Hur ska landstingen gå in i molntjänsten - Och hur vet vi vilka vi är?

Anne-Marie Eklund Löwinder, säkerhetschef
amel@iis.se

Kort om IIS

Oberoende allmännyttig stiftelse med två huvudsakliga verksamhetsområden:

- ansvar för driften och administrationen av toppdomänerna .se och .nu
- Främjar utvecklingen och användningen av internet i Sverige

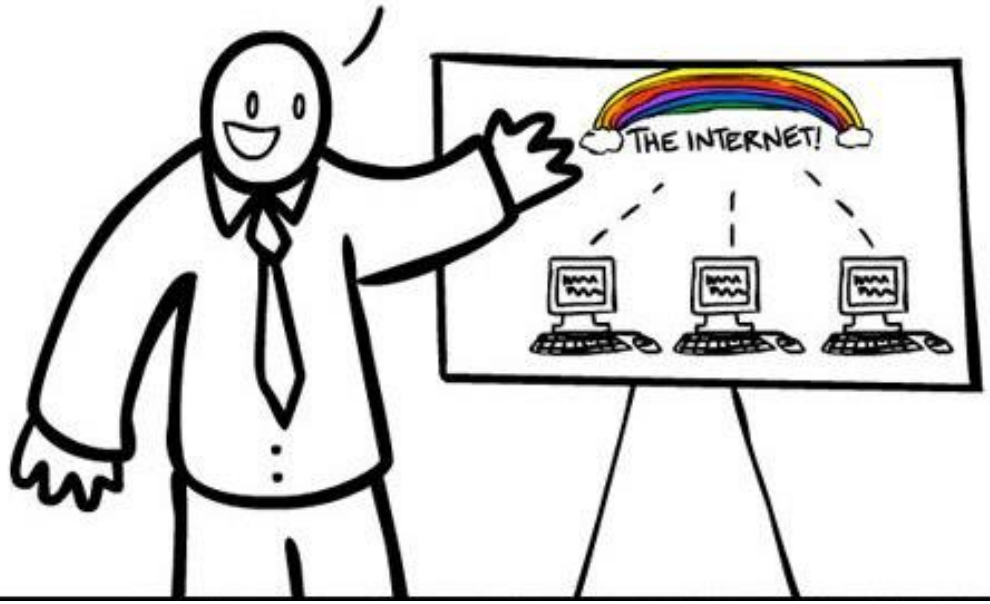
Sambi

möjliggör en säker åtkomst till digitala tjänster för hela sektorn vård, hälsa och omsorg.

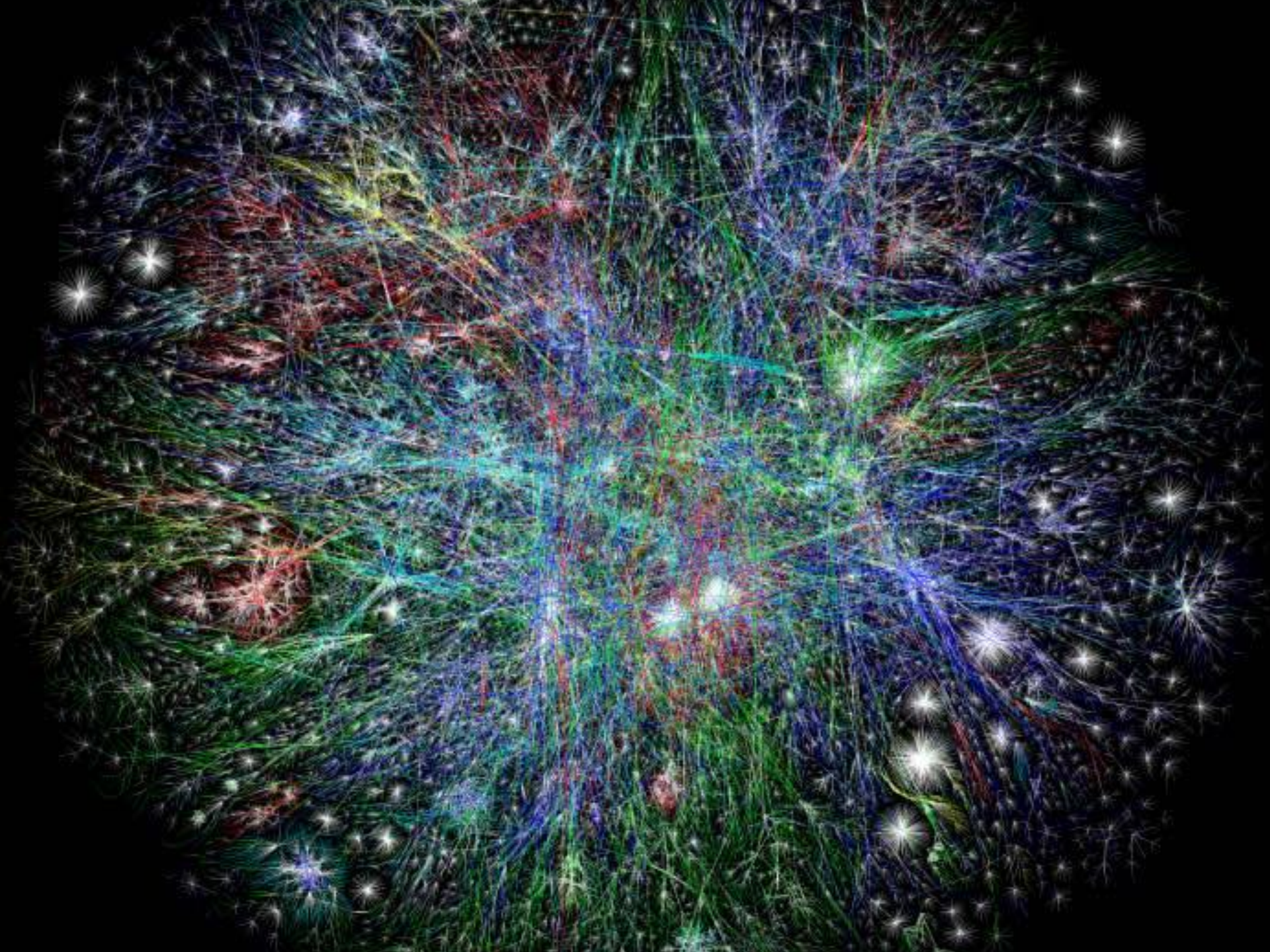
Bakom Sambi står eHälso-myndigheten och Inera med stöd av Internetstiftelsen i Sverige, IIS.

BEFORE THE INTERNET

JUST THINK OF ALL THE POSSIBILITIES! THE INSTANTANEOUS EXCHANGE OF IDEAS & INFORMATION! JUST IMAGINE HOW PRODUCTIVE OUR SOCIETY WILL BECOME!

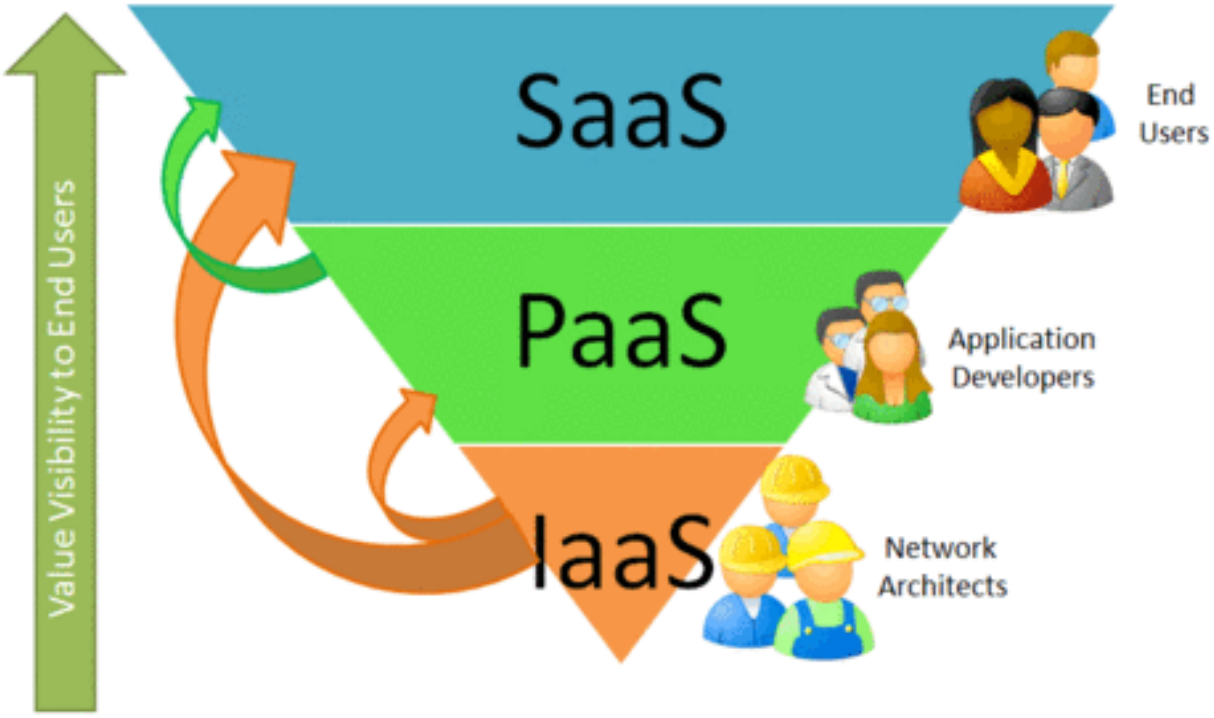



NOW:
OH GOD...
WHAT HAVE
I DONE?
endlessorigami.com



Molntjänster

Vad finns under ytan?



Tillgång till en lösning

- Så snabbt som möjligt
- Så billigt som möjligt
- Så bra som möjligt

Molntjänster är attraktiva

- Låg inkörningströskel
- Betala i kassan
- Anpassa efter behov (skala upp/ner)
- Hög tillgänglighet (kanske)

Livscykel

- Säkerhetskravställning
- Utvärdering
- Avtal
- Audit/uppföljning

Orosmoln…

Rädsla är lidande i förskott, men…..

Potentiella sårbarheter i molntjänster

- Tillförlitlighet och tillgänglighet
- Konfidentialitet (kryptering)
- Dataskydd och portabilitet
- Inlåsning hos leverantör
- Internetberoende

Någonstans finns en fysisk maskin

Kan du lita på din leverantör?

- Vem äger eller har nyttjanderätten till den information som skickas upp till molnet?
- Vem äger metadata eller information som skapas i molnet som en del i nyttjandet av tjänsten (statistik, loggar)?
- Vad händer när molnleverantören säljs, går i konkurs, har allvarliga driftsproblem, blir ertappad med något fuffens eller bara inte sköter sig?

Efteråt?

- Försvinner känslig information från lagringsenheter efter avslutat avtal?
- Vad händer med data som lagras i molnet när det har passerat ägarens bäst före-datum?
- Vad har molnleverantören för policy för datasanering när de ska pensionera gamla lagringsenheter och maskiner?

Ställ konkreta krav på leverantören

- Finns professionell säkerhetspersonal för kameraövervakning, hantering av intrångsdetekteringssystem och andra skyddsåtgärder?
- När en anställd inte längre behöver komma åt datacentret tas då privilegierna omgående bort?
- Loggas all fysisk och logisk access och granskas loggarna regelbundet?
- Har leverantören sådan spårbarhet att en kund när som helst kan se hur data lagras, skyddas, används?

Säkerhetskravställning ISO 27017:2015

- Tillgänglighet
- Autentisering och behörighetshantering
- Kryptering
- Nätverkssäkerhet
- Spårbarhet
- Gallring
- Avveckling och förstöring

Utvärdering

- Gruppera och ställ krav till rätt målgrupp:
  - driftkrav (alla nivåer)
  - krav på tjänsten (SaaS)
  - integrationskrav (SaaS)

Utvärdering - drift

- Ändringshantering
- Behörighetsprocess
- Härdning/patchning
- Lagring och backup
- Spårbarhet - åtkomst till loggarna
- Incidenthantering (inkl. säkerhet)

Utvärdering - tjänst

- Säker utveckling (SDL, OWASP)
- Säkerhetstester (pen-test)
- Web Application Firewall (WAF)
- Autentiseringsmekanismer
- Kryptering av information
- Spårbarhet

Utvärdering - integration

- Autentisering (SAML/ADFS)
- Vilka nätintegrationer krävs?
- Vilken infrastruktur krävs internt?
    - API gateway
    - integration gateway
    - proxy lösningar
- Tredjepartsintegratörer

Uppföljning

- Hur skall man kunna följa upp det som avtalats?
- Går det att genomföra audit (enligt avtalet)?
- Extern revision eller kunden själv?
- Regelbundna pentester
    - Kräv rapport från test och hantering av upptäckta sårbarheter

Avslut

- Strategi för avslut?
- Finns det stöd i avtalet att informationen kan exporteras till en annan tjänst eller kunden själv?
- Tas informationen bort efter exit?
- All information? Även behörigheter? Loggar?

Inget nytt under solen…

- Behovsanalys
- Kravspecifikation
- Ansvarsfördelning
- Avtal
- Uppföljning
- Granskning

The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

Sammanfattning 1 (2)

- Molntjänster är här för att stanna
- Många är bra, men det finns spelare med bristande rutiner
- Utvärdera kvalitet och säkerhet på alla nivåer
- Avtal bör innehålla alla relevanta delar
- Beräkna en totalkostnad inklusive integration

Sammanfattning 2 (2)

- Genomför risk- och sårbarhetsanalys
  - vad blir konsekvensen för dig och din information
  - agera efter det

Hur vet vi vilka vi är?

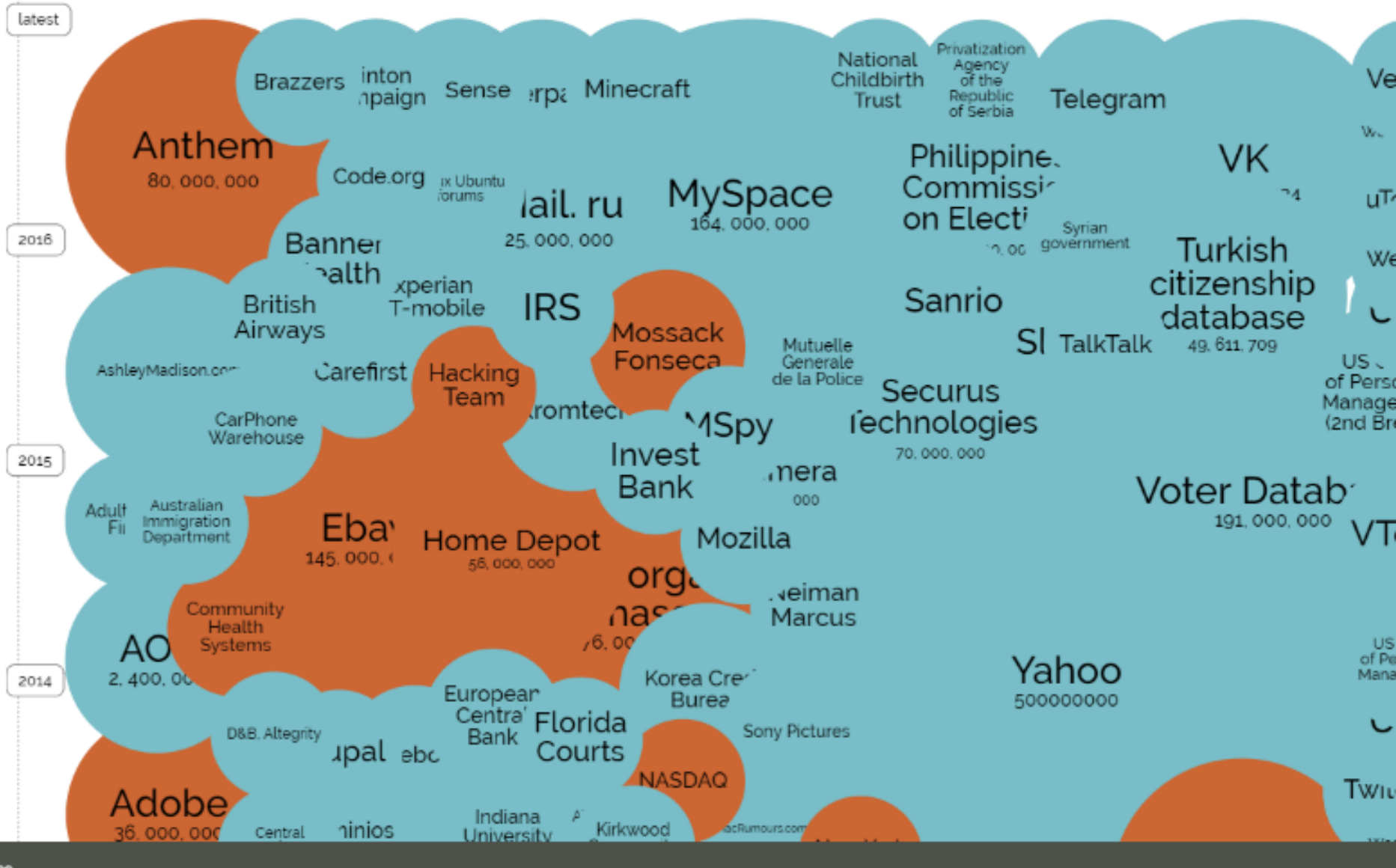
World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 24rd September 2016)

YEAR

BUBBLE COLOUR | YEAR | METHOD OF LEAK | BUBBLE SIZE | NO OF RECORDS STOLEN | DATA SENSITIVITY



Nätfiske – fastna inte på kroken

Flera källor vittnar om att cirka 90 procent av alla attacker börjar med riktade nätfiskemejl

Lämna inte ut information i onödan

- Användarnamn
- Lösenord
- Personnummer
- PIN-koder
- Servernamn
- Systeminformation
- Kreditkortsnummer
- Känslig information i allmänhet

Med koden 2016IND får ni 20 procent rabatt på avgiften

Välkomna!


Frågor?
Tack!
Anne-Marie Eklund Löwinder
Säkerhetschef, IIS
amel@iis.se
@amelsec