

Sicher auf die Datenautobahn

Roland Herbst
herbst@cms.hu-berlin.de

Fakten und Zahlen

Die Teilnehmer des Netzwerkes der Universitätsverwaltung (nachfolgend Verwaltungsnetz) können seit fast 10 Jahren die Dienste des Internets nutzen. Dass dies nicht immer so war, kann sich sicher heute niemand mehr vorstellen. Auch gegenwärtig ist es noch nicht an allen universitären Einrichtungen der Fall, dass der Zugang zum Internet von den PCs der Mitarbeiter der Verwaltung möglich ist.

Das Firewall-System wurde im Zuge mehrerer DFN-Projekte in den Jahren 1997-2003 aufgebaut und weiterentwickelt. In diesem Zeitraum entstand eine VPN-Installation zur sicheren Fernanbindung der Fakultäten, die an anderer Stelle in diesem Heft thematisiert wird. Da sich ein Firewall-System technisch an der Grenze zwischen Netzwerk- und Servertechnik bewegt, wird es in enger Kooperation mit den Netzwerk-Spezialisten designed, entwickelt und administriert.

Ein Firewall-System befindet sich immer am Übergang zwischen zwei Bereichen unterschiedlicher Sicherheitsanforderungen. In unserem Fall bildet es die Grenze zwischen dem Verwaltungsnetz und dem Universitätsnetz und damit auch den Diensten des Internets. Es versteht sich von selbst, dass dies eine sensible Verbindung zwischen beiden Netzwerk-Bereichen darstellt. Ein Ausfall dieser Verbindung führt in zunehmendem Maß zu einer starken Beeinträchtigung der Arbeitsfähigkeit der Mitarbeiter/innen der Universitätsverwaltung. Viele Kommunikationsbeziehungen werden mittlerweile zu großen Teilen oder gar gänzlich via gemeinsamer Nutzung von

Dateien, Verzeichnissen oder E-Mail innerhalb des Verwaltungsnetzes abgewickelt.

Ausfallsicherheit

Im Oktober 2003 kam es infolge eines Stromausfalls zu einer Havarie. Der vermutlich durch Selbstinduktion im Stromkreis aufgetretene Stromstoß beim automatischen Reboot der Systeme erzeugte bei zwei Hauptkomponenten des Firewall-Systems trotz des Vorhandenseins einer USV einen technischen Ausfall der Stromversorgung. Zu diesem

Eine Brücke verbindet. Das Firewall-System des Verwaltungsnetzes verbindet dieses mit dem Universitätsnetz und damit auch mit den verschiedenen Diensten des Internets. Es war schon des Öfteren Gegenstand von Artikeln im CMS-Journal. Diesmal soll es um die Neuerungen gehen, die sich durch den Aufbau des Windows-Netzwerkes und die gezielte Öffnung nach außen durch das System für die Online-Prüfungsanmeldung ergeben.



Abb. 1: Die derzeit höchste Autobahnbrücke der Welt überquert im Süden Frankreichs den Flusslauf des Tarn auf einer Strecke von 2,5 km in 270 m Höhe über dem Tal. Funktion und Komplexität eines solchen Bauwerkes lassen sich auf die Anforderungen der Anbindung des Verwaltungsnetzes an Internet-Dienste übertragen. Foto: 2005 Roland Herbst

Zeitpunkt war Redundanz mit den uns zur Verfügung stehenden finanziellen und technischen Mitteln nur in begrenztem Rahmen möglich. Die Netzteile der Server waren redundant ausgelegt. Doch dies konnte uns vor dem geschilderten Ausfall nicht bewahren, denn die Steuer-Elektronik, die die Funktion beider Netzteile überwacht, war ausgefallen und hatte zu einem Folgeschaden geführt.

Zu diesem Zeitpunkt befand sich das neue Firewall-System bereits in der Planung. Aufgrund dieses Vorfalles wurde im Konzept besonders auf Redundanz geachtet. Schon in den DFN-Projekten wurde auf die Nutzung von Open-Source-Lösungen orientiert. Das aktuelle Firewall-System besteht aus verschiedenen Komponenten, die aus diesem Bereich stammen. Auf die Open-Source-Problematik soll hier nicht näher eingegangen werden, da sich ein anderer Artikel des Heftes speziell mit dieser Fragestellung auseinandersetzt.

Mittlerweile sind Systeme verfügbar, die den redundanten Aufbau der sensiblen Komponenten eines Firewall-Systems ermöglichen und damit die zu erwartenden Systemausfallzeiten auf ein erträgliches Maß zu reduzieren helfen.

Neue Bedrohungen

Das Firewall-System des Verwaltungsnetzes gerät immer wieder in die Kritik, da sich die Nutzer des Verwaltungsnetzes von diesem in ihrer Arbeitsfähigkeit eingeschränkt fühlen. Es werden Meinungen laut, man solle die Sicherheitsrichtlinien reduzieren. Dies ist ein verständlicher Wunsch, wenn es um die Bequemlichkeit geht. Neue Angriffsformen, die in der zurückliegenden Zeit entstanden sind, haben unsere restriktive Sicherheitspolitik im Verwaltungsnetz bestätigt. Dabei ist das Firewall-System eine Komponente, die gemeinsam mit einer Standard-Systeminstallation, einem automatischen Einspielen von Patches und einem automatischen zentral administrierten Virens Scanner – um hier nur einige Komponenten zu nennen – für die Sicherheit der Systeme sorgt. Computer, die sich nicht hinter einem Firewall-System befinden und keine eigenen Fire-

wall-Funktionen besitzen, sind immer wieder Ziele erfolgreicher Angriffe ohne Einwirkung des Nutzers aus dem Netzwerk heraus. Es ist ausreichend, dass sich das System in einem Netzwerk befindet.

Bot-Viren und Bot-Netze

Bots sind Programme, die sich auf Wirtsrechnern einnisten und von dort aus meist ferngesteuert ihr Unwesen treiben. Der Prozess der Infektion erfolgt fast immer nach dem gleichen Schema: Von einem Angreifer aus wird eine Vielzahl von Systemen z. B. mittels netzwerkbasierender Würmer kompromittiert. Danach wird meist eine Trojaner-Komponente nachgeladen, die es dem Angreifer ermöglicht, das System fernzusteuern. Die daraus entstandenen Bot-Netze werden von den Angreifern z. B. zur Versendung von Massenmails missbraucht. Außerdem können die kompromittierten Systeme auch im Rahmen einer konzentrierten Aktion gegen die Systeme eines Netzwerkbetreibers oder eines Softwareherstellers für einen Angriff auf dessen Verfügbarkeit genutzt werden. Man spricht dann auch von einem DDoS-Angriff (Distributed Denial of Service).

Phishing

Phishing ist eine Wortschöpfung, die sich inhaltlich aus »Password« und »Fishing« bildet. Alternativ lässt sich der Begriff auch so erklären, dass in der Cracker-Szene das »F« als Anfangsbuchstabe eines Wortes gern durch »Ph« ersetzt wird. Welche genaue Erklärung man nun heranzieht, Ziel ist es immer, die Authentifizierungsinformationen eines autorisierten Nutzers zu erlangen. Besonders häufig tritt diese Angriffsform im Zusammenhang mit der Nutzung von Online-Banking-Verfahren auf. Das Opfer des Angriffes erhält eine speziell präparierte E-Mail, die einen Web-Link enthält, dessen Zieladresse erst nach genauer Analyse zu erkennen ist. Zur Anwendung kommen hier meist Redirect-Technologien.

Mittlerweile gibt es wohl kaum noch einen Nutzer, der in seinem Postfach keine E-Mail einer Bank gefunden hat, in

der er aufgefordert wird, aus Sicherheitsgründen ein paar seiner Transaktionsnummern (TANs) zu verwenden, um auf das aktuelle Sicherheitsverfahren umzustellen. Bei diesen E-Mails handelt es sich immer um Phishing-Versuche. Banken fordern ihre Nutzer niemals zur Preisgabe der Identitätsinformationen über ungeschützte Kommunikationskanäle auf.

Öffnung zum Internet

Anfang 2006 werden die Systeme der Universitätsverwaltung erstmals für einen breiten Nutzerkreis zur Online-Prüfungsanmeldung für den Zugang aus dem Internet geöffnet. Der Aufbau dieses Systems erfolgte zeitgleich mit dem der Hauptkomponenten des neuen Firewall-Systems. Aufbau und Funktion des Systems zur Online-Prüfungsanmeldung werden in einem separaten Artikel in diesem Heft beschrieben. Die Testphase verläuft bisher erfolgreich. Die öffentlich zugänglichen Web-Server des Systems befinden sich in der Demilitarisierten Zone (DMZ) des Firewall-Systems. Die Kommunikation wird über SSL abgesichert. Dies ist eine Anwendung der PKI-Services der Humboldt-Universität (HUC-A). Da man auf eine funktionierende Verschlüsselungsinfrastruktur auf Basis von X.509 zurückgreifen kann, wird es überhaupt möglich, Verschlüsselungs- und Authentifizierungslösungen in der geforderten Professionalität umzusetzen.

Angreifer

Die Abbildung 2 zeigt den Ausschnitt eines automatisch generierten und anonymisierten Log-Files aus dem aktuellen Firewall-System.

Auf Port 135 und 445 werden die bekanntesten netzwerkbasierenen Angriffe auf Windows-basierte Systeme durchgeführt. Port 135 ist der Microsoft RPC-Port (Remote Procedure Call), auf dem verschiedene andere Netzwerk-Dienste aufbauen und Port 445 ist ein Standard-Port für den Datenaustausch von Microsoft-Systemen über das SMB-Protokoll (Server Message Block). Derjenige, der

```

Nov 10 06:17:15 TCP 141.20.HU-Subnetz-1.host-1:1442 -> 141.20.UV-Subnetz-1.host-1:445
Nov 10 11:52:35 TCP 141.20.HU-WLAN-1.host-1:3693 -> 141.20.UV-Subnetz-1.host-1:135
Nov 10 12:07:03 TCP 141.20.HU-Subnetz-2.host-1:1143 -> 141.20.UV-Subnetz-1.host-1:445
Nov 10 12:13:57 TCP 141.20.HU-WLAN-1.host-1:4809 -> 141.20.UV-Subnetz-2.host-2:135
Nov 10 12:43:42 TCP 141.20.HU-Subnetz-2.host-1:1311 -> 141.20.UV-Subnetz-2.host-1:135
Nov 10 14:44:42 TCP 141.20.HU-WLAN-2.host-1:3455 -> 141.20.UV-Subnetz-2.21:135
Nov 10 14:48:56 TCP 141.20.HU-Subnetz-3.host-1:3749 -> 141.20.UV-Subnetz-2.host-1:135
Nov 10 14:48:59 TCP 141.20.HU-Subnetz-3.host-1:3749 -> 141.20.UV-Subnetz-2.host-1:135
Nov 10 15:16:30 TCP 141.20.HU-Subnetz-4.host-2:4801 -> 141.20.UV-Subnetz-3.host-1:135
Nov 11 00:54:44 TCP 141.20.HU-Dialin-1.host-1:3499 -> 141.20.UV-Subnetz-1.host-2:135
Nov 11 00:57:55 TCP 141.20.HU-Dialin-1.host-2:1070 -> 141.20.UV-Subnetz-3.host-1:135

```

Abb. 2: Ausschnitt eines automatisch generierten und anonymisierten Log-Files aus dem aktuellen Firewall-System.

für den privaten DSL-Zugang zu Hause einen Router mit integrierter Firewall-Funktion verwendet, sollte doch einmal in das von diesem generierte Log-File schauen. Falls dort ähnliche Informationen gefunden werden, ist das private Netzwerk bezüglich dieser Angriffsformen technisch ähnlich geschützt wie das Verwaltungsnetz.

Externer Browser

Um dennoch eine uneingeschränkte Web-Nutzung zur Internet-Recherche zu ermöglichen, wurde mit den Administratoren der zentralen Terminalserverfarm des CMS eine Nutzung für die Mitarbeiter der Universitätsverwaltung vereinbart. Da nur Bildschirminformationen zum Nutzer hin übertragen werden, bleiben eventuell vorhandene Schädlingsfunktionen außerhalb des Verwaltungsnetzes und können dessen Funktion nicht beeinträchtigen. Die Anbindung erfolgt hierbei über die gleiche Technologie, wie sie zur Anbindung an einen externen Application Service Provider (ASP) zum Einsatz kommt. Die Nutzung steht jedem Mitarbeiter der Universitätsverwaltung, der einen E-Mail-Account besitzt, offen. Die Anleitung zur Nutzung findet man unter:

http://www.cms.hu-berlin.de/dl/vwvedv/empfehlg/spdienste/citrix_adlershof/

OpenBSD – eine Alternative zu Linux

Neben den verfügbaren Lösungen im Linux-Umfeld wird bei Installationen im sicherheitskritischen Bereich in zunehmendem Maß auf Systeme der BSD-

Familie der UNIX-Derivate zurückgegriffen. Im Wesentlichen ist dies auf die Verfügbarkeit von technologischen Lösungen zurückzuführen, die sonst nur mit sehr großem finanziellen Aufwand realisiert werden können. Ein treffendes Beispiel hierzu ist das OpenBSD-System. OpenBSD zeichnet sich durch eine Vielzahl von Funktionen aus, die es im Bereich der Netzwerksicherheit als Schweizer Offiziersmesser erscheinen lassen. Stellvertretend seien hier nur einige Eigenschaften erwähnt:

- Die (bisher nicht widerlegte) Aussage, dass in den letzten 8 Jahren nur eine Sicherheitslücke aufgetreten ist, die

remote (von einem anderen System aus dem Netzwerk heraus) ausgenutzt werden konnte,

- der IP-Filter PF, der eine zustandsbasierte Filterung von IP-Diensten auch für verbindungslose Protokolle (UDP) gestattet,
- das CARP (Common Address Redundancy Protocol), welches den Aufbau von hochverfügbaren Firewalls erlaubt und
- die Möglichkeit, das System in einen Zustand versetzen zu können, in dem zur Laufzeit keine Änderungen an den Filtertabellen durchgeführt werden können.

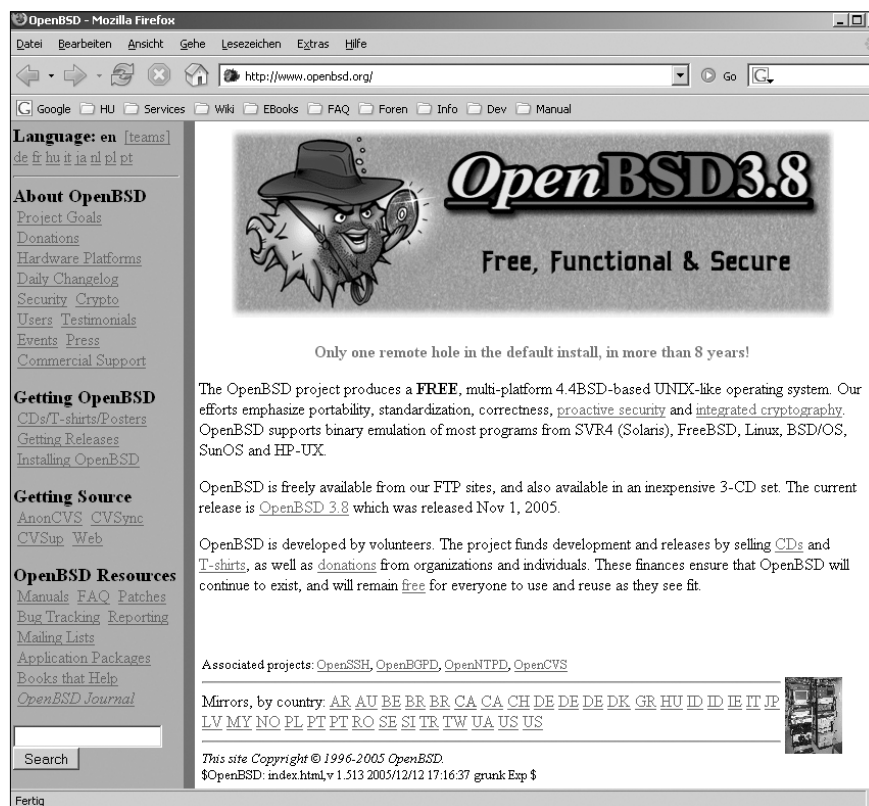


Abb. 3: Die OpenBSD-Installation hatte in den letzten 8 Jahren nur eine Sicherheitslücke, die remote aus dem Netzwerk heraus ausgenutzt werden konnte.

OpenBSD liegt vollständig im Quellcode vor und ist unter der speziellen BSD-Lizenz frei verfügbar. Zum gegenwärtigen Zeitpunkt ist Version 3.8 aktuell.

Eines der oben beschriebenen Features, das CARP-Protokoll, wird später näher erläutert, da es eine wesentliche Eigenschaft des neuen Firewall-Systems verkörpert. Das CARP-Protokoll ist seit Version 3.5 des Betriebssystems in OpenBSD integriert. In der letzten Zeit sind mehrere Artikel in Fachzeitschriften erschienen, die sich mit dem Einsatz von OpenBSD als Firewall-System auseinander setzen [2],[3].

Neuerungen

Nachfolgend werden die wichtigsten Neuerungen des Firewall-Systems beschrieben. Dazu zählen:

- Dynamische Filterung mit PF (Packet Filter)
- Redundanz durch CARP
- Neue interne Dienste
- Windows-Netzwerk

Dynamische Filterung mit PF (Packet Filter)

Das bisherige Firewall-System nutzt IP-Filter, die mit statischen Regeln für Hin- und Rückrichtung der Pakete konfiguriert werden. Mittlerweile kann die IP-Filterung zustandsorientiert (stateful) durchgeführt werden. Jede Verbindung, die die Filter-Engine zugelassen hat, wird in einer dynamischen Zustandstabelle gespeichert.

Pakete, die das Firewall-System erreichen, werden mit den in dieser Zustandstabelle vorhandenen Verbindungen verglichen und entsprechend behandelt. Gehört das Paket zu einer bestehenden, also dem System bekannten Verbindung, lässt es der IP-Filter passieren, ohne die Filterregeln darauf anzuwenden. Andernfalls wird das Regelwerk normal durchlaufen. In Abhängigkeit vom Resultat wird entweder eine neue Verbindung in die Tabelle aufgenommen oder das Paket wird im einfachsten Fall verworfen (drop).

Die grundsätzliche Funktion einer TCP-Verbindung (Transmission Control

Protocol) ist bereits in [1] erklärt worden, deshalb sind hier nur die Änderungen bezüglich der Verbindung bei der zustandsorientierten Filterung durch einen IP-Filter aufgeführt. Beim Verbindungsaufbau wird in Richtung des Zieles ein TCP-Paket mit gesetztem SYN-Flag gesendet. Der IP-Filter prüft das Paket gegen das Regelwerk. Handelt es sich um eine erlaubte Verbindung, wird diese in die Zustandstabelle übernommen. Alle zu dieser Verbindung gehörenden Pakete betrachtet das System als evaluiert. Die Beschreibung des Hin- und Rückweges einer Verbindung erfolgt mit nur einer Regel. Deshalb werden insgesamt weniger Regeln für die Beschreibung der erlaubten Kommunikationsbeziehungen benötigt.

Die beschriebene Zustandsorientierung gilt prinzipiell auch für UDP-Pakete (User Datagram Protocol). Obwohl UDP nicht verbindungsorientiert arbeitet, löst man das Problem, indem Anfrage und Antwort in einem kurzen Zeitintervall betrachtet werden. Ist an die entsprechende Ziel-Adresse im betrachteten Zeitraum eine Anfrage gesendet worden, können die Antwortpakete den IP-Filter

passieren. Abbildung 4 zeigt die Konfiguration für einen einfachen IP-Filter.

Redundanz durch CARP

Das CARP-Protokoll (Common Address Redundancy Protocol) stellt die Entwicklung einer Alternative zum patentierten HSRP (Hot Standby Router Protocol) dar, welches eine Implementierung des im RFC 3768 veröffentlichten Vorschlages für einen offenen Standard VRRP (Virtual Router Redundancy Protocol) darstellt (<http://www.ietf.org/rfc/rfc3768.txt>). HSRP ist ein Produkt des Netzwerkhersellers Cisco Systems und unterliegt patentrechtlichen Beschränkungen. Da HSRP auf VRRP basiert, hätte VRRP nicht in ein offenes System wie OpenBSD integriert werden können. Soweit ein kleiner Exkurs in die Welt der Software-Patente, deren Wirkung an diesem Beispiel vielleicht besonders deutlich wird.

Seit Version 3.5 ist CARP in OpenBSD integriert.

Beim CARP-Protokoll werden zwei Maschinen (Master, Backup) betrachtet, die sich im gleichen Netzwerk befinden (s. Abb. 5).

```
ext_if = »fxp0«
int_if = »dc0«
lan_net = »192.168.0.0/24«
# scrub incoming packets
scrub in all
# setup a default deny policy
block in all
block out all
# pass traffic on the loopback interface in either direction
pass quick on lo0 all
# activate spoofing protection for the internal interface.
antispoof quick for $int_if inet
# only allow ssh connections from the local network if it's from the
# trusted computer, 192.168.0.15. use »block return« so that a TCP RST is
# sent to close blocked connections right away. use »quick« so that this
# rule is not overridden by the »pass« rules below.
block return in quick on $int_if proto tcp from ! 192.168.0.15 \
to $int_if port ssh flags S/SA
# pass all traffic to and from the local network
pass in on $int_if from $lan_net to any
pass out on $int_if from any to $lan_net
# pass tcp, udp, and icmp out on the external (Internet) interface.
# keep state on udp and icmp and modulate state on tcp.
pass out on $ext_if proto tcp all modulate state flags S/SA
pass out on $ext_if proto { udp, icmp } all keep state
# allow ssh connections in on the external interface as long as they're
# NOT destined for the firewall (i.e., they're destined for a machine on
# the local network). log the initial packet so that we can later tell
# who is trying to connect. use the tcp syn proxy to proxy the connection.
pass in log on $ext_if proto tcp from any to { !$ext_if, !$int_if } \
port ssh flags S/SA synproxy state
```

Abb. 4: Beispiel einer PF-Konfigurationsdatei für einen IP-Filter, der SSH-Verbindungen in das innere Netz zulässt

Es existiert eine Virtuelle IP-Adresse, die Master und Backup bekannt ist. Die Kommunikationspartner kennen nur diese Virtuelle IP-Adresse. Der Initiator der Kommunikation baut eine Verbindung zu dieser virtuellen IP-Adresse auf. Er sendet also eine ARP-Anfrage in das Netzwerk hinein, um die Ethernet-Adresse des Kommunikationspartners (MAC-Adresse) in Erfahrung zu bringen. Beide beteiligten Systeme sind für die CARP-Funktion speziell konfiguriert. Ein System befindet sich dabei im aktiven Zustand (Master) und ein anderes wartet passiv auf seinen Einsatz (Backup). Der Master sendet an eine bestimmte Multicast-Netzwerk-Adresse Informationen über seine Erreichbarkeit (Advertisements). Das Backup-System lauscht auf dieses Lebenszeichen und befindet sich solange in diesem Zustand, bis die Advertisement-Informationen nicht mehr bei ihm ankommen. Ist dies der Fall, geht der Backup-Server von einem Ausfall des Master-Systems aus und übernimmt dessen Funktion. ARP-Anfragen an die Virtuelle IP-Adresse werden jetzt vom neuen Master-System beantwortet. Diese Konfigurationsänderung erfolgt automatisch und im Bereich von Sekundenbruchteilen.

Auf diese Weise kann man Server oder wie hier die IP-Filter eines Firewall-Systems redundant aufbauen, was in der neuen Sicherheits-Infrastruktur des Verwaltungsnetzes verwirklicht worden ist. Die Proxy-Server-Komponenten werden über andere Technologien redundant ausgelegt. Zur Anwendung kommen hier Virtuelle Maschinen, die Gegenstand eines weiteren Artikels in diesem Heft sind und deshalb an dieser Stelle nicht weiter beschrieben werden sollen.

Basisdienste

Um das Windows-Netzwerk im inneren Verwaltungsnetz in Betrieb nehmen zu können, mussten neben den notwendigen inhaltlichen und organisatorischen Voraussetzungen zusätzliche Basisdienste innerhalb des Verwaltungsnetzes aufgebaut werden, die in ihrer Funktion hier kurz skizziert werden sollen. Die Anbindung an das Universitätsnetz erfolgt über das Firewall-System. Deshalb

sind diese Basisdienste integraler Bestandteil des neuen Firewall-Konzeptes.

Zeitsynchronisation

Eine Grundvoraussetzung für den Betrieb des Windows-Netzwerkes im Verwaltungsnetz ist ein Zeit-Service. Mit der Außenwelt wird der interne Zeit-Service über einen Proxy im Firewall-System synchronisiert, der sich wiederum mit dem zentralen Zeitserver des CMS abgleicht. Am Ende der Kette steht ein Zeitnormal einer Funkuhr, wie sie sich mittlerweile in jedem modernen Haushalt befinden dürfte. Erst durch konsequente Zeitsynchronisation erhält man überhaupt die Möglichkeit, Systemereignisse im Kontext zu interpretieren. Dies können z. B. Informationen zu Systemstörungen technischer Art oder Verstöße gegen die Sicherheit der Systeme sein.

Interner DNS

Dass die Infrastruktur des Verwaltungsnetzes »erwachsen« geworden ist, ist auch an den internen DNS-Systemen zu erkennen. Bisher wurde diese Funktion durch einen in der Installation relativ einfachen DNS-Proxy im Firewall-System realisiert. Der Aufbau des Windows-Netzwerkes erforderte auch hier eine grundsätzliche Änderung. Der DNS-Service wurde um zusätzliche interne DNS-Server erweitert. Die Systeme sind als Master und Slave konfiguriert. Fällt der Master aus, übernimmt der Slave

dessen Funktion und die Namensauflösung in IP-Adressen und umgekehrt funktioniert weiterhin zuverlässig. Diese Funktionalität wird bereits durch das Design der eingesetzten BIND-Software ermöglicht.

In der DMZ des Firewall-Systems befinden sich zwei weitere DNS-Server, die über einen reduzierten Datenbestand verfügen. Diese sind für die DNS-Informationen zuständig, die extern angeboten werden. Man spricht hierbei von einer Splitting-DNS-Konfiguration. DNS-Abfragen zu internen Systemen können nur von innen erfolgen und müssen nicht in den Systemen der DMZ vorgehalten werden.

Der aufmerksame Leser wird feststellen, dass eine solche Konfiguration prinzipiell auch mit Windows-Servern möglich ist. In Anlehnung an den Standard des CMS im Windows-Netzwerk des übrigen HU-Netzes wurde die Installation der DNS-Server auf UNIX-Basis auch im Verwaltungsnetz realisiert.

Zentrale Windows Log-Hosts

Will man Dienste professionell betreiben, ist es notwendig, dass man jederzeit über die Betriebsbereitschaft der Systeme informiert ist. An den Stellen, wo der Aufwand vertretbar ist, versucht man, Systeme redundant auszulegen. Dies ist jedoch nicht nur eine finanzielle, sondern sehr oft auch eine technische Herausforderung. Die Server des Windows-Netz-

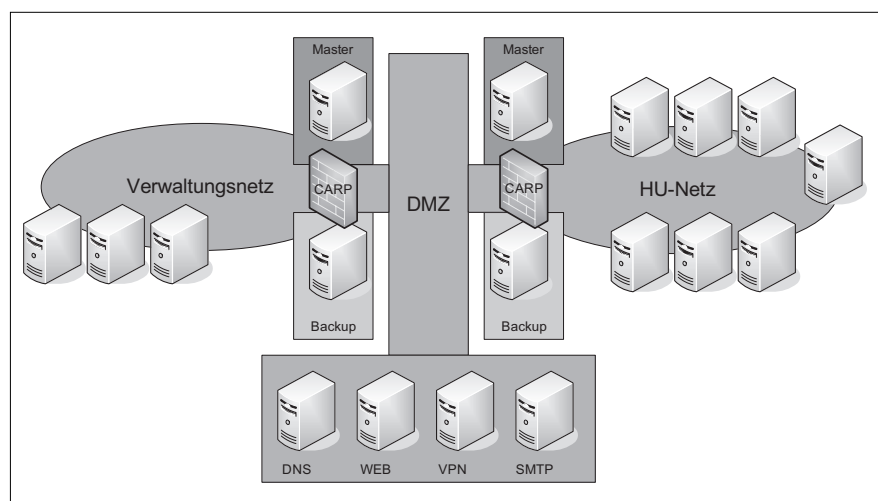


Abb. 5: Durch die Anwendung von OpenBSD CARP kann für die IP-Filter Redundanz erreicht werden. Bei Ausfall des primären Systems übernimmt das Backup-System automatisch die Funktion.

werkes werden zentral administriert. Die Komplexität eines solchen Netzes ist um einiges höher als in dem bisherigen genutzten System. So sind einzelne Dienste voneinander abhängig, der Ausfall eines einzigen führt zum Stillstand des gesamten Komplexes. Genau hier ist der Ansatz für ein System, welches zentral Systemmeldungen entgegennimmt, automatisiert auswertet und die Administratoren zeitnah informiert.

Die Kern-Komponenten des Windows-Netzwerkes der Universitätsverwaltung werden abteilungsübergreifend von den Spezialisten des CMS administriert. Die automatisierte Überwachung des Zustandes des Windows-Netzwerkes durch die Kombination der Open-Source-Systeme Syslog-NG und Nagios ermöglicht eine zeitnahe Reaktion der Administratoren auf kritische Systemzustände. Mittlerweile wurden in das Log-System auch andere Dienste des Verwaltungsnetzes integriert.

Fazit

Die Anforderungen an die IT entwickeln sich zunehmend in Richtung mobiler Nutzung von Ressourcen. Diese Entwicklung wird auch vor den eingesetzten Sicherheitsmechanismen im Verwaltungsnetz nicht haltmachen. War noch bis vor einigen Jahren der stationäre PC das vorherrschende Arbeitsmittel, so wird dieser infolge ständig fallender Preise für Hardware und Equipment zu-

nehmend von Notebooks verdrängt. Dadurch ergeben sich neue Anforderungen an das Sicherheitskonzept.

Theoretisch sind die Nutzer in der Lage, die alltäglichen Aufgaben quasi an jedem beliebigen Ort der Welt durchzuführen, praktisch benötigen sie dazu eine sichere Umgebung, um auf ihre Applikationen und Daten zuzugreifen. Um auch mit dem Notebook auf der Datenautobahn sicher zu reisen, sind zusätzliche Sicherheitsmaßnahmen erforderlich. Dies betrifft sowohl das Notebook selbst als auch die Infrastruktur, die den Nutzern vom CMS zur Verfügung gestellt wird.

Die Anforderungen diesbezüglich werden in den kommenden Jahren stark ansteigen. Die Anfänge dieser Entwicklung sind schon jetzt für uns spürbar. Aus der Lektüre dieses Beitrages ist vielleicht zu entnehmen, dass das CMS große Anstrengungen unternimmt, die Bedingungen der netzwerkbasierter Zusammenarbeit zu verbessern. Der Autor denkt, es ist im Sinne aller Mitarbeiter der Universität, dass zusätzliche Dienste in der Universitätsverwaltung erst dann zur Verfügung gestellt werden, wenn dies mit dem Sicherheitskonzept des Verwaltungsnetzes vereinbar ist und ausreichend Zeit für Design, Entwicklung, Erprobung und Einführung von neuen Lösungen investiert wird. Ein diesbezüglicher Schnellschuss könnte zu leicht ins Auge gehen.

Literatur

- [1] HERBST, R.: Das Firewall-System des Verwaltungsnetzes. *cms-journal* Nr. 23, 18.04.2002.
- [2] TESCH, ST.: Doppelwacht – Redundante Firewalls mit OpenBSD. *iX* 5/05, Seite 150.
- [3] RICKAUER, ST., A.: »Wehrhaft abtauchen« – HA-fähige Firewall mit OpenBSD/PF (Packet Filter). *Linux-Magazin* 12/05, Seite 64.
- [4] <http://www.cms.hu-berlin.de/ueberblick/projekte/firewall/index.html>
- [5] <http://webdoc.sub.gwdg.de/ebook/ah/dfn/UVsec.pdf>
- [6] <http://www.dfn.de/content/fileadmin/2Entwicklungen/SichereHSVerwaltung.pdf>
- [7] <http://www.ietf.org/rfc/rfc3768.txt>
- [8] <http://www.heise.de/ct/browsercheck/>
- [9] <http://www.heise.de/>
- [10] <http://www.microsoft.com/security/>
- [11] <http://www.openbsd.org/>
- [12] <http://www.openbsd.org/faq/pf/>