Sichere modulbasierte Zugriffslisten für Perimeter-Router

Kai Simon, Thomas Schwenkler
Fraunhofer IESE
Sauerwiesen 6
67661 Kaiserslautern
{simon,schwenkl}@iese.fhg.de

Stephan Groß
Technische Universität Dresden
Fakultät Informatik
01062 Dresden
st.gross@inf.tu-dresden.de

Zusammenfassung

Sicherheit ist mittlerweile ein zentrales Thema beim Aufbau und Betrieb von Rechnernetzen. Allzu oft konzentrieren sich die hierfür durchgeführten Maßnahmen jedoch alleine auf die Firewall. Dabei lassen sich viele potentielle Risiken bereits einen Schritt vorher, am Übergang vom lokalen zum Weitverkehrsnetz, erfolgreich eindämmen. Dieser Artikel gibt einen Überblick von „Best Practices“ zur Konfiguration der dafür eingesetzten Perimeter-Router.

1 Einführung

Mit der in den letzten Jahren fortschreitenden Anbindung an das Internet hat die Gefährdung betrieblicher Netzwerke durch Datenraub, Industriespionage, mutwillige Zerstörung und inzwischen auch vermehrt durch eigene Mitarbeiter enorm zugenommen. Jedes Jahr entsteht bei Industrie, Handel und Banken ein wirtschaftlicher Schaden in zweistelliger Milliardenhöhe [TüV00].

Ein Teil der Schäden könnte ohne größere Probleme vermieden werden. Sicherheits-Patches müssten regelmäßig eingespielt und Log-Dateien ständig überprüft werden. Grundsätzlich müsste der Sicherheitgedanke bereits bei der Erstellung von Netzwerkkonzepten berücksichtigt, umgesetzt und gelebt werden. Aber schon die Einhaltung einfachster Regeln bei der Konfiguration von Perimeter-Routern, dem Übergangspunkt zwischen lokalem und Weitverkehrsnetz, könnten das Gefährdungspotential erheblich senken.

Perimeter-Router müssen mit Zugriffslisten in ein- und ausgehender Richtung versehen werden, um unerwünschten und nicht plausiblen Datenverkehr zu blockieren. Das Problem liegt zum einen in der Definition des nicht plausiblen Datenverkehrs und zum anderen am Arbeits-

aufwand, denn für jedes Aufgabengebiet und Netzwerk müssen die entsprechenden Zugriffslisten speziell angepasst werden.

Im folgenden beschreiben wir die modulbasierte Erstellung von Zugriffslisten zur sicheren Konfiguration von Perimeter-Router und deren Anwendung in der Praxis. Vergleichbar mit ähnlichen Ansätzen in der Software-Entwicklung ermöglicht der modulare Aufbau von Zugriffslisten, dass diese einfach wiederverwendet werden können. Mit der Zeit entstehen so regelrechte *Pattern* als Lösungen für konkrete Teilaspekte der Router-Konfiguration, die nur noch miteinander kombiniert werden müssen. Durch Verwendung solcher erprobter Mustervorlagen wird insgesamt eine Verbesserung der Systemsicherheit erreicht.

Nach einer kurzen allgemeinen Einführung in die Materie (Abschnitt 2) gehen wir in Kapitel 3 zunächst auf das von uns propagierte Rüstzeug für die Absicherung lokaler Netze ein: die Perimeterfilterung. Darauf aufbauend beschreiben wir einige der häufigsten Angriffe und wie man sie mit den zuvor eingeführten Methoden verhindern oder zumindest eindämmen kann (Kapitel 4). Wir schließen mit einigen zusammenfassenden Empfehlungen für die Praxis.

2 Verwandte Arbeiten

Router und ihre Konfiguration sind an und für sich kein neues Thema sondern vielmehr eine Problematik, die uns seit den Anfängen des Internet beschäftigt. Im Laufe der Jahre hat sich der Blickwinkel hierauf bedingt durch neue Anforderungen häufig verändert. Dies gilt insbesondere für den Aspekt der IT-Sicherheit. So müssen wir heute immer wieder zu Tage tretende Schwachstellen ausbessern, die auf Implementierungsfehlern der dem Internet zugrunde liegenden Kommunikationsprotokolle beruhen. Besonders problematisch sind dabei solche Fehler, die von missverständlichen oder gar fehlerhaften Standards herrühren. Als Grund hierfür sind insbesondere unvollständig formulierte oder heute nicht mehr allgemein gültige Voraussetzungen anzuführen. Da Administratoren nicht immer Zugang zum Quellcode fehlerhafter Systeme haben, müssen solche Lücken immer wieder durch geschickte und trickreiche Konfiguration der Netzinfrastruktur gestopft werden ohne dabei deren Funktionalität zu beeinträchtigen. Neben der hohen Komplexität macht jedoch vor allem der überall herrschende Zeitmangel dies zu einem recht gefährlichen Unterfangen. Um dem entgegen zu wirken bedarf es einer fundierter Hilfestellung.

Gute Handreichungen für die sichere Konfiguration von Routern findet man zum einen direkt bei den Herstellern. Neben den jeweiligen Benutzerhandbüchern und Kommandoreferenzen zu ihren unterschiedlichen Systemen bietet die Firma Cisco beispielsweise auch weiterführende Literatur an, die sich mit speziellen Aspekten wie z.B. der Netzsicherheit beschäftigt [Wen01]. Die wachsende strategische und wirtschaftliche Bedeutung des Internet hat außerdem dazu geführt, dass viele Regierungen eigene Institutionen ins Leben gerufen haben, um Richtlinien für den sicheren Betrieb von Datennetzen zu erarbeiten. Beispielhaft seien hier das Bundesamt für Sicherheit in der Informationstechnik (BSI)[1] und die National Security Agency (NSA)[2] genannt. Letztere hat mit [ABB+02] konkrete Empfehlungen für die sichere Konfiguration von Routern veröffentlicht, die detaillierte Instruktionen für den Einsatz von

[1] www.bsi.de

[2] www.nsa.gov

Cisco-Routern beinhalten. Daneben gibt es weitere, nicht staatliche Organisationen, wie z.B. das CERT Coordination Center[3] oder das SANS Institute[4], die sich ebenfalls mit Fragen der IT-Sicherheit befassen. Schließlich sind eine Vielzahl von unabhängigen Buchpublikationen zu dem Thema erhältlich. Hiervon sei exemplarisch das Buch von Northcutt, Zeltser und Winters [NZW02] erwähnt, dass sich durch seine ganzheitliche Betrachtungsweise auszeichnet.

3 Perimeterfilterung

Unter Perimeterfilterung verstehen wir die Kontrolle der ein- und ausgehenden Datenströme an einem Router. Als Kontrollmerkmale verwenden wir dabei zum einen die Sende- bzw. Empfangsadresse (IP-basierte Filterung) und zum anderen die angesprochenen Anwendungen (Port-basierte Filterung). Einen Sonderfall stellen ICMP-Nachrichten dar, die eigentlich den reibungslosen Betrieb des Internet auch im Falle von auftretenden Fehlern sicherstellen sollen. Aufgrund der bereits in Kapitel 2 angesprochenen Probleme können diese Nachrichten jedoch für Angriffe missbraucht werden und sind daher ebenfalls zu kontrollieren.

3.1 IP-basierte Filterung

Im folgenden geben wir einen Überblick über Adressbereiche, die als Quelladresse für eingehenden (ingress) und als Zieladresse für ausgehenden (egress) Datenverkehr gefiltert werden sollten. Zudem werden die entsprechenden praktischen Umsetzungsmöglichkeiten besprochen und bewertet. Zum besseren Verständnis wurde die Betrachtung in die drei Bereiche reservierte, nicht verwendete und eigene Adressbereiche aufgespalten. Die betrachteten Adressbereiche wurden jeweils durch Angabe der Netzwerkadresse und des Netzwerkpräfix spezifiziert (vgl. hierzu [KR01, Kapitel 4.4.1]).

- **Reservierte Adressbereiche:** RFC 3330 [IAN02] vermittelt einen guten Überblick über Adressbereiche für spezielle Anwendungsgebiete:
  - *0.0.0.0/8:* Adressen aus diesem Bereich werden verwendet, um spezielle Komponenten im eigenen Netzwerk zu adressieren. Ein typisches Beispiel ist das Default-Gateway.
  - *10.0.0.0/8:* Dieser Adressblock ist nach RFC 1918 [RMK+96] für die Benutzung in privaten Netzwerken reserviert.
  - *127.0.0.0/8:* Dieser Adressblock ist für die Loopback-Adresse von Rechnern reserviert. Verschiedene Anwendungen auf gleichen Rechnern können somit auch ohne Verwendung einer Netzwerkkarte miteinander kommunizieren. Typischerweise wird lediglich die 127.0.0.1/32 für Loopback-Kommunikation verwendet, trotzdem ist der komplette Adressraum reserviert und sollte nicht andersartig verwendet werden.

[3] `www.cert.org`

[4] `www.sans.org`

- *169.254.0.0/16:* Dieser Adressblock ist der Autokonfiguration von Rechnern vorbehalten. Nach dem Ausfall eines DHCP-Servers bedienen sich z.B. Windows-Rechner automatisch mit IP-Adressen aus diesem Pool.
- *172.16.0.0/12:* Dieser Adressblock ist nach RFC 1918 [RMK+96] für die Benutzung in privaten Netzwerken reserviert.
- *192.0.2.0/24:* Dieser Adressblock, TEST-NET genannt, ist reserviert für Dokumentationen und Beispiele. Oft wird er in Zusammenhang mit Domainnamen wie example.com und example.net in Hersteller- und Protokoll-Dokumentationen verwendet. Er sollte nicht im öffentlichen Netzwerkbereich eingesetzt werden.
- *192.88.99.0/24:* Adressblock für die nach RFC 3068 [Hui01] bei Übergangsroutern zwischen IPv6 und IPv4 benötigten Anycast-Adressen.
- *192.168.0.0/16:* Dieser Adressblock ist nach RFC 1918 [RMK+96] für die Benutzung in privaten Netzwerken reserviert.
- *198.18.0.0/15:* Dieser Adressblock wird nach RFC 2544 [BM99] für Performance-Analysen von Netzwerkkomponenten verwendet.
- *224.0.0.0/4:* Dieser Adressblock ist nach RFC 3171 [AAMS01] für IPv4-Multicast Kommunikation reserviert.
- *240.0.0.0/4:* Dieser als Class-E Netzwerk bekannte Block ist für zukünftige Anwendungen reserviert. Hier befindet sich auch die bekannte LIMITED BRODCAST-Adresse 255.255.255.255, die auf keinen Fall geroutet werden darf.

Die praktische Umsetzung der Filterung kann auf unterschiedlichen Wegen erfolgen. Beispielsweise können einfache Zugriffslisten eingesetzt werden. Alternativ könnte auch Null-Routing eingesetz werden, bei dem alle zu filternden Pakete an das sogenannte Null-Inferface geroutet und dann verworfen werden. Aus Sicht der Performance ist Null-Routing schneller als der Einsatz von Zugriffslisten. Null-Routing bietet allerdings keinen Hitcounter, welcher die Anzahl der Treffer pro Filterregel angibt. Da hierdurch die Überwachung des Netzwerkverkehrs nicht mehr lückenlos möglich ist, sollte Null-Routing nur bei Performance-Engpässen in Erwägung gezogen werden.

- **Nicht vergebene Adressbereiche:** Die oberste Instanz bei der Vergabe von IP-Adressen ist die Internet Assigned Numbers Authority (IANA)[5]. Ihr sind vier regionale Vergabestellen (Regional Internet Registrys, RIR) unterstellt: APNIC (Asia Pacific Network Information Centre) für den asiatisch-pazifischen Raum, ARIN (American Registry for Internet Numbers) für Nordamerika und einen Teil Afrikas, LACNIC (Regional Latin-American and Caribbean IP Address Registry) für Lateinamerika und die Karibischen Inseln sowie RIPE NCC (Réseaux IP Européens) für Europa, den mittleren Osten, Zentralasien und Afrika nördlich des Äquators.

  Grundsätzlich sollten Datenpakete von allen nicht vergebenen Adressbereichen verworfen werden. In der Praxis ist dies allerdings nur bedingt möglich, da sich der Vergabeprozess stark dynamisch gestaltet. Aus diesem Grund haben wir uns auf die Datenbank der IANA beschränkt (siehe Tabelle 1). Sie wird regelmäßig aktualisiert und stellt somit einen akzeptablen Kompromiss zwischen Sicherheit und Wartbarkeit dar.

[5] `www.iana.org`

1-2.0.0.0/8	5.0.0.0/8	7.0.0.0/8	23.0.0.0/8
27.0.0.0/8	31.0.0.0/8	36-37.0.0.0/8	39.0.0.0/8
41-42.0.0.0/8	58-59.0.0.0/8	70-79.0.0.0/8	83-126.0.0.0/8
173-187.0.0.0/8	189-190.0.0.0/8	197.0.0.0/8	223.0.0.0/8

Tabelle 1: Nicht vergebene Adressbereiche nach IANA (Stand: 05.04.2003)

- **Im eigenen Netz verwendete Adressbereiche:** Im eigenen Netz verwendete Adressbereiche dürfen nicht als Quelladresse bei eingehendem Datenverkehr erscheinen und sollten gefiltert werden (ingress traffic filtering, siehe RFC 2827 [FS00]). Ausgehender Datenverkehr sollte ebenfalls auf korrekte Quelladressen (aus dem eigenen Adressbereich) überprüft werden (egress traffic filtering).

  Für die praktische Umsetzung der Filterung kann entweder auf einfache Zugriffslisten oder auf Unicast Reverse Path Forwarding (Unicast RPF) zurückgegriffen werden. Beim Unicast RPF werden auf Basis der Routingtabellen die Adressbereiche hinter den Schnittstellen ermittelt. Stimmt die Quelladresse eines eingehenden Datenpakets nicht mit der eingehenden Schnittstelle überein, so wird es verworfen. Der Vorteil von Unicast RPF gegenüber den Zugriffslisten liegt in der einfachen Konfiguration: Es braucht lediglich einmal aktiviert zu werden und verrichtet dann auch bei geänderter IP-Konfiguration des Routers seinen Dienst. Leider wird Unicast RPF nicht von allen Routern unterstützt.

3.2 Port-basierte Filterung

Die Port-basierte Filterung ist stark anwendungs- und ideologieabhängig. In der Literatur finden sich keine einheitlichen Aussagen zu diesem Thema. Beispielsweise verzichtet Cisco komplett auf die Port-basierte Filterung [GS01]. Die NSA [ABB+02] und das Landeshochschulnetz von Baden-Württemberg (BelWü) [Bel03] hingegen empfehlen die Blockierung einer ganzen Reihe von Ports. Im BelWü ist die Empfehlung auch praktisch umgesetzt. Daher dienen die im folgenden aufgeführten und nach privilegierten (≤ 1023) und unprivilegierten (> 1023) Ports separierten Empfehlungen lediglich als Orientierungshilfe.

- **Filterung privilegierter Ports:** Die Filterung priviligierter Ports ersetzt keine Firewall, sie filtert lediglich den „gröbsten Unfug“ an der Außengrenze des eigenen Netzes heraus. Laut [Bel03] basieren die meisten Angriffe auf wenigen, teilweise sehr alten Sicherheitslücken. Tabelle 2 listet die diesbezüglich am Perimeterrouter zu filternden Ports auf.
- **Filterung unprivilegierter Ports:** Die Filterung von unprivilegierten Ports sollte nur im konkreten Verdachtsmoment oder nach exakter Überprüfung der Sachlage eingesetzt werden, da sie die normale Kommunikation beeinträchtigt. Tabelle 3 zeigt einige bevorzugte Ports von bekannten DDoS (Distributed Denial of Service) Angriffen [ABB+02]. Grundsätzlich empfehlen BelWü [Bel03] und NSA [ABB+02] die Sperrung der in Tabelle 4 angegebenen Ports.

Die Port-basierte Filterung sollte mit Hilfe einer Zugriffskontrollliste in eingehender Richtung (ingress-traffic-filter) realisiert werden, um das Intranet und den Router selbst zu schützen. Zur

Port	Typ	Port	Typ	Port	Typ
1/tcp,udp	tcpmux	7/udp	echo	9/tcp,udp	discard
11/tcp	systat	13/tcp,udp	daytime	15/tcp	netstat
19/tcp,udp	chargen	39/tcp,udp	time	43/tcp	whois
67/udp	bootps	68/udp	bootpc	69/udp	tftp
93/tcp	supdup	111/tcp,udp	sunrpc	123/udp	ntp
135/tcp,udp	loc-srv	137/tcp,udp	netbios-ns	138/tcp,udp	netbios-dgm
139/tcp,udp	netbios-ssn	161/tcp,udp	snmp	162/tcp,udp	snmptrap
177/udp	xdmcp	445/tcp	netbios-ds	512/tcp	regex
513/tcp	rlogin	514/tcp,udp	rsh,syslog	515/tcp	lpd
517/udp	talk	518/udp	ntalk	540/tcp	uucp

Tabelle 2: Filterung privilegierter Ports

Angriffsart	Port
Stacheldraht	16660/tcp, 65000/tcp
Subseven	2222/tcp, 6711/tcp, 6712/tcp, 6669/tcp, 6776/tcp, 7000/tcp
Trinity V3	33270/tcp, 39168/tcp
Trinoo	27665/tcp, 31335/udp

Tabelle 3: Filterung bekannter unprivilegierter Ports

Vermeidung von nicht gewolltem Datenverkehr vom Intranet zum Internet und zur Reduzierung des Datenvolumens auf der Standleitung zum Provider kann Port-basierte Filterung auch zusätzlich in ausgehender Richtung (egress-traffic-filter) eingesetzt werden

3.3 ICMP Behandlung

Auf der einen Seite wird ICMP (Internet Control Message Protocol) [Pos81] zum reibungslosen Netzwerkbetrieb benötigt, auf der anderen Seite stellt es auch eine große Gefahr für Netzwerke dar. Eine generelle Blockierung ist somit nicht zu empfehlen. Es gibt allerdings Möglichkeiten, nicht benötigte und unsichere Nachrichtentypen (Message Types) zu sperren. Einige Nachrichtentypen können Anwendungsprogrammen zugeordnet werden. Beispielsweise verwendet das Ping-Kommando die Nachrichtentypen ECHO (Typ 8) und ECHO-REPLY (Typ 0). Ping erlaubt es, einen Plan der Netzwerke und Server hinter Perimeter-Routern zu

Port	Typ	Port	Typ	Port	Typ
1080/tcp	socks	1214/tcp	kazaa	1234,5501/tcp	hotline
1900/tcp,udp	MS ssdp	2049/tcp,udp	nfs	3128/tcp	squid
4045/tcp,udp	lockd	4661,4662/tcp	eDonkey	5000/tcp,udp	MS ssdp
6000-6063/tcp	x11	6346,6347/tcp	gnutella	6667/tcp	irc
6699/tcp	WinMX	12345/tcp,udp	Chat	31337/tcp,udp	BackOrifice

Tabelle 4: Grundsätzlich empfohlene Filterung unprivilegierter Ports

erstellen und danach gezielt Komponenten anzugreifen. Mit ICMP-REDIRECTS (Typ 5) ist es möglich, Routing-Tabellen von Routern und Rechnern negativ zu beeinflussen. Für eingehenden Verkehr (ingress-traffic-filter) sollten laut NSA [ABB+02] die Nachrichtentypen ECHO, REDIRECT und MASK-REQUEST gesperrt werden. Das BelWü [Bel03] empfielt hingegen die Sperrung von ECHO und ECHO-REPLY, womit Ping in beiden Richtungen unterbunden wird. In ausgehender Richtung (egress-traffic-filter) filtert das BelWü [Bel03] keine ICMP-Pakete. Die NSA [ABB+02] hingegen macht einen Vorschlag für eine Positivliste, nach der lediglich ECHO, PARAMETER-PROBLEM, PACKET-TO-BIG und SOURCE-QUENCH erlaubt sind. Cisco fordert zur MTU-Discovery für IPSec- und PPTP-Verbindungen auf jeden Fall die Freischaltung von UNRECHABLE-Nachrichten (Typ 3) in beide Richtungen [Cis03b].

Abhängig von den individuellen Anforderungen könnten die Zugriffslisten für die ICMP-Filterung auf einem Cisco-Router wie folgt aussehen:

```
ip access-list extended ingress-traffic-filter
  ! deny   icmp any any echo log ! (kein ping vom Internet erlaubt)
  deny   icmp any any redirect log
  deny   icmp any any mask-request log
  permit icmp any any
!

ip access-list extended egress-traffic-filter
  ! permit icmp any any echo ! (ping zum Internet erlaubt)
  permit icmp any any parameter-problem
  permit icmp any any packet-too-big
  permit icmp any any source-quench
  ! permit icmp any any unrechable ! (bei IPSec bzw. PPTP-Kommunikation)
  deny   icmp any any log
!
```

4 Angriffe und Gegenmaßnahmen

Nachdem wir im vorangegangenen Abschnitt beschrieben haben, wie man allgemein Netze mittels Perimeterfilterung auf Routern schützen kann, gehen wir nun auf einige konkrete Angriffe und passende Gegenmaßnahmen ein. Die dabei verwendeten Zugriffslisten verwenden zum Teil durch spitze Klammern eingefasste Variablennamen, an deren Stelle die jeweilige IP-Adresse gesetzt werden muss.

4.1 Land Attack

Der Land Angriff besteht aus IP-Paketen, deren Sender- und Empfängeradresse identisch sind mit der des angegriffenen Ziels. Gleiches gilt für den Sender- und Empfänger-Port. Der angegriffene Router bzw. Host glaubt somit, er „spräche mit sich selbst“. Dies kann den Datendurchsatz stark vermindern und im ungünstigsten Fall sogar zu einem vollständigen Ausfall (Denial of Service) führen. Die folgende Zugriffsliste schützt vor diesem Angriff.

```
ip access-list extended ingress-traffic-filter
  deny   ip host <router ip> host <router ip> log
  permit ip any any
!
```

4.2 Smurf und Fraggle Attack

Smurf- und Fraggle-Angriffe gehören zur ebenfalls zu den sogenannten Denial of Service (DoS) Attacken. Beim Smurf-Angriff wird ein gefälschtes ICMP-ECHO-Paket an die Netz- oder Broadcast-Adresse des Netzwerkes gesendet. Es wird vorrausgesetzt, dass ein Router zwischen Layer 3 (Network) und Layer 2 (Data Link) des ISO/OSI-Schichtenmodells [DZ83] Broadcast-Funktionalität bereitstellt [Bak95]. Alle aktiven Rechner im angesprochenen Netzwerk antworten auf die Anfrage mit einem ICMP-ECHO-REPLY-Paket, dessen Ziel die gefälschte Quelladresse des Anfragepaketes ist. Der Angriff auf das Opfer wird dadurch noch verstärkt. Eine Variante des vorgestellten Angriffes ist unter dem Namen Fraggle-Attack bekannt. Der Unterschied besteht in der Verwendung von UDP-Paketen.

Eine Möglichkeit, diesen Angriff zu vereiteln, besteht in der Deaktivierung der Directed-Broadcast-Funktionalität. Dies erfolgt bei Cisco-Routern mit dem Kommando `no ip directed-broadcast` im Interface-Konfigurationsmodus. Diese Funktionalität ist ab der IOS (Internet Operation System) Version 12 standardmäßig deaktiviert. Alternativ dazu kann eine Zugriffsliste eingesetzt werden, die auch alle weiteren hinter dem Perimeterrouter verwendeten Netze schützen kann. Der Hitcounter der Zugriffsliste lässt sich zudem als Informationsquelle für potentielle Angriffsversuche auswerten. Eine entsprechende Zugriffsliste könnte wie folgt lauten:

```
ip access-list extended ingress-traffic-filter
  deny   ip any host <broadcast ip> log
  deny   ip any host <network ip> log
  permit ip any any
!
```

4.3 TCP-SYN-Flooding

Beim TCP-SYN-Flooding versucht der Angreifer auf dem Zielsystem halboffene Verbindungen zu etablieren. Der Angreifer beginnt dabei den 3-Wege-Verbindungsaufbau normal durch das Senden eines IP-Paketes mit gesetztem SYN-Flag. Die korrekte Antwort darauf besteht aus einem Paket mit gesetztem SYN- und ACK-Flag, aber der Angreifer vollendet den Verbindungsaufbau nicht mit dem abschließenden ACK-Paket. Die Verbindung ist somit halboffen und verbraucht Speicherressourcen. Nach einer gewissen Anzahl von halboffenen Verbindungen ist der Server nicht mehr in der Lage, neue Verbindungen anzunehmen. Er steht somit für reguläre Anwender nicht mehr zur Verfügung [BSI03]. TCP-SYN-Flooding wird häufig in Verbindung mit IP-Spoofing eingesetzt. Die Antwortpakete (SYN-ACK) vom Server werden dann nicht mehr zum Angreifer, sondern zu nicht erreichbaren Netzen oder zu ahnungslosen Rechnern umgeleitet, von denen ebenfalls keine Antwort zu erwarten ist.

Ein Schutz vor TCP-SYN-Flooding ist in der Praxis mit Zugriffslisten nur bedingt realisierbar [ABB+02]. Der folgende Vorschlag blockiert alle externen Verbindungsaufbauwünsche, womit Verbindungen nur noch vom internen Netz initalisiert werden können. Das Betreiben von Servern (z.B. WWW-Servern) wäre damit jedoch auch nicht mehr möglich!

```
ip access-list extended ingress-traffic-filter
  permit tcp any <network intern> established
  deny   ip any any log
!
```

Bessere Mechanismen zur Abwehr dieses Angriffes werden von den Router-Herstellen geliefert. Cisco Systems bietet z.B. in seinem IOS den TCP-INTERCEPT Mechanismus [Cis03a] an, welcher nur erreichbaren Rechnern den Verbindungsaufbau zu internen Servern erlaubt. Die restlichen Verbindungen werden abgelehnt. Es wird folgendermassen aktiviert:

```
ip tcp intercept list 144
!
access-list 144 permit tcp any <intern network>
access-list 144 deny   ip any any
!
```

Der TCP-INTERCEPT Mechanismus ist in vielen IOS-Versionen ab 12.0 enthalten. Er sollte jedoch nur im konkreten Bedarfsfall und mit Vorsicht eingesetzt werden, da es zu Performance-Engpässen kommen kann.

5 Empfehlungen für die Praxis

Zum Abschluss fassen wir die vorgestellten Maßnahmen nochmals in Empfehlungen für den konkreten Einsatz in der Praxis zusammen. Hierfür definieren wir zunächst ein beispielhaftes Umfeld, in dem mehrere Perimeter-Router zu konfigurieren sind (vgl. Abbildung 1). Dieses besteht im wesentlichen aus drei Teilen mit folgenden Aufgaben:

1. Dem *Backbone eines Internet Service Providers (ISP).* Dieser stellt seinen Kunden eine Anbindung an das Internet zur Verfügung. Dabei muss er zum einen seine Kunden soweit wie möglich vor Angriffen aus eben diesem schützen. Andererseits muss er sich selbst bzw. seine zentrale Verbindung mit dem Internet und seine Kunden vor Angriffen bewahren, die von Seiten eines Teils seiner eigenen Kunden durchgeführt wird. Seine Perimeter-Router an den Übergangspunkten zu den einzelnen Kundennetzen müssen also sowohl den ein- wie auch den ausgehenden Verkehr kontrollieren.

2. Einem *Universitätsnetzwerk,* bestehend aus einer beliebigen Anzahl von Intranets einzelner Lehrstühle und einer zentralen Anbindung an den ISP-Backbone über ein Rechenzentrum (RZ). Dieses tritt quasi als ISP gegenüber den einzelnen Lehrstühlen auf und hat demnach ganz ähnliche Aufgaben zu erfüllen. Bei der Konfiguration der Perimeter-Router einzelner Lehrstühle würde eigentlich eine Kontrolle des eingehenden Verkehrs genügen, jedoch sollte aus Sicherheitsgründen auch der ausgehende Verkehr geregelt

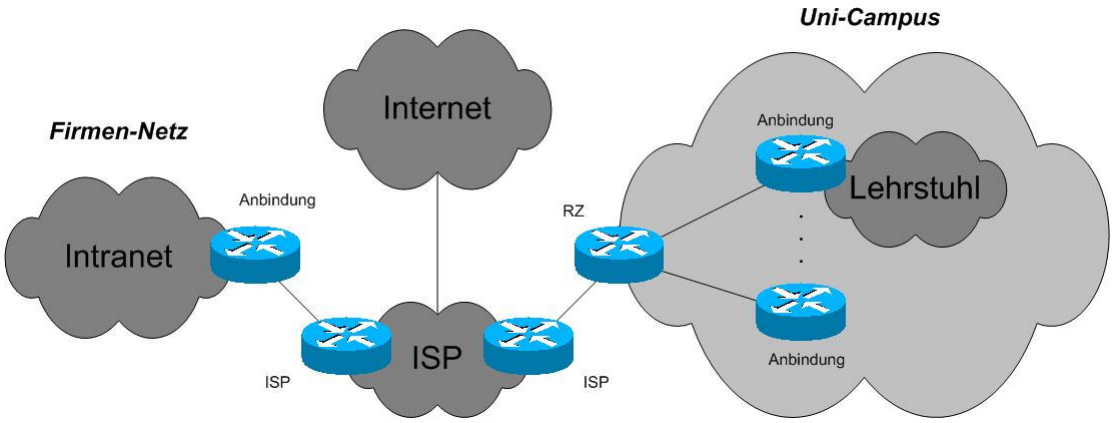

Abbildung 1: Beispielszenario

werden, um beispielsweise durch E-Mails verbreitete Wurm-Angriffe bereits im Keim zu ersticken. Es ist sinnvoll, wenn eine solche Konfiguration durch eine Sicherheitspolitik seitens des Rechenzentrums verbindlich vorgeschrieben wird.

3. Dem *Intranet einer Firma,* das auch als degenerierte Variante des Universitätsnetzes angesehen werden kann. Auch hier macht daher die Kontrolle sowohl des ein- als auch des ausgehenden Verkehrs Sinn.

Unsere Empfehlungen zur Erstellung von Zugriffslisten für die einzelnen Router haben wir in Tabelle 5 zusammengefasst. Dabei unterscheiden wir zunächst die eingesetzten Router nach ihrem Einsatzort und der daraus resultierenden Aufgabenstellung (zweite bis vierte Tabellenspalte). Aufgabe der *ISP-Router* ist einzig und allein die Netzanbindung von Kunden an den Backbone des ISP und damit an das Internet. Sie sind mit einem *Anbindungs-Router* verbunden, der – wie der Name schon sagt – die Intranet-Anbindung an das Internet auf Kundenseite regelt. Anbindungs-Router sind häufig das letzte Glied in einer ganzen Kette von Routern. Der *RZ-Router* stellt schließlich eine Mischung aus beiden Fällen dar und wird daher gesondert betrachtet. Gegenüber dem ISP tritt er als Anbindungs-Router auf, aus Sicht der Lehrstühle ist er ein ISP-Router.

In den einzelnen Tabellenzeilen sind ferner die bereits aus Kapitel 3 bekannten Filtermethoden und den in Kapitel 4 eingeführten Angriffstypen aufgeführt. Für sämtliche daraus resultierende Fälle geben wir eine Empfehlung für oder gegen die Einrichtung einer entsprechenden Filterregel ab. In den einzelnen Zellen steht dabei ein Kreuz für eine positive und ein Minus für eine negative Empfehlung. Klammern bedeuten, dass nur eine eingeschränkte Empfehlung gegeben werden kann. Jede Zelle enthält außerdem zwei Empfehlungen: die erste für die Filterung in ingress-, die zweite für die Filterung in egress-Richtung.

6 Zusammenfassung

Wir haben in dem vorliegenden Artikel eine Auswahl von Maßnahmen für die Erstellung sicherer modulbasierter Zugriffslisten für Perimeter-Router vorgestellt. Dabei wurde versucht, für

Erläuterung	ISP	RZ	Anbindung
IP-basierte Filterung			
Reservierte Adressbereiche	×/×	×/×	×/×
Nicht vergebene Adressbereiche	×/×	×/×	×/×
Anti Spoofing	×/×	×/×	×/×
Port-basierte Filterung			
Filterung priviligierter Ports	-/-	(×)/-	×/-
Filterung unpriviligierter Ports	-/-	(×)/-	(×)/-
ICMP-Filterung			
ICMP-Behandlung	-/-	(×)/(×)	×/×
Maßnahmen gegen Angriffe			
Land Attack	×/×	×/×	×/×
Smurf und Fraggle Attack	×/-	×/-	×/-
TCP-SYN-Flooding	-/-	-/-	(×)/-

Tabelle 5: Einsatzorte und Empfehlungen

einzelne spezielle Angriffsmuster maßgeschneiderte Module zu entwerfen, die als Bausteine für größere Installationen verwendet werden können. Es ist aber auch deutlich geworden, dass es diesem Ansatz noch an Systematik fehlt. So würde beispielsweise eine einheitliche Klassifikation von unerwünschten Angriffen und gewünschten Funktionsmerkmalen eine Entwicklung in Richtung einer Pattern-Language ermöglichen. Diese Technik wird im Bereich Software-Engineering schon länger erfolgreich zur Minimierung von Programmierfehlern eingesetzt und wird seit neuestem auch im Bereich IT-Sicherheit zur Verbesserung des Sicherheitsniveaus propagiert [Sch03]. Nach unserer Überzeugung ließe sich dadurch die Komplexität bei der Konfiguration eines Netzwerkes erheblich reduzieren und damit die Systemsicherheit entscheidend verbessern.

Literaturverzeichnis

[AAMS01] Z. Albanna, K. Almeroth, D. Meyer, and M. Schipper. RFC3171: IANA Guidelines for IPv4 Multicast Address Assignments. Technical report, Internet Engineering Task Force (IETF), August 2001.

[ABB+02] V. Antoine, R. Bongiorni, A. Borza, P. Bosmajian, D. Duesterhaus, M. Dransfield, B. Eppinger, K. Gallicchio, J. Houser, A. Kim, P. Lee, T. Miller, D. Opitz, F. Richburg, M. Wiacek, M. Wilson, and N. Ziring. Router Security Configuration Guide. Technical Report 1.1, System and Network Attack Center (SNAC), National Security Agency (NSA), September 2002.

[Bak95] F. Baker. RFC1812: Requirements for IP Version 4 Routers. Technical report, Internet Engineering Task Force (IETF), June 1995.

[Bel03] Sicherheitsmaßnahmen im BelWü (Baden-Württembergs extended LAN). `http://www.belwue.de/security/massnahmen.html/`, December 2003.

[BM99] S. Bradner and J. McQuaid. RFC2544: Benchmarking Methodology for Network Interconnect Devices. Technical report, Internet Engineering Task Force (IETF), March 1999.

[BSI03] TCP-SYN-Flooding. http://www.bsi.de/fachthem/sinet/vulner/begriffe3.htm#tcp/, December 2003.

[Cis03a] Cisco IOS 12.3 Command Reference – TCP-Intercept. http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr%/secur_r/sec_i1g.htm#1074780/, December 2003.

[Cis03b] Cisco PIX 6.3 Command Reference – ICMP. http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/, December 2003.

[DZ83] J. D. Day and H. Zimmermann. The OSI Reference Model. *Proceedings of the IEEE*, 71, 12:1334–1340, 1983.

[FS00] P. Ferguson and D. Senie. RFC2827: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. Technical report, Internet Engineering Task Force (IETF), May 2000.

[GS01] Barry R. Greene and Philip Smith. Cisco ISP Essentials – Essential IOS Features Every ISP Should Consider. Technical Report 2.9, Cisco Systems Inc., June 2001.

[Hui01] C. Huitema. RFC3068: An Anycast Prefix for 6to4 Relay Routers. Technical report, Internet Engineering Task Force (IETF), June 2001.

[IAN02] IANA. RFC3330: Special-Use IPv4 Addresses. Technical report, Internet Engineering Task Force (IETF), September 2002.

[KR01] James F. Kurose and Keith W. Ross. *Computer Networking: A Top-Down Approach Featuring the Internet*. Addison Wesley, 1 edition, 2001.

[NZW02] Stephan Northcutt, Lenny Zeltser, and Scott Winters. *Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems*. New Riders, 2002.

[Pos81] J. Postel. RFC792: Internet Control Message Protocol. Technical report, Internet Engineering Task Force (IETF), September 1981.

[RMK+96] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear. RFC1918: Address Allocation for Private Internets. Technical report, Internet Engineering Task Force (IETF), February 1996.

[Sch03] Markus Schumacher. *Security Engineering with Patterns – Origins, Theoretical Model, and New Applications*. Number 2754 in Lecture Notes in Computer Science (LNCS). Springer Verlag, August 2003.

[TüV00] TüV: Milliarden-Schäden durch Computerkriminalität. Xdial.de, http://www.xdial.de/news/Meldung.asp?Id=970, February 2000.

[Wen01] Michael Wenstrom. *Managing Cisco Network Security*. Cisco Press, 2001.