Checklista Identitetshanteringssystem för SWAMID 2.0

Utarbetad tillsammans med SUNET CERT och SUSEC

Bakgrund

- 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

Checklistans olika avsnitt

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

Checklistans användningsområde

- Checklistan skall användas vid följande tillfällen:

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

Systemadministration allmänt

1.1 **System- och maskinbeskrivning ska finnas över autenticieringssystemets ingående komponenter.**

Detta ska bl.a. beskriva dataflödet mellan ingående komponenter, speciellt med hur användare är definierade på olika nivåer och vilket/a system som är källan till/äger denna information.

1.2 **Ingående datorer/system ska ha utsedda ansvarig(a) systemadministratörer.**

Vid exempelvis en incident ska det klart gå att se vilka som är ansvariga för driften respektive har systemkonton på i autenticieringssystemet ingående komponenter.

1.3 **Systemen ska förvaras i en säker fysisk miljö, t ex en datorhall med lås, larm etc.**

Det ska således inte finnas någon risk att obehöriga får fysisk tillgång till berörda datorer. Driften skall vara säkerställd. I och med att identiteter kan nyttjas även på andra högskolor så kan även dessa drabbas vid driftproblem.

Systemadministration allmänt (forts)

1.4 **IdP:n och bakomliggande system ska köras på en separata maskiner. Dessa ska inte ha orelaterade tjänster.**

Som exempel ska IdP:n inte köras på samma maskin(er) som webbservrar, databaser etc. IdP:n (som är riskexponerad) ska inte köras på samma maskin som bakomliggande system. Dedikerad hårdvara bör användas.

1.5 **Hårdvara som tas ur drift ska destrueras på ett korrekt sätt.**

Diskar ska destrueras fysiskt under säkra former, alternativt skrivas över på ett säkert sätt (exempelvis mha DBAN eller ATA 'security erase').

Nätverk och omgivande system

2.1 Nätverket skall vara segmenterat så att IdP och bakomliggande system sitter på separat segment.

Detta för att minska riskexponeringen om ett intrång skulle inträffa på andra system.

2.2 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.

2.3 För undvikande av dns-problem, ska mer än en central dnsserver vara konfigurerad.

Åtminstone en av dessa bör vara belägen utanför högskolans nät.

2.4 Det ska finnas routerfilter(motsv) som begränsar åtkomst till systemen till relevanta portar från relevanta ipnummer/nät.

Motsvarande filter bör finnas även på aktuella servrar (djupförsvar).

Loggning, återställning och övervakning

3.1 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.

Exempel på säkerhetsrelevanta loggar är applikationsloggar samt accessloggar på OS-nivå.

3.2 Förutom servrarnas lokala loggning ska samtidig loggning på central säker syslogserver utnyttjas.

Vid en incident är det vanligt att serverloggar raderas. Därför ska oberoende loggar finnas.

3.3 Rutiner ska finnas för fortlöpande kontroll av relevanta loggar.

Loggar ska rutinmässigt granskas på lämpligt sätt i syfte att tidigt upptäcka intrång eller driftproblem.

Loggning, återställning och övervakning forts.

3.4 För att säkerställa att loggar visar rätt tid, skall synkroniserade centrala tidsservrar utnyttjas, alternativt annan metod som ger motsvarande funktion.

3.5 Det ska finnas rutiner för regelbunden säkerhetskopiering av (minst) loggfiler, konfigurationsfiler, IdP-data. Säkerhetskopior som innehåller lösenord bör vara krypterade. Rutiner ska finnas för test av återställning.

Inga kommentarer behövs här.

Härdning, uppsäkring mm

4.1 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 m.a.p.säkerhetspatchar får ej användas.

4.2 Tjänster som EJ används ska inte vara aktiverade.

Varje tjänst innebär en exponering. Onödiga sådana skall undvikas.

4.3 Tjänster som används ska vara säkra och korrekt uppsatta.

Tjänster kan behövas konfigureras för att bli säkra.

4.4 Osäkra tjänster får EJ vara aktiverade.

Exempelvis netbios, NFS, telnet.

Säker hantering av identitetsuppgifter

5.1 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 (10^14).

Lösenord för administration skall vara av minst samma kvalitet som de lösenord som administreras.
Se: **http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf**
samt **http://www.idmanagement.gov/documents/CommonCAP.xls**

5.2 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.

5.3 Trafiken mot IdP:er och bakomliggande system skall vara krypterad.

5.4 För administration av ingående komponenter bör 2-faktorautenticiering eller konsol användas.

Som ovan: administrativ påloggning ska vara av minst samma säkerhet som de säkraste administrerade objekten.

Kommentarer?