Abuse-Message [AbuseID:535EA2:1E]: AbuseInfoMail: [CB-Report#20181001-10004541] DDoS-Angriffe von Systemen in AS24940

abuse an sirzimt 1. Okt.

Sehr geehrte(r) Herr Sebastian Anderie,

wir haben einen Spam- bzw. Abuse-Hinweis von reports@reports.cert-bund.de erhalten.

Die Weiterleitung dieser Beschwerde dient nur als Information für Sie.
Es steht Ihnen frei, ob Sie dem Grund der Beschwerde nachgehen.
Wir erwarten bezüglich dieser Beschwerde keine Rückmeldung Ihrerseits

Informationen:
Sehr geehrte Damen und Herren,

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.).

Im Anhang 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>

Diese E-Mail ist mittels PGP digital signiert.
Informationen zu dem verwendeten Schlüssel finden Sie unter:
<https://reports.cert-bund.de/digitale-signatur>

Bitte beachten Sie:
Dies ist eine automatisch generierte Nachricht. Antworten an die
Absenderadresse <reports@reports.cert-bund.de> werden NICHT gelesen
und automatisch verworfen. Bei Rückfragen wenden Sie sich bitte
unter Beibehaltung der Ticketnummer [CB-Report#...] in der
Betreffzeile an .

!! Bitte lesen Sie zunächst unsere HOWTOs und FAQ, welche unter
!! <https://reports.cert-bund.de/> verfügbar sind.

Mit freundlichen Grüßen
Team CERT-Bund

Bundesamt für Sicherheit in der Informationstechnik
Federal Office for Information Security (BSI)
Referat CK22 - CERT-Bund

Godesberger Allee 185-189, 53175 Bonn, Germany

24940 176.9.82.54 2018-09-30 06:49:35 100000 4 111/udp; 100000 3 111/udp; 100000 2 111/udp; 100000 4 111/udp; 100000 3 111/udp; 100000 2 111/udp;

Wichtiger Hinweis:
Wenn Sie uns antworten, lassen Sie bitte die Abuse-ID [AbuseID:535EA2:1E] im Betreff unverändert.

Mit freundlichen Grüßen

Konrad Mallok

Fachinformatiker Anwendungsentwicklung

Hetzner Online GmbH
Industriestr. 25
91710 Gunzenhausen
Tel: +49 9831 505-0
Fax: +49 9831 505-3
abuse@hetzner.com
www.hetzner.de

Registergericht Ansbach, HRB 6089
Geschäftsführer: Martin Hetzner