SYS.1.10 Server unter OpenBSD

1. Beschreibung

1.1. Einleitung

OpenBSD ist ein freies, Unix-ähnliches Betriebssystem, das aus einer Abspaltung von NetBSD hervorging. Es ist international bekannt für seinen proaktiven Sicherheitsansatz, die hohe Qualität des Quellcodes und die vollständige Integration kryptografischer Funktionen. Das erklärte Ziel der Entwickler ist es, das sicherste verfügbare Mehrzweck-Betriebssystem zu sein. Diesem Ziel wird durch eine "Secure by default"-Philosophie, kontinuierliche Code-Audits und die Entwicklung innovativer Sicherheitsmechanismen wie pledge(2) und unveil(2) nachgegangen.
Aufgrund dieser Eigenschaften wird OpenBSD häufig für sicherheitskritische Aufgaben eingesetzt, beispielsweise als Firewall, DNS-Server, VPN-Gateway oder als Plattform für Intrusion-Detection-Systeme. Die Architektur, die Werkzeuge (insbesondere die Packet Filter Firewall pf) und das Release-Modell unterscheiden sich signifikant von anderen Unix-Derivaten und erfordern daher spezifische Kenntnisse für eine sichere Konfiguration und den Betrieb.

1.2. Zielsetzung

Dieser Baustein zeigt einen systematischen Weg für die Installation, den Betrieb und die Härtung von Servern auf Basis von OpenBSD auf. Ziel ist es, die im System integrierten, fortschrittlichen Sicherheitsfunktionen korrekt zu nutzen, um eine extrem robuste und widerstandsfähige Server-Plattform gemäß den Anforderungen des IT-Grundschutzes bereitzustellen.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.10 ist auf alle Serversysteme anzuwenden, auf denen das Betriebssystem OpenBSD eingesetzt wird.
Er konkretisiert und ergänzt die allgemeinen Anforderungen aus SYS.1.1 Allgemeiner Server. Er ersetzt diesen nicht. Aufgrund des häufigen Einsatzes als Netzkomponente bestehen enge Bezüge zu Bausteinen der Schicht NET, insbesondere zu NET.3.2 Firewall.

2. Gefährdungslage

Für den Baustein SYS.1.10 sind folgende spezifische Bedrohungen und Schwachstellen von besonderer Bedeutung:

Umgehung der Sicherheitsmechanismen durch fehlerhafte Konfiguration

Obwohl OpenBSD standardmäßig sehr sicher konfiguriert ist, können Administratoren durch unsachgemäße Anpassungen die eingebauten Schutzmechanismen aushebeln. Beispiele sind übermäßig freizügige Regeln in der pf.conf, das Deaktivieren von Sicherheitsfunktionen in Drittanbieter-Software oder das fehlerhafte Erstellen eigener Skripte ohne Nutzung von pledge und unveil.

Veraltete Systemversionen durch inkonsequentes Patching

Das OpenBSD-Projekt veröffentlicht alle sechs Monate eine neue Version und stellt für die jeweils aktuelle und die vorherige Version Sicherheitspatches über syspatch bereit. Werden diese Patches nicht zeitnah eingespielt oder die halbjährlichen Upgrades via sysupgrade versäumt, bleibt das System auf einem veralteten Stand und ist gegen neu entdeckte Schwachstellen ungeschützt.

Unsichere Konfiguration von Diensten aus dem Ports-System

Während das Basissystem einem intensiven Audit unterliegt, gilt dies nicht im selben Maße für die Tausenden von Softwarepaketen, die über das Ports-System verfügbar sind. Die Installation und der Betrieb einer schlecht konfigurierten oder fehlerhaften Drittanbieter-Anwendung kann die hohe Sicherheit des Basissystems untergraben.

Kompromittierung durch unsachgemäße Administration

Trotz der robusten technischen Absicherung bleibt der Faktor Mensch eine Schwachstelle. Die Verwendung des root-Kontos für alltägliche Arbeiten, die Nutzung schwacher Passwörter (obwohl SSH standardmäßig auf Schlüssel-Authentifizierung setzt) oder die unsachgemäße physische Absicherung des Servers können das System kompromittieren.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.10 aufgeführt.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.10.A1 Gesicherte und minimalistische Installation (B)

Die Installation von OpenBSD MUSS von einem verifizierten Installationsmedium (z. B. via signify) erfolgen. Während der Installation DÜRFEN nur die zwingend benötigten Dateisets ausgewählt werden. Es MUSS ein sicheres Passwort für das root-Konto vergeben werden.

SYS.1.10.A2 Regelmäßes Einspielen von Sicherheitspatches (B)

Es MUSS ein Prozess etabliert werden, der sicherstellt, dass die für die eingesetzte OpenBSD-Version bereitgestellten Sicherheitspatches mittels des syspatch-Werkzeugs zeitnah eingespielt werden.

SYS.1.10.A3 Aktivierung und grundlegende Konfiguration der pf-Firewall (B)

Die Paketfilter-Firewall pf MUSS aktiviert sein. In der Konfigurationsdatei pf.conf MUSS eine "Default Deny"-Strategie umgesetzt sein, bei der jeglicher Netzwerkverkehr standardmäßig blockiert und nur explizit benötigter Verkehr erlaubt wird.

SYS.1.10.A4 Absicherung des SSH-Zugangs (B)

Der SSH-Dienst (sshd) MUSS so konfiguriert sein, dass ein direkter Login des root-Benutzers verboten ist (PermitRootLogin no). Die Authentifizierung MUSS

ausschließlich über kryptografische Schlüssel erfolgen; die Passwort-Authentifizierung MUSS deaktiviert sein (PasswordAuthentication no).

SYS.1.10.A5 Kontrollierte Installation von Drittanbieter-Software (B)

Software, die nicht Teil des Basissystems ist, DARF nur über das offizielle Paketmanagement-System (pkg_add) aus vertrauenswürdigen Quellen installiert werden. Es DARF nur Software installiert werden, die für den Betrieb des Systems zwingend erforderlich ist.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.10.A6 Systematische Release-Upgrades (S)

Es SOLLTE ein Prozess etabliert werden, um die halbjährlichen Release-Upgrades zeitnah durchzuführen, vorzugsweise unter Nutzung des automatisierten sysupgrade-Mechanismus. Ziel SOLLTE sein, stets eine vom OpenBSD-Projekt unterstützte Version zu betreiben.

SYS.1.10.A7 Konsequente Deaktivierung nicht benötigter Dienste (S)

Alle im Basissystem enthaltenen, aber für den spezifischen Einsatzzweck nicht benötigten Dienste SOLLTEN mittels des rcctl-Werkzeugs dauerhaft deaktiviert werden.

SYS.1.10.A8 Härtung der Dateisysteme in /etc/fstab (S)

In der Konfigurationsdatei /etc/fstab SOLLTEN sicherheitsrelevante Mount-Optionen für die Dateisysteme gesetzt werden. Dies umfasst insbesondere nodev, nosuid und noexec für Partitionen, auf denen keine Geräte, Setuid-Binaries oder ausführbare Programme erwartet werden (z. B. /tmp, /var, /home).

SYS.1.10.A9 Konfiguration der Systemprotokollierung (S)

Der syslogd-Dienst SOLLTE so konfiguriert werden, dass er relevante Sicherheitsereignisse protokolliert. Die Protokolldaten SOLLTEN an ein zentrales Log-Management- oder SIEM-System weitergeleitet werden, wobei die Übertragung verschlüsselt erfolgen SOLLTE.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Die folgenden Anforderungen sind exemplarische Vorschläge für ein Schutzniveau, das über den Stand der Technik hinausgeht. Sie SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden.

SYS.1.10.A10 Einsatz von Festplattenverschlüsselung (H)

Das gesamte System oder zumindest Partitionen mit sensiblen Daten SOLLTEN bei der Installation mit der integrierten softraid(4)-Verschlüsselung verschlüsselt werden.

SYS.1.10.A11 Erstellung und Nutzung von Firewall-Clustern mit CARP und pfsync (H)

Wird OpenBSD als sicherheitskritische Netzwerkkomponente (z. B. Firewall) eingesetzt, SOLLTE ein hochverfügbarer Cluster mittels des Common Address Redundancy Protocol (CARP) und pfsync aufgebaut werden, um eine redundante und ausfallsichere Funktion zu gewährleisten.

SYS.1.10.A12 Einsatz von pledge(2) und unveil(2) für eigene Skripte (H)

Werden auf dem System eigene oder komplexe Skripte und Anwendungen betrieben, SOLLTEN diese so angepasst werden, dass sie die Sicherheitsmechanismen pledge (zur Einschränkung der verfügbaren Systemaufrufe) und unveil (zur Beschränkung des sichtbaren Dateisystems) aktiv nutzen.

SYS.1.10.A13 Erstellung eines gehärteten, angepassten Kernels (H)

Für Systeme mit maximalen Schutzanforderungen SOLLTE ein eigener Kernel kompiliert werden, aus dem alle nicht benötigten Treiber, Protokolle und Funktionalitäten entfernt wurden, um die Angriffsfläche auf das absolute Minimum zu reduzieren.

SYS.1.10.A14 Regelmäßige Überprüfung der Systemintegrität (H)

Die Integrität der Dateien des Basissystems SOLLTE regelmäßig überprüft werden, indem die Checksummen der installierten Dateien mit den offiziellen Checksummen des jeweiligen Releases (SHA256.sig) verglichen werden.