UPPSALA UNIVERSITET

Dnr UFV 2013/1490

Riktlinjer för informationssäkerhet vid Uppsala universitet

Lösenordshantering

Fastställd av Säkerhetschef 2013-11-06

Innehållsförteckning

1 Inledning

Detta dokument anger Uppsala universitets riktlinjer för kvalitet på samt hantering av lösenord i enlighet med identitetsfederationen SWAMIDs policy [1].

2 Ansvar

Som användare av universitetets informationssystem ansvarar du själv för

- att dina lösenord uppfyller den kvalitet och hantering som anges i dessa riktlinjer.
- att du håller dina lösenord hemliga.
- att, som en del av ovanstående punkt, aldrig uppge dina lösenord till någon som efterfrågar dem via e-post, i telefon eller på annat sätt.

För system som är kopplade till universitetets gemensamma inloggnings- och autentiseringsrutiner (*Gemensam webbinloggning* och *Active Directory*) finns systemstöd för efterlevnad av riktlinjerna.

För system med egen lösenordshantering är det Objekt- eller Systemägare som ansvarar för efterlevnad av dessa riktlinjer inom sitt objekt/system.

3 Definitioner

Lösenordskvalitet. God lösenordskvalitet innebär att ett lösenord är tillräckligt långt och komplext sammansatt för att reducera risken för att en inkräktare kan gissa sig till rätt lösenord. Två saker avgör svårigheten i att gissa ett lösenord: längden och komplexiteten på lösenordet. Med hjälp av dessa kan man räkna ut lösenordets entropi [2]. Ju högre entropi ett lösenord har desto svårare är det att gissa det. Lösenordsentropi räknas i bitar och enligt följande formel från *NIST SP 800-63 bil. A:*

- Första tecknet ger fyra bitar.
- Tecken 2 till 8 ger 2 bitar.
- Tecken 9 till 20 ger 1,5 bitar.
- Tecken 21 och uppåt ger 1 bit.
- Ett tillägg om 6 bitar fås om lösenorden är komplexa, dvs. lösenordet innehåller minst en versal, minst en gemen och antingen minst en siffra och ett specialtecken.
- Ett tillägg om 6 bitar fås om omfattande ordlistekontroll sker så länge lösenordet inte överstiger 20 tecken.

Se pkt. 6.1 för vidare information.

Lösenordsskydd. Säker lösenordshantering innebär, förutom att varje användare ansvarar för att hålla sina lösenord hemliga, att inloggningstjänsten skyddar lösenord från otillbörlig åtkomst och användning. Se pkt. 6.2 för vidare instruktioner.

Tvåfaktorautentisering. Identitetskontroll (autentisering) med två skilda faktorer; ”något man vet” (t.ex. ett lösenord) och ”något man har” (t.ex. ett kort).

[1] http://www.swamid.se/11/policy/swamid-2.0.html

[2] Begreppet entropi används inom informationsteorin som ett mått på sannolikheten för ett visst informationsinnehåll i ett meddelande.

4 Syfte

Det övergripande syftet med dessa riktlinjer är att så långt det är möjligt skydda universitetets lösenordsskyddade informationssystem från obehöriga användare.

5 Strategier

Alla informationssystem (applikationer) ska vara kopplade till universitetets gemensamma inloggningstjänst [3] om inte särskilda skäl föreligger.

Universitetets gemensamma inloggningstjänst innehåller teknikstöd för god lösenordskvalitet och säker lösenordshantering, se pkt. 6.1 och 6.2.

Varje användare har ett masterlösenord (A-lösenord) för inloggning till universitetets nätverkstjänster. För inloggning till vissa universitetsgemensamma IT-tjänster som t.ex. det trådlösa nätverket [4] har varje användare dessutom ytterligare ett lösenord. Därutöver kan verksamhets- och/eller systemspecifika lösenord finnas.

Tvåfaktorautentisering ska användas för åtkomst till IT-tjänster eller system (applikationer) som enligt universitetets riktlinjer för informationsklassificering innehåller konfidentiell information med HÖGA eller SÄRSKILDA KRAV på att skydda informationen från obehöriga användare

6 Omfattning

Riktlinjerna för lösenordshantering gäller för alla IT-tjänster och system (applikationer) vid universitetet.

Riktlinjerna omfattar två områden, *lösenordskvalite*t och *lösenordsskydd*.

6.1 Lösenordskvalitet

6.1.1 Lösenordssammansättning

Ett lösenord ska vara sammansatt på följande sätt:

- Bestå av minst 10 tecken.
- Vara sammansatt av följande tecken:
  - A – Z
  - a – z
  - 0 – 9
  - mellanslag
  - följande specialtecken: ~,!, @, #, $, %, ^, &, (,), _, +, -, *, /, =, {, }, [,], |, \, : (kolon), ; (semikolon), ’ (enkelt citationstecken), ” (dubbelt citationstecken), <, >, , (kommatecken), . (punkt), och ?.
- Innehålla minst en versal, minst en gemen och antingen minst ett specialtecken eller en siffra.

Ovanstående sammansättning av ett lösenord medför en lösenordsentropi på 27 bitar vilket är universitetets minimikrav på god lösenordskvalitet.

[3] Gemensam webbinloggning, LDAP och Active Directory (AD)

[4] eduroam

6.1.2 Lösenordskontroll

I universitetets gemensamma inloggningstjänst finns teknikstöd för att säkerställa god lösenordskvalitet. Vid lösenordsbyte kontrolleras att dessa lösenord med avseende på att de

- är sammansatta enligt pkt. 6.1.1 ovan
- inte återfinns i en katalog med lösenord av dålig kvalitet (123456, egennamn, årstider, bilmärken etc.)
- inte är detsamma som det närmast föregående
- inte är för lika varandra.

När användaren skriver in sitt nya lösenord visas kvaliteten på valt lösenord enligt följande skala:

- Rött = uppfyller inte universitetets minimikrav på lösenordskvalitet.
- Gult = uppfyller minimikraven.
- Grönt = överträffar minimikraven med en entropi på ytterligare 6 bitar. Lösenordet går inte att spara förrän det uppfyller minimikraven.

6.1.3 Undantag

Om det i enskilda system som inte är kopplade till den gemensamma inloggningstjänsten föreligger särskilda tekniska skäl för att inte följa ovanstående riktlinjer för god lösenordskvalitet ska undantag godkännas av objekt- eller systemägare och dokumenteras i objektets/systemets förvaltningsspecifikation eller motsvarande dokument. Vidare måste särskild hänsyn tas vid åtkomst av data hämtade från andra system.

6.2 Lösenordsskydd

6.2.1 Datalagring och transport av lösenord

För att reducera risken för obehörig åtkomst till lösenord gäller följande riktlinjer för lagring och transport av lösenord:

- Lösenord ska alltid lagras och transporteras i krypterad form. Detta gäller även back up- media.
- 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 över medarbetare med dessa priviligierade behörigheter ska finnas vid den organisation som sköter driften av systemet, t.ex. IT-avdelningen.

6.2.2 Skydd mot nätbaserade gissningsattacker (Rate limiting)

För att reducera risken för automatiserade gissningsattacker mot lösenord ska inloggningen vara skyddad genom s.k. rate limiting som förhindrar en inkräktare att göra många upprepade lösenordsgissningar på kort tid.

I universitetets gemensamma inloggningstjänst är detta skydd utformat på följande sätt:

- Max. antal felaktiga gissningar under en tidsperiod på 60 minuter = 10.
- Därefter automatisk kontolåsning = 5 minuter.

6.2.3 Lösenordsbyte

För att ytterligare reducera risken att en inkräktare avslöjar ett lösenord till universitetets IT- och informationssystem ska varje användare kontinuerligt byta lösenord inom ett fastställt tidsintervall.

I universitets gemensamma inloggningstjänst gäller följande regler för lösenordsbyte:

- Tvingande lösenordsbyte senast inom 24 månader för anställda, övriga verksamma samt för s.k. funktionskonton.
- Tvingande lösenordsbyte senast inom 5 år för studenter.

6.2.4 Undantag

Om det i enskilda system föreligger särskilda tekniska skäl för att inte följa ovanstående riktlinjer för lösenordsskydd ska undantag godkännas av objekt- eller systemägare och dokumenteras i objektets/systemets förvaltningsspecifikation eller motsvarande dokument. Vidare måste särskild hänsyn tas vid åtkomst av data hämtade från andra system.

7. Implementering

Implementering av dessa riktlinjer kommer att ske stegvis enligt separat upprättad införandeplan.

8. Referenser

Riktlinjer för informationssäkerhet vid Uppsala universitet (UFV 2010/424)

Anvisningar för genomförande av informationsklassificering (UFV 2012/714)

NIST Special Publication 800-63-2 Electronic Authentication Guideline,
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf