

Ett ledningsperspektiv på informationssäkerhet

Anne-Marie Eklund Löwinder
Kvalitets- och säkerhetschef

.se



Min presentation i korthet

- Kort om .SE
- Vad är domännamnssystemet (DNS)?
- Säkerhet i elektroniska affärer
- Så här arbetar .SE med informationssäkerhet



.se



Vår historia

- Stiftelsen för Internetinfrastruktur grundades 1997.
- Fram till 1997 sköttes toppdomänen .se av en privatperson, Björn Eriksen.
- VD är Danny Aerts, styrelseordförande är Rune Brandinger.
- Brett sammansatt styrelse:
 - ISOC-SE
 - Konsumentverket
 - LO
 - Svenska Bankföreningen
 - Svensk Handel
 - Sveriges Internetoperatörers forum (SOF)
 - Svenskt Näringsliv



.se



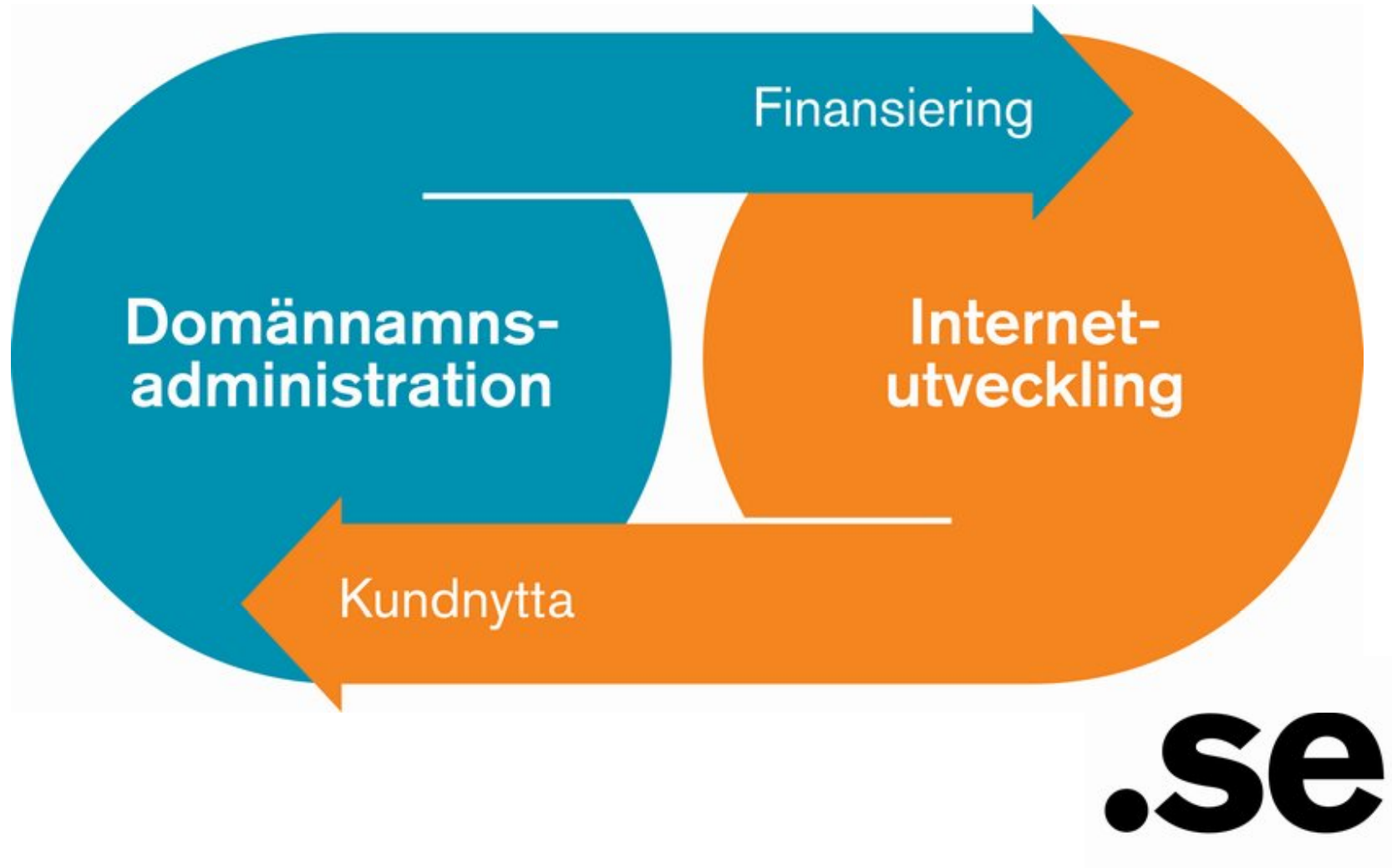
.SE:s verksamhet

- .SE:s sköter administration och teknisk drift av det nationella domännamnsregistret under .se.
- omkring 500 nyregistreringar per dag.
- Ca 40 anställda.
- Ca 200 ombud.
- Omsättning 2007; 74 miljoner kronor.
- .SE står under tillsyn av:
 - PTS genom Lagen om nationella toppdomäner på Internet i Sverige (SFS:2006:24).
 - Länsstyrelsen genom Stiftelselagen.



.se

.SE enligt urkunden



Hur fungerar DNS?



.se



IT- och informationssäkerhet

- För vem?
 - För oss själva, för ägare, kunder eller andra oroliga intressenter.
- För vad?
 - Kontroll över verksamheten.
- Hur?
 - Tekniska lösningar är inte det första ni ska tänka på . rutiner och kunskap är viktigare än produkter.

.se

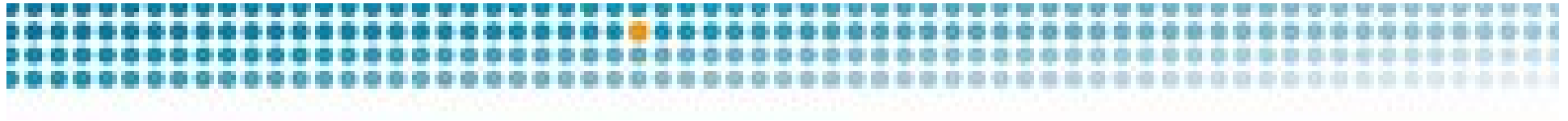


Krav på intern kontroll

- Ansvaret ligger på styrelsen i ett bolag
- I samverkan med ansvarig ledning och medarbetare
- Uppfylla mål inom följande kategorier:
 - Effektiv verksamhet
 - Tillförlitlig finansiell rapportering och information om verksamhetens resultat
 - Efterlevnad av tillämpliga lagar och föreskrifter



.se



+Allting bör göras så enkelt som möjligt, men inte enklare +
Albert Einstein

.se



Hur ser ditt företag ut?

- Vilka produkter och tjänster gör er unika?
- Vilka är era kunder?
- Hur är ni organiserade?
- Vilka samarbetspartners har ni?



.se



Hur ser människorna i företaget ut?

- Har ni egen IT-kompetens eller anlitas extern kompetens?
- Hur hanteras känslig information utanför företagets lokaler?
- Har företaget någon form av utbildningsprogram på plats?
- Hur teknikmogna är medarbetarna?
- Finns roller/ansvar för att hantera tillgänglighet och kvalitet i information?

.se



Infrastruktur

- Hur ser företagets nätverk ut?
- Vilka in- och utgångar , nns i nätverket?
- Är nätet segmenterat, eller finns det externa tjänster på samma nätverk som det interna?
- Får anställda själva installera program i nätverket?
- Hur hanteras behörigheter och befogenheter?

.se



Det kan hända vem som helst!

- Skadlig kod
- Spoofing och identitetsstölder
- Stöld av datorer och information
- War Driving och annan avlyssning
- Hacking
- Dataförluster p.g.a. bristande säkerhet skopiering
- Ö .



.se



Grundläggande synsätt

- Riskanalys
- Säkerhetskrav
- Funktionell säkerhetslösning
- Teknisk säkerhetslösning



.se



Säkerhet är en process

- Reaktivt . förstå problemet och lös det
- Proaktivt . undvik problemet
- Hitta rotorsaken!
- Välkomna kritik som det första steget mot en förbättring . även om det betyder att du måste börja om från början



.se

Hur arbetar vi?

- Policy, ansvar, organisation
- Systematiskt säkerhetsarbete
- Kompetens
- Övervakning
- Regelbundna granskningar
- Säkerhetsåtgärder
- Tekniska lösningar



.se

Dokumentation enligt ISO/IEC 27001

Arbete pågår

Intern remiss

Klar

2008-08-04

A. Policy

Formuleras på en övergripande nivå och uttrycker ledningens vilja

Informations-Säkerhetspolicy för .SE 2004-49

Policy för krishantering 2005-1

Integritetspolicy 2008-12

Kvalitetspolicy 2008-11

B. Riktlinjer

Anger VAD som skall göras och pekar ut ansvar och mål

Grundskyddsnivå IT-säkerhet internt 2007-22

Grundskyddsnivå IT-säkerhet slavserverdrift

C. Anvisningar

Anger HUR skyddet ska införas och vilka säkerhetsåtgärder som ska vidtas

Systemsäkerhetsanalyser

Generella krav och villkor säkerhetskopiering 2008-6

Skalskydd och tillträdesskydd

Informationsklassificering 2006-7

Incidenthantering 2004-41

Plan för krishantering

Nätverk och brandväggar
BKS
NICEasy
Zondistribution

Brandskyddsdocumentation 2005-8
Besökshantering 2005-22
Hantering av larm

IT-säkerhet Anvisningar för förvaltning 2008-3

D. Instruktioner

Detaljerad information till anvisningarna

Informationssäkerhet Handbok för medarbetare 2005-6

IT-säkerhetsinstruktion standardplattform OS-basnivå 2008-4

Checklistor

Mallar

- Checklista vid hot 2006-2
- Checklista vid resor 2006-1
- Checklista vid nyanställning
- Akuta personalärenden

- Användarförbindelse 2005-7
- Mall för kvittering av lambricka
- Mall incidentrapport

.se



Frågor?

.se