Aktive Teilnahme an DDOS-Attacken

CERT-Bund liegen Beschwerden zu Systemen in Ihrem Netzbereich vor, welche **aktiv** an DDoS-Angriffen gegen Dritte teilgenommen haben.

Es handelt sich dabei um DDoS-Reflection-Angriffe, welche unter Ausnutzung offen aus dem Internet erreichbarer UDP-basierter Dienste ausgeführt wurden (offene DNS-Resolver, NTP-Server mit aktiver "monlist"-Funktion, offene SNMP-Server, etc.).

Nachfolgend senden wir Ihnen eine Liste der Systeme in Ihrem Netzbereich, welche aktiv an den DDoS-Angriffen beteiligt waren.

Der Zeitstempel (Zeitzone UTC) gibt an, wann das erste Angriffspaket von dem jeweiligen System gesendet wurde.

Weiterhin sind der Quellport sowie der missbrauchte Dienst angegeben. Viele der offenen Dienste wurden Ihnen bereits seit längerer Zeit regelmäßig präventiv von CERT-Bund gemeldet mit der Bitte, den Zugriff aus dem Internet auf diese Dienste zu unterbinden, um einen Missbrauch für DDoS-Angriffe zu verhindern.

Wir möchten Sie nun bitten, den Sachverhalt zu prüfen und **umgehend** entsprechende Maßnahmen zu ergreifen, welche den weiteren Missbrauch der Dienste für DDoS-Angriffe gegen Dritte wirksam verhindern.

Weitere Informationen zu dieser Benachrichtigung sowie Hinweise zur Absicherung der jeweiligen Dienste (HOWTOs) finden Sie unter: https://reports.cert-bund.de/

Quelle: https://support.belwue.de/sicherheit/sicherheitswarnungen/aktive-teilnahme-an-ddos-attacken/