Open Resolver

Im Rahmen des Shadowserver "Open Resolver Scanning Projects" werden offene DNS-Resolver identifiziert. Diese können potenziell für DDoS-Angriffe mittels DNS-Amplification missbraucht werden, sofern keine entsprechenden Gegenmaßnahmen wie Rate-Limiting implementiert wurden.

Nachfolgend senden wir Ihnen eine Liste identifizierter offener DNS-Resolver in Ihrem Netzbereich. Der Zeitstempel gibt an, wann der betreffende DNS-Server geprüft wurde. Der Wert "Min. Amplification" gibt den Verstärkungsfaktor (Verhältnis der Größe des Antwortpakets zur Paketgröße der Anfrage) an, welche von Angreifern bei Missbrauch des DNS-Servers für DNS-Amplification-Angriffe mindestens erreicht werden kann. Mit dieser Benachrichtigung werden nur DNS-Server gemeldet, bei denen der Verstärkungsfaktor im Rahmen der Tests mindestens 5.0 betrug.

Wir möchten Sie bitten zu prüfen, ob die offenen Resolver in Ihrem Netzbereich beabsichtigt als solche konfiguriert sind und falls ja, ob entsprechende Schutzmaßnahmen zur Verhinderung des Missbrauchs der Server für DDoS-Angriffe implementiert wurden.

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/open-resolver/