EU-Agentur ENISA: Internetdienstanbieter ungenügend im Anwenden von Filtern gegen Großangriffe im Netz

In ihrer Analyse eines kürzlich stattgefundenen massiven Internet-Angriffs stellt die EU Internet-Sicherheitsagentur ENISA heute fest, dass Internetdienstanbieter (Internet Service Providers, ISPs) bis heute allgemein bekannte Sicherheitsmaßnahmen, die bereits seit mehr als einem Jahrzehnt zur Verfügung stehen, nur ungenügend anwenden. Die Agentur hebt in ihrer Informations-Flash-Note 'Können kürzlich stattgefundene Internet-Angriffe die Verfügbarkeit des Internets tatsächlich gefährden' hervor, dass dieser Fehler ein Hauptgrund dafür ist, dass das Abwehren größerer Internet-Angriffe scheitert.

Die Flash Note bezieht sich auf einen groß angelegten Internet-Angriff, der im März gegen die gemeinnützige Organisation Spamhaus, die in Genf und Londen ihren Sitz hat, inszeniert wurde. Der digitale Angriff verursachte spürbare Behinderungen für die Internet-Nutzer, insbesondere in Großbritannien, Deutschland und anderen Teilen Westeuropas. Laut Angaben der Online-Medien war der Angriff auf Spamhaus, der am 16. März begann, der größte Angriff verteilter Service-Verweigerung (Distributed Denial of Service, DDoS) in der Geschichte des Internets. Bei DDoS-Angriffen wird die Fähigkeit einer Internetseite, den eingehenden Datenverkehr zu bewältigen, „überladen". Der Angriff auf Spamhaus dauerte mehr als eine Woche an. In seiner finalen Phase verursachte die enorme Menge an generiertem Datenverkehr Probleme beim Londoner Internet-Austauschpunkt (London Internet Exchange).

ENISA hebt hervor, dass die Technik, die bei DDoS-Angriffen verwendet wird, keinesfalls neu ist. Dennoch werden eine Reihe von Empfehlungen, auch bekannt als optimale Vorgehensweise (Best Current Practice 38, BCP38), von vielen Internet-Anbietern auch heute noch nicht genutzt, obwohl es die BCP38 bereits seit fast 13 Jahren gibt. Bereits das Nutzen einer ähnlichen Reihe von Empfehlungen für DNS-Server-Betreiber (BCP140, veröffentlicht im Jahr 2008) würde die Anzahl der Server, die für DNS-Überladungsangriffe missbraucht werden können, reduzieren. Würden obig genannte Empfehlungen von allen Betreibern umgesetzt werden, würden solche Angriffe durch Filtern des Datenverkehrs automatisch geblockt.

Laut ENISA gibt es eine Reihe von Lehren, die aus dem Angriff gezogen werden können, unter anderem:

- Immer größere Datenmengen werden bei Angriffen erreicht. Der Angriff auf Spamhaus im März 2013 erreichte eine Datenmenge von mehr als 300 Gigabits pro Sekunde, während der bis dahin größte DDoS-Angriff im Jahr 2012 eine Datenmenge von 100 Gigabits pro Sekunde erreichte.

- Die erreichte Datenmenge hat Auswirkungen. Bei bestimmten Größenordnungen können selbst geschäftliche Internet-Austauschpunkte, die im Allgemeinen ein sehr hohes Fassungsvermögen haben, beeinträchtigt werden.

Die Agentur hat 3 technische Empfehlungen:

- Wichtige Service-Betreiber sollten die BCP38 einführen
- Betreiber von DNS-Servern sollten überprüfen, ob ihre Server missbraucht werden können und sollten die BCP140 einführen
- Betreiber von Internet-Austauschpunkten sollten sicherstellen, dass sie gegen direkte Angriffe geschützt sind.

Der Executive Director der ENISA, Professor Udo Helmbrecht, sagt: *„Internet-Anbieter, welche die BCP38 und BCP140 noch implementieren müssen, sollten ernsthaft in Betracht ziehen, dies so schnell wie möglich vorzunehmen, andernfalls werden ihre Kunden und ihr Ruf darunter leiden. Prävention ist der Schlüssel zur wirksamen Bekämpfung der Internet-Angriffe. Daher begrüßen wir die Internet-Sicherheitsstrategie der EU, die eine verstärkte Rolle der ENISA vorschlägt und angemessene Mittel bereitstellt, um dabei zu helfen, die digitale Gesellschaft und Wirtschaft der EU zu schützen.“*

Zur vollständigen ENISA Flash Note
Hintergrund: die **Internet-Sicherheitsstrategie** der EU
Für Interviews: Ulf Bergstrom, Sprecher, press@enisa.europa.eu, oder Handy: +30 6948 460 143, oder Dr. Louis Marinos, louis.marinos@enisa.europa.eu

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.

http://www.enisa.europa.eu/media/enisa-auf-deutsch/
www.enisa.europa.eu