Der Tag danach ...

Die Vorstellung, daß ein System hundertprozentig sicher sei, ist oft ein Trugschluß. Hier soll kurz darauf eingegangen werden, was zu tun ist, wenn ein Einbruch auf einem UNIX-System festgestellt wurde. Auch wenn Ihr UNIX-System nicht kompromittiert wurde, helfen vielleicht diese Hinweise, Ihr System richtig abzusichern. Die Erfahrung zeigt, daß es kein Patentrezept für die Reihenfolge der Maßnahmen gibt. Sie richtet sich in der Regel nach der Schwere des Angriffs, den eigenen Fähigkeiten und den zur Verfügung stehenden Ressourcen.

Es erscheint immer ratsam, vom kompromittierten System ein Komplettbackup anzulegen. Dies kann helfen, falls man bei der Suche Spuren und Daten zerstört.

1. Versuchen Sie, die Spur des Eindringlings zu seinem Ausgangspunkt zurückzuverfolgen. Dazu sollten Informationen aus folgenden Quellen zu Rate gezogen werden:

- `who`
- `w`
- `last`
- `lastcomm`
- `netstat`
- `snmpnetstat`
- Informationen des Routers
- `/var/adm/messages` etc. - Eindringlinge versuchen häufig, Mails an „ihre“ Accounts zu schicken
- `syslog` - schickt Syslogmeldungen an einen eventuell vorhandenen Loghost
- Logfiles von `tcp_wrapper`, `cgi_wrapper`, `suid_wrapper` und ähnlicher Software
- `finger` auf alle lokalen Nutzer; Informationen, wer sich wann von wo aus als Letzter angemeldet hat, können von großem Nutzen sein
- History-Dateien von Shells, `.history` etc.
- Mailboxen kompromittierter Accounts.

Die Untersuchung personenbezogener Daten (auch Verbindungsdaten) sollte in Abstimmung mit dem behördlichen Datenschutzbeauftragten oder der Rechtsabteilung erfolgen.

Informationen der Befehle `who`, `w`, `last` und `lastcomm` basieren in der Regel auf `/var/adm/pacct`, `/usr/adm/wtmp`, `/etc/utmp` etc. Die meisten Hintertürprogramme von Eindringlingen verhindern aber das Speichern von Informationen in diesen Dateien. Wenn ein Eindringling noch nicht dazu gekommen ist, diese Hintertürprogramme zu installieren oder die Dateien einfach zu löschen, kann man dort eventuell Informationen finden. Dies trifft besonders zu, wenn Sie keine Standardnamen oder Verzeichnisse für diese Dateien definiert haben.

Hilfreich ist die Installation von `xinetd` oder `tcp_wrapper`. Mit diesen Tools kann man u. a. alle Verbindungsversuche frühzeitig protokollieren, noch bevor der angesprochene Daemon via `inetd` gestartet wird. Sinnvoll ist auch ein Weiterleiten von `Syslog`-Informationen zu einem zentralen, speziell abgesicherten Loghost mit semi-automatischer Intruder Detection. Es gibt eine Vielzahl von Intruder Detection Systemen, die im Netzverkehr nach speziellen Hackersignaturen suchen und entsprechende Maßnahmen einleiten. Auch eine simple Protokollierung der Verbindungsanforderungen im lokalen Netzwerk hilft oft, Einstiegslöcher zu orten.

2. Schließen Sie alle externen Netzzugänge zu diesem System. Dies kann durch Beenden der lokalen Netzwerkdienste oder durch eine physische Trennung vom Netzwerk geschehen. Ein sich entdeckt geglaubter Eindringling könnte sonst versuchen, seine Spuren zu verwischen, beispielsweise mit `rm -rf /`. So kann sich ein „nur Neugieriger“ schnell in einen Vandalen verwandeln.

3. Vergleichen Sie die auf dem System vorhandenen Programme mit den Originaldateien des Herstellers oder der Originaldistribution. Achten Sie besonders auf folgende Programme, da sie häufig durch trojanische Pferde ersetzt werden, die dem Eindringling eine vom Administrator unbemerkte Hintertür öffnen:

- `/bin/login`
- `/usr/etc/in.*` (z. B. `in.telnetd`)
- `/lib/libc.so*`
- alle Programme, die von `inetd` gestartet werden (in `/etc/inetd.conf` definiert).

Häufig werden auch folgende Programme ersetzt:

- `netstat` - Netzverbindungen können „versteckt“ werden
- `ps` - laufende Prozesse können „versteckt“ werden (z. B. ein Paßwort-Crackprogramm)
- `ls` - Verzeichnisse oder Dateien können „versteckt“ werden
- `ifconfig` - verschleiert, daß sich ein Netzwerkdevice im Promiscuous Mode befindet und so den gesamten Netzwerkverkehr ablauscht
- `sum` - Prüfsummen der Originalprogramme werden verfälscht wiedergegeben; meistens werden aber die Programme so verändert, daß sie die Originalprüfsummen aufweisen(!).

Mit `ls -lac` kann man den Zeitpunkt der Veränderung von Dateien überprüfen. Überprüfen Sie alle Ihnen zur Verfügung stehenden Protokolldateien auf Hinweise, daß die Systemzeit verändert wurde. Vergleichen Sie Dateigröße und MD5-Prüfsummen mit

den Daten auf den Original-Installationsmedien oder den MD5-Prüfsummen, die Sie nach der Installation erstellt haben. Sie haben doch MD5-Prüfsummen erstellt, oder?

Eine andere populäre Hintertür ist das Hinzufügen des `suid`-Bits zu einem normalen Programm (z. B. `/bin/time`), um dieses von einem normalen Account mit Administratorrechten auszuführen. Sie können alle vorhanden suid-Programme mit `find / -type f -perm -4000 -exec ls -la` ausfindig machen.

Das unbedingt zu empfehlende Programm `tripwire` überwacht die Veränderung von Systemdateien und -verzeichnissen. Bei Unsicherheiten, ob noch Hintertürprogramme vorhanden sind, sollte das gesamte System neu installiert werden.

4. Installieren Sie Mechanismen, die sicherstellen, daß die Nutzer ihr Paßwort regelmäßig erneuern. Mit `anlpasswd`, `npasswd` oder `passwd+` können Sie Programme einsetzen, die als Ersatz für `/bin/passwd` oder `/bin/yppasswd` die Nutzer dazu zwingen, sichere Paßwörter zu wählen. Dieses geschieht zum einen durch einen einfachen Rulecheck und zum anderen durch Wörterbuchabfragen. Setzen Sie selbst Paßwort-Rateprogramme wie Crack ein und überprüfen Sie, ob die Nutzer sichere Paßwörter gewählt haben, bevor es der Eindringling für Sie tut. Sinnvoll ist auch der Einsatz von Einmalpaßwortsystemen, wie z. B. S/Key oder OPIE.

5.Überprüfen Sie die Dateien `.rhosts` und `.forward` in jedem Nutzerverzeichnis (besonders auch Administrator- und Systemaccounts) nach verdächtigen Einträgen. Enthält z. B. die Datei `/.rhosts` den Eintrag `+ +`, bedeutet das, daß sich jeder Nutzer von jedem anderen System im Netzwerk als Administrator ohne Paßwortabfrage anmelden kann. Das Programm `COPS` beinhaltet u. a. ein Script, mit dem solche verdächtigen Einträge aufgespürt werden.

Mit `find / -name .rhosts -exec ls -o -name .forward` kann man dies auch selbst tun (evtl. per Cronjob).

Suchen Sie nach allen Dateien, die in der Zeit erstellt oder verändert wurden, die als Angriffszeit vermutet wird, mit `find / -ctime -2 -ctime +1 -exec ls.`

Alle Dateien `.login`, `.logout`, `.profile`, `.cshrc`, `.bashrc`, `.bash_profile` in den Nutzerverzeichnissen sollten nach verdächtigen Einträgen und der Uhrzeit überprüft werden. Stellen Sie sicher, daß die Verzeichnisse von gesperrten oder System Accounts (sync, news, sundiag) keine `.rhosts`-Datei enthalten. Diese Accounts sollten als Login-Shell `/bin/false` haben. Suchen Sie in allen Verzeichnissen nach Dateien, die mit „`.`“ oder „`..`“ beginnen. Diese werden häufig in `/tmp`, `/var/tmp`, `/usr/spool/*` oder in anderen für Nutzer schreibbaren Systemverzeichnissen gefunden. Es kommt auch vor, daß Dateien versteckt werden, die Zeichen wie `^T` etc. im Dateinamen enthalten oder mit „`...`“ oder „`.. `“ (Punkt, Punkt, Leerzeichen) beginnen. Dies soll eine Inspektion erschweren.

6. Prüfen Sie, daß Ihre mit NFS exportierten Verzeichnisse nicht für jeden schreibbar sind. Mit `showmount -e` können Sie überprüfen, welche Filesysteme Sie mit welchen Rechten exportieren. Einige ältere NFS-Server ignorieren Access-Listen, wenn sie eine bestimmte Größe überschreiten. Kontrollieren Sie, was Sie wie importieren! Wenn möglich sollte das `nosuid`-Flag gesetzt sein.

7. Stellen Sie unbedingt sicher, daß Sie die aktuellste `Sendmail`-Version installiert haben oder installieren Sie einen `Sendmail_wrapper`.

8. Versuchen Sie, alle Security-Patches zu installieren, die der Hersteller Ihres Systems veröffentlicht hat. Beziehen Sie diese Patches nur von einer vertrauenswürdigen Stelle und überprüfen Sie gegebenenfalls die digitalen Signaturen.

9. Informieren Sie alle befreundeten Sites und Systeme, daß Ihr System kompromittiert wurde. Vertrauen ist häufig symmetrisch. Wenn Sie einem System via `.rhosts` oder `/etc/hosts.equiv` trauen, wird es Ihnen wahrscheinlich auch trauen. Ein Eindringling kann sich so von System zu System „durchhangeln“, weltweit. Es ist dringend ratsam, eine geeignete zentrale Koordinierungsstelle für Netzwerksicherheit zu informieren (z. B. DFN-CERT).

10. Installieren Sie einen Packet-Filter oder ein Firewall-System am Übergang zu Ihrem Internet Service Provider.

- Mit `rpcinfo -p` können Sie auf Ihrem System überprüfen, ob RPC-Dienste laufen, die eigentlich nicht laufen sollten, z. B. `rexd`.
- Prüfen Sie `/etc/hosts.equiv` auf den Eintrag `+`.
- Prüfen Sie, ob `tftp` auf Ihrem System deaktiviert ist. Wenn es unbedingt laufen muß, dann stellen Sie sicher, daß es nicht mit Superuserprivilegien läuft und es mit der Option '`-s`' auf einen sicheren Bereich zeigend gestartet wird. Setzen Sie den `tcp_wrapper` ein und beschränken Sie den Zugriff.
- `cron`- und `at`-Jobs sollten auf „Zeitbomben" überprüft werden.
- Überprüfen Sie die Scripte, die beim Systemstart abgearbeitet werden (`/etc/rc.boot`, `/etc/rc.local` oder bei SYSV `/etc/rc*.d/*`). Prüfen Sie alle anderen Dateien in `/etc/`, die Systemkonfigurationen enthalten (`sendmail.cf`, `hosts.allow`, `at.allow`, `at.deny`, `cron.allow`, `hosts`, `hosts.lpd`, etc.). Die Datei `/etc/aliases` sollte keine Definition verdächtiger Accounts beinhalten (`uudecode` ist nur ein Beispiel).
- Die Datei `/etc/inetd.conf` sollte keinen Dienst enthalten, der eventuell vom Eindringling hinzugefügt wurde.
- Kopieren Sie alle Logdateien an einen sicheren Ort, damit Sie sie später kontrollieren können. Sie könnten unangenehm überrascht werden, wenn der Eindringling nur vergessen hat, sie zu löschen und es später nachholt. Suchen Sie nach anderen temporären Dateien, die eventuell während des Angriffes erstellt worden sind und Hinweise auf das Vorgehen des Eindringlings geben. (Werfen Sie dazu einen Blick auf `/tmp`, bevor Sie rebooten.)
- Legen Sie eine Sicherungskopie von `/etc/passwd` an und verwahren Sie sie auf einem anderen sicheren System. Ändern Sie die Paßwörter der privilegierten Nutzer, wenn Sie sicher gestellt haben, daß `/bin/passwd` und `/bin/su` nicht kompromittiert wurden. Alle Nutzer müssen ihr Paßwort umgehend ändern, denn es könnte sein, daß der Eindringling bereits Paßwörter erraten hat. Sperren Sie gegebenfalls alle Accounts.
- Prüfen Sie, ob die vorhandenen Dienste ordnungsgemäß konfiguriert sind (Anon-FTP, WWW etc.).
- Installieren Sie Wrapper- und Audit-Software.
- Definieren Sie nur `/dev/console` als sicheres Terminal, so daß sich der Superuser nicht über das Netz anmelden darf.
- Überprüfen Sie `/etc/hosts.equiv`, `/etc/hosts` und `.rhosts` auf Einträge wie `#` u. ä. Der Eindringling kann durch Fälschung von DNS-Informationen als Host `#` auftreten. Er würde dann als vertrauenswürdig eingestuft und hätte Zugang zu Ihrem System. Diese Dateien werden gern vom Hersteller mit `# comment` ausgeliefert.
- Es gibt sehr viele Mittel und Wege, in ein System einzudringen.

Halten Sie die Augen immer offen!

Abb.: Eine kurze unvollständige Checkliste, um den Sicherheitsstatus zu überprüfen

Alexander Geschonneck
geschonneck@rz.hu-berlin.de
http://www.hu-berlin.de/~h0271cbj/