Zum Hauptmenü

Das Sicherheitskonzept

Einleitung
Der vorrangige Einsatzbereich der mp-Firewall ist die Sicherung der internen Arbeitsplätze gegenüber dem Internet.

Das Konzept
Das Konzept der mp-Firewall zur Erreichung eines hohen Sicherheitsniveaus basiert auf dem Zusammenspiel mehrerer Sicherheitskomponenten und Prinzipien, deren wichtigste im Folgenden kurz skizziert werden sollen:

1. Gehärtetes Server-Betriebssystem
    1. Bereits bei der sorgfältigen Zusammenstellung der Software wurde die Auswahl auf notwendige Funktionalitäten und Dienste beschränkt
    2. Die Auswahl fiel dabei bevorzugt auf Daemons, welche auf Sicherheit optimiert wurden
    3. Der Kern des Linux-basierten Betriebssystems wurde um ein feingranulares Rechtemanagement erweitert. Das dabei eingesetzte RSBAC-System ist eines der weltweit anerkanntesten und umfangreichsten. Es folgt dem Generalized Framework for Access Control (GFAC)-Standard.
    4. Die Kern-Sicherheitserweiterung PaX bietet generischen Schutz gegen die meisten Buffer-Overflow-basierten Angriffe.
    5. Eine weitere Ergänzung des Kerns sorgt für eine zufällige Vergabe von Prozess-IDs – deren übliche Vorhersagbarkeit ermöglicht die Ausnutzung vieler Programmschwächen insbesondere bei Temporär-Dateien.
    6. Alle quelloffenen Programme wurden mit sicherheitsoptimiertem Compiler neu übersetzt.
2. Abbildung organisatorischer und rechtlicher Vorgaben
    1. Alle Daemons laufen mit angepassten RSBAC-Rollenrechten, welche u.a. für Netzwerkzugriffe nur positiv definierte Aktionen zulassen.
    2. Die Administrationsrechte wurden in bereichsspezifische Rollen aufgeteilt – es gibt keinen allmächtigen Superuser mehr.
    3. Lokale Firewall-Regeln verhindern IP-Spoofing, unerwünschte Verbindungsaufbauten und Sicherheitsrisiken durch vertauschte Netzwerkkabel.
    4. Bereits implementierte zweckgebundene Rollen (z.B. Revision/DSB) erleichtern die Aufgabenerfüllung und setzen organisatorische und rechtliche Vorgaben verbindlich um. („Abbildung von Recht in Technik“). Ein Hilfsmenü erlaubt eine zielgerichtete Inspektion ohne viel Lernaufwand.
    5. Revisionssichere Protokollierung aller sicherheitsrelevanten Änderungen von Systemeinstellungen.
    6. Eingeschränkter Zugriff auf Backup-Daten und optionale Verschlüsselung des Backups, sobald es das gesicherte System verlässt.
    7. Unterstützung von Log-Pseudonymisierung und (optional) externem Logserver.

Fazit: Durch die strikte Kapselung der ausführbaren Programme lässt sich auf der mp-Firewall im Allgemeinen ein höheres Sicherheitsniveau erreichen als es im internen Netz (Intranet) möglich ist.

Zum Hauptmenü