SEKTOR CERT

Håndbog om SektorCERTs 25 anbefalinger

Udgivet: November 2024

TLP:CLEAR

Anbefalinger

SEKTOR CERT

Generelt

SektorCERT har udarbejdet 25 konkrete anbefalinger, som vi anbefaler alle aktører indenfor kritisk infrastruktur at implementere i deres administrationsnetværk/IT-miljø samt produktionsnetværk/OT-miljø.

Læsevejledning

For mere information om anbefalingernes opbygning, hensigten med implementeringstrinene samt en ordliste, henviser vi til læsevejledningen på side 30.

Baggrunden bag '25 anbefalinger'

De 25 anbefalinger er konkrete forslag til forbedring af cybersikkerheden som er baseret på en dybdegående analyse af kendte, succesfulde cyberangreb mod selskaber indenfor kritisk infrastruktur i Europa samt tre års data fra SektorCERTs sensorer. Anbefalingerne medvirker derfor til at godt forsvar mod kendte angrebsteknikker.

Udarbejdelsen af 'Håndbog om SektorCERTs 25 anbefalinger' er sket i samarbejde med udvalgte medlemmer af SektorCERT. Medlemmerne blev udvalgt på baggrund af deres sektor samt organisationsstørrelse. De udvalgte medlemmer repræsenterer derfor de fleste sektorer som SektorCERT dækker, samt både små, mellemstore og store virksomheder.

Anbefalingerne beskriver, hvordan I, som aktører indenfor dansk, kritisk infrastruktur, bedst muligt kan forhindre cyberangreb samt forberede jer på et cyberangreb.

Afgrænsning

SektorCERT har cybersikkerhed som vores primære fokusområde. Der kan i mange tilfælde være grænsetilfælde eller ligefrem overlap mellem fysisk sikkerhed og cybersikkerhed (fx ved fysisk adgang til netværksporte eller USB-porte). SektorCERT forholder sig ikke til fysiske sikkerhedsforanstaltninger i denne håndbog om 25 anbefalinger.

God cybersikkerhed

Det er vigtigt at understrege, at anbefalingerne ikke er en udtømmende liste, men skal ses som et sæt af minimumsanbefalinger, som alle aktører indenfor kritisk infrastruktur i SektorCERTs optik skal tage stilling til. Anbefalingerne er netop anbefalinger fra SektorCERTs side – de er hverken krav eller forventninger – og skal betragtes som en hjælp til at forbedre cybersikkerheden.

Cloud

Mange virksomheder vælger at lægge dele af deres OT i 'skyen'. Årsagerne hertil kan være mange, men det endelige sikkerhedsansvar hviler fortsat hos vores medlemmer. Uanset hvordan I har valgt at opstille jeres infrastruktur, er de 25 anbefalinger stadig relevante og ledelsen skal sikre, at der er taget stilling til de enkelte anbefalinger.

Rettidig omhu

Implementeringen af anbefalingerne skal foregå uafhængigt af det aktuelle trusselsniveau, da det vil være for sent at påbegynde implementeringen af valgte tiltag når først behovet opstår. Listen af anbefalinger skal derfor ses som en mulighed for at kontrollere, at man enten allerede har alle anbefalingerne implementeret - eller til at få fornyet fokus på at få de manglende anbefalinger implementeret.

Brug SektorForum

Hvis du har brug for sparring omkring gode måder at implementere anbefalingerne på, kan du bruge SektorForum, hvor både vi i SektorCERT og dine kolleger i andre selskaber indenfor kritisk infrastruktur er at finde.

ANBEFALINGER

1 Firewall

Firewall er implementeret og holdes opdateret - gerne med geoblokering af de lande, som ikke er nødvendige at modtage trafik fra.

Derfor er det vigtigt

En firewall leverer basal beskyttelse mod uautoriseret adgang og angreb fra internettet. Firewallens vigtigste rolle er at sikre, at kun internettrafik med relevans for forretningen tillades. Al anden trafik blokeres. Hvis virksomhedens infrastruktur har adgang til internettet, skal man derfor have en firewall.

Anbefalinger – IT

Firewallen skal konfigureres og holdes opdateret med seneste opdateringer af software og/eller firmware. Desuden skal firewallregler, der tillader og blokerer bestemte typer datatrafik fra internettet, holdes opdateret, så de passer til det aktuelle trusselsbillede samt virksomhedens drift (herunder brugen af VPN).

Firewalls kan med fordel benyttes til geoblokering af trafik fra andre lande eller regioner end dem som virksomheden (og evt. jeres leverandører) normalt kommunikerer med, som fx Asien, Afrika og Sydamerika. Det anbefales at geoblokeringen indføres med en allowliste fremfor en denyliste.

Hvis jeres firewall tilbyder supplerende funktionaliteter, skal man overveje fx at filtrere trafikken baseret på selve indholdet, beskytte mod overbelastningsangreb (DDoS), logge datatrafik samt udføre intrusion detection.

Anbefalinger – OT

Firewalls benyttes til at adskille de forskellige lag i OT-infrastrukturen samt til at adskille OT fra virksomhedens øvrige IT-infrastruktur (jvnf. Purdue-modellen - se ordliste).

Implementeringstrin

Niveau 1

- ❑ Installer firewalls ved alle forbindelser til internettet.
- ❑ Verificer at firmwaren på firewalls holdes opdateret.
- ❑ Verificer at firewallregler holdes opdateret.

Niveau 2

- ❑ Indfør geoblokering på både ind- og udgående forbindelser.
- ❑ Verificer at alle porte (både ind- og udgående) som standard er lukket, så kun nødvendige porte er åbne.
- ❑ Eksponer ikke webinterfacet til administration af firewallen mod internettet.
- ❑ Deaktiver svar på ICMP-pakker imod firewallen.
- ❑ Brug statisk IP på ydersiden af firewallen.
- ❑ Genstart regelmæssigt firewallen.

Niveau 3

- ❑ Aktiver DDoS-beskyttelse.
- ❑ Implementer firewalls i cloudtjenester.
- ❑ Indfør logning af, hvem og hvornår der blev lavet ændringer i reglerne.
- ❑ Opsaml logs fra alle firewalls (hvis flere) til et centralt sted.
- ❑ Udfør løbende analyser af opsamlede logdata.
- ❑ Dokumenter alle firewallregler udenfor firewallen (se anbefaling 18).

Niveau 4

- ❑ Installer interne firewalls (som minimum mellem IT og OT, men gerne mellem flere lag).
- ❑ Udfør regelmæssige eksterne pentests mod virksomhedens ydre firewall (se anbefaling 25).
- ❑ Lav regelmæssige kopier af de seneste firewallkonfigurationer og -regler. Kopierne skal sikres offline (se anbefaling 4).

2 Eksponering af services

Kun absolut nødvendige services eksponeres mod internettet.

Derfor er det vigtigt

En interneteksponeret service er fx hjemmesider, API'er, fjernskrivebordsadgange, webinterfaces på enheder samt kamerafeeds. Mange udviklingsafdelinger bruger både eksisterende services (fx API'er) samt udvikler nye services til kommunikation og/eller dataoverførsler. En service som er åben fra internettet ind mod virksomheden, risikerer at blive en åben dør for hackeren. Virksomheden mindsker risikoen for cyberangreb ved kun at eksponere de nødvendige services mod internettet.

Anbefalinger – IT

Virksomheden skal løbende sørge for at gennemgå alle internetvendte services og skabe klarhed over, hvilke der er nødvendige at eksponere mod internettet for at understøtte forretningens drift.

Anbefalinger – OT

Sørg for, at der ikke er direkte adgang til OT-netværket fra de internetvendte services.

Implementeringstrin

Niveau 1

- ❑ Skab overblik over alle services på samtlige enheder, som er eksponeret mod internettet.
- ❑ Sørg for der ikke er direkte adgang fra en interneteksponeret service til enheder i OT-netværket.

Niveau 2

- ❑ Sørg for at kun services som er nødvendige for virksomhedens drift, er eksponeret mod internettet.
- ❑ Deaktiver som standard, alle services på nye internetvendte enheder.

Niveau 3

- ❑ Sørg for at alle interneteksponerede services er dokumenterede, evaluerede og godkendte af en relevant leder.
- ❑ Brug 'security by design' ved (videre-) udvikling af services (fx nye funktioner og/eller nye produkter).
- ❑ Bloker for automatiserede scanninger (såsom SHODAN, Nessus, Qualys eller lign. – evt. udført via TOR-exitnodes) på alle åbne services; med mindre automatiserede scanninger bruges aktivt i virksomheden.

Niveau 4

- ❑ Foretag regelmæssige scanninger efter eksponerede porte og services (se anbefaling 25).
- ❑ Følg alle scanninger op med en evaluering. Vurder om de rette services er eksponerede mod internettet, eller om der skal blokeres yderligere.
- ❑ Sørg for, at de eksponerede services som er egenudviklede, er testet mod et rammeværk som fx OWASP Application Security Verification Standard.

3 Endpoint beskyttelse

Endpoint beskyttelse og firewall aktiveres og opdateres på alle systemer.

Derfor er det vigtigt

Mange angreb starter på en computer fx via phishingemails, besøg på en ondsindet hjemmeside, indsættelse af uautoriseret USB-nøgle eller lign. Endpoint beskyttelse minimerer risikoen for at de enkelte enheder i netværket bliver kompromitteret. Hvis en enhed bliver kompromitteret, sørger endpoint beskyttelsen for, at angrebet ikke spreder sig til andre enheder på netværket.

Anbefalinger – IT

Alle enheder skal hærdes inden tilkobling til netværket. Derudover kan man have logopsamling fra enheden, samt overvåge netværkstrafikken for unormal trafik. Den lokale firewall på enheden skal også aktiveres og vedligeholdes.

Derudover kan man vælge at installere EDR (Endpoint Detection & Response) på alle IT-systemer - både klienter og servere – og lade styringen ske centralt. EDR minder om en traditionel antivirusscanner, men med langt bedre muligheder for beskyttelse.
Husk at logge og advare om, når endpoint-beskyttelse er deaktiveret, da dette kan være et tegn på en ransomwarehændelse.

Anbefalinger – OT

Vær opmærksom på at EDR kan kræve internetforbindelse, samt kan lukke ned for den enhed hvorpå EDR er installeret. I OT-miljøet kan EDR derfor begrænses til enheder, som ikke direkte driver den kritiske infrastruktur (fx engineering workstations, jump hosts osv.).

Implementeringstrin

Niveau 1

- ❑ Sørg for at alle enheder (både IT og OT) er blevet hærdet inden implementering.

Niveau 2

- ❑ Installer endpointbeskyttelse på alle enheder i IT-netværket.
- ❑ Installer endpointbeskyttelse på relevante enheder i OT-netværket.

Niveau 3

- ❑ Sørg for at relevante logs fra de enkelte enheder (både IT og OT) opsamles centralt, hvorfra de bliver analyseret med jævne mellemrum.

Niveau 4

- ❑ Alarmer til centralt hold, hvis lokale EDR-installationer og/eller lokale firewalls bliver deaktiveret.
- ❑ Verificer hærdningen vha. en pentest.

4 Backup

Backup er til stede (herunder off-site backup) og restore afprøves regelmæssigt.

Derfor er det vigtigt

Backup skaber sikkerhedskopier af virksomhedens data og giver derfor virksomheden et trumfkort mod bl.a. ransomwareangreb. Lykkes det en aktør at installere ransomware og kryptere data på virksomhedens systemer, kan en backup gøre det muligt at genetablere systemer og data og dermed sikre virksomhedens drift.

Anbefalinger – IT

Det skal besluttes, fra hvilke enheder der tages backup, hvor ofte der tages backup, og hvor længe backuppen skal opbevares. Backuppen skal gå så langt tilbage i tid, at den kan indlæses uden risiko for at genetablere systemerne med kompromitterede data. Beslutningen kan træffes vha. en kritikalitetsmatrix eller en lignende prioriteret rækkefølge.

Gem en kopi af sikkerhedskopien offsite og offline, så den ikke påvirkes af et ransomwareangreb eller fysiske hændelser (fx brand).

Backup- og restoreprocessen skal regelmæssigt testes og evalueres. Backuppen skal inkludere alle data (herunder også konfigurationer og dokumentation), der er nødvendige for at kunne gendanne forretningskritiske systemer. Genetableringsproceduren skal øves, så virksomheden er sikker på at forretningskritiske systemer kan genetableres indenfor en fastlagt tidsramme.

Anbefalinger – OT

Det er ikke altid muligt at indføre automatiseret backup af OT-enheder (såsom PLC'er og RTU'er), så derfor skal de beskyttes på anden vis. Det kan fx være ved at have opdateret dokumentation af disse OT-enheder samt en kopi af konfigurationsfilerne (og altså ikke af hele enheden). Der skal også foretages backup af SCADA-systemet.

Implementeringstrin

Niveau 1

- ❑ Klarlæg hvilke data og systemer, der er nødvendige fra henholdsvis IT- og OT-netværket, for at gendanne forretningskritiske ydelser.
- ❑ Lav backup af de mest forretningskritiske data og systemer.

Niveau 2

- ❑ Verificer at backuppen virker efter hensigten.
- ❑ Gennemgå alle relevante forretningsområder, og lav en prioriteret rækkefølge af kritiske systemer og data indenfor hvert forretningsområde.
- ❑ Gem backuppen offsite og offline.

Niveau 3

- ❑ Verificer at backuppen er krypteret både under transport (fra relevante enheder til lagringsmediet) samt "i hvile" (når data er gemt på lagringsmediet).

Niveau 4

- ❑ Indfør genetableringsproceduren af backups i beredskabsplanlægningen.
- ❑ Afprøv backupproceduren, med fokus på:
  - at måle tidsforbruget
  - en klar beskrivelse af hvem (medarbejdere) der kan udføre de enkelte trin og hvordan de udføres.
- ❑ Indfør tidsbaserede firewallregler, der kun er aktive i forbindelse med backup.
- ❑ Sørg for at evt. 'backup servicekonti' følger anbefalingerne vedr. begrænsede rettigheder (se anbefaling 19) og passwordlængde (se anbefalnig 5).

5 Passwordlængde

Passwords er udformet efter gældende standarder - dvs. hellere meget lange passwords som skiftes sjældent end kortere passwords der skiftes hyppigt.

Derfor er det vigtigt

Et svagt password er ofte et kort password. En ofte benyttet angrebsteknik er brute force-angreb, hvor en angriber forsøger at logge ind på virksomhedens systemer og/eller netværk ved at afprøve en række brugernavne og passwords for at finde en 'svag' kombination. Lange passwords reducerer risikoen for, at angrebet lykkes.

Anbefalinger – IT

Definer interne krav til passwords og sørg for, at disse krav bliver anvendt i hele virksomheden. Længden er den afgørende parameter for et stærkt password. Krav om at benytte tal og specialtegn (som $ eller @) i passwordet samt at skifte det hyppigt betragtes i dag som forældede.

Et stærkt password...

- er længere end 15 tegn og må gerne indeholde mellemrum. Udtænk gerne en sætning, du selv kan huske.
- indeholder ikke kendte ord eller sætninger, som let kan gættes.
- er længere end 20 tegn, hvis der er tale om en administrator- eller servicekonto.
- skal kun skiftes ved indikation på, at passwordet er blevet kompromitteret.

Et dårligt password...

- består af kendte ord eller sætninger som fx "sommerferie123456" eller "passwordpassword".

Ovenstående praksis skal indføres på alle systemer hvor det er muligt, herunder konti på alle klienter og servere samt eksterne systemer hos leverandører fx i cloud (se også anbefaling 22).

Anbefalinger – OT

Nogle OT-enheder, specielt af ældre dato, tilbyder kun begrænsede muligheder for passwords, og derfor kan det være nødvendigt at have mindre strikse krav til fx passwordlængde. Vær varsom med brugen af specialtegn, mellemrum og danske bogstaver (æ, ø, å), da nogle OT-enheder har svært ved at håndtere dette.

Implementeringstrin

Niveau 1

- ❑ Indfør krav vedrørende passwordlængde for alle konti på alle systemer.

Niveau 2

- ❑ Indfør striksere krav til passwords for administrator- og servicekonti end for alm. konti.

Niveau 3

- ❑ Stil en password manager til rådighed for alle medarbejdere. Sørg for at medarbejderne ikke benytter private password managers til håndtering af virksomhedens passwords.
- ❑ Password manageren der anvendes i OT-miljøet, skal være 'on premise' (dvs. installeret i eget miljø).
- ❑ Indfør sikkerheds-Group Policy på alle AD og standalone systemer, som vedrører krav til passwordlængde og -kompleksitet.

Niveau 4

- ❑ Indfør kontrol af at passwords overholder interne krav på både IT- og OT-miljøet.
- ❑ Sørg for at alle anvendte passwords hashmetodikker er af en langsom type, der er svær at kompromittere. Fravælg hurtige og/eller usikre metodikker.

6 Ingen genbrug af password

Ingen genbrug af passwords - specielt ikke på tværs af IT og OT.

Derfor er det vigtigt

Genbrug af passwords giver en ondsindet aktør bedre muligheder for at kunne bevæge sig på tværs af hjemmesider, applikationer og systemer i virksomheden og øger risikoen for, at aktøren får succes med sit angreb. Har aktøren først skaffet sig adgang til ét system ved at gætte eller stjæle et password, vil det potentielt kunne udnyttes til at logge ind i andre systemer, hvor samme password benyttes.

Genbrug af passwords kan foregå internt i en virksomhed (samme password giver adgang til flere systemer), men kan også ske ved at medarbejdere genbruger passwords på tværs af private adgange (fx Facebook, LinkedIn osv.) og virksomhedens systemer.

Single Sign On (SSO) er en autentificeringsteknologi, hvor en bruger kun skal logge ind én gang, og herefter får adgang til flere uafhængige systemer. SSO er som udgangspunkt en praktisk og sikker teknologi, men kræver at brugernes login håndteres sikkert – bl.a. i form af stærke passwords som ikke genbruges.

Anbefalinger – IT

Implementer SSO hvor muligt. For systemer som ikke understøtter SSO, skal det sikres at passwords ikke bliver genbrugt på forskellige IT-systemer eller brugerkonti.

Anbefalinger – OT

Det kan være en udfordring praktisk at implementere SSO i OT-miljøer. Genbrug aldrig passwords fra virksomhedens IT-systemer (herunder SSO) i OT. Det mindsker risikoen for, at et angreb breder sig fra IT til OT. Brug aldrig det samme password til at logge ind på forskellige OT-systemer.

Implementeringstrin

Niveau 1

- ❑ Implementer, hvor muligt, SSO i IT-netværket.

Niveau 2

- ❑ Stil en password manager til rådighed for alle medarbejdere, som kan afhjælpe risikoen for genbrug af passwords. Ved valg af en password manager, skal der bl.a. tages stilling til hvorvidt løsningen skal være online eller offline. Se også anbefaling 5.

Niveau 3

- ❑ Indfør tiltag, der forhindrer genbrug af passwords på tværs af applikationer og tid. Det kan fx være SSO, awareness og passwordmanagers.
- ❑ Indfør tiltag, der forhindrer genbrug af passwords til administrator- og servicekonti på tværs af applikationer og tid. Det kan fx være SSO, awareness og passwordmanagers.

Niveau 4

- ❑ Indfør tiltag, der forhindrer genbrug af passwords på tværs af IT og OT. Det kan fx være SSO, awareness og passwordmanagers.

7 Ingen fælles logins og standard passwords

Ingen fælles logon og ingen default/standard passwords.

Derfor er det vigtigt

Fælles logins (også kaldet generiske logins) er når en brugerkonto benyttes af flere medarbejdere, hvilket gør virksomhedens infrastruktur sårbar over for angreb. Brug af fælles logins åbner også en mulighed for, at tidligere medarbejdere fortsat kan få adgang til virksomhedens systemer efter ansættelsens ophør.

Vær opmærksom på at fælles logins, i denne sammenhæng, er noget andet end fx SSO, som er en teknologi hvor ét login kan bruges til at logge ind på mange andre systemer.

Standard passwords fra producentens side (fx brugernavn og adgangskode Admin/Admin), udgør en betydelig sikkerhedsrisiko, da passwordet ofte kan findes i manualer, som er tilgængelige online.

Standard passwords sat af virksomheden som bruger enheden, udgør en betydelig sikkerhedsrisiko, da de ofte er lette at knække fx ved brug af et brute force- eller dictionaryangreb og da passwordet kan være kendt af flere medarbejdere.

Anbefalinger – IT

Alle medarbejdere skal have deres egne konti med egne logins. Der skal ikke være fælles konti som bruges af flere medarbejdere – heller ikke selvom disse konti har minimale rettigheder. Passwords skal være personlige og må ikke deles med andre.

Standard passwords, sat af enten producenten eller virksomheden, skal deaktiveres.

Anbefalinger – OT

Som virksomhed skal det tilstræbes at undgå fælles logins og standard passwords i OT. Vær dog opmærksom på at der i dele af OT-miljøet kan være særlige prioriteter og krav, fx vedr. tilgængelighed og vagtskifte/overvågning, der kan gøre det sværere at implementere.

Implementeringstrin

Niveau 1

- ❑ Verificer at der ikke findes fælles anvendte konti på IT- og OT-netværket.
- ❑ Deaktiver standard passwords, ved implementering af nyt udstyr og nye systemer.

Niveau 2

- ❑ Verificer at system- og firmwareopdateringer, ikke genaktiverer standard passwords.
- ❑ Indfør SSO hvor muligt.
- ❑ Gør det nemt at oprette nye midlertidige konti til fx eksterne medarbejdere og praktikanter.

Niveau 3

- ❑ Indfør begrænsning, hvor muligt og hvor relevant, således enhver konto til enhver tid kun kan logge ind ét sted.
- ❑ Indfør GPO ved alle servicekonti, der forhindrer brug af standard passwords.

Niveau 4

- ❑ Udfør regelmæssig kontrol af at kontiindstillinger lever op til interne krav.
- ❑ Evaluer loginlogs for uregelmæssigheder.
- ❑ Indfør, så vidt muligt, at alle IT-konti er domænekonti og ikke lokale konti.
- ❑ Udfør regelmæssige pentests med henblik på at identificere standard passwords (se anbefaling 25).

8 Fjern inaktive brugere

Brugerkonti der ikke anvendes fjernes eller deaktiveres.

Derfor er det vigtigt

En inaktiv brugerkonto udgør en potentiel angrebsvektor for en ondsindet aktør. Dette kan omfatte konti fra tidligere ansatte i virksomheden, som ikke er blevet fjernet eller deaktiveret efter ansættelsens ophør.

Anbefalinger – IT

Det skal jævnligt (og altid ved ansættelsesophør) tjekkes, at der kun er aktive brugerkonti til nuværende ansatte i virksomheden samt evt. relevante underleverandører og kontraktarbejdere. Brugerkonti, som ikke længere benyttes, skal omgående slettes eller deaktiveres.

Anbefalinger – OT

Der gælder som udgangspunkt de samme anbefalinger for OT som for IT.

Implementeringstrin

Niveau 1

- ❑ Hav overblik over nuværende (interne og eksterne) medarbejdere og brugerkonti.

Niveau 2

- ❑ Gennemgå regelmæssigt samtlige brugerkonti, og verificer om disse stadig er gyldige. Gennemgangen involverer både HR og IT-drift og kan enten foregå manuelt eller automatiseret.

Niveau 3

- ❑ Gennemgå regelmæssigt interne systemer for medarbejdere, der ikke længere er ansat i samme rolle (herunder også interne rokader, andre arbejdsområder, forfremmelser, opsigelser m.m.). Vær i denne forbindelse også opmærksomme på eksterne systemer og adgange.
- ❑ Afgør på ledelsesniveau hvorvidt konti til medarbejdere på fx orlov eller barsel, skal deaktiveres eller holdes åbne. Der kan i afgørelsen gøres forskel på eksterne og interne medarbejdere.

Niveau 4

- ❑ Indfør scripts, hvor muligt og relevant, der deaktiverer alle ubrugte konti efter fx 3 eller 6 måneder.

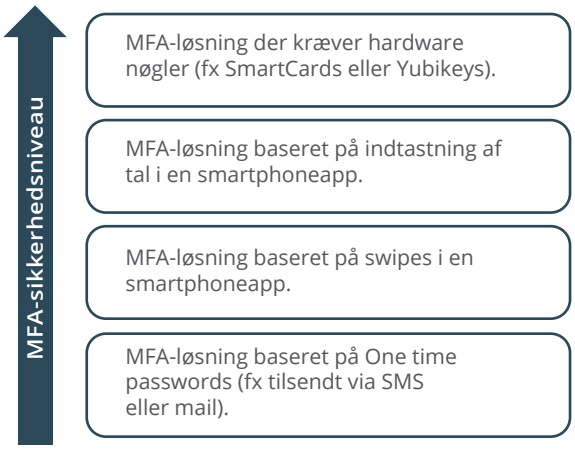
9 Multifaktor validering

Alle services med login, der er eksponeret mod internettet, sikres med multifaktor validering og fjernadgang begrænses mest muligt.

Derfor er det vigtigt

Multifaktorvalidering (MFA) tilføjer et ekstra lag af sikkerhed ved login på virksomhedens systemer via internettet. Multifaktorvalidering benytter princippet om "noget du ved, noget du har og noget du er". Ud over et password kræves også godkendelse via fx en authenticatorapp. Det gør det sværere for en ondsindet aktør at bryde ind i virksomhedens systemer, da det ikke længere er nok at kunne gætte eller stjæle et password.

Vær opmærksom på at der findes forskellige tekniske kategorier af multifaktorvalideringer, med hver deres fordele og ulemper. Det konkrete valg af en multifaktorløsning i virksomheden kan bero på en konkret risikovurdering.



Anbefalinger – IT

Benyt multifaktorvalidering på alle internetvendte og interne tjenester, hvor det er muligt.

Anbefalinger – OT

OT-miljøer består i nogle tilfælde af ældre systemer fra en tid, hvor sikkerhed ikke var i fokus. Derfor kan det være mere udfordrende at sikre OT-systemer med multifaktorvalidering, men det skal gøres, hvor det er muligt og hvor det giver mening.
Vær opmærksom på at nogle MFA-løsninger kræver internetadgang, hvilket frarådes i OT-miljøer.

Implementeringstrin

Niveau 1

- ❑ Aktiver MFA for alle eksterne systemer (adgange via internettet).

Niveau 2

- ❑ Klarlæg hvilke interne systemer (både IT og OT), der både kan og skal have aktiveret MFA.
- ❑ Aktiver MFA for alle administratorkonti.
- ❑ Indfør MFA-app der lever op til virksomhedens IT-sikkerhedspolitik.

Niveau 3

- ❑ Aktiver MFA for alle brugere i relevante systemer i IT.
- ❑ Aktiver MFA for alle brugere i relevante systemer i OT.
- ❑ Indfør forhøjet MFA-sikkerhedsimplementering (se graf til venstre) på relevante systemer.

Niveau 4

- ❑ Gør brug af kontekstuelle MFA-kontroller, der også tager højde for eks. brugerens fysiske lokation, enheds-ID og/eller adfærdsmønstre.
- ❑ Gør så vidt muligt brug af offline MFA-enheder (fx Smart Cards og Yubi-keys) fremfor online (smartphoneapp).

10 Opdatering

Systemerne holdes opdaterede / patchede inklusiv tredjeparts-software.

Derfor er det vigtigt

Softwareleverandører og sikkerhedsforskere opdager jævnligt sikkerhedshuller i programmer, som derefter lukkes ved at leverandøren udsender opdateringer/patches. Holder virksomheden ikke sin portefølje af software opdateret, efterlades softwaren med sårbarheder, der potentielt kan udnyttes af ondsindede aktører til at få adgang til virksomhedens infrastruktur.

Anbefalinger – IT

Sørg for at holde IT-enheder opdaterede. Opdateringer kan verificeres inden installation, for at undgå utilsigtede konsekvenser.

Vær opmærksom på forskellige kategorier af opdateringer. Sikkerhedsopdateringer vedrørende kritiske sårbarheder skal verificeres og installeres hurtigere end eksempelvis funktionsopdateringer.

Aktivér automatiske opdateringer på alle systemer, hvor det er muligt, og hvor nye opdateringer ikke risikerer at føre til driftsforstyrrelser.

Anbefalinger – OT

Der kan være andre risiko-, test- og funktionskrav (herunder certificeringer) til OT-enheder end IT-enheder. Opdateringer af OT-enheder skal derfor håndteres særskilt, så der bl.a. sikres kontinuerlig tilgængelighed og stabilitet af driften.

Implementeringstrin

Niveau 1

- ❑ Aktiver autoupdate på alle systemer, hvor det er muligt, og hvor nye opdateringer ikke risikerer at føre til driftsforstyrrelser.
- ❑ Verificer at der modtages information om nye opdateringer fra leverandører.

Niveau 2

- ❑ Vær klar til at patche enheder hurtigt i både IT og OT-netværket ved kritiske sårbarheder.
- ❑ Verificer at opdateringer ikke fører til driftsforstyrrelser.
- ❑ Hold interneteksponerede enheder, samt enheder som kan modtage mails, opdaterede.

Niveau 3

- ❑ Hold alle IT-enheder opdaterede med verificerede opdateringer.

Niveau 4

- ❑ Hold alle OT-enheder opdaterede under hensyntagen til driftsstabilitet.

11 Identificere end-of-life systemer

Sårbare systemer som ikke kan patches (end-of-life fx) identificeres og der implementeres passende modforanstaltninger for at beskytte dem.

Derfor er det vigtigt

Hardware (herunder firmware) og software (fx applikationer og operativsystemer) bliver på et tidspunkt erstattet af nye versioner. Efter en periode ophører supporten til den ældre version af softwaren, hvilket som regel indebærer, at leverandøren ikke længere leverer opdateringer og patcher sikkerhedshuller. Dette kaldes end-of-life (EOL), og hvis virksomheden ikke identificerer denne type systemer, øges risikoen for angreb på sårbare enheder i infrastrukturen.

Anbefalinger – IT

Vedligehold et opdateret overblik over virksomhedens IT-systemer (se anbefaling 17) og identificér de systemer, som står over for EOL. Udarbejd en plan for, hvad der skal ske med de konkrete systemer (herunder valg af leverandør og passende substitut for enheden). Dette skal gøres rettidigt, da det kan være en tidskrævende proces.
Hvis et system, som fortsat er nødvendigt for forretningens drift, ikke kan udskiftes, skal der træffes en beslutning om alternative sikkerhedsforanstaltninger (fx segmentering og/eller implementering af firewalls).

Anbefalinger – OT

Der gælder som udgangspunkt de samme anbefalinger for OT som for IT. Vær dog opmærksom på, at der ofte er mange EOL-enheder i OT-miljøer, som skal sikres med fx segmentering og/eller firewalls.

Implementeringstrin

Niveau 1

- ❑ Vedligehold en liste EOL for alle systemer (både software og hardware).

Niveau 2

- ❑ Identificer de processer der vil blive påvirket, når et produkt og/eller system, enten er eller nærmer sig EOL.
- ❑ Udnævn en 'OT asset manager' (se anbefaling 17).
- ❑ Udnævn en 'IT asset manager' (se anbefaling 17).

Niveau 3

- ❑ Læg en plan, i samarbejde med procesejere og ledelse, for, hvordan EOL-systemer skal håndteres.

Niveau 4

- ❑ Udfør regelmæssige gennemgange af lister over enheder, der nærmer sig EOL.
- ❑ Lav planen for håndtering af EOL på forkant, så nye systemer kan EOL-systemer i tide (eller alternativt, at EOL-systemer suppleres med sikkerhedsforanstaltninger).

12 Beredskabsplan

En beredskabsplan udarbejdes og vedligeholdes.

Derfor er det vigtigt

En beredskabsplan formulerer på skrift, hvad virksomheden skal gøre i tilfælde af et cyberangreb. Beredskabsplanen skal afspejle virksomhedens strategi for at sikre den primære drift (forsyningssikkerheden) i en krisesituation.

Anbefalinger – IT

For opbygningen af en god beredskabsplan, henviser vi til CFCS' *Cyberforsvar der virker* fra 2023[1]. SektorCERT henviser i øvrigt til gældende lovgivning inden for kritisk infrastruktur.

Afprøv beredskabsplanen jævnligt og hold den regelmæssigt opdateret (herunder kontaktoplysninger på relevante medarbejdere). Sørg for at onboarde nye medarbejdere, så de kender beredskabsplanen.

Anbefalinger – OT

Beredskabsplanen skal fokusere på at holde OT-miljøet fuldstændig afskåret fra konsekvenserne af et cyberangreb, så driften kan fortsætte med mindst mulig forstyrrelse.

Implementeringstrin

Niveau 1

- ❑ Definer virksomhedens overordnede strategiunder en cyberhændelse. Strategien skal tage hensyn til forsyningssikkerheden.
- ❑ Udpeg en OT-beredskabsansvarlig.
- ❑ Udpeg en IT-beredskabsansvarlig.

Niveau 2

- ❑ Udarbejd en beredskabsplan, på baggrund af strategien, der omfatter hændelser i IT-miljøet. Planen skal tage højde for en kritisk hændelse på alle tidspunkter af døgnet.
- ❑ Udarbejd en beredskabsplan, på baggrund af strategien, der omfatter hændelser i OT-miljøet. Planen skal tage højde for en kritisk hændelse på alle tidspunkter af døgnet.
- ❑ Indgå aftale med tredjepart om mulighed for assistance ved en cyberhændelse.

Niveau 3

- ❑ Hold IT-beredskabsplanen ajourført.
- ❑ Hold OT-beredskabsplanen ajourført.
- ❑ Afprøv regelmæssigt dele af både IT- og OT-beredskabsplanen (eksempelvis afgrænset til funktioner eller afdelinger). Brug evalueringer fra øvelserne til at forbedre beredskabsplanerne.

Niveau 4

- ❑ Opbyg de specificerede hændelser (både IT og OT) med udgangspunkt i anerkendte scenarier (fx ROS).
- ❑ Afprøv regelmæssigt hele IT- og OT-beredskabsplanen (på tværs af funktioner og afdelinger). Brug evalueringer fra øvelserne til at forbedre beredskabsplanerne.

[1] Publikationen kan downloades gratis fra CFCS' hjemmeside: https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/-cyberforsvar-der-virker-2023-.pdf

13 Logopsamling

Monitorering / logopsamling implementeres så angreb kan opdages og reageres på rettidigt - fx via SektorCERTs sensorer, honeypots på OT-netværket samt udvidet, intern monitorering.

Derfor er det vigtigt

Monitorering af netværket og logopsamling er afgørende for at kunne opdage og reagere på cyberangreb i tide. Hvis ikke dette er på plads, risikerer virksomheden at overse oplagte indikatorer på ondsindet aktivitet i IT- eller OT-miljøet.

Vær opmærksom på at der findes forskellige former for logs (logs til brug i audits, hændelseslogs på klienter, sikkerhedslogs vedr. administrative loginforsøg og handlinger, netværkslogs, logs fra industrielle enheder m.m.). Det skal derfor defineres hvilke logs der er relevante at opsamle, håndtere og gemme.

Anbefalinger – IT

Aktivér logopsamling på alle relevante enheder i netværket, fx i firewalls, servere og gateways. SektorCERT tilbyder installation af netværkssensorer, som overvåger trafikken til og fra virksomheden og dermed kan hjælpe med at logge og opdage trusler mod infrastrukturen, så der kan træffes modforanstaltninger i tide.

Det kan desuden overvejes at installere udvidet monitorering fra SektorCERT, som omfatter logning og overvågning af processer i udvalgte IT-enheder.

Anbefalinger – OT

På OT-netværket kan der installeres honeypots (se ordliste). Mens en ondsindet aktør forsøger at kompromittere en honeypot, afledes opmærksomheden fra virksomhedens rigtige OT-netværk. En honeypot kan desuden afsløre viden om en aktørs angrebsteknikker.

Det kan desuden overvejes at installere udvidet monitorering fra SektorCERT, som omfatter overvågning af processer i udvalgte OT-enheder.

Implementeringstrin

Niveau 1

- ❑ Indfør logning på alle internetvendte tjenester eller sørg for, at netværkstrafikken logges.
- ❑ Tag stilling til hvilke logs der skal opsamles – herunder forskellige former for logs fra forskellige segmenter – fx
  - Kritikalitetsniveau
  - IT og OT
  - Audits
  - Loginforsøg.

Niveau 2

- ❑ Indfør logning på alle centrale interne IT-systemer – fx via SektorCERTs Udvidet Monitorering.
- ❑ Sørg for, at alle logs har en fælles tidskilde og samme tidszone.
- ❑ Definer
  - hvordan logs skal anvendes
  - hvor længe logs skal gemmes
  - hvordan logs bliver slettet.

Niveau 3

- ❑ Indfør logning på udvalgte OT-systemer (fx jump hosts) – fx via SektorCERTs Udvidet Monitorering.
- ❑ Sørg for, at alle logs bliver opsamlet og opbevaret centralt.
- ❑ Begræns adgangen til logs.
- ❑ Håndter relevante logs (fx kritiske alarmer) 24/7 via et SIEM eller SOC-system.

Niveau 4

- ❑ Sørg for, at logindsamlingen følger gældende best practice (fx
  - NSA m.fl. *Best Practices for event logging and threat detection*
  - CFCS' *Logning – en del af et godt cyberforsvar*
  - CIS-kontrol nr. 6.
- ❑ Indfør backup af logs (se anbefaling 4) eller sørg for, at logs er replikeret på flere systemer.
- ❑ Indfør logning på relevante PLC'er, RTU'er m.m.

14 Awareness

Awareness-træning af medarbejdere gennemføres løbende for at sikre fokus på OT- og IT-sikkerheden.

Derfor er det vigtigt

Opmærksomhed på IT- og OT-sikkerhed i hverdagen er vigtigt for at reducere risikoen for cyberangreb. Hvis ikke medarbejderne udviser kontinuerlig opmærksomhed omkring sikkerheden, risikerer virksomheden at skabe huller i det bolværk, der skal beskytte virksomhedens IT- og OT-miljø.

Afholdelse af awarenesskampagner kan foregå som jævnligt afholdte informationskampagner, ophængning af plakater, afholdelse af phishingtest m.m.

Anbefalinger – IT

Hold løbende fokus på at vedligeholde awareness blandt medarbejderne.

Awareness kan fx omfatte brug afstærke passwords, opmærksomhed omkring phishing emails eller potentielle farer ved at bruge offentlig WiFi.

Awarenesskampagner skal være baseret på det aktuelle trusselsniveau, som virksomheden oplever. Skift jævnligt fokusområder, så der sikres dækning af flere emner.

Der gælder som udgangspunkt de samme anbefalinger for OT som for IT. Dog bør det overvejes at tilrette awarenesstræningen til det aktuelle miljø i OT.

Implementeringstrin

Niveau 1

- ❑ Oplys samtlige medarbejdere om risikoen for cyberhændelser, og gennemgå basale forholdsregler.
- ❑ Afhold awarenesskampagner vedrørende cybersikkerhed.

Niveau 2

- ❑ Indfør differentierede oplysningskampagner, der er tilpassede til specificerede grupper af medarbejdere og samarbejdspartnere. De enkelte kampagner er afstemt det aktuelle trusselsbillede mod den relevante gruppe.
- ❑ Sørg for at alle medarbejdere regelmæssigt får gennemgået træningen og genopfrisket virksomhedens IT-sikkerhedspolitik.
- ❑ Gennemfør tests efter gennemgået træning.

Niveau 3

- ❑ Gennemfør ikke-annoncerede øvelser (fx phishingkampagner) og dokumenter resultatet.
- ❑ Tag hensyn til særlige behov blandt medarbejdere (fx ordblindhed) vha. fx videoer.
- ❑ Opbyg awarenesskampagnerne efter en positiv indstilling og med ros til medarbejdere (ikke 'management by fear').

Niveau 4

- ❑ Indfør awarenesskampagner som 'gamification'.
- ❑ Indfør mål for awarenesstræningen, og dokumenter fremskridt.

15 Kortlægge netværksindgange

Alle netværksindgange til produktionsnetværket kortlægges.

Derfor er det vigtigt

En kortlægning af alle netværksindgange til IT- og OT-miljøet skaber overblik over, hvilke porte der skal monitoreres og eventuelt lukkes af for netværkstrafik. Dermed får virksomheden bedre mulighed for at sikre, at kun forretningskritiske netværksindgange er åbne og overvåges, hvilket reducerer risikoen for angreb.

Kortlægningen vil desuden skabe grundlag for, at der kan implementeres de rette firewalls (se anbefaling 1) og den rette segmentering (se anbefaling 16).

Derudover er det nemmere at gå i ødrift, når alle netværksadgangene er kortlagt. Det kan reducere risikoen for, at et angreb spreder sig fra IT til OT (se anbefaling 24).

Anbefalinger – IT

Skab et overblik over netværkadgange fra IT-infrastrukturen mod OT (produktionsnetværket). Sørg for at holde dette overblik opdateret, når der sker ændringer på netværket.

Anbefalinger – OT

Kortlæg alle netværksadgange ind og ud af produktionsnetværket (både mod IT samt mod andre segmenter og mod internettet). Husk at overveje alternative forbindelser (WiFi, 4G-modems, serielle forbindelser, bluetooth, satellitforbindelser m.m.).

Implementeringstrin

Niveau 1

- ❑ Kortlæg alle netværksadgange til produktionsnetværket med direkte forbindelse til internettet.

Niveau 2

- ❑ Kortlæg alle netværksadgange til produktionsnetværket fra andre segmenter (IT, DMZ m.m.).

Niveau 3

- ❑ Identificér og luk netværksadgange til produktionsnetværket, som ikke er nødvendige for virksomhedens drift.
- ❑ Overvej om nogle netværksadgange kun skal bruges sporadisk (fx ved support). Luk dem, når de ikke bruges.
- ❑ Sørg for at netværksadgangene er beskrevet i beredskabsplanen (se anbefaling 12) så ødrift kan effektiveres.

Niveau 4

- ❑ Kortlæg alternative netværksadgange som fx WiFi, 4G-modems, satellitforbindelser m.m. og beslut om disse er nødvendige.
- ❑ Hold løbende øje med, om nye forbindelser oprettes.

16 Segmentering

Netværket segmenteres i flere lag - som minimum så OT er separeret fra IT. Overvej at isolere eller segmentere yderligere for at opdæmme eller begrænse potentialet i en hændelse.

Derfor er det vigtigt

Opdeling af et netværk i mindre segmenter forhindrer brugere i at få adgang til dele af netværket, som ikke er relevant for deres arbejde. Segmenteringen kan samtidig bremse en ondsindet aktør eller virus/malware i at sprede sig fra en del af netværket til en anden. Dette er især vigtigt for at forhindre angreb på IT-infrastrukturen i at sprede sig til OT-miljøet.

En fysisk segmentering af netværk indbefatter separate netværkskabler, switches osv. En logisk segmentering er opdeling af netværket i separate VLANs, som typisk håndteres i switches. En fysisk segmentering er som udgangspunkt mere sikker end en logisk segmentering, men vil have en større økonomisk omkostning.

Anbefalinger – IT

Gennemgå IT-infrastrukturen og identificér delmængder af netværket, som med fordel kan inddeles i forretningsrelaterede delnetværk som segmenteres fra hinanden. Et delnetværk kan eksempelvis være gæste-WiFi, infoskærme, printere, HR-afdelingen m.m.

Sørg for, at de interneteksponerede services er i et segment for sig (fx en DMZ).
De enkelte segmenter skal kun kommunikere med hinanden via autoriserede forbindelser – fx via en firewall.

Anbefalinger – OT

Sørg for at segmentere IT og OT med en firewall, så der kun er kontrolleret netværksadgang mellem de to segmenter. Det bør overvejes at segmentere OT-netværket yderligere ved at bruge Purdue-modellen som referencearkitektur.

Implementeringstrin

Niveau 1

- ❑ Sørg for at IT-miljøet er segmenteret fra OT-miljøet.
- ❑ Indfør særskilt segment for gæstenetværk.

Niveau 2

- ❑ Sørg for at de internetvendte services er i et særskilt segment.
- ❑ Indfør firewalls mellem segmenterne og definer hvordan (hvis overhovedet) der skal kommunikeres mellem de enkelte segmenter.
- ❑ Indfør en strategi der definerer formålet med de enkelte segmenteringer, herunder om de skal fysisk eller logisk segmenteres.
- ❑ Tilstræb at hver segmentering er opbygget efter 'least privilege'-princippet.

Niveau 3

- ❑ Brug Purdue-modellen (eller en lignende model) som referencearkitektur i den nuværende OT-infrastruktur.
- ❑ Brug Purdue-modellen (eller en lignende model) som referencearkitektur, ved fremtidige udvidelser/opgraderinger af OT-miljøet.

Niveau 4

- ❑ Gennemfør regelmæssige audits og/eller tests for at sikre, at segmenteringen fungerer som forventet.

17 Identificer enheder

Alle enheder i produktionsmiljøet identificeres og dokumenteres.

Derfor er det vigtigt

Nye sårbarheder i software og firmware til computere og netværksudstyr opdages jævnligt og forsøges udnyttet af ondsindede aktører. Ved at identificere og dokumentere alle enheder i produktionsmiljøet gør virksomheden det lettere at få overblik over, hvilke enheder der er sårbare og skal patches. Desuden skaber det overblik over enheder som er, eller nærmer sig, end-of-life, hvorfor virksomheden bedre kan forberede sig på udskiftning af disse (se anbefaling 11).

Vær opmærksom på at enheder både omfatter fysiske enheder (fx computere, PLC'er og RTU'er), software, virtuelle maskiner samt netværkskomponenter (firewalls, switche osv.).

Anbefalinger – IT

Opbyg og vedligehold en fortegnelse over enheder (både hardware og software) herunder pc'er, servere, operativsystemer, applikationer, netværksudstyr m.m. i IT-infrastrukturen, som understøtter driften i produktionsnetværket.

Anbefalinger – OT

Opbyg og vedligehold en fortegnelse over enheder (både hardware og software) herunder pc'er, servere, operativsystemer, applikationer, netværksudstyr m.m. i OT-netværket.

Implementeringstrin

Niveau 1

- ❑ Opret en fortegnelse over de mest kritiske fysiske enheder i produktionsmiljøet.

Niveau 2

- ❑ Identificér de tilhørende enheder, som er nødvendige for at holde de mest kritiske enheder i produktionsmiljøet kørende.
- ❑ Identificér de enheder i IT, som er nødvendige for, at de kritiske processer i produktionsnetværket kan fungere.
- ❑ Udnævn en 'OT asset manager' som har ansvaret for at vedligeholde listen.
- ❑ Udnævn en 'IT asset manager' som har ansvaret for at vedligeholde listen.

Niveau 3

- ❑ Opbyg et system til automatiseret passiv scanning i relevante segmenter af produktionsmiljøet for at kunne opdage nye og ukendte enheder.

Niveau 4

- ❑ Indfør et 'asset management-system'.
- ❑ Gennemfør regelmæssige, tekniske tests for at identificere enheder i produktionsnetværket – bl.a. for at kunne identificere enheder, som ikke aktivt kommunikerer på netværket.

18 Dokumentation

Både logisk og fysisk dokumentation af arkitekturen udarbejdes.

Derfor er det vigtigt

Dokumentation af arkitekturen skaber et overblik over og forståelse for, hvordan enheder i hhv. IT- og OT-miljøet er forbundet til og kommunikerer med hinanden. Vedligeholdt dokumentation gør det nemmere at udarbejde tiltag, som øger sikkerheden og begrænser følgerne i tilfælde af et cyberangreb.

Anbefalinger – IT

Det kan være en stor intern hjælp hvis dokumentationen følger en standard. Dette kan være en international standard (fx NIST, ISO eller andre) eller egne standarder (fx navngivning af enheder).

Arkitekturen skal dokumenteres på et niveau, hvor alle fysiske netværksenheder i arkitekturen indgår. Dokumentationen kan omfatte hardwarespecifikationer, software- og firmware-versioner. Den logiske dokumentation af arkitekturen skal omfatte kommunikation mellem enheder på netværket.

Prioriter at få udarbejdet og vedligeholdt kritisk dokumentation, som eksempelvis skal indgå i en beredskabsplan (se anbefaling 12) og bruges ved en genetablering.

Anbefalinger – OT

Der gælder som udgangspunkt de samme anbefalinger for OT som for IT.

Implementeringstrin

Niveau 1

- ❑ Udarbejd den mest kritiske dokumentation som skal bruges i en beredskabssituation.
- ❑ Udfør regelmæssig opdatering af den kritiske dokumentation.

Niveau 2

- ❑ Dokumenter den logiske opbygning af relevante dele af både IT- og OT-netværksinfrastrukturen.

Niveau 3

- ❑ Dokumenter den fysiske arkitektur – herunder netværksenheder – af relevante dele af både IT- og OT-miljøet (se anbefaling 17) og de fysiske netværksindgange (se anbefaling 15).
- ❑ Sørg for at kritisk dokumentation er tilgængelig i en krisesituation (fx når IT er utilgængelig).

Niveau 4

- ❑ Gennemfør regelmæssigt audits af dokumentation, så der sikres aktualitet og korrekthed.

19 Begræns rettigheder

Rettigheder på brugerkonti begrænses - specielt fokus på at begrænse administrative rettigheder for brugerne, når det ikke er nødvendigt.

Derfor er det vigtigt

Jo færre rettigheder, en bruger har på et system, jo ringere muligheder har en ondsindet aktør for at misbruge en kompromitteret brugerkonto til at bevæge sig længere ind i virksomhedens IT- eller OT-infrastruktur.
Ved at begrænse rettighederne reduceres desuden risikoen for menneskelige fejl, som kan føre til huller i cybersikkerheden.

Anbefalinger – IT

Begræns brugeres rettigheder til de nødvendige (principle of least privilege) for at medarbejderen kan varetage deres arbejdsopgaver. Dette omfatter både hvilke systemer, de må bruge, og hvilke ressourcer (fx netværksdrev), de har adgang til.

Tildel kun administratorrettigheder til de, som har brug for det – herunder relevante IT-administratorer. Begræns desuden rettighederne som administratorer, så der også her benyttes principle of least privilege.

Hvis en medarbejder får nye arbejdsområder, skal vedkommendes adgange til IT-netværket revurderes. Formålet er at sikre, at medarbejderen har de korrekte rettigheder tilpasset sine arbejdsopgaver, og at vedkommende ikke, med tiden, får akkumulerede rettigheder til systemer.

Anbefalinger – OT

Der gælder som udgangspunkt de samme anbefalinger for OT som for IT. Det skal dog sikres, at de medarbejdere, som har ansvaret for driften af den kritiske infrastruktur, har mulighed for at foretage de ændringer, der er nødvendige i en krisesituation – fx via "break the glass" konti.

Implementeringstrin

Niveau 1

- ❑ Sørg for, at brugerne ikke er lokaladministratorer på deres PC i både IT og OT.
- ❑ Opret kun administratorkonti til udvalgte medarbejdere med et arbejdsbetinget behov.

Niveau 2

- ❑ Opret brugerkonti efter 'principle of least privilege'.
- ❑ Kategoriser medarbejdere i roller (såsom ledelse, administration, IT og drift), hvortil der defineres nødvendige arbejdsopgaver. Opret konti i henhold til disse roller.
- ❑ Indfør forskellige grader af IT-administratorkonti, såsom lokal administrator, domæne administrator og systemadministrator.
- ❑ Indfør særskilte konti for IT- og OT-miljøet.
- ❑ Sørg for at service-konti ikke har administratorrettigheder, men er oprettet efter 'principle of least privilege'.

Niveau 3

- ❑ Indfør begrænsninger i OT-miljøet, således at brugere i OT-miljøet ikke kan rette i systemer, som bruges til driften af den kritiske infrastruktur, uden et arbejdsbetinget behov.
- ❑ Udfør regelmæssige checks af alle roller og konti, hvor det sikres at rollerne kun har tilstrækkelige rettigheder til at udføre deres opgaver. Desuden skal det sikres, at alle konti stadig er relevante (se anbefaling 8), samt at alle konti er tilknyttet en relevant rolle.

Niveau 4

- ❑ Monitorer alle aktiviteter udført af administrator-konti.
- ❑ Indfør tidsbegrænsning på brugen af administratorkonti.

20 Politik for adgang

Politik for adgang til produktionsnetværket etableres.

Derfor er det vigtigt

En politik for adgang systematiserer adgange til virksomhedens OT-miljøer ved at sikre, at kun de rigtige personer har adgange til de relevante systemer på de nødvendige tidspunkter. Politikken skal omfatte logiske adgange. En manglende adgangspolitik risikerer at give medarbejdere og eksterne leverandører adgang til dele af produktionsnetværket, som de ikke skal have adgang til. Denne adgang kan potentielt udnyttes af en ondsindet aktør, der har kompromitteret en medarbejders eller leverandørs brugerkonto.

Anbefalinger – IT

Et produktionsnetværk omfatter som udgangspunkt ikke IT. Der kan dog være tilfælde, hvor produktionsnetværket modtager data fra IT-systemer og -services (herunder vejrdata og tariffer), som derfor også skal være omfattet af produktionsnetværkets politik for adgang.

Anbefalinger – OT

Udarbejd og håndhæv en politik for adgang til virksomhedens OT-produktionsnetværk. Dette omfatter den logiske adgang til systemer gennem brugerlogin samt evt. fjernadgang til produktionsnetværket.

Særligt i større virksomheder, kan det være en fordel at definere roller og privilegier, baseret på arbejdsområder i virksomheder, som metode til at håndtere alle medarbejdere og sikre et højere sikkerhedsniveau. Politikken for adgang skal tildele adgangsrettigheder ud fra personens rolle i organisationen og altid begrænse adgangen til kun de absolut nødvendige ressourcer i produktionsnetværket.

Implementeringstrin

Niveau 1

- ❑ Definer brugerroller og ansvarsområder, baseret på 'principle of least privilege'.

Niveau 2

- ❑ Indfør RBAC (Role Based Access Control) for alle konti i OT. Rettigheder skal tildeles rollerne og ikke de enkelte personer.

Niveau 3

- ❑ Sørg for at politikken dækker alle brugeradgange, og verificer at disse er i den rigtige kategori samt om kategorierne er dækkende for tildelte arbejdsopgaver.
- ❑ Adgangspolitikken skal bl.a. tage højde for VPN-adgange ind i OT-miljøet.

Niveau 4

- ❑ Sørg for at Access Control Configuration er kodeordsbeskyttet, som minimum på administratorniveau (se anbefaling 5).
- ❑ Sørg for at kun OT-enheder får adgang til produktionsnetværkets AD.

21 Politik for ændringer

Politik for ændringer til den digitale del af produktionsnetværket etableres.

Derfor er det vigtigt

En politik for ændringer i den digitale del af produktionsnetværket, systematiserer ændringer, så det fx specificeres hvem der må udføre ændringer og hvornår de må udføres. Hermed minimeres risikoen for fejl, og der sikres roll-back procedurer i tilfælde af uforudsete fejl.

Anbefalinger – IT

Et produktionsnetværk omfatter som udgangspunkt ikke IT. Der kan dog være tilfælde, hvor produktionsnetværket modtager data fra IT-systemer og -services (herunder vejrdata og tariffer), som derfor også skal være omfattet af produktionsnetværkets politik for adgang.

Anbefalinger – OT

Udarbejd og implementér roller og processer for, hvem i organisationen der må udføre hvilke ændringer i OT-infrastrukturen.

Ændringer kan omfatte, men er ikke begrænset til:

- Opdateringer/opgraderinger
- Patches
- Netværkstopologi
- Udrulning af nye programmer
- System-/brugeradgange

Overvej at følge etablerede standarder for ændringsstyring (fx ITIL).

Implementeringstrin

Niveau 1

- ❑ Dokumenter alle ændringer af konfigurationer i OT-miljøet.

Niveau 2

- ❑ Informer relevant personale og samarbejdspartnere om ændringer i produktionsnetværket.

Niveau 3

- ❑ Brug en skabelon for alle typer af ændringer i OT-miljøet.
- ❑ Implementer en politik for ændringer i OT.
- ❑ Indfør en change management proces.

Niveau 4

- ❑ Etabler et CAB-board (Change Advisory Board), der kan hjælpe med at prioritere ændringer.
- ❑ Indfør systemmæssig understøttelse af change management processer.

22 Leverandørstyring

Politik for leverandørstyring inklusiv hvordan det kontrolleres, at leverandørerne lever op til dine sikkerhedskrav, etableres.

Derfor er det vigtigt

Leverandørstyring øger sandsynligheden for, at virksomhedens IT- og OT-leverandør(er) lever op til virksomhedens krav til cybersikkerhed.

Anbefalinger – IT

Virksomheden skal udpege en medarbejder med ansvar for at opstille sikkerhedskrav til leverandører, samt sikre at IT -leverandøren lever op til disse krav .
Sikkerhedskravene til leverandører skal afspejle virksomhedens egne krav og politikker, herunder krav om opdatering (se anbefaling 10), politik for adgang (se anbefaling 20) samt eksponering af services (se anbefaling 2).

Kravene til leverandøren skal bero på en konkret vurdering af fx leverandørens IT-løsninger og leverandørens procedurer for håndtering af en cyberhændelse. Vurderingen skal desuden afspejle, om leverandørens IT-systemer håndterer forretningskritiske processer hos virksomheden og/eller følsomme persondata. Dokumentation af leverandørens løsninger og tilhørende ansvar, kan evt. håndteres af revisorerklæringer.

Som virksomhed skal man tage stilling til sine leverandørers kædeansvar (dvs. leverandørens leverandører). Overvej i hvilken grad der skal afkræves dokumentation for dette kædeansvar.

Center for Cybersikkerhed har udgivet en vejledning om cybersikkerhed i leverandørforhold, som giver en indføring i leverandørstyring.

Anbefalinger – OT

Der gælder som udgangspunkt samme anbefalinger for OT som for IT, men vær opmærksom på at manglende sikkerhedskrav til OT-leverandører, kan have større indvirkning på driftsstabiliteten.

Implementeringstrin

Niveau 1

- ❑ Udpeg en medarbejder (evt. pr. leverandør), der er ansvarlig for den sikkerhedsmæssige leverandørstyring.
- ❑ Dokumenter og ajourfør en liste over leverandører til IT- og OT-miljøer.
  Listen skal opdele leverandører i relevante kategorier, såsom:
  - Indflydelse på drift
  - Kontinuerlig adgang til egne systemer.

Niveau 2

- ❑ Stil krav til relevante leverandører (både nuværende og kommende). Kravene skal være:
  - Specifikke
  - Målbare
  - Anvisende
  - Relevante
  - Tidsbestemte.
- ❑ Foretag en konkret vurdering af alle leverandørers indflydelse og ansvar for relevante dele af jeres forretningsprocesser samt infrastrukturen.

Niveau 3

- ❑ Udarbejd en særskilt vurdering for kritiske leverandører – herunder leverandørens indflydelse og ansvar.

Niveau 4

- ❑ Sørg for der kun er indgået aftaler med leverandører, der kan leve op til kriterierne.
- ❑ Sørg for en klar rolle- og ansvarsfordeling med leverandøren – både ved normaldrift og ved en cyberhændelse.
- ❑ Etabler en proces for dialog med leverandøren.
- ❑ Før kontrol med leverandøren.

23 Alternative kommunikationskanaler

Alternative kommunikationsmetoder, fx satellittelefon eller SINE-radio som supplement til e-mail og telefon, etableres.

Derfor er det vigtigt

Cyberangreb mod kritisk infrastruktur kan potentielt ramme internet og telefoni. Med alternative kommunikationskanaler til rådighed kan virksomheden bevare evnen til at kommunikere med medarbejdere, samarbejdspartnere, myndigheder og kunder i en krisesituation.

Anbefalinger – IT

Indfør alternativer til internet eller mobilnet, såsom satellittelefon, satellitbaseret internet eller SINE-radio.

Afprøv med jævne mellemrum, at de alternative kommunikationsmidler fungerer efter hensigten. Sørg for at kommunikere tydeligt til relevante samarbejdspartnere, at virksomheden kan kontaktes via disse kommunikationskanaler i nødsituationer.

Anbefalinger – OT

Der gælder som udgangspunkt de samme anbefalinger for OT som for IT.

Implementeringstrin

Niveau 1

- ❑ Klarlæg behovet (dvs. opstil forskellige scenarier) for alternative kommunikationskanaler – fx i tilfælde hvor internet og mobiltelefoner ikke længere er tilgængelige.

Niveau 2

- ❑ Indfør alternative kommunikationskanaler, så nødvendig drift kan opretholdes.
- ❑ Beskriv konkrete procedurer til forskellige scenarier (fx SMS-udsendelser til alle medarbejdere).

Niveau 3

- ❑ Test og evaluer de alternative kommunikationskanaler regelmæssigt.

Niveau 4

- ❑ Revurder jævnligt behovet for og implementeringen af hvordan alternative kommunikations-kanaler kan sikre opretholdelse af driften.

24 Nødprocedurer

Nødprocedurer for alle forretningskritiske processer udarbejdes så funktionen kan udføres i tilfælde af længerevarende IT nedbrud, inklusiv en plan for ø-drift.

Derfor er det vigtigt

Nødprocedurer kan være afgørende for at reducere skadevirkningerne af et cyberangreb. Ved længerevarende forstyrrelser af IT-driften som følge at et angreb kan nødprocedurer for forretningskritiske processer hjælpe virksomheden med at holde de væsentlige dele af driften kørende, mens angrebet håndteres.

Anbefalinger – IT

Udarbejd relevante nødprocedurer for virksomhedens kritiske processer og afprøv løbende, at de fungerer efter hensigten.

Nødprocedurer kan omfatte:

- Udbetaling af løn uden IT. Dette kan fx håndteres ved at udbetale seneste månedsløn manuelt og så justere senere.
- Kommunikation til kunder om nedbrud, hvis internettet er utilgængeligt. Dette kan fx håndteres ved altid at have nok papir og toner på lager, til husstandsomdeling af informationer.
- Nødstrøm fra generatorer eller UPS-anlæg. Dette kan fx håndteres ved installation af eget anlæg eller ved indgåelse af aftale med leverandør, der kan opstille generatoranlæg indenfor en nærmere angivet tidsfrist.

Nødprocedurerne skal omfatte en plan for ø-drift. Denne plan kan bl.a. beskrive hvordan forretningskritiske IT-systemer isoleres fra øvrige IT-systemer samt hvordan virksomhedens hovedsæde isoleres fra datterselskaber/eksterne lokationer.

Anbefalinger – OT

Nødproceduren skal beskrive hvordan OT-miljøet kan isoleres fra virksomhedens IT-netværk, herunder hvordan driften sikres.
Desuden skal der udarbejdes en plan for at isolere og holde OT-miljøet kørende i det tilfælde, hvor virksomhedens OT-leverandør er utilgængelig.

Implementeringstrin

Niveau 1

- ❑ Identificer virksomhedens kerneydelser i en krisesituation.

Niveau 2

- ❑ Opstil forskellige krisesituationer.

Niveau 3

- ❑ Beskriv de nødvendige procedurer for at kunne opretholde kerneydelsen i de opstillede krisesituationer.

Niveau 4

- ❑ Test regelmæssigt de beskrevne procedurer for hver af de opstillede krisesituationer.
- ❑ Afhold øvelse min. 1 gang om året for skiftende scenarier. Øvelserne dokumenteres og evalueres.

25 Sårbarhedsscanninger

Løbende sårbarhedsscanninger og eventuelt penetrationstest gennemføres for at skabe overblik over angrebsfladen ud mod internettet.

Derfor er det vigtigt

Scanninger og penetrationstest af virksomhedens internetvendte samt interne systemer kan hjælpe med at afsløre sårbarheder i den scannede del af IT-& OT-infrastrukturen .

En sårbarhedsscanning kan hjælpe med at identificere sikkerhedshuller, som er offentligt kendte, i ens system samt opstille de tilgængelige patches. En penetrationstest kan klarlægge en potentiel vej ind i infrastrukturen.

Anbefalinger – IT

Sårbarhedsscanninger af virksomhedens interne services samt virksomhedens internetvendte services skal udføres løbende. Scanningerne kan fx afsløre, om eksponerede services er konfigureret på en usikker måde, eller om tilhørende protokoller og software indeholder sårbarheder, der kan patches.
Derudover kan en sårbarhedsscanning være med til at bekræfte, at kun autoriserede tjenester har adgang til internettet.

Forud for en sårbarhedsscanning og/eller en penetrationstests, skal formålet klarlægges. Aktiviteten kan have forskellige fokusområder, såsom:

- Sårbarhedsscanning af internetvendte systemer.
- Sårbarhedsscanning af interne IT-systemer.
- Penetrationstests fra internettet og ind i virksomheden infrastruktur.

Anbefalinger – OT

Vær opmærksom på at OT-enheder kan være mere sårbare overfor aktive scanninger og penetrationstest end IT-enheder. Scanninger og penetrationstests i OT-miljøer skal derfor altid ske, under hensyntagen til driftsstabiliteten. Fokusområdet for en sårbarhedsscanning af interne OT-systemer kan derfor fx være en passiv scanning.

Implementeringstrin

Niveau 1

- ❑ Afdæk behovet for en sårbarhedsscanning.

Niveau 2

- ❑ Beskriv så detaljeret som muligt, formålet og omfanget af en sårbarhedsscanning – fx om formålet er alene at få en liste over eksponerede sårbarheder, eller om disse også må forsøges udnyttet (penetrationstest).

Niveau 3

- ❑ Udfør en sårbarhedsscanning eller penetrationstest og oplist de fundne sårbarheder efter kritikalitet.
- ❑ Gennemfør nødvendige handlinger, som blev klarlagt under sårbarhedsscanningen eller penetrationstesten.
- ❑ Udnævn en 'patch-ansvarlig'.

Niveau 4

- ❑ Udfør regelmæssigt sårbarhedsscanninger eller penetrationstests, med skiftende fokusområder.

LÆSEVEJLEDNING

Anbefalingernes opbygning

Alle anbefalingerne er opbygget efter samme struktur.

Derfor er det vigtigt
En kort beskrivelse af, hvorfor det er vigtigt at tage stilling til denne anbefaling i relation til virksomhedens øvrige sikkerhedstiltag.

Anbefalinger – IT
Ved nogle anbefalinger gælder de samme anbefalinger for IT som for OT. Ved andre anbefalinger er der særlige forhold der gør sig gældende i OT fremfor IT.
I dette punkt vil vi beskrive anbefalingen i henhold til administrations-netværket.

Anbefalinger – OT
Der gælder som udgangspunkt de samme anbefalinger for OT som for IT. Ved nogle anbefalinger kan der være særlige forhold der gør sig gældende i OT fremfor IT, hvilket vil blive beskrevet i dette punkt, som forholder sig til produktions-netværket.

Implementeringsniveauer
Konkrete tiltag, oplistet med de grundlæggende tiltag i niveau 1 og stigende sikkerhedskrav frem mod niveau 4.

13 Logopsamling

Monitorering / logopsamling implementeres så angreb kan opdages og reageres på rettidigt - fx via SektorCERTs sensorer, honeypots på OTnetværket samt udvidet, intern monitorering.

Derfor er det vigtigt

Monitorering af netværket og logopsamling er afgørende for at kunne opdage og reagere på cyberangreb i tide. Hvis ikke dette er på plads, risikerer virksomheden at overse oplagte indikatorer på ondsindet aktivitet i IT- eller OT-miljøet.

Vær opmærksom på at der findes forskellige former for logs (logs til brug i audits, hændelseslogs på klienter, sikkerhedslogs vedr. administrative loginforsøg og handlinger, netværkslogs, logs fra industrielle enheder m.m.). De enkelte virksomheder skal definere hvilke logs der er relevante at opsamle, håndtere og gemme.

Anbefalinger – IT

Aktivér logopsamling på alle relevante enheder i netværket, f.eks. i firewalls, servere og gateways. SektorCERT tilbyder installation af en netværkssensor, som overvåger trafikken til og fra virksomheden og dermed kan hjælpe med at opdage trusler mod IT-infrastrukturen, så der kan træffes modforanstaltninger i tide.

Det kan desuden overvejes at installere udvidet monitorering fra SektorCERT, som omfatter overvågning af processer i udvalgte IT-enheder

Anbefalinger – OT

På OT-netværket kan der installeres honeypots (se ordliste). Mens en ondsindet aktør forsøger at kompromittere en honeypot, afledes opmærksomheden fra virksomhedens rigtige OT-netværk. En honeypot kan desuden afsløre viden om en aktørs angrebsteknikker.

Det kan desuden overvejes at installere udvidet monitorering fra SektorCERT, som omfatter overvågning af processer i udvalgte OT-enheder.

Implementeringstrin

Niveau 1

- ❑ Indfør logning på alle internetvendte tjenester.
- ❑ Tag stilling til hvilke logs der skal opsamles – herunder forskellige former for logs fra forskellige segmenter – f.eks.
  - Kritikalitets-niveau
  - IT og OT
  - Audits
  - Loginforsøg
  - Overvågning af enhedsressourcer

Niveau 2

- ❑ Indfør logning på alle centrale interne IT-systemer.
- ❑ Sørg for alle logs har en fælles tidskilde og samme tidszone.
- ❑ Definer
  - hvordan logs skal anvendes
  - hvor længe logs skal gemmes
  - hvordan logs bliver slettet

Niveau 3

- ❑ Indfør logning på alle centrale interne OT-systemer.
- ❑ Sørg for alle logs bliver opsamlet og opbevaret centralt.
- ❑ Begræns adgangen til logs.
- ❑ Håndter relevante logs (f.eks. kritiske alarmer) 24/7 via et SIEM eller SOC-system.

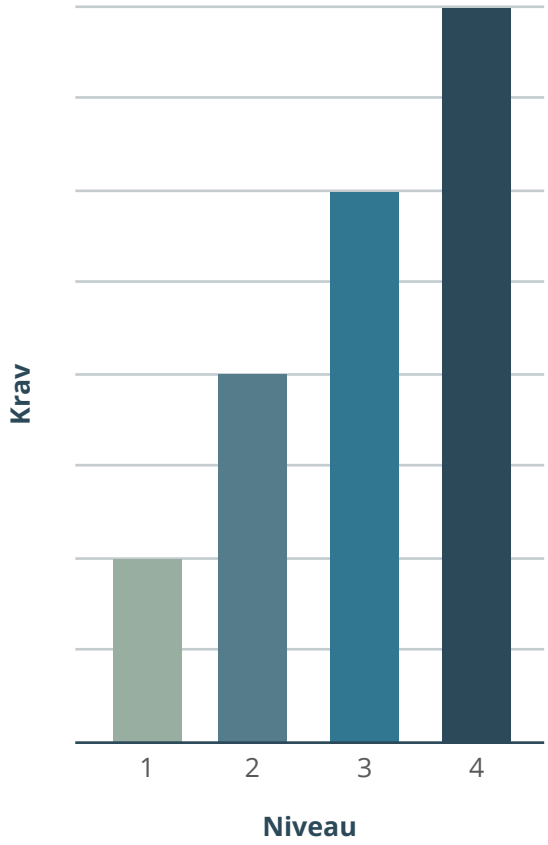
Niveau 4

- ❑ Sørg for logindsamlingen følger gældende best practice (f.eks.
  - NSA Best Practices for event logging and threat detection,
  - CFCS' Logning – en del af et godt cyberforsvar
  - CIS-kontrol nr. 6.
- ❑ Indfør backup af logs (se anbefaling 4).

Implementeringstrin

Til hver anbefaling har vi oplistet en række konkrete tiltag og opdelt i niveauer. Niveau 1 er det grundlæggende niveau, hvor vi forventer mange af vores medlemmer kan opfylde alle tiltagene.

Det bliver gradvist sværere at opfylde alle tiltagene i niveau 2, 3 og 4. For at være på et givet niveau, skal man opfylde alle de listede tiltag samt alle tiltagene i de underliggende niveauer.



Implementeringstrin

Niveau 1

- ❑ Grundlæggende tiltag, som beskytter mod basale cyberangreb.

Niveau 2

- ❑ Simple tiltag, som beskytter mod tilsigtede, dog også ukomplicerede, cyberangreb.

Niveau 3

- ❑ Tiltag, som beskytter mod tilsigtede og mere komplicerede, cyberangreb.

Niveau 4

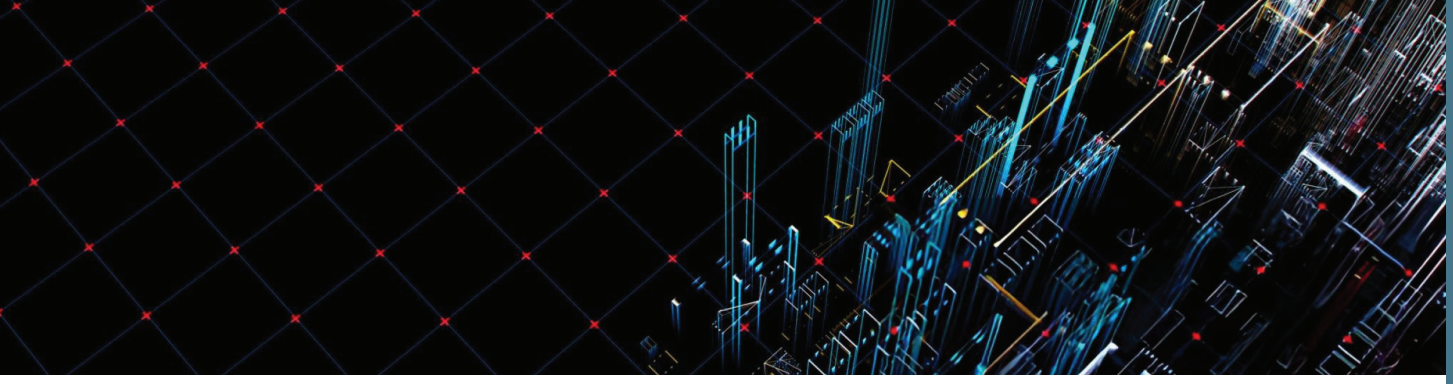
- ❑ Avancerede tiltag, som beskytter mod sofistikerede angreb.

Hensigten med implementeringsniveauerne, er at I, som medlemmer, tager aktivt stilling til, i hvor høj grad I ønsker at implementere den konkrete anbefaling – samt at give mulighed for at måle, hvor langt I er med implementeringen.

Det er vigtigt at understrege at ikke alle medlemmer har behov for at være på niveau 4 i alle 25 anbefalinger. Behovet kan afvejes i forhold til fx økonomi, tilgængelige ressourcer, konsekvens ved et hackerangreb, afvejet risikoanalyse og andet.

SektorCERT anbefaler vores medlemmer at foretage en vurdering af hver enkelt anbefaling, som, sammenholdt med viden om virksomhedens organisation og infrastruktur og risikovillighed, er med til at definere den konkrete implementering (herunder relevante implementeringstrin).

SEKTOR CERT



Ordliste

Nedenstående liste er en forklaring af nogle af de faglige og/eller tekniske ord, der optræder i de 25 anbefalinger.

Der ikke nødvendigvis enighed blandt fagfolk om definitionen af alle ordene i ordlisten. I disse tilfælde er formålet med listen at klarlægge definitionen eller betydningen som SektorCERT arbejder med.

Listen er ikke udtømmende, og afspejler kun de fagtekniske termer som er nævnt i relation til ovenstående anbefalinger. Nedenstående forklaringer er heller ikke nødvendigvis uddybende for det pågældende ord på listen.

Purdue-modellen

Purdue Enterprise Reference Architecture (PERA) - mere populært kendt som "Purdue-modellen" - er en referencemodel til segmentering (adskillelse) af en virksomheds industrielle kontrolssystemer (ICS) fra virksomhedens øvrige forretningssoftware og fra internettet.

Honeypot

En honeypot er en hardwareenhed, der kan programmeres til at ligne en server eller OT-hardware fra producenter som fx ABB, Siemens, Microsoft eller Schneider Electric. En honeypot bruges til at detektere angrebsforsøg mod virksomhedens infrastruktur og opbygge viden om angriberens teknikker og taktikker.

Hærdning

Hærdning er både en strategi og en procedure for minimering af en enheds potentielle angrebsflade. Hærdningen kan omfatte:

- fjernelse af unødvendigt software
- verifikation af, at kun relevante services er aktiverede
- installation af sikkerhedspatches
- deaktivering af USB-porte eller andre fysiske adgange
- begrænsning af rettigheder
- kryptering af harddiske og databaser
- deaktivering af unødvendige netværksporte

Single-Sign-On (SSO)

Single sign-on (SSO) er en autentificeringsteknologi, der gør det muligt for en bruger kun at logge ind med et enkelt ID, og derefter have adgang til flere relaterede, men alligevel uafhængige, softwaresystemer.

Noter

SektorCERT er en non-profit forening, ejet og finansieret af selskaber indenfor dansk kritisk infrastruktur. SektorCERT samarbejder med Europas andre CERT'er, og er med i en række sikkerhedsorganisationer, som gør, at vi har stor viden om angreb mod kritisk infrastruktur.

digital tryghed

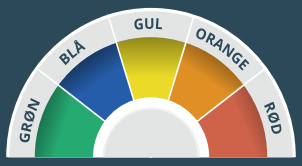
Denne rapport skal give dig svar på følgende spørgsmål:

- Hvorfor er det vigtigt for SektorCERTs medlemmer at implementere de 25 anbefalinger?
- Hvilke konkrete cybersikkerhedstiltag anbefaler SektorCERT til medlemmerne?
- Hvilke forskelle er der på cybersikkerhed i IT- og OT-miljøer?
- Hvordan afgør SektorCERTs medlemmer, i hvilken rækkefølge de prioriterer implementeringen af konkrete tiltag for cybersikkerheden?

Trusselsniveauer

SektorCERT anvender en 5-trins skala til angivelse af trusselsniveau.

Skalaen er baseret på en international standard udarbejdet af Center for internet Security (CIS).



SektorCERTs miljøfokus

CO2 neutral
CLIMATECALC
CC-000091/DK

SVANEMÆRKET
Tryksag
5041 0200

FSC
www.fsc.org
MIX
Papir | Støtter ansvarligt skovbrug
FSC® C109833

SektorCERT har mere end 300 sensorer indenfor dansk, kritisk infrastruktur.

SektorCERT er de kritiske sektorers cybersikkerheds-center. Vi er med til at opdage og håndtere, når den kritiske infrastruktur udsættes for cyberangreb.

Dette dokument er TLP:CLEAR

TLP:**CLEAR**
Informationen kan deles ubegrænset.

Læs mere om Traffic Light Protocol hos FIRST: www.first.org/tlp/

Målgruppe

Alle de af SektorCERTs medlemmer med det strategiske og operationelle ansvar for cybersikkerheden i dansk, kritisk infrastruktur.

- ☑ **Strategisk**
- ☑ **Operationelt**
- ☐ **Taktisk**

Udarbejdelsen af 'Håndbog om SektorCERTs 25 anbefalinger' er sket i samarbejde med udvalgte medlemmer af SektorCERT. Medlemmerne blev udvalgt på baggrund af deres sektor samt organisationsstørrelse. De udvalgte medlemmer repræsenterer derfor de fleste sektorer som SektorCERT dækker, samt både små, mellemstore og store virksomheder.

SEKTOR CERT

Telefonnummer:

+45 88 32 71 40

E-mail adresse:

info@sektorcert.dk

PGP nøgle:

C2EF 6314 7860 2B1E 2341 ACF4 DBC3 511D 3D06 BB3A

Besøgs- og postadresser:

Sommerfuglevej 2A
6000 Kolding

Bredgade 45
1260 København K

CVR nummer:

41369841

Satellittelefon:

+88 16 22 45 60 29

SINE radio:

73 12 056