IKT og sikkerhet i VA-sektoren: Hva kan gå galt?

Av Inger Anne Tøndel, Martin Gilje Jaatun, Jon Røstum

Inger Anne Tøndel og *Martin Gilje Jaatun* er henholdsvis forskningsleder og seniorforsker ved SINTEF IKT innen informasjonssikkerhet. *Jon Røstum* er seniorforsker ved SINTEF Byggforsk innen vann og avløp.

Innlegg på fagtreff i Norsk vannforening 12. mars 2013.

Sammendrag

Bruk av IKT gir flere gevinster for VA-sektoren, i form av bedre oversikt og mer effektiv drift. Samtidig fører økt bruk av IKT til at sektoren må forholde seg til trusler også mot IKT-systemene. Denne artikkelen gir en oversikt over utfordringer knyttet til IKT-sikkerhet. Den forklarer sentrale begreper innen informasjonssikkerhet og gir eksempler på hva IKT-trusler kan føre til. Bevissthet om hva som kan gå galt er et viktig grunnlag for å treffe gode tiltak. Artikkelen viser videre til eksisterende veiledere som gir konkrete råd om dette.

Informasjons- og kommunikasjonsteknologi (IKT) har blitt stadig viktigere i alle sektorer av samfunnet, og er en integrert del av infrastrukturer som energi, helse, transport, og også vann og avløp. IKT brukes for å kommunisere, lagre data, samle data, utføre målinger, gjøre overvåking, og styre prosesser, for å nevne noe. IKT har gjort det mulig å hente ut effektiviseringsgevinster og få bedre tilgang til statusinformasjon. Samtidig har IKT ført med seg ny trusler i forhold til tidligere.

Prosesskontroll til glede og sorg

Prosesskontrollsystemer eller driftskontrollsystemer brukes innen en rekke sektorer for å styre og overvåke prosesser. Prosesskontrollsystemene har blitt stadig mer avanserte. De har gått fra å være spesiallagde og proprietære til å være hyllevare-PC-er med f.eks. Windows operativsystem. Der prosesskontrollsystemene før var skilt fra omverdenen – og ofte heller ikke sett på som IKT – er de nå ofte koblet til nettverk. Selv om det er en utbredt målsetning i mange virksomheter at prosesskontrollsystemer skal være helt adskilt fra f.eks. kontorsystemer, er det vanskelig å få til dette i praksis. Behov for fjerntilgang, behov for statusinformasjon, og behov for å gjøre oppgraderinger og vedlikehold gjør at prosesskontrollsystemer ikke lenger kan ses på som isolerte systemer.

I en studie av informasjonssikkerhet knyttet til integrerte operasjoner på norsk sokkel for noen år tilbake [1] ble det opplevd at det var et stort skille mellom de som jobbet med prosesskontroll og de som jobbet med IKT, eksemplifisert med uttalelsen ”Vi har ikke IT, vi har programmerbar logikk”. Tradisjonelt har man tenkt lite på tradisjonell IKT-sikkerhet for prosesskontrollsystemer. Sikkerheten har ligget i at få har hatt kunnskap om disse systemene og at de har vært skilt fra omverdenen. Nå er dette helt annerledes. Det finnes egne søkemotorer på nettet som kan benyttes til å finne prosesskontrollsystemer som er koblet til internett. Det finnes angrepsverktøy tilgjengelig som letter angrep mot slike systemer. På grunn av stadig mer bruk av standard programvarekomponenter

også for prosesskontroll, er disse systemene ofte sårbare for de samme angrepene som andre mer tradisjonelle IKT-systemer. Dette gjør at sikkerhet må være på dagsorden også for prosesskontrollsystemer.

Noen eksempler

For å illustrere hva som kan gå galt, bruker vi noen offentlig kjente, virkelige hendelser som eksempler.

Hevnangrep fra tidligere ansatt (Maroochy Shire, Australia, 2000)

Maroochy Shire-hendelsen [2] fra Australia, 2000, er et klassisk eksempel på et målrettet angrep mot et prosesskontrollsystem fra en angriper med meget god kjennskap til systemet.

Et konsulentselskap ved navn Hunter Watertech hadde hatt i oppdrag å installere et SCADA system som via radioforbindelser styrte 300 pumpestasjoner for kloakk. En av de ansatte, Vitek Boden, hadde et noe anstrengt forhold til sin arbeidsgiver. Han sa opp hos Hunter Watertech, og søkte jobb i vannverket – men fikk nei. Han hevnet seg både på sin tidligere arbeidsgiver og vannverket ved å manipulere pumpestasjoner og ventiler/luker slik at en million liter ubehandlet kloakk rant ut i nærliggende vassdrag.

Avansert målrettet dataorm (Stuxnet)

Stuxnet [3] er en dataorm som hadde som hovedmål å sabotere Iran sin anrikning av uran. Den infiserte Siemens Simatic systemer, og var konfigurert for bare å kontrollere og overvåke veldig spesifikke industrielle prosesser. Stuxnet var svært avansert, og benyttet ikke mindre enn fire "zero-day exploits" – det vil si sårbarheter som man ikke var kjent med på det tidspunktet.

Stuxnet spredde seg over hele verden, med markert konsentrasjon i Iran i tidlig fase. Det er verdt å merke seg at Stuxnet også infiserte systemer som ikke var koblet til internett. Infeksjonen skjedde gjennom minnepinner som ble koblet til systemer på prosessnettet, og så spredte dataormen seg videre derifra. Ifølge Nasjonal sikkerhetsmyndighet (NSM) var dette første gang en så dataormer/trojanere som var spesiallaget for å ta kontroll over prosess- og kontrollsystemene [5].

Stuxnet ble oppdaget i 2010, men i etterkant har det blitt oppdaget versjoner av Stuxnet fra 2007 [4].

Driftskontrollsystem på nett (South Houston, 2011)

I 2011 fikk en hacker tilgang til brukergrensesnittet til driftskontrollsystemet til vann- og avløpsverket til South Houston, Nevada [6] [7] [8]. Systemet var tilgjengelig via internett, og passordet var et standardpassord på kun tre bokstaver. Denne hackeren gjorde ingen skade i systemet, men publiserte skjermdump som viste hva han hadde fått tilgang til. Uvedkommende skal således ha vært i stand til å endre på driftsparametre ved vannverket.

Hardkodede passord er heller ikke så lurt

I 2010 ble det oppdaget skadevare (*malware*) som brukte et kjent standardpassord, som var hardkodet i Siemens Simatic systemer for å beskytte databasen. Passordet kunne heller ikke endres, da det ville gjøre at systemet ikke virket lenger. Hardkodede passord er imidlertid ikke et problem bare for dette systemet. Joe Weiss, en ekspert på elektroniske trusler mot prosesskontrollsystemer, uttalte i forbindelse med denne oppdagelsen at over halvparten av leverandørene av kontrollsystemer hardkodet passord inn i deres systemer [9].

Hva menes med IKT-sikkerhetsbrudd?

Når det gjelder sikring av IKT-systemer og den informasjonen som ligger i disse systemene, snakker man gjerne om sikring av [11]:

- Konfidensialitet; det å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang
- Integritet; det å sikre at informasjonen og metodene/beregningene er nøyaktige og fullstendige. Dette innebærer at uvedkommende ikke kan endre informasjonen eller systemet som behandler informasjonen

- Tilgjengelighet; det å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov.

Når det gjelder drifts- og styringssystemer vil ofte integritet og tilgjengelighet være vel så viktig som konfidensialitet. Man er avhengig av at systemet er tilgjengelig og gjør de oppgavene det er satt til; dette forutsetter også at systemet har tilgang til riktig informasjon til enhver tid.

Trusler mot IKT-systemer kan deles opp i to hovedkategorier:

- Tilfeldige og utilsiktede feil som kan skje på grunn av svakheter i IKT-systemet, uheldige ansatte eller utenforliggende hendelser
- Bevisst skadeverk, som igjen kan deles inn i:
  - Generelle angrep som ikke er direkte rettet mot VA-verket, men som kommer som en følge av det generelle trusselbildet mot IKT-systemer
  - Målrettede angrep der angripere benytter IKT-systemer for å skade VA-verket spesielt.

I eksemplene over var det snakk om bevisst skadeverk. Det er imidlertid viktig å være klar over at tilfeldige og utilsiktede feil også kan føre til store konsekvenser. Utilsiktede feil i form av sårbarheter i systemene, usikre konfigurasjoner eller feilhandlinger gjort av ansatte kan også åpne muligheter for angripere når det gjelder å gjennomføre bevisst skadeverk.

Men hva har dette med VA å gjøre?

Godt vann og god og trygg håndtering av avløp er viktig for Norge! Det er få ting som kan skape slik utrygghet i samfunnet som usikkerhet om drikkevann. Håndtering av vann og avløp er også viktig for mange andre kritiske infrastrukturer. IKT har åpnet muligheter for bedre overvåking av VA-anlegg, og dermed tryggere og mer effektiv drift. Det er imidlertid viktig at man også tar på alvor den økte sårbarheten som kommer med bruk av IKT. I en rapport utarbeidet for VA-sektoren i USA ble det fremhevet følgende konsekvenser av bevisste IKT-angrep i denne sektoren [10]:

- Angriper griper inn i driften av vannbehandlingsanlegg, noe som kan føre til over- eller underdosering av kjemikalier
- Angriper gjør endringer i programmerbare instruksjoner i lokale prosessorer og klarer dermed å ta over kontroll av utstyr innen VA-systemer, noe som kan føre til redusert drift av pumpestasjoner, uønsket overløpsutslipp, osv.
- Angriper endrer programvare til kontrollsystemet, noe som gir uforutsigbare resultater
- Angriper blokkerer eller sender falsk informasjon til operatører for å hindre at de blir klar over forhold, eller for å trigge uheldige handlinger
- Angriper endrer terskler/grenser for alarmer, eller deaktiverer dem
- Angriper hindrer tilgang til brukerkontoinformasjon
- Selv om mange anlegg har manuelle backuprutiner, kan feil på mange systemer overbelaste personalressursene – selv om hver feil er håndterbar i seg selv
- Utpressingsvare (*ransomware*) – hindre tilgang, og kreve løsepenger for å låse opp IT-systemet.

Det er også verdt å merke seg at et angrep kan ha stor effekt selv om det ikke skulle resultere i noen konsekvenser for VA direkte – dette fordi folk kan miste tillit til vannkvaliteten. På samme måte kan angrepstrusler og usikkerhet om sikkerheten i VA-systemer ha store konsekvenser både for samfunnet og for VA-sektoren dersom det fører til utrygghet rundt kvaliteten på drikkevannet. Derfor er det viktig at VA-sektoren kan vise til at de har gjort gode tiltak og er godt rustet for å håndtere også trusler i IKT-systemene.

Det finnes hjelp å få!

IKT-sikkerhet, og sikkerhet i prosesskontrollsystemer spesielt, er ikke noe nytt. De endringene man ser innen prosesskontroll med mer kompleksitet, mer sammenkobling og mer bruk av standardkomponenter har vart i flere år og har skjedd i mange bransjer. Det finnes derfor mange gode anbefalinger og veiledninger rundt dette.

For norske forhold vil vi spesielt trekke frem "Veileder for sikkerhet av driftskontrollsystemer for VA-systemer", gitt ut av Norsk Vann. Denne veilederen går dypere inn i de driftskontrollsystemene som brukes innen vann og avløp, og gjennomgår mulige årsaker til svikt i disse systemene. I tillegg gis det en bred oversikt over tiltak, både på organisatorisk og teknisk plan. Denne veilederen inneholder også en sjekkliste som kan brukes for å vurdere sikkerheten til driftskontrollsystemer for VA. Styrken til denne veilederen er at det gis konkrete råd og anbefalinger til tiltak, spesielt tilpasset behovene i VA-sektoren.

Det kan også være mye å lære fra andre sektorer. En sektor som har kommet langt når det gjelder IKT for styring er oljebransjen, og i denne sektoren har det blitt utarbeidet et sett av basis-krav for informasjonssikkerhet i prosesskontrollsystemer (OLF Guideline 104) [12]. Mange av disse kravene vil også være relevante innen VA-sektoren.

Noen pumper brenner opp av seg selv

Selv om det er viktig å ta på alvor den risikoen som kommer med økt bruk av IKT, er det stor grunn til å glede seg over de gevinster IKT gir. Det er også viktig å være klar over at mange har egeninteresse av å "skremme litt". Alle oppslag om hackere er heller ikke like velbegrunnet. I november 2011 kunne vi lese at en vannpumpe i Springfield, Illinois, brant opp [13]. Når man studerte nettverksloggen så man forbindelser fra Russland – og myndighetene var raskt ute med konklusjonen: Hackere! Dette var nok litt overilet, for snart ble det klart at eieren av firmaet som satte opp SCADA-systemet var på ferie i Russland fem måneder tidligere, og hadde logget seg inn derfra for å sjekke noen data som vannverket hadde ringt og bedt ham om [14]. Når alt kom til alt var det ikke mulig å finne noen bevis på skumle hensikter, og vi må slå fast at enkelte pumper brenner opp av seg selv.

Tenk risiko

IKT er kommet for å bli. Det er derfor viktig å håndtere risiko knyttet til IKT slik man allerede gjør for andre områder. Sentralt i denne sammenheng er gjennomføring av risikoanalyser. Man må ha et bevisst forhold til hva som kan gå galt, hvor sannsynlig det er og hvilken skade det kan medføre. Målet er ikke å bremse utviklingen, men å treffe gode tiltak som kan redusere risikoen på en god måte. Dette kan gjøres både ved å hindre at ting kan oppstå og ved å gjøre organisasjonen og systemer bedre i stand til å oppdage og takle problemer når de skjer. Dette arbeidet kan gjerne lettes ved å samarbeide med andre i bransjen. Slik sett er den nye veilederen fra Norsk Vann et godt utgangspunkt for å enes om en bransjenorm etter modell fra norsk olje og gass.

Referanser

1. Martin Gilje Jaatun, Eirik Albrechtsen, Maria B. Line, Inger Anne Tøndel, Odd Helge Longva: "A Framework for Incident Response Management in the Petroleum Industry." *International Journal of Critical Infrastructure Protection*, vol. 2, pp. 26-37, April 2009.

2. Jill Slay, Michael Miller, "Lessons learned from the Maroochy Water Breach," *Critical Infrastructure Protection*, Vol. 253, E. Goetx, S. Shenoi, Eds., ed: Spronger Boston, 2007, pp. 73-82.

3. Nicolas Falliere, Liam O. Murchu, Eric Chien, "W32. Stuxnet Dossier", Symantec Security Response, Version 1.4, February 2011, http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

4. Jim Finkle, "Researchers say Stuxnet was deployed against Iran in 2007," Reuters, 26.02.13, http://www.reuters.com/article/2013/02/26/us-cyber-war-stuxnet-idUSBRE91P0PP20130226

5. Kjetil Berg Veire, "Mye oppmerksomhet rundt Stuxnet," NSM Sikkerhetsbloggen, 27.09.10, http://blogg.nsm.stat.no/archives/155

6. http://pastebin.com/Wx90LLum

7. Eric Byres, "SCADA Security Breached at U.S. Water Utilities," Tofino, Nov 21 2011, http://www.tofinosecurity.com/blog/scada-security-breached-us-water-utilities

8. Eric Byres, "U.S.Water Utilities and Poor Passwords," Tofino, Nov 22 2011, http://www.tofinosecurity.com/blog/us-water-utilities-and-poor-passwords

9. Kim Zetter, "SCADA System's Hard-Coded Passwords Circulated Online for Years," Wired, 07.19.10, http://www.wired.com/threatlevel/2010/07/siemens-scada/

10. Water Sector Coordination Council Cyber Security Working Group, "Roadmap to Secure Control Systems in the Water Sector," March 2008, http://tisp.org/index.cfm?cdid=11044&pid=10261

11. Martin Gilje Jaatun, Jon Røstum, Stig Petersen, "Sikkerhet og sårbarhet i driftskontrollsystmer for VA-anlegg," Norsk Vann R195, 11. mars 2013, http://www.norskvann.no/kompetanse/va-bokhandelen/rapporter/product/418-r195-sikkerhet-og-sarbarhet-i-driftskontrollsystemer-for-va-anlegg

12. Norwegian Oil and Gas Association, "104 - Recommended guidelines for information security baseline requirements for process control, safety and support ICT systems," 2006, http://www.norskoljeoggass.no/no/Publikasjoner/Retningslinjer/Integrerte-operasjoner/104-Anbefalte-retningslinjer-krav-til-informasjonssikkerhetsniva-i-IKT-baserte-prosesskontroll--sikkerhets--og-stottesystemer/

13. Kim Zetter, "H(ackers)$_2$O: Attack on City Water Station Destroys Pump," Wired, 11.18.11, http://www.wired.com/threatlevel/2011/11/hackers-destroy-water-pump/

14. Kim Zetter, "Exclusive: Comedy of Errors Led to False 'Water-Pump Hack' Report," Wired, 11.30.11, http://www.wired.com/threatlevel/2011/11/water-pump-hack-mystery-solved/