it-safe: Achten Sie gerade jetzt auf Cybersicherheit!

DDoS Angriffe gegen Unternehmen

cert.at warnt vor Erpresser-E-mails

Stand: 15.06.2021

Beschreibung

Seit einigen Wochen versucht eine Gruppe, die sich "Fancy Lazarus" nennt, mittels DDoS-Angriffen und der Androhung von Folgeangriffen, Schutzgelder zu erpressen. Vergleichbare Angriffe gab es global auch schon ab August 2020 unter ähnlichen Namen.

Nachdem wir Meldungen von Partner-CERTs an uns über Angriffe auf Ziele in anderen EU Staaten bekommen haben, sind jetzt auch in Österreich einige Fälle aufgetreten.

Modus Operandi:

- Erpressungs-E-Mail an Unternehmen (Ankündigung des Demo-Angriffs, Zahlungsfrist 7 Tage, sonst großer Angriff)
- Kurz darauf ein DDoS-Angriff (30 - 250 GBit/s DNS-Reflection gegen die autoritativen Nameserver des Ziels, Dauer 2+ Stunden)
- Uns liegen einige Meldungen vor, dass nach dem Verstreichen der sieben Tage der angedrohte Angriff nicht stattgefunden hat. Gegenteilige Meldungen liegen nicht vor.

Auswirkungen

Überlastung der Internetanbindung, dadurch werden sowohl die vom Ziel angebotenen Dienste, als auch die Nutzung des Internets vom Netz des Zieles aus, gestört.

Abhilfe

Wie bei vielen anderen Bedrohungen auch, sollte man hier nicht auf das Eintreten warten, sondern sich proaktiv mit dem Thema beschäftigen.

- DDoS-Angriffe sind seit einigen Jahren Teil der Bedrohungslage für alle im Internet aktiven Firmen.
- Im Risikomanagement ist daher zu bewerten, was die essentiellen Dienste sind und welche Ausfallzeiten bei diesen akzeptabel sind.
- Im Business Continuity Management sollte überlegt werden, wie die essentiellen Dienste auch unter erschwerten Bedingungen weitergeführt werden können.
- Bei den zu erwartenden Bandbreiten ist eine Mitigation rein im eigenen Netz nicht möglich: es braucht die Mithilfe des Upstream Providers oder eines Cloud-Services. Reden sie vorab mit ihrem ISP über die Optionen und welche Hilfe sie erwarten können. Stellen sie auch Kontaktmöglichkeiten außerhalb der Geschäftszeiten sicher.
- Im aktuellen Fall werden die autoritativen Nameserver angegriffen. Da das DNS schon im Protokolldesign redundante Nameserver unterstützt, ist es sehr einfach, für die eigenen Domains zusätzlich weitere Nameserver außerhalb des eigenen Netzes zu nutzen. Entsprechende Angebote, die auch per Anycasting viel Resilienz und Geodiversität einbringen, sind vergleichsweise günstig.
- Existiert eine redundante Anbindung über mehrere ISPs, so macht es Sinn vorzubereiten, den Datenverkehr so aufzuteilen, dass der Angriff möglichst einen anderen Weg nimmt, als der legitime Datenverkehr.
- Stellen Sie sicher, dass der Fernwartungszugang für das Betriebspersonal nicht rein von der potentiell überlasteten Internetanbindung abhängig ist.

Informationsquelle(n):

- *Proofpoint Artikel vom 10. Juni 2021 (englisch)*
- *DDoS Whitepaper des CSC (Juli 2020)*

Quelle: cert.at, 14. Juni 2021

Weitere Informationen:

- https://cert.at/de/ nationales Computer Emergency Response Team mit Warnungen, Alerts und Tipps für Cybersicherheit
- https://www.watchlist-internet.at// Infos zu Internetbetrug, Fallen & Fakes
- https://www.schutzverband.at/ Schutzverband gegen unlauteren Wettbewerb
- Aktuelle Betrugswarnungen