Särimner

Patrik Fältström, Teknik- och Säkerhetsskyddschef


We’re Still running Rock-solid Internet Services

100% Uptime since 2002

For maximum resilience, Netnod's IXP infrastructure is secured in military-grade bunkers.


Brussels
Chicago
Dubai
Frankfurt
Helsinki
Geneva
Hong Kong
London
Oslo
Paris
Palo Alto
St. Petersberg
Stockholm
70+
GLOBAL DNS LOCATIONS


“There are only 13 root name servers in the world. The world trusts Netnod to operate one. “

Projekt Särimner

Bakgrund

- Idag är en stor del av den samhällskritiska informationen centraliserad (fysiskt placerad) till Stockholm

- Det gör den sårbar för attacker mot den (i många fall enda) datakällan
- Sårbart i händelse av kabelbrott, cyberattacker eller annan störning då befolkningen i andra delar av landet inte kan nå samhällskritisk information

Bakgrund

- Idag är en stor del av den samhällskritiska informationen centraliserad (fysiskt placerad) till Stockholm

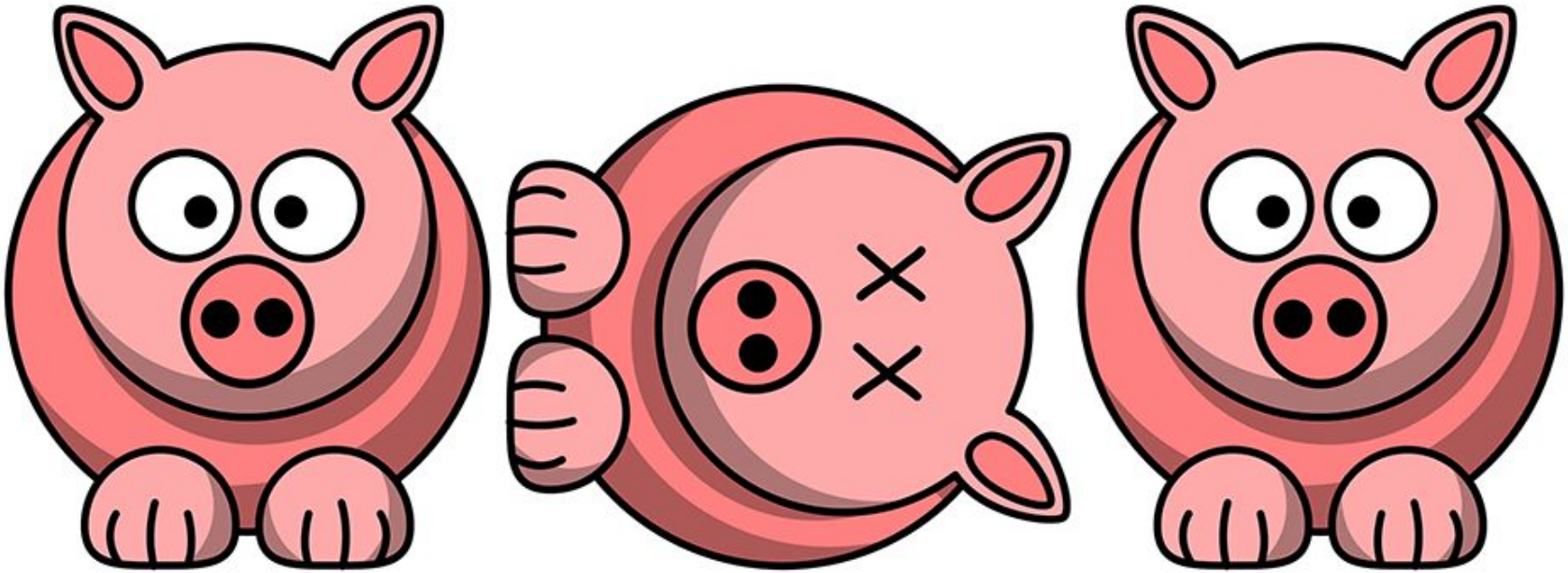
- Det gör den sårbar för attacker mot den (i många fall enda) datakällan
- Sårbart i händelse av kabelbrott, cyberattacker eller annan störning då befolkningen i andra delar av landet inte kan nå samhällskritisk information

- **Möjliga lösningar är**
  - **Förstärk infrastruktur så kontakt med Stockholm ej tappas**
  - **Distribuera information så isolerade delar av Sverige fortsätter fungera**

Projekt Särimner

- Särimner, efter grisen i mytologin som aldrig försvinner även om man äter upp honom vid varje gille

- Snorre Sturlasons Edda forteller at selv om Særimne blir spist om dagen, er den like hel, og levende om kvelden



Projekt Särimner

- Totalförsvarsplaneringen utgår från teorier att Sverige kan geografiskt bli fragmenterat

- PTS (Post- och Telestyrelsen) anser att robustheten höjs om operatörerna fysiskt kopplas ihop på många ställen, samt att viktiga infrastrukturtjänster finns på fler ställen

Regeringens skrivelse
2016/17:213

Nationell strategi för samhällets informations- och cybersäkerhet

Skr.
2016/17:213

Regeringen överlämnar denna skrivelse till riksdagen.

Stockholm den 22 juni 2017

Projekt Särimner

- Projekt Särimner ser om det är möjligt att distribuera information så att delar av Sverige kan fortsätta fungera autonomt utan kontakt med Stockholm

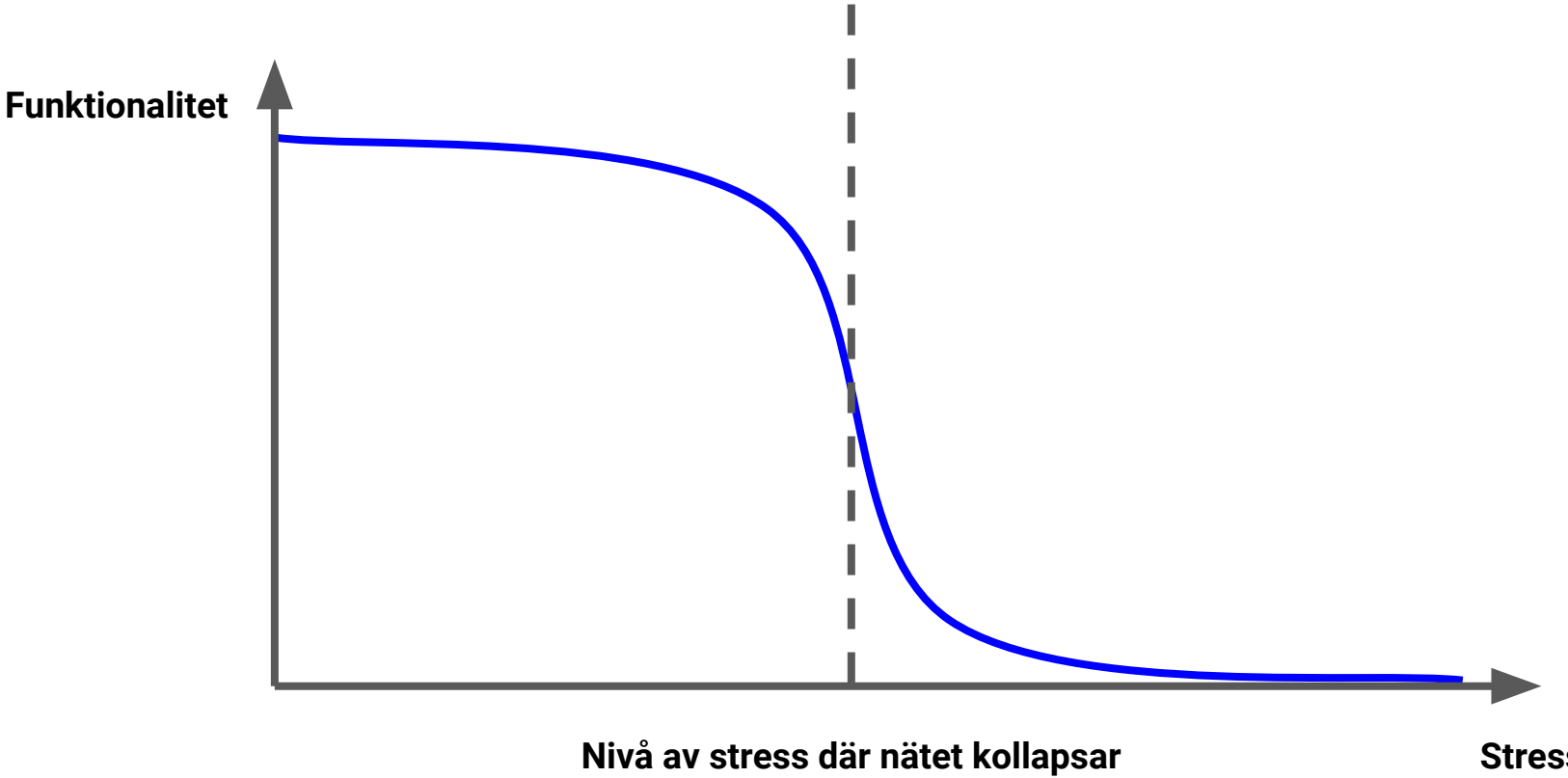
- Samarbetsprojekt mellan Netnod och SUNET, finansierat av PTS
- Har som mål att ta fram en lösning för robust kommunikation
- Består primärt av två delar
  - Stabilt och säkert trafikutbyte mellan operatörer i Sverige
  - Spridning av information vid extrem stress till mottagare/medborgare
- Projektet pågår under 2018

Arbetsfördelning

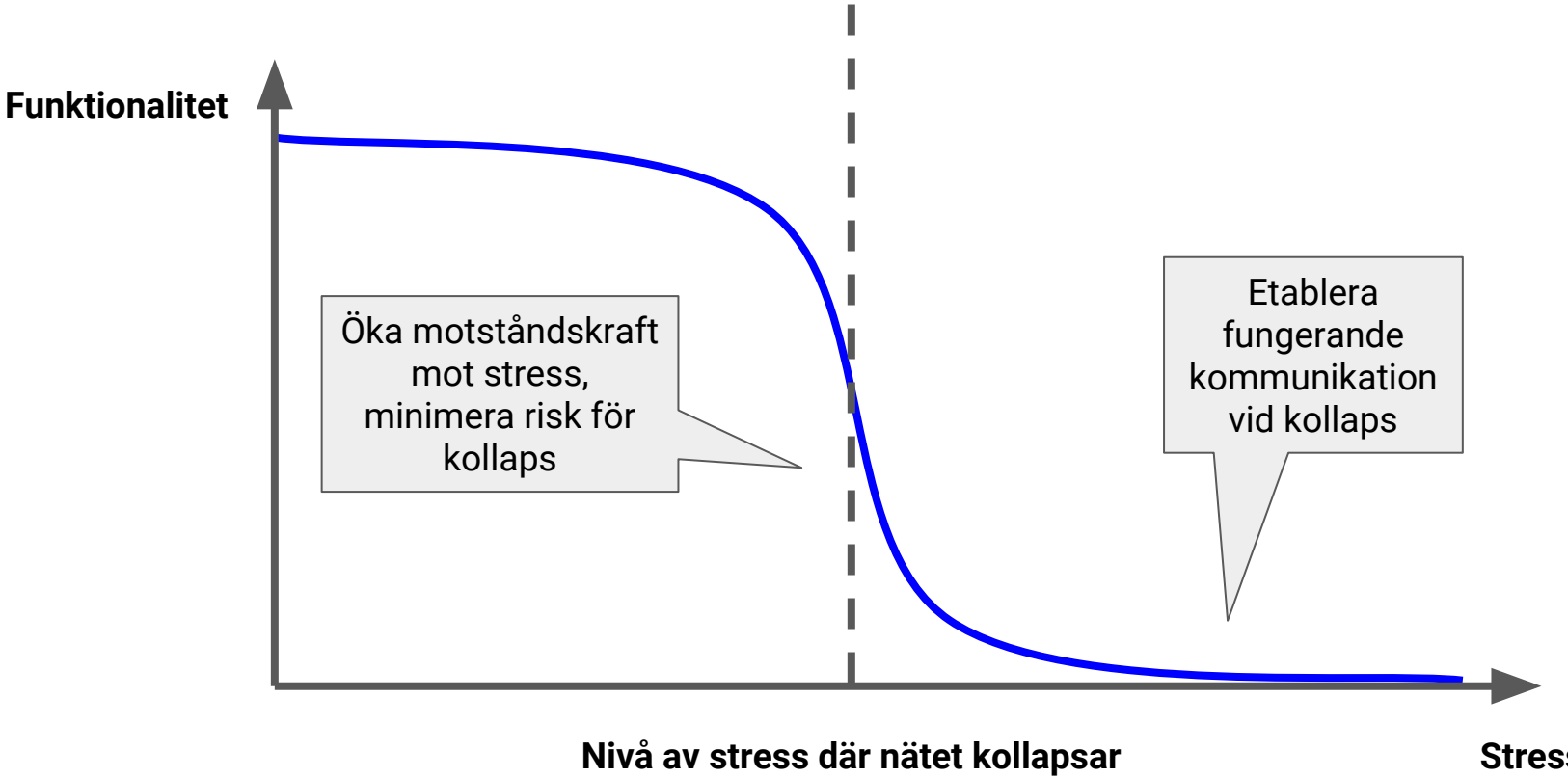
- Hårdvara och hosting (IP-adresser)
- Utveckling av secure boot (via Assured)
- Provisionering och drift av noder
- Kompetens gällande routing
- Koppling till kunder
- Skrivande av rapport (via Governo)
- Hantering av skyddsvärd information

- Transit och transmission
- Utveckling av CDN-del
- Utveckling av Scraper
- Koppling till tex Cryptech
- Kompetens gällande routing
- Koppling till kunder

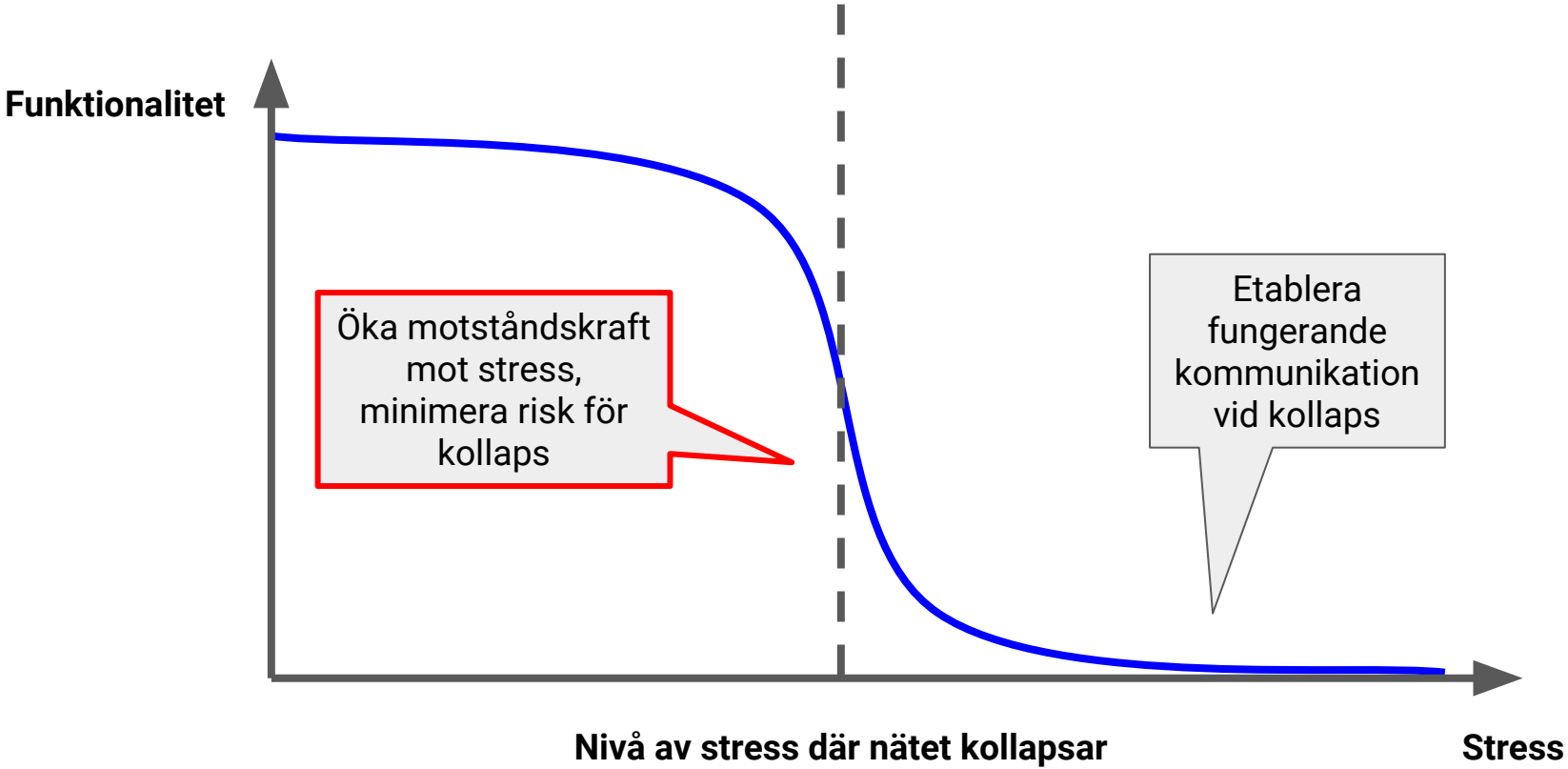
Stress och funktionalitet i paketbaserade nät



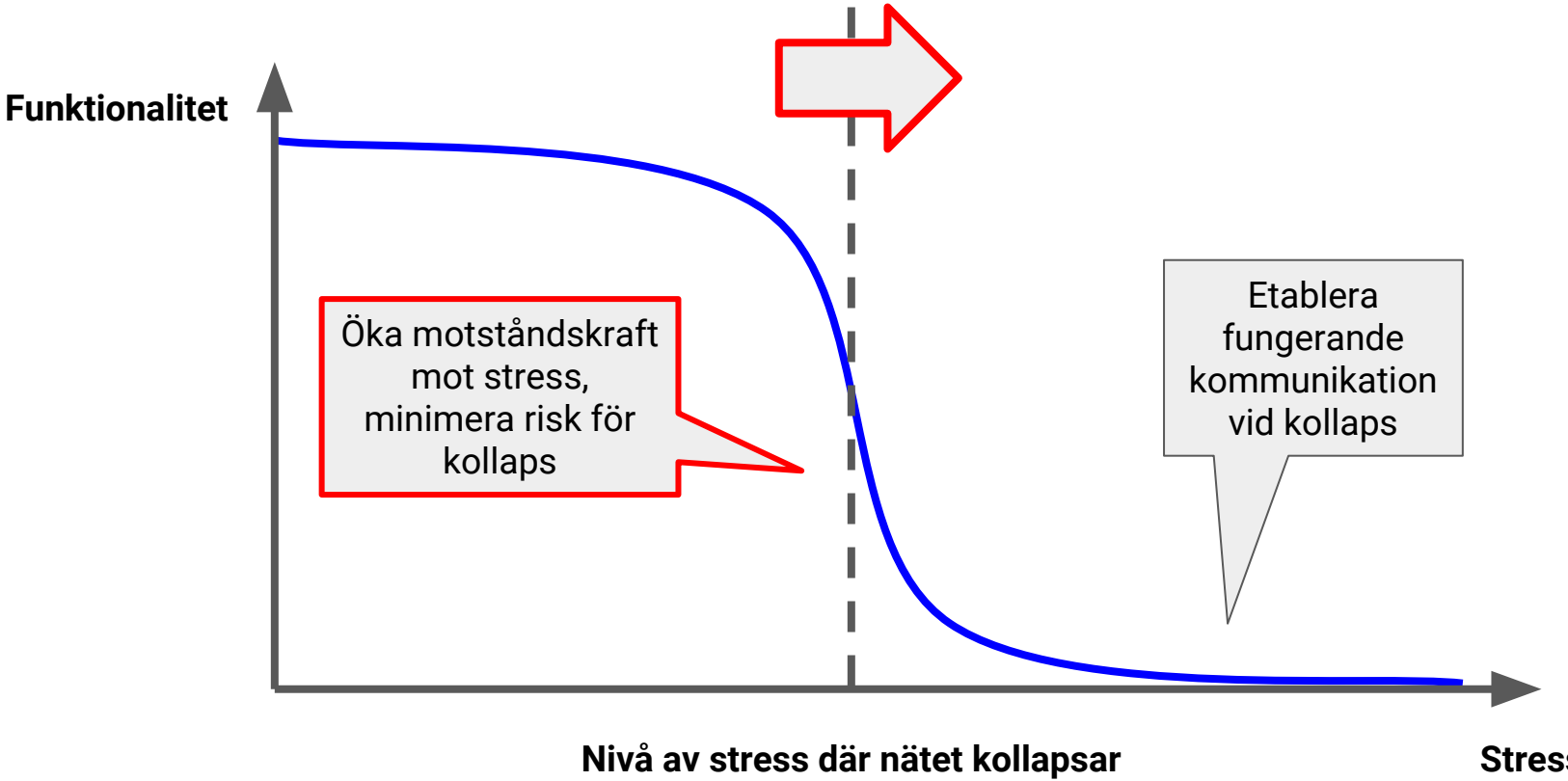
Stress och funktionalitet i paketbaserade nät



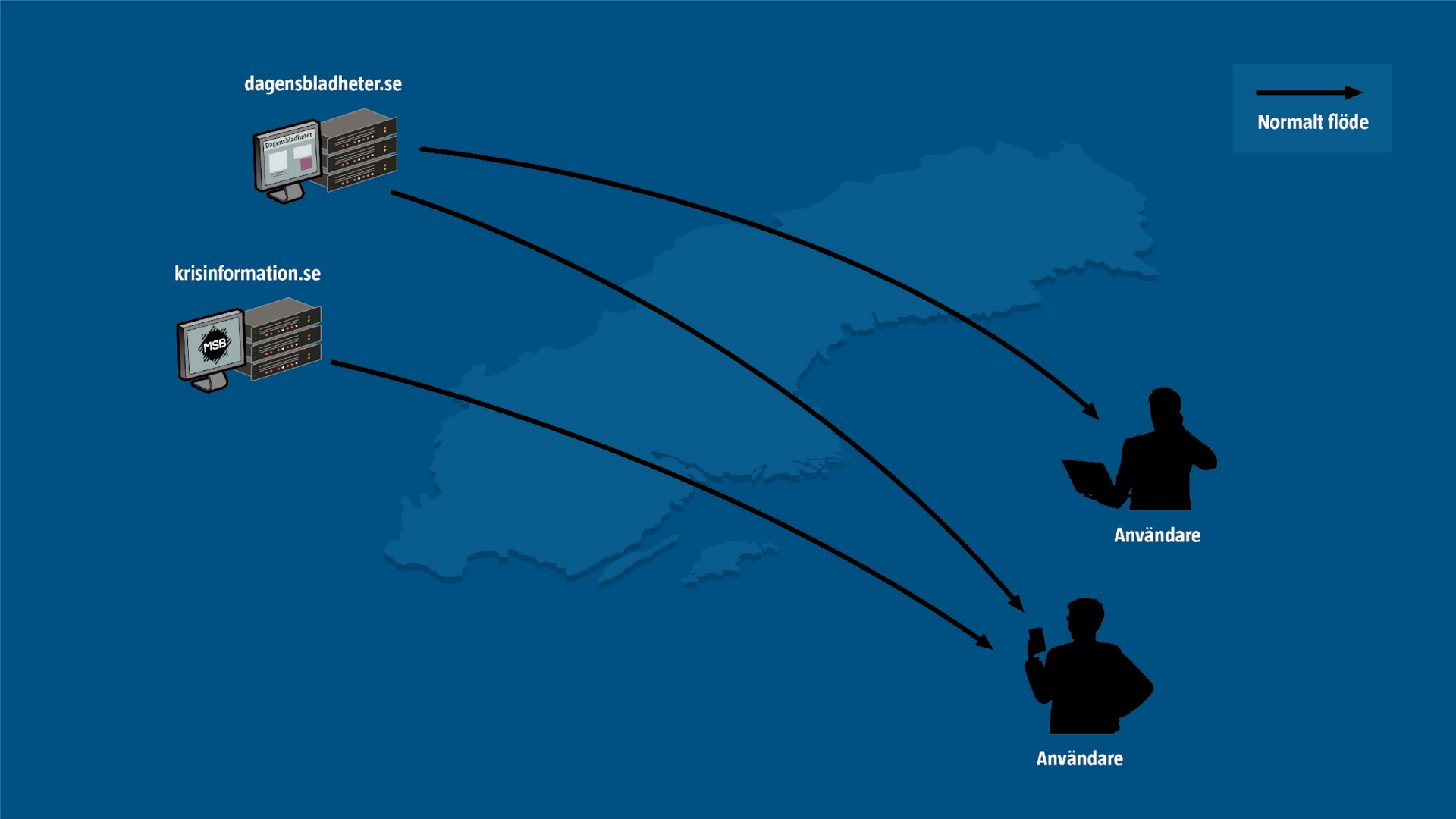
Stress och funktionalitet i paketbaserade nät

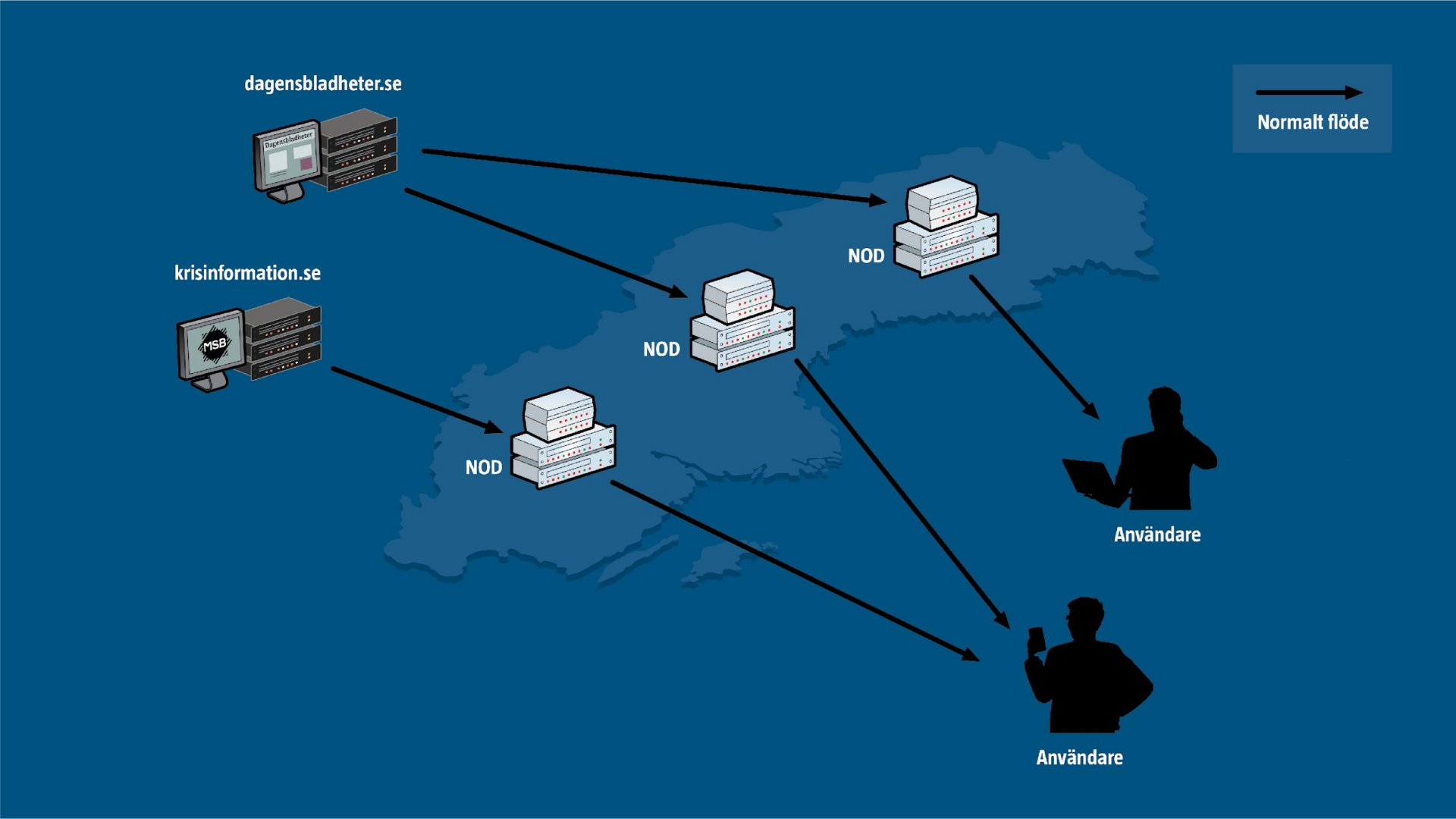


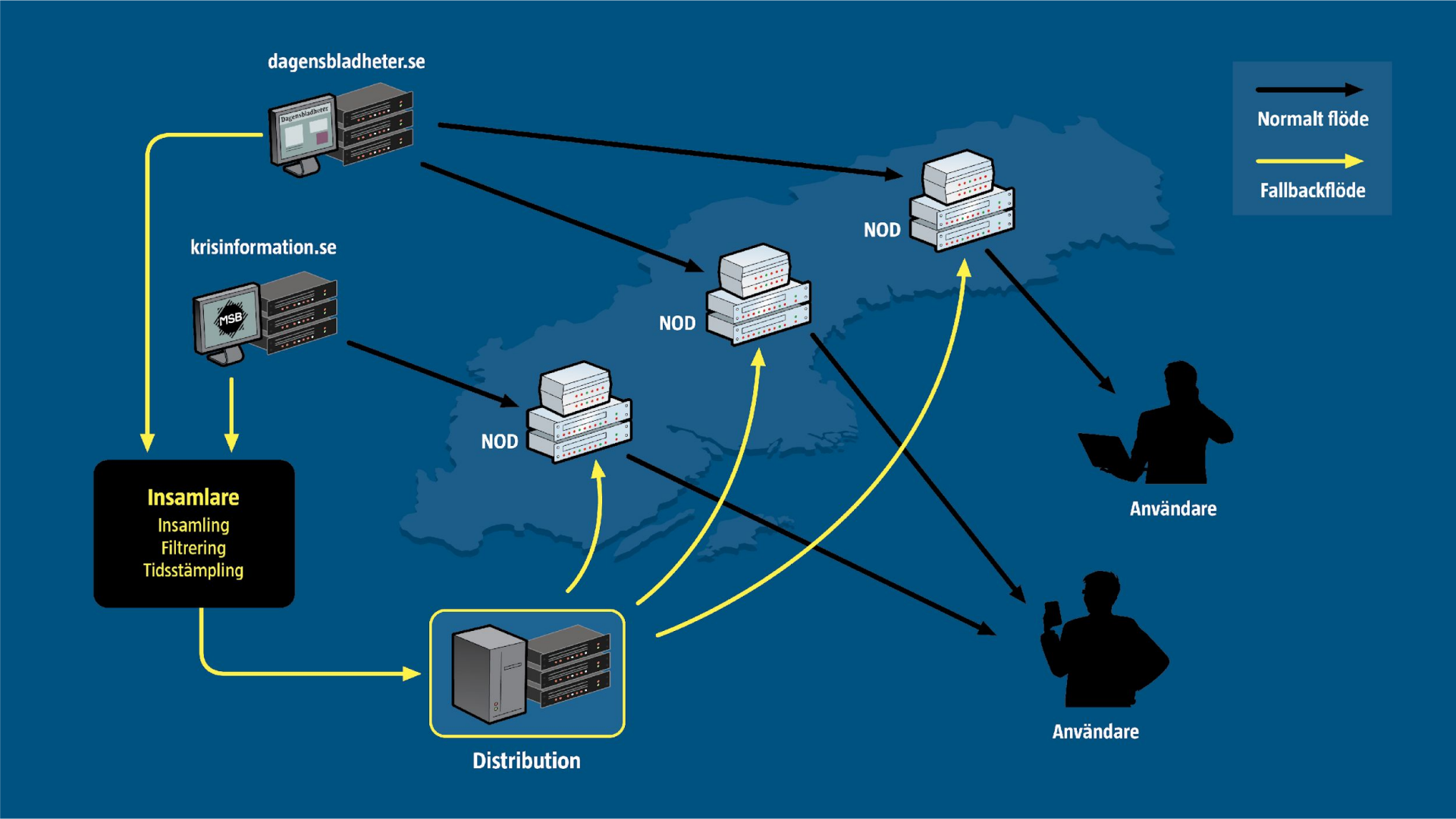
Stress och funktionalitet i paketbaserade nät

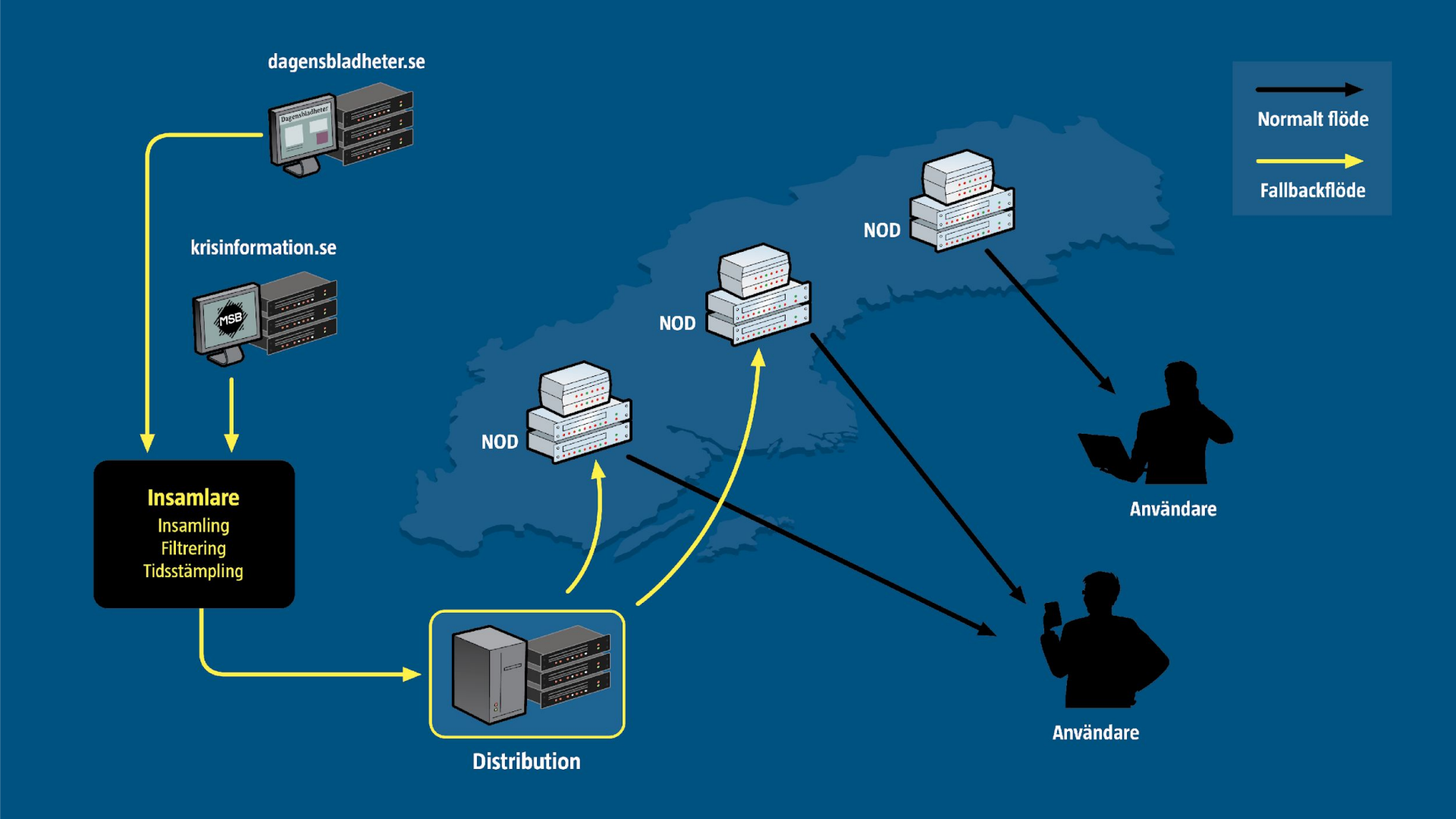


Stress och funktionalitet i paketbaserade nät

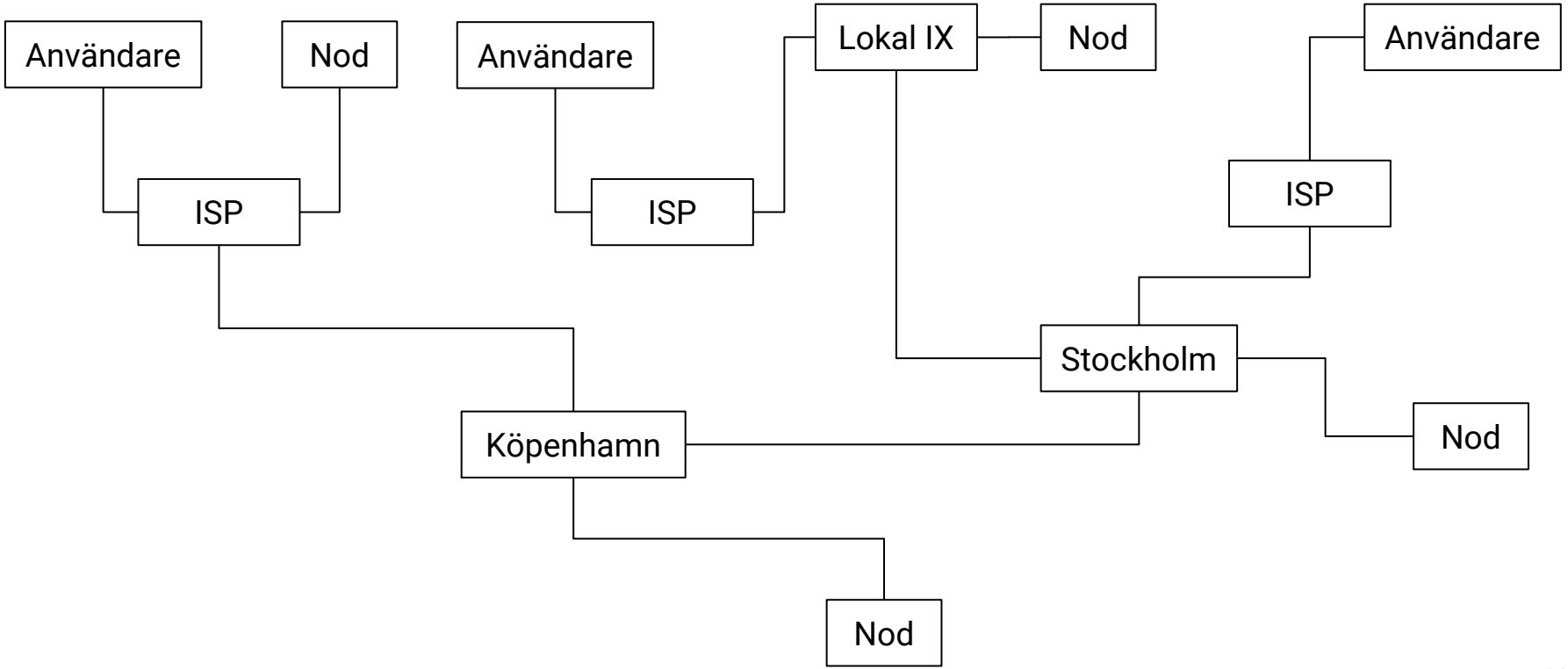

dagensbladheter.se
krisinformation.se
MSB
Normalt flöde
Användare
Användare


dagensbladheter.se
Normalt flöde
krisinformation.se
NOD
NOD
NOD
Användare
Användare

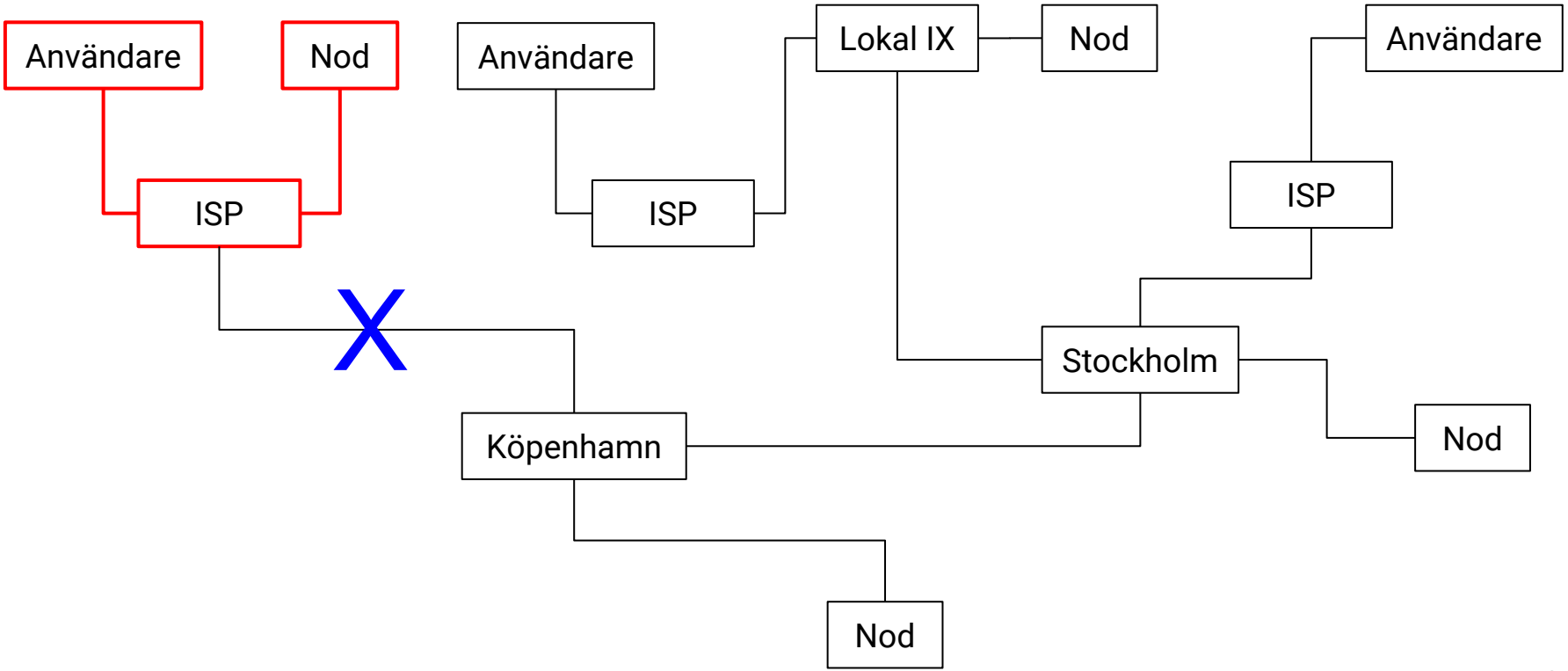

dagensbladheter.se
krisinformation.se
MSB
Insamlare
Insamling
Filtrering
Tidsstämpling
NOD
NOD
NOD
Distribution
Användare
Användare
Normalt flöde
Fallbackflöde


dagensbladheter.se
krisinformation.se
Insamlare
Insamling
Filtrering
Tidsstämpling
Distribution
NOD
NOD
NOD
Användare
Användare
Normalt flöde
Fallbackflöde

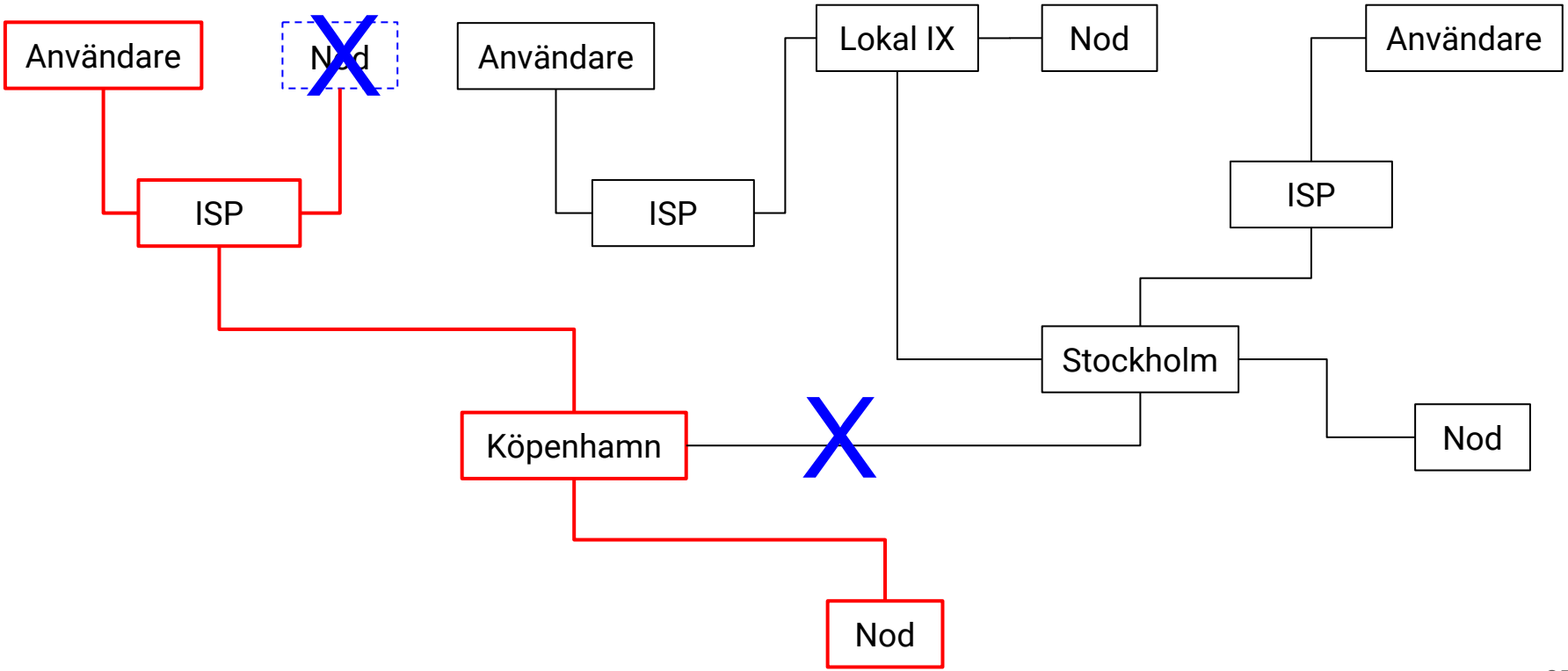
Generellt flöde av information



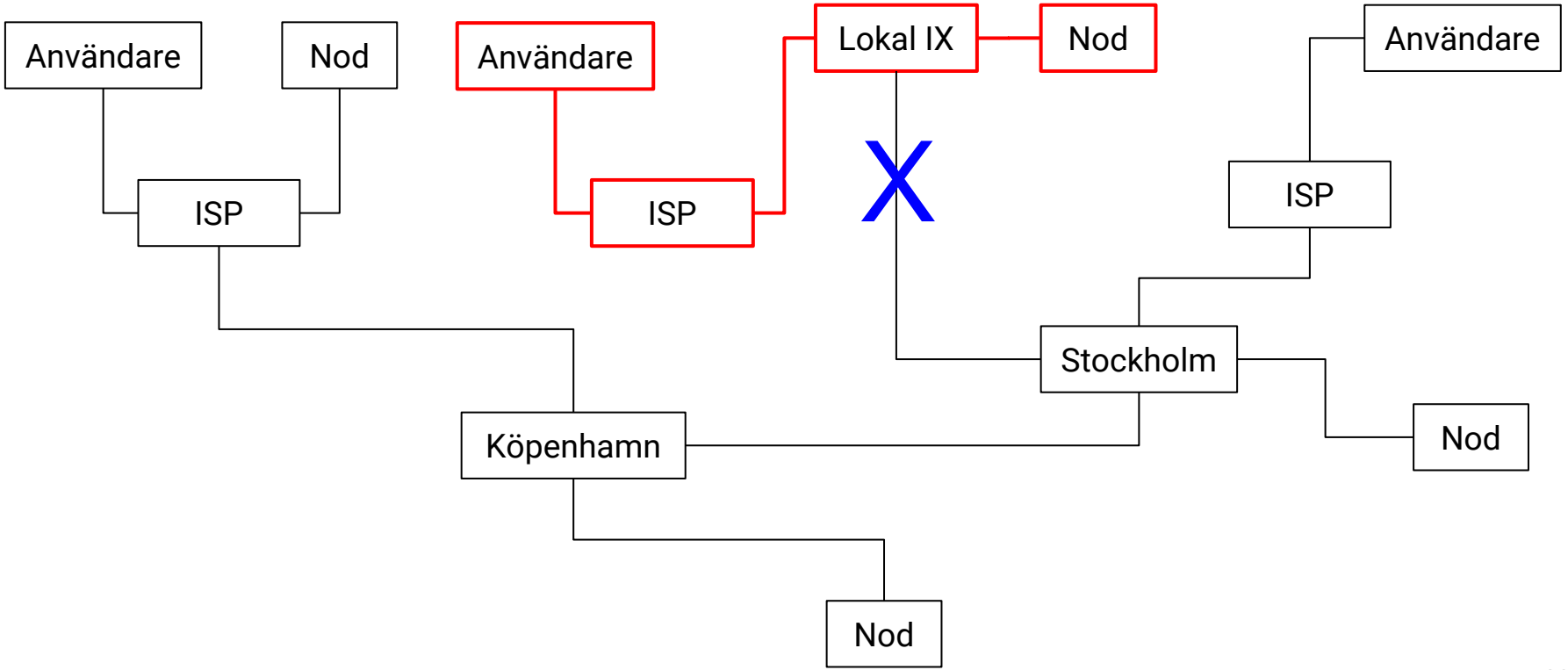
Generellt flöde av information



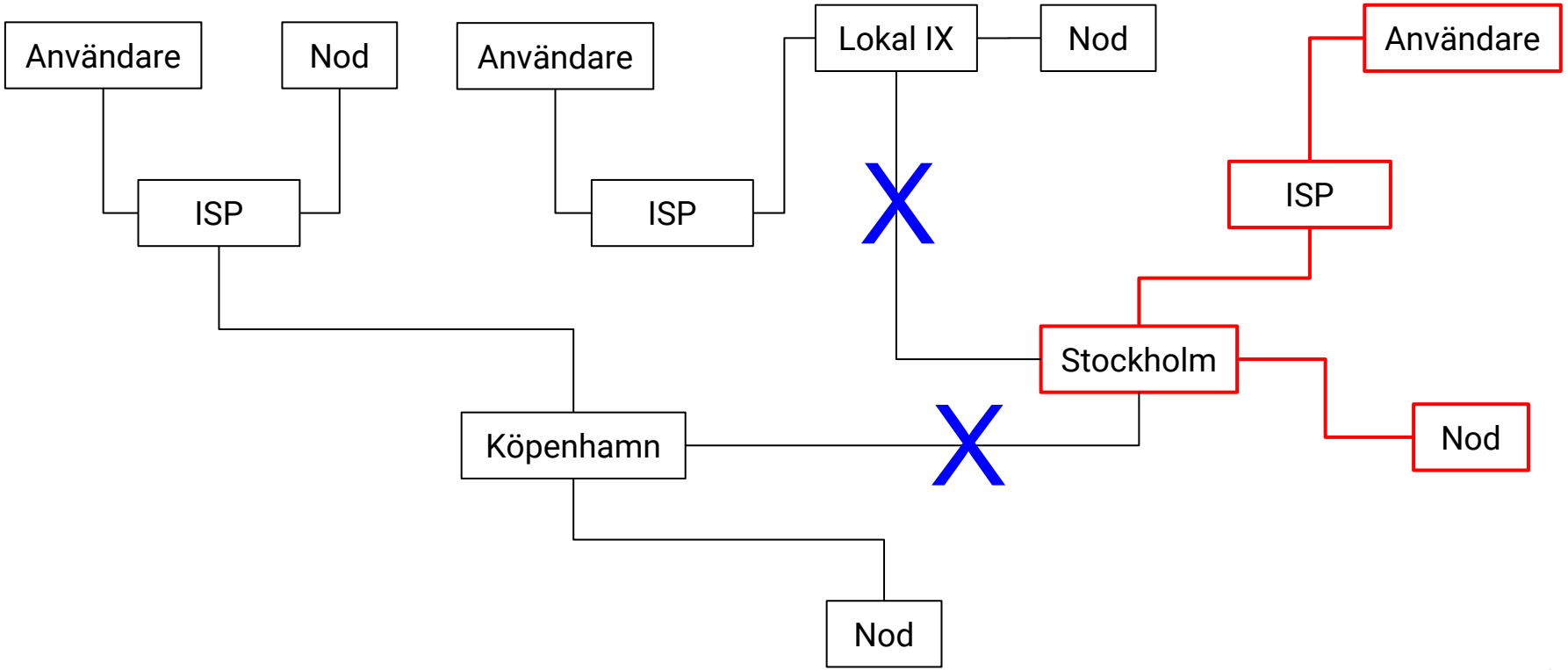
Generellt flöde av information



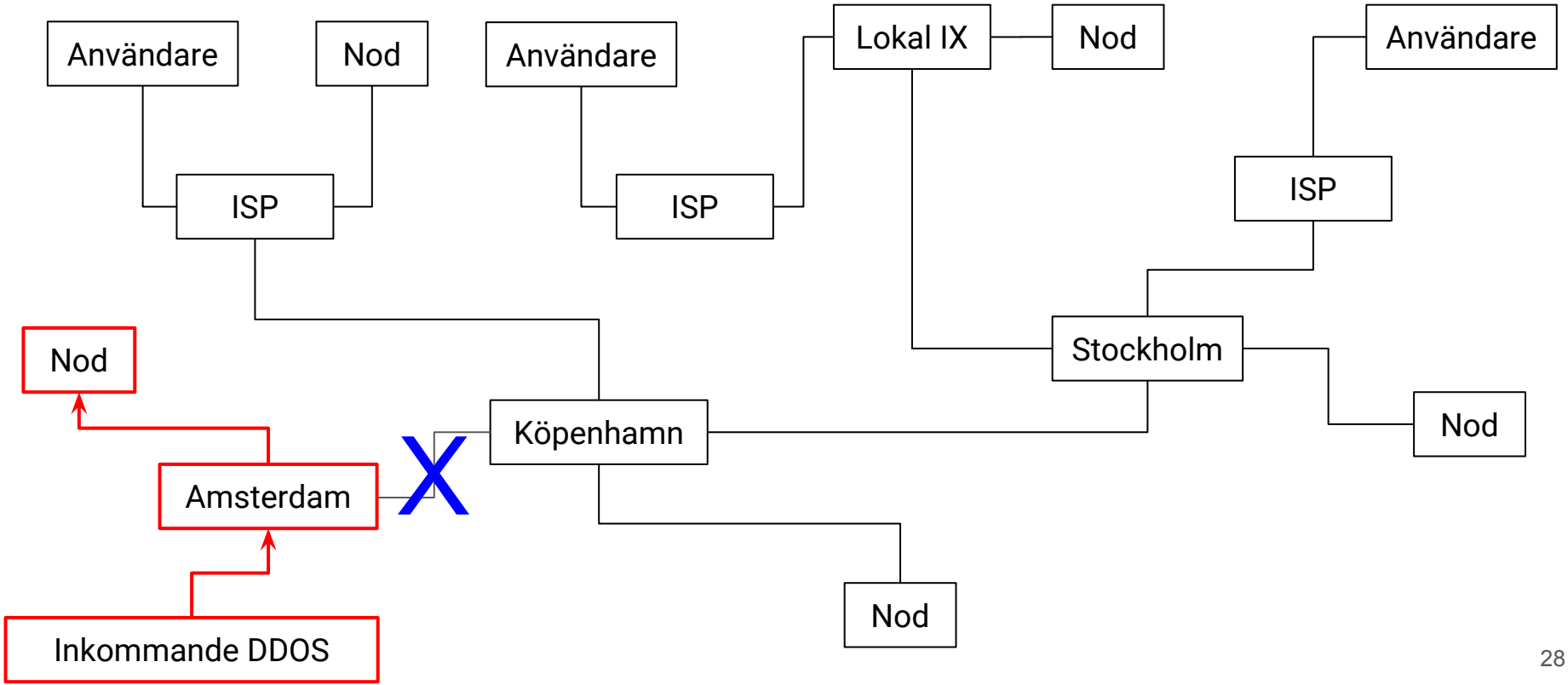
Generellt flöde av information



Generellt flöde av information



Hantering av honeypot



Projekt Särimner

- Trafikutbyte mellan deltagare ska fungera under extrem attack
  - Separata överenskommelser mellan operatörer
  - Fler mötesplatser
- Systemet ska klara av stor trafikmängd
  - Storleksordningen 1 request per 10 sek per innevånare => 1 miljon request/s
  - Det ska alltid ges svar på request (“ingen 404 här inte”)
- Noder ska primärt vara proxy för web/HTTPS
  - Distribuerat system för att hantera den höga belastningen
  - Det enklaste sättet att “ha saker på plats innan det smäller”
- Systemet ska klara en partitionering av Sverige
  - Enstaka noder ska kunna fungera autonomt
  - Först 5-10 noder, i andra steget 30

Noder

- Placeras vid:
  - Netnod IX
  - Andra IX för projekt Särimner - kan vara STHIX, Norrnod, IXOR, ...
  - Som en on-net cache inuti en ISPs nät
  - En eller flera strategiska platser (öar, isolerade områden etc)
- Exponerar DNS och HTTP/HTTPS mot slutanvändaren
  - Anycast, alla noder använder samma AS och samma IP-adresser
  - Auktoritativ DNS-server för Root, SE, NU och fler delar av DNS-kedjan
  - Resolver för DNS (kanske även extern resolver...)
  - Terminerar HTTP/HTTPS.
  - Validerar och signerar informationen (ingen Fake News)
  - Speciella processer för att validera integriteten hos en nod inkl self-destruct om det behövs
  - Secure boot, TPM etc

Utbyggnad

- Stockholm
- Göteborg
- Köpenhamn / Malmö
- Sundsvall
- Luleå
- ~~Visby~~
- Amsterdam
- ~~London~~
- Operator-placed, *You?*

Frågor?

Patrik Fältström paf@netnod.se


THE WORLD TRUSTS
netnod.se