SWAMID

SWAMID Identity Assurance Level 1 Profile

SWAMID

- SWAMID AL1 – ger oss en starkare gemensam grund
- SWAMID AL1 är fortfarande en s.k. obekräftad användare, dvs mycket låg säkerhet i att det är rätt person.
- Dagens hantering av identiteter är ”spretig”. Genom AL1 ställer SWAMID gemensamma krav – krav som är högre än nuvarande BAS-profil.
- Vi förbereder för SWAMID AL2 – vissa vitala delar är gemensamma såsom lösenordshanteringen.

SWAMID

- SWAMID Identity Assurance Level 1 Profile är SWAMIDs nya obligatoriska basprofil SWAMID BoT har beslutat att SWAMID AL1 ersätter nuvarande basprofil från och med december 2014

- SWAMID Identity Assurance Level 2 Profile kommer att vara en frivillig utökad profil SWAMID AL2 kommer att färdigställas under våren 2014

- Vissa tjänster kommer att kräva SWAMID AL2

- SWAMIDs nya basprofil bygger på Kantara AL1 och är verifierad att den håller samma nivå av kantaraauktoriserad IT-revisor.
- SWAMID AL1 är uppdelad i olika delar:
- Organisationella krav
- Användarregler och strukturerad tjänstebeskrivning
- Identitetshantering (motsv. obekräftad användare)
- Lösenord
- Tekniska krav
- Revision

SWAMID

SWAMID template Password Policy

- SWAMID template Password Policy är skriven för att uppfylla både SWAMID AL1 och kommande SWAMID AL2
- De största skillnaderna mellan kraven i AL1 och kommande AL2 när det gäller lösenord
  - kravet på begränsa antalet gissningsförsök genom tekniskt stöd
  - kravet på att byta lösenordet med jämna mellanrum

Strategier för bättre inloggningsskydd

- Använd teknikstöd för god lösenordskvalitet och säker lösenordshantering
- Använd skiktad inloggningssäkerhet för att förbättra skyddet, gärna tre nivåer
  - Använd en basnivå för de flesta tjänsterna
  - För system med högre teknisk risknivå, t.ex. eduroam, använd annat lösenord, och ev. användarnamn, än ni använder i övrigt
  - För system med högre krav på åtkomst använd inte bara lösenord utan både något man har och vet, s.k. tvåfaktorsinloggning

Inledning

- Det finns två primära faktorer för att definiera hur bra ett lösenord är:
  - Lösenordskvalité: Genomsnittsligt antal gissningar innan en angripare behöver genomföra att hitta det rätta lösenordet
  - Lösenordsskydd: Hur snabbt och enkelt en angripare kan genomföra gissningsattack för varje enskilt lösenord

Lösenordskvalitet

- Ett lösenord ska minst vara sammansatt på följande sätt:
  - bestå av minst 8 tecken
  - vara sammansatt av följande tecken:
    - A – Z
    - a – z
    - 0 – 9
    - mellanslag *(räknas inte in i komplexitet)*
    - Specialtecken *(alla 7-bitars specialtecken ska vara tillåtna)*
  - Innehålla minst en versal, minst en gemen och antingen minst ett specialtecken eller en siffra

Lösenordskvalitet

- Vid lösenordsbyte ska lösenordet
  - vara sammansatta enligt föregående bild
  - inte vara detsamma som närmast föregående
  - *inte återfinnas i en katalog med lösenord av dålig kvalitet**
  - *inte vara samma som användarens övriga lösenord vid lärosätet**

  ** Alla inloggningssystem klarar inte av detta. För att bibehålla motsvarande risknivå öka minimalt antal tecken i lösenordet till 10.*

- Uppmana användaren att inte använda lösenord som de använder i andra IT-tjänster

Lösenordsskydd

- Skydd mot nätbaserade gissningsattacker ska finnas (Rate limiting):
  - 10 felaktiga gissningar innan automatisk kontolåsning
  - 5 minuters automatisk kontolåsning efter maximalt antal felaktiga gissningar
  - Räknaren över antalet felaktiga gissningar nollställs efter korrekt inloggning eller efter 60 minuter efter senaste felaktiga inloggningsförsök

Lösenordsskydd

- Följande stöd för lösenordsbyte ska finnas:
  - Alla användare måste kunna byta lösenord
  - Alla lösenord måste bytas med jämna mellanrum, t.ex. var femte år för studenter och vartannat år för övriga
  - Alla lösenordsbyten måste vara historiskt spårbara

Lösenordsskydd

- Datalagring och transport av lösenord
  - Lösenord ska alltid lagras och transporteras i krypterad form, gäller även backupmedia
  - Lösenord ska aldrig presenteras i läsbar form
  - Lösenord ska aldrig kommuniceras via epost, telefon eller motsv.
  - IT-personal med teknisk åtkomst till de datorer och datamedia där lösenord lagras ska underteckna särskilda ansvarsförbindelser. En uppdaterad lista ska finnas vid den organisation som sköter driften av systemet *(följer av MSBFS 2009:10)*

Till sist…

- Frågor?
  - Fråga oss nu…
  - Skicka epost till SWAMID Operations eller
  - ring någon i SWAMID Operations och fråga!
- Mer information på SWAMIDs Wiki:
  - SWAMID template Password Policy
    - https://wiki.swamid.se/display/SWAMID/SWAMID+template+Password+Policy
  - SWAMID Identity Assurance Level 1 Profile
    - https://wiki.swamid.se/display/SWAMID/SWAMID+Identity+Assurance+Level+1+Profile

Nästa SWAMID Workshop

Workshop 1 2014

17-18 mars i Uppsala

https://wiki.swamid.se/display/SWAMID/Workshop+1+2014

Kom gärna med förslag och idéer på frågor att diskutera dag 2.