



KAPITEL 13

Sicherheit eines Netzwerks

Die Installation von Firewalls ist nur ein Teil der Maßnahmen, die dazu beitragen, Computer vor Missbrauch zu schützen. Weitere Maßnahmen sind auf den Computern hinter der Firewall zu ergreifen, um diese Computer gegen die verschiedenen Angriffe zu wappnen. Bei direkt an das Internet angeschlossenen Computern sind diese Maßnahmen unabdingbar. Isolierte *Linux*-Computer benötigen nur dann Sicherheitsmaßnahmen, wenn sie allgemein zugänglich sind.

Schutz vor Einbrüchen

Ein Computer im Netz stellt für manche Internet-Nutzer eine attraktive Beute dar. Anstelle des Wegnehmens wie bei einem klassischen Diebstahl wird der Computer entgegen seinem Bestimmungszweck verwendet.

Charakterisierung eines Einbruchs

Ein Einbruch kann durch das

- In-Besitz-nehmen einer Shell (Hacken),
- das In-Besitz-Nehmen eines Anwendungsprogramms oder
- das Einschleusen von Code (Exploit)

erfolgen. Kennzeichnend für einen Einbruch ist, dass der Angreifer Befehle oder Code auf der Zielmaschine zur Ausführung bringt. Sportlich gesinnte Hacker hinterlassen eine Datei oder eine Grafik mit dem Hinweis auf einen vorgenommenen Einbruch und vielleicht sogar die Aufforderung, die Lücke zu schließen.

Andere, weniger freundliche Hacker verwenden eroberte Computer etwa, um Ansichten zu verbreiten, die den Interessen des Computereigentümers entgegenstehen. Der eroberte Computer wird auch zum Durchführen strafbewehrter Handlungen, wie illegales Verbreiten von Bildern und Filmen, Angriffe auf Dritte oder Versenden von Massen-E-Mails verwendet. Oft nutzen böswillige Hacker auch den einmal gewonnenen Zugriff auf das

System dazu, eine spezielle Zugangssoftware (Backdoor) oder ein modifiziertes Programm zu hinterlassen, was dann dem Hacker einen einfacheren, schlechter zu entdeckenden Zugang möglich macht.

Entdeckung eines Einbruchs

Im besten Fall wird ein Einbruch genau dann, wenn er begangen wird entdeckt. Das erfordert immer eine Nachuntersuchung, die Änderungen am *Linux*-Computer erfasst. Während eines Einbruchs kann über die Prozesstabelle ermittelt werden, ob mehr und andere Programme laufen, als der Eigentümer des *Linux*-Computers gewöhnlich laufen lässt.

```
ps ax
```

zeigt die Prozesstabelle. Hinweise auf Einbrüche können auch erhöhter Rechenzeitverbrauch sein, der mit

```
top
```

angezeigt werden kann. Besonders kritisch sind Prozesse, die vom Systemverwalter *root* ausgeführt werden. Die Prozesse können auf alle Daten und Programme zugreifen. Im Fall eines entdeckten akuten Einbruchs sollte als erste Maßnahme sofort die Netzverbindung getrennt werden, sofern dies möglich ist. Auf das Trennen kann nur dann verzichtet werden, wenn die Entlarvung des Einbrechers wichtiger ist als der von ihm angerichtete Schaden oder wenn der *Linux*-Computer nicht direkt über eine Tastatur zugänglich ist. Danach können die verdächtigen Prozesse vermittels

```
kill -15 999
```

– hier für den Prozess mit der Nummer 999 – zwangsweise beendet werden. Es sollte das TERM-Signal 15 und nicht das KILL-Signal 9 verwendet werden, damit etwaige Veränderungen von Dateien bei der Programmbeendigung unterbunden werden. Bei *Linux*-Computern, die nur über das Netz erreichbar sind, ist darauf zu achten, dass nicht die eigene Shell und die eigene Verbindung (meist *ssh*) beendet wird. Die Analyse von Rechenzeitverbrauch und üblicherweise laufenden Programmen und Diensten muss – auch ohne Verdacht – regelmäßig vorgenommen werden, um einen Eindruck vom Verhalten des *Linux*-Computers im Normalfall zu erhalten.

Nach einem tatsächlichen oder vermuteten Einbruch werden die Spuren ausgewertet. Dies sind

- die Systemprotokolle, die auch Systemanmeldungen des Benutzers *root* auflisten,
- Dateien, die nicht von den regulären Benutzern angelegt worden sind; sie sind vornehmlich in den Systemverzeichnissen zu finden,
- veränderte Dateien und Programme, die oft dem Einbrecher ein erleichtertes Wiedereindringen erlauben sollen.

In den Systemprotokollen werden Zeit und Datum der Systemanmeldungen von *root* festgehalten. Ein Vergleich mit den eigenen Aktivitäten gibt Hinweise darauf, dass ein Einbrecher sich die Anmeldung von *root* zunutze gemacht hat.

Die Paketmanager *RPM*, *DPKG* und andere führen Datenbanken für jede regulär installierte Datei beziehungsweise jedes Programm. Sie erlauben es, die vorhandenen Dateien gegen diese Datenbank abzuprüfen.

Wenn eine Datei oder ein Programm keiner regulären Softwareinstallation zugewiesen wurde, ist der Verdacht nahe liegend, dass dieses Objekt auf einen Einbruch zurückgeht. Ausnahmen sind Protokolldateien in */var/log* und einige Konfigurationsdateien in */etc*. Im Verzeichnis */tmp* und */var/tmp* liegen Dateien und Verzeichnisse, die jedermann anlegen darf. Sie bilden daher oft die erste Stufe für einen komplexen Einbruch. Die Dateien in */tmp* und */var/tmp* sollten daher regelmäßig von einem *cron*-Job gelöscht werden. Die meisten Distributionen haben solch einen Job standardmäßig vorgesehen.

Eine Veränderung von Daten und Programmen kann mithilfe von Prüfsummen entdeckt werden. Die Paketmanager führen eine Prüfsummendatenbank, die für alle Dateien in der Datenbank mit hoher Wahrscheinlichkeit eine Veränderung entdeckt. Die Überprüfung der Dateien und Programme im Verzeichnis */etc* erfolgt mit

```
rpm -Vf /etc/*
```

für den RPM.

Linux-Computer mit hohen Sicherheitsanforderungen sollten nicht auf Prüfsummen-Datenbanken zurückgreifen, die auf denselben Festplatten wie die Nutzdaten abgespeichert sind. Die zu verwendenden Prüfsummen werden auf einem externen, mit Schreibschutz ausgerüsteten Wechselspeicher wie Floppy, USB-Speicher oder CD-WORM (Compact-Disk Write Once Read Many, gebrannte CD) abgespeichert. Die RPM-Datenbank findet man unter */var/lib/rpm*. Die Dateien in diesem Verzeichnis liegen im *Berkeley-DB*-Format¹ vor. Das Programm *rpm* lässt sich mit der Option *-r /media/dvd* anweisen, nicht das gewöhnlich genutzte Verzeichnis zu verwenden, sondern */media/dvd* für die Datenbanken.

Schutz vor Einbrüchen

Der erste Schritt zum Schutz vor Einbrüchen ist die Einrichtung einer geeigneten Firewall-Lösung. Das Grundprinzip bei der Auslegung der Firewall ist, alles nicht unbedingt Notwendige zu sperren oder zu untersagen.

Der nächste Schritt zum Schutz vor Einbrüchen ist der konsequente Verzicht auf alle nicht unbedingt benötigten Programme und Dienste – alles, was nicht läuft oder nicht installiert ist, kann nicht missbraucht werden.

¹ <http://www.sleepycat.com/>

Die installierten Programme und Dienste werden daraufhin überprüft, ob sie tatsächlich benötigt werden. Für häufig verwendete Dienste wie Webserver oder FTP-Server gibt es verschiedene Versionen mit unterschiedlichen Leistungsmerkmalen. Der Version mit dem geringsten, aber ausreichenden Umfang an Leistungsmerkmalen ist der Vorzug zu geben. Gemeinhin ist die Fähigkeit, viele Anfragen zu bedienen – insbesondere bei Webservern – bei Servern mit wenigen Leistungsmerkmalen größer als bei Servern mit vielen Leistungsmerkmalen.

Passwörter zur Verwaltung des *Linux*-Computers sind ein häufiges Ziel eines Einbrechers. Sie müssen dem Einbrecher nicht unbedingt bekannt sein – es gibt spezielle Programme, um sie zu erraten. Passwörter, die Namen, Begriffe und gängige Bezeichnungen enthalten sind besonders gefährdet, da sie durch Angriffe per Katalog leicht zu erraten sind. Passwörter sollten daher nach Möglichkeit keiner Sprache entnommen werden. Passwörter sollen zudem Sonderzeichen und Zahlen enthalten und so lang wie möglich sein. Die ausgewertete Länge eines Passworts umfasst mindestens 8 Zeichen und hängt von den bei der Installation vorgenommenen Einstellungen des Verschlüsselungsalgorithmus ab. Passwörter sollten regelmäßig gewechselt werden, bei höheren Sicherheitsanforderungen in kürzeren Zeiträumen. Programme zum Erraten oder Brechen von Passwörtern werden von sicherheitsbewussten Systemadministratoren regelmäßig dazu verwendet, verwendete Passwörter auf ihre Sicherheit hin zu prüfen und bei Bedarf nachlässige Benutzer aufzufordern, Abhilfe zu schaffen.

Sowohl Programme als auch der Kernel sind nicht vor Programmierfehlern gefeit. Programmierfehler, ihre Auswirkungen und die Fehlerbehebungsstrategien werden von spezialisierten Arbeitsgruppen² untersucht und veröffentlicht. Die Organisationen bieten auch Mailing-Listen an, die von Betreibern kritisch exponierter *Linux*-Computer abonniert werden sollten. Nach einer Veröffentlichung müssen unverzüglich die beschriebenen Maßnahmen (Abschalten eines Programms, Austausch von installierter Software, Installation eines fehlerbereinigten Kernels) vorgenommen werden.

Schutz vor Ausspähung

Kenntnisse über die Beschaffenheit von Computersystemen erlauben es Angreifern, Einbrüche, Datendiebstähle und Missbräuche von Computern vorzunehmen. Je genauer die Kenntnis ist, desto mehr können die Angriffe zielgerichtet sein. Die Auslegung eines *Linux*-Computers erfolgt so, dass ein Außenstehender keine kritischen Informationen gewinnen kann.

Charakterisierung von Ausspähungen

Bei einem *Linux*-System sind Passwörter, Konfiguration von Serverdiensten, Netzwerk- anbindung und installierte Software und deren Versionen empfindliche Informationen.

² <http://www.cert.org> <http://www.bsi.bund.de>

Alle Passwörter können durch systematisches Probieren erraten werden. Je ungewöhnlicher – das heißt unnatürlicher – ein Passwort ist, desto mehr Aufwand muss zum Erraten getrieben werden. Passwörter, die weder einer Sprache entstammen noch bekannte Ziffernkombinationen enthalten, sondern alle Zeichen des Zeichensatzes in Gleichverteilung verwenden, sind einigermaßen sicher. Serverdienste wie Webserver oder FTP-Server verwenden eigene Passwort-Verwaltungsmechanismen, die einen geringeren Schutz als das *Linux*-System selbst haben können. Manche Implementierungen speichern gar die Passwörter im Klartext ab. Mit den so erlangten Passwörtern können weitere Informationen gewonnen oder es kann direkt eine Schaden verursachende Aktion gestartet werden. Passwörter von schwach geschützten Systemen dürfen nicht für andere Systeme verwendet werden.

Viele Distributoren bieten für ihre Serverdienste vorkonfigurierte Installationen, die Standardmeldungen bereithalten. Die Standardmeldungen enthalten viele verwertbare Informationen, die durch reguläre Zugriffe gewonnen werden können. Darauf aufbauend können weitere Kenntnisse der Beschaffenheit des *Linux*-Computers gewonnen werden. Insbesondere ist bei vielen Webservern das Fehlen von Indexseiten eine Möglichkeit, auf die Daten des Webserver unkontrolliert zuzugreifen. Durch geeignete Anfragen an einen nicht gehärteten, extern sichtbaren Webserver lassen sich beispielsweise Informationen über vorhandene interne Webserver gewinnen.

Durch spezielle über das Netzwerk übermittelte Pakete, wie Source-Route-Pakete, können Informationen über Vorhandensein, Art und Einstellungen von Computern hinter einer Firewall gewonnen werden. Damit können andere Angriffe zielgerichtet begonnen werden.

Linux-Computer und ihre Serverdienste geben die Versionsnummern ihrer Software bekannt, sofern sie nicht anders angewiesen werden. Die Kenntnis der Version einer auf einem *Linux*-Computer installierten Software kann dazu genutzt werden, bekannte Fehler dieser Software dazu auszunutzen, Kenntnisse über den Computer zu erlangen, Daten zu stehlen, Schad-Software einzuschleusen und vieles mehr.

Zuletzt ist auch die Verfügbarkeit der Systemdokumentation zu beachten. Detaillierte Systemdokumentation darf nur vertrauenswürdigen Personen zugänglich sein.

Entdeckung von Ausspähungen

Direkte Angriffe auf Passwörter können im einfachsten Fall dadurch bemerkt werden, dass bei einer erfolgreichen Anmeldung des rechtmäßigen Benutzers die Anzahl der gescheiterten Anmeldungen nach der letzten erfolgreichen Anmeldung angezeigt wird. Da dieser Zähler nach jeder erfolgreichen Anmeldung gelöscht wird, kann ein Angreifer mit einer erfolgreichen Anmeldung seine Aktivitäten verschleiern. Zuverlässiger sind die Meldungen des syslog-Dämon, die standardmäßig in den Systemprotokollen im Verzeichnis */var/log* abgelegt werden. Diese müssen bei exponierten *Linux*-Computern gegen Manipulation geschützt werden. Dies kann durch gleichzeitiges Mitprotokollieren

der Dateien auf einen anderen Rechner erfolgen oder durch das unverzügliche Ausdrucken auf Papier.

Die Art und Weise der vom `syslog`-Dämon zu protokollierenden Daten kann in seiner Konfigurationsdatei, oft `/etc/syslogd.conf` konfiguriert werden. So kann ein Ausdruck auf Papier auf die Aktivitäten des Benutzers `root` beschränkt werden.

Einige Serverdienste schreiben eigene Protokolldateien. Sie sollten nach den Standards *FHS*³ und *LSB*⁴ im Verzeichnis `/var/log` liegen, einige Dienste wie die Netzwerk-Uhr-Synchronisierung `ntpd` schreiben aber nach wie vor in ihr Arbeitsverzeichnis wie `/etc`. Eine dauernde Überwachung der Protokolldateien liefert Hinweise auf illegale Zugriffe. Neben bisher nicht üblichen Zugriffsarten sind neue, mit großer Anzahl auftretende Ursprungsadressen verdächtig.

Andere Hinweise sind ungewöhnliche Belastungen und Rechenzeitverbrauch des *Linux*-Computers. Wenn etwa systematisch ein Passwort-Erraten versucht wird, ist hoher Netzwerkverkehr zu beobachten, der in keinem Zusammenhang mit den legalen Aktivitäten des *Linux*-Computers steht.

Eine sorgfältige Beobachtung der Foren für Computer-Sicherheit⁵ bietet Sicherheit, rechtzeitig vor Programmierfehlern von *Linux*-Kernel, Serverdiensten und Programmen gewarnt zu werden, um diese dann gegen fehlerbereinigte Versionen auszutauschen.

Das Entdecken von Ausspähungsversuchen verlangt hohe Aufmerksamkeit und einigen Aufwand. Ausspähungsversuchen sind deswegen besonders heimtückisch, weil ihre weiteren Auswirkungen nicht unmittelbar gesehen werden können. Die Ausspähung selber kann oft nur unmittelbar beobachtet werden, da die Abgrenzung zu legaler Nutzung im Nachhinein schwierig ist.

Schutz vor Ausspähung

Der Zugang auf vorhandene, schriftliche, für die Installation spezifische Dokumentation sollte auf diejenigen Benutzer beschränkt werden, die vertrauenswürdig sind. Insbesondere sind Passwort-Listen mit großer Vorsicht zu verwenden.

Passwörter werden je nachdem, wie der *Linux*-Computer Angriffen aus dem Internet und von Benutzern ausgesetzt ist, regelmäßig gewechselt. Ein *Linux*-Computer mit Netzzugang durch einen einzigen Benutzer mag mit einem Wechsel alle 4 Wochen gut versorgt sein, eine direkt im Internet befindliche *Linux*-Firewall mit `ssh`-Zugang für die Fernwartung, die einen bekannten Webserver versorgt, sollte täglich ein neues Passwort bekommen. Passwörter sollen aus mindestens 8 Zeichen bestehen – mehr ist dann sinnvoll, wenn die installierte Software auch dies unterstützt – und aus allen Zeichen des Zeichensatzes bestehen,

³ <http://www.pathname.com/fhs>

⁴ <http://www.lsb.org/>

⁵ <http://www.cert.org>

Serverdienste werden so konfiguriert, dass alle Standardseiten oder Meldungen ersetzt werden. Alle nicht notwendigen Funktionen werden abgeschaltet. Es sind Protokolle anzulegen, die alle passwortbezogenen Aktivitäten protokollieren sollten. Insbesondere ist bei Web-Servern darauf zu achten, dass jedes Verzeichnis eine Indexdatei – meist *index.html* oder *index.htm* – enthält, die Verzeichnisaufstellungen verhindert. Bei einigen Webserver-Varianten lässt sich auch auf Serverebene ein Verzeichnisaufstellen verhindern.

Eine vollständige Firewall-Proxy-Kombination verhindert Ausspähen über Source-Route-Pakete und andere Mechanismen. Es darf kein Netzwerkverkehr ohne Filterung durch die Firewalls und Umsetzung durch die Proxys von innen nach außen und von außen nach innen stattfinden.

Überflutungsangriffe (Denial-of-Service-Angriffe)

Während sich die bisher beschriebenen Angriffsformen ausschließlich gegen einen bestimmten Computer oder eine Gruppe richteten, sind *Denial-of-Service*-Angriffe (Angriffe durch Überflutung) sowohl gegen einzelne Computer, Computergruppen als auch gegen die Internetanbindung selbst wirksam. Denial-of-Service-Angriffe werden auch gewöhnlich nicht von einem einzelnen Computer aus vorgenommen, sondern setzen voraus, dass der Angreifer mehrere verschiedene Computer an ganz verschiedenen Orten in Besitz gebracht hat.

Was ist ein Angriff durch Überflutung

Ein Denial-of-Service-Angriff verwendet Netzwerk-Pakete, die an sich zulässig sind. Es werden aber viel mehr Pakete abgesetzt, als zur Bedienung einer regulären Anforderung notwendig sind. Die eigentlich erwartete oder erforderliche Antwort wird gar nicht abgewartet, sondern es werden weitere Anfragen oder Anforderungen abgesetzt. Damit kann der Zielrechner gestört, das Betriebssystem oder die Software auf dem Ziel des Angriffs zum Absturz gebracht, die Erreichbarkeit einer Internetseite beeinträchtigt, E-Mail-Verkehr blockiert und alle sonstigen Netzwerkdienste beeinträchtigt werden. Es kann aber auch – ohne einen Computer, Router oder eine Firewall im lokalen Netz direkt zu beeinträchtigen – die gesamte Bandbreite einer Internetanbindung in Anspruch genommen werden.

Entdeckung eines Überflutungsangriffs

Anzeichen eines Denial-of-Service-Angriffs, der die gesamte Bandbreite einer Internet-Anbindung in Anspruch nimmt, ist das Fehlen von Antworten auf Anfragen und Anforderungen aus dem Internet. Web-Seiten werden nicht mehr dargestellt, Herauf- und Herunterladen per FTP scheitert und E-Mails werden nicht empfangen und können nicht versandt werden.

Wenn ein an das Internet angebundener *Linux*-Computer abstürzt oder ein Dienst oder ein Programm unplanmäßig beendet werden, kann dies die Folge eines Denial-of-Service-Angriffs sein. Dieses Verhalten wiederholt sich nach einem Neustart des *Linux*-Computers, dem Neustart des Dienstes oder des Programms. Wenn die Beeinträchtigung des *Linux*-Computers durch das Abschalten der Netzanbindung per

```
init 2
```

unterbleibt, ist die Ursache gefunden.

Linux-Computer zeigen eine Statistik der eingegangenen und versandten Pakete

```
ifconfig eth0
```

für reguläre Ethernetschnittstelle oder

```
ifconfig ppp0
```

für Internetverbindungen mit Modem zeigen viel mehr eingehende Pakete als sonst üblich.

Bei Internetanbindungen mit fester Adresse ist der Internet-Provider um Hilfe um Hilfe zur Untersuchung des Angriffs zu bitten. Oft kann der Anwender gegen einen solchen Angriff von vielen verschiedenen Computern aus selber nichts unternehmen und ist auf Hilfe angewiesen.

Schutz vor einem Überflutungsangriff

Bei Internetanbindungen, die mit dynamischer Adressvergabe arbeiten, kann schon eine neu aufgebaute Verbindung mit neuer Adresse den Angriff ins Leere laufen lassen.

Wenn ein *Linux*-Computer an das Internet angebunden ist, muss er durch Firewallfunktionen geschützt werden. Die Software oder der Kernel ist immer dann zu erneuern, wenn Fehler bekannt werden. Auf nicht benötigte Software ist zu verzichten, die benötigte Software ist so zu konfigurieren, dass alle nicht benötigten Leistungsmerkmale (Features) abgeschaltet werden.

Ein *Linux*-Computer, der sich hinter einer Leitung oder hinter einem Router oder Firewall befindet, ist gegen Denial-of-Service-Angriffe auf eine andere Art empfindlich als ein *Linux*-Computer, der an eine breitbandige Backbone-Leitung eines Providers angeschlossen ist. Der *Linux*-Computer an der Breitbandanbindung ist immer selbst das Ziel, während der *Linux*-Computer hinter der bandbreitenbegrenzenden Anbindung auch durch Verstopfen der Leitung an der Wahrnehmung seiner Aufgaben gehindert werden kann.

Untersuchung des Netzwerkverkehrs

Linux bietet Werkzeuge, um den Verkehr auf roher Paketebene zu beobachten. Damit können sowohl alle ordentlichen als auch alle böswilligen Datenübertragungen erfasst werden. Der Zugriff auf diese Werkzeuge muss auf den Systembetreuer beschränkt werden, um Missbrauch vorzubeugen.

Werkzeuge zur Netzwerkverkehrsanalyse

Das klassische Werkzeug aus der *Linux*-Welt ist `tcpdump`. Diese Programm erlaubt es für Netzwerkgeräte, alle über sie versandten und empfangenen Pakete darzustellen. Es wird neben dem Inhalt auch Quelle, Ziel, Protokoll und diverse Zähler aufgezeigt. Der Aufruf für die erste Ethernetschnittstelle eines Linux-Computers lautet

```
tcpdump -i eth0
```

Es muss unbedingt vor dem Auftreten von Fehlern, am besten sofort nach der ersten Inbetriebnahme des gesamten Systems, eine Netzwerkverkehrsanalyse mit `tcpdump` vorgenommen werden, um ein Bild vom nicht beeinträchtigten Netzwerkverkehr zu gewinnen. Zu `tcpdump` gibt es weitere Analysewerkzeuge, die den rohen Paketverkehr analysieren und differenziertere Aussagen ermöglichen. Daneben gibt es weitere Programme wie `ipgrab` und `netacct`, die eine automatisierte Überwachung ermöglichen.

Schlüsse aus den Ergebnissen von Netzwerkverkehrsanalysen

Alle Pakete sind verdächtig, deren Ursprungsorte nicht vertraut sind. Alle Protokolle, die üblicherweise nicht gebraucht werden, sind Anzeichen für einen Fehler oder einen Angriff. Wenn Verdächtiges auftaucht, werden die Protokolle der Firewall analysiert. Hier finden sich oft schon Hinweise auf früher aufgetretene Angriffsversuche. Wenn es irgendwie möglich ist, den Verursacher herauszufinden, kann neben gezieltem Vorgehen gegen ihn eine spezielle Sperre in der Firewall für ihn eingerichtet werden. Sollte der Angreifer einen Konfigurationsfehler oder einen Programmierfehler entdeckt haben, wird dieser behoben. Gelegentlich deckt eine Verkehrsanalyse auch Hardware- und Softwarefehler im eigenen lokalen Netz auf. Solche können wie hausgemachte Denial-of-Service-Angriffe aussehen.

