

Sicherheit in Netzwerken (2)

Universitätsverwaltung mit Internet-Zugriff - ein Widerspruch?

In jeder Gesellschaft gibt es einen gewissen Prozentsatz von Leuten, der anderen mutwillig schadet. Das Internet umfaßt derzeit schätzungsweise 60 bis 70 Millionen Nutzer. Auch wenn der Anteil böswilliger Benutzer weniger als ein Prozent der Gesellschaft ausmacht, ist er doch groß genug, um sich mit Netzwerksicherheit auseinandersetzen zu müssen.

Durch das ständig steigende Angebot von Informationen im Internet wächst auch das Bedürfnis der Mitarbeiter, an diese Informationen zu gelangen. Da viele von diesen Mitarbeitern aber täglich mit sensiblen und vertraulichen Daten in unseren lokalen Netzwerken arbeiten, können wir den direkten und ungeschützten Zugang zum Internet nicht gestatten. Hierzu hält das Berliner Datenschutzgesetz und der Abschlußbericht 1995 des Berliner Landesdatenschutzbeauftragten klare Richtlinien für die Berliner Verwaltung bereit. Aus diesen Gründen sahen wir uns gezwungen, diesbezüglich Lösungen bereitzustellen. Diese Lösungen basieren einerseits auf den gegenwärtigen Standards im Sicherheitsmanagement, andererseits auf eigenen Lösungen, die aus unserer Netz-Infrastruktur resultieren. Durch ein Projekt unter finanzieller Beteiligung des DFN-Vereins¹ wollen wir in Zukunft performancebedingte Engpässe beseitigen und die Transparenz für den Anwender erhöhen.

Nachfolgend möchte ich auf einige Konstruktionsansätze bei der Entwicklung einer Firewall-Architektur eingehen. Dieser kleine Streifzug soll die Komplexität und Dynamik eines solchen Firewall-Systems darstellen, hat aber keinen Anspruch auf Vollständigkeit!

Was ist eine Firewall, und welche Vorteile bringt sie uns? Eine Firewall bietet die Möglichkeit, die Kommunikation zwischen dem Internet und unserem internen Netz einzuschränken. Wir haben sie dort eingerichtet, wo sie den größten Effekt erzielen kann: an dem Punkt, wo unser zu schützendes lokales Netz an das Internet angeschlossen ist. Mit einer Firewall läßt sich die Wahrscheinlichkeit erheblich verringern, daß Angreifer von außen in unsere inneren Systeme und Netze eindringen können. Zudem kann die Firewall interne Benutzer davon abhalten, unsere Systeme zu gefährden, indem sie sicherheitsrelevante Informationen, wie unverschlüsselte Paßwörter oder vertrauliche Daten, nach außen geben.

Die heute zu beobachtenden Angriffe auf ans Internet angeschlossene Systeme sind gravierender und technisch komplexer als früher. Um diese Angriffe abzuwehren, benötigen wir jede erdenkliche Hilfe. Firewalls bieten *eine* wirksame Methode, um einen Standort vor Angriffen zu schützen.

¹ Verein zur Förderung eines Deutschen Forschungsnetzes e.V. - DFN-Verein

Sicherheitsstrategien

Bevor wir uns an den Aufbau des Firewall-Systems machten, waren einige Vorarbeiten unumgänglich. Besonders wichtig im Vorfeld eines solchen Projektes war für uns, daß wir eine funktionierende und realistische Security-Policy ausgearbeitet haben. Anhand dieser Policy konnten wir erkennen, welchen Bedarf an Internet-Diensten die Nutzer des Verwaltungsnetzes haben. Besonderes Augenmerk richteten wir auf die Arbeitsplätze, an denen mit personenbezogenen Daten gearbeitet wird. Wir entschieden uns für eine Lösung mit minimalen Zugriffsrechten im Zusammenspiel mit einer mehrschichtigen Verteidigung. Als Übergang zum Internet wurde eine Passierstelle definiert, die durch verschiedene Schutzzonen gesichert ist. Dies setzt natürlich eine gründliche Ist-Analyse voraus. Die Sicherheit des gesamten Systems orientiert sich an der Unsicherheit des schwächsten Gliedes unserer Konstruktion. *Was nützen die geschlossenen Türen, wenn die Fenster geöffnet sind?* An diesem Punkt sind es die Nutzer, die eine wichtige Funktion bei der Netzwerksicherheit innehaben.

Durch realistisches Einschätzen der Fehlersicherheit und -toleranz gelang es uns, innerhalb kürzester Zeit Backup-Systeme bereitzustellen, um die sensiblen Netzwerkbereiche physisch vom Universitätsnetz zu trennen, so daß sie weiterhin lokal einsatzfähig sind. Es gilt bei uns der Grundsatz: Alles ist verboten, was nicht ausdrücklich erlaubt ist. Wir partizipieren von den Vorteilen dieser Policy, akzeptieren aber auch die entstehenden Nachteile.

Dem Grundsatz, daß solche Systeme so einfach wie möglich gehalten werden müssen, steht die Komplexität der vom Anwender geforderten Transparenz, Ausfallsicherheit und Performance gegenüber.

Firewall-Architekturen

Nachfolgend sollen einige gängige Firewall-Architekturen vorgestellt werden.

Architektur mit Dualhomed-Host

Eine Architektur mit Dualhomed-Host wird um einen Host herum aufgebaut, der über mindestens zwei Netzwerkschnittstellen verfügt. Ein solcher Host ist als Router zwischen den Netzen einsetzbar, die an die Schnittstellen angeschlossen sind. Er kann dann IP-Pakete von Netz zu Netz routen. Für diese Firewall-Architektur muß diese Routingfunktion jedoch deaktiviert werden. IP-Pakete werden somit nicht direkt von dem einen Netz (dem Internet) in das andere Netz (das interne, geschützte Netz) geroutet. Systeme innerhalb der Firewall und Systeme außerhalb (im Internet) kön-

nen jeweils mit dem Dualhomed-Host, aber nicht direkt miteinander kommunizieren. Der IP-Verkehr zwischen ihnen wird vollständig blockiert. Die Netzarchitektur für eine Firewall mit Dualhomed-Host ist denkbar einfach: der Dualhomed-Host sitzt in der Mitte, wobei er mit dem Internet und dem internen Netz verbunden ist.

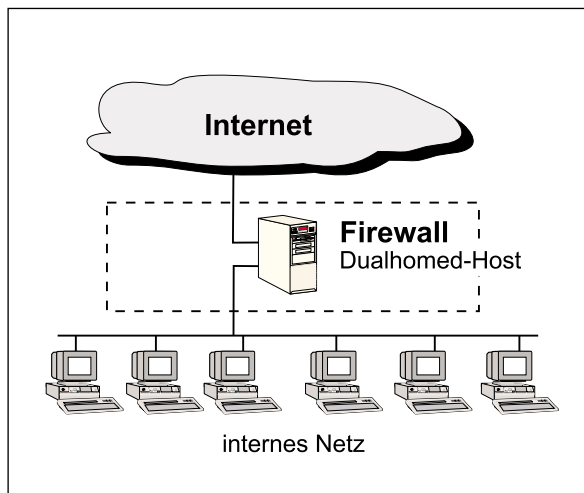


Abb.1: Dualhomed-Host

Es kostet beträchtlichen Aufwand, die Vorteile von Dualhomed-Hosts konsequent zu nutzen. Ein Dualhomed-Host kann Dienste nur anbieten, indem er Proxies (Stellvertreter) einsetzt oder direkte Nutzerzugriffe gestattet. Nutzerzugriffe auf einem Dualhomed-Host stellen aber Sicherheitsprobleme dar.

Architektur mit überwachtem Host

Die Architektur mit überwachtem Host (screened host architecture) bietet Dienste von einem Rechner an, der nur an das interne Netz direkt angeschlossen ist, wobei ein getrennter Router verwendet wird. Der Bastion-Host befindet sich im inneren Netz. Auf diesem Router verhindern Paketfilter das Umgehen des Bastion-Host durch die Nutzer. Die Paketfilterung auf dem Sicherheitsrouter muß so konfiguriert werden, daß der

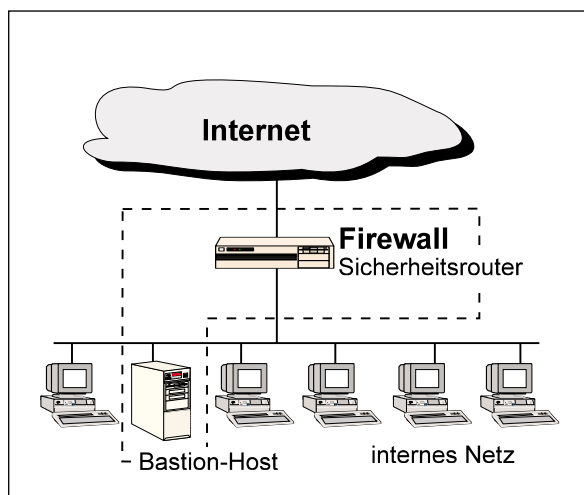


Abb.2: Screened Host

Bastion-Host das einzige System im internen Netz darstellt, zu dem Rechner aus dem Internet Verbindungen aufbauen können, und selbst dann sind nur gewisse Dienste zugelassen. Alle externen Systeme, die auf interne Systeme zugreifen wollen, und auch alle internen Systeme, die externe Dienste wahrnehmen wollen, müssen sich mit diesem Rechner verbinden.

Daraus ergibt sich ein besonderes Schutzbedürfnis für diesen Bastion-Host.

Der Vorteil bei dieser Konstruktion ist die Tatsache, daß ein Router leichter zu verteidigen ist. Dies liegt u.a. daran, daß auf ihm keine Dienste angeboten werden. Nachteilig wirkt sich aus, daß bei einer eventuellen Erstürmung des Bastion-Host das interne Netz vollkommen schutzlos ist.

Architektur mit überwachtem Teilnetz

Die Architektur mit überwachtem Teilnetz (screened subnet architecture) erweitert die Architektur mit überwachtem Host um eine Art Pufferzone, die als Grenznetz das interne Netz vom Internet isoliert. Diese Isolierzone wird auch Demilitarisierte Zone (DMZ) genannt.

Bastion-Hosts sind von ihrer Art her die gefährdetsten Rechner in einer Firewallkonstruktion. Auch wenn

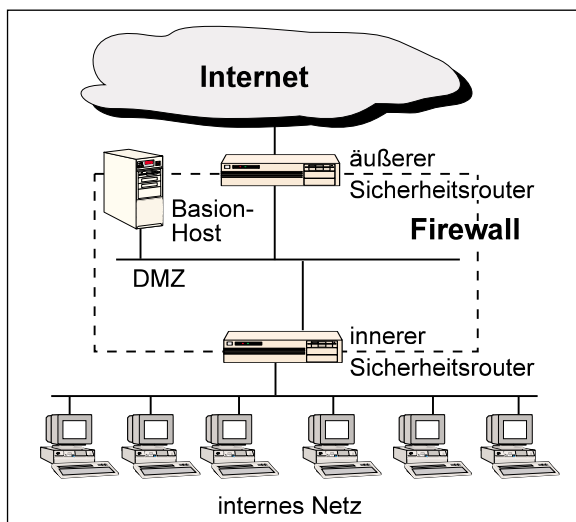


Abb.3: Screened Subnet

sie in der Regel mit allen Mitteln geschützt sind, werden sie doch am häufigsten angegriffen. Die Ursache liegt darin, daß ein Bastion-Host als einziges System Kontakt zur Außenwelt unterhält.

Verschlüsselung

Bei nichtanonymen Diensten (auch Dienste mit Authentifizierung genannt) muß der Benutzer, der auf den Dienst zugreifen will, erst seine Identität nachweisen. Daran entscheidet der Server, ob der Anwender den gewünschten Dienst benutzen darf. Mit strenger Authentifizierung könnten folgende Dienste gestattet

werden, die sonst einen Verstoß gegen unsere Security-Policy darstellen würden:

- Mit Telnet können sich Benutzer aus dem Internet einloggen, z.B. beim Besuch einer Konferenz oder auf Dienstreisen.
- Forscher und Kollegen fremder Standorte können sich auf dem System einloggen.
- Es kann ein gemeinsamer Datenbestand genutzt und gepflegt werden.

Authentifizierung bedeutet im wesentlichen beweisbare Identifizierung. Doch wie beweisen Benutzer einem System gegenüber, daß sie wirklich diejenigen sind, als die sie sich ausgeben? Wichtig ist hierbei der Unterschied zwischen Authentifizieren (Herausfinden, wer jemand ist) und Autorisieren (Herausfinden, was jemand darf). Authentifizierung ist eine Voraussetzung für Autorisierung. Es handelt sich dabei jedoch um zwei unterschiedliche Konzepte.

Kryptographie

Wieso ist Kryptographie sinnvoll? Nicht nur der Mitarbeiter einer Universitätsverwaltung, auch jeder andere Teilnehmer an Datennetzen hat den Anspruch und das Recht, daß seine Daten ihre Integrität behalten und nicht verfälscht werden. Genauso unangenehm ist es natürlich, wenn eine E-Mail unter einem gefälschten Absender verschickt wird.

Zum Verständnis muß hier geklärt werden, welches die wichtigsten Unterschiede zwischen kryptographischen Verfahren mit privaten und solchen mit öffentlichen Schlüsseln sind.

Private-Key-Verschlüsselungsverfahren

Zu den Algorithmen mit privaten Schlüsseln (private key algorithms) gehören der Data Encryption Standard (DES), der in Kerberos benutzt wird, IDEA, und der Skipjack-Algorithmus, der die Grundlage des Clipper-Chips bildet. Bei dieser Gruppe von Algorithmen kennen beide Partner einen einzelnen Schlüssel (den privaten Schlüssel), den sie geheimhalten müssen. Der Absender einer Nachricht chiffriert diese mit dem geheimen Schlüssel. Der Empfänger muß sie mit dem gleichen Schlüssel dechiffrieren. Um mit jemandem chiffrierte Nachrichten auszutauschen, muß der Partner den benutzten kryptographischen Schlüssel kennen. Dritte dürfen diesen Schlüssel nicht entdecken oder abhören. Es ist schwierig und umständlich, den Schlüssel auf geheime Art auszutauschen.

Public-Key-Verschlüsselungsverfahren

Zu den Algorithmen mit öffentlichem Schlüssel (public key algorithms) gehört u.a. RSA. Bei diesen Algorithmen erzeugt ein mathematischer Prozeß für beide Parteien je einen Schlüssel, zwischen denen ein mathematischer Zusammenhang besteht. Eine Nachricht, die mit

einem Schlüssel (dem öffentlichen Schlüssel) chiffriert wurde, kann nur mit dem anderen Schlüssel (dem geheimen oder privaten Schlüssel) dechiffriert werden. Der öffentliche Schlüssel kann bekanntgegeben werden, der private Schlüssel muß dagegen geheim bleiben. Zur Übermittlung einer geheimen Nachricht chiffriert der Absender diese mit dem öffentlichen Schlüssel des gewünschten Empfängers. Dieser dechiffriert die Nachricht mit seinem eigenen geheimen Schlüssel. Der einzige Schlüssel, mit dem die Nachricht dechiffriert werden kann, ist der geheime Schlüssel, der zu dem bei der Chiffrierung benutzten öffentlichen Schlüssel gehört. Mit diesem Public-Key-Verfahren kann man Nachrichten auch „unterschreiben“. Wenn der Absender eine Nachricht mit seinem privaten Schlüssel unterschreibt, kann der Empfänger die Unterschrift überprüfen, indem er den öffentlichen Schlüssel des Absenders auf die Nachricht anwendet. Dechiffriert dieser öffentliche Schlüssel die Nachricht erfolgreich, muß sie mit dem zugehörigen privaten Schlüssel unterschrieben worden sein.

Public-Key-Verfahren sind langsam, oft mehrere tausendmal langsamer als entsprechend sichere Private-Key-Verfahren. Aus diesem Grund werden Public- und Private-Key-Verfahren häufig in Kombination verwendet, wie z.B. das Verschlüsselungspaket Pretty Good Privacy (PGP). Um eine chiffrierte Nachricht an einen Empfänger zu senden, erzeugt das sendende PGP-Programm einen zufälligen „Sitzungsschlüssel“. Die Nachricht wird mit diesem Sitzungsschlüssel und einem Private-Key-Verfahren chiffriert, was schnell geht. Der Sitzungsschlüssel selbst wird mit einem Public-Key-Verfahren und dem öffentlichen Schlüssel des Empfängers chiffriert. Das ist zwar langsam, aber der Sitzungsschlüssel ist nur sehr kurz, vor allem im Vergleich zur eigentlichen Nachricht. Der chiffrierte Sitzungsschlüssel wird zusammen mit der chiffrierten Nachricht zum Empfänger übertragen. Dieser dechiffriert mittels Public-Key-Verfahren und seinem eigenen privaten Schlüssel zuerst den Sitzungsschlüssel. Mit dem Sitzungsschlüssel und dem Private-Key-Verfahren dechiffriert er dann die gesamte Nachricht, was wiederum schneller geht. Ein interessanter Aspekt dieses Schlüsselmanagements ist die Tatsache, daß man öffentliche Schlüssel von einer anderen Person oder Instanz beglaubigen (digital unterschreiben) lassen kann. Beispielsweise könnte man dann nur einem öffentlichen Schlüssel trauen, der von einer offiziellen Instanz oder Person digital unterschrieben worden ist.

PGP ist für den Mailverkehr derzeit das wichtigste Verschlüsselungs-Programm. Lösungen gibt es für eine große Anzahl gängiger Betriebssysteme. Die Komplexität der ganzen Thematik darf natürlich nicht unterschätzt werden. Deshalb steht für uns auch hier wieder im Vordergrund, die Transparenz für den Anwender so hoch wie möglich zu halten. Innerhalb des oben

erwähnten DFN-Projektes werden wir eine Lösung schaffen, die es den Nutzern gestattet, mit Partnern aus dem Internet verschlüsselte und digital signierte Informationen auszutauschen. Dabei wird unser lokales Messaging-System integriert werden müssen. Das ganze Schlüsselmanagement und eventuelle automatische Signaturen werden von einem Crypt-Mailserver durchgeführt werden.

Verschlüsselung ist ein Thema, das nicht nur auf Elektronik Mail beschränkt ist. Bei vielen Formen des elektronischen Kommunizierens in öffentlichen Netzwerken ist eine Verschlüsselung ratsam und zwingend erforderlich. Beispielsweise werden bei Telnet-, FTP- und WWW-Verbindungen Informationen und Paßwörter im Klartext über das Netzwerk transportiert und wären für jeden, der Zugang zu diesem Netzwerkabchnitt hat, lesbar! Ein Lösung für dieses Problem bietet ein durchdachtes Verschlüsselungsregime. In unserem Rechenzentrum sind zum Beispiel WWW-Server im Einsatz, die mit der geeigneten Client-Software verschlüsselt kommunizieren. Ebenso werden alle administrativen oder sensiblen Zugriffe, die öffentliche Netze durchqueren, nur noch in verschlüsselter Form gestattet. Für diese verschlüsselten Verbindungen setzen wir das Softwarepaket SSH (secure shell) und das SSL-Protokoll (secure socket layer) ein. Wenn diese Techniken auch für das gesamte Netz der Zentralen Universitätsverwaltung eingesetzt werden, könnten auch Zu-

griffe auf Datenbanken mit sensiblen Daten über einen WWW-Browser durchgeführt werden. Solche Browser sind heute an fast jedem Arbeitsplatz installiert.

Zusammenfassend kann man sagen, daß wir durch unsere Sicherheitsmaßnahmen, die eine Kombination aus Hard- und Software sind, folgende Dinge erreichen wollen:

- Schaffung eines einzelnen, alleinigen Übergangs in das öffentliche Universitätsnetz,
- Schutz des internen Netzes gegen unbefugten Zugriff von außen,
- Schutz des Firewall-Systems gegen Angriffe aus dem externen Netz, aber auch gegen Manipulationen aus dem internen Netz,
- Schutz der lokal übertragenen und gespeicherten Daten gegen Angriffe auf deren Vertraulichkeit und Integrität,
- Schutz der lokalen Netzkomponenten gegen Angriffe auf deren Verfügbarkeit,
- Schutz vor Angriffen, die auf Protokollmängeln und Fälschungen von Herkunftsadressen beruhen,
- Schutz vor Angriffen durch das Bekanntwerden von neuen sicherheitsrelevanten Softwareschwachstellen,
- suffiziente Beweissicherung bei Verstößen gegen unsere Security-Policy.

Alexander Geschonneck, RZ

E-Mail: geschonneck@rz.hu-berlin.de

WWW:<http://hppool0.rz.hu-berlin.de/~h0271cbj/>