Hva er vitsen med sikkerhetspolicies?

Ketil Stølen

Oslo 23. november 2006

Innhold

- Hva er en policy?
- En policy er ikke en …..
- Overordnet struktur for en policy
- Hvordan klassifiseres policyer?
- Tre policymodaliteter
- Hva er en sikkerhetspolicy?
- Hva er vitsen?

- Organisering av seminaret

Hva er en policy?

- Policyer er spesielle regler laget med det formål å regulere forhold ved en organisasjon eller ved et system innenfor en organisasjon.
- Disse reglene er typisk definert, implementert av håndhevet av organisasjonen selv.
- Et kjennetegn på en policy er at det som reguleres potensielt kan bryte med den.
- En policy beskriver hva som bør velges i en valgsituasjon.

En policy er ikke

- en retningslinje
  - En retningslinje er typisk en samling av systemspesifikke forslag til ”best praksis”
  - En retningslinje er ikke et krav (som hører hjemme i en policy) men mer en sterk anbefaling
- en standard
  - En standard er et dokument som beskriver viktige deler av et produkt, en tjeneste eller en arbeidsprosess
  - Standarder gir for eksempel løsninger på hvordan produkter bør fremstilles og hvordan systemer bør beskrives
  - Standarder er typisk mer generelle, og har et bredere domene enn policyer

En policy er ikke

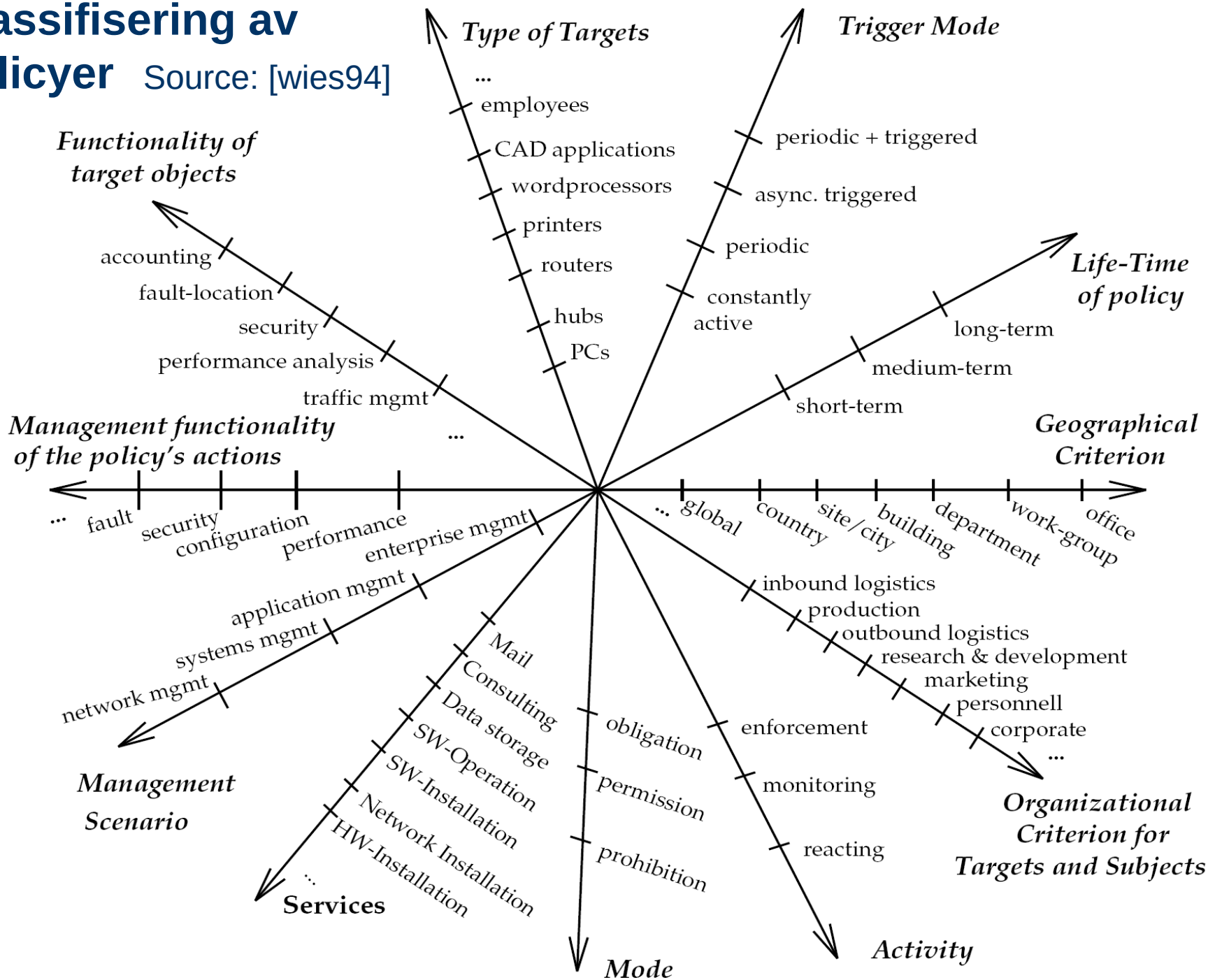
- en kravspesifikasjon
  - En kravspesifikasjon beskriver krav til et systems funksjonalitet, kvalitet etc.
  - En policy beskriver krav til hvordan systemet skal konfigureres, og hvordan det skal brukes
  - En policy implementeres på toppen av den vanlige funksjonaliteten
  - Det er implisitt at det som begrenses av policyen har potensial til å bryte med den

Struktur for et policydokument

1. Hensikt – formålet med policyen
2. Domene – avgrensning av dens gyldighetsområde
3. Policy – selve policybeskrivelsen
4. Håndhevelse – konsekvensen ved ikke å følge den
5. Definisjoner – viktig å definere sentrale begreper
6. Revisjonshistorie – en policy endrer seg over tid, og dette må dokumenteres

Se www.sans.org for maler

Klassifisering av policyer Source: [wies94]



Policymodaliteter

- Policyer klassifisere i henhold til tre modaliteter:
  - Forpliktelse: Karakteriserer betingelser under hvilke en spesiell oppførsel er påkrevd
  - Tillatelse: Karakteriserer betingelser under hvilke (en ellers forbudt) oppførsel er tillatt
  - Forbud: Karakteriserer betingelser under hvilke en spesiell oppførsel ikke tillates

Hva er en sikkerhetspolicy?

- Håndbok i Informasjonssikkerhet (http://helmersol.nr.no/haandbok/):
  - En sikkerhetspolicy definerer sikkerheten i en virksomhet. Alle generelle overordnede regler for håndtering av informasjon skal nedfestes i et policydokument.
  - En sikkerhetspolicy uttrykker hva og ikke hvordan.

- Informasjonssikkerhet (Datatilsynet):
  - Tiltak iverksatt for å sikre
    - at informasjon ikke er tilgjengelig uten autorisasjon (konfidensialitet),
    - at informasjon ikke uautorisert endres eller ødelegges (integritet), og
    - at informasjon er tilstede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (tilgjengelighet).

Policy på bruk av bærbare maskiner ved UiO - www.usit.uio.no/it/pc/sikkerhet/baerbare.html

- Maskinen skal kjøre minimum Windows 2000 - helst Windows XP
- Maskinen skal være innmeldt i domenet
- Maskinen skal ha en primær ip-adresse, enten i form av statisk dhcp , eller en fast adresse. Denne adressen er mest hensiktsmessig å ha på det nettet hvor brukeren oppholder seg mest. På andre nett kan maskinen kjøre vanlig dhcp, men enkelte ting i forhold til domenet vil da være problematisk.
- DNS-navn og nettbios-navn skal være det samme, når maskinen bruker sin primære ip-adresse.
- Brukeren skal ha en lokal konto på maskinen. Denne kontoen skal ha brukernavn på formen "brukernavn_loc".
  Passordet på den lokale kontoen skal **ikke** være det samme som på UiO kontoen.
  Denne kontoen bør ikke ha administrative rettigheter.
- Brukere som jevnlig trenger adminrettigheter anbefaler vi at får en lokal konto til på maskinen sin. Denne skal være på formatet "uiobrukernavn_adm" der uiobrukernavn er en gyldig UiO- brukerkonto. Det er viktig at den er på akkurat dette formatet for at daily skal kunne rapportere riktig.
- Hvorvidt brukeren skal ha administrator rettigheter eller ikke, må vurderes i hvert enkelt tilfelle av den lokale IT-ansvarlige.
- Maskinen skal settes opp med automatisk oppgradering (patching) via Windows update
- Maskinen skal kjøre antivirus programvare. F-secure Antivirus i hjemmemaskin-variant er å anbefale.

Hvorfor alt maset?

www.usit.uio.no/it/pc/sikkerhet/baerbare.html

- **Når det gjelder "brukernavnloc", er det flere grunner:**
  - Færre misforståelser:
    Når brukeren har skiftet passord på UiO-kontoen sin, slipper man misforståelser med hvorfor dette ikke fungerer på den bærbare.
  - Lettere for brukerne å holde orden på hvilke konti det er snakk om.
  - Enklere å hjelpe brukerne, siden man vet hvordan maskinen er organisert:
    Lokale IT-ansvarlige eller pcadm kan enkelt finne ut av om kontoen er lokal eller ikke, og dermed tenke i riktige baner med en gang,
    uten masse mail fram og tilbake.
  - UiO-brukerens passord skal ikke gis bort!:
    Man unngår situasjoner hvor brukeren ender opp med å gi bort sitt UiO-passord til familiemedlemmer og venner. Da er det bedre at det lokale passordet til maskinen blir gitt bort.
- **Når det gjelder hele ordningen generelt:**
  - Vi er klar over at det ofte er lite hensiktsmessig å ordne med alle disse tingene bare en gjesteprofessor skal ha maskinen sin på nett et par dager i måneden.
    Men to dager er nok i massevis dersom maskinen blir hacket og brukt som portal videre inn på UiO-nettet. Den beste løsningen er kanskje i slike tilfeller
    å ha en utlånsmaskin og legge filene folk har med seg over på denne. Er det en fast ansatt ved UiO som bare av og til er innom med sin bærbare,
    er det absolutt verdt å ha en fast ip-adresse dedikert til bare dette formålet, når alternativet er dårlig sikkerhet.

Hovedoppgave [Rot05]

- ”Denne oppgaven tok utgangspunkt i at policyer hadde minimal eller ingen effekt dersom de ikke ble utviklet og implementert som en del av et større sikkerhetsarbeide, dette ser ikke ut til å være tilfelle. Sannheten ser ut til å ligge nærmere at alt sikkerhetsarbeide er nyttig, og noe er bedre enn ingenting.”

Referanser

- [Wies94] Ren´e Wies. Policy Definition and Classification: Aspects, Criteria, and Examples. Proceeding of the IFIP/IEEE InternationalWorkshop on Distributed Systems: Operations & Management, Toulouse, France, 10 - 12 October 1994
- [Rot05] Britt Karin Rotmo. Har policyer noen effekt som enkeltstående sikkerhetsmekanismer? MSc-avhandling, Høyskolen på Gjøvik, 2005.

Policy for dette seminaret

- Hver foredragsholder har 20 minutter til rådighet
- Jeg reiser meg når det gjenstår 3 minutter
- Spørsmål stilles etter hvert foredrag
- Det er satt av 5 minutter til spørsmål og svar for hvert foredrag