

Key Player rund um Domains

Datum:
03.05.2011

Alexander Mayrhofer
Teamleiter Forschung & Entwicklung

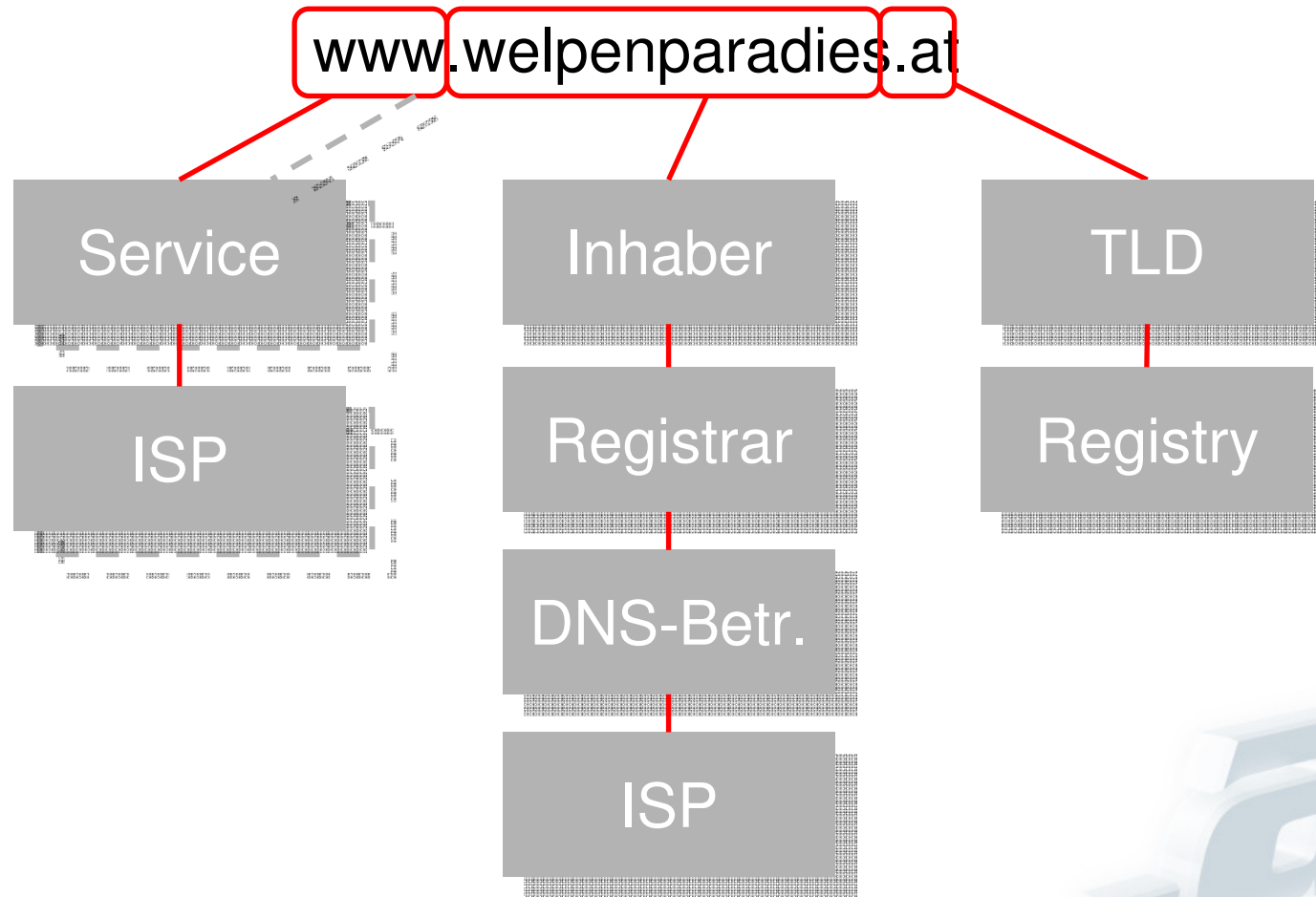


Agenda

- Überblick – die Player
- Zu jedem Player:
 - Welche Aufgaben nimmt er wahr?
 - Wie sind seine Eingriffsmöglichkeiten?
 - Wie identifiziere ich ihn?
- Fragen?



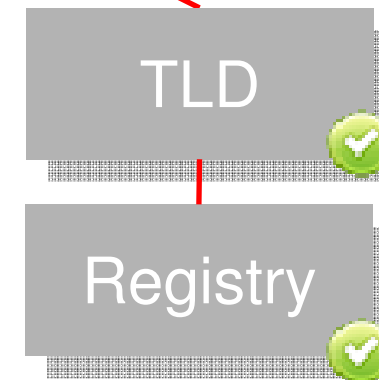
Die Player



Top Level Domain (TLD)

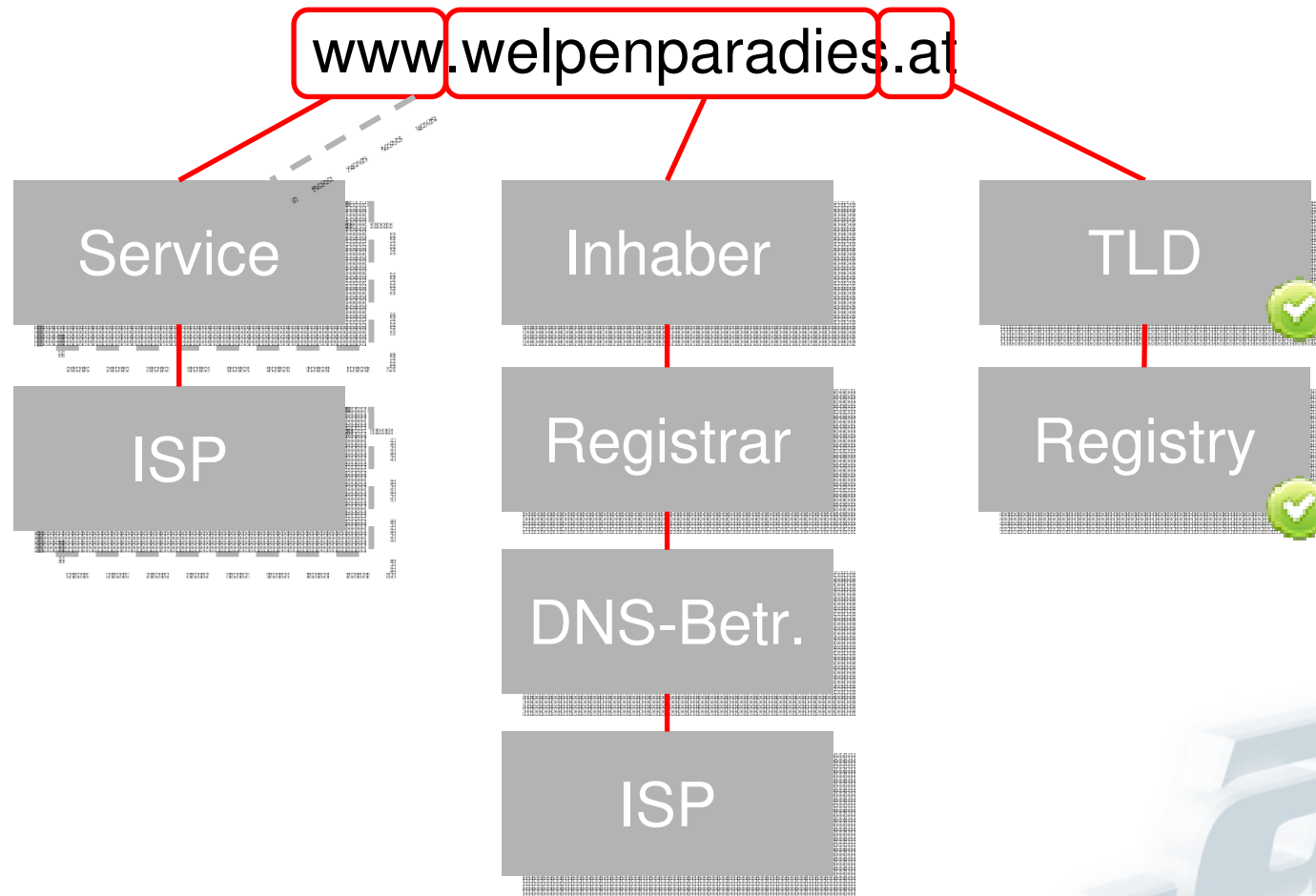
www.welpenparadies.at

- Der „letzte Teil“ der Domain
- ccTLD – zweistellig (.at, .de, .ch, ..)
- gTLDs / sTLDs – alle anderen
- Werden von „Registries“ betrieben
- Registry für TLD finden:
<http://www.iana.org/domains/root/db/>
- nic.at ist die Registry für „.at“



.at

TLD & Registry gefunden



Registries

- Datenquellen:
 - Inhaberdaten+Nameserver-Verweise: z.B. <http://who.is/> (oder eigene WHOIS-Abfrage der Registry)
- Eingriffsmöglichkeiten
 - Technisches Sperren der Domain – allerdings nur komplett (alle Dienste, alle Sub-Domains)



WHOIS-Ergebnis

domain: welpenparadies.at
registrant: BG7802608-NICAT
admin-c: BG7802609-NICAT
tech-c: UD7802610-NICAT
nserver: bluemoon.webma.net
nserver: redsun.webma.net
changed: 20110110 16:28:17
source: AT-DOM

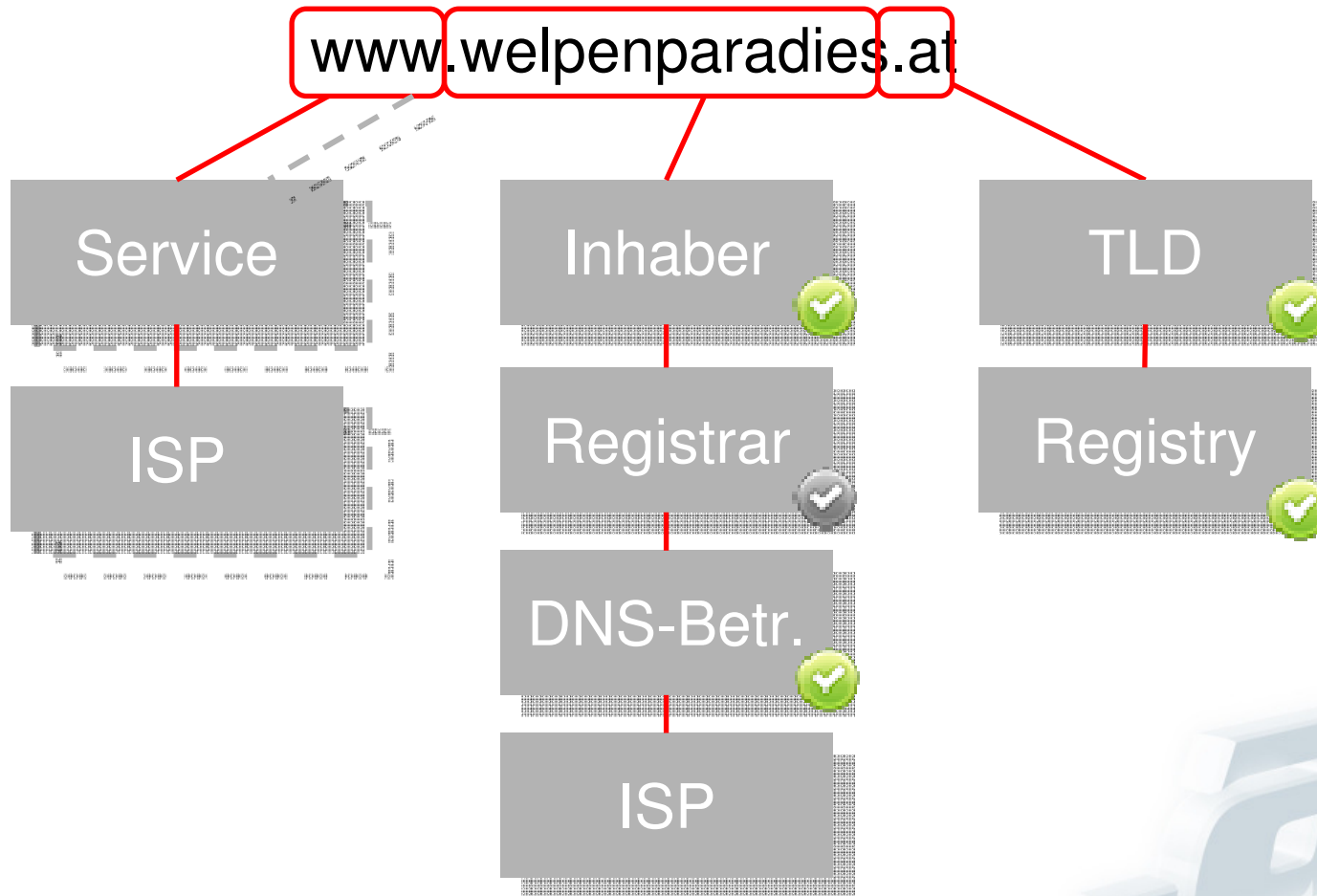
personname: Bauchinger GEORG
organization:
street address: Hauping 7
postal code: A-4912
city: RIED I. I.
country: Austria
nic-hdl: BG7802608-NICAT
changed: 20110110 16:28:13
source: AT-DOM

- Nameserver
 - Schlüssel zum ISP des Nameserver-Betreibers
- Inhaber



WHOIS-Abfrage durchgeführt

www.welpenparadieses.at



ISP der Nameserver finden

- Ausgangsdaten: Nameserver-Namen
 - Bluemoon.webma.net
 - Redsun.webma.net
- IP-Adressen herausfinden:
 - (z.b. auf <http://ip-lookup.net/domain-lookup.php> unter „Domain Lookup“ eingeben)
 - [213.208.135.100](#)
 - [213.208.132.20](#)
- Provider zu den IP-Adressen finden:
 - Z.b. auf obiger Website auf die IP-Adresse klicken, und dann “IP owner info” anklicken (WHOIS)

Ergebnis IP-Adress-Abfrage

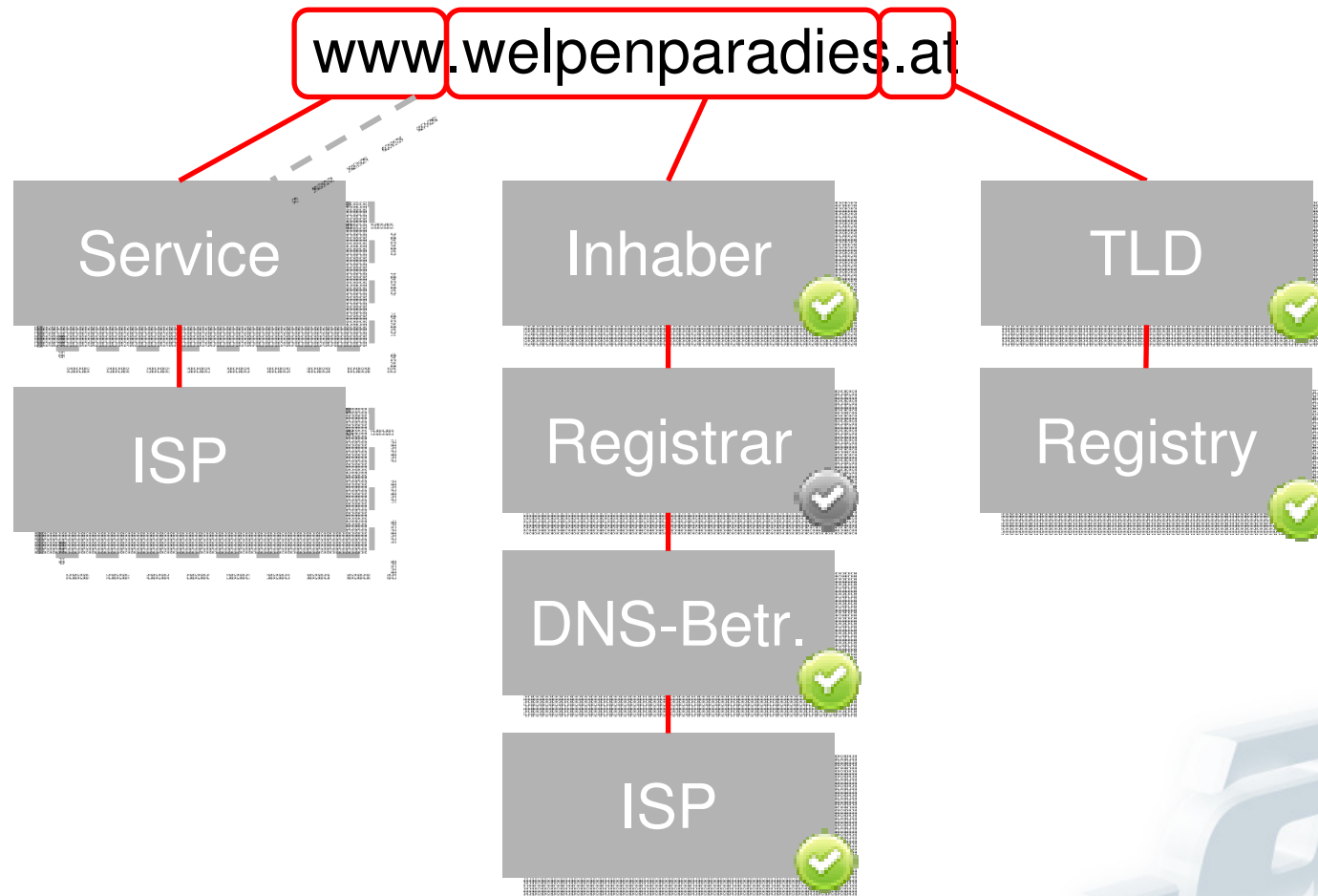
inetnum: [213.208.132.0](#) - [213.208.132.255](#)
netname: WEBMACHINE-NET-2
descr: WebMachine Unixsecurity Network 2 VIE-IX
country: AT
org: ORG-UI7-RIPE
admin-c: FS3177-RIPE
tech-c: uN256-RIPE
status: ASSIGNED PA
mnt-by: AS1764-MNT
source: RIPE # Filtered

organisation: ORG-UI7-RIPE
org-name: Unixsecurity Internetdienstleistungsgmbh
org-type: OTHER
address: Rotensterngasse 20/3
address: A-1020 Wien, Austria / Europe
mnt-ref: NEXTLAYER-MNT
mnt-by: NEXTLAYER-MNT
source: RIPE # Filtered

- ISP der Nameserver



DNS-Betreiber identifiziert



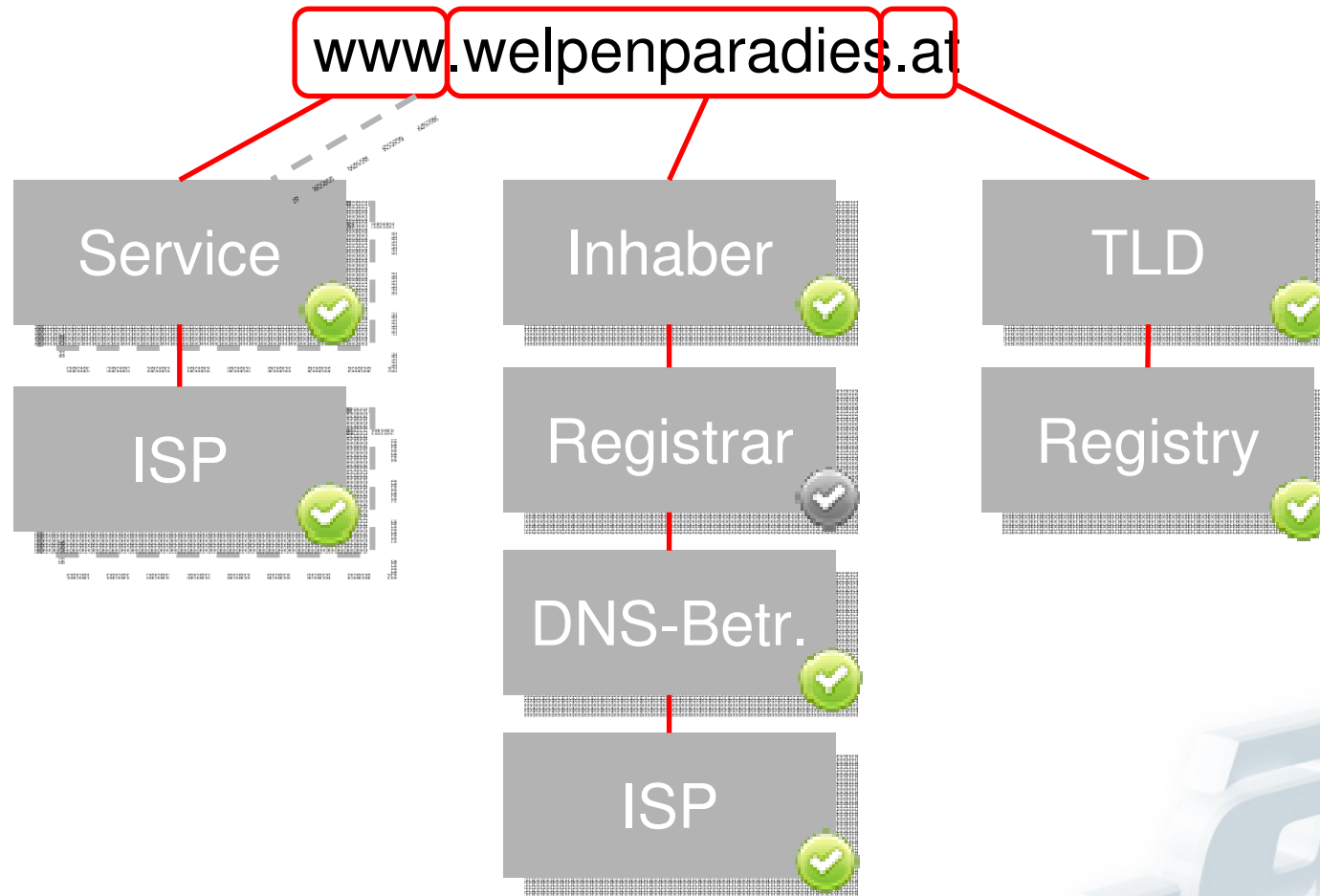
Aufgabe DNS-Betreiber



ISP eines Dienstes finden

- Ausgangsdaten: „erraten“ Services
 - www.welpenparadies.at
 - (Mailserver für welpenparadies.at)
- IP-Adressen herausfinden:
 - (z.b. auf <http://ip-lookup.net/domain-lookup.php> unter „Domain Lookup“ eingeben)
 - www.welpenparadies.at -> 213.208.132.55
- Provider zu den IP-Adressen finden:
 - Z.b. auf obiger Website auf die IP-Adresse klicken, und dann “IP owner info” anklicken (WHOIS)

Alle Player identifiziert*

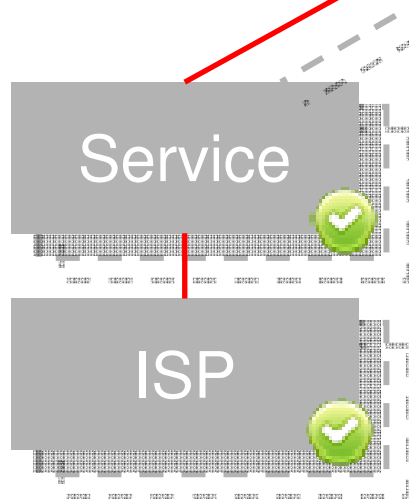


*Small print: Es kann leider noch viel komplizierter sein..



Aufgabe Service-Betreiber

www.welpenparadies.at



- Betreibt den entsprechenden Service
 - (Webserver/email/Chat/...)
- Hat vollen Zugriff auf alle Daten und Server
- Kann sehr granular in die Dienste eingreifen
 - Einzelne Webseiten der Site ändern/löschen
 - Einzelne email-Adressen blockieren
 - Zugang beschränken

Danke für die Aufmerksamkeit!



alexander.mayrhofer@nic.at

