# IdM-checklista

För att upprätta förtroende i en federation krävs inte bara att identitetsutdelningsprocessen uppfyller vissa krav. Exempelvis är det viktigt att

man har förtroende för att ingen oriktigt kan tillägna sig andras identitet.I det sammanhanget blir det också viktigt att man har förtroende för

att alla delar av identitetshanteringen sköts på ett sätt som minimerar risken för intrång och identitetsstöld och att man har en fungerande

process för återställning om intrång ändå skulle ske. IdM-checklistan är ett försök att fastställa ”Best Practice” för drift av de miljöer där

identitetshanteringens olika delar residerar. I listan nedan finns också

exempel för de olika kraven.

# Checklistans användningsområde

- Vid revision av IdP hos en SWAMID-medlem
- Som dokumentation för revision vid LA2 och LA3
- Vid ansökan om medlemskap i SWAMID
- Vid kartläggning i samband med dataintrång (Sunet CERT)

# Systemadministration allmänt

- **System- och maskinbeskrivning ska finnas över autenticieringssystemets ingående komponenter.**
  *Detta skall bland annat beskriva dataflödet mellan ingående komponenter, speciellt med avseende på hur användare är definierade på olika nivåer och vilket/vilka system som är källan till/äger denna information.*
- **Ingående datorer/system ska ha utsedd(a) ansvarig(a) systemadministratörer**.
  *Vid exempelvis en incident skall det klart gå att se vilka som är ansvariga för driften respektive har systemkonton på de komponenter som ingår i autenticieringssystemet.*
- **Systemen ska förvaras i en säker fysisk miljö, t ex en datorhall med lås, larm etc**.
  *Det skall inte finnas någon risk att obehöriga får fysisk tillgång till berörda datorer. Driften skall vara säkerställde enligt etblerade, beskrivana processer. I och med att identiteter kan nyttjas även på andra högskolor, kan även dessa drabbas vid driftproblem.*
- **IdP:n och bakomliggande system skall köras på separata maskiner. Dessa skall inte ha orelaterade tjänster**.
  *Exempelvis skall inte IdP:n köras på samma maskin(er) som webbservrar, databaser etc. IdP:n (som är riskexponerad) skall inte köras på samma maskin som bakomliggande system. Dedikerad hårdvara eller motsvarande lösning med adekvat säkerhet bör användas.*
- **Hårdvara som tas ur drift ska destrueras på ett korrekt sätt**.
  *Diskar och andra permanenta lagringsmedia skall destrueras fysiskt under säkra former, alternativt skrivas över på ett säkert sätt. (exempelvis med hjälp av DBAN eller ATA 'Security Erase').*

# Nätverk och omgivande system

- **Nätverket skall vara segmenterat så att berörda IdP och bakomliggande system sitter på separat segment**.
  *Detta för att minska riskexponeringen om intrång skulle inträffa på andra system.*
- **För att möjliggöra undersökning av incident/driftstörning skall det finnas trafikloggar ('Netflow' eller motsvarande).**
  *Avsikten är att man ska kunna få en oberoende bild av vad som inträffat.*
- **För undvikande av dns-problem, ska mer än en central dnsserver vara konfigurerad.**
  *Åtminstone en av dessa bör vara belägen utanför högskolans nät. Dnssec bör användas.*
- **Det ska finnas routerfilter(motsv) som begränsar åtkomst till systemen till relevanta portar från relevanta ipnummer/nät**.
  *Motsvarande filter bör även finnas på aktuella servrar ('djupförsvar').*

# Loggning, återställning och övervakning

- **Ingående system ska vara konfigurerade så att säkerhetsrelevant information loggas. Loggar ska sparas på lämpligt sätt så att de finns tillgängliga fastställd period, minst 6 månader. Loggar skall endast vara åtkomliga för utsedda personer**.
  *Exempel på säkerhetsrelevanta loggar är applikationsloggar samt accessloggar på OS-nivå.*
- **Förutom servrarnas lokala loggning ska samtidig loggning på central säker server utnyttjas, exempelvis via syslog.**
  *Vid en incident är det vanligt att serverloggar raderas. Därför skall oberoende loggar finnas.*
- **Rutiner ska finnas för fortlöpande kontroll av relevanta loggar.**
  *Loggar skall rutinmässigt granskas på lämpligt sätt i syfte att tidigt upptäcka intrång eller driftsproblem.*
- **För att säkerställa att loggar visar rätt tid, skall synkroniserade tidsservrar utnyttjas, alternativt annan metod som ger motsvarande funktion**.
- **Det ska finnas rutiner för regelbunden säkerhetskopiering**.
  *Man skall åtminstone säkerhetskopiera loggfiler, konfigurationsfiler, IdP-data. Säkerhetskopior som innehåller lösenord skall vara krypterade. Lösenord för backupper skall finnas sparade på lämpligt sätt (kassaskåp eller motsvarande). Rutiner skall finnas för test av återställning.*

# Härdning, uppsäkring mm

- **Det ska finnas rutiner för att regelbundet följa upp att säkerhetspatchar installerats, och att systemet i övrigt är korrekt konfigurerat.**
  *Operativsystem och program som ej underhålls av leverantören med avseende på säkerhetspatchar får ej användas.*
- **Tjänster som EJ används ska inte vara aktiverade**.
  *Varje tjänst innebär en exponering. Onödiga sådana skall undvikas.*
- **Tjänster som används ska vara säkra och korrekt uppsatta**.
  *Tjänster kan behöva konfigureras för att bli säkra. Konfigurationer skall dokumenteras.*
- **Osäkra tjänster får EJ vara aktiverade**.
  *Exempel på sådana tjänster är netbios, NFS, telnet.*

# Säker hantering av användarID, lösenord och motsvarande

- **Lösenord ska vara av tillfredsställande kvalitet och ska inte överföras i klartext**.
  *För AL1 krävs en entropi på 1024 (2^10) och för AL2 16384 (2^14). Lösenord för administration skall vara av minst samma kvalitet som de lösenord som administreras. Någon form av ratelimit bör användas för att försvåra lösenordsattacker. Se: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf samt http://www.idmanagement.gov/documents/CommonCAP.xls*
- **Det ska finnas rutiner för hantering av administrativa konton. Administrativ åtkomst skall begränsas till så få personer som möjligt**.
  *Vilka som har administrativ åtkomst skall dokumenteras och det skall finnas rutiner för rensning av inaktuella konton.*
- **Trafiken mot IdP:er och underliggande system skall vara krypterad**.
  *Servercertifikat skall användas med en nyckellängd motsvarande minst RSA 2048 och nyckeln skall bytas minst vart tredje år. Jämför basprofilen samt NIST SP 800-57. Privata nycklar med tillhörande lösenord skall förvaras säkert.*
- **För administration av ingående komponenter bör 2-faktorautenticiering eller konsol användas**.
  *Som ovan: Administrativ påloggning skall vara av minst samma säkerhet som de administrerade objekten*