

Eigenschaften eines Taps

Ein Tap (Test Access Point) kann direkt in eine Netzwerkverbindung eingefügt werden. Taps sind verfügbar für 10/100/1000 Mbps Kupfer oder Glasfaser Netzwerke. Sie spiegeln den full-duplex Verkehr dieser Verbindung zu einem Sensor (jeweils die Sende- und Empfangsrichtung).



Abbildung 1: Netzwerk-Tap

Bei Taps handelt es sich um eine passive Komponente. Dies hat folgende Vorteile:

- Keine IP-Adresse
- Keine Rückwärtskommunikation des Sensors in das überwachte Netzwerk
- Keine ARP-Pakete

Das bedeutet, dass das IDS-Netzwerk im Verborgenen bleibt. Daten werden nur zum Sensor geschickt. Von ihm werden keine Daten angenommen. Somit ist der Sensor für einen Angreifer nicht erreichbar und kann nicht direkt angegriffen werden.

- Kein single point of failure

Wird der Strom unterbrochen, wird der Netzwerkverkehr durchgeschleift. Es gibt somit keine Unterbrechung der Verbindung.



Taps machen es möglich den gesamten Verkehr der überwachten Netzwerkverbindungen zu analysieren:

- Keine Verzögerungen der Datenströme

Der Sensor erhält den selben Traffic, als wenn er in-line wäre, da der Tap das full-duplex Signal ohne Verzögerungen oder Veränderungen der Pakete weiterreicht.

- Netzwerkperformance wird nicht beeinträchtigt

- Keine Fehlerkorrektur auf dem Tap

Im Gegensatz zu einem Span-Port gelangen fehlerhafte Pakete in unverändertem Zustand bis zum Sensor, wo sie vom Intrusion Detection System analysiert werden können.

Durch Taps ist es möglich, den gesamten Verkehr der überwachten Netzwerkverbindung zu analysieren. Sie sorgen weiterhin dafür, dass keine Daten aus dem IDS-Netzwerk oder von dem Sensor in das Produktivnetz gelangen. Dadurch bleibt das gesamte IDS im Verborgenen. Es kann weder angegriffen noch belauscht werden.

Neben Taps gibt es auch die Möglichkeit einen Sensor über einen Span (Switch Port Analyzer)-Port eines Switchs mit Daten des Netzwerkverkehrs zu versorgen.

Vergleich zwischen einem Tap und einem Span-Port eines Switchs:

Vergleich	Tap	Span-Port
Weiterleitung der Pakete	alle Pakete	verwirft zu kleine oder korrupte Pakete
Mitlesen des Verkehrs	kann full-duplex mitlesen	abhängig von der Kapazität des Ports
Kopieren der Pakete	in real-time	Performanceverluste möglich

Um effektiv arbeiten zu können muss ein Intrusion Detection System korrekte sowie unkorrekte Pakete sehen können und in real-time die Pakete zur Verfügung haben. Taps ermöglichen den Zugriff auf alle Pakete aller Schichten in real-time. Sie reichen den gesamten Netzwerkverkehr weiter.

