Vorbeugende Maßnahmen zur Verbesserung der Rechnersicherheit

Stefan Rapp

Universität Dortmund
Hochschulrechenzentrum
Abteilung S3

15. Februar 2000

1 Hackerangriffe auf die Universität

Hacker sind für die Universität Dortmund nicht neu. Es hat immer wieder Einbruchsversuche und auch „erfolgreiche“ Einbrüche in Uni-Rechner gegeben. Scans auf Subnetze der Universität sind inzwischen fast an der Tagesordnung, i.d.R. beschränken sie sich aber darauf die Erreichbarbeit von Rechnern zu testen. Tests auf bekannte Schwachstellen von Dienste-Implementationen gibt es seltener und Einbrüche unter Erlangung von Root-Rechten waren bisher Einzelfälle.

1.1 Historie

Anfang September 1999 wurde eine neue Runde eingeläutet, die energische Maßnahmen gegen Hacker-Attacken erforderlich macht. Ziel waren diverse UNIX-Rechner aus verschiedenen Fachbereichen und Einrichtungen, wobei die Hacker bei 40 von 150 Einbruchsversuchen Root-Rechte erlangen konnten. Ende November gab es noch einen zweiten ähnlich durchgeführten Hackerangriff. Diesmal wurden trotz der Warnungen nach den ersten Einbrüchen immerhin noch 10 von 300 Rechnern „erfolgreich“ gehackt. Es wurden jeweils diverse Systemprogramme ausgetauscht oder gelöscht und Ethernet-Scanner installiert, die Dienste wie FTP, TELNET und RLOGIN auf dem Netzwerk verfolgten und Benutzerkennungen und Paßwörter im Klartext lieferten.

Betroffen waren in beiden Fällen Sun-Rechner mit dem Betriebssystem Solaris. Die Hacker haben sich allgemein bekannter Fehler im Tooltalk-Daemon (rpc.ttdbserverd) und Kalendermanager Daemon (rpc.cmsd) bedient, deren Korrektur schon länger Bestandteil der (frei verfügbaren) „Recommended Patch Cluster“ der Firma Sun ist. Wären die Systeme regelmäßig gewartet worden, hätten die Hacker mit diesen Angriffen nichts ausrichten können[1].

Das DFN-CERT wurde jeweils informiert und die betroffenen Rechner neu installiert. Wir haben keine weiteren Informationen über die Identität der Hacker, wissen allerdings inzwischen, daß die Universität Dortmund kein Einzelfall war. Auch Sun-Rechner anderer Einrichtungen im DFN waren betroffen.

[1] Die gleichen Fehler gibt es auch in anderen UNIX-Derivaten, die ungenügende Korrekturstände aufweisen. Die Hacker bräuchten nur leicht modifizierte Werkzeuge um sie auszunutzen.

1.2 Konsequenzen

Solche Vorkommnisse wie Anfang September und Ende November dürfen sich nicht wiederholen. Es wurden nach unseren Erkenntnissen zwar keine wissenschaftlichen Daten ausgekundschaftet oder Benutzerdaten zerstört, aber allein der Arbeitsaufwand für die Neuinstallationen und die weiter existierende Unsicherheit sind nicht zu vernachlässigen.

Man kann leider nicht davon ausgehen, daß alle Rechner an der Universität gleich hohe Sicherheitsstandards erfüllen, daher muß man an zentraler Stelle zusätzliche Vorkehrungen zur Gefahrenabwehr vorsehen.

2 Alternativen

Hier sollen nun verschiedene Möglichkeiten vorgestellt werden, die Rechner an der Universität vor der Außenwelt zu schützen und den Hackern die Arbeit auf jeden Fall zu erschweren[2]. In Frage kommen lokale Aktionen auf potentiell gefährdeten Rechner und zentrale Maßnahmen am Außenzugang der Universität in Form von Filterfunktionen.

2.1 Lokale Maßnahmen

Im Idealfall sollten „unsichere“ Maschine gar nicht ans Netz, in der Realität ist es allerdings schwierig festzustellen, ob ein Rechner sicher ist. Zu einer sicheren Maschine gehört ein Betriebssystem mit einem aktuellen Korrekturstand und eine „vernünftige“ Konfiguration. Beides ist nur lokal auf der Maschine überprüfbar, bei der Vielzahl von Rechnern und Betriebssystemen aber nur mit großem Aufwand. Im Idealfall wird eine Maschine mit Hilfe eines Skripts (Vorbild: TIGER) überprüft und nur wenn sie die Prüfung besteht, darf sie ans Netz. Dieser Test wäre natürlich regelmäßig zu wiederholen, da immer wieder neue Sicherheitslücken entdeckt werden oder der Rechner durch lokale Administrationsmaßnahmen unsicher wird.

Eine, wenn auch nicht so umfassende, Alternative wäre die Überprüfung der Systeme von außen mit Hilfe von Tools wie z.B. SATAN, SAINT oder NESSUS. Hier wird über das Netzwerk nach Schwachstellen im Diensteangebot der Rechner gesucht und bei möglichen Problemen gewarnt. Korrekturstände sind so nicht zu überprüfen, aber grobe Konfigurationsmängel oder allgemein bekannte Sicherheitsprobleme werden sichtbar. Dieser Test kann von einer zentralen Stelle gesteuert und überwacht werden. Durch die regelmäßige Anwendung solcher Werkzeuge kann man zwar nicht Hackerangriffe gegen dedizierte Maschinen verhindern, aber den „Erfolg“ externer Scans über Subnetze der Universität oder generelle Scans des Universitätsnetzes minimieren.

2.2 Zentrale Filterung

Bei einer zentralen Filterung des Datenverkehrs am Außenzugang der Universität hat man grundsätzlich zwei Alternativen. Man kann entweder alle nicht ausdrücklich erlaubten Dienste blockieren oder den Datenverkehr bis auf einige gesperrte Dienste erlauben[3]. Die erste Variante hat den Vorteil der größeren Sicherheit, führt aber dazu, daß gewisse Dienste nicht mehr oder nur

[2] Nicht außer acht lassen sollte man vielleicht die Frage, ob wir die Außenwelt auch vor Angriffen aus der Universität schützen wollen. Ebenfalls zu untersuchen wären Maßnahmen gegen inneruniversitäre Hackversuche.

[3] Derzeit ist SMTP (Mail-Protokoll) nur für dedizierte Rechner möglich und der Sun RPC-Verzeichnisdienst ganz gesperrt.

eingeschränkt unterstützt werden können. Mit der zweiten Variante kommt man zwar in die Gefahr, den Hackern immer einen Schritt hinterher zu sein, man macht ihnen die Arbeit auf jeden Fall schwerer und produziert weniger Einschränkungen für den Forschungsbetrieb.

In den aktuellen Versionen des Betriebssystems für die CISCO-Router (IOS) sind verschiedene Sicherheitsfunktionen eingebaut, die über geeignete Konfigurationen aktiviert werden können. Hier sollen die drei wichtigsten Funktionen zur mehr oder weniger „intelligenten“ Filterung des Datenverkehrs kurz vorgestellt werden.

2.2.1 Portfilter

Die Portfilter erlauben Einschränkungen des Netzverkehrs auf der Basis von Rechner- und/oder Port-Tabellen. Abgehender und ankommender Verkehr kann dabei getrennt reglementiert werden. In dieser reinen Form kann man eigentlich nur den Zugriff auf gewisse Dienste sperren, wie z.B. potentiell unsichere Dienste wie RPC, FINGER, ... Die Umkehrung mit der selektiven Freischaltung bekannter Dienste würde dazu führen, daß noch nicht einmal einfachste Programme wie WWW und SSH funktionieren (hier sind zumindest auf einer Seite dynamisch generierte Ports beteiligt).

2.2.2 Reflexive Access-Listen

Bei restriktiv gehandhabten Portfiltern müssen unbekannte Ports für den Verkehr gesperrt werden. Um aber dennoch abgehende Verbindungen zu externen oder ankommende Verbindungen zu eigenen Servern (z.B. WWW, SSH) aufbauen zu können, muß der Rückweg zum dynamisch generierten Port für die Dauer der Verbindung geöffnet werden. Dies ist die Aufgabe der reflexiven Access-Listen. Hiermit können alle Dienste auf festen Ports, zu denen ein Klient aktiv eine Verbindung aufbaut abgehandelt werden. Wenn allerdings im Verlauf einer solchen Sitzung dynamisch weitere Kanäle mit nicht definierten Ports eröffnet werden (z.B. FTP) hat man ein Problem.

2.2.3 CBAC

Hierbei handelt es sich um eine Erweiterung der reflexiven Accesslisten. Bei CBAC werden spezielle höhere Protokolle (z.B. FTP) ausgewertet, um die Öffnung der Portfilter für dynamisch generierte Ports zu steuern. Durch die Protokollauswertung ist hier aber ein relativ hoher Rechenaufwand notwendig, den unsere CISCO-Gateways nicht verkraften würden. Auch gerät man hier leicht in eine Abhängigkeit von der Firma CISCO bei Anforderungen zur Unterstützung neuer Protokolle.

2.3 Firewall

Bei weitergehenden Sicherheitsanforderungen für sensitive Bereiche reichen einfache Portfilter nicht mehr aus. Hier möchte man im Idealfall alle direkten Verbindungen zwischen internen und externen Rechnern unterbinden. Möglich wird dies über Proxies (der Firewall als Relaisstation zwischen Innen- und Außenwelt) für spezielle Dienste. Das führt zwangsläufig auch zu Änderungen in den Anwendungen oder der Bedienung von Anwendungen und kommt für die zentrale Anbindung der Universität an das Wissenschaftsnetz nicht in Betracht. Sinn machen Firewalls höchstens in einzelnen besonders kritischen Bereichen als Ergänzung allgemeinerer zentraler Maßnahmen. Dabei darf aber nicht vernachlässigt werden, daß der sichere Betrieb eines

Firewalls einen nicht geringen Aufwand für Installation und insbesondere Wartung erfordert!

3 Empfehlung

Wenn man die derzeitig verfügbare Hardware und das zur Verfügung stehende Personal in die Überlegungen mit einzieht, fallen einige der vorgestellten Möglichkeiten direkt aus. Auch darf man die vielfältigen Anforderungen einer Forschungs- und Lehreeinrichtung wie der Universität an die Qualität und Vielfalt der Außenanbindung nicht vernachlässigen.

Übrig bleibt zentral eine Kombination der Nutzung von CISCO-Filterfunktionen auf der Basis von Portfiltern und von regelmäßigen Sicherheitsüberprüfungen im Universitätsnetz. Darüberhinaus muß die Aufklärung von Benutzern und Systemverwaltern in der Universität verstärkt werden. Gerade der letzte Hackerangriff hat wieder gezeigt, wie unsicher die traditionellen TCP-Anwendungen (FTP, TELNET, RLOGIN, POP) mit ihrer unverschlüsselten Datenübertragung sind. Es ist kein Problem unter UNIX mit Systemverwalterrechten den Netzverkehr mitzuschneiden und damit an Benutzer- und Paßwortinformationen zu kommen. Hier kann man nur die sichere Alternative SSH empfehlen, bei der nicht nur der Verbindungsaufbau, sondern auch der komplette Datenverkehr verschlüsselt wird. Erst damit kann man sicher über das Netzwerk arbeiten oder administrieren. Systemadministratoren muß außerdem die regelmäßige Pflege und Wartung ihrer Systeme ans Herz gelegt werden. Das Rechenzentrum kann hier unterstützend tätig werden, indem es die notwendigen Korrekturen innerhalb der Universität an zentraler Stelle zur Verfügung stellt[4].

Weitere Informationen zu Sicherheitsaspekten in der Rechnerwelt und entsprechenden Werkzeugen finden sich auf den HRZ-Seiten unter http://www.hrz.uni-dortmund.de/s3/sicherheit/ und beim DFN-CERT in Hamburg unter http://www.cert.dfn.de/.

[4] Derzeit schon für Sun Solaris Patch-Cluster realisiert.

4 Empfohlene Protokollfilter

Die hier aufgeführten Protokolle sind zum größten Teil für die Nutzung in Intranets gedacht und sollten deshalb an den Außenzugängen zum Internet in beiden Richtungen blockiert werden. Normale Anwender sind in ihrer Arbeit von diesen Einschränkungen nur unwesentlich betroffen, Hackern wird ihre „Arbeit“ dagegen wesentlich erschwert. Die Liste ist sicher nicht vollständig und muß regelmäßig neuen Erkenntnissen angepaßt werden.

In der Liste sind Internet-Dienste mit ihrem symbolischen Namen, der IP-Portnummer und dem verwendeten Protokoll aufgelistet.

SYSTAT/11/TCP Dieser Dienst liefert bei manchen Unix-Systemen eine Liste aller lokalen Prozesse an beliebige Benutzer im Netzwerk.

NETSTAT/15/TCP Analog zu SYSTAT, nur daß hier eine Liste aller Netzwerkdienste und Verbindungen abzufragen ist.

SMTP/25/TCP SMTP (Simple Mail Transfer Protokoll) ist schon derzeit nur für einige dedizierte Mail-Server freigeschaltet. Alle anderen Rechner müssen indirekt über diese Server kommunizieren. Dies dient zum einen dem Schutz vor Hackern, zum anderen der Verhinderung von Mißbrauch durch SPAM.

TFTP/69/UDP Dieser Dateitransfer dient zum Booten und Konfigurieren verschiedener Netz-Komponenten. Heruntergeladene Dateien könnten Hackern nützliche Informationen liefern.

FINGER/79/TCP Der Dienst liefert auf vielen Systemen interessante Informationen über lokale Benutzer, die Hackern helfen könnten.

SUNRPC/111/UDP,TCP Der Verzeichnisdienst aller RPC-Dienste ist seit dem zweiten Hackerangriff generell blockiert, auf diese Weise wird der Zugang zu RPC-Anwendungen erheblich erschwert. Viele dieser Programme sind fehlerbehaftet und wurden wiederholt für Einbrüche mißbraucht.

SNMP/161,162/UDP Über SNMP (Simple Network Management Protocol) erhält man Informationen von Netzwerkkomponenten und Rechnern, die teilweise auch übers Netz administrierbar sind. Auf vielen Systemen laufen die entsprechenden Dämonen standardmäßig mit.

PRINTER/515/TCP Das Druckprotokoll für verteiltes Drucken im UNIX-Bereich. Viele Netzwerk-Drucker und Druckserver nehmen über dieses Protokoll Druckaufträge beliebiger Rechner an.

BACKORIFICE/31337/* Hier handelt es sich um eine verbreitete Hintertür in Windows-Systeme.

Darüberhinaus stellt sich die Frage, inwieweit UDP- oder ICMP-Protokolle generell blockiert werden können. Die meisten darauf aufsetzenden Dienste sind zwar nicht grundsätzlich gefährlich, können aber für DOS (Denial of Service) Angriffe genutzt werden oder die Protokolle werden von Hacker-Tools zum Datentransfer mißbraucht. Hier sind noch weitere Überlegungen notwendig, da teilweise auch solche Anwendungen wie MBONE oder Streaming Audio/Video auf UDP aufsetzen.