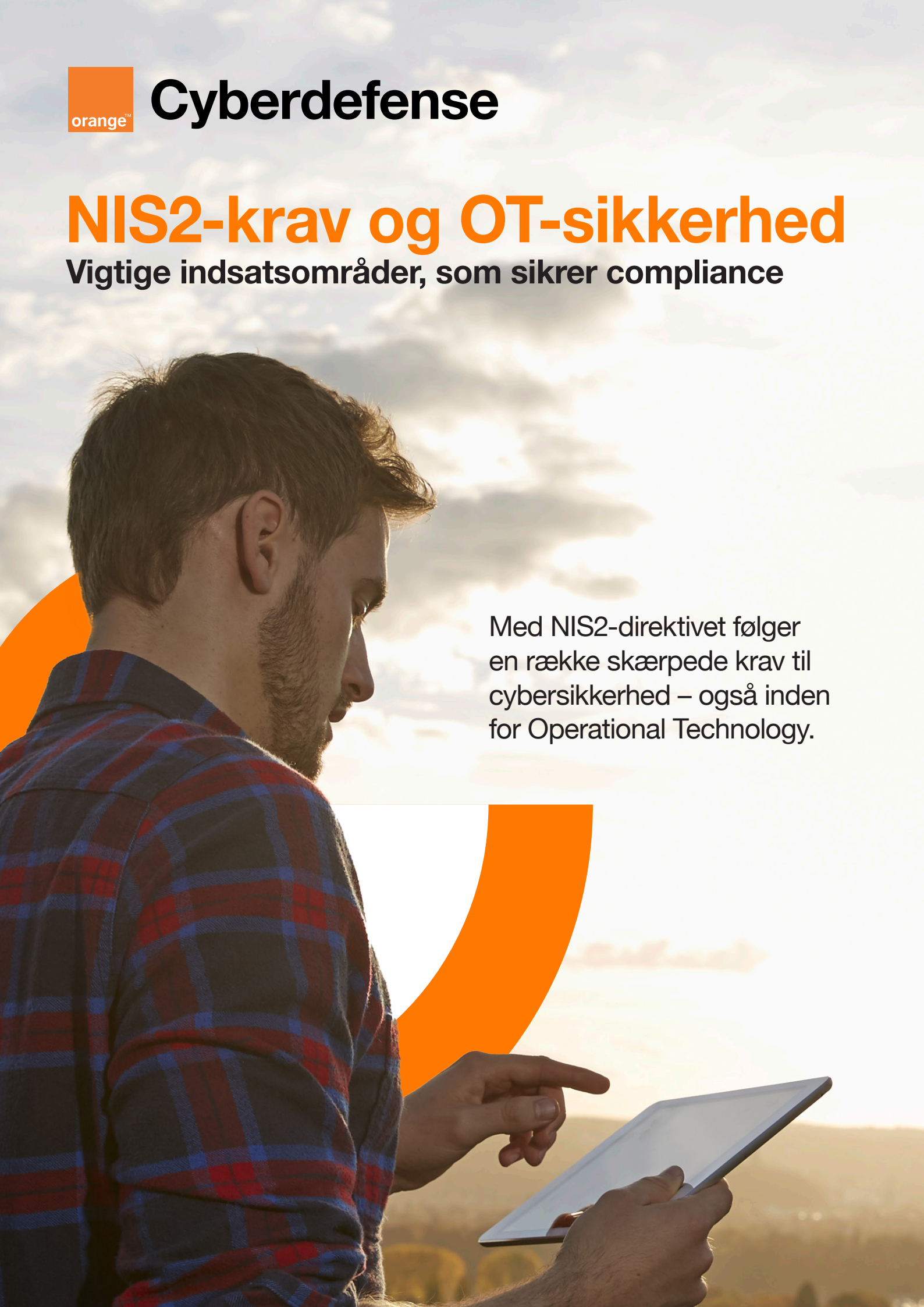
Cyberdefense

NIS2-krav og OT-sikkerhed

Vigtige indsatsområder, som sikrer compliance



Med NIS2-direktivet følger en række skærpede krav til cybersikkerhed – også inden for Operational Technology.

1. Governance i OT-miljøer

2. Risikostyring i OT-miljøer

3. Risikostyring i hele forsyningskæden

4. Hændelseshåndtering og krisestyring i OT-miljøer

5. Adgangskontrol til OT-miljøet

6. Asset Management i OT-miljøet

7. Overvågning og test af OT-miljøet

8. Håndtering af sårbarheder i OT-miljøet

9. Security by Design i OT-miljøet

10. Træning og awareness for alle OT-medarbejdere

11. Fysisk sikring af OT-miljøet

Denne oversigt beskriver de vigtigste indsatsområder, du bør prioritere.

Hvert område er vigtigt, fordi de bidrager til at opbygge den nødvendige robusthed i jeres cyberforsvar og styrke modstandskraften overfor cyberangreb, samtidig med at I opfylder compliancekravene i NIS2-lovgivningen.

1. Governance i OT-miljøer

Styrk overblikket, ansvaret og kontrollen med sikkerheden i OT-miljøet.

- Implementer tydelige governance-rammer for cybersikkerheden i jeres OT-miljøer og sørg for, at ledelsen har det nødvendige overblik over jeres sikkerhedspraksis og indsigt i, hvem der har ansvaret for OT-sikkerheden.
- Sørg for, at have jeres disaster og recovery strategier og beredskabsplaner for katastrofegenopretning af jeres OT-systemer på plads, så I sikrer, at driften og produktionen kan fortsætte også under angreb.
- Udarbejd og implementer følgende lokale OT-dokumenter:
  - OT-sikkerhedspolitik
  - Katastrofeberedskabsplan
  - Incident response-plan
  - Plan for forretningskontinuitet
- Udpeg en dedikeret OT-sikkerhedsansvarlig (DSO) som har ansvar for at implementere cybersikkerhedsstrategien og håndtere risici. Sørg for at DSO'en har relevant erfaring, de nødvendige kompetencer og de rette ressourcer til at udføre opgaven effektivt.
- Udpeg en lokal OT-ansvarlig og styrk det globale OT-sikkerhedsteam som udvikler og vedligeholder blueprints, politikker, procedurer, navngivningsstandarder m.m., og sørg for, at de samarbejder tæt med lederne af jeres forskellige produktionsmiljøer og IT-afdelingen.
- Sørg for, at der er en OT-ansvarlig på hvert site, som har det fulde overblik over hele produktionsnetværket, med cybersikkerhed som førsteprioritet, samt et klart mandat og de nødvendige ressourcer, der skal til for at sikre hele OT-miløet.

2. Risikostyring i OT-miljøer

Integrer risikostyring i den daglige drift og gør det til en del af jeres faste rutine.

- Udarbejd og implementer en strategi, der kan fungere som en ramme for jeres risikostyring i OT-miljøet.
- Planlæg og gennemfør løbende risikovurderinger. Det er nødvendigt at udføre regelmæssige risikovurderinger af jeres OT-systemer for at identificere sårbarheder og trusler og sikre løbende tilpasning til nye risici.

3. Risikostyring i hele forsyningskæden

Få styr på sikkerheden i hele værdikæden – også hos jeres leverandører.

- Vurder løbende sikkerheden i jeres OT-relaterede forsyningskæder, og sikr, at leverandører og tredjepartsudbydere følger ensartede og opdaterede OT-cybersikkerhedskrav for at reducere risikoen for eksterne sårbarheder.
- Sørg for, at der er passende foranstaltninger på plads, som sikrer, at I er i stand til at håndtere risici fra tredjeparts-leverandører – især dem, der interagerer med OT-systemer, som f.eks. udstyrsproducenter og softwareleverandører.
- Kræv, at alle leverandører og underleverandører opfylder de samme sikkerhedskrav som gælder internt, herunder at de har de tekniske og organisatoriske foranstaltninger, som styrker sikkerheden og robustheden i deres netværks- og informationssystemer.
- Gennemfør due diligence på jeres leverandører og underleverandører for at sikre, at de har de nødvendige sikkerhedsforanstaltninger på plads
- Indfør krav om cybersikkerhed i alle kontrakter med leverandører og underleverandører, der forpligter dem til at leve op til jeres krav.
- Pålæg leverandører og underleverandører at underrette jer om enhver sikkerhedshændelse. Kræv at de rapporterer om alt, der har betydning for sikkerheden i jeres OT-systemer, hvis det vil kunne få væsentlig indvirkning på jeres OT-miljø.

4. Hændelseshåndtering og krisestyring i OT-miljøer

Vær klar til at reagere – hurtigt og effektivt.

- Udarbejd en veldefineret hændelseshåndteringsplan (incident response-plan), som specifikt er målrettet OT-miljøer, så I hurtigt har mulighed opdage, reagere og komme jer efter cybersikkerhedshændelser.
- Udfør en risikovurdering af det aktuelle trusselsbillede for at identificere de potentielle hændelser, I muligvis skal forholde jer til, f.eks. cyberangreb, naturkatastrofer, fysisk sabotage, datalæk og andre typer af sikkerhedsbrud.
- Opret et tværfagligt hændelseshåndteringsteam (incident response-team) som består af de nøglemedarbejdere i organisationen, som er ansvarlige for at håndtere hændelser og kriser.
- Udarbejd klare procedurer for håndtering af enhver potentiel hændelse. Procedurerne skal inkludere trin for identifikation, håndtering og inddæmning, vurdering af konsekvenser, kommunikation og genopretning.
- Opbyg klare protokoller for både ekstern og intern kommunikation, som tydeliggør, ledelsens og nøglemedarbejderes rolle i forbindelse med rapportering om væsentlige, cybersikkerhedshændelser, der påvirker jeres OT-systemer til relevante myndigheder, ansatte, kunder og medier.
- Test jeres hændelseshåndteringsplan regelmæssigt for at identificere svagheder. Gennemfør jævnligt træning, simuleringer og bordøvelser – og opdater planen efter behov.
- Sæt jer godt ind i NIS2-lovgivningen – både den juridiske del og den del, der specifikt handler om rapportering af sikkerhedshændelser til relevante tilsynsmyndigheder og ledelsesansvar i forhold til governance, risk & compliance, så I ikke bliver taget på sengen, når I bliver ramt af et cyberangreb hvor I risikerer påbud og store bøder-og systemer.

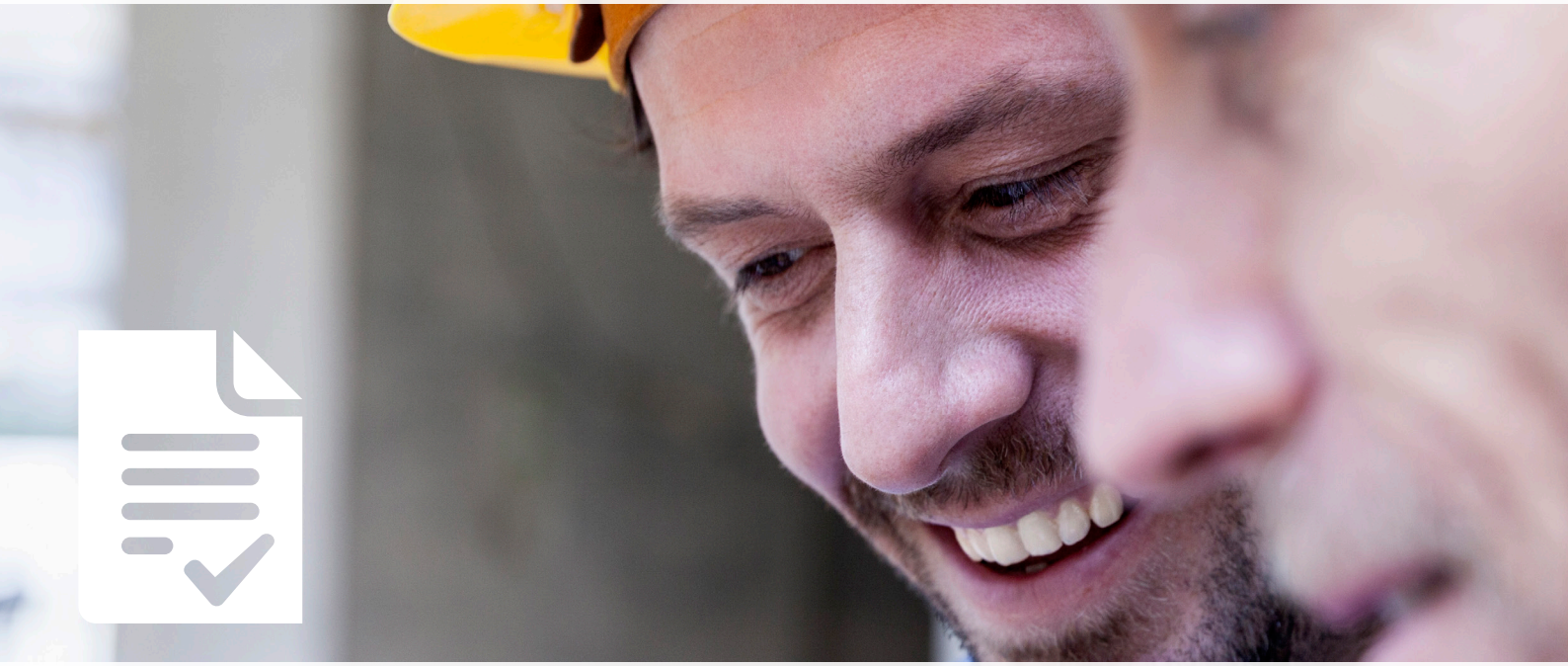
5. Adgangskontrol til OT-miljøet

Hvis alle har adgang, er intet sikkert. Få styr på sikkerheden i jeres OT-miljøer gennem adgangsstyring -og kontrol – og luk truslerne ude.

- Implementer stærke identitets- og adgangsstyringskontroller for at begrænse og overvåge adgangen til jeres OT-systemer.
- Sørg for at adgangen til OT-infrastrukturen udelukkende gives til autoriseret personale gennem passende adgangskontroller, for at sikre, at det kun er de personer, der skal have adgang til jeres OT-netværk og infrastruktur, der har adgang.
- Sørg for, at der kun er én fjernadgangsløsning (remote acces-løsning) til al support og fjernkonfiguration.
- Sørg for at løsningen har overvåget adgang og mulighed for logning og optagelse af alle sessioner.
- Brug også fjernadgang til intern IT-OT-kommunikation.
- Fjernadgangsløsningen bør også anvendes til intern kommunikation fra IT-netværket til OT-systemerne.

6. Asset Management i OT-miljøet

Få overblik over jeres aktiver og sikr at de altid optimalt beskyttet.



- Identificer jeres kritiske OT-aktiver, herunder industrielle kontrolsystemer (ICS), SCADA-systemer og andre centrale OT-komponenter.
- Opret og vedligehold en opdateret oversigt over OT-netværk -og systemer.Sørg for, at der kun er én fjernadgangsløsning (remote acces-løsning) til al support og fjernkonfiguration.
- Implementer en passende praksis for Asset Management for at sikre korrekt håndtering og sikring af aktiverne.
- Dette kan omfatte regelmæssige sårbarhedsvurderinger, patch management og konfigurationsstyring af enheder.

7. Overvågning og test af OT-miljøet

Sørg for, at I kan opdage truslerne i tide – før de gør skade.

- Sørg for at overvåge jeres OT-systemer kontinuerligt og hold godt øje med afvigelser, trusler og ydeevne. Tidlig opdagelse af uregelmæssigheder er afgørende for, at I kan håndtere cybertrusler effentivt.
- Gennemfør regelmæssige test og revisioner (audit) af OT-sikkerheden for at sikre, at systemerne er robuste og modstandsdygtige over for angreb.
- Anvend passiv scanning som standardmetode til overvågning af jeres OT-systemer. Suppler overvågningen med aktiv detektion – særligt på Windows-baserede OT-enheder – hvis det er muligt.

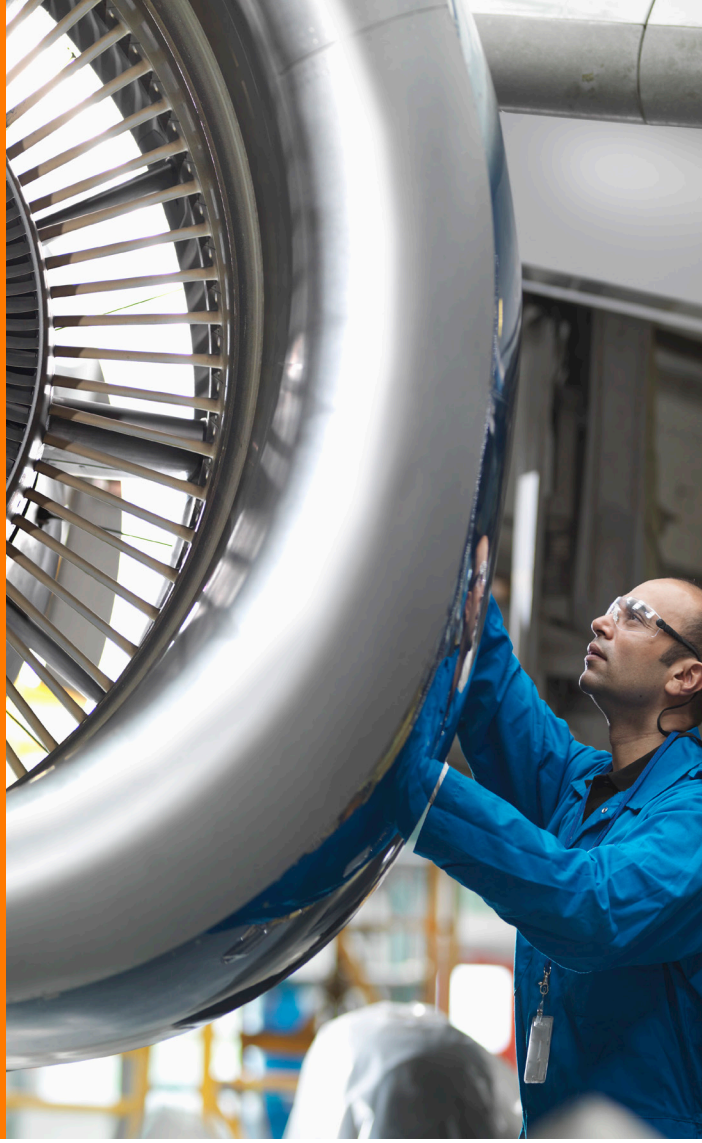
Overvåg især følgende områder:

- Ondsindet eller skadelig kode – som minimum på de mest udsatte aktiver.
- Uautoriserede forbindelser og enheder – overvågningsværktøjet skal kunne se og analysere al trafik.
- Netværkstrafik, infrastrukturaktivitet og infrastrukturændringer – logning er essentielt for at opdage potentielle sikkerhedsbrud.
- Uautoriseret software.

8. Håndtering af sårbarheder i OT-miljøet

Tag hånd om svagheder før de bliver udnyttet.

- Implementer en proces for håndtering af sårbarheder i jeres OT-netværk -og systemer.
- Udfør regelmæssige opdateringer og patching inden for planlagte vedligeholdelsesvinduer. Det er vigtigt at prioritere Patch Management og sætte den nødvendige tid af til åbne servicevinduer – selvom det kan være vanskeligt
- Hvis patching ikke er muligt, skal der udføres en risikovurdering og implementeres passende afværgeforanstaltninger og andre nødvendige tiltag.



9. Security by Design i OT-miljøet

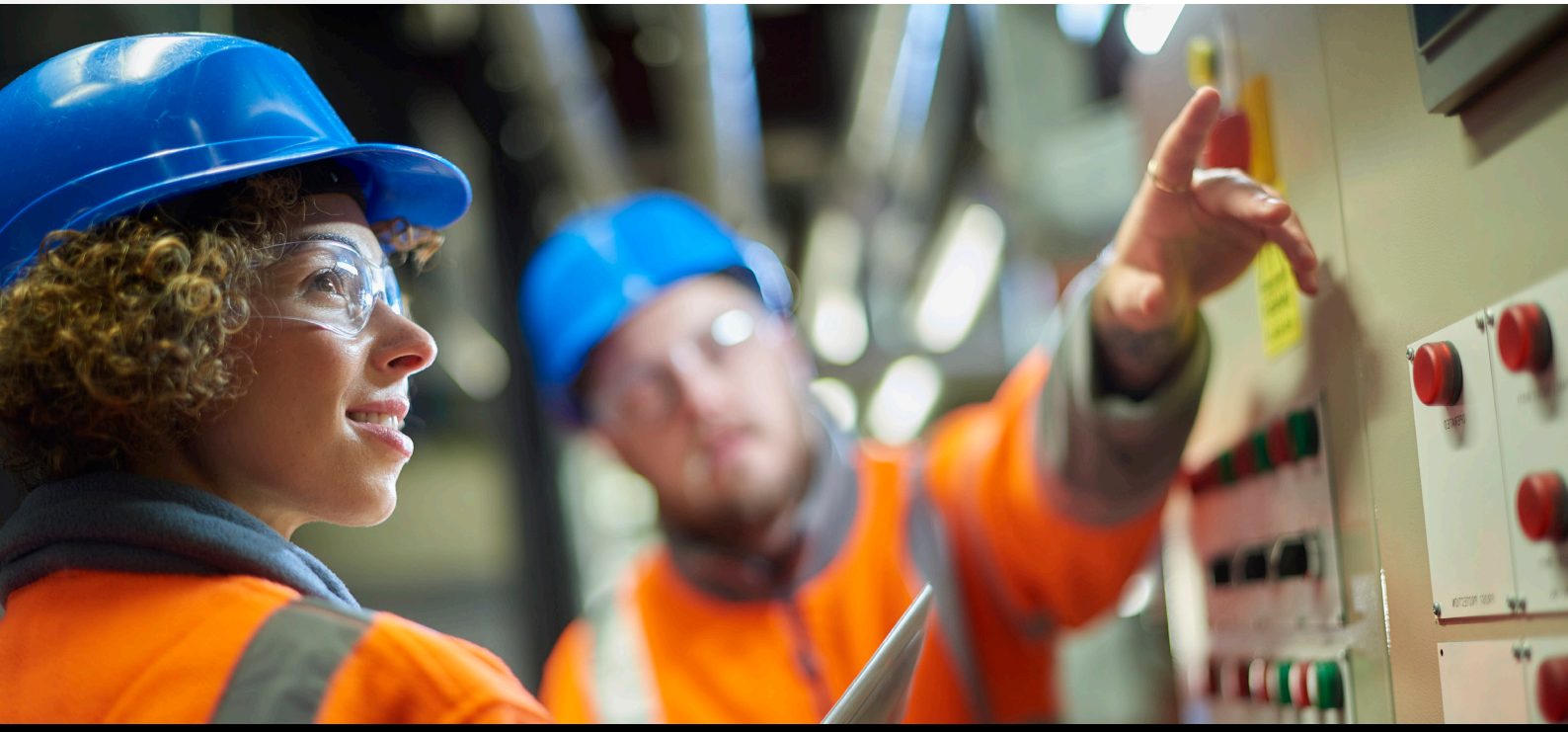
Byg altid sikkerheden ind i jeres OT-systemer fra start.

- Implementer Security by Design i alle nye OT-systemer og følg principperne konsekvent hver gang nye OT-systemer implementeres.
- Etabler processer, der sikrer korrekt konfiguration af jeres OT-netværk -og systemer og kontroller, at konfigurationsændringer håndteres korrekt.
- Indfør passende sikkerhedsforanstaltninger som adgangskontrol, sikre netværksarkitekturer og sikre device-konfigurationer af enheder og software.
- Implementer passende segmentering og isolation af jeres OT-netværk -og infrastruktur for at forhindre uautoriseret adgang.
- Beskyt jeres OT-systemer mod netværksbaserede angreb såsom DDoS ved at implementere egnede sikkerhedsløsninger.
- Segmenter og isoler OT-netværk og infrastruktur for at forhindre uautoriseret adgang.
- Implementer malwarebeskyttelse såsom antivirus og intrusion detection systems, som beskytter jeres OT-systemer mod netværksbaserede trusler og malwareangreb.
- Etabler robuste backup- og genopretningsprocedurer, så jeres OT-netværk -og systemer er modstandsdygtige over for angreb og forstyrrelser.
- Udfør regelmæssige, automatiske backups med korte intervaller. OT-backups bør gemmes på OT-netværket, og offline-backups skal foretages jævnligt for alle enheder.
- Brug værktøjer til automatisk backup af PLC-projekter med versionskontrol og sammenligning af online og offline versioner.
- Følg og dokumenter alle backup-procedurer, verificer eksisterende backups og indfør faste rutiner for periodisk kontrol.

10. Træning og awareness for alle OT-medarbejdere

Sikkerhed starter med viden

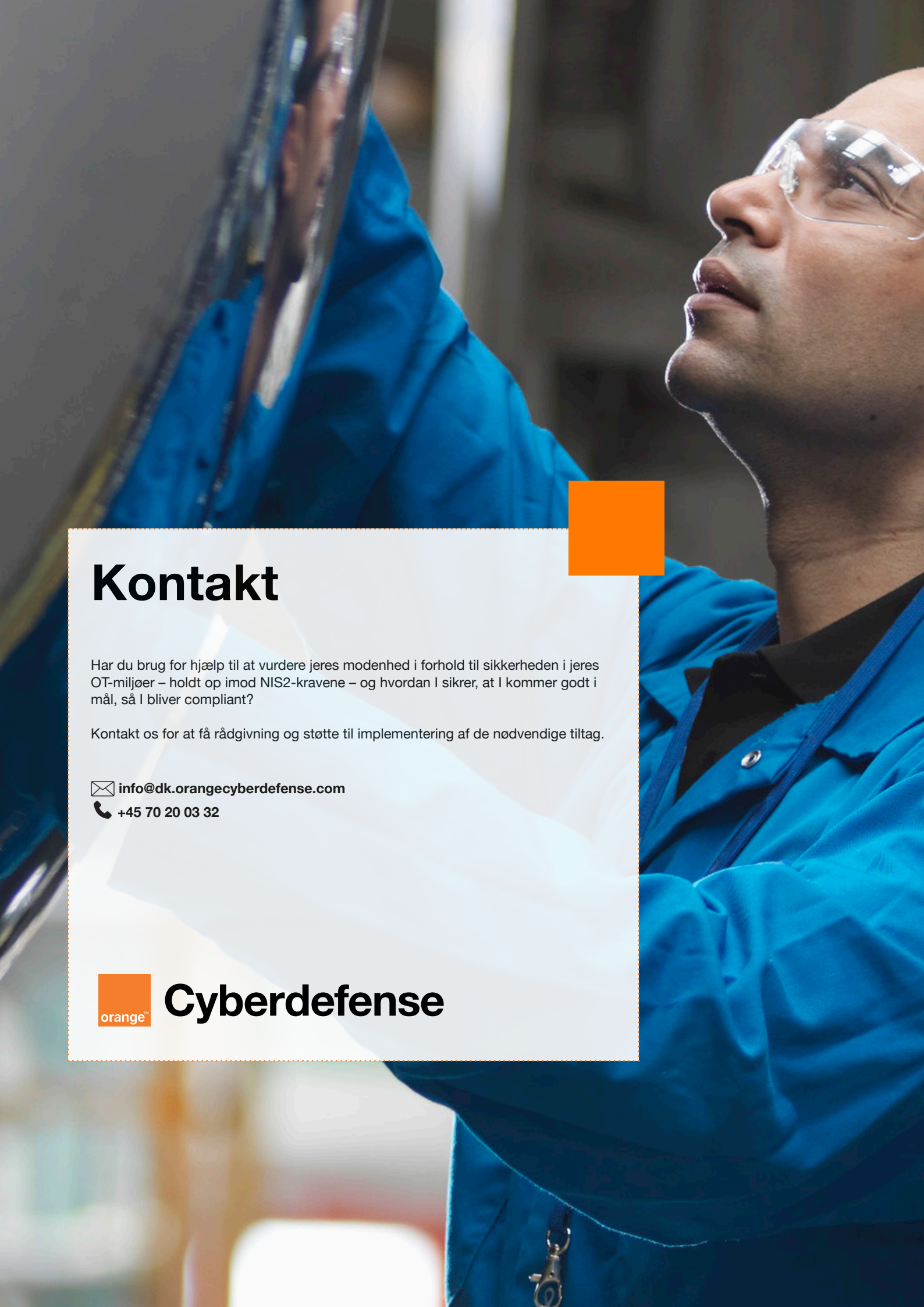
- Implementer awareness-programmer for alle medarbejdere der arbejder med Operational Technology i jeres OT-miljøer.
- Sørg for at alle medarbejdere med ansvar for jeres OT-systemer modtager regelmæssig awarenesstræning og at de kan genkende og reagere effektivt og korrekt på trusler.



11. Fysisk sikring af OT-miljøet

Beskyt det fysiske miljø – ikke kun det digitale.

- Fysisk sikkerhed er vigtig, derfor bør I sørge for at have en stærk adgangskontrol med f.eks. biometrisk autentificering, adgangsbegrænsning til følsomme områder og vagtordninger med sikkerhedsgodkendt personale. Sørg for at etablere processer, der sikrer, at jeres OT-netværk -og systemer er konfigureret korrekt og kontroller, at konfigurationsændringer håndteres korrekt.
- Styrk perimetersikkerheden gennem sikring af jeres yderområder med hegn, barrierer og overvågningskameraer for at forhindre uautoriseret adgang til jeres kritiske OT-infrastruktur.
- Styrk overvågning og patruljering med f.eks. videokameraer, indtrængningsdetektion og sikkerhedsvagter, som kan hjælpe jer med at opdage og reagere hurtigt på sikkerhedshændelser.



Kontakt

Har du brug for hjælp til at vurdere jeres modenhed i forhold til sikkerheden i jeres OT-miljøer – holdt op imod NIS2-kravene – og hvordan I sikrer, at I kommer godt i mål, så I bliver compliant?

Kontakt os for at få rådgivning og støtte til implementering af de nødvendige tiltag.

info@dk.orangecyberdefense.com
+45 70 20 03 32

orange™ Cyberdefense