Anoubis

Eine Security Suite für Linux und OpenBSD

Dirk Geschke

Linux User Group Erding

27. Januar 2010

Gliederung

Wozu Anoubis

- Granularere Sicherheit jenseits von IPtables und Zugriffsrechten auf Dateien
- Zugriffsregelungen pro Anwendung
- Durch Administrator vorgebbare Regeln
- Durch Benutzer anpassbare Regeln
- Integrität von Dateien/Dokumenten kann sichergestellt werden

Allgemeines zu Anoubis

- BSI–Projekt aus Mitteln des Zukunftsfonds
- Open Source, es steht unter BSD-Lizenz
- Plattformunabhängig: derzeit Linux und OpenBSD
- *Einfache* Benutzbarkeit
- Wird von GeNUA realisiert: CC-konforme Spezifikation, Review-Prozess, Codescanning, Fuzzy-Testing, Scrum-Entwicklung, ...
- Im Internet zu finden: `http://www.anoubis.org/`

Technisches Konzept

- 3 Pakete:
  - Kernelerweiterung
  - Anoubis–Daemon `anoubisd`
  - Benutzertools: `xanoubis` und ein paar Kommandozeilentools
- 3 Sicherheitsmodule

ALF	Application Level Firewall
Sandbox	Sichere Ausführungsumgebung für Programme
SFS	Secure Filesystem

- Kommunikation über drei Unix-Stream-Sockets

Kontrolle von Netzwerkzugriffen

- Eingehende Verbindungen
- Ausgehende Verbindungen
- Anwendungsbezogen
- Es können Kontexte verwendet werden
- Bekannt von Windoze Personal Firewalls.
- Funktioniert effektiv nur auf dem Desktop

Kontrolle von Dateizugriffen

- Überwacht Systemcalls: `read, write, create, unlink, ...`
- Anwendungsbezogen
- Es können Kontexte verwendet werden

Integrität von Dateien

- Programme
- Dateien
- Checksummen
- Mehrere Signaturen möglich
- Überprüfung zur Laufzeit

Typischer Anwendungsfall

- Browser darf ins Internet
- PDF–Viewer darf es nicht
- Schreibzugriff des Browsers nur auf bestimmte Verzeichnisse
- Nachfragen beim Aufbau von VPN–Verbindungen
- `hosts`–Datei darf nicht geändert
- Zugriff auf geänderte Dateien via Nachfrage

Derzeit gibt es noch einige Probleme

- Effektiv nur in grafischer Umgebung nutzbar
- Auswahl von vordefinierten Policies nur optional, Standardpolicy erlaubt alles.
- Anwender muss sich selber beschränken!
- Läuft kein `anoubisd` funktioniert kein Netzwerk
- GUI *noch* nicht intuitiv.
- Man kann sich leicht in den Fuß schießen.
- root kann Anoubis leicht deaktivieren.
- Kernelpatch ist erforderlich
- Handbuch ist suboptimal, Source-Code so gut wie nicht dokumentiert

Praxis. . . !