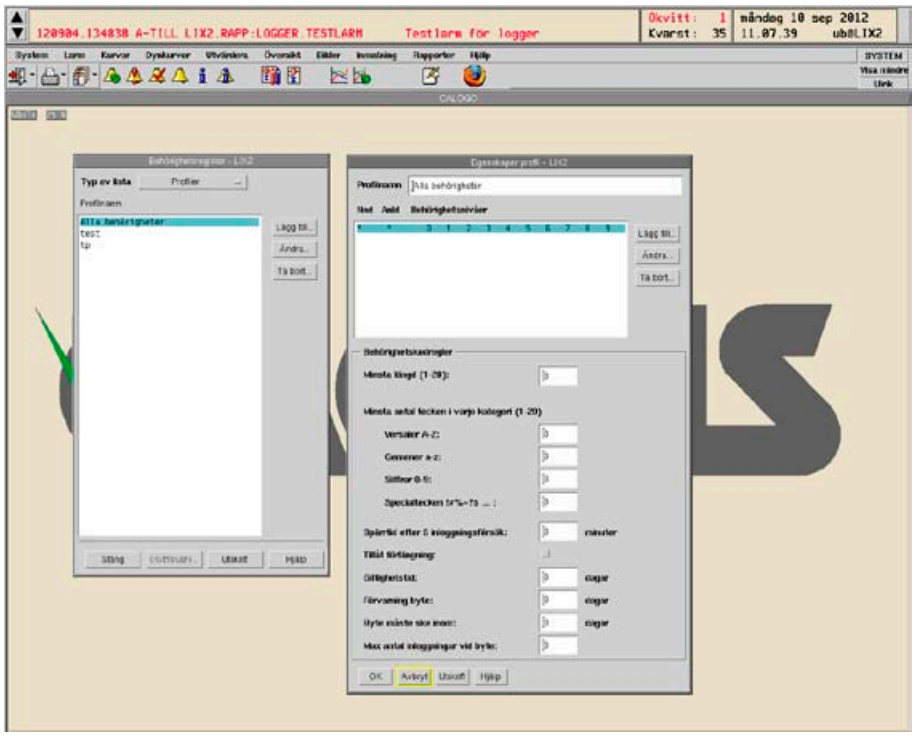
Behörighetssystem.

Högre säkerhet med nytt behörighetssystem.

Säkerhet för VA-verk har kommit allt mer i fokus. Anläggningarna är sårbara med nya och högra krav på inre och yttre säkerhet. MSB har till exempel tagit fram en vägledning för det industriella kontrollsystemet.



Vatten och avlopp.

Kraft- och fjärrvärme.

Biogas.

Elnät.

Industri.

Järnväg.

På Cactus har vi därför utvecklat behörighetssystemet i Cactus CSX till att bli ännu säkrare på flera punkter:

- Större överblick över användare och behörighetskoder.
- Enklare att underhålla för systemansvarig.
- Minimerar risken att inga obehöriga har tillgång till systemet (personer som slutat, gått i pension, korttidsanställda, etc.)
- Möjlighet att tvinga användarna byta sin behörighetskod.

Behörighetskoder och tidsintervall.

I det nya systemet registrerar fortfarande systemadministratören signaturer, men användarna ansvarar själva för att underhålla sina egna behörighetskoder. Användarna kan nu också byta sina behörighetskoder när de själva önskar.

Systemadministratören sätter också fördefinierade tidsintervall där systemet uppmanar och tvingar användaren att byta sin behörighetskod.

Ny och tuffare autentisering.

I det nya behörighetssystemet blir maxlängden för en signatur 6 tecken och för behörighetskod 20 tecken.

Efter 5 misslyckade autentiseringsförsök blir användaren avstängd en förbestämd tid, samt att ett larm sätts. Det kan endast systemadministratören återställa, vilket försvårar möjligheten att testa sig fram till användarens lösenord.

En ensam operatör kan i dag övervaka och fjärrstyra VA-verkets alla pumpar, ventiler och vattenledningsnät. Arbetsplatsen är inte längre bunden till en välbevakad fysiskt skyddad driftcentral, utan kan lika gärna vara en bärbar dator i hemmet.

Ledningskartor, systembeskrivningar och ritningar digitaliseras, vilket ökar tillgängligheten. Kommunikationen mellan datorer sker numera allt oftare över nätverk som dessutom sträcker sig långt utanför det lokala VA-verkets egna lokaler.

Allt det här är exempel på faktorer som påverkar säkerheten.

Bestäm behörighetskodens komplexitet.

I behörighetssystemet är det möjligt att bestämma hur komplicerad en behörighetskod måste vara för att accepteras.

En redan använd behörighetskod blir möjlig att återanvända först efter 10 gånger. Reglerna för behörighetskod är konfigurerbara per användarprofil.

Flera tidsbegränsningar.

Systemadministratören sätter följande tider för varje användarprofil:

- Behörighetskodens giltighetstid i antal dagar.
- Antal dagar före giltighetens slut som användaren uppmanas byta sin behörighetskod.
- Antal dagar om användaren inte byter sin behörighetskod.
- Antal minuter som användaren inaktiveras efter ett bestämt antal misslyckade autentiseringsförsök.

Efter korrekt byte av behörighetskod förlängs automatiskt giltighetstiden det angivna antalet dagar.

Ytterligare nyheter.

Tillfälliga användarkonton är ofta ett bekymmer. Nu är det möjligt att bestämma att behörighetskoden inte kan förnyas. Det visas ingen uppmaning om kodbyte för användaren och behörigheten spärras direkt vid giltighetstidens slut.

När systemet uppmanar användaren att byta behörighetskod efter giltighetstidens slut har användaren ett antal inloggningar eller dagar på sig innan behörigheten spärras (s.k. Grace-login).

Kompletterande användarinformation.

I det nya behörighetssystemet går det också att förse varje användare med en valfri beskrivning på max. 40 tecken. Informationen är enbart tillgänglig för systemadministratören.

Behörighetssystemet är en del i vår verktygslåda för ökad säkerhet. För ytterligare information och hur vår Verktygslåda bäst används i ditt system, är varmt välkommen att kontakta din kundansvarige.

2012-10 SE