Written by Marco Attard
18 April 2013

The EU cyber-security agency, ENISA, analyses the recent massive cyber-attack on Spamhaus-- and concludes ISPs still lack well-known security measures available for over 10 years.

Such an error is a key factor behind the failure to counter major attacks, the agency says in the "Can Recent Cyber Attacks Really Threaten Internet Availability?" information flash note.

The note analyses the recent attack against spam filtration firm Spamhaus , one described as "the biggest attack in history." The massive DDoS attack was over 1 week long, caused problems at the London Internet Exchange and slowed internet access in the UK, Germany and other W. European countries.

While crude in technique, DDoS attacks remain effective-- and according to ENISA many ISPs fail to comply with Best Current Practice 38 (BCP38), a recommendations list nearly 13-years old.

Meanwhile BCP140 (2008), a similar recommendations set for DNS server operators, can reduce the number of servers misused for DNS amplification attacks.

ENISA says we can learn 2 lessons from the attack. Attacks are growing in size (the Spahmaus

attack reached over 300Gbps, while the largest reported DDoS attack in 2012 reached 100Gbps), and as such can compromise even commercial internet exchange points with very high capacity infrastructure.

The Agency also makes 3 technical recommendations:

- Relevant service operators should implement BCP38
- DNS server operators should check whether their servers can be misused and implement BCP 140
- Internet exchange point operators should ensure they are protected against direct attacks

"Network Operators that have yet to implement BCP38 and BCP140 should seriously consider doing so without delay, failing which their customers, and hence their reputations, will suffer," ENISA director Professor Udo Helmbrecht concludes. "Prevention is key to effectively countering cyber-attacks. We therefore welcome the EU's Cyber Security Strategy, which is proposing a strengthened role for ENISA, with adequate resources, to help protect Europe's digital society and economy."

Go ENISA Flash Note: Can Recent Attacks Really Threaten Internet Availability?