Anforderungen an eine sichere Installationsumgebung für Blockchain-Nodes

K. Wittek[1], T. Spielmann[1]
[1] Institut für Internet-Sicherheit – if(is), Westfälische Hochschule, Gelsenkirchen, Deutschland
kontakt_reallabor@fit.fraunhofer.de

Ausgangssituation und Problemstellung

Blockchain-Nodes sind teilnehmende Komponenten an einem P2P Blockchain-Netzwerk. Sie übernehmen unterschiedlichste Aufgaben: Vorhaltung einer Ausprägung der Blockchain, Minen neuer Blöcke, Validieren neuer Blöcke, Ausführen von Smart Contracts, etc. Nodes sind hierbei potentiell verwundbare Stellen eines Blockchain-Netzes und auch lohnenswerte Angriffsziele. Daher muss nicht nur die spezifische Blockchain-Software, sondern auch das darunterliegende System sehr robust konfiguriert und entsprechend gehärtet werden.

Anwendungskontext

Blockchain-Nodes sind gleichzeitig Server und Client. Sie stellen eine oder mehrere Dienste in einem Netzwerk zur Verfügung und sind als essentielle Komponente eines Blockchain-Netzwerks vielen Zugriffen ausgesetzt. Diese Zugriffe stellen zweierlei Risiko da.
Zum einen muss der Server in der Lage sein, eine große Anzahl von simultanen Zugriffen verarbeiten zu können. Sollte dies nicht möglich sein, droht ein ungewollter und nicht boshafter denial-of-service (DOS). Dies muss durch verschiedene Strategien und Konzepte im Hardware- Software- und Netzwerk-Stack (load balancing, backpressure, parallelisierung, scheduling) verhindert werden.
Zum anderen muss man im Sinne einer sicheren Systemarchitektur damit rechnen, dass nicht jeder Zugriff gutartig ist. Sollte ein bösartiger Zugriff die Node erreichen, darf dieser nicht bis zu seinem Ziel durchdringen, sondern muss so früh wie möglich erkannt werden. Diese Erkennung ist jedoch nicht auf die Ressourcen des Servers beschränkt. Hier kann klassisches Netzwerk-Monitoring eingesetzt werden. Somit können Anomalien frühzeitig erkannt werden.

Eine kompromittierte Node gefährdet die Sicherheit und Integrität des gesamten Blockchain-Systems.

Lösungsansätze

Die Absicherung des Servers ist ein allseits bekanntes Problem. Daher gibt es Standardmaßnahmen, welche für jeden Internet-Server ergriffen werden sollten:

- Auswahl eines geeigneten Serverbetriebssystems inklusive Härtung (z.B. durch SELinux)
- Schließung von nicht notwendigen Ports durch die Firewall
- Rechte- und Rollensystem für Benutzer und Betreiber des Servers
- Schlüsselmaterial und Zertifikate in geschützten Ordnern ablegen, Festplattenverschlüsselung (Encryption at rest)
- Installation von nicht benötigter Zusatzsoftware vermeiden (Minimierung des Attack-Surface)

Ein Load-Balancer kann dafür sorgen, dass die Zugriffe auf einen Server so gesteuert werden, dass dieser, in Kombinationen mit einem Ressourcen-Pool, die Last jederzeit gut bewältigen kann. Doch welche Anforderungen müssen an einen Load-Balancer für eine Blockchain-Node gestellt werden? Ist dieser überhaupt notwendig? Wenn ja, wie muss er umgesetzt werden? Wo muss er topologisch angeordnet werden, auf dem Server, in einer separaten Instanz davor, usw.?

Auch das Netzwerk-Monitoring inklusive der Erkennung von Anomalien im Netzwerk ist ein mächtiges Werkzeug zur Früherkennung von möglichen Angriffen. Da jedoch der Netzwerk-Traffic in einem P2P Blockchain-Netzwerk andere Regeln folgt, als ein herkömmliches Client-Server-Netzwerk müssen hierfür unter Umständen neue Regeln und Algorithmen entwickelt werden. Wie unterscheidet sich "normaler" Traffic eines Blockchain-Systems von

sonstigem Netzwerkverkehr in Client-Server-Netzwerken? Wie sehen Anomalien aus, die auf einen Angriff hinweisen können?

Ziel dieser Forschungsfrage soll eine Guideline für Administratoren von Blockchain-Nodes sein. Diese sollen hieraus entnehmen können, mit welchen Maßnahmen ein Server im Allgemeinen abgesichert werden kann, und welche Maßnahmen darüber hinaus erforderlich sind, wenn hierauf ein Blockchain-Node sicher betrieben und überwacht werden soll.

Literatur

1. Martin Hensel, Andreas Donner; 29.10.2018; "IT-Awards 2018 - Die beliebtesten Netzwerk-Monitoring-Anbieter 2018"; veröffentlicht auf: https://www.ip-insider.de/die-beliebtesten-netzwerk-monitoring-anbieter-2018-a-769242/

2. Norbert Pohlmann, 2019, "Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung", Kapitel 7: Trusted Computing

Forschungseinrichtungen

Zur Bearbeitung dieser Forschungsfrage sind Kompetenzen aus folgenden Bereichen erforderlich:

- Cyber-Security
- Informatik (UX)