Nasjonal sikkerhetsmyndighet

Veiledning

Sist oppdatert: 2014-03-26

Sikring av industrielle automatiserte kontrollsystemer

Nasjonal sikkerhetsmyndighet

Nasjonal sikkerhetsmyndighet (NSM) er et direktorat for forebyggende sikkerhetstjeneste. NSM skal innen sitt ansvarsområde beskytte informasjon og objekter mot spionasje, sabotasje og terrorhandlinger gjennom å:

- gi råd og veiledning

- utvikle sikkerhetstiltak

- varsle og håndtere alvorlige dataangrep

- føre tilsyn og utøve myndighet iht. regelverk

NSM skal være en pådriver for bedring av sikkerhetstilstanden og gi råd om utviklingen av sikkerhetsarbeidet i samfunnet.

Hensikt med veiledning

NSM sin veiledningsvirksomhet skal bygge kompetanse og øke sikkerhetsnivået i virksomhetene, gjennom økt motivasjon, evne og vilje til å gjennomføre sikkerhetstiltak. NSM gir jevnlig ut veiledninger til hjelp for implementering av de krav sikkerhetsloven stiller. NSM publiserer også veiledninger innen andre fagområder relatert til forebyggende sikkerhetsarbeid.

Postadresse
Postboks 814
1306 SANDVIKA

Sivil telefon/telefax
+47 67 86 40 00/+47 67 86 40 09
E-postadresse
post@nsm.stat.no

Militær telefon/telefaks
515 40 00/515 40 09

Internettadresse
www.nsm.stat.no

Innhold

1 Introduksjon

Denne veiledningen er ment å være en overordnet teknisk veiledning for sikring av industrielle automatiserte kontrollsystemer (IAK). Dokumentet er ikke ment å være noe erstatning til veiledninger eller råd gitt fra de ulike leverandørene på markedet. Anbefalinger og tiltak gitt i denne veiledningen er basert på *sikkerhet i dybden*. Dette betyr å implementere uavhengige sikkerhetstiltak på flere nivåer i systemet. I en situasjon hvor ett av sikkerhetstiltakene blir kompromittert skal andre redundante sikkerhetstiltak stoppe trusselen.

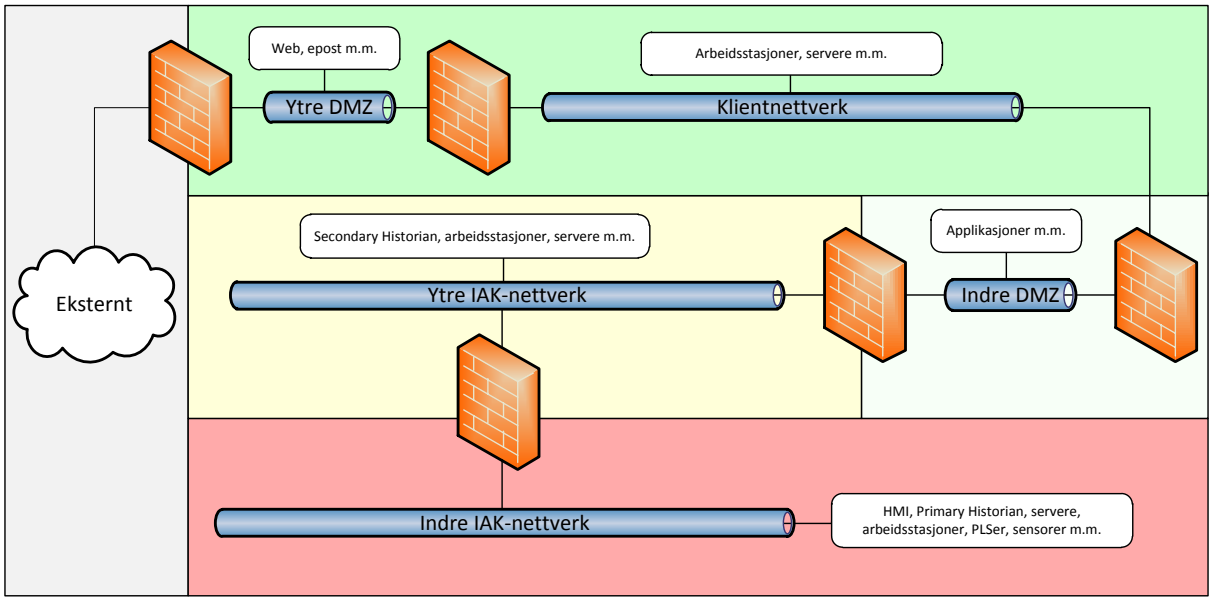
Industrielle automatiserte kontrollsystemer (IAK) vil i denne veiledningen dekke alle systemer som benyttes til å overvåke, kontrollere og styre fysiske prosesser. Med andre ord vil IAK-systemer inkludere *Supervisory Control and Data Acquisition* (SCADA), *Distributed Control Systems* (DCS) og *Process Control Systems* (PCS). Dette er systemer som er svært viktig å sikre ettersom de blir benyttet i kritisk infrastruktur innenfor kraft, tele, vann, transport og petroleum [1].

Veiledningen starter med å gi anbefalinger innenfor området nettverksdesign og perimetersikkerhet, hvor det blir gitt sikkerhetsmessige anbefalinger rettet mot soneinndeling, autentisering og trådløse nettverk. Neste kapittel tar for seg sikkerhetsmessig herdig som gir generelle råd rundt herding av enheter og tjenester, samt sikkerhetsoppdateringer av de enkelte komponentene i IAK-systemet. Videre gis det anbefalinger vedrørende brukerhåndtering og bruk av passord. Til slutt blir det gitt tiltak som omfatter analyse av logger og deteksjon av sikkerhetstruende hendelser og skadevare.

2 Perimetersikkerhet

2.1 Soneinndeling

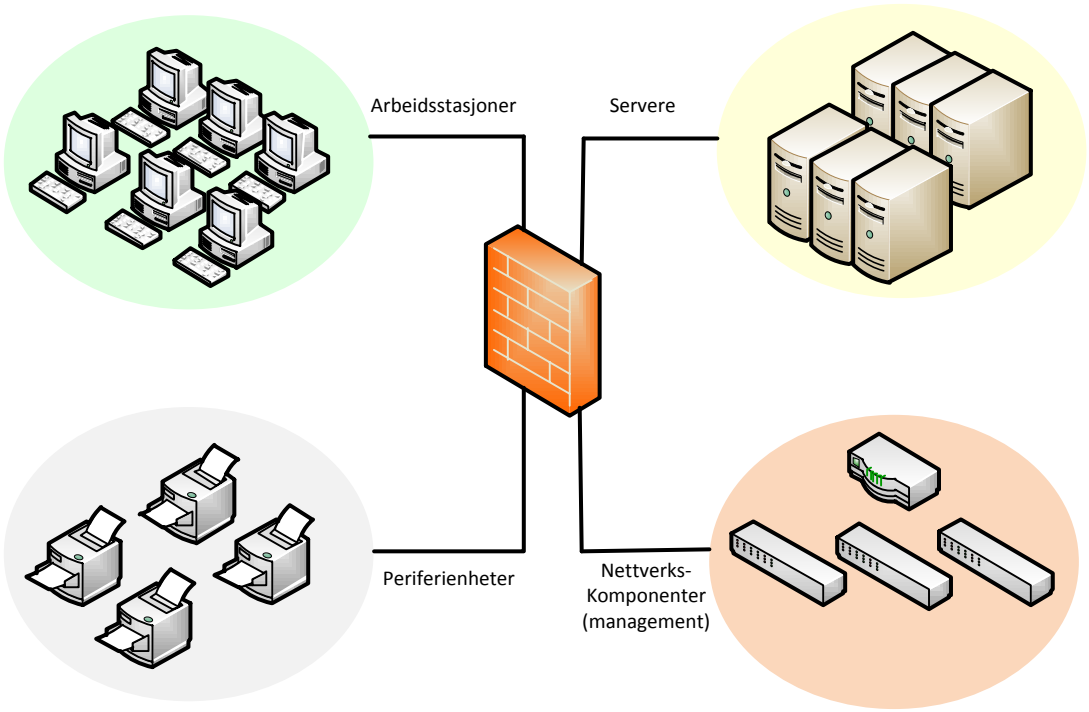
Første steget for å implementere sikkerhet i dybden er å benytte soneinndeling. Dette skaper klare skiller mellom ulike deler av IAK-systemet. Nettverksinfrastrukturen bør deles inn i soner og segmenter ut i fra funksjonalitet og rolle. Mellom hver sone implementeres en brannmur, hvor autorisert trafikk gjenspeiler den nødvendige systemfunksjonaliteten. Dette betyr at all trafikk mot IAK-nettverket bør rutes gjennom en eller flere brannmurer [2, 3, 4].



Figur 1: Overordnet soneinndeling og DMZ-er

For å forhindre direkte kommunikasjon med IAK-nettverket så anbefales det å implementere en eller flere demilitariserte soner (DMZ). All ekstern kommunikasjon med IAK-nettverket bør skje via disse DMZ-ene. Dette vil skape en ekstra barriere for videre angrep fra mindre kritiske soner. Figur 1 viser en overordnet soneinndeling med egne soner for DMZ-ene, hvor de enkelte sonene er representert med ulike farger.

Ytterligere soneinndeling enn de som angitt i figur 1, bør ta sikte på å skille ut administrasjonsgrensesnitt til nettverkskomponenter, arbeidsstasjoner, servere, periferienheter m.m. i egne soner. Ved å benytte svært restriktive brannmurregler vil kun absolutt nødvendig trafikk passere. Dermed begrenses angrepsflaten betraktelig i en situasjon hvor en kompromittering har inntruffet i en sone. Dette er tiltak som bør implementeres i klientnettverket, ytre IAK-nettverk, og hvis mulig i det indre IAK-nettverket (se figur 2).



Figur 2: Soneinndeling

Det anbefales på det sterkeste at IAK-nettverket ikke er eksponert mot Internett, samt at Internettaksess og e-post fra dette nettverket blir blokkert.

2.2 Autentisering

Aksessering av tjenester innad/utad av soner bør benytte autentisering, samt kryptert kommunikasjon for å forhindre at passord blir sendt i klartekst. Det anbefales at fjerntilgang mot IAK-nettverket holdes til et minimum og benytter sterk autentisering (multi-faktor) og kryptering, for eksempel VPN.

2.3 Trådløse nettverk

Trådløse nettverk (WiFi) bør ikke implementeres i et IAK-system. Dersom WiFi er helt nødvendig i systemet, bør det bare tas i bruk etter en grundig risikoanalyse og sikres med autentisering og sterk kryptering.

3 Sikkerhetsmessig herdig

3.1 Herding av enheter og tjenester

All infrastruktur bør gjennomgå sikkerhetsmessig herdig for å forhindre nettverksbaserte angrep. Dette betyr at ubrukte porter og tjenester deaktiveres, innebygde sikkerhetsmekanismer aktiveres, enhetene holdes oppdatert med nyeste sikkerhetsoppdateringer, samt alle standardpassord forandres [5, 6].

Datamaskiner, servere, nettverkskomponenter og IAK-enheter bør herdes før de kobles til nettverket. Enheter som ikke er oppdatert og som benytter standardinnstillinger kan under gitte forutsetninger gjøre deler av nettverket sårbart for angrep. I tillegg bør det innføres tiltak som reduserer skadefølgene av uautorisert fysisk tilgang til datamaskiner. Eksempelvis kryptering av harddisk og sikker oppstart er tiltak som sikrer konfidensialitet og integritet ved uautorisert fysisk tilgang [7].

3.2 Sikkerhetsoppdateringer

Det anbefales å innføre gode rutiner for *oppdatering* av operativsystem og programvare. Ved oppdatering av systemer i IAK-nettverket, bør oppdateringene testes i et eget testmiljø før endelig utrulling. For å minimere sannsynligheten for driftsforstyrrelser eller andre uforutsette problemer bør testmiljøet være så likt produksjonsmiljøet som mulig.

Virksomhetene bør fokusere på å implementere alle oppdateringer som er godkjente av sine respektive leverandører. For kritiske sårbarheter som enda ikke er godkjente anbefales det på det sterkeste å implementere kompenserende tiltak. Det anbefales også at alle systemeiere kontakter sine respektive leverandører for å få leverandørene til å teste og godkjenne oppdateringer så snart som mulig.

Oppgradering til en nyere produktversjon fører ofte til bedret sikkerhet. Det er anbefales å oppgradere programvare, eksempelvis operativsystemer [10], til nyeste versjon som er støttet av produsenten. Nye produktversjoner introdusere ofte ny sikkerhetsfunksjonalitet som beskytter mot nye typer angrep, samt umuliggjør og/eller vanskeliggjør eldre angrep. Derfor anbefales det på det sterkeste å oppgradere systemer i IAK-nettverket når dette støttes av leverandør.

4 Brukerhåndtering og passord

4.1 Brukerkontoer

For å tilstrebe individuell autorisasjon og brukeransvar mot et IAK-system, bør alle brukerkontoer være personlige. Det anbefales at man unngår bruk av felleskontoer. Felleskontoer svekker sporbarheten i systemet ved alvorlige brukerfeil eller misbruk av konto [9].

Ved brukerhåndtering så anbefales det at prinsippet om minste privilegium følges. Forhøyede privilegier bør kun gis til personell som har tjenstlig behov og for øvrig holdes til et minimum. Brukere som får tildelt forhøyde rettigheter bør i tillegg gis en brukerkonto med normale (lave) rettigheter. All systembruk som ikke krever førhøyde rettigheter bør gjøres med en konto med normale rettigheter. Dette betyr at brukere bør tilordnes standardiserte roller som bidrar å redusere brukerfeil og misbruk av brukerkontoer. En rolle inkluderer både privilegier og spesifikke oppgaver knyttet til et sett med brukere.

Rollen som domeneadministrator bør være tilordnet svært få brukere. NSM anbefaler normalt 2-3 brukere med administratorprivilegier. Disse bør ikke brukes såfremt ikke strengt nødvendig. Virksomhetens behov for administratortjenester bør betjenes av separate brukere med de privilegier som er nødvendig for at brukeren kan utføre spesifikke oppgaver [8, 9].

Rutiner for gjennomgang av brukerrettigheter og deaktivering av gamle kontoer bør etableres. Brukerkontoer for personer som har forlatt virksomheten eller ikke lenger trenger tilgang til systemet bør deaktiveres. I tillegg bør brukerkontoene fratas alle systemrettigheter. Tilsvarende rutiner bør innføres eksempelvis for konsulenter eller driftsingeniører som bare trenger tilgang til systemet for å gjøre en spesifikk jobb i en angitt periode.

4.2 Passord

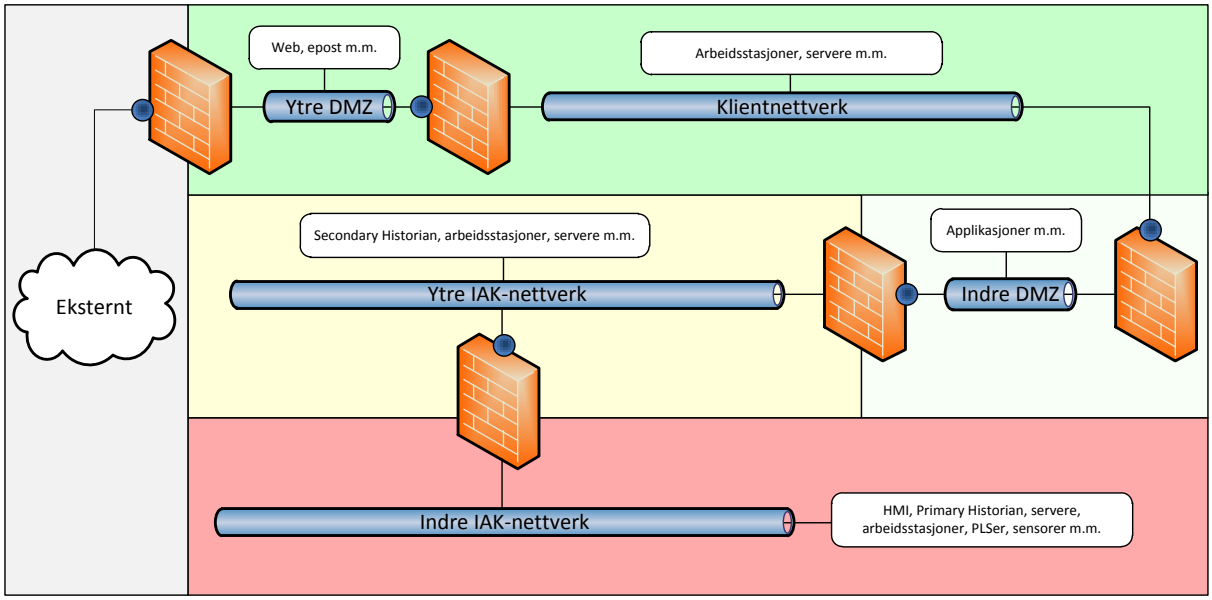
Passord som gir tilgang til essensiell systemfunksjonalitet bør ha tilstrekkelig lengde, kompleksitet og ikke gjenbrukes i andre systemer, eller andre deler av systemer. Videre anbefales det at passord til privilegerte og ordinære brukere forandres ved jevnlig basis. Det anbefales at brukere gjøres bevisst på hva som er gode/dårlige passord og det er viktig å lære brukere praktiske teknikker for å lage gode passord.

NSM anbefaler en minimumslengde på 14 tegn for passord til bruk i IKT-systemer. I tillegg kreves det at passordene inkluderer store og små bokstaver, tall og spesialtegn [9]. I tillegg bør aldri passord lagres ukryptert eller i sårbare formater, eksempelvis LM-hash.

5 Deteksjon

5.1 Intrusion Detection Systems (IDS)

Nettverkstrafikken mellom ulike soner bør overvåkes i sanntid ved bruk av *intrusion detection systems* (IDS) for å identifisere uvanlig oppførsel og potensielle angrep. IDS-er bør plasseres i hver enkelt sone for å oppdage angrep utenfra, samt ondsinnet trafikk sendt fra kompromitterte maskiner. Figur 3 viser et eksempel på plassering av IDS-er, hvor de ulike IDS-ene er representert med en blå sirkel.



Figur 3: Overordnet soneinndeling, DMZ-er og IDS-er

Plassering av IDS-er bør gjøres etter en risikoanalyse. Det vil være fordeler og ulemper ved å plassere en IDS enten på et *ingress*- eller *egress*-punkt i brannmuren. Ved plassering på et *ingress*-punkt vil IDS-en detektere potensielle angrep mot nettverket og mot selve brannmuren. En brannmur plassert mot for eksempel internett vil risikere, med denne plasseringen av IDS, falske positiver som er et resultat av «støy»[1] og ikke reelle angrep. Ved plassering av IDS på *egress*-punktet vil brannmuren filtrere bort slik «støy», men igjen vil IDS-en ikke være i stand til å oppdage potensielle angrep mot brannmuren.

Det anbefales at de implementerte IDS-ene oppdateres jevnlig med nye signaturer for å kunne identifisere nye sårbarheter og angrep. I tillegg bør de støtte egenutviklede signaturer for å dekke spesifikke scenarioer som kan oppstå i IAK-nettverket.

En avvart av IDS, kalt Intrusion Prevension Systems (IPS), bør *ikke* installeres i IAK-systemer.

5.2 Antivirus

Antivirus bør installeres på alle klienter og servere. Dette gjelder også for klienter og servere i IAK-nettverket, hvis det støttes av leverandør. Merk at de største leverandører for IAK-utstyr ofte støtter spesifikke antivirusprodukter. Her har de gjennomført en rekke tester for å undersøke hvorvidt en produktserie er kompatibel med en spesifikk antivirusløsning [2]. Det bør også vurderes andre

[1] Generell kartleggingstrafikk o.l.

løsninger som for eksempel *gateway antivirus*, hvor nettverkstrafikken blir skannet for skadevare i sanntid.

Det anbefales at det etableres rutiner for sjekk av skadevare på flyttbare media, spesielt for eksterne aktører (konsulenter, driftsingeniører etc.) og begrens bruk av disse enhetene i DMZ(-er) og IAK-nettverket.

5.3 Logging

Logger fra sikkerhetsrelevante servere, IDS-er, brannmurer og andre nettverkskomponenter inneholder alle data som er nødvendig for å gi et komplett bilde over sikkerhetstilstanden i IAK-systemet. I tillegg så er dette svært viktig informasjon som benyttes i forbindelse med etterforskning og håndtering av angrep.

Det anbefales å benytte *Security Incident Event Management* (SIEM) til å samle, korrelere og analysere logger produsert av enhetene nevnt ovenfor. I noen tilfeller kan også et SIEM-produkt samle logger fra IAK-enheter. Et SIEM-produkt bør i tillegg kunne visualisere hendelser, være i stand til å visualisere angrep og indikasjoner på angrep i sanntid [5].

Kilder

1. NOU 2006: 6, Når sikkerheten er viktigst – Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner, Justis- og beredskapsdepartementet.

2. Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defence-In-depth Strategies, Homeland Security 2009.

3. NIST SP 800-82, Guide to Industrial Control Systems (ICS), NIST 2011.

4. PA Consulting Group and PNI, Good Practice Guide – Process Control and SCADA Security, Centre for the Protection of National Infrastructure.

5. N-01 Network Security Guidance, Nasjonal sikkerhetsmyndighet.

6. N-02 Security Guidance For Switches And Routers, Nasjonal sikkerhetsmyndighet.

7. G-03 Baseline IT Security Functionality, Nasjonal sikkerhetsmyndighet.

8. G-04 Baseline IT Security Design, Nasjonal sikkerhetsmyndighet.

9. G-05 Baseline Infosec Configuration, Nasjonal sikkerhetsmyndighet.

10. G-06 Baseline IT Security Assurance, Nasjonal sikkerhetsmyndighet.