



NetBSD

— Das Betriebssystem —



Was ist das NetBSD-Projekt?

Das NetBSD-Projekt stellt ein vollständiges Unix-ähnliches Betriebssystem bereit, das zu 100% den aktuellen Open-Source- und Security-Kriterien entspricht. Industriestandard APIs und Vernetzungsprotokolle, sowie eine große Anzahl an Hardware-Plattformen, werden unterstützt. NetBSD eignet sich dabei für alle Anwendungsgebiete: robuste Server-Systeme und Workstations ebenso wie Handheld-Rechner und Eingebettete Systeme.

NetBSD wird oft gewählt um neu entwickelte Hardware, u.a. in den Bereichen Netzwerk-Computer, Ein-Platinen-Rechner oder sogar WebCams, anzusteuern; darüber hinaus wird es im Bereich von Netzwerkentwicklung auf der ganzen Welt eingesetzt. Internet-Service-Provider benutzen NetBSD wegen seines breiten Spektrums an Netzwerk-Möglichkeiten, und begeisterte Liebhaber entscheiden sich für NetBSD aufgrund seiner breiten Hardware-Unterstützung.

Warum ist NetBSD so einzigartig?

Seit NetBSD 1993 als Nachfolger der BSD-Linie aus der Taufe gehoben wurde, war es immer an der Spitze bei der Entwicklung von Open-Source-Betriebssystemen anzutreffen. In vielen Fällen diente NetBSD als vollständige Grundlage oder Referenz für andere Projekte. Viele der Stärken sind in keinem anderen freien Betriebssystem zu finden.

NetBSD unterstützt zur Zeit 55 verschiedenen Hardware-Plattformen auf insgesamt 17 CPU-Architekturen von der DEC Alpha über Sparc64 hin zum ARM.

Crosskompilierung des Kernels und des Userlands wird von der Standard-Werkzeugen unterstützt.

Es gibt für Entwickler drei unterschiedliche Arten den Betriebssystemkern zu debuggen: local, remote und post-mortem.

Der vollständige Quellcode ist, inklusive Entwicklungsgeschichte, via anonymem CVS, CVSweb, SUP und rsync verfügbar.

Unterstützung der unterschiedlichsten Netzwerktechnologien wie ATM, HIPPI, FDDI, HSSI, IEEE 802.11, Token-Ring, ARCnet und Ethernet sind bereits im Basissystem vorhanden!

NetBSD war das erste Open Source Betriebssystem das USB, USB2 und PCMCIA Audio unterstützte.

Applikationen in Hülle und Fülle.

Mit Hilfe des Paketsystems *pkgsrc* können mittlerweile weit über 5500 frei erhältliche Software-Pakete (z. B. KDE, GNOME, XFCE, OpenOffice, Apache, PostgreSQL, Mozilla, Samba, L^AT_EX etc.) ohne Aufwand installiert werden. Die Software kann von CDs, DVDs, FTP-Servern oder Dank dem *pkgsrc*-Paketensystem mit einem einfachen `make install` installiert werden.

Ausgewählte Systeme werden in freien Veröffentlichungen detailliert beschrieben.

Verfügbar in allen Größen!

NetBSD läuft auf einer breiten Palette von Hardware-Plattformen, angefangen von der VAX 11/750 bis zu den modernsten PCs und Windows CE Palmtops. Egal ob Sie den alten Computer vom Dachboden entstauben oder die neueste Errungenschaft aus dem Laden mit nach Hause bringen, NetBSD wird für Sie da sein! Nach dem Entfernen einiger optionaler Komponenten passt NetBSD auch sehr gut in Eingebettete Systeme.

Sicherheit für Paranoide.

Mit integrierten Firewall-Werkzeugen, IPsec, Kerberos 5 und OpenSSL sowie Kryptographie wie OpenSSH und PGP, die einfach aus unserer Softwaresammlung installiert bzw. aktualisiert werden können, steht Ihnen ein Sicherheitssystem zur Verfügung, das dem Stand der Technik entspricht. Selbstverständlich wurde unser gesamtes System auf Sicherheitslücken untersucht!

In den öffentlichen Foren zum Thema „Sicherheit“ – wie etwa der Bugtraq-Mailing-Liste trat NetBSD in der Vergangenheit konstant mit den wenigsten bekannten Sicherheitsproblemen im Vergleich zu seinen Alternativen auf. Ein Grund, warum Sicherheitsberater NetBSD wählen!

Verlieren Sie nicht den Anschluss!

NetBSD wächst und gedeiht seit März 1993 – länger als jede andere Alternative im Open-Source-Bereich – und es ist stärker denn je. Wir werden nicht einfach von der Bildfläche verschwinden und Sie allein lassen, oder Ihre Plattform nicht weiter unterstützen. Sie können nachts beruhigt mit dem sicheren Gewissen schlafen, daß Ihr Betriebssystem von fähigen Experten weiterentwickelt wird.

Hilfe ist nur eine Mail entfernt!

Hilfe bei Problemen bieten wir schnell und unbürokratisch über Mailing Listen und unser Bug-Tracking-System. Für formelle Unterstützung stehen auch die auf unserer Webseite aufgelisteten professionellen Berater zu Ihrer Verfügung. Es existiert zwar keine Service-Telefonnummer, Ihre Fragen werden von uns aber selbstverständlich beantwortet – ohne daß Sie in einer Warteschleife hängen.

Dokumentationen

Auf <http://www.NetBSD.org> finden Sie ausführliche Dokumentationen zum gesamten System und zu *pkgsrc*.

www.NetBSD.org



NetBSD

— Sicherheit frei Haus —



NetBSD - Sicherheit frei Haus

Das NetBSD Projekt verfolgt den selben Ansatz zur Sicherheit wie auch zum restlichen System: *Lösungen und keine Hacks*. Fragen zur Sicherheit werden bei NetBSD vom NetBSD Security Officer und dem NetBSD Security Alert Team behandelt. Neben der Untersuchung, dem Dokumentieren und dem Verbessern von Code bezüglich aktueller Sicherheitslücken beschäftigt sich das Team auch mit regelmäßigen Inspektionen des Codes um potentielle Sicherheitslücken zu finden und auszubessern.

NetBSD hat Kerberos IV (KTH-KRB), Kerberos 5 (Heimdal) OpenSSH und IPSEC für IPv4 und IPv6 in das System mit aufgenommen. Zusätzlich sind alle Dienste prinzipiell von vornherein bei und nach der Installation abgeschaltet.

Sicherheitshinweise

Wenn ernsthafte Sicherheitsprobleme in NetBSD gefunden und verbessert werden, wird ein „Security Advisory“ veröffentlicht, daß das Problem beschreibt und einen Verweis auf die Lösung enthält. Diese Anweisungen werden im weiten Kreise angekündigt und auf der Projektseite archiviert.

Das NetBSD-Projekt verwaltet eine Liste von bekannten Sicherheitslücken in Paketen die im Paketsystem vertreten sind. Weitere Informationen finden Sie auf www.NetBSD.org.

File Flags & Security Level

File Flags ermöglichen es den Benutzern oder dem Administrator Dateien mit bestimmten „Flags“ zu markieren und so vor Manipulationen zu schützen. Möglich sind etwas die Optionen *sappnd* oder *uappnd*, mit der Daten an Dateien nur mehr angehängt aber nicht mehr verändert werden dürfen. Markiert man eine Datei als *schg*, kann sie überhaupt nicht mehr verändert werden.

Kernel Security Levels schränken bestimmte Systemfunktionen ein und ermöglichen den Einsatz von File Flags. Hat man z.B. Level 2 aktiviert, sind alle Datenträger nur-lesbar verfügbar und können nicht mehr ein- oder ausgemountet werden. Der TCP/IP-Filter kann nicht mehr verändert werden, und die Systemzeit lässt sich nur noch vor- nicht aber zurückstellen.

Dateimanipulationen erkennen

mtree ist ein Instrument um eine Dateihierarchie gegen eine Spezifikation abzugleichen. Eingesetzt wird es vor allem um installierte Binärdateien gegen eine vorher spezifizierte Liste abzugleichen. Ähnlich *tripwire* oder *AIDE*, kann man *mtree* dazu verwenden Manipulationen an Dateien aufzudecken. Dazu erstellt man einen Fingerabdruck eines Dateisystems, in dem Informationen zu den Dateien (Prüfsummen, Zugriffsrechte) abgelegt werden. Dieser Fingerabdruck kann dann gegen das laufende System abgeglichen werden und deckt so Veränderungen an Dateien (bspw. Würmer, Rootkits oder ähnliches) zuverlässig auf.

Trojaner aussperren

Der NetBSD-Kernel unterstützt „verified executable“, ein System um manipulierte Binärdateien an der Ausführung zu hindern.

Hierzu wird eine Prüfsumme der Binärdateien angelegt und vom Kernel beim Aufruf der Datei mit den aktuellen Daten verglichen. Wurde die Binärdatei verändert (bspw. von einem Wurm, Rootkit oder Einbrecher), verweigert der Kernel die Ausführung des Systems.

Partitionen verschlüsseln

Mit *cgd* kann man auch die Swap- und Temp-Partition verschlüsseln, um zu verhindern daß dort geheime Daten öffentlich werden.

System Calls kontrollieren

Niels Provos' *systrace* erlaubt es eine Policy zu erstellen, mit der man einzelne Syscalls eines Programms kontrollieren kann. So ist es bspw. möglich, Apache von einem normalen Benutzer aus zu starten, weil dieser Benutzer via *systrace* Apache an den Port 80 binden darf - so daß Apache selbst nicht mehr mit Root-Rechten läuft.

Tägliche Sicherheitsüberprüfung

Die beiden Shellskripte */etc/daily* und */etc/security* erlauben es das gesamte System auf Sicherheitslücken hin zu untersuchen. Sie können nächtlich von cron gestartet werden und generieren einen umfassenden Bericht zu Sicherheitsproblemen.

Sicherheitslücken finden

Durch das *audit-packages*-Paket kann eine vom Projekt gepflegte Liste mit Sicherheitslücken heruntergeladen werden und mit dem System verglichen werden. Es werden so alle Pakete mit Sicherheitsproblemen aufgelistet und können dementsprechend aktualisiert werden.

Paketfilter

Mit *IPFilter* und *pf* unterstützt NetBSD im Basissystem zwei ausgereifte Paketfilter für IP-Pakete, die jedes NetBSD-System zur ausgereiften und stabilen Firewall befähigen.

Umfangreiche Sicherheitspakete

Mit *pkgsrc* lassen sich problemlos viele der ausgereiftesten und wichtigsten Sicherheitspakete installieren. Dazu gehören u.a. *snort*, *AIDE*, *Tripwire*, *CFS*, *chkrootkit*, *Nessus*, *Amap*, *GnuPG* und *honeyd*.