SYS.1.11 Server unter FreeBSD

1. Beschreibung

1.1. Einleitung

FreeBSD ist ein freies, leistungsfähiges und stabiles Unix-derivatives Betriebssystem, das für seine Robustheit im Netzwerk- und Serverbereich bekannt ist. Es zeichnet sich durch eine Reihe von fortschrittlichen und tief im System integrierten Technologien aus, die es von anderen Unix-artigen Systemen, insbesondere Linux-Distributionen, unterscheiden. Zu den Kernmerkmalen gehören das leistungsfähige Dateisystem ZFS, das standardmäßig integriert ist, das leichtgewichtige Virtualisierungs- und Sicherheitssystem "Jails" zur Isolation von Prozessen und Diensten sowie ein klares Trennungsmodell zwischen dem Basissystem und Drittanbieter-Software (Ports/Packages).
Diese spezifischen Architekturentscheidungen und Werkzeuge erfordern angepasste Sicherheitsstrategien. Die Konfiguration von ZFS-Datasets, die Absicherung von Jails oder das Management des Basissystems über freebsd-update folgen anderen Paradigmen als bei anderen Systemen. Ein dedizierter Baustein ist daher notwendig, um die Sicherheitsfunktionen von FreeBSD korrekt zu nutzen und zu härten.

1.2. Zielsetzung

Dieser Baustein zeigt einen systematischen Weg für die sichere Installation, Konfiguration und den Betrieb von Servern unter FreeBSD auf. Ziel ist es, eine robuste, sichere und performante Server-Plattform zu schaffen, indem die spezifischen Sicherheits- und Verwaltungsfunktionen des Betriebssystems, insbesondere Jails und ZFS, sachgerecht eingesetzt und abgesichert werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.11 ist auf alle Serversysteme anzuwenden, auf denen das Betriebssystem FreeBSD eingesetzt wird.
Er ergänzt und konkretisiert die allgemeinen Anforderungen aus SYS.1.1 Allgemeiner Server. Bei der Nutzung von Jails bestehen konzeptionelle Bezüge zum Baustein CON.5 Containerisierung, obwohl die technische Umsetzung sich unterscheidet. Anforderungen an die Speichersicherheit bei der Nutzung von ZFS werden hier spezifisch behandelt und ergänzen APP.4.4 Speicherlösungen.

2. Gefährdungslage

Für den Baustein SYS.1.11 sind folgende spezifische Bedrohungen und Schwachstellen von besonderer Bedeutung:

Ausbruch aus FreeBSD-Jails

Eine fehlerhafte Konfiguration einer Jail kann einem Angreifer ermöglichen, aus der isolierten Umgebung auszubrechen und auf das Host-System zuzugreifen. Dies kann durch die Vergabe zu weitreichender Privilegien an die Jail, Schwachstellen im Kernel oder unsichere Interaktionen zwischen Host und Jail verursacht werden.

Kompromittierung durch unsichere Drittanbieter-Pakete

FreeBSD bietet ein riesiges Repositorium an Software von Drittanbietern über das Ports- und Paketsystem. Wird Software aus nicht vertrauenswürdigen Quellen installiert oder werden bekannte Schwachstellen in installierten Paketen nicht zeitnah behoben, kann dies als Einfallstor zur Kompromittierung des gesamten Systems dienen.

Fehlkonfiguration mächtiger Systemkomponenten wie ZFS

Das ZFS-Dateisystem bietet eine Vielzahl von Funktionen wie Snapshots, Klone und Replikation. Eine unsachgemäße Konfiguration, beispielsweise die unverschlüsselte Replikation sensibler Daten über ein unsicheres Netzwerk oder fehlende Snapshots zur Wiederherstellung nach einem Ransomware-Angriff, kann zu Datenverlust oder -offenlegung führen.

Deaktivierung von Sicherheitsfunktionen durch unsachgemäßes System-Tuning

FreeBSD erlaubt eine weitreichende Konfiguration von Kernel-Parametern über sysctl. Werden hier ohne genaue Kenntnis der Auswirkungen Änderungen vorgenommen, können versehentlich wichtige Sicherheitsfunktionen deaktiviert oder das System für Denial-of-Service-Angriffe anfällig gemacht werden.

Veraltetes Basissystem und unzureichendes Patching

Eine Besonderheit von FreeBSD ist die strikte Trennung zwischen dem Basissystem (gepflegt via freebsd-update) und den installierten Paketen (gepflegt via pkg). Wird einer dieser beiden Update-Pfade vernachlässigt, entstehen Sicherheitslücken, die von Angreifern ausgenutzt werden können.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.11 aufgeführt.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.11.A1 Gesicherte und minimalistische Installation (B)

Die Installation von FreeBSD MUSS von einem verifizierten, offiziellen Installationsmedium erfolgen. Während der Installation DÜRFEN nur die für den Betrieb zwingend erforderlichen Komponenten des Basissystems ausgewählt werden. Ein sicheres Passwort für das root-Konto MUSS vergeben werden.

SYS.1.11.A2 Konsequentes Patch-Management für Basissystem und Pakete (B)

Es MUSS ein Prozess etabliert sein, der sicherstellt, dass sowohl das Basissystem mittels freebsd-update als auch alle installierten Drittanbieter-Pakete mittels pkg upgrade zeitnah aktualisiert werden. Bekannte Schwachstellen in Paketen MÜSSEN mittels pkg audit regelmäßig geprüft werden.

SYS.1.11.A3 Aktivierung einer systemeigenen Firewall (B)

Eine der in FreeBSD integrierten Firewalls (PF oder IPFW) MUSS aktiviert und mit einer restriktiven "Default Deny"-Regelbasis konfiguriert sein, die nur explizit benötigten Verkehr erlaubt.

SYS.1.11.A4 Absicherung des SSH-Zugangs (B)

Der SSH-Dienst MUSS so konfiguriert sein, dass ein direkter Login des root-Benutzers verboten ist. Die Authentifizierung MUSS ausschließlich über kryptografische Schlüssel erfolgen.

SYS.1.11.A5 Deaktivierung nicht benötigter Dienste (B)

Alle Dienste, die standardmäßig aktiviert sind, aber für den spezifischen Betriebszweck nicht benötigt werden, MÜSSEN in der Datei /etc/rc.conf deaktiviert werden.

3.2. Standard-Anforderungen

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

SYS.1.11.A6 Isolation von Diensten mittels Jails (S)

Netzwerkdienste SOLLTEN voneinander und vom Host-System isoliert werden, indem jeder Dienst in einer eigenen, dedizierten FreeBSD-Jail betrieben wird.

SYS.1.11.A7 Strukturierte Nutzung von ZFS-Dateisystemen (S)

Das ZFS-Dateisystem SOLLTE genutzt werden, um Daten logisch zu strukturieren (z. B. separate Datasets für das Basissystem, Jails, Benutzerdaten). Es SOLLTEN regelmäßig automatisiert Snapshots erstellt werden, um die Wiederherstellung von Daten zu ermöglichen.

SYS.1.11.A8 Härtung des Kernels über sysctl (S)

Sicherheitsrelevante Kernel-Parameter SOLLTEN in der Datei /etc/sysctl.conf konfiguriert werden, um das System zu härten. Dies SOLLTE Maßnahmen zum Schutz vor Netzwerkangriffen und zur Einschränkung von Informationslecks umfassen.

SYS.1.11.A9 Konfiguration von Ressourcenlimits (S)

Um Denial-of-Service-Angriffe durch Ressourcenerschöpfung zu erschweren, SOLLTEN über die Login-Klassen in der Datei /etc/login.conf Ressourcenlimits für Benutzer und Dienste festgelegt werden.

SYS.1.11.A10 Zentrale Protokollierung von Systemereignissen (S)

Der syslog-ng- oder syslogd-Dienst SOLLTE so konfiguriert werden, dass sicherheitsrelevante Ereignisse vom Host und aus den Jails an ein zentrales Log-Management- oder SIEM-System weitergeleitet werden.

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.1.11.A11 Einsatz von ZFS-Verschlüsselung (H)

Datasets auf ZFS, die sensible Daten enthalten, SOLLTEN mit der nativen Verschlüsselungsfunktion von ZFS verschlüsselt werden.

SYS.1.11.A12 Erweiterte Härtung von Jails (H)

Jails SOLLTEN zusätzlich gehärtet werden, indem ihnen dedizierte Ressourcenlimits mittels rctl zugewiesen und ihre Berechtigungen über spezifische Jail-Parameter (z. B. securelevel, allow.*) auf das absolute Minimum reduziert werden.

SYS.1.11.A13 Absicherung des Boot-Prozesses (H)

Sofern die Hardware dies unterstützt, SOLLTE der UEFI Secure Boot Mechanismus genutzt werden, um sicherzustellen, dass nur ein signierter Bootloader ausgeführt wird.

SYS.1.11.A14 Einsatz des Mandatory Access Control (MAC) Frameworks (H)

Für Systeme mit besonders hohen Schutzanforderungen SOLLTE das Mandatory Access Control (MAC) Framework von FreeBSD aktiviert und mit einem geeigneten Sicherheitsrichtlinienmodul (z. B. mac_bsdextended) konfiguriert werden, um die Zugriffsrechte von Prozessen und Benutzern feingranular zu steuern.

SYS.1.11.A15 Erstellung eines gehärteten, angepassten Kernels (H)

Für hochkritische Systeme SOLLTE ein angepasster Kernel kompiliert werden, aus dem alle für den Betrieb nicht erforderlichen Treiber und Funktionen entfernt wurden.