router gegen Standard-Angriffe wie IP-Address-Spoofing oder Routing-Attacken und überwacht gleichzeitig den Zugriff auf das DMZ-Netz. Dadurch können externe Rechner nur auf den Bastion-Host und eventuell den Information-Server zugreifen.

Durch den internen Router wird eine zweite Verteidigungslinie aufgebaut. Dieses Gerät überwacht den Zugriff vom DMZ zum privaten Netz indem es nur Pakete akzeptiert, die vom Bastion Host kommen. Damit kommen nur Benutzer in das interne Netz, die sich vorher am Bastion-Host authentifiziert haben.

› Fazit

Wer sein Firmennetzwerk an das Internet anschließt geht ein nicht unerhebliches Risiko ein. Da aber kaum noch eine Firma ohne Internet-Anschluss auskommt, gehört eine Firewall zum Pflichtprogramm. Die Paranoia lässt sich beliebig weit treiben, man muss nur genügend Zeit und Geld investieren.

Jede Firewall - egal welcher Art - ist allerdings nur so gut wie ihre Konfiguration und die Absicherung des Hosts, auf dem die Firewall läuft. Wer einfach das Softwarepaket aufspielt oder einen fertigen Firewall-Rechner in sein Netz hängt und sich damit sicher wähnt, handelt fahrlässig. Deshalb ist es oftmals besser, sich an ein auf Netzwerkabsicherung spezialisiertes Unternehmen zu wenden.

Wie Sie eine Firewall unter Linux aufsetzen, zeigen wir in einem späteren Beitrag. (mha)

› Weitere Themen zu diesem Artikel:

Test: Virenscanner (http://www.tecchannel.de/special/970/index.html)
Virenscanner - alle Daten im Überblick (http://www.tecchannel.de/tecdaten/show.php3?article=214)
Computerviren: Grundlagen (http://www.tecchannel.de/special/971/index.html)
Viren unter Linux (http://www.tecchannel.de/special/972/index.html)
Test: Personal Firewalls (http://www.tecchannel.de/special/975/index.html)
Personal Firewalls - alle Daten im Überblick (http://www.tecchannel.de/tecdaten/show.php3?navid=2&catid=84&pageid=425)
Desktop Firewall mit Linux (http://www.tecchannel.de/special/978/index.html)
Workshop: Sicher Linux Workstation (http://www.tecchannel.de/special/979/index.html)
Office säubern und signieren (http://www.tecchannel.de/special/973/index.html)
Sichere E-Mail (http://www.tecchannel.de/special/983/index.html)
Sicher im Web unterwegs (http://www.tecchannel.de/special/974/index.html)
Safer Surfen (http://www.tecchannel.de/special/981/index.html)
Dem Surfer auf der Spur (http://www.tecchannel.de/special/982/index.html)
Sicher durch Biometrie (http://www.tecchannel.de/special/984/index.html)
Kryptographie Grundlagen (http://www.tecchannel.de/special/980/index.html)