



IPv6 Intrusion Detection Forschungsprojekt Ergebnis-Workshop — 12. Juni 2013

European Advanced Networking Test Center

Carsten Rossenhövel – Managing Director

Gefördert durch:



Unternehmensprofil EANTC

- Herstellerunabhängige Qualitätssicherung in Telekommunikationsnetzen seit über 20 Jahren
- Umfangreiche internationale Testerfahrung in neuesten Technologiebereichen mit Herstellern und Netzbetreibern

Geschäftsbereiche



EANTC Berlin

- Tests und Zertifizierung von Netzkomponenten für Hersteller
- Netzdesign-Beratung und Prototype-Tests für Service Provider
- Ausschreibungsunterstützung, Vergleichs- und Abnahmetests sowie Audits für Unternehmen und Behörden
- Herstellerunabhängige **Technologieseminare**



- Gegründet 1991 als Forschungsschwerpunkt der Technischen Universität Berlin (TUB)
- 1999 Ausgründung als AG
 - Registrierte Namensaktien
 - Aktienmehrheit in den Händen des Managements
 - Nicht börsennotiert
- Forschung und Entwicklung
 - Deutsche und europäische Forschungsprojekte in Kooperationen mit Universitäten
 - Aktive Mitarbeit in Standardisierungsgremien



Testdienstleistungen für Hersteller



- EANTC bietet Konformitäts-, Leistungs- und Interoperabilitätstests für Hersteller von Netzkomponenten



- Ziel: Qualitätssicherung neuer Geräte, unabhängige Bewertung, Produktmarketing



- Positive Testergebnisse werden durch EANTC zertifiziert

Company Name	Product Name
<input checked="" type="checkbox"/>	Routing Protocols
<input checked="" type="checkbox"/>	Signalling Protocols
<input checked="" type="checkbox"/>	Traffic Engineering
Test Period: February 2012 DUT Software Version © 2012 EANTC AG	
Certified by EANTC 2012	

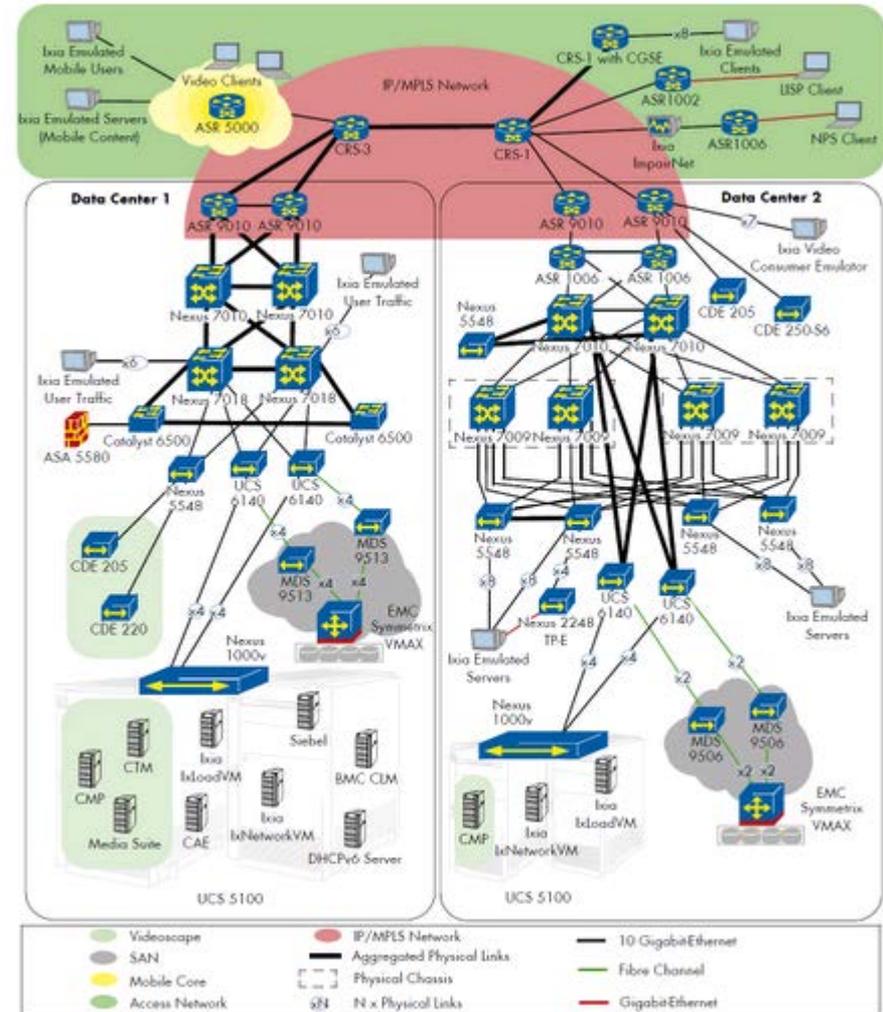
Beispiel – Cisco Cloud/DataCenter Megatest



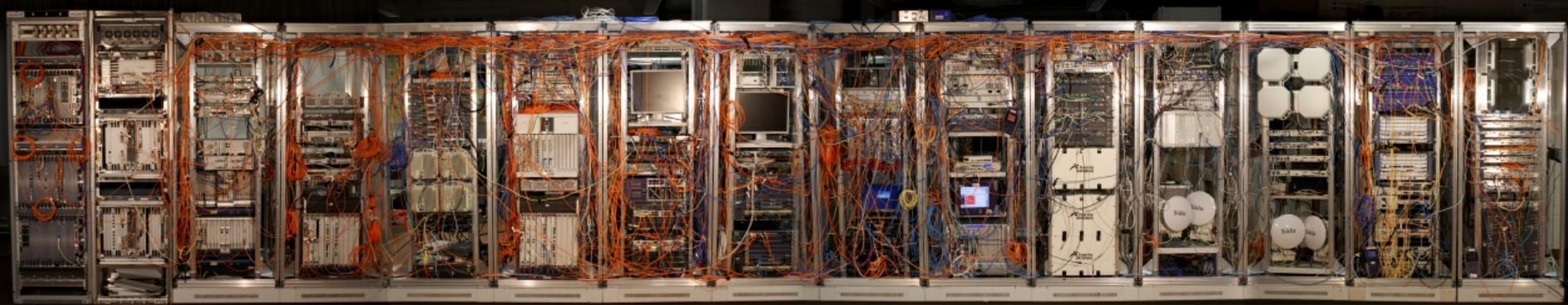
Von Light Reading beauftragt, prüfte EANTC alle Aspekte von Cloud Services mit Cisco Komponenten:

- Intelligentes Transportnetz
- Cloud Data Center Infrastruktur
- Zusammenspiel von VMware Diensten und Data Center Netz über mehrere Standorte
- Cloud-Dienste und Anwendungen

40 Seiten Report verfügbar unter <http://clientadmin.lightreading.com/ciscoseries>



Interoperabilitätstest-Events



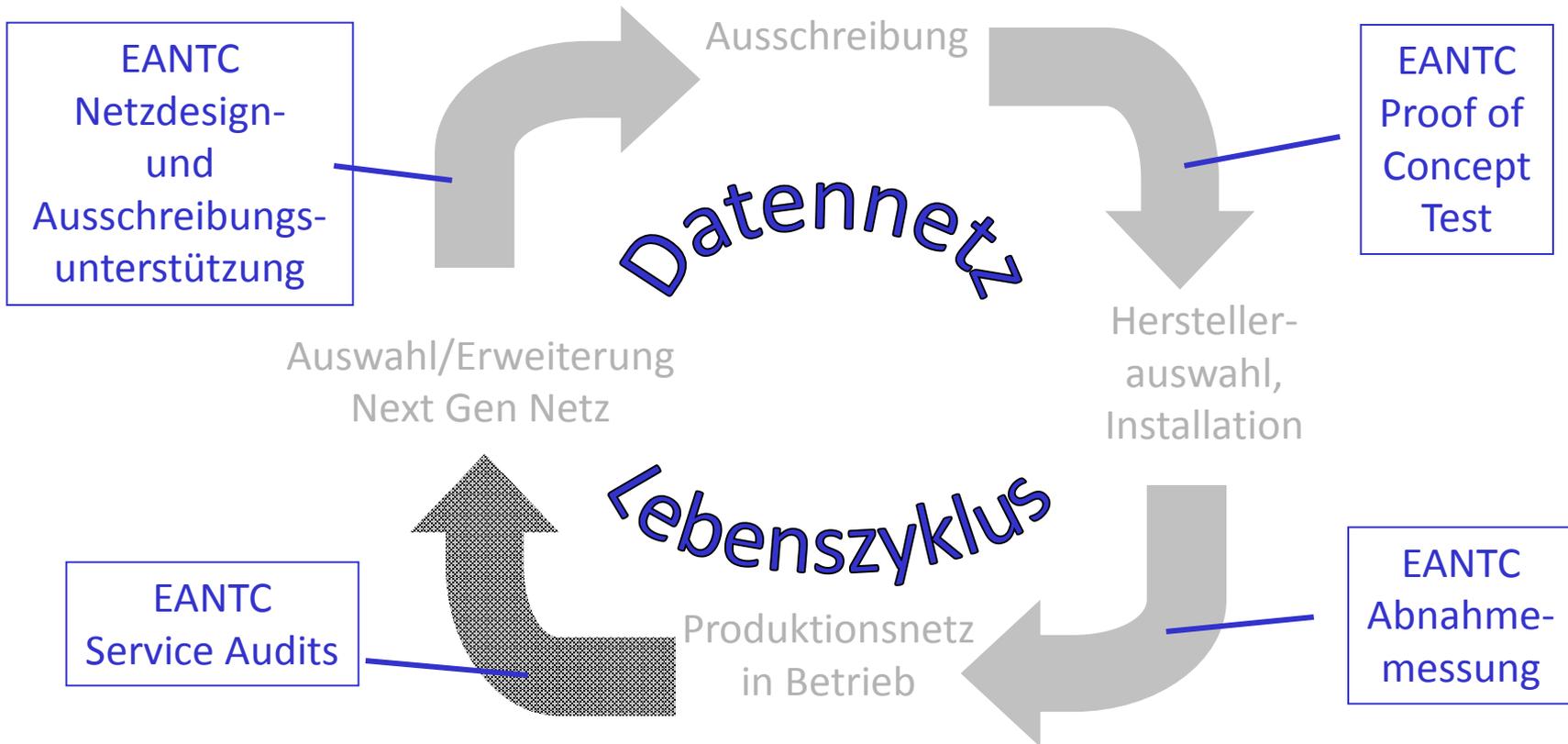
Regelmäßige Teilnehmer:

*Alcatel-Lucent, ADVA, Aviat,
Brocade, Ceragon, Ciena,
Cisco, Calnex, ECI Telecom,
Ericsson, Extreme, Hitachi,
Huawei, Ixia, Juniper,
Metaswitch, MRV, NEC, Nokia
Siemens, Orckit, RAD, Spirent,
Symmetricom, Telco Systems,
ZTE, ...*

■ EANTC lädt regelmäßig alle Hersteller zu Interoperabilitätstest-Events ein:

- Seit 2005: Carrier Ethernet World Congress
- Seit 2008: Carrier Ethernet Asia-Pacific
- Seit 2003: MPLS & Ethernet World Congress (Paris)
- Ergebnisse werden öffentlich und live präsentiert

Überblick über EANTC Testdienstleistungen



IPv6 Intrusion Detection Forschungsprojekt

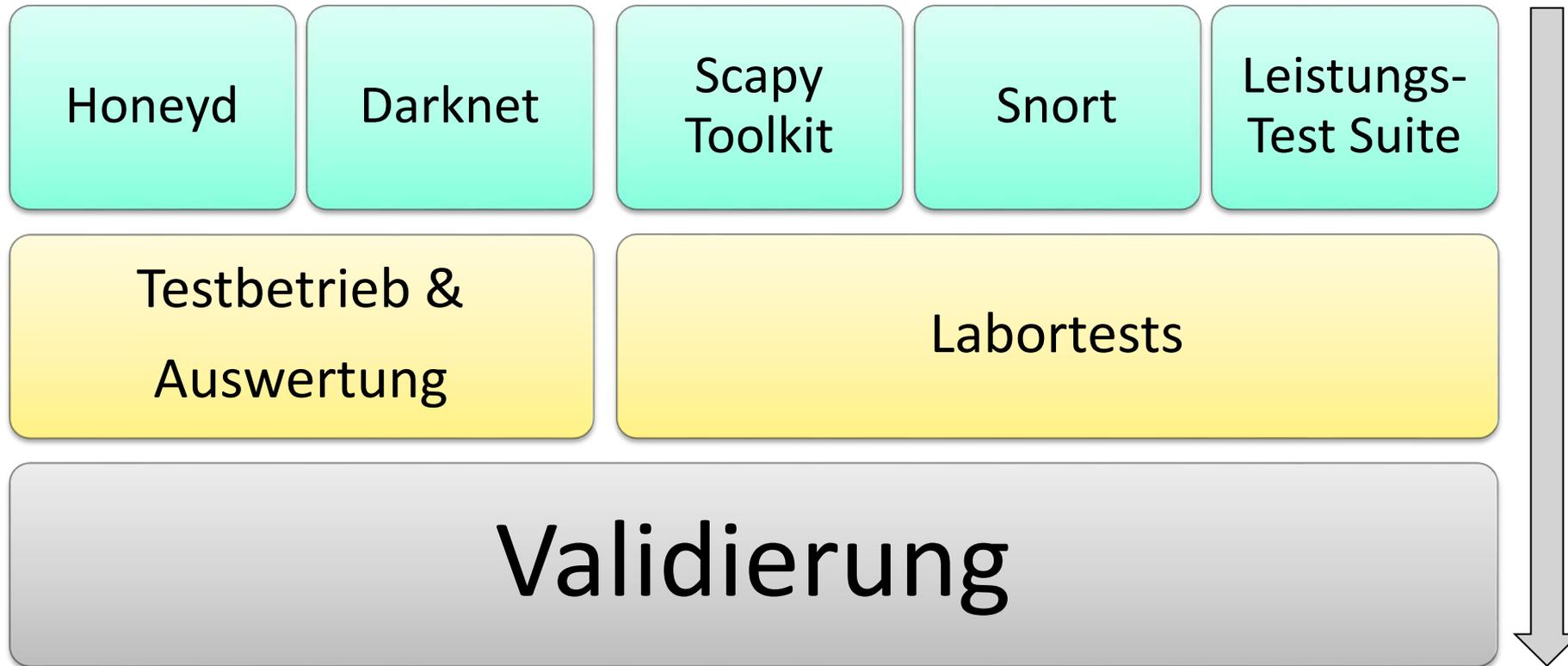


Projektrahmen

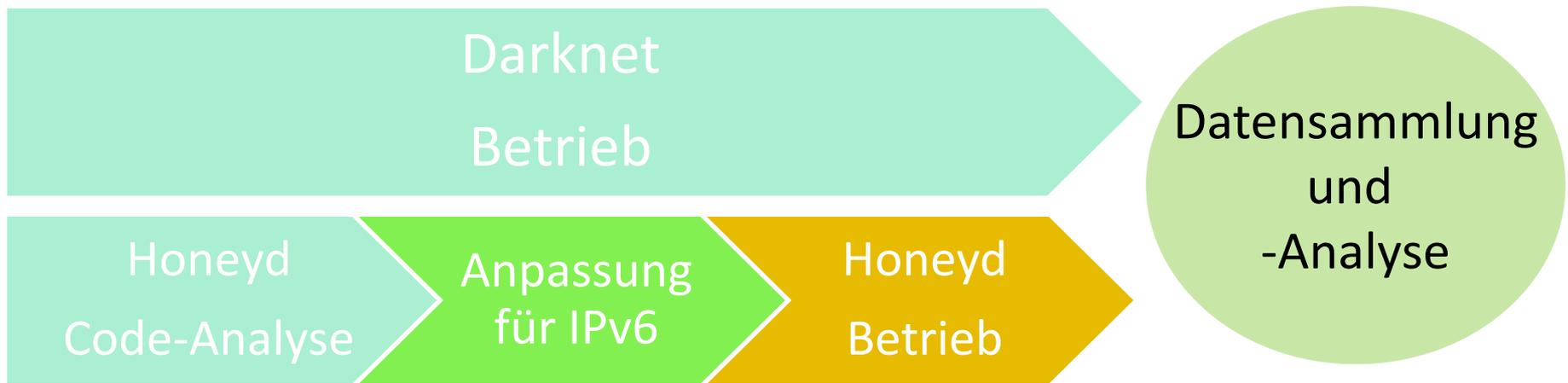
- Partner:
 - Universität Potsdam
 - Beuth-Hochschule für Technik Berlin
 - EANTC AG
- Assoziierter Partner:
 - STRATO AG
- Förderung durch Bundesministerium für Bildung und Forschung
- Projektlaufzeit 2011-2013

IPv6 Intrusion Detection Forschungsprojekt

Arbeitsplan



Untersuchung Realer Angriffe aus dem IPv6 Internet



- Vor Projektbeginn waren sehr wenige Analysen der aktuellen IPv6-Angriffslage bekannt
- Projektpartner untersuchten Angriffe passiv und aktiv

IPv6 Security Test Suite

Test Suite

- Firewall Lasttests und Protokolltests
- IDS Tests

Snort Präprozessor

- Erweiterung des Präprozessors für IPv6
- Validierung durch die Test Suite (IDS Tests)

Scapy Toolkit

- Entwicklung einer automatisierten Testlösung
- Module entsprechen der Test Suite (Firewall Protokolltests)

Quo Vadis IPv6?

- Einsatz in Europa steigt langsam und linear, mit regional großen Sprüngen
- IPv6 Sicherheit ist ein gern gesehenes Thema auf Konferenzen (12 Vorträge beim Heise Kongress Juni 2013)
- Komplexität des IPv6 Protokolls und Designfehler führen zu ungünstigen Angriffsmöglichkeiten
- Sicherheitsprobleme
+ steigende Verbreitung
= wachsendes Risiko

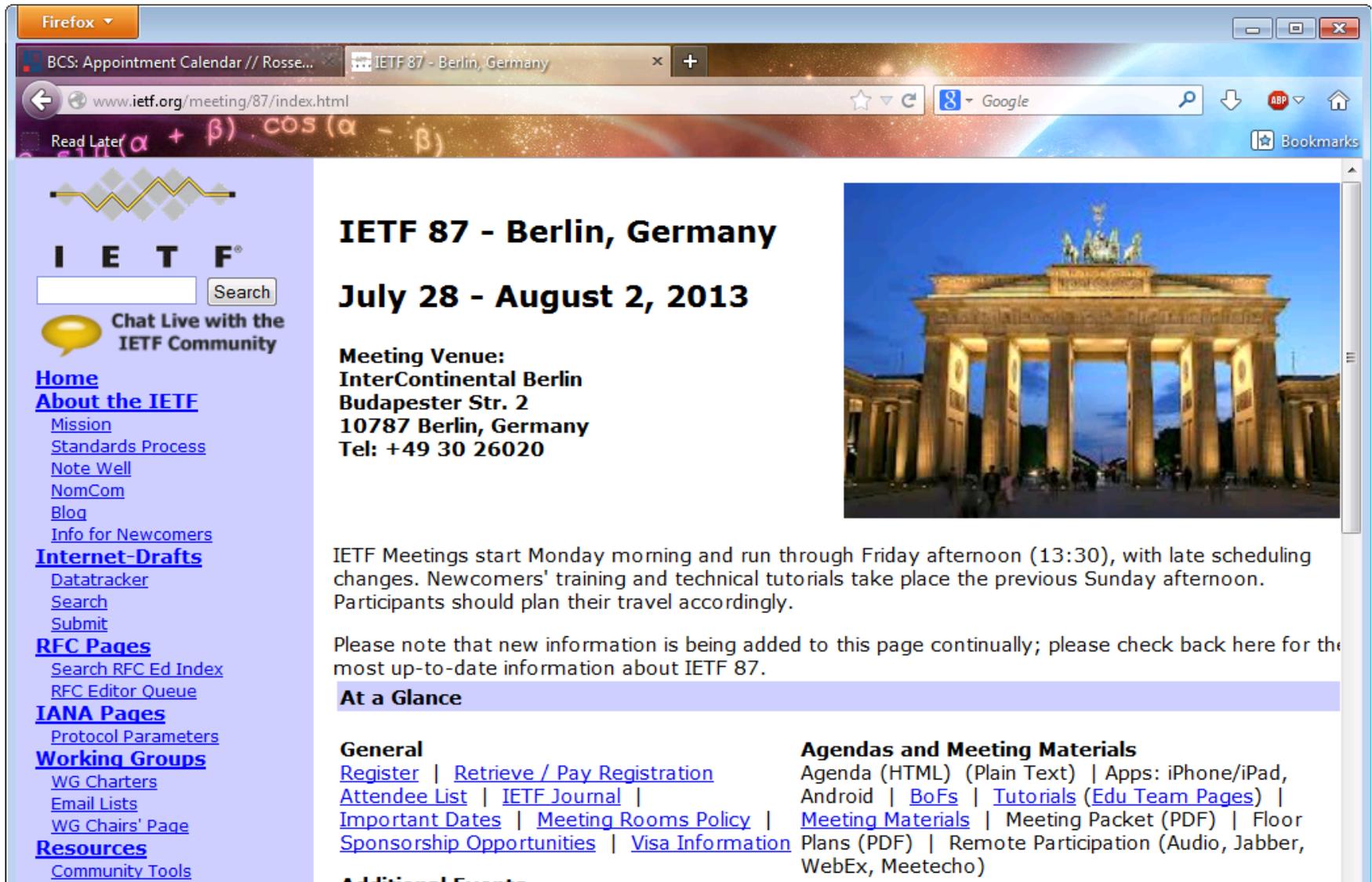
Quo Vadis IPv6? (2)

- Reale Denial of Service-Angriffsmuster zeigten sich im Projekt noch deutlich seltener/schwächer als die gefühlte Risikolage
- Schwer zu unterscheiden: Heute bestehende Risiken, zukünftige Risiken, er-/aufge-fundene Risiken der Sicherheitsindustrie ... Werden erfundene zu selbsterfüllenden Risiken?
- Hersteller, Berater, Integratoren, *Hacker* und *Gurus* haben unterschiedliche wirtschaftliche oder ideelle Interessen
- Starke Profilierung = Größerer Marktanteil

Quo Vadis IPv6? (3)

- Kein Grund, nicht vorzusorgen!
- Wer entwickelt Best Practices, die allgemein verfügbar und praxistauglich sind?
- IPv6-IDS Projekt steuerte einige Erfahrungen bei.
- Wer bringt die Standardisierung voran im Hinblick auf sichere(re) und effiziente IPv6 Implementierungen?

Nächste Schritte ...



Firefox

BCS: Appointment Calendar // Rosse... IETF 87 - Berlin, Germany

www.ietf.org/meeting/87/index.html

Read Later $(\alpha + \beta) \cdot \cos(\alpha - \beta)$

Google

Bookmarks

IETF 87 - Berlin, Germany

July 28 - August 2, 2013

Meeting Venue:
InterContinental Berlin
Budapester Str. 2
10787 Berlin, Germany
Tel: +49 30 26020



IETF Meetings start Monday morning and run through Friday afternoon (13:30), with late scheduling changes. Newcomers' training and technical tutorials take place the previous Sunday afternoon. Participants should plan their travel accordingly.

Please note that new information is being added to this page continually; please check back here for the most up-to-date information about IETF 87.

At a Glance

General Register Retrieve / Pay Registration Attendee List IETF Journal Important Dates Meeting Rooms Policy Sponsorship Opportunities Visa Information	Agendas and Meeting Materials Agenda (HTML) Plain Text Apps: iPhone/iPad, Android BoFs Tutorials (Edu Team Pages) Meeting Materials Meeting Packet (PDF) Floor Plans (PDF) Remote Participation (Audio, Jabber, WebEx, Meetecho)
--	--

Resources
[Community Tools](#)

Working Groups
[WG Charters](#)
[Email Lists](#)
[WG Chairs' Page](#)

IANA Pages
[Protocol Parameters](#)

Internet-Drafts
[Datatracker](#)
[Search](#)
[Submit](#)

RFC Pages
[Search RFC Ed Index](#)
[RFC Editor Queue](#)

Note Well
[NomCom](#)
[Blog](#)
[Info for Newcomers](#)

About the IETF
[Mission](#)
[Standards Process](#)

Home
[Chat Live with the IETF Community](#)