Die Sicht von Außen

Otmar Lendl
<lendl@cert.at>

Intro

- Otmar Lendl
  - Seit 1991 als Sysadmin im Internet tätig
  - Ehemals sbg.ac.at/Ping/EUnet/KQ/EUnet2/Tiscali…
  - Seit 2002 bei nic.at (R&D)
  - Seit 2008 Teamleader CERT.at
- Inhalt:
  - CERT.at?
  - Bedrohungen
  - Empfehlungen

CERT.at ?

- Nationales Computer Emergency Response Team
  - nic.at in Kooperation mit dem Bundeskanzleramt
  - Seit 2008
  - Keine Behörde
- Aufgaben:
  - Datendrehscheibe
  - Warnungen
  - Hilfe bei Notfällen
- Technischer Teil des GovCERT

Konnex zu ISPs

- Tägliche Arbeit:
  - Telemetrie zu infizierten PCs an die richtigen Abuse-Teams weitergeben
  - Defacement Meldungen
  - Phishings
- Ab und zu:
  - Denial of Service
  - Andere bösere Sachen

Einschränkung

- Wir kümmern uns um Sicherheit im Internet
- Nicht PSTN
- Nicht Layer 0-2 Networks
  - WDM
  - MPLS
  - …
- Nicht basic Network / Service – Design
  - Nebenbemerkung: Resilience ist nicht gratis
- Fokus ist hier der Internet Service Provider

Bedrohungen

- ISPs sind Firmen wie alle anderen auch
  - Interne Sicherheit
- ISPs betreiben Webseiten
  - Klassische Websecurity
- Das Netz selber
  - Plus dessen Lieferanten
- Kunden!
  - Housing, Hosting, Infizierte Endkunden

Empfehlungen

- Ich weiß nicht, was wer schon macht
- Nicht alles ist für jeden hier sinnvoll

- Das sind unsere Erfahrungswerte

- Siehe auch „The Service Provider Tool Kit" von Barry Greene
  http://www.nanog.org/meetings/nanog54/abstracts.php

Vernetzen

“Never underestimate the power of human communications as a tool to solve security problems. Our history demonstrates that since the Morris Worm, peer communication has been *the* most effect security tool.”

Barry Raveendran Greene

Kein Produkt kann ein kompetentes NOC – Team ersetzen.

Internationale Foren

- RIPE
- NANOG
- ISACs (mehr die Carrier-Schiene)
- Diverse Mailinglisten
  - nsp-sec
  - ops-t
  - routesec, nxdomains, mwp, yasml, ii, …
- iNOC-DBA
- SANS / ISC / DSHIELD

National

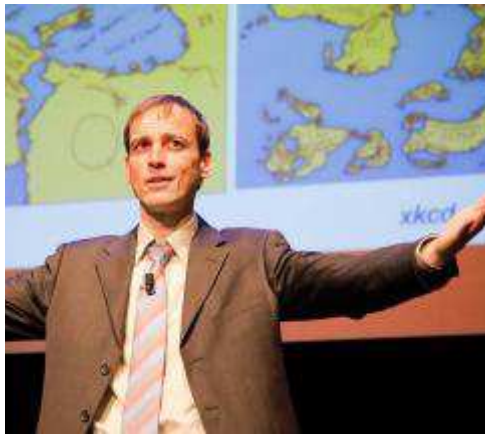
- Viele Länder haben mehr oder weniger informelle Netzwerk-Security Foren
  - ISP Security Forum Denmark
  - DENOG (Deutschland)
  - SwiNOG (Schweiz)
  - …
- In Österreich
  - „Man kennt sich“
  - Ad hoc bei diversen sozialen Anlässen
  - CERT Security Stammtisch ist zu breit
- Daher …

Austrian Trust Circles

- „Selbsthilfe“ in den Sektoren im Bereich Sicherheit
- Vertrauen schaffen, wenn Zeit ist
- Operative Kontakte für CERT.at
  - Information über Sicherheitsvorfälle und Themen
  - Behandlung von Sicherheitsvorfällen
- Operative Experten für Behörden im Krisenfall
- Vernetzung und Informationsaustausch
  - in den Sektoren
  - zwischen den Sektoren

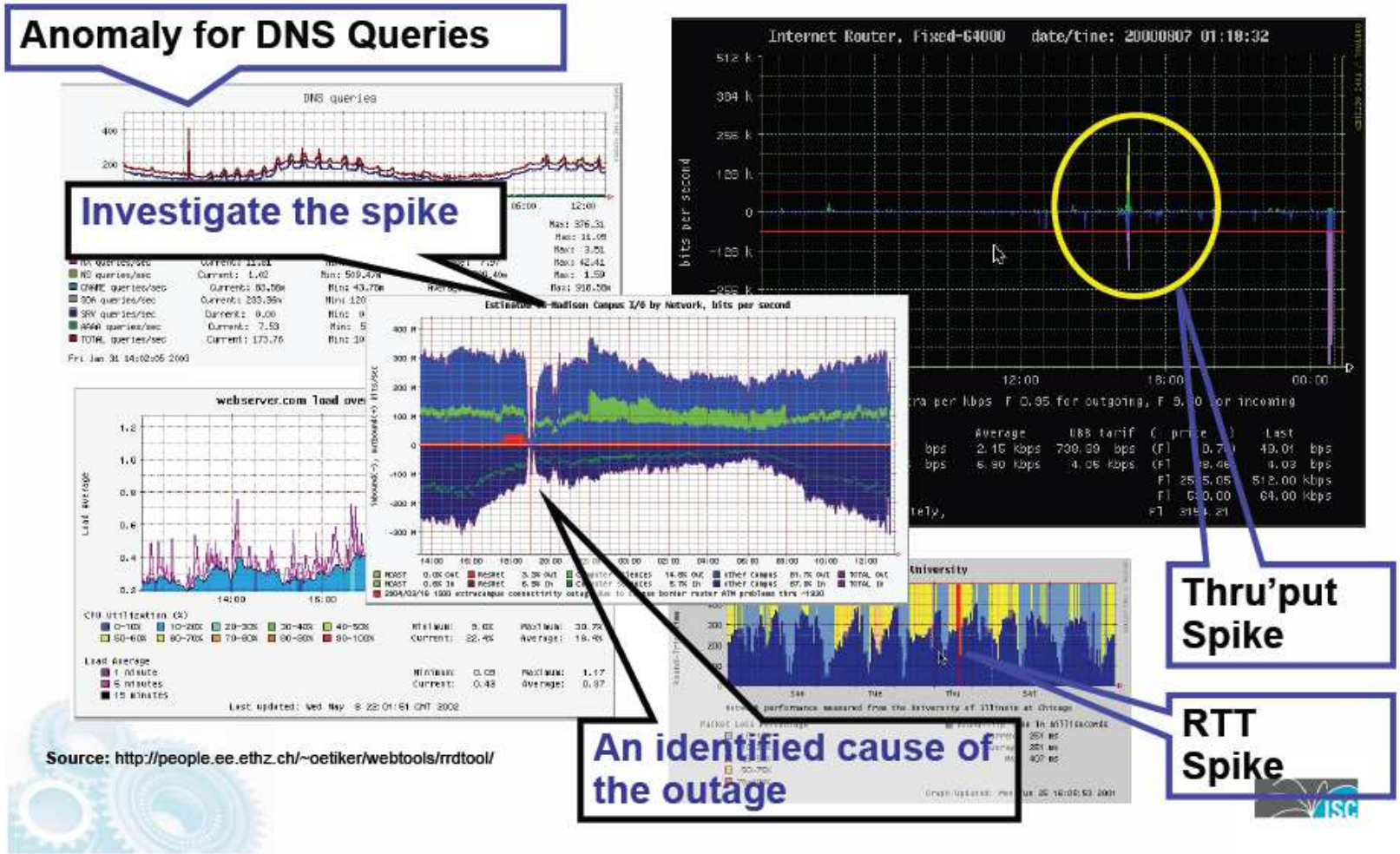
2. Austrian Trust Circle Treffen

7. und 8. Mai - Waidhofen an der Ybbs



- Podiumsdiskussion zum Thema „Vertrauen, Selbsthilfe, Hilfe“
  - BMI / BVT Mag. Gridling
  - BMLVS Oberst Unger
  - Bundeskanzleramt Ing. Ledinger
  - CERT.at Mag. Schischka
- Vortrag „Bedrohungen aus Sicht eines Herstellers Industrieller Steuerungssysteme
  - Dipl. Ing (FH) Thomas Brandstetter, Leiter Siemens ProductCERT, MSc.
- Sektorspezifische Workshops
- Sektorübergreifender Workshop
  - TableTop Notfallsübung
- KeyNote „Cybercrime: a new approach“
  - Peter Zinn, Senior Cybercrime Advisor for the Dutch National High Tech Crime Unit
  - Keynote ist gemeinsam mit LSZ Security & Risk Management Kongress

Instrumentierung



Tools

- Netflow
  - Nfsen, Arbor peakflow, ..
- SNMP / RRDtool
  - mrtg, Cacti, ….
- RMON
- Rancid

- Jede Menge kommerzielle NMS

Externe Datenquellen

- Vulnerability feeds (Cisco, Juniper, HP, …)
- RIPE RIS & co: BGP Anomalitäten
- Probleme bei Kunden
  - Spam Feedback loops
    - Hotmail, gmail, …
  - Team Cymru, Shadowserver
  - Diverse RBLs, IP reputation services
  - … und die CERT.at Meldungen

Network Security

- Control Plane Protection / Infrastructure ACL
- BCP 38 (Anti-Spoofing auf Kundeninterfaces)
- Routing zum Kunden
  - Kein IGP, BGP auf Prefix-basis filtern
- BGP Filter bei Peerings
- Realtime Blackholing für DDOS mitigation
- Walled Garden für Zombies
- CPE Security: Updates!

Tools + Brains

- Produkte alleine reichen nicht
- Aber: Techniker brauchen Tools

- Automate. Automate. Automate.

- Wissen weitergeben.
  - Wir spielen gerne Beichtstuhl

Fragen?

- Wünsche an das CERT?
- Wer macht bei den ATC mit?

- http://www.cert.at/
- Otmar Lendl <lendl@cert.at>