DE-CIX Blackholing Service

12.06.2014
KG Infrastruktursicherheit

Petr Marciniak
Systems Engineer
petr.marciniak@de-cix.net
What is Blackholing?

- Blackholing effectively means diverting the flow of data to a different (Blackhole) Next-hop, where the traffic is discarded.
- The result is that no traffic is reaching the original destination and hence hosts located within the "blackholed" prefix are protected.
- Thus blackholing is an effective way of mitigating the effects of Distributed Denial of Service (DDoS) attacks, etc.
Blackholing @DE-CIX
In case of attack

- Customers advertise their prefixes with a unique DE-CIX-provided Blackhole Next-hop IP address (BN)
  - IPv4: /8 <= up to = /32 (if and only if the BN is set)
  - IPv6: /19 <= up to = /128 (if and only if the BN is set)

- Further, same security checks apply as usual (whether the advertised prefix belongs to customer’s ASN, etc.)

- L2 filtering
  - Blackhole Next-hop (BN) has a unique MAC address (determined by ARP for the BN IP address)
  - All traffic with BN’s MAC address as destination is denied ingress
Statistics

- DE-CIX Blackholing Service is available since September 2012
- Ran over 7 days in March 2014
  - More than 600 routes with Blackhole Next-Hop IP
  - From 28 customers

Statistics www.de-cix.net
Customer Feedback

• Technical challenges
  – Route filtering based on BGP Next-Hop
• Accepting more specific routes (up to /32)
• New ideas
  – IXP-wide standard Blackholing Community (Euro-IX, RFC?)
  – Dedicated route server for blackhole routes only

• We would like to hear from you!
  – discuss@lists.rtbh.me
  – https://lists.rtbh.me/cgi-bin/mailman/listinfo/discuss
Questions/Discussion

http://go.de-cix.net/blackholing/
Thank you

Join DE-CIX now!

DE-CIX Competence Center
Lindleystrasse 12
60314 Frankfurt/Germany

Phone +49 69 1730 902 - 0
info@de-cix.net

DE-CIX Competence Center @
Kontorhaus Building
Frankfurt Osthafen (Docklands)