Fjärråtkomst över internet

Säkerhet för ett av våra viktigaste livsmedel – dricksvatten – är viktigt för samhället. För NIS-regleringen är det driftsäkerheten och förmågan att kontinuerligt och uthålligt tillhandhålla dricksvatten utan störningar pga av IT-system som är central. En annan viktig aspekt är att ha förmågan att hantera en störning om den ändå inträffar.

Denna kontinuitet säkerställs genom att införa åtgärder för att förebygga störningar samt skapa en förmåga att hantera situationer då störningar, trots åtgärder, ändå uppstår. NIS inriktar sig på störningar som har sin orsak i att nätverksuppkopplad digital utrustning inte är tillgänglig eller inte fungerar korrekt – oavsett om det skett av misstag, naturfenomen eller genom angrepp.

Detta informationsblad ger några tips och förslag på åtgärder som kan ge effekt på driftssäkerheten och som kan vara underlag för beslut kring säkerhetshöjande åtgärder för fält- eller distansarbete. Dock poängteras att detta *inte* är en uttömmande lista utan en hjälp att komma igång med säkerhetsarbetet.

Behovet av fjärråtkomst via internet

Många driftorganisationer i VA-Sverige är, sett till personalstyrkan, ganska små. Det ställer ibland stora krav på tillgänglighet och flexibilitet från personalens sida, speciellt i samband med extraordinära händelser. Men även enkla saker som vård av sjuka barn kan innebära begränsningar i personalens möjligheter att åka till jobbet eller rycka ut på larm. Behovet av fjärråtkomst till driftsystem både hemifrån och ute i fält ökar.

Flerfaktorsautentisering vid fjärråtkomst

Flerfaktorsautentisering vid fjärråtkomst är en grundläggande säkerhetshöjande åtgärd för industriella kontrollsystem. Det finns en betydande risk för allvarliga störningar om obehöriga får fjärråtkomst till nätverks- och informationssystem som är av betydelse för leverans och distribution av dricksvatten. Vid åtkomst till viktiga system utifrån, primärt via internet, är användarens identitet central.

Traditionell åtkomstkontroll baserad på användarnamn och lösenord innebär ett flertal olika risker och problemställningar, exempelvis att användare delar lösenord med varandra eller väljer för enkla lösenord. En annan nackdel med just lösenord är att de ofta återanvänds på flera ställen – privata webtjänster, konton på jobbet m.m. – och då blir lättare att stjäla.

En fjärruppkoppling erbjuder inte heller samma möjlighet att kontrollera att den som loggar in faktiskt är den person eller maskin den utger sig för att vara – på en fysisk arbetsplats finns det ett skalskydd och kollegor som delvis fungerar som en kontrollmekanism vilket helt saknas vid fjärruppkoppling.

Val av lösning för flerfaktorsautentisering

Kostnaderna för tvåfaktorsautentisering är, som i många fall, beroende på vilken lösning som väljs. Som högst blir kostnaden per användare vid användning av hårdvara i form av så kallade lösenordsdosor, tokens eller smarta kort. Det finns också lösningar baserade på moln-tjänster, SMS och applikationer till mobiltelefoner som i många fall har en betydligt lägre prisbild, men säkerheten och tillgängligheten i dessa lösningar kan bli en flaskhals.

Inför valet av lösning bör man i sin riskanalys fundera på hur driftsäker lösningen blir. Det finns tydliga fördelar ur driftsäkerhetssynpunkt om möjligheten till fjärråtkomst inte är beroende av externa tredjepartstjänster, exempelvis sms. Anledningen är att verifieringen av användarens identitet sker utanför verksamhetsutövarens kontroll, vilket kan introducera sårbarheter i åtkomstkontrollen men också att det kan försvåra inloggning i krissituationer då det kräver fler tjänster som samtidigt ska fungera.

Reglera åtkomst och rättigheter

Om verksamheten möjliggör åtkomst via VPN så bör det regleras tydligt vilka användare som får tillgång till fjärrstyrning av industriella kontrollsystem. Identifiera tydligt vilka grupper av anställda som behöver fjärranslutningsmöjligheter för att utföra sina arbetsuppgifter och begränsa i möjligaste mån den grupp av användare som har möjlighet att på distans påverka dricksvattenförsörjningen.

För att förhindra obehörig åtkomst och obehörig eller oavsiktlig förändring i de digitala system som används för l*everans och distribution* av dricksvatten bör regelbunden kontroll/revision av åtkomst och behörigheter göras. Det är extra viktigt vid nyetablering av en fjärråtkomst-lösning då det annars är lätt att gamla behörigheter ligger kvar, som då kan ge åtkomst via internet.

Styrning av åtkomsträttigheter, användarkonton och lösenordshantering säkerställer att det endast är behörig personal som har åtkomst till de digitala system som används för l*everans och distribution* av dricksvatten. Det innebär att även underleverantörers eventuella åtkomst ska kontrolleras på samma sätt som anställdas åtkomst.

Ytterligare ett problem kopplat till underleverantörer med fjärråtkomst är att de inte alltid har användarunika konton för sina användare utan delar ett gemensamt leverantörskonto med ett gemensamt lösenord för flera av underleverantörens anställda. Det innebär att lösenord och användarnamn för fjärråtkomst med tiden sprids i vida kretsar och att de inte byts när underleverantörens anställda byter jobb eller befattning.

Informativa länkar

Lag 2018:1174: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-20181174-om-informationssakerhet-for_sfs-2018-1174

Livsmedelsverket: www.livsmedelsverket.se/nis

FOI / NCS3 Fjärranslutningstekniker för industriella informations- och styrsystem: https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4751--SE

Har ni frågor? Kontakta oss på: **nistillsyn@slv.se**

Livsmedelsverket