Das Sicherheitskonzept der Universität Karlsruhe

Bruno Lortz

Universität Karlsruhe
Rechenzentrum
76128 Karlsruhe
lortz@rz.uni-karlsruhe.de

1 Grundkonzepte

Die zunehmende Zahl der Hackerangriffe aus dem Internet führte auch an der Universität Karlsruhe dazu, dass immer wieder kompromittierte Rechner neu installiert werden mussten. Dies bedeutete jedes mal einen hohen Aufwand für die Systemverwalter und einen mehrtägigen Ausfall der betroffenen Rechner. Oft gingen auch wichtige Daten verloren. Daraus ergab sich die Notwendigkeit, die am Campusnetz angeschlossenen Rechner verstärkt zu schützen. Deshalb hat eine Arbeitsgruppe am Rechenzentrum ein Sicherheitskonzept (siehe [1]) entwickelt, das schrittweise realisiert werden soll. Neben einer Reihe weiterer Maßnahmen wurden die folgenden fundamentalen Sicherheitskonzepte diskutiert und gegeneinander abgewogen:

- Der direkte Schutz der Endgeräte
- Der Schutz von Netzen durch vorgeschaltete Firewallsysteme

1.1 Direkter Schutz der Endgeräte

Ein direkter Schutz der Endgeräte selbst erlaubt es, in Abhängigkeit von den jeweiligen Anforderungen des Anwenders gezielte Maßnahmen zu ergreifen und so das Gerät optimal zu sichern. Es können Angriffe von allen Rechnern am Netz (lokal und aus dem Internet) abgewehrt werden. Es gibt also kein Insider-Problem. Auf diese Weise ist theoretisch ein optimaler Schutz erreichbar.

In der Praxis sind aber sehr viele aufwändige Vorkehrungen zu treffen, u.a.:

- Auf dem Gerät müssen alle nicht benötigten Funktionen (Ports) gesperrt werden.
- Alle bekannten Fehler im Betriebssystem und in den Anwendungen müssen beseitigt werden. Da immer wieder neue Fehler bekannt werden, ist dies eine permanente Aufgabe.
- Es ist darauf zu achten, dass für den Zugriff über das Netz eine sichere Authentisierung durchgeführt wird. Dies erfordert mindestens das Erzwingen von sicheren Passwörtern für den Rechnerzugang.

Diese Vorkehrungen bedingen für jedes Endgerät einen sehr hohen Aufwand, der nur für wenige, besonders wichtige Geräte ohne Abstriche geleistet werden kann. Dennoch sollten auf allen Geräten wenigstens die gravierendsten Sicherheitslücken beseitigt werden. Dies ist eine wichtige Ergänzung zum Schutz durch Firewallsysteme.

1.2 Schutz von Netzen durch Firewallsysteme

Ein Firewallsystem schützt ein ***inneres*** Netz gegen Angriffe von außen, z.B. ein Universitätsnetz gegen das Internet. Ein wichtiger Vorteil dabei ist, dass nur eine Sicherheitseinrichtung für ein ganzes Netz notwendig ist und dass dadurch der Aufwand zur Pflege und Überwachung im Vergleich zum Endgeräteschutz wesentlich geringer wird. Firewallsysteme unterstützen ferner in der Regel das Erkennen von Angriffen durch umfangreiches Logging.

Leider gibt es auch eine Reihe von Nachteilen. Ein Firewallsystem bietet niemals absoluten Schutz, insbesondere professionelle Angreifer haben gute Aussichten, Firewallsysteme zu überwinden. Der erreichbare Schutz hängt von Anforderungen an die möglichen Außenverbindungen (***Konnektivität***) ab. Diese werden mit einer ***Sicherheitspolicy*** beschrieben, die festlegt, welche Anwendungen für welche Endgeräte zugelassen sind. Das Anwendungsspektrum sollte dabei möglichst weitgehend beschränkt werden, da in der Regel jede zusätzliche Anwendung die erreichbare Sicherheit verringert. Besondere Vorsicht ist geboten, wenn der Zugriff von außen nach innen zugelassen wird. Eine strenge Policy ist nur dann möglich, wenn im inneren Netz weitgehend einheitliche Anwendungen genutzt werden. Diese Voraussetzung ist in der Regel nur bei kleinen Netzen gegeben.

Zu beachten ist ferner, dass Angriffe nicht nur von außen, sondern auch von innen, also aus dem eigenen Netz erfolgen können. Die Gefahr solcher ***Insider-Angriffe***, gegen die kein Firewallsystem schützen kann, steigt mit der Größe des inneren Netzes.

Universitätsnetze sind in der Regel sehr groß. In Karlsruhe gibt es weit mehr als 10000 Endgeräte. Die Anforderungen der verschiedenen Anwenderkreise sind extrem unterschiedlich:

- ***Studenten:*** Die Studenten fordern eine breites Anwendungsspektrum. Dazu gehört auch eine Reihe von Anwendungen, die nicht mit Firewallsystemen verträglich sind. Einschränkungen werden nur selten akzeptiert, Sicherheitsanforderungen sind daneben zweitrangig.
- ***Institute:*** Die einzelnen Institute haben in der Regel ein beschränktes Anwendungsspektrum. Ihre Teilnetze können meist sehr gut über Firewallsysteme abgesichert werden. Untereinander unterscheiden sich die Institute erheblich durch ihre speziellen Anforderungen an Sicherheit und Konnektivität. So legt ein Teil der Institute hauptsächlich Wert darauf, dass seine Rechner nicht durch Fremde missbraucht werden können, andere dagegen speichern auf ihren Systemen sehr sensitive Daten, die keinesfalls von dritten eingesehen oder gar verändert werden dürfen. Dies macht es unmöglich, für alle Institute eine gemeinsame Policy mit hoher Schutzwirkung zu definieren.
- ***Universitätsverwaltung:*** Hier gibt es besonders hohe Sicherheitsanforderungen. Die Verwaltung betreibt daher ihre Sicherheitseinrichtungen selbstständig. Sonst sind die Gegebenheiten ähnlich wie bei den Instituten.

2 Verteilte Firewallsysteme

Diese vielfältigen Anforderungen können durch ein zentrales Firewallsystem allein nicht abgedeckt werden. Um die Anforderungen besser erfüllen zu können, plant die Universität Karlsruhe ein mehrstufiges, verteiltes Firewallsystem aufzubauen.

2.1 Stufe1: zentrales Firewallsystem

An der Universität Karlsruhe erfolgt der Übergang zum Internet über einen sehr leistungsfähigen Router. Dieser wird schon seit längerer Zeit zusätzlich als einfaches Firewallsystem genutzt und wehrt über statische Filterlisten eine Reihe bekannter Angriffe ab. Er bildet so eine erste Barriere, die ***Hauptpforte***. Diese hat sich durchaus bewährt, so dass ihre Funktionalität ausgebaut wurde. Die ursprünglich negative Filterliste (*alles, was nicht verboten ist, ist erlaubt*) wurde auf eine positive Liste (*alles, was nicht erlaubt ist, ist verboten*) umgestellt.

Mit der Hauptpforte kann aber nur ein eingeschränkter Grundschutz realisiert werden. Gründe dafür sind:

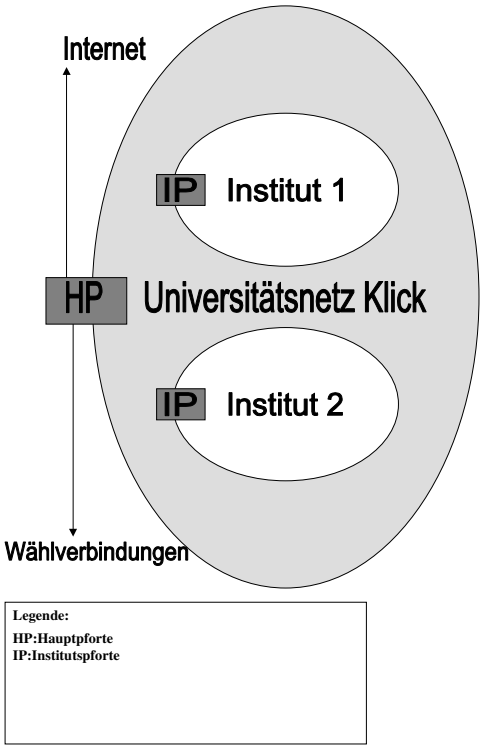
- Die stark differierenden Konnektivitätsanforderungen der verschiedenen Benutzerkreise, die eine gemeinsame Sicherheitspolicy sehr erschweren.

- Der große Benutzerkreis, der eine hohe Wahrscheinlichkeit von Insiderangriffen bedingt.

Der Schutz würde nur wenig verbessert, wenn man den Router durch ein separates Firewallsystem ergänzen würde. Wegen unseren hohen Bandbreiteanforderungen (mehrere G-Bit/s) würden aber erhebliche zusätzliche Kosten entstehen. Da dies nicht wirtschaftlich wäre, sind hier derzeit keine technischen Änderungen geplant.

2.2 Stufe 2: dezentrale Firewallsysteme

Eine zweite, dezentrale Barriere schützt Teilnetze gegeneinander und gegen das Internet. Typisch für solche Teilnetze sind die Institutsnetze, aber auch einige sonstige sensitive Netzbereiche. Hier werden leistungsfähige Firewallsysteme, die ***Institutspforten***, eingerichtet. Für diese werden strenge Sicherheitspolicys definiert, die dem jeweiligen Bedarf der Einrichtung angepasst sind. Es wird angestrebt, Installation und Pflege dieser Systeme weitgehend am Rechenzentrum durchzuführen, da dort ein weit geringerer Personalaufwand notwendig ist, als wenn jedes Institut diese Aufgabe selbst durchführt.



An die Institutspforten werden in der Regel drei Netze angeschlossen:

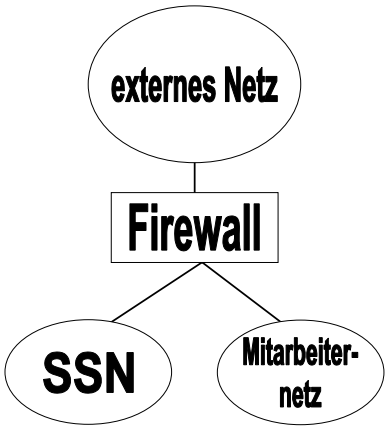
- Das allgemeine Universitätsnetz mit Anschluss an das Internet
- Das Mitarbeiternetz
- Ein sicheres Servernetz (SSN), das die öffentlich zugänglichen Server des Instituts enthält. Für das SSN findet man auch häufig die Bezeichnung *demilitarisierte Zone (DMZ).*

In einigen Fällen besteht auch ein Bedarf an weiteren separaten Teilnetzen wie z.B.:

- ein Sekretariatsnetz
- ein Studentennetz
- ein Hochsicherheitsnetz mit Rechnern, auf denen besonders vertrauliche Daten gehalten werden.

Standardpolicy

Für die Institutsnetze wird eine Standardpolicy festgelegt, die ein grundlegendes Sicherheitskonzept für Institutsnetze beschreibt. Ausgangspunkt ist dabei eine Netzstruktur, die aus einem Mitarbeiternetz und einem SSN besteht. Vom Mitarbeiternetz aus darf weitgehend uneingeschränkt auf das externe Netz und auf das SSN zugegriffen werden. Von der



Verwendung von Protokollen mit unverschlüsselten Passwörtern (Telnet, FTP,...) wird jedoch dringend abgeraten, sie werden nur auf expliziten Wunsch der Institute freigeschaltet. Daneben sind solche Protokolle gesperrt, die über Firewallsysteme nicht oder nur mit erheblichen Sicherheitseinschränkungen vermittelt werden können. Dies sind in der Regel Protokolle mit dynamischen Ports, wie sie auch die meisten Dateizugriffsprotokolle (z.B. NFS) verwenden.

Der Zugriff vom externen Netz auf das Mitarbeiternetz ist gesperrt. Ausgenommen ist lediglich das SSH-Protokoll, das selbst recht gut gesichert ist. Es wird auf Wunsch für vorgegebene Zielrechner im Mitarbeiternetz zugelassen. Der externe Zugriff auf das SSN richtet sich nach den Funktionen der einzelnen Server. So werden für einen WWW-Server die Protokolle HTTP und HTTPS freigegeben.

Die Sperrung von NFS ist problematisch, da an der Universität ein zentraler Dateiserver im Einsatz ist, auf den viele Institute mit NFS zugreifen. Dies muss auch weiterhin möglich sein. Hier ist geplant, eine Verbindung zum Fileserver unter Umgehung des Firewallsystems einzurichten. Um die notwendigen Sicherheitsvorkehrungen zu treffen, ist der Einsatz eines Routers mit Filterfunktionen vorgesehen.

Nach den Vorgaben der Standardpolicy wird eine Anfangskonfiguration für die Institutspforte erstellt. Diese wird dann in Absprache mit dem Institut so modifiziert, dass sie den betrieblichen Anforderungen gerecht wird.

Zugriff aufs Mitarbeiternetz von außen, Laptops

Für Mitarbeiter, die zeitweise von zu Hause aus oder auf Reisen über das Internet arbeiten, reicht die Zugriffsmöglichkeit über SSH auf die Rechner in ihrem Mitarbeiternetz oft nicht aus. In diesem Fall bietet sich die Einrichtung von virtuell privaten Netzen (***VPN***) über Techniken wie ***PPTP*** und ***IPSec*** an. Nach einer sicheren Authentisierung beim VPN-Server ermöglichen es die Protokolle, so auf die Rechner im internen Netz zuzugreifen, als sei das Endgerät dort direkt angeschlossen.

Der Einsatz von VPN erfordert zusätzliche Maßnahmen, die in der Literatur nur selten erwähnt werden. Das externe Gerät ist nämlich in der Regel an einem ungeschützten Netz angeschlossen und kann dort selbst angriffen werden. Ein erfolgreicher Angreifer kann heimlich das VPN mitbenutzen und so das Firewallsystem umgehen. Ähnliche Probleme treten auch dann auf, wenn SSH zum *Tunneln* anderer Protokolle eingesetzt wird. Geräte, die über VPN auf ein geschütztes Netz zugreifen, müssen daher selbst gut geschützt werden. Hier bieten sich u.a. sogenannte ***persönliche Firewalls*** an, welche einen Endgeräteschutz unter Verwendung von Firewalltechniken realisieren. Die derzeitigen Implementierungen sind aber leider noch unvollständig, ihre Meldungen sind für den nicht

ausgebildeten Benutzter oft schwer verständlich. Trotz dieser Nachteile reduziert der Einsatz persönlicher Firewalls die Gefahren deutlich, man sollte deshalb keinesfalls darauf verzichten.

Eine besonders kritische Situation liegt vor, wenn Geräte (z.B. Laptops) abwechselnd an ein externes und an das geschützte Netz angeschlossen werden. Es besteht dann die Gefahr, dass ein solches Geräte am externe Netz kompromittiert wird und dann später die Sicherheit im internen Netz gefährdet. Die Praxis, mit dem gleichen Laptop zeitweise im Institutsnetz und zeitweise sonst wo am Internet zu arbeiten, ist weit verbreitet, sie nach der Einführung von Firewallsystemen zu verbieten, ist an einer Universität kaum möglich. Die einzige Behelfslösung ist auch hier der Einsatz von persönlichen Firewalls.

Pilotsysteme

Erste Erfahrungen mit Institutspforten wurden mit vier Pilotsystemen gewonnen. Diese Systeme sind Linux-Rechner, auf denen mit dem für Universitäten kostenfreien ***TIS Firewall Toolkit*** ein ***Applikationgateway*** implementiert wurde, das mit den ***Linux ipchains*** zu einem ***hybriden Firewallsystem*** erweitert wurde. Mit diesem System wurden recht gute Erfahrungen gemacht, wenn man von einigen Einschränkungen der Funktionalität absieht. Das Erstellen und Modifizieren der Konfiguration ist jedoch recht aufwendig und fehleranfällig, da es hierfür erforderlich ist, mehrere Textdateien manuell zu editieren. Dies ist sehr fehleranfällig. Für eine große Anzahl betriebener Systeme wird hierdurch zu viel Personalkapazität gebunden. Ferner ist nicht sichergestellt, dass dieses System weiterentwickelt wird, um damit neuartige Anwendungen zu ermöglichen und künftige Angriffstechniken abzuwehren.

Kommerzielle Firewallsysteme

Kommerzielle Firewallsysteme werden in der Regel mit einem übersichtlichen grafischen Managementsystem konfiguriert und überwacht. Ein Wartungsvertrag stellt die rasche Fehlerbeseitigung und die laufende Verbesserung der Systeme sicher, so dass auch neuartige Angriffsmuster erkannt und abgewehrt werden. Auch neuartige Anwendungen werden berücksichtigt. Aus diesen Gründen sollen die Institutspforten auf kommerziellen Firewallsystemen implementiert werden. Dies kann entweder durch Komplettsysteme (Hard- und Software aus einer Hand) oder durch reine Softwaresysteme, die auf einer gängigen Hardwarearchitektur arbeiten - aus preislichen Gründen vorzugsweise PC-Systeme - realisiert werden.

Das Management der dezentralen Firewallsysteme erfolgt zentral vom Rechenzentrum aus. Der Zugriff über offene Netzteile muss dabei sicher authentisiert werden, Managementdaten dürfen nur verschlüsselt übertragen werden. Dies kann u. a. durch IPSec-Tunnels zwischen Managementstation und Firewallsystem erfolgen.

Verwaltungsnetz

Das Netz der Universitätsverwaltung wird schon seit mehreren Jahren durch ein Firewallsystem geschützt. Im Gegensatz zu den Institutsnetzen wird dieses System direkt durch die Universitätsverwaltung konfiguriert und gepflegt.

2.3 Stufe 3: Endgeräteschutz

Als dritte Stufe sollten auch auf den Endgeräten Schutzmaßnahmen vorgenommen werden. Dies ist zwar nur in geringerem Maße notwendig als in einer offenen Umgebung, dennoch sollten bei den Betriebssystemen und Anwendungen die wichtigsten Sicherheitskorrekturen eingespielt werden.

3 Ergänzende Maßnahmen

3.1 Private IP-Adressen

Die Realisierung der dezentralen Firewallsysteme wird einige Zeit benötigen, ferner wird es immer ungeschützte Netzteile geben müssen. Um auch hier den illegalen Zugriff zu erschweren, werden auf Rechnern mit geeigneten Anwendungen ***private IP−Adressen*** (siehe [2]) eingerichtet. Diese Adressen werden im Internet nicht geroutet, die entsprechenden Rechner können von dort nicht *direkt* erreicht werden. Dies stellt einen Grundschutz gegen Angriffe von außen dar. Rechner mit privaten Adressen können über einen Server, der eine Adressumsetzung durchführt (***NAT,*** *Network Address Translation*), auf das Internet zugreifen.

3.2 Zentrale Server

Eine Reihe von Rechnern verbleibt im zentralen Netzbereich, der nur schwach gesichert ist. Dazu gehören:

- Rechner mit Anwendungen, die nicht mit Firewallsystemen verträglich sind.
- Zentrale Server, auf die von der ganzen Universität oder vom Internet aus zugegriffen wird.
- Ausbildungs- und Studentenrechner wegen ihres breiten Anwendungsspektrums.

Auch diese Rechner müssen geschützt werden. Dies gilt ganz besonders für Server, die wichtige Dienste für die Universität oder für das Internet anbieten, so auch für den Supercomputer ***IBM SP***. Unter anderem werden je nach Bedarf folgende Maßnahmen vorgesehen:

- Intensiver Endgeräteschutz, insbesondere für die Server.
- Einsatz privater IP-Adressen soweit möglich.
- Einsatz der Secure Shell SSH.
- Einsatz von DCE/DFS beispielsweise auf dem Parallelrechner IBM SP.

3.3 Mailsystem

Besondere Schutzmaßnahmen sind auch auf den zentralen Mailservern realisiert. In den letzten Jahren sind im Mailbereich zwei Arten von Missbrauch aufgetreten, die teilweise zu erheblichen Problemen geführt haben:

- Mailserver wurden häufig von externen Einrichtungen missbraucht um Massenmails zu verteilen (Mail Relaying).
- Es wurden *aktive Inhalte* in den Anhängen (*Attachments*) zu Angiffen auf die Empfänger der Mails ausgenutzt. Die Empfängersysteme wurden dabei häufig dazu missbraucht, die schädliche Mail weiterzuverbreiten (*Mail Wurm, z.B "I love You"*).

An der Universität Karlsruhe werden deshalb alle eingehenden Mails über einen zentralen Server (*Mail Firewall*) geführt, der eine Reihe von Überprüfungen durchführt. Er verhindert unerlaubtes Mail Relaying und sperrt Anhänge, die ausführbare Programme enthalten. An dieser Stelle sind jederzeit zusätzliche Maßnahmen implementierbar, wenn dies erforderlich werden sollte.

3.4 Organisatorische Maßnahmen

Ergänzend zum Sicherheitskonzept wurden eine Reihe von ergänzenden organisatorischen Maßnahmen vorgenommen:

- Ein ständiger Arbeitskreis aus Mitarbeitern des Rechenzentrums und der Fakultät Informatik beschäftigt sich mit Sicherheitsfragen. Er untersucht Konzepte und Lösungen und schlägt Maßnahmen vor. Dieser Kreis hat das Sicherheitskonzept der Universität entworfen, er wird es den zukünftigen Erkenntnissen und Anforderungen anpassen.
- Eine weitere Arbeitsgruppe, das *Abuse-Team*, erfasst und behandelt Sicherheitsverletzungen durch Universitätsangehörige und Externe.

Literatur

[1] B. Lortz (Federführung), "Das Sicherheitskonzept der Universität Karlsruhe, Maßnahmen zur Abwehr von Angriffen auf Rechensysteme über Netzverbindungen", http://www.uni-karlsruhe.de/Uni/RZ/Netze/sicherheit.pdf. Hier finden sich auch weitere Literaturhinweise.

[2] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, "Address Allocation for Private Internets", RFC 1918