Medlemskab i SektorCERT
- *sammen er vi stærkere*

AUGUST 2025

TLP:**CLEAR**

SEKTORCERT

SektorCERT er de kritiske sektorers cybersikkerhedscenter.

SektorCERT er en væsentlig del af sektorens forsvar mod cybertrusler. Vi er med til at opdage og håndtere, når de kritiske sektorer udsættes for cyberangreb, og det er hos os, den afgørende viden som kan forebygge det næste angreb, opbygges, og deles.

Vi varetager blandt andet monitoreringen af de virksomheder i sektorerne, som er tilsluttet vores omfattende sensornetværk. Via sensornetværket monitorerer vi internettrafikken med henblik på at opdage cyberangreb mod dansk, kritisk infrastruktur.

SektorCERT er en non-profit forening ejet og finansieret af de selskaber, som driver den kritisk infrastruktur i Danmark.

Vi samarbejder med Europas andre CERT'er, og er med i en række cybersikkerhedsorganisationer, som gør, at vi har stor viden om truslerne mod kritisk infrastruktur.

Formål

Formålet med SektorCERT er, at gå fra en situation hvor hvert selskab der driver den danske, kritiske infrastruktur, står alene med opgaven med at forsvare sig på cyberområdet - til en situation hvor vi står sammen.

Fordi vi ved, at vi er stærkere sammen, end vi er hver for sig.

CERT

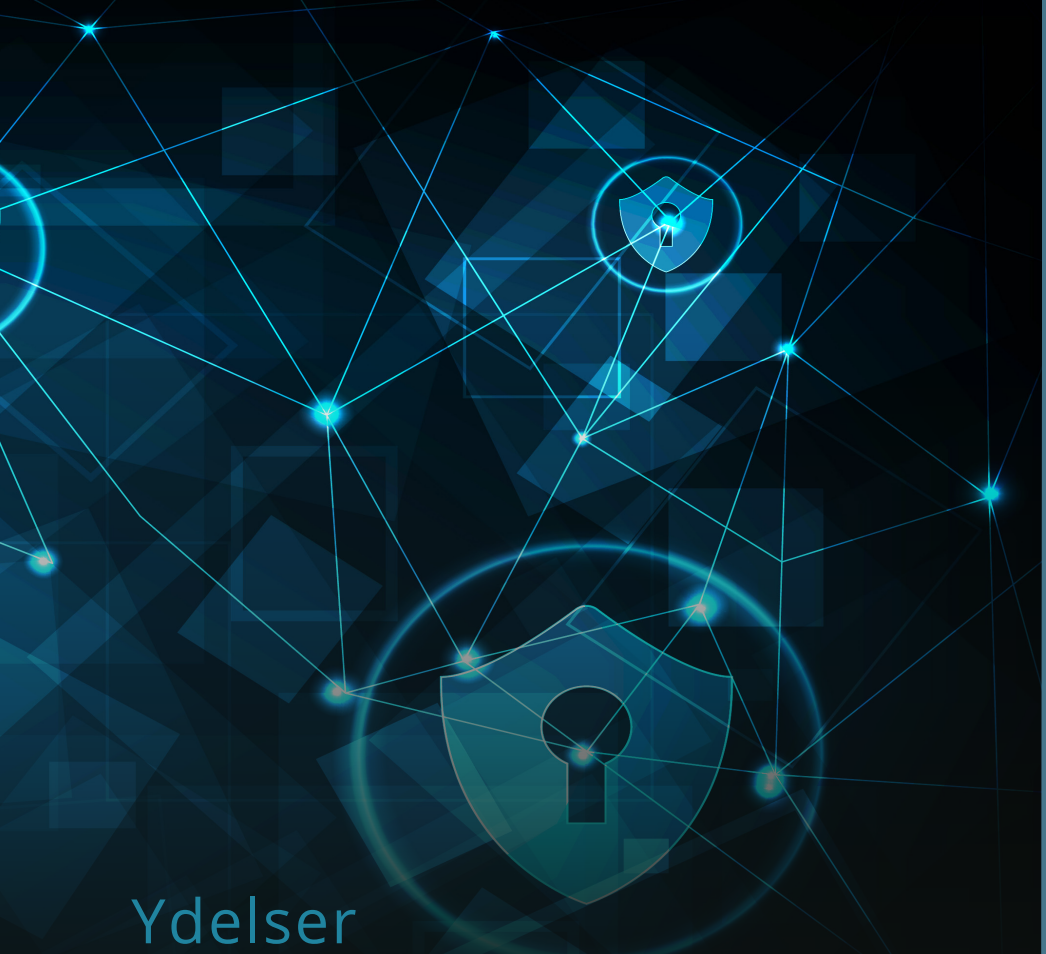
CERT betyder Computer Emergency Response Team, og er en international betegnelse for organisationer, som hjælper en eller flere sektorer med at forhindre, opdage og reagere på cyberangreb.

Medlemskab

Et medlemskab i SektorCERT er en frivillig, men forpligtende aftale, hvor begge parter forpligter sig til at hjælpe med at højne cybersikkerheden for de kritiske sektorer.

Et medlemskab betyder, at I indgår i et fællesskab, hvor I både modtager og giver. Fx har I forpligtet jer til at dele de sikkerhedshændelser, I oplever, med os.

Det er et fællesskab, hvor vi er sammen om at beskytte den danske, kritiske infrastruktur. Og hvor vi deler åbent og ærligt med hinanden.



Ydelser

SektorCERT leverer en række ydelser til vores medlemmer.

Ydelser som har til formål at styrke sektorerne, skabe viden om de trusler, der er relevante for os i den danske, kritiske infrastruktur, samt understøtte videndeling, samarbejde og koordinering.

Som medlem i SektorCERT kan du gøre brug af vores ydelser til at beskytte den kritiske infrastruktur. Disse er beskrevet på de følgende sider.

Ydelser til alle medlemmer

SektorCERT er en non-profit forening, og skal derfor ikke levere et overskud. Derfor kan vi fokusere på at lave de rigtige, langsigtede beslutninger - også selvom det ikke nødvendigvis betaler sig på kort sigt.

Da den kritiske infrastruktur er tæt forbundet, forsøger vi at sikre, at alle medlemmer kan få glæde af vores ydelser - uanset om man er 2 ansatte eller 2.000.

Pris

De fleste ydelser er inkluderet i medlemskabet.
Det gør vi for at få så mange medlemmer som muligt til at benytte ydelserne, så vi får den bedst mulige beskyttelse af kritisk infrastruktur.

Netværks-monitorering

SektorCERT driver et stort sensornetværk, som har til formål at opdage cyberangreb mod de kritiske sektorer samt give et nationalt billede af truslerne. Sensorerne er placeret i medlemmernes infrastruktur med henblik på at monitorere netværkstrafikken til og fra selskaberne.

Sensorernes monitorering udføres af SektorCERT, og er baseret på viden om angreb, som SektorCERT har fra andre CERT'er, åbne og kommercielle kilder, europæiske myndigheder samt internationale samarbejdspartnere.

Passiv

Sensoren er en passiv installation, hvilket betyder, at den ikke kan påvirke eller forstyrre jeres netværk eller infrastruktur.

Sensoren monitorerer trafikken ind og ud mod internettet, og kan alene se den trafik, I allerede sender ud på det åbne internet.

Data

Data fra sensorerne sendes tilbage til SektorCERT via en såkaldt "out-of-band" forbindelse. Det betyder, at de data der sendes tilbage, ikke forstyrrer jeres internetlinje, eller bruger jeres båndbredde.

Data er krypteret både i transit, og når de lagres.

Analyse

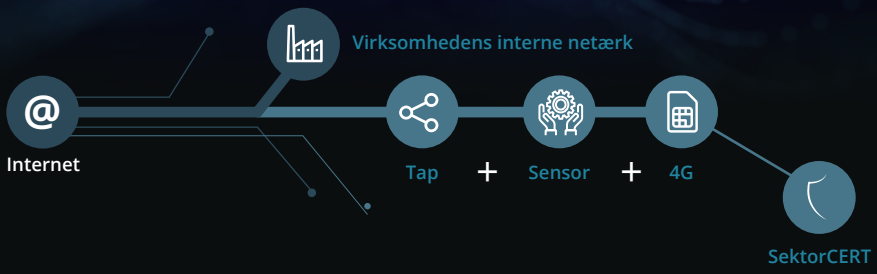
Jeres data analyseres af SektorCERTs egne sikkerhedsgodkendte analytikere.

Hvis der er begrundet mistanke om, at I er ramt af en sikkerhedshændelse, vil vi kontakte jer og informere jer om hændelsen.

ICS

Sensoren analyserer industriprotokoller som Modbus, Profinet m.m.

Dette bruges til at opdage trafik fra PLC'er, RTU'er, SRO'er og andet industrielt udstyr, samt analysere angreb rettet specifikt mod industrielle systemer.



Installation

Tap'en er en passiv enhed, der kopierer netværkstrafikken.

Sensoren får data fra tap'en, og danner information om netværkstrafikken.

Data sendes krypteret til SektorCERTs SOC via en separat 4G-forbindelse.

Honeypot

SektorCERT kan tilbyde at installere en honeypot i jeres produktionsmiljø.

En honeypot er en fysisk netværksenhed, som konfigureres til at ligne fx en PLC, og som alarmerer, hvis en angriber forsøger at tilgå produktions-systemerne.

Rapporter

Data fra netværks-monitoreringen danner grundlag for mange af vores rapporter og notifikationer. Sensorerne giver os en unik viden og indsigt, som gør os i stand til at målrette vores kommunikation.

Fokus på alvorlige trusler

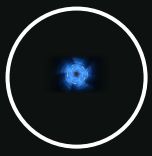
Sensornetværket er alene et ekstra lag af beskyttelse, baseret på den unikke viden, som SektorCERT har via sit internationale netværk.

Vores fokus med sensornetværket er at opbygge viden om trusselsaktører, og de teknikker de benytter mod de kritiske sektorer i Danmark. Denne viden bruger vi til at sikre, at jer der driver den kritiske infrastruktur kan implementere de rette beskyttelsesforanstaltninger.

Udvidet Monitorering

Udvidet Monitorering er SektorCERTs terminologi for MDR (Managed Detection & Response). Med Udvidet Monitorering installeres letvægst-agenter (små stykker software) på hver server og PC i jeres infrastruktur (idéelt set både IT og udvalgte systemer i OT).

Disse agenter kan opdage angreb, vi ikke kan se med vores netværksmonitorering, og bidrager til et samlet 360 graders billede af cybersikkerheden hos jer og på tværs af den kritiske infrastruktur.



Agenten

Vi bruger, hvad vi vurderer er den bedste EDR (Endpoint Detection & Response)-agent, der findes.

Vi har testet alle de ledende produkter, og har valgt at basere os på Crowdstrike, fordi den har vist sig mest effektiv i forhold til at opdage avancerede angreb.

Agenten kan køre på Linux, Mac og Windows

Installation

Der er blot en enkelt fil, som skal installeres på maskinerne.

Det kræver ikke en genstart og kan gøres både manuelt og via software-distributions-værktøjer.

Agenten kan koeksistere med eksisterende antivirus-produkter som fx Microsoft Defender.

Vedligeholde

SektorCERT håndterer al vedligehold og opdateringer, og sikrer, at agenterne hele tiden kan opdage de nyeste typer af angreb.

Hvis man ønsker det, er det muligt at udvælge bestemte PC'ere og servere, som kører den nyeste version, mens de øvrige altid er en version bagud.

Lokalt

SektorCERT har en stor viden om den danske, kritiske infrastruktur, og bringer denne viden i spil i vores analyse af det data, vi indsamler fra agenterne.

Vi kender vores medlemmer, er til stede lokalt, og kan hjælpe jer, når uheldet er ude.

Via vores samarbejde med Nordens største incident response selskab mnemonic, har vi sikret, at alle medlemmer kan få hjælp af både os og de mere end 400 incident respondere i mnemonic.

I har os. Og vi har jer.

Globalt

De dygtigste i verden til at finde "nålen i høstakken" er ubetinget Red Canary.

Med 450 analytikere der i døgndrift leder efter angreb i data, har de en skala og erfaring, vi ikke kan matche.

Derfor hjælper de os med at analysere data og opdage og håndtere angreb, så vi kan sikre, at selvom mange er under angreb samtidig, kan vi stadig håndtere det.

Lokal tilstedeværelse og viden om sektoren. Kombineret med et globalt team af eksperter.

24x7

Hos SektorCERT sidder der fra udgangen af 2025 altid danske, sikkerhedsgodkendte analytikere på vores kontorer i Danmark.

Dermed kan vi opdage og reagere på angreb døgnet rundt og hjælpe jer, når angrebet sker.

Red Canary er også en 24x7-organisation, og har også øjnene på bolden døgnet rundt.

Sammen får i det bedste af det bedste. Alle ugens 7 dage. Alle døgnets 24 timer.

Bemærk

For alle medlemmer af SektorCERT er de første 5 endpoints (PC'ere og servere) inkluderet i medlemskabet.

Der er et ekstra gebyr til sit medlemsskab af SektorCERT for yderligere endpoints som bl.a. dækker licensomkostningerne.

Det samlede billede

Med en netværkssensor kan vi opdage og reagere på angreb, som sker hos jer ved at monitorere internettrafikken fra ydersiden af firewall'en.

Ved at udvide monitoreringen til også at omfatte PC'ere og servere, vil der være en række situationer, hvor vi kan opdage angreb tidligere samt med højere præcision sige, præcist hvor i jeres netværk angrebet er startet, og hvor vi i fællesskab skal sætte ind for at stoppe det.

PC'ere

De fleste angreb starter på de PC'er, som medarbejderne bruger. Fx hvor en medarbejder klikker på noget i en phishing e-mail, besøger en hjemmeside, eller sætter et inficeret USB-drev i.

Udvidet Monitorering giver mulighed for at opdage angrebene, straks når de starter.

Servere

På servere vil monitoreringen hjælpe til at opdage ransomware, og andet som begynder at sprede sig internt i netværket.

Derfor kan det være en fordel både at monitorere PC'ere og servere.

Analyse

Vores SOC - som fra udgangen af 2025 er døgnbemandet - leder konstant efter tegn på angreb i jeres infrastruktur.

Her hjælper Udvidet Monitorering til både at opdage angrebene, og præcisere hvor i jeres infrastruktur de foregår.

SEKTORCERTS SOC

Analytikerne i SektorCERTs SOC (Security Operations Center) analyserer de mange data der indsamles. Data indsamles både fra udvidet monitorering, netværksmonitorering og honeypots på tværs af mere end 300 selskaber indenfor kritisk infrastruktur.

Analytikerne benytterne avancerede SIEM (Security Incident & Event Management) systemer til denne monitorering, og er i stand til at opdage og reagere på angreb på tværs af alle SektorCERTs medlemmer.

Et komplet billede

Ved at se på data på tværs af hundredevis af danske selskaber, kan vi opdage tegn på angreb, man ikke kan se ved kun at se på egne data.
Alle informationer matches direkte mod truslerne, vi kender fra kritisk infrastruktur i andre lande.

Både IT og OT

Både systemer i OT-netværket (netværket hvor de industrielle kontrolsystemer er placeret) samt IT-netværket (typisk kontornetværket) bør monitoreres for at få den bedst mulige beskyttelse.

Data fra netværk kombineret med endpoints (PC'ere og servere) = fuld visibilitet

SektorCERT har nok verdens mest finmaskede net af sensorer i kritisk infrastruktur. Vi dækker mere end 300 selskaber, og kan se al den internettrafik, der går til og fra selskaberne.

Den data er unik. Og kombineret med data fra PC'ere og servere via Udvidet Monitorering, kan vi opdage mere, hurtigere.

Incident Response

Når en virksomhed i en kritisk sektor rammes af et angreb, kan der være brug for hjælp til at håndtere sikkerhedshændelsen.

SektorCERT hjælper med at vurdere og håndtere hændelsen samt sikre koordinering med myndigheder og andre CERT'er. Er opgaven større end vi sammen kan håndtere, har vi sikret, at alle medlemmer er garanteret hjælp fra nordens største IR-selskab.

Fokus på OT/ICS

SektorCERT har fokus på den industrielle sikkerhed, og på kritisk infrastruktur.

Vores viden på området kan hjælpe til at vurdere, om et angreb skal håndteres som en ren IT hændelse eller som en trussel mod kritisk infrastruktur.

Samarbejde

Alle medlemmer af SektorCERT er dækket af en såkaldt retaineraftale med mnemonic - Nordens største IR selskab.

Aftalen sikrer, at alle kan få hjælp - selv ved store hændelser som kræver mange ressourcer.

Mulig observatør

SektorCERT kan også deltage som observatør i håndtering af hændelser.

Herved sikrer vi, at viden om sikkerhedshændelser i kritisk infrastruktur opsamles centralt, og efterfølgende kan deles, så alle kan lære af hinandens hændelser.

Hvornår har man brug for incident response?

Hvis I oplever en konkret hændelse, eller har mistanke om, at I har ubudne gæster i jeres systemer, så er det en god idé at kontakte os.

Det bedste råd er: kontakt os hellere en gang for meget end en gang for lidt.

Eksempler på hændelser

- Ransomware som blokerer for anvendelsen af virksomhedens IT og/eller OT-systemer.
- Virus som spreder sig og ødelægger filer.
- Data som stjæles (fx persondata).

FORBEREDELSE

Plan

Det er vigtigt at have en beredskabsplan, så I er klar, når uheldet er ude.

Øvelse

Øv beredskabs-planen i "fredstid" så I alle ved præcis, hvad der skal gøres.

Kontakt

Hav kontakt-informationer på medarbejdere, SektorCERT og eksterne på et udskrevet ark sammen med beredskabsplanen.

Bemærk

Fra slutningen af 2025 er vi bemandet 24x7. Indtil da leveres ydelsen som "best effort".

Vi har ikke bemanding til at garantere, at vi selv kan rykke ud til alle hændelser.

Derfor har vi indgået aftalen med mnemonic som sikrer alle hjælp - også selvom flere selskaber er ramt på samme tid. Selve retaineraftalen er en del af medlemskabet, mens de timer mnemonic eventuelt bruger på at håndtere hændelsen, betales af medlemmet.

Arrangementer

SektorCERT afholder en række arrangementer, der har til formål at højne sikkerheden indenfor dansk, kritisk infrastruktur.

Vores månedskald, webinarer og undervisning er vores mest direkte måde, hvorved vi kan opkvalificere sektorerne indenfor cybersikkerhed. Vores viden om hvad der sker, sikrer, at vi fokuserer på det, sektorerne faktisk er udsat for.

OT Lab

SektorCERT har opbygget et OT Lab, som består af industrielle komponenter og netværk.

Dette lab anvendes i undervisningen, men der er også mulighed for, at I kan benytte dette lab til test eller udforskning.

Webinarer og månedskald

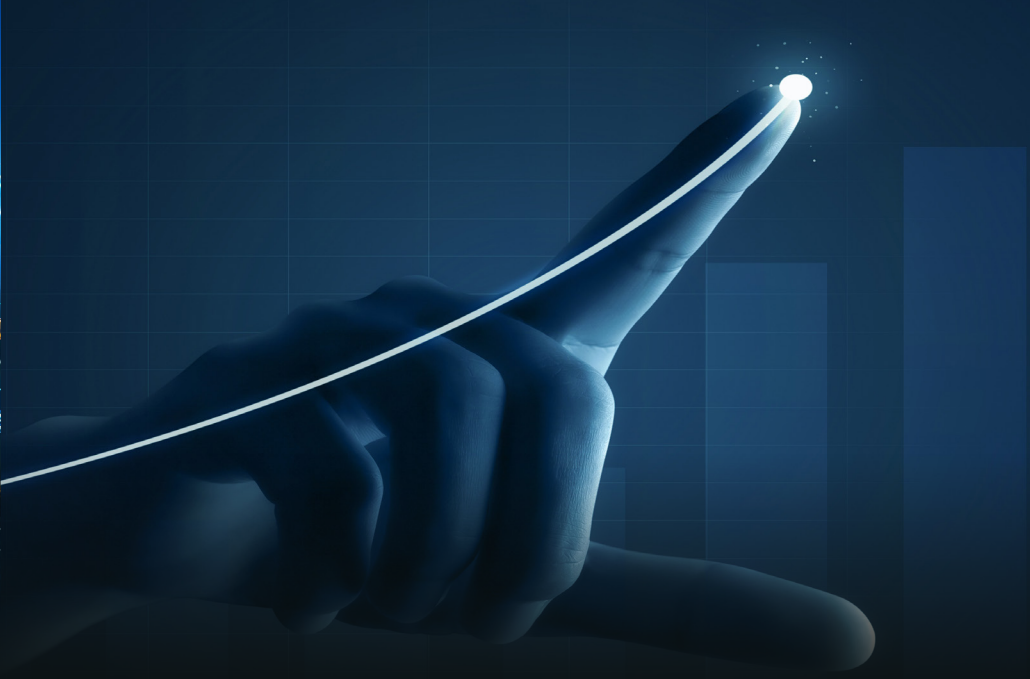
På vores webinarer vil vi præsentere et aktuelt emne for vores medlemmer.

Månedskaldet er en månedlig, 30 minutters opsummering af trusselsbilledet, de angreb vi har observeret, samt medlemmernes egne observationer.

Kurser

SektorCERTs kurser dækker lige fra 2 timers introduktionskurser til flerdags hands-on kurser.

Kurserne afholdes enten fysisk i Kolding eller online. Når vi afholder fysiske kurser, er der gode muligheder for at netværke.



SektorCERTs årlige konference

SektorForum LIVE! er SektorCERTs årlige konference for SektorCERTs medlemmer. Konferencen er skabt for at give dansk kritisk infrastruktur en mulighed for, i et lukket forum, at udveksle erfaringer samt få ny viden om cybersikkerhed indenfor kritisk infrastruktur.

Oversigt

På vores hjemmeside er det muligt at læse mere om vores arrangementer, samt se en oversigt over de aktuelle kurser.

Det er desuden muligt at vælge kurser ud fra ens rolle.

Tilmelding

Du kan tilmelde dig SektorCERTs kurser og konference på hjemmesiden.

Bemærk

Månedskald, webinarer og OT-lab er inkluderet i medlemskabet, mens der er et gebyr for at deltage i konferencen og kurserne.

SektorForum

Vi står stærkere sammen. Derfor driver vi en unik, digital samarbejdsplatform, hvor medlemmerne kan få hjælp og vejledning fra både andre medlemmer og direkte fra os.

Det er på denne platform værdien fra fællesskabet skabes. Her deles erfaringer, angreb, trusler og meget andet. Ved at deltage aktivt på platformen bliver du en del af et fællesskab, og står ikke alene med at beskytte jeres kritiske infrastruktur.

Sikkerhed

SektorForum kører på en sikret platform, som driftes hos SektorCERT i Kolding. Kun SektorCERTs sikkerhedsgodkendte medarbejdere har adgang til infrastrukturen.

Der kræves to-faktor godkendelse for at benytte platformen.

Platform

SektorForum er SektorCERTs primære kanal til kommunikation med medlemmerne.

På denne platform deler SektorCERT information om de senste anbefalinger, angreb, trusler mod den danske, kritiske infrastruktur.

Netværk

Når I stiller spørgsmål på platformen, får I svar fra personer, som også arbejder med kritisk infrastruktur, og kan dermed trække på erfaringer, som andre har gjort sig.

Tilsvarende kan I dele ud af egen erfaring, og være med til at øge viden.

Hvad diskuteres på SektorForum?

SektorForum er et fortroligt forum, hvor alle medlemmer kan mødes og diskutere cybersikkerhedsrelaterede emner, og hvor SektorCERT deler oplysninger om de aktuelle trusler mod sektorerne.

Værdien af ens medlemskab er derfor afhængigt af, at man deltager aktivt på SektorForum.

Eksempler

- Sårbarheder i Zyxel-enheder og hvad man kan gøre for at beskytte sig.
- Ledelsesrapportering og hvad der virker.
- Logning, og hvordan det enkelte selskab forholder sig.
- Observationer omkring phishing.

Opstart

I kommer i gang med at anvende SektorForum ved at skrive til SektorCERT og bede om adgang. I kan tilmelde så mange medarbejdere, som I ønsker.

Adgang

I kan tilgå SektorForum via web (i din browser) mobil (Android og iOS), tablets og via applikationer til Windows og Mac.

Konto

En konto er personlig og knyttet til en e-mailadresse. Derfor skal hver medarbejder, som ønsker at anvende SektorForum, have sin egen konto.

Bemærk

SektorForum bliver endnu bedre, når alle deltager aktivt i dialogen, og deler ud af egne erfaringer.
Note: SektorForum hedder LeverandørForum for leverandørmedlemmer.

Publikationer

SektorCERTs arbejde med threat intelligence er datadrevet. I stedet for at tale om, hvad vi tror, bygger vores rapporter og andre publikationer på data.
Data fra vores egne sensorer og monitorering på PC'ere og servere. Samt data indsamlet fra vores omfattende samarbejde med bl.a. andre CERT'er i verden.

Publikationerne er vores måde at omdanne store datamængder og information fra mange kilder, til den viden I skal bruge for at beskytte den kritiske infrastruktur.

Tekniske rapporter

Fra vores sensornetværk ved vi bl.a. hvilke sårbarheder, der til enhver tid forsøges udnyttet mest mod vores medlemmer.

SektorCERTs tekniske rapporter kan I bruge til at identificere tiltag, der kan forbedre jeres forsvar.

Hændelsesbeskrivelser

Ved at gennemgå succesfulde angreb mod andre aktører i dansk, kritisk infrastruktur, kan der udtrækkes læringspunkter.

Formålet er, at give jer mulighed for at forhindre at en konkret hændelse gentager sig hos jer.

Løbende opdateringer

På SektorForum - vores online delingsplatform - deler vi løbende mindre publikationer om igangværende angreb, angrebsaktørers ændrede angrebsteknikker og meget andet.

SektorCERTs 25 anbefalinger

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.

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 et godt forsvar mod kendte angrebsteknikker.

Sparring

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.

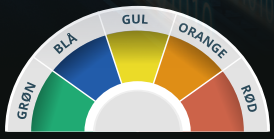
Forbered

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

Trusselsvurdering

SektorCERT holder kontinuerligt øje med cybertruslen mod dansk kritisk infrastruktur, og holder løbende sektorerne informerede om det aktuelle trusselsniveau. Derudover kommer SektorCERT med anbefalinger til tiltag.

Trusselsniveauet vises på en 5-trins skala, som er baseret på en international standard.



Sammenhænge

En dokumenteret sammenhæng mellem motivation, aktører, teknikker og trusler, kan bruges til at skabe overblik over det samlede trusselsbillede.

Konkrete anbefalinger

Trusselsvurderingen giver både baggrunden for vurderingen samt anbefalinger til hvilke konkrete tiltag, I bør have fokus på at validere effekten af.

Anbefalingerne er valgt ud fra den konkrete cybertrussel.

Aktører og angrebsteknikker

Trusselsvurderingen beskriver de aktører, som er relevante for den danske, kritiske infrastruktur samt de angrebsteknikker, de benytter.
Formålet er at hjælpe vores medlemmer til at fokusere deres forsvar mod det, som har størst sandsynlighed for at ramme dem.

Hvad er trusselsvurderingen baseret på?

Vi følger en række trusselsaktører tæt. Disse trusselsaktører er – eller er på vej til at blive - relevante for den danske, kritiske infrastruktur. Ved at følge trusselsaktørerne tæt får vi et indblik i de indledende angrebsteknikker, de benytter til at opnå adgang til infrastrukturen hos deres mål.

De teknikker, som de relevante aktører er meste tilbøjelige til at benytte, kortlægges for at gøre det nemmere for medlemmerne at prioritere, hvor den største beskyttelsesindsats bør lægges.

CERT'er

Som CERT (Computer Emergency Response Team) samarbejder SektorCERT med de andre landes CERT'er samt de andre CERT'er i Danmark.

Internationalt

Vi indgår i en række internationale fællesskaber omkring cybersikkerhed. Herfra får vi viden om angreb mod andre landes virksomheder.

Varsler

Vi modtager varsler fra leverandører, sikkerheds-virksomheder og mange andre. Det bidrager til vores samlede trusselsbillede.

Bemærk

Trusselsvurderingen fra SektorCERT er lavet med henblik på at klæde alle medlemmer, som driver den danske, kritiske infrastruktur, på til at kunne forberede sig på de angreb, de kan blive mødt af. Med baggrund i trusselsvurderingen, bør medlemmer kontrollere, at de og deres leverandører har de rigtige processer og kontroller implementeret, og at de er klar til både at opdage og reagere på de angreb, der kan være på vej.

Medlemskab

Der er fire måder at have et medlemskab hos SektorCERT:

Branchemedlem
Styrken i SektorCERT er størst, når vi står sammen.
Ved at indgå et branchemedlemskab, aftaler en hel branche at indgå i SektorCERT-fællesskabet.
Dette sker ved, at brancheforeningen indgår en aftale om medlemskab på vegne af deres medlemmer.
I dag er Green Power Denmark, Dansk Fjernvarme og DANVA alle branchemedlemmer i SektorCERT.

Individuelt medlem
Er det ikke muligt at indgå en aftale om medlemskab for en hel branche, kan individuelle selskaber få et individuelt medlemskab.
Medlemskabet har præcist samme fordele som et branchemedlemskab.

Brancheforeningsadministreret medlem
En brancheforening kan indgå aftale med SektorCERT om at indmelde en delmængde af de selskaber, der hører under brancheforeningen.
Denne form for medlemskab giver en rabat på kontingentet til medlemmerne i forhold til individuelle medlemskaber, og sikrer SektorCERT et minimumsantal medlemmer fra en ny sektor.

Leverandørmedlem
Hvis vores medlemmer vurderer, at en leverandør er kritisk for at drive den kritiske infrastruktur, kan du som leverandør blive medlem af SektorCERT.
Det kræver, at mindst to medlemmer vil være "Garant" for dig.

Hvordan bliver du medlem?

Kontingent

SektorCERT er 100% finansieret via kontingenter fra vores medlemmer og der indgår ingen offentlige midler i SektorCERT.
Dette er blandt andet for at sikre, at SektorCERT kan agere uden påvirkning af politiske agendaer, og at vores finansiering ikke afhænger af, hvilke agendaer der har fokus i dansk politik.

Derudover sikrer denne form for finansiering, at SektorCERT kan agere som privat, non-profit organisation, og at man dermed ikke kan søge aktindsigt hos os. Dette sikrer, at deling af hændelser og anden følsom information kan ske med sikkerhed for, at informationerne forbliver fortrolige.

Kontingentets størrelse afhænger af, hvilken af de 4 typer medlemskab man har, samt hvor stort et selskab man er.

Kontingentet justeres årligt med et prisindeks som besluttes af bestyrelsen.

SEKTOR CERT

Telefonnummer:

+45 88 32 71 40

E-mail:

info@sektorcert.dk

PGP nøgle:

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

Besøgs- og postadresse:

Sommerfuglevej 2A
6000 Kolding

Bredgade 45
1260 København K

CVR nummer:

41369841

Satellittelefon:

+88 16 22 45 60 29

SINE radio:

73 12 056