Paketfilter und Firewalls

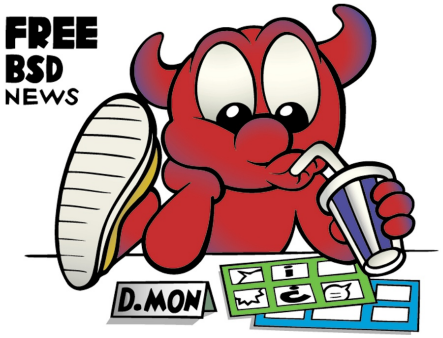
Neben dem von OpenBSD übernommenen Paketfilter »pf« gibt es unter FreeBSD noch »ipfw« (welches auch unter MacOSX eingesetzt wird) und »IPFilter« als Firewall.

Im Zusammenspiel mit pfsync und CARP eröffnet pf absolut einmalige Fähigkeiten ein Netzwerk zu schützen. Mit vergleichsweise wenig Aufwand können Netzwerke vollkommen redundant und verbindungsorientiert an das Internet angeschlossen werden. Will man redundante Firewalls aufsetzen, so müssen diese Informationen allen Knoten im Verbund zur Verfügung stehen, da sonst die Verbindung beim Ausfall einer Komponente nicht aufrecht erhalten werden könnte. Für diese Aufgabe wurde das pfsync-Protokoll entwickelt, das zum Austausch der Verbindungsstatusinformationen dient. Mit CARP ist es einfach ausgedrückt möglich, eine Reihe von Rechnern hinter der gleichen IP-Adresse zu verstecken. Fällt einer der Rechner aus, so übernimmt ein anderer weitere Anfragen. Zusätzlich ist es möglich die Last über alle vorhandenen Knoten zu verteilen und auch beim Ausfall eines oder mehrerer Teilnehmer die verbleibenden Knoten zu übernehmen. CARP hat volle Unterstützung für IPv6 und ist durch Verschlüsselung gegen eine Reihe von Angriffen gegen VRRP (Virtual Router Redundancy Protocol) geschützt.

Jails

Eine der ältesten Sicherheitsmassnahmen ist chroot, welches den Zugriff auf einen Teil des Dateisystems beschränkt. FreeBSD verfügt natürlich auch über chroot. Es ist für kleinere Aufgaben geeignet, stösst aber an Grenzen. FreeBSD hat daher Jails (Gefängnisse) implementiert. Das sind, vereinfacht gesagt, virtuelle Umgebungen (client) auf einem Dateisystem, welche aber vollkommen isoliert vom eigentlichen System sind. Während es in einer chroot-Umgebung für root möglich ist „auszubrechen“, ist dies in einer Jail nicht der Fall. Sie haben eigene IP-Adressen, eine eigene Konfiguration und können eigene Programme ausführen.

Eine Jail teilt sich die Ressourcen des Servers mit dem Hostsystem. Veränderungen am Host können die Jail beeinflussen, Veränderungen in einer Jail aber das Hostsystem nicht. Es handelt sich um eine spezielle Form des sog. "sandboxing". Jails können übrigens auch als Ordnungsinstrument und für Backups dienen, da sie leicht kopierbar sind. Für sehr ausführliche Informationen lesen Sie bitte: http://www.grunix.de/dokumentationen/jails/



Verschlüsselung

FreeBSD unterstützt unter anderem die komplette Verschlüsselung von Partitionen und Swap mittels geli(8) und gdbe(8) inklusive Auslagerung der Schlüssel auf USB-Sticks etc. Die Möglichkeiten sind sehr weitgehend und wir empfehlen Ihnen daher die Lektüre des Flyers Geom mit ausführlichen Informationen hierzu.

Security Event Auditing (TrustedBSD)

Als Erweiterung für spezielle Hochsicherheitsanforderungen steht ab FreeBSD 6.2 audit zur Verfügung, welches mit dem Solaris-kompatiblen Audit-Framework OpenBSM in TrustedBSD entwickelt wurde. Es wird darauf hingewiesen, dass das auditing nur nach umfangreichen Tests produktiv eingesetzt werden sollte, da dieses Feature neu hinzugefügt wurde. Weitere Information finden Sie hier: http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/audit.html

Weitere Informationen

http://www.FreeBSD.org/

http://www.FreeBSD.org/doc/de/books/handbook/

http://lists.FreeBSD.org/mailman/listinfo

http://www.BSDForen.de/

Wir können nicht auf 2 Seiten alle Sicherheitsmerkmale von FreeBSD auch nur annähernd detailliert aufzählen. Weitere Flyer werden folgen, z.B. zu Firewalls. Wenn Sie Kritik, Anregungen oder Verbesserungsvorschläge haben, so bitten wir Sie, sich mit Daniel.Seuffert@allBSD.de in Verbindung zu setzen. Herzlichen Dank!

FreeBSD: The Power To Serve

FreeBSD

Sicherheit ohne Kompromisse

Wie generell alle BSDs ist FreeBSD seit langer Zeit für seine kompromißlose Einstellung zur Sicherheit bekannt. Um Sicherheit zu gewährleisten, wurde eine über Jahre erprobte organisatorische Struktur aufgebaut, die laufend verbessert und erweitert wird. Dieser Flyer stellt Ihnen grundlegende Sicherheitsmechanismen in FreeBSD vor.

Das Security Team und dessen Struktur

Alle relevanten Abläufe und Strukturen sind tranparent und jederzeit öffentlich einsehbar, siehe http://www.FreeBSD.org/security/ . Hierbei trägt der FreeBSD Security Officer die Verantwortung. Ihm zur Seite stehen der Security Officer Emeritus, der Deputy Security Officer, ein Mitglied des Core Teams und eine ganze Reihe von weiteren Mitgliedern des Sicherheitsteams. Alle erkannten und verifizierten Sicherheitslücken werden in einer öffentlich einsehbaren Datenbank publiziert: http://www.vuxml.org/FreeBSD/

Selbstverständlich werden auch ältere Releases von FreeBSD hinsichtlich Sicherheit gepflegt:

Early adopter: Releases, welche von -CURRENT (der Entwicklungslinie) abstammen, werden mindestens 6 Monate nach Veröffentlichung unterstützt.

Normal: Releases aus -STABLE (der Produktivlinie) werden mindestens 12 Monate weitergepflegt, meistens länger.

Extended: Ausgewählte Releases werden mindestens 24 Monate mit Sicherheitsupdates versorgt, oft länger.

Wo finde ich Informationen als Nutzer?

FreeBSD ist exzellent dokumentiert, das Handbuch beschreibt natürlich auch alle Sicherheitsmechanismen, siehe http://www.FreeBSD.org/doc/de/books/handbook/security.html

Hier finden Sie Hinweise über die Installation, Nutzung und Update von OpenSSL, Kerberos, VPNs mit IPSEC, OpenSSH, Einmalpasswörter, PAM, TCP-Wrapper, Zugriffskontrolllisten für Dateisysteme (ACL, access control list), Prozess-Überwachung (Process accounting) usw. Sie sehen bereits an der kurzen Aufzählung, wie vielfältig Ihre Möglichkeiten sind, sich zu schützen.

Sicherheitshinweise - Security advisories

Sicherheitslücken können jederzeit auftreten. Um die Nutzer zu informieren, veröffentlicht das FreeBSD-Security-Team nach Bedarf sogenannte security advisories (SA), welche per Email und auf der FreeBSD-Projektseite veröffentlicht werden. Es gibt allerdings keine SA für Applikationen (Ports). In diesen SA werden die jeweiligen Probleme präzise geschildert und klare Hinweise für das Schliessen der Lücken nebst patches und Erläuterung der Anwendung derselben gegeben. Die Zahl der SA schwankt naturgemäß. Man kann aber von ca. 20-40 pro Jahr ausgehen. Allerdings ist nicht jeder von allen SA betroffen. Sie sollten sich jedes SA sorgsam durchlesen und sicher sein, dass es Sie überhaupt betrifft. Stellen Sie sicher, dass Sie auf der Announce- oder Security-Mailingliste eingeschrieben sind oder nutzen Sie den RSS-Feed.

Binäre Updates mit FreeBSD Update

Viele Nutzer und vor allem Administratoren von Serverfarmen wünschen sich binäre Updates, welche möglichst einfach anzuwenden sind und keine Neukompilierung erfordern. Das seit FreeBSD 6.2 in der Basisinstallation aufgenommene **Freebsd-Update** ermöglicht ein automatisches Einspielen von Betriebssystem-Sicherheitslücken-Updates, vergleichbar mit "Windows Update" von Microsoft. Diese Updates betreffen nicht nur den eigentlichen Kernel sondern auch andere Bestandteile der Basisinstallation. Updates gibt es für alle vom Security-Team unterstützen Versionen. Das Update kann per cronjob in beliebigen Intervallen automatisiert werden, alle Updates sind signiert und selbstverständlich kann man per rollback auch Updates rückgängig machen, falls erforderlich. Wir weisen darauf hin, dass Freebsd-Update momentan nur auf Systemen mit GENERIC-Kernel angewendet werden. Das System wird allerdings ständig verbessert.

Sicherheitsprofile, Securelevel, File System Security Flags

Ein Sicherheitsprofil (security profile) ist eine Sammlung von Einstellungen, das versucht ein vorgegebenes Verhältnis von Sicherheit und Bedienbarkeit einzustellen. Dazu werden bestimmte Programme und Optionen aktiviert oder deaktiviert. Je schärfer das Sicherheitsprofil ist, desto weniger Programme werden in der Voreinstellung aktiviert. Ein Prinzip von BSD: Lassen Sie nur die Programme laufen, die Sie auch wirklich benötigen.

Beachten Sie, dass ein Sicherheitsprofil nur eine Vorgabe ist. Nachdem Sie FreeBSD installiert haben, können Sie alle Programme in der Datei /etc/rc.conf aktivieren oder deaktivieren. Sehen Sie hierzu auch: http://www.FreeBSD.org/doc/de/books/handbook/install-post.html

Securelevel ist ein weiterer Sicherheitsmechanismus, er wird durch die Variable kern.securelevel, die mit sysctl gesetzt werden kann, angegeben. Nachdem Sie die Sicherheitsstufe auf 1 gesetzt haben, sind schreibende Zugriffe auf raw devices verboten und die speziellen chflags Optionen, wie schg werden erzwungen. schg ist das sog. "system immutable flag", schärfer als sappnd verbietet dieses flag jede Änderung der Datei. FreeBSD verwendet das routinemäßig auf einer ganzen Menge von Konfigurationsdateien, aber auch auf dem Kernel. Zu beachten gilt, dass diese Mechanismen auch Nachteile haben und nur von erfahrenen Nutzern genutzt werden sollten und das Securelevel nichts mit den z.B. in Linux bekannten runlevel zu tun haben.

Wie finde ich verwundbare Applikationen?

FreeBSD ist nicht in der Lage für jedes der über 16.000 Programme (Ports) SA zu erstellen und zu verteilen. Dennoch gibt es einen Weg, auch diese Programmpakete zu überwachen. Das in der Ports-Sammlung enthaltene Programm »Portaudit« wurde gezielt dafür entwickelt.

Der Port security/portaudit fragt dazu eine Datenbank, die vom FreeBSD Security Team sowie den Ports-Entwicklern aktualisiert und gewartet wird, auf bekannte Sicherheitsprobleme ab. Während der Installation werden die Konfigurationsdateien für periodic(8) aktualisiert, was es Portaudit erlaubt, seine Ausgabe in den täglichen Sicherheitsbericht einzufügen. Sie müssen nur sicherstellen, daß diese (an das E-Mail-Konto von root gesendeten) Sicherheitsberichte auch gelesen werden.

Nach Installation der Datenbank kann man über die Ports-Sammlung installierte Softwarepakete Dritter jederzeit überprüfen. Existiert in Ihren installierten Softwarepaketen eine Sicherheitslücke, wird Portaudit eine Ausgabe mit einer URL produzieren. Diese kann mit einem Internetbrowser aufgerufen werden, um zusätzliche Informationen abzurufen. Portaudit ist ein mächtiges Werkzeug und insbesondere in Zusammenarbeit mit »Portupgrade« und »Portsnap« äußerst hilfreich.

Zusätzliche Programme installieren

FreeBSD verfügt mit über 16.000 Ports eine reichhaltige Auswahl an zusätzlicher Software, welche Sie einsetzen können. In http://www.freshports.org/security/ finden Sie momentan über 600 Applikationen, vom Intrusion Detection System snort über GnuPG bis hin zu aide und honeyd. Die Auswahl ist riesig und für jeden Zweck werden Sie aller Wahrscheinlichkeit nach eine geeignete Lösung finden.

Codequalität: Audits, Coverity, Styleguides

FreeBSD ist für seine Codequalität berühmt und setzt alles daran, diese laufend zu verbessern. Es gibt ein öffentliches, auch über ein Webinterface einsehbares, CVS und viele Menschen überprüfen täglich jede Änderung der Codebasis. FreeBSD ist eine professionelle Organisation und jeder committer hat strenge Richtlinien einzuhalten, welche auch der Sicherheit dienen. Ein Beispiel: http://www.FreeBSD.org/doc/en_US.ISO8859-1/books/developers-handbook/secure.html

Um diesen Prozess zu unterstützen setzt FreeBSD das Coverity Prevent Analysis Tool ein, welches auf einem eigens dafür reservierten Server täglich jede Codeänderung überprüft. Es entdeckt Sicherheitslücken in C und C++ Code in über 30 verschiedenen Kategorien. Zusätzlich werden laufend Regressionstests durchgeführt. Eine eigene Infrastruktur für tägliche und automatisierte Regressionstests ist im Entstehen. Weiterhin gibt es eine dedizierte Testumgebung. Dort werden laufend Stress Tests durchgeführt werden (http://www.holm.cc/stress/), um die Stabilität des Codes zu verifizieren.

Jeder Nutzer von FreeBSD kann auf einfache Weise auch über ein Webinterface Bugs und Probleme melden sowie patches einsenden. Diese Informationen können natürlich auch öffentlich eingesehen werden: http://www.FreeBSD.org/cgi/query-pr-summary.cgi oder http://www.FreeBSD.org/prstats/index.html