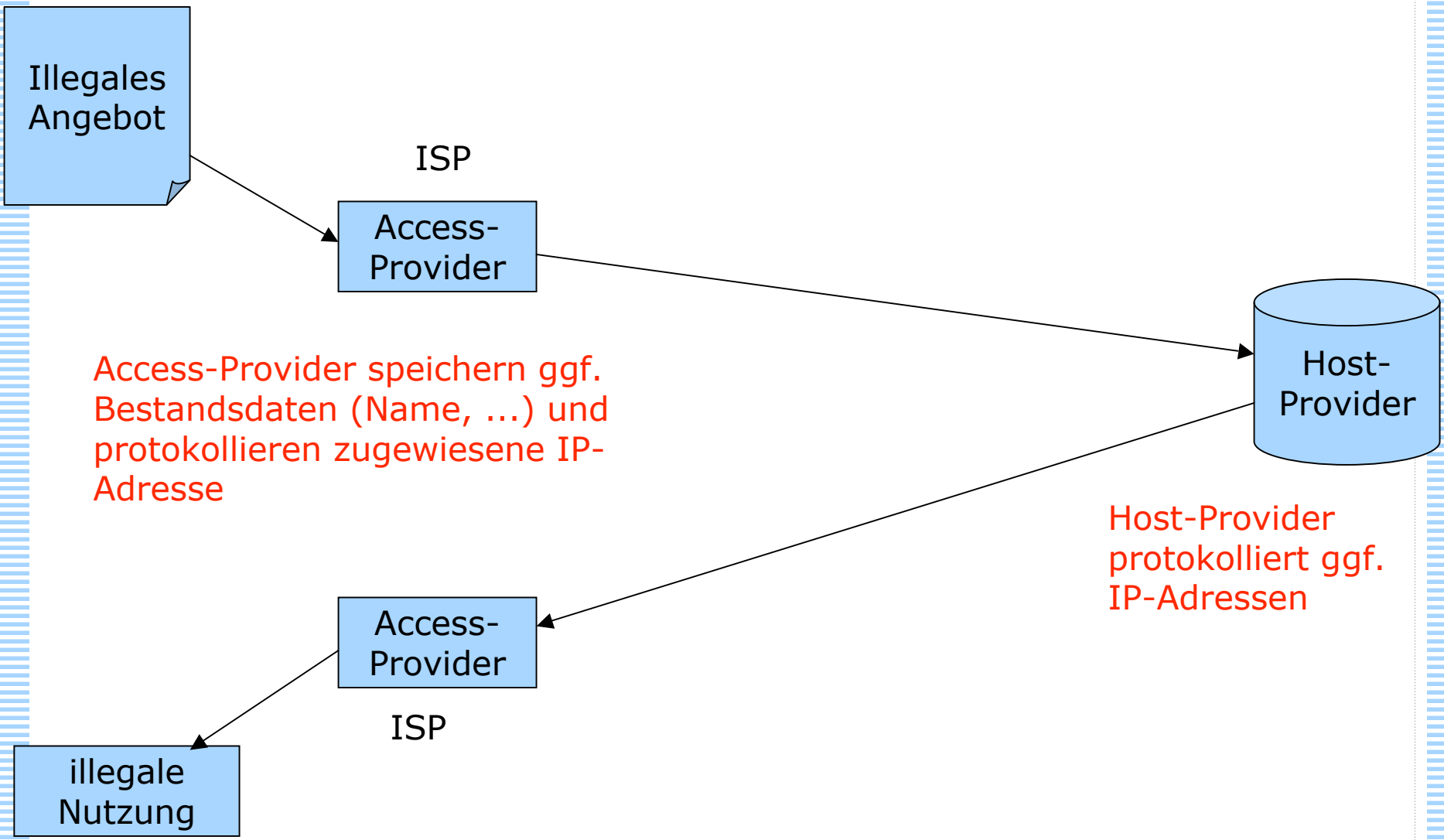
Technische Grundlagen von Auskunftsansprüchen

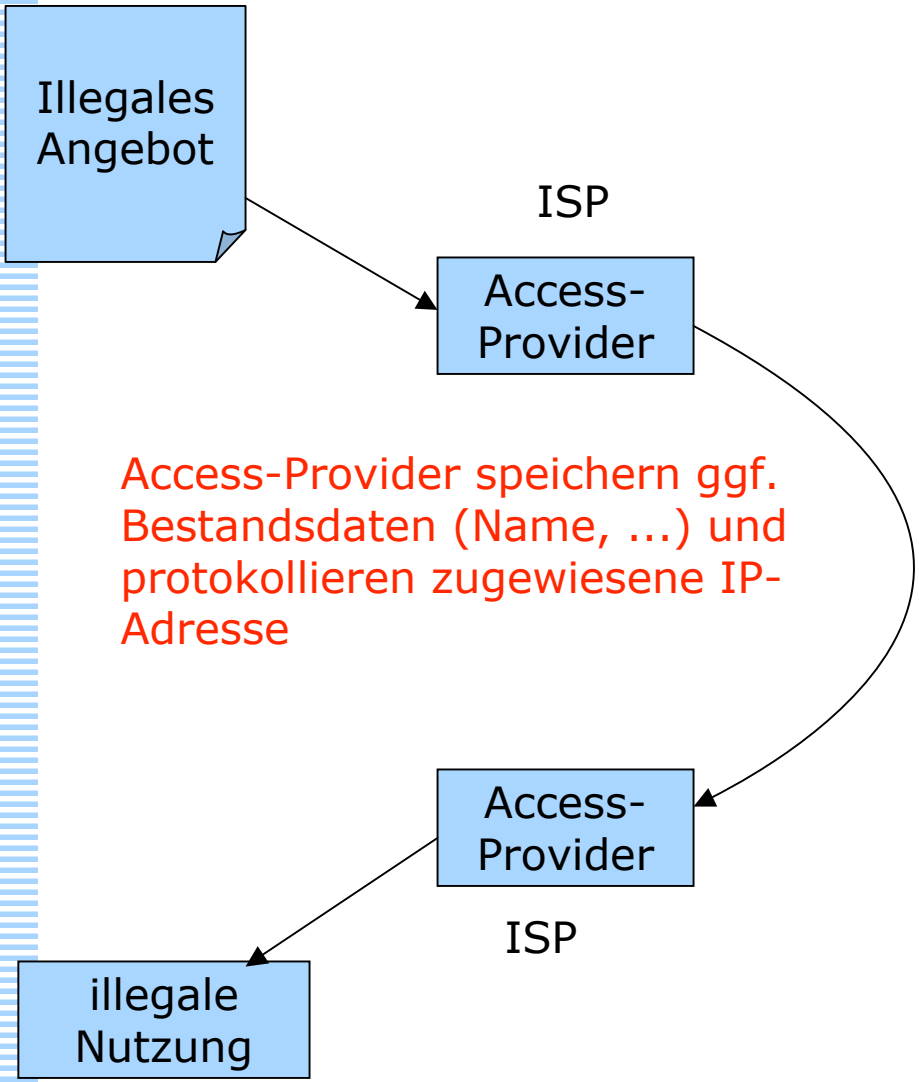
Prof. Dr. Hannes Federrath
Lehrstuhl Management der Informationssicherheit
Universität Regensburg

http://www-sec.uni-regensburg.de/

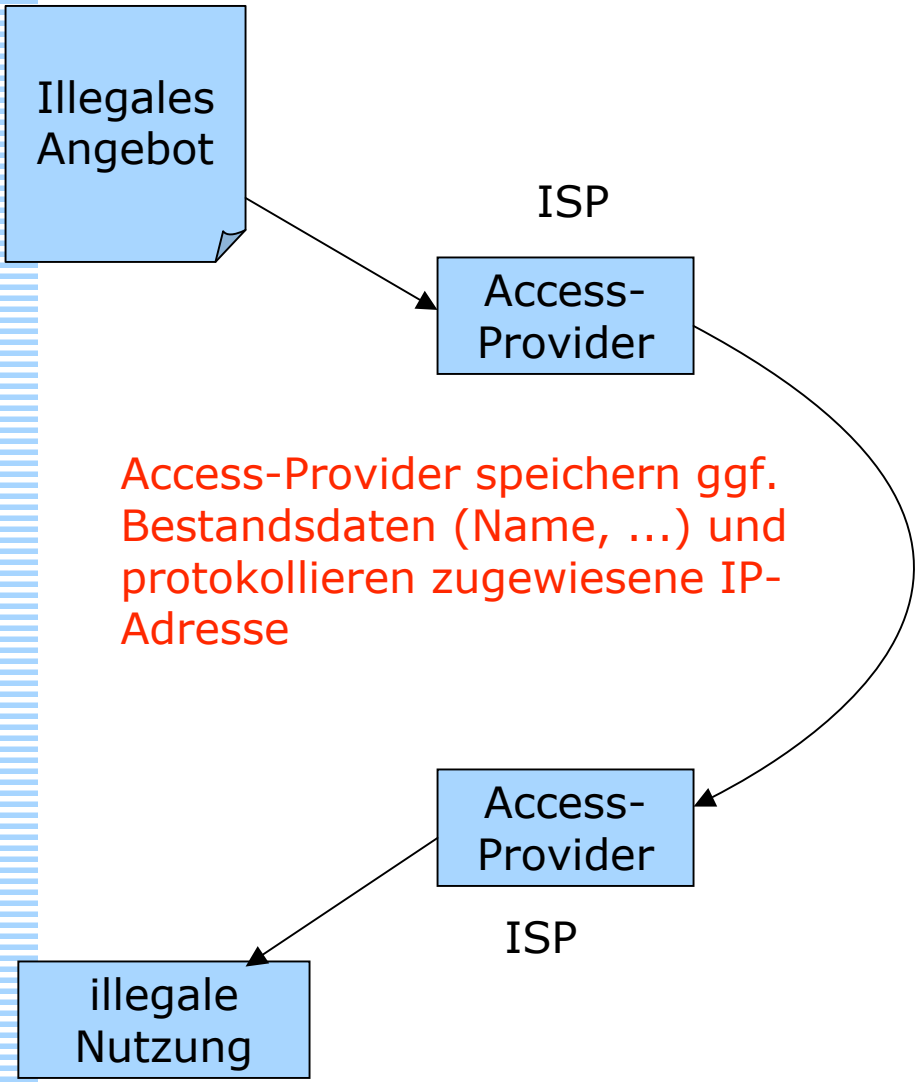
Zentraler Fileserver zum illegalen Austausch



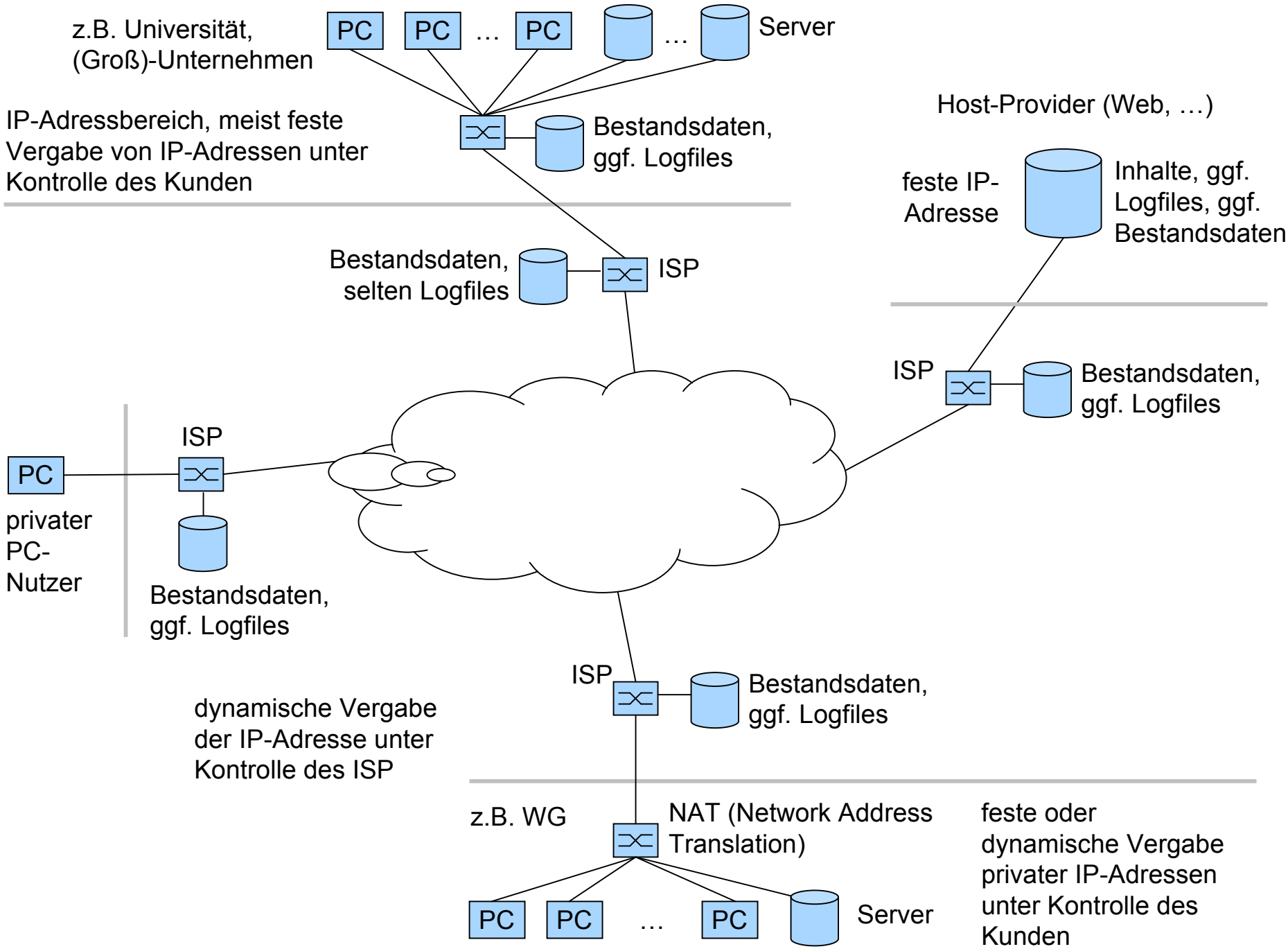
Peer-to-Peer-Abruf von illegalen Inhalten



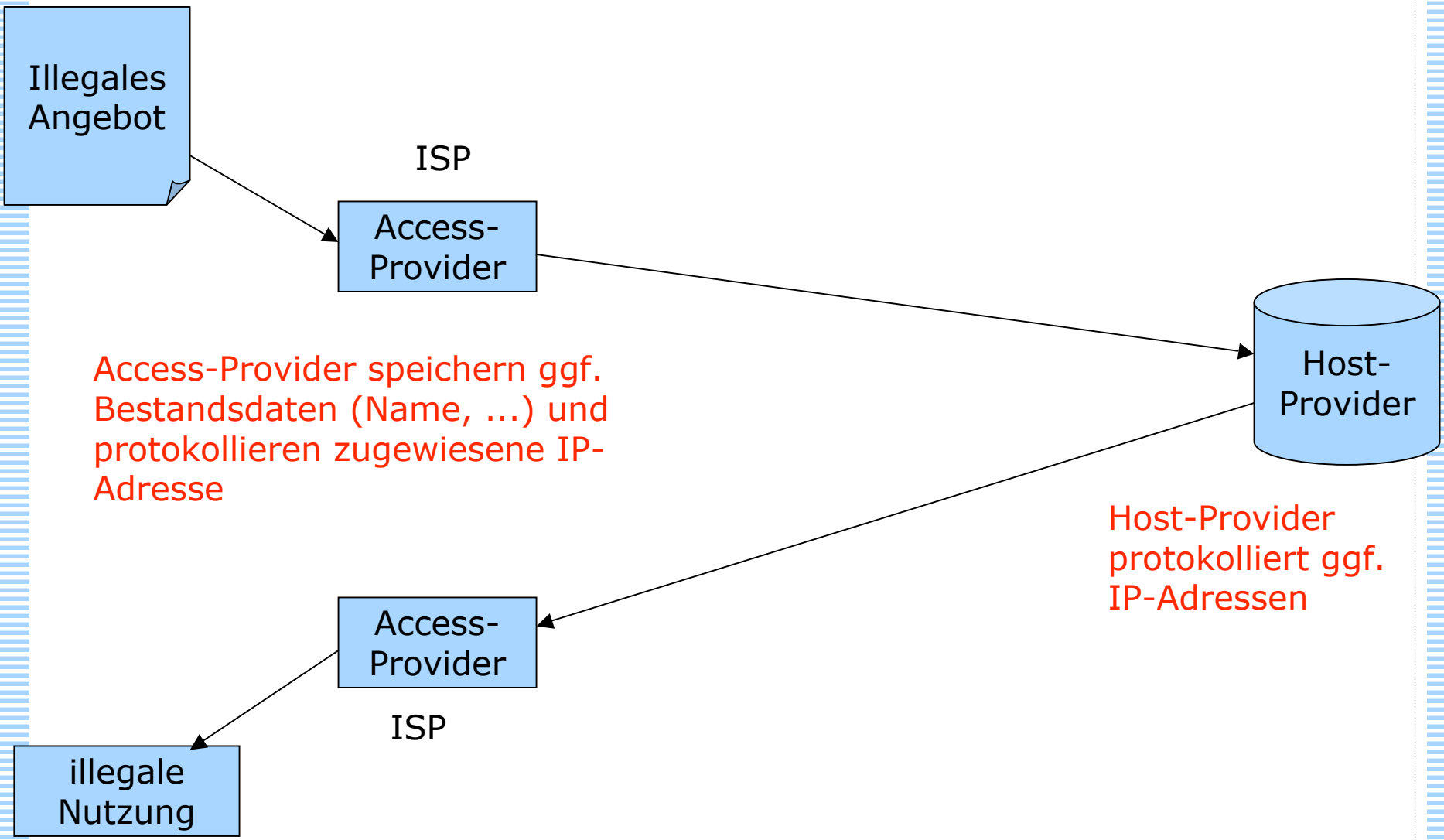
Peer-to-Peer-Abruf von illegalen Inhalten



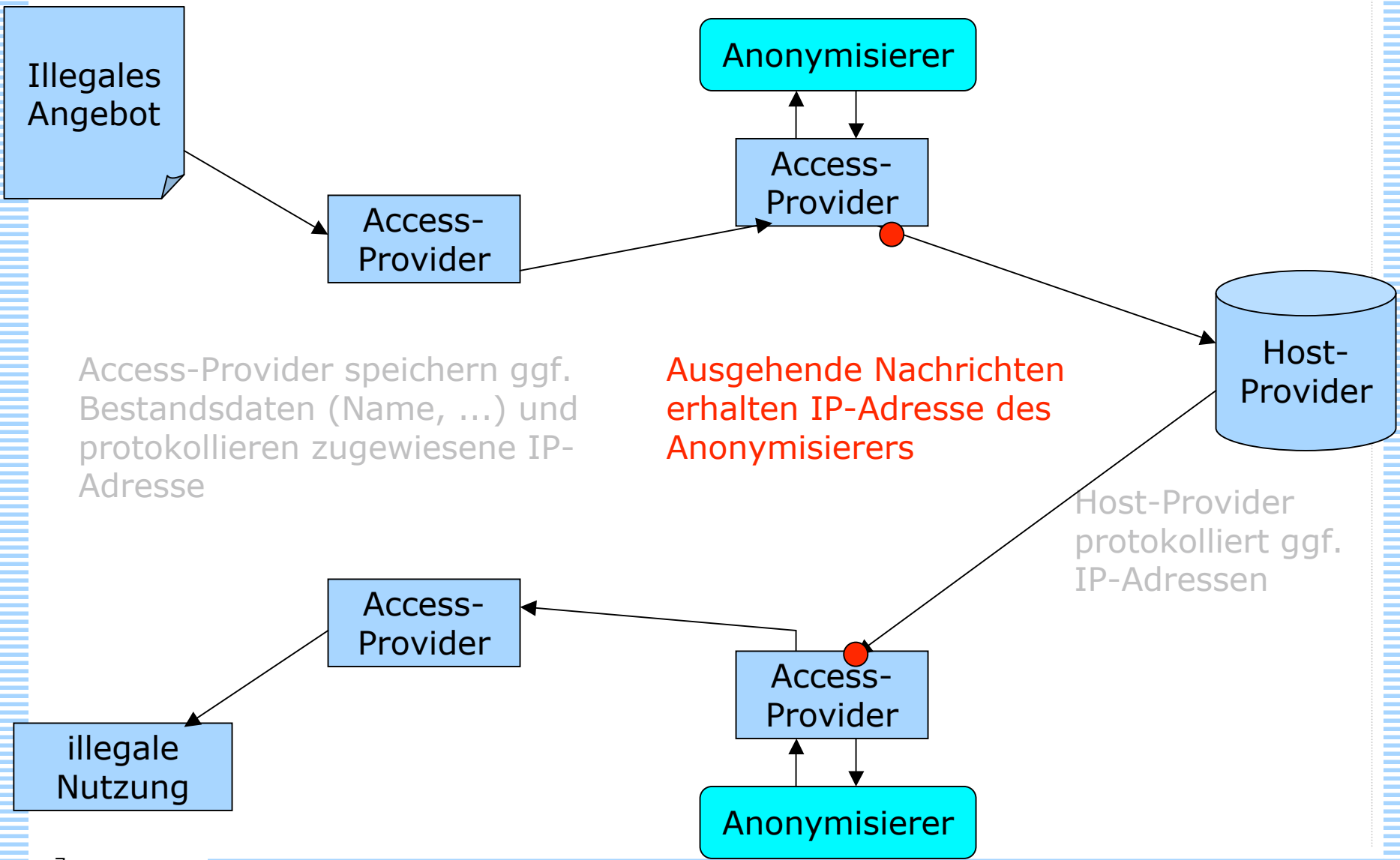
- ISP speichert meist vergebene IP-Adresse in Logfile
- dient meist der "Aufrechterhaltung des Dienstes"
- bei Auskunftsersuchen Abfrage der Logdaten und Zuordnung zu Bestandsdaten (Name, Adresse)
- typische Speicherdauer der Logeinträge – wenn überhaupt vorhanden – schwankt zwischen einigen Stunden und unendlich


z.B. Universität,
(Groß)-Unternehmen
PC
PC
…
PC
…
Server
IP-Adressbereich, meist feste
Vergabe von IP-Adressen unter
Kontrolle des Kunden
Bestandsdaten,
ggf. Logfiles
Host-Provider (Web, …)
feste IP-
Adresse
Inhalte, ggf.
Logfiles, ggf.
Bestandsdaten
Bestandsdaten,
selten Logfiles
ISP
ISP
Bestandsdaten,
ggf. Logfiles
PC
privater
PC-
Nutzer
ISP
Bestandsdaten,
ggf. Logfiles
ISP
Bestandsdaten,
ggf. Logfiles
dynamische Vergabe
der IP-Adresse unter
Kontrolle des ISP
z.B. WG
NAT (Network Address
Translation)
feste oder
dynamische Vergabe
privater IP-Adressen
unter Kontrolle des
Kunden
PC
PC
…
PC
Server

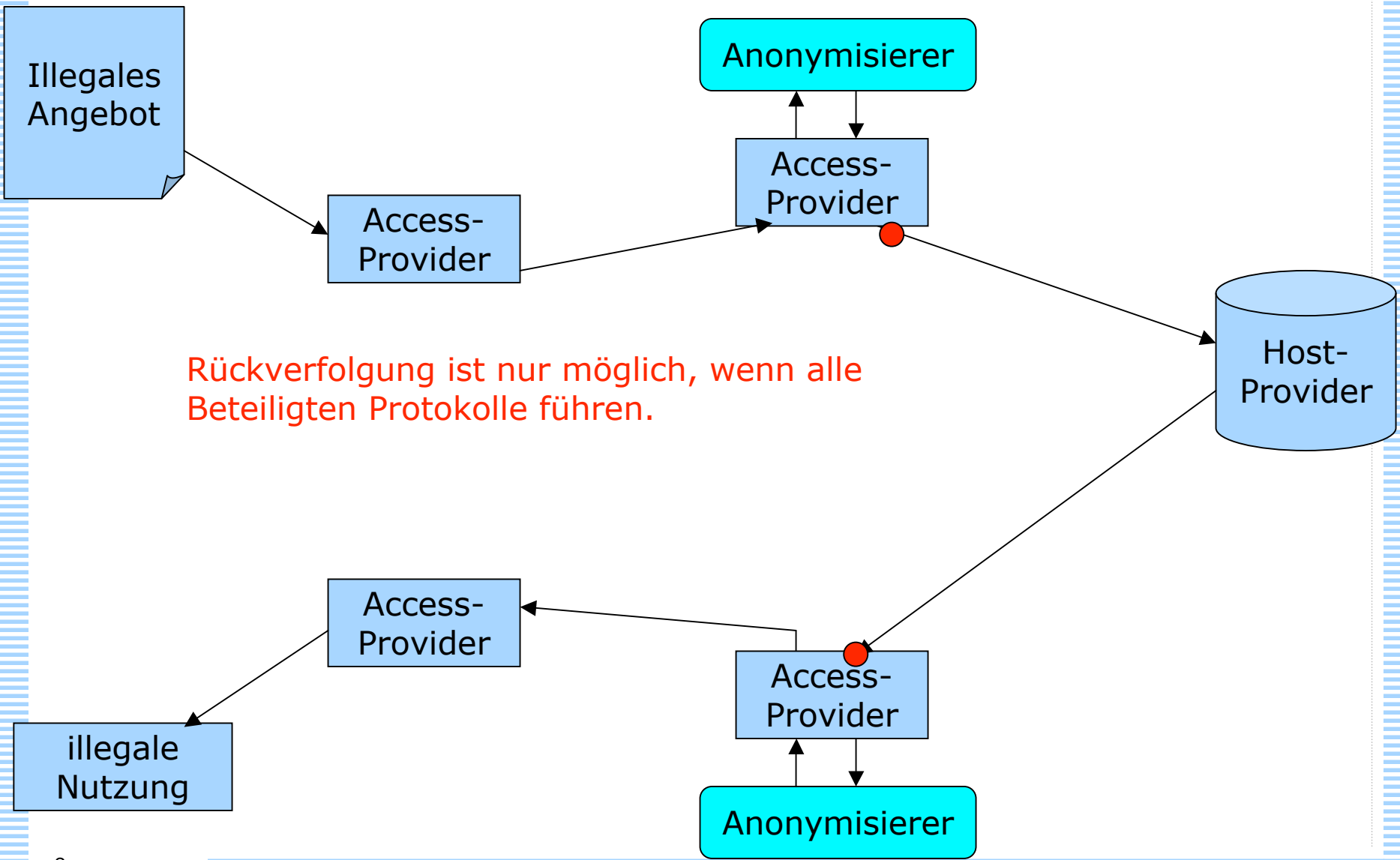
Zentraler Fileserver zum illegalen Austausch

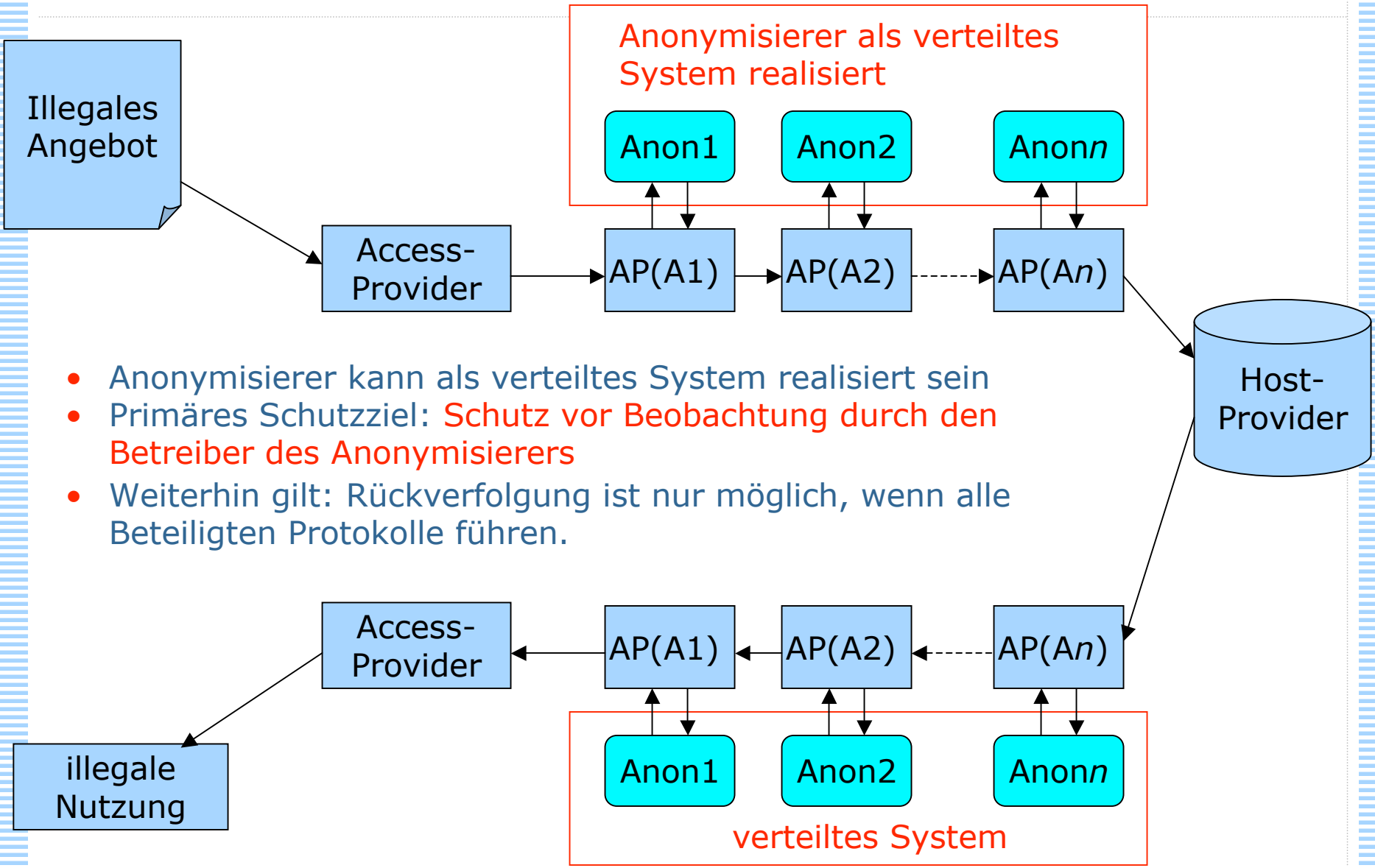


Rollen im Internet



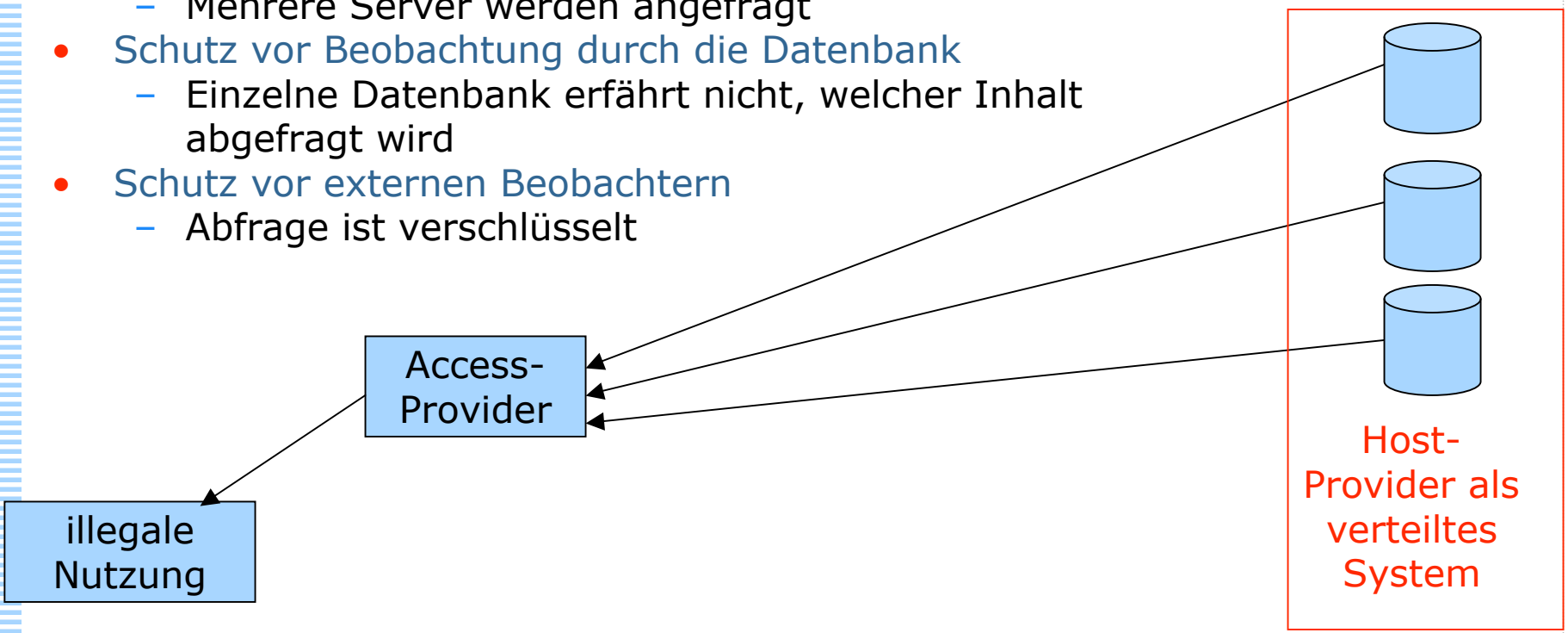
Rollen im Internet

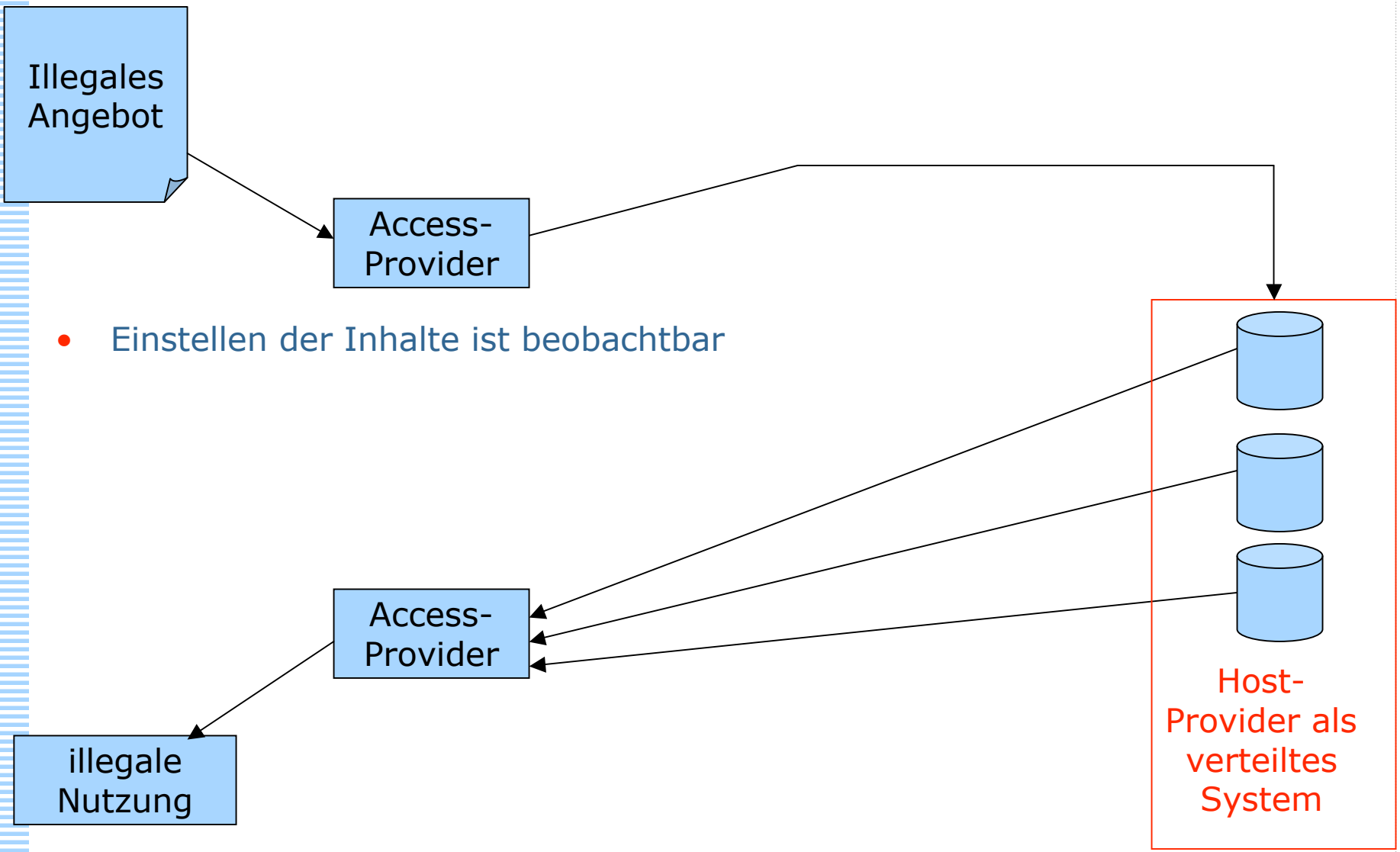




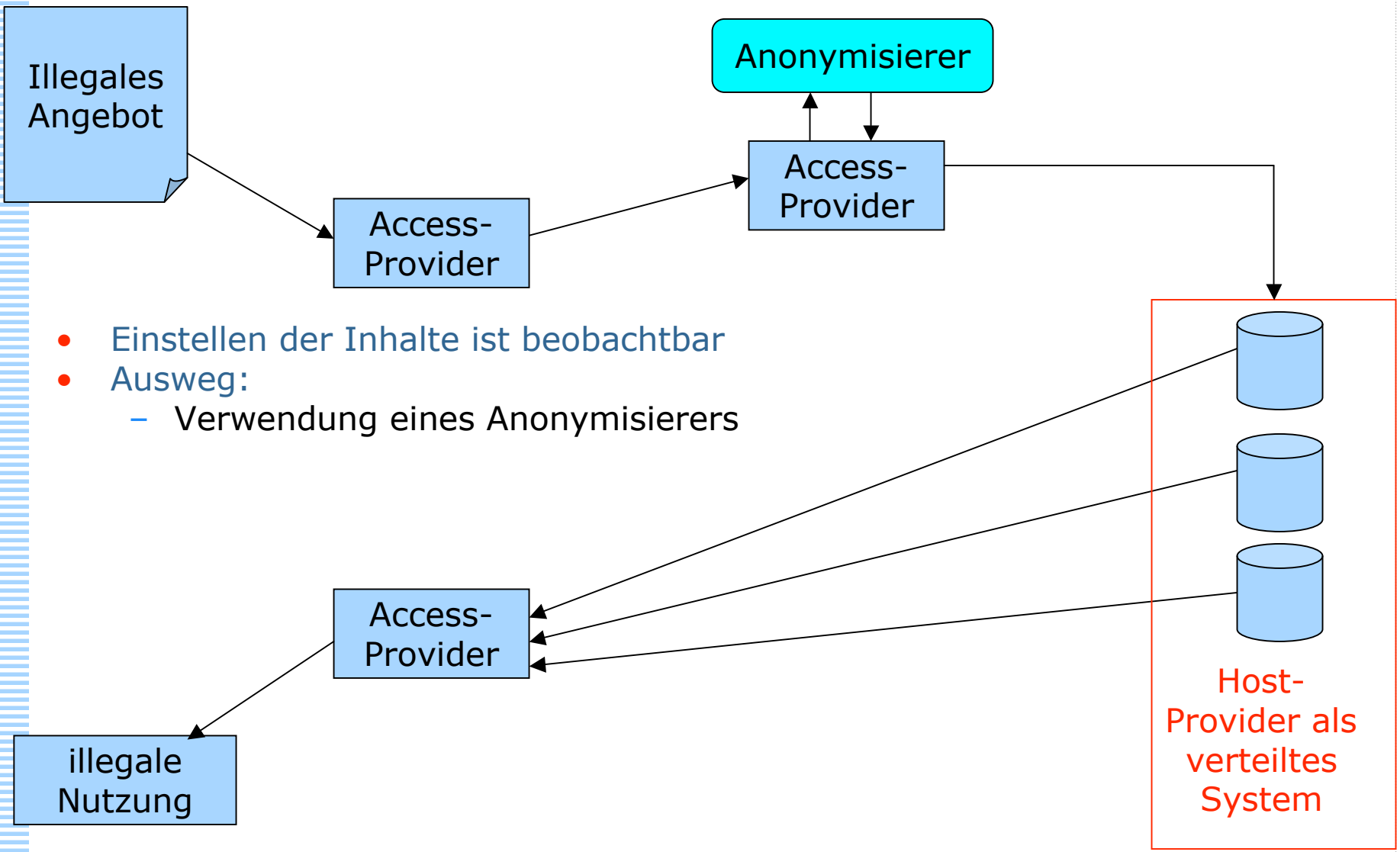
- Anonymisierer kann als verteiltes System realisiert sein
- Primäres Schutzziel: Schutz vor Beobachtung durch den Betreiber des Anonymisierers
- Weiterhin gilt: Rückverfolgung ist nur möglich, wenn alle Beteiligten Protokolle führen.

- Auch Host-Provider kann als verteiltes System realisiert sein
- Beispiel: Blind-Message-Service
- Schutzziel: Unbeobachtbares Abrufen von Inhalten
  - Replizierte Datenbanken: exakt gleiche Inhalte auf allen Servern
  - Mehrere Server werden angefragt
- Schutz vor Beobachtung durch die Datenbank
  - Einzelne Datenbank erfährt nicht, welcher Inhalt abgefragt wird
- Schutz vor externen Beobachtern
  - Abfrage ist verschlüsselt

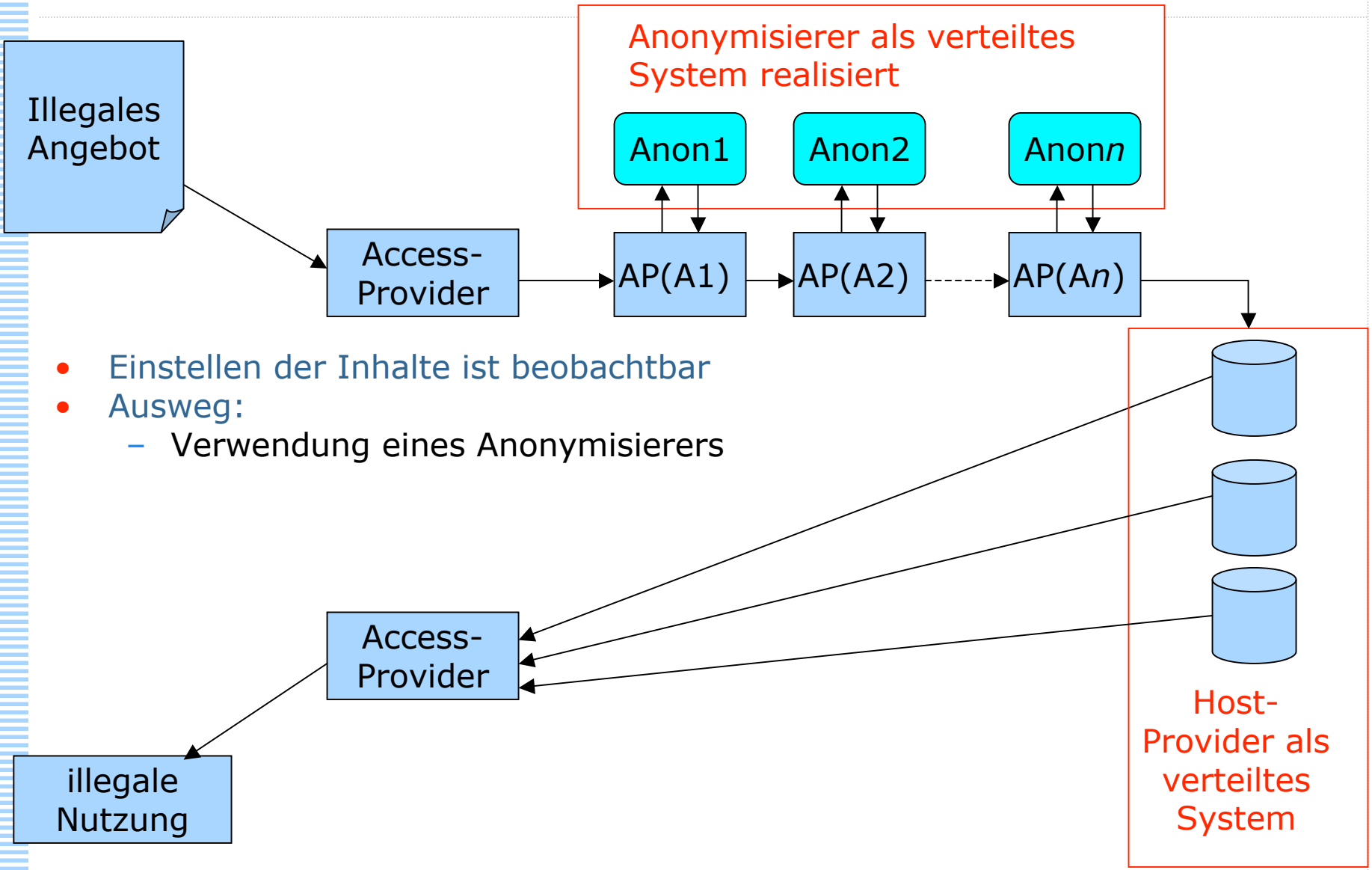




- Einstellen der Inhalte ist beobachtbar



- Einstellen der Inhalte ist beobachtbar
- Ausweg:
  - Verwendung eines Anonymisierers



- Einstellen der Inhalte ist beobachtbar
- Ausweg:
  - Verwendung eines Anonymisierers

Unbeobachtbare Peer-to-Peer-Systeme