Datasäkerhet och integritet

OH-9 v1

- Juridiska frågor
- Lagändringar i Sverige
- IT-säkerhetspolicy
- Metodverktyg & resurser
  - PAPAI
  - SBA m.m.

Juridiska frågor

- Tekniska och administrativa åtgärder bör genomföras på ett sätt som är förenligt med lagar, olika föreskrifter, avtal etc.
- Skilj mellan informationsobjekt och infrastruktur ur rättslig synvinkel
  - Tekniker och jurister tänker oftast i olika banor vad gäller dessa objekt
- Åtgärder som rör arbetstagare
  - Arbetsgivaren bestämmer säkerhetsnivån, det är därför viktigt att denne sätter upp tydliga regler för hur de anställda får använda IT-resurserna och dels hur företaget skall sköta sin datasäkerhet
- PUL (PersonUppgiftsLagen)
  - Bör konsulteras redan i ett tidigt skede av säkerhetsarbetet

PUL (PersonUppgiftsLagen)

- Ansvarig på företaget enligt PUL bör
  - Bestämma tydliga ändamål för personuppgiftsbehandlingar
  - Se till att behandlingar är relevanta
  - Informera de som behandlats
  - Gallra bort uppgifter som ej längre är relevanta
- Lagra personuppgifter kräver samtycke från arbetstagare
- PUL-ansvarig är skyldig att skydda personuppgifter mot utomstående åtkomst
- www.datainspektionen.se och www.regeringen.se
  - Rapport 2003:3 - Behandling av personuppgifter
  - Betänkande 2002:18 - Personlig integritet i arbetslivet

Straffrättsligt skydd

- PUL-ansvarig behöver veta
  - Vilket skydd ger lagstiftningen inom området mot obehörig åtkomst från arbetstagare eller utomstående?
  - Vilka kontroll och skyddsåtgärder kan företaget vidta utan att göra sig skyldigt till straffbart intrång, olovlig åtkomst till andras nät m.m.
- Förslag om persondataskydd regel från integritetsutredningen
  - Arbetsgivare får ej läsa privat e-post etc.
- Det är viktigt att informera och involvera arbetstagarna/facket i säkerhetsarbetet så man får de **med** sig och inte **mot** sig

Lagändringar i Sverige

- På senaste tiden har många lagändringar skett i Sverige (EU-beslut etc.) för att kunna bekämpa terrorism och organiserad brottslighet.
  - I december 2005 röstade Europaparlamentet igenom lagstiftning om obligatorisk lagring i 6-24 månader av information om alla människors ringande, e-postande, SMS:ande liksom viss information om Internetanvändning.
  - Hemlig telefonavlyssning tillåten i stor skala, även överskottsinformation m.m. m.m.
- Många menar att vi är på väg mot ett övervakarsamhälle där stora risker finns för missbruk av uppgifter som kränker integriteten
  - ”Bodströmsamhället” (http://bodstrom.omfg.se)
  - Säkerhetspolisen (www.sakerhetspolisen.se)
    - Rubriken: Utredningar som berör oss
  - Många företag har systematisk övervakning via programvaror (mönsterigenkänning) av sina anställda
- Läs mer om allt detta på: www.stoppastorebror.se

IT-säkerhetspolicy

- IT-säkerhet sid 277
  - Säkerhet – produkter, tjänster, organisation och
  - IT-resurser
    - Hårdvara, systemprogram, tillämpningar, datainformation
- Bevara
  - Tillgänglighet – för auktoriserade användare, svarstid
  - Integritet – förändringar genomförs på ett auktoriserat sätt
  - Sekretess – endast auktoriserad åtkomst
- Företagets högsta ledning ansvarar för att en säkerhetspolicy finns
  - IT-chef/IT-säkerhetschef är ansvariga för att upprätthålla den
  - Tjänsteägarna är kravställare mot systemägarna

IT-säkerhetspolicy

- Effektiv IT-säkerhet kan enbart införas då hotbild, svagheterna och sårbarhet är kända
  - Hot + svaghet + sårbarhet = hotbild
- **Hot** – är någon form av handling eller händelse som kan skada företagets IT-resurser
  - Fysiska, logiska, mänskliga hot etc.
  - Hot-tabeller med påverkan för t.ex. tillgänglighet, integritet, sekretess etc. kan minska komplexiteten
- **Svaghet** – benämningen för en IT-resurs tekniska utformning med kända/okända brister, kan även vara bristande beredskap, rutiner etc.
- **Sårbarhet** – är benämningen för hur utsatt en IT-resurs är genom sannolika hot och kända svagheter

IT-säkerhetspolicy

- Motåtgärder
  - Fysiska - redundans
  - Logiska – behörigheter, virusskydd
  - Administrativa – tydliga regler/organisation etc.
- Säkerhetsnivåer (exempel)
  - Ingen skada – resurser som man kan avvara
  - Liten skada – resurser som märks, billigt
  - Skada – resurser som ej är kritiska, kostar en del
  - Allvarlig skada – kritiska resurser, mycket kostsamt
  - Mycket allvarlig skada – mycket vitala resurser

IT-säkerhetspolicy

- Tabeller med motåtgärder kan skapas för varje säkerhetsnivå, se sid. 282-283
- Allmänna motåtgärder (måste finnas impl.)
  - Identifiering och autentisering
  - Spårbarhet (loggning)
  - Åtkomstkontroll
- Säkerhetsnivåer och teknikområden
  - Lokala nätverket
  - Fjärrförbindelser
  - Servrar och klienter
  - Distribuerade tillämpningar
  - Gemensam IT

IT-säkerhetspolicy

- Exempel på enkel modell för hot-identifiering inom varje teknikområde
- **Lokalt nätverk** - kan delas upp i två delar - fysiska nätet och logiska nätverket (protokoll)
  - Exempel på tabell s287 för olika nätverksprotokoll och dess påverkan på säkerheten
- Begreppet säkerhetsdomäner
  - Kommunikation uppåt i säkerhets-hiearkin är ej tillåten default (bestäms av den högre nivån)
  - Exempel på motåtgärders-tabeller för de 5 olika säkerhetsnivåerna sid. 289 - 291

IT-säkerhetspolicy

- Kända hot och svagheter för **lokalt nätverk** bör detaljspecificeras av systemägaren
  - Fysiska hot och svagheter
    - Komponentfel, mänskliga faktorn etc.
  - Logiska hot och svagheter
    - Obehörig inloggning eller åtkomst till nätverket
  - Administrativa hot och svagheter
    - Användare får felaktiga åtkomsträttigheter

IT-säkerhetspolicy

- **Fjärrförbindelser**
  - Uppringda förbindelser
  - VPN-förbindelser
  - Fasta förbindelser
  - Telefon- eller faxförbindelse
- Tabell för vilka hot/svagheter som förekommer s293
- Tabell (s294 – 295) för olika motåtgärder i de 5 olika säkerhetsnivåerna (inneh. som tid. följ. kolumner)
  - Generella och specifika motåtgärder
  - Vad skyddas inte
  - Konsekvenser
  - Kostnad

IT-säkerhetspolicy

- Kända hot och svagheter för **fjärrförbindelser** bör detaljspecificeras av systemägaren
  - Fysiska hot och svagheter
    - Avgrävd kabel, systemhaveri hos leverantör
  - Logiska hot och svagheter
    - Avlyssning av telefoni/fax, felaktiga nummer
  - Administrativa hot och svagheter
    - Obehörig installation

IT-säkerhetspolicy

- **Server**
  - Många olika hårdvaru- och OS plattformar
  - Hitta duktiga systemadministratörer som kan säkra OS plattformarna genom kompetens
- Tabell för olika motåtgärder i de 5 olika säkerhetsnivåerna s297-298
  - Generella och specifika motåtgärder
  - Vad skyddas inte
  - Konsekvenser
  - Kostnad

IT-säkerhetspolicy

- Kända hot och svagheter för **server** bör detaljspecificeras av systemägaren
  - Fysiska hot och svagheter
    - Miljö (brand, strömavbrott)
    - Olika hårdvarufel
    - Obehörig fysisk åtkomst
  - Logiska hot och svagheter
    - Obehörig åtkomst/inlogging
    - Manipulering av data
    - Införande av skadlig kod
  - Administrativa hot och svagheter
    - Inga brister får finnas i ansvarsfördelning och privilegier

IT-säkerhetspolicy

- **Klienter**
  - Många olika miljöer finns både tekniskt (nätverkstyp, datortyp etc.) och fysiskt (mobil, stationär etc.)
- Tabell för olika motåtgärder i de 5 olika säkerhetsnivåerna s300 - 302
  - Generella och specifika motåtgärder, vad skyddas inte, konsekvenser, kostnad
- Extra säkerhetsnivå för mobila arbetsplatser
  - Kryptering, PIN-kod etc.

IT-säkerhetspolicy

- Kända hot och svagheter för **klienter** bör detaljspecificeras av systemägaren och liknar server
  - Fysiska hot och svagheter
    - Miljö (brand, strömavbrott)
    - Olika hårdvarufel
    - Obehörig fysisk åtkomst
  - Logiska hot och svagheter
    - Obehörig åtkomst/inlogging
    - Manipulering av data
    - Införande av skadlig kod
  - Administrativa hot och svagheter
    - Att någon avviker från de enhetliga standards som gäller för arbetsplatsen

IT-säkerhetspolicy

- **Distribuerade tillämpningar**
  - Nätverksapplikationer – Två oberoende delar (klient och server)
  - Avgränsa vilka tjänster som skall vara med som distribuerad tillämpning
  - Varje tjänst för sig?
- Tabell för olika motåtgärder i de 5 olika säkerhetsnivåerna s304 - 306
  - Generella och specifika motåtgärder, vad skyddas inte, konsekvenser, kostnad

IT-säkerhetspolicy

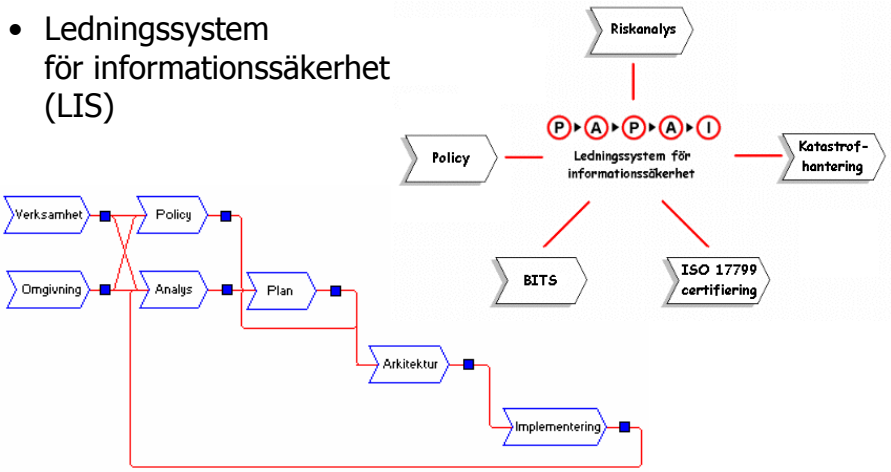
- Kända hot och svagheter för **distribuerade tillämpningar** bör detaljspecificeras av systemägaren
  - Fysiska hot och svagheter
    - Obehörig påverkan
  - Logiska hot och svagheter
    - Obehörig åtkomst/inlogging
    - Manipulering av data
    - Införande av skadlig kod
  - Administrativa hot och svagheter
    - Samma som för servrar och klienter

IT-säkerhetspolicy

- **Gemensam IT**
  - Systemen är inte isolerade företeelser!
  - Ett heltäckande angreppssätt krävs
  - Syftet är att hitta gemensamma balansen för säkerhetsnivå med bibehållen funktionalitet
  - Alltså få system som harmoniserar med varandra!
- Tabell för olika motåtgärder i de 5 olika säkerhetsnivåerna s307 - 310
  - Generella och specifika motåtgärder
  - Vad skyddas inte
  - Konsekvenser
  - Kostnad

PAPAI (Policy - Analys - Plan - Arkitektur - Implementering)

- Ledningssystem för informationssäkerhet (LIS)



PAPAI

www.mixtum.se

Verksamhet
Allt säkerhetsarbete måste utgå från verksamhetens krav. Därför är det nödvändigt att kartlägga alla informationstillgångar och vilka krav som ställs på dessa t.ex. i fråga om sekretess, riktighet och tillgänglighet.

Omgivning
På samma sätt måste omgivningen kartläggas för att identifiera den hotbild som organisationen står inför.

Säkerhetspolicy
Organisationens mål och visioner med informationssäkerhetsarbetet beskrivs i en policy. Den övergripande säkerhetspolicyn skall hållas kort och får ej innehålla tekniska detaljer för att den skall kunna leva många år utan förändring. Detaljerna utarbetas sedan i områdesspecifika policies, riktlinjer, instruktioner etc.

Riskanalys
Analys är kärnan i säkerhetsarbetet. Här identifieras vilken påverkan hoten har mot organisationens informationstillgångar. Man skapar sig en uppfattning om de risker man utsätts för och tar fram förslag till åtgärder inför planarbetet.

PAPAI

www.mixtum.se

Säkerhetsplan

I planen fördelas resurser så att policyn kan förverkligas. Med utgångspunkt från policies och resultaten från riskanalysen initieras olika säkerhetshöjande aktiviteter som
- säkerhetsutbildningar
- framtagning av riktlinjer och instruktioner
- utveckling av incident- och katastrofhantering
- revision och uppföljning

Säkerhetsarkitektur

På arkitekturnivån närmar vi oss tekniken men på ett produktoberoende sätt. Här väljs den kombination av olika tekniker som ger de bästa egenskaperna i organisationens infrastruktur och IT-system.

Implementering

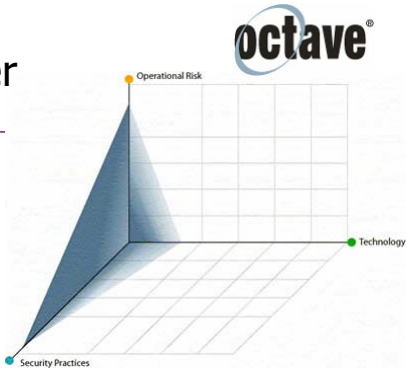
Först när vi kommer hit till den lägsta nivån intresserar vi oss för produkter och deras egenskaper. Innan vi väljer säkerhetsprodukt måste vi gjort klart hela säkerhetsarbetet. Det är ingen mening med att skaffa säkerhetsprodukter utan att dessförinnan ha analyserat vad som är skyddsvärt och på vilket sätt det skall skyddas. Här ägnar vi oss också åt praktiska säkerhetsdetaljer i den dagliga driften.

SBA metoden (Dataföreningen)

www.dfs.se/products/sba/

- Är mer ett koncept där man tittar på analys och säkerhetsarbete inom datarelaterade affärsområden
  - Man utgår från en ”human model”, dvs. expertkunskap hos medarbetare vilket resulterat i en programsvit
- SBA Check
  - Verktyg för nulägesanalys av informationssäkerheten
- SBA Project
  - Analysverktyg för att tidigt identifiera tänkbara risker med ett projekt
- SBA Scenario
  - En metod och verktyg för att värdera och analysera framtida risker och hot i verksamheten
- SBA Virusvarning & helsäkert
  - Utbildningspaket för datoranvändare

Mer resurser



- Center of Internet security expertise (CERT)
  - http://www.cert.org/
  - OCTAVE - http://www.cert.org/octave/
- The SANS Security Policy Project
  - http://www.sans.org/resources/policies
  - Essential Security Actions Step-by-Step, mallar etc.
- Internet Security Policy: A technical Guide
  - www.rxn.com/services/faq/internet/ISPTG.html
- Utdrag ur Säkerhet & Sekretess
  - http://arkiv.idg.se/pdfdownload/free/?item=13990