Checklista Identitetshanteringssystem för SWAMID 2.0

Utarbetad tillsammans med SUNET CERT och SUSEC

Bakgrund

- För att upprätta fortroende 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

Checklistans olika avsnitt

- Systemadministration allmänt
- Nätverk och omgivande system
- Loggning, återställning och övervakning
- Härdning, uppsäkring mm
- Säker hantering av identitetsuppgifter

- Checklistan har varit ute på remiss och i huvudsak har den mött god respons, dock krävs genomgående mer utförliga förklaringar

Systemadministration allmänt

- System- och maskinbeskrivning ska finnas över autenticieringssystemets ingående komponenter.
- Ingående datorer/system ska ha utsedda ansvarig(a) systemadministratörer.
- Systemen ska förvaras i en säker fysisk miljö, t ex en datorhall med lås, larm etc.
- IdP:n ska köras på en separat maskin. Bakomliggande system skall inte köras på samma maskiner som har orelaterade tjänster. *(BÖR OMFORMULERAS!)*
- Hårdvara som tas ur drift ska destrueras på ett korrekt sätt.

Nätverk och omgivande system

- Nätverket skall vara segmenterat så att berörda datorer sitter på separat(a) segment.
- För att möjliggöra undersökning av incidenter skall det finnas netflowloggar (motsvarande).
- För undvikande av dns-problem, ska mer än en dnsserver vara konfigurerad.
- Det ska finnas routerfilter(motsv) som begränsar åtkomst till systemen till relevanta portar från relevanta ipnummer/nät.

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 i minst 6 månader.
- Förutom lokal loggning ska samtidig loggning extern/central säker syslogserver utnyttjas.
- Rutiner ska finnas för fortlöpande kontroll av relevanta loggar.
- För att säkerställa att loggar visar rätt tid, skall synkroniserade tidsservrar utnyttjas.
- Det ska finnas rutiner för regelbunden säkerhetskopiering.

Härdning, uppsäkring mm

- Det ska finnas rutiner för att regelbundet följa upp att säkerhetspatchar installerats, och att systemet i övrigt är korrekt konfigurerat. M.a.p. säkerhetspatchar får osupportade operativsystem och program ej användas.
- Tjänster som EJ används ska inte vara aktiverade.
- Tjänster som används ska vara säkra och korrekt uppsatta.
- Osäkra tjänster som netbios, NFS får EJ vara aktiverade.

Säker hantering av identitetsuppgifter

- Lösenord ska vara av tillfredsställande kvalitet och ska inte överföras i klartext.
- Det ska finnas rutiner för hantering av administrativa konton. Administrativ åtkomst skall begränsas till så få personer som möjligt.
- Trafiken mot IdP:er och underliggande system skall vara krypterad.
- För administration av ingående komponenter bör 2faktorspåloggning eller konsol användas