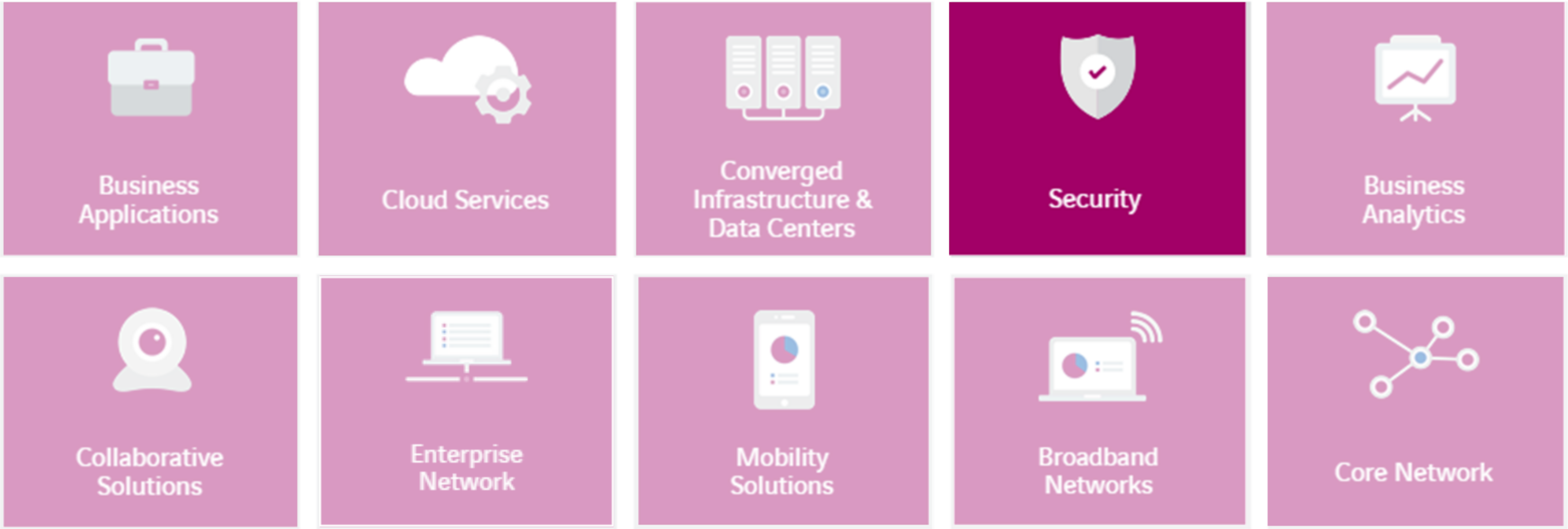
DENIAL-OF-SERVICE ATTACKS

40 years old & more present then ever

Robert Dürr, Brühl, 16./17.09.2015
Axians Networks & Solutions GmbH
email: robert.duerr@axians.de

WHO IS AXIANS?

- Axians is the new brand of VINCI Energies dedicated to ICT solutions and services
- We are present in 15 countries, have 7.000 employees and a revenue of € 1,6 billions
- Axians Germany: Axians Networks & Solutions, Crocodial IT-Security and Fritz & Macziol
- Our solution range:



- Business Applications
- Cloud Services
- Converged Infrastructure & Data Centers
- Security
- Business Analytics
- Collaborative Solutions
- Enterprise Network
- Mobility Solutions
- Broadband Networks
- Core Network

QUIZ

- How many German companies were target of an DDoS attack in past 3 years?

> 33%[*]

- Which amount do DDoS attacks currently have in cyber threat landscape?

46%[**]

[*] Survey by Alliance of Cyber-Security (www.allianz-fuer-cybersicherheit.de)

[**] Radware ERT report 2014/2015

DEFINITION

In computing, a denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

A distributed denial-of-service (DDoS) is where the attack source is more than one–and often thousands–of unique IP addresses (bot-nets).

Source: https://en.wikipedia.org/wiki/Denial-of-service_attack

Outline ➡ YOUR systems & services are not or only partial available any more!

CONSEQUENCES OF SYSTEM / SERVICE UNAVAILABILITY?

- Dissatisfied and disappointed customers / business partners
- Loss of confidence
- Reputation might be damaged
- Loss of business and money
- Existential problem

SOME FACTS RELATED TO (D)DOS ATTACKS

- DDoS is the no. 1 threat to Internet Pipes and Data Centers
- Government, Finance and Providers are the primary targets
- Amount of reflection attacks is increasing and representing highest percentage
- Size of volume-based attacks is increasing
- Most successful attacks are under 1 Gbps
- 80% of attacks have less than 50 Mbps
- Attacks are getting more complex and longer
- Layer 7 attacks use SSL, are more sophisticated and the fastest growing type
- DDoS are used to mask other attacks or data breaches
- Mobile devices, IoT, Cloud and Virtualization add further targets and challenges

Sources: Fortinet, Radware and Axians

MOTIVATION OF ATTACKERS

C.H.E.W.

Cybercrime

Hacktivism

Espionage

War (Cyber)

WHICH ATTACK TYPES ARE WE FACING?

- Network attacks
  - Flooding (UDP, ICMP, IGMP), Reflection and Amplification Attacks to saturate the „Internet Pipe“
- Server attacks
  - TCP (SYN Flood, RST, PSH+ACK) and „Low & Slow“ to misuse servers’ resources
- Application attacks
  - Flood (HTTP, DNS and SMTP), „Low & Slow“ (e.g. slow HTTP GET/POST) and SSL to misuse application behavior
- Blended / Combined Attacks

HOW TO DEFEND?

Firewall? IPS? WAF?

- Firewall, IPS and WAF
  - Cannot stop DDoS attacks!
  - Were not designed to handle today’s emerging DDoS threats
- Firewall and IPS have poor level 7 attack detection capabilities
- Especially Firewall and IPS become the bottlenecks themselves during a DDoS attack
- If integrated, Geo-Location and IP-Reputation Services have only limited efficacy

SOLUTIONS – LAYER 3/4 DDOS PROTECTION SERVICE

- Delivered as a Service by a Carrier or specialized (Cloud) Service Provider
- Detection on OSI Layer 3/4 via xFlow analysis (volume-based)
- No detection of SSL-encrypted and Layer 7!
- Time between detection and traffic diversion: typically 30 minutes and more
- Attack traffic will be manually redirected and restored
- Leaves the organization to a DDoS attack until the diversion is completed
- Complete or partial diversion of traffic to free up the Internet Pipe
- Blackholing, Sinkholing to protect against bigger damages – the attacked site is offline
- If a Scrubbing Center is part of the diversion service:
  - Distinction between „good“ and „bad“ traffic is possible
  - Layer 7 threats can be filtered if traffic is not encrypted

SOLUTIONS - ON-PREMISE

- Inline & transparent device between CPE and firewall
- DDoS mitigation response time < 20 seconds
- Analyses and blocks network traffic up to OSI Layer 7
- Adaptive ACLs/signatures
- Behavior-based detection
- Challenge suspicious sources
- Geo-location, IP-reputation and signature services
- Integrated monitoring and reporting
- Recommended additions which communicate with each other and interact automatically:
  - SSL Inspection
  - Web Application Firewall
- In case auf volume-based attacks only limited protection against Internet Pipe saturation

SOLUTIONS - HYBRID

- On-premise plus Cloud-based Scrubbing Center as an fully integrated solution
- On-premise and cloud mitigation components share information about the attack to ensure immediate and transition-free mitigation
- Automatic redirection of traffic and restore after attack
- Complete or partial diversion of traffic to free up the Internet Pipe
- Distinction between „good“ and „bad“ traffic
- Comprehensive monitoring and reporting capabilities
- Recommended additions which communicate with each other and interact automatically:
  - SSL Inspection
  - Web Application Firewall

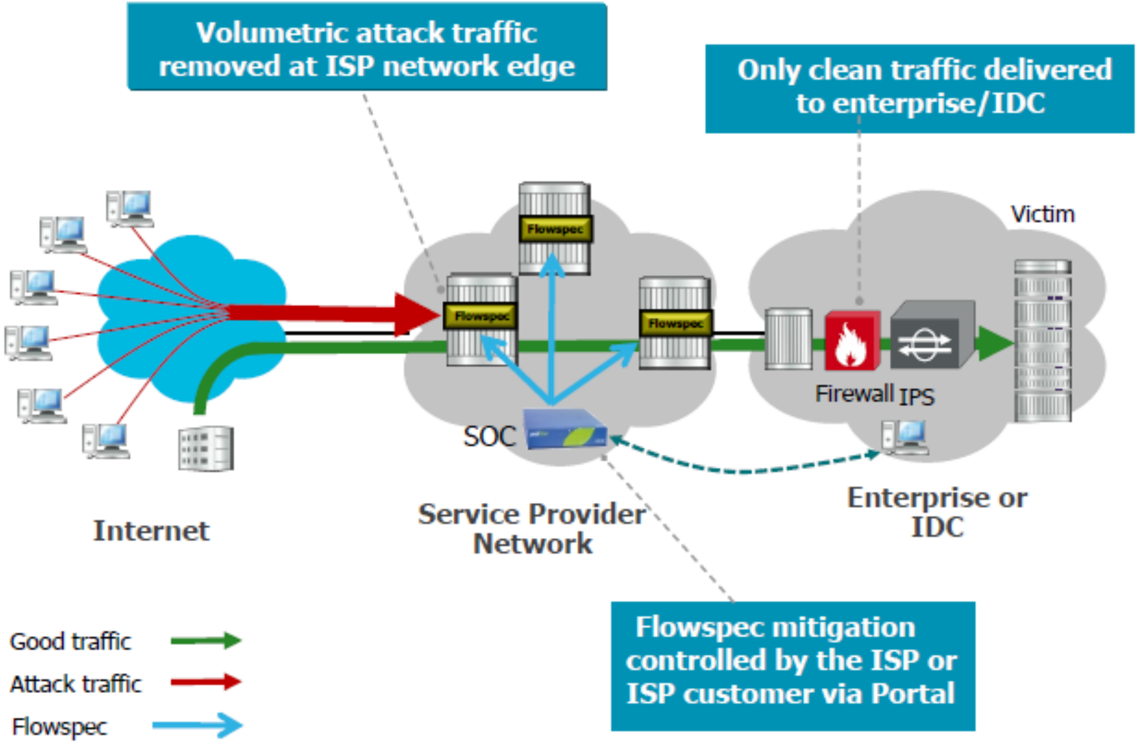
TIPS AND OUTLOOK

- Perform a Security Analysis to identify company individual attack vectors (not only for DDoS!)
- Build an Emergency Response Team (ERT) with clear responsibilities and processes
- In case of emergency ensure that you have an experienced (service) partner at your side
- If you use IaaS, SaaS or other Cloud-Services for business critical applications, assure your provider has adequate DDoS protections in place
- Be prepared for SSL-encrypted attacks
- For fast mitigation and forensics comprehensive reporting and monitoring shall be in place
- Incorporate SDN and NFV capabilities into your considerations and planning
- Mobile devices, IoT, Cloud and Virtualization add further potential for DDoS attacks
- Trend to integrated solutions: Firewall + IPS + DDoS (Inline & Cloud)

THANK YOU!

Cloud-based DDoS Defense with BGP Flowspec

Intra-domain flowspec injection



Volumetric attack traffic removed at ISP network edge

Only clean traffic delivered to enterprise/IDC

Flowspec mitigation controlled by the ISP or ISP customer via Portal