Governance, Risk & Compliance

Det stærke led mellem forretning og cybersikkerhed

orange™ Cyberdefense

Indholdsfortegnelse

We build a safer digital society

Cyberforsvar – fra risiko til robusthed

Digitalisering skaber enorme muligheder, men åbner også døren for nye risici. I takt med at kompleksiteten øges og vi bliver mere og mere afhængige af teknologi, vokser angrebsfladen. Det øger sårbarheden overfor cyberangreb.

Det handler ikke længere om at undgå cyberangreb, men om at være klar, når de rammer. Fordi IT er rygsøjlen i enhver organisation, er det altafgørende at tænke IT-sikkerhed ind overalt fra start og integrere det som en central del af forretningen. Derfor ligger det overordnede ansvar for at skabe en robust og holistisk forsvarsstrategi altid hos ledelsen.

Angrebsfladen har aldrig været større

Jo mere digitaliseret et samfund er, jo større en angrebsflade har de cyberkriminelle at boltre sig på. Derfor ser vi hvert år også stadig flere alvorlige eksempler på, hvordan DDoS-angreb og cyberafpresning gennem ransomware-angreb, samt forskellige typer af cyber-aktivisme, rammer virksomheder og organisationer med voldsom kraft. I dag har cyberkriminalitet nået et omfang, der gør det til en af verdens største økonomier. Og i takt med at de cyberkriminelle hele tiden bliver dygtigere til at anvende ny teknologi i deres angrebsmetoder, ændrer trussels- og risikobilledet sig. Derfor skal vi i højere grad forholde os til, hvornår vi bliver ramt – ikke hvis vi bliver ramt.

Tænk sikkerhed ind i alt fra start

For at bekæmpe det stigende antal cyberangreb har vi brug for nye stærke modtræk. Det kræver, at vi udvikler en mere holistisk tilgang til cybersikkerhed på. Nu skal vi tænke sikkerhed ind fra start i alt, hvad vi foretager os, for at vi kan opbygge et tilstrækkeligt robust cyberforsvar.

Tidligere blev cybersikkerhed udelukkende betragtet som et anliggende for IT-afdelingen - en støttefunktion med forstand på firewalls og perimetersikkerhed, som man i værste fald godt kunne drive forretningen uden. For de fleste virksomheder har det ændret sig radikalt. I dag spiller IT en central og afgørende rolle i enhver organisation: Ingen IT, ingen forretning.

Et robust forsvar kræver en strategi

I takt med IT's voksende betydning og udviklingen i trusselsbilledet er det blevet hele organisationens ansvar at implementere og indføre de tiltag og processer, der er nødvendige for at opretholde den beskyttelse, der skal til for at holde kerneforretningen kørende selv under store, velkoordinerede cyberangreb. Et robust cyberforsvar kræver dog mere end det. For uden en fælles forståelses-ramme, en overordnet strategi og kompetent styring, kommer man ikke i mål. Alt dette skal være forankret hos en ansvarlig ledelse, der sammen med medarbejderne, er i stand til at håndhæve strategien og eksekvere på den beredskabsplan, der er lagt.

Ledelsen har det overordnede ansvar

Det overordnede ansvar for virksomhedens cyber-sikkerhed ligger altid hos direktionen og bestyrelsen. Idéen om at man kan outsource dette ansvar, hører for-tiden til. Derfor er det, fra et Governance, Risk & Com-pliance perspektiv, afgørende, at topledelsen har en dyb forståelse for, hvor vigtigt et stærkt cyberforsvar er for forretningens overlevelse. Det sikrer, at ledelsen kan træffe velinformerede beslutninger, baseret på kvalificeret rådgivning fra interne eller eksterne eksperter i risikostyr-ing, inden det er for sent og skaden er sket.

Det er her Orange Cyberdefense' Governance, Risk & Compliance ekspertise kommer ind i billedet.

Før i tiden var cybersikkerhed mest en opgave, der blev klaret i IT-afdelingen, men i dag er det hele organisationens ansvar.

Det stiller større krav til kommunikationen, og GRC er sproget, der får teknologi, forretning og ledelse til at smelte sammen.

Katrine Krogedal | Team Lead GRC
Orange Cyberdefense

Hvorfor er Governance, Risk & Compliance relevant i forhold til cybersikkerhed?

Tilsammen gør de tre indsatsområder, Governance, Risk & Compliance, jer i stand til at nå jeres mål for cybersikkerhed og opbygge et robust cyberforsvar på en pålidelig og effektiv måde.

Governance fokuserer på de regler, processer og strukturer, der styrer jeres organisations beslutningsprocesser i forhold til cybersikkerhed. Det skal sikre, at de er transparente, involverer alle relevante interessenter og passer til jeres forretning.

Cybersecurity Risk Management hjælper med at afdække de risici, som kan forhindre jer i at nå jeres mål. På basis af en velovervejet risikoprofil kan I vurdere deres sandsynlighed og mulige konsekvenser og ud fra det vælge de bedste strategier for jeres cybersikkerhed.

Compliance sikrer, at jeres organisation til enhver tid overholder al gældende lovgivning og alle branchemæssige standarder, så I undgår juridiske problemer, bøder og mulige skader på jeres organisations renommé.

Implementering af en GRC-strategi bygger blandt andet på best practices fra standarder som COSO, ISO og NIST. Ved at kombinere dem med velvalgte sikkerhedsløsninger og en stærk sikkerhedskultur, kan I ruste jeres organisation til at modstå selv store cyberangreb.

Styrken ved GRC

GRC handler ikke blot om at vurdere risici, lægge strategier og træffe de bedste beslutninger. Det er også nøglen til at skabe en helhedsorienteret tilgang til IT-sikkerhed på tværs af hele organisationen, hvilket er uhyre vigtigt.

Kigger man på cybersikkerhed i et holistisk GRC-perspektiv, finder man ud af, at det handler om mere end blot at beskytte forretningskritiske data, netværk og systemer. Det handler også om at beskytte mennesker, vores relationer og vores tillid til hinanden samt det samfund, vi alle er en del af.

En stærk GRC-strategi ude i de enkelte organisationer og virksomheder skaber ikke alene et markant løft i evnen til at modstå cyberangreb og styre uden om de værste trusler mod forretningen, som kan have meget alvorlige konsekvenser. Det er også med til at gøre den verden, vi lever i, mere tryg og sikker.

Derfor er GRC et stærkt ledelsesværktøj

Hvor cybersikkerhed tidligere var en teknisk opgave for IT-afdelingen, er det, nu også blevet et vigtigt anliggende for alle direktioner og bestyrelser. Med et stærkt GRC-fokus får I et effektivt greb om dette nye ledelsesansvar.

En god GRC-strategi kan skabe det fundament, som danner rygraden i jeres cyberforsvar, og her spiller ledelse en afgørende rolle. Opmærksomheden omkring cybersikkerhed bør altid starte på direktionsgangen og i bestyrelseslokalet, fordi det er her, rammerne og retningslinjerne for en effektiv sikkerhedskultur dannes. Det udløser ofte et behov for forandring og en nødvendig kulturændring, som skal have tid til at forplante sig ned gennem hele organisationen, hvis virksomhedens modstandskraft over for cyberangreb skal styrkes.

Med GRC som rammeværktøj kan ledelsen sende et klart signal om, at cybersikkerhed har høj prioritet og ikke skal håndteres som en slags eftertanke, men som en forretningskritisk risikofaktor, der kræver fuld opmærksomhed fra alle afdelinger og medarbejdere.

I dag har langt de fleste virksomheder brug for en sikkerhedstrategi, som beskytter forretningen uden at hæmme drift, vækst og konkurrenceevne.

Det kræver, at organisationen opbygger en fælles forståelse af samspillet mellem risiko, teknik, lovgivning og økonomi – og det er netop dét, vores GRC-rådgivning fokuserer på.

Kristine Reme | Security Manager
Orange Cyberdefense

Fem råd om implementering af GRC

Det første spørgsmål til vores GRC-specialister er ofte: "Hvordan kommer vi i gang?" Her er nogle af deres svar:

1 Definér klare governance-politikker
Etablér tydelige governance-politikker, der klart beskriver roller, ansvar og beslutningsprocesser relateret til cybersikkerhed og sørg for, at retningslinjerne er flugter med organisationens strategiske mål. Involvér alle relevante interessenter – herunder ledelsen, IT-teams og juridiske specialister.

2 Udfør en risikovurdering
Start med at identificere jeres organisations unikke cybersikkerhedsrisici. Forstå de trusler, I står over for, sårbarhederne i jeres systemer og hvordan brud på sikkerheden kan påvirke jer, så I ved, hvad I kan tåle at miste, og hvad I ikke må miste kontrollen over.

3 Fokusér på compliance
Vurdér løbende om I overholder alle relevante love, regulativer og industristandarder. Udfør regelmæssige audits. Hold jer opdateret om lovgivningsmæssige ændringer, der kan påvirke organisationen.

4 Skab en sund sikkerhedskultur
Gør bevidsthed og ansvarlighed omkring cybersikkerhed til en af organisationens centrale fællesværdier. Beløn f.eks. god sikkerhedsadfærd. Træn medarbejderne i at genkende og reagere på trusler og tilskøn løbende alle til at rapportere brud på sikkerheden uden frygt for negative konsekvenser.

5 Indfør en cirkulær arbejdsmodel
Cybersikkerhed er et område, som hele tiden bør være en top-of-mind prioritet i alle jeres beslutninger og i alt, hvad i foretager jer, som har direkte eller indirekte indflydelse på organisationen og kerneforretningen. Vurder derfor regelmæssigt effektiviteten af jeres tiltag og investeringer i cybersikkerhed ud fra jeres GRC-principper og foretag justeringer efter behov.

Jo mere komplekse jeres IT-systemer bliver, jo vigtigere er vurderingen af de medfølgende risici.

Her kan professionel rådgivning og sparring fra et stærkt GRC-team, hjælpe med at skabe tætte forbindelser mellem jeres sikkerheds- og forretningsbehov på en måde, som gør en værdifuld forskel.

Mats Lindblad | GRC Manager
Orange Cyberdefense Sverige

Strategisk, taktisk og operationel GRC

I en verden, hvor cybertrusler udvikler sig med en hidtil uset hastighed, er det at arbejde målrettet med Governance, Risk og Compliance, i relation til cybersikkerhed, nødvendigt i enhver organisation, der ønsker at beskytte sin infrastruktur og overholde lovkravene på sikkerhedsområdet gennem en styrkelse af cyberforsvaret.For at få det fulde udbytte af indsatsen på GRC-området, bør arbejdet foregå holistisk på tre niveauer: det strategiske, det taktiske og det operationelle. Hvert niveau spiller en afgørende rolle i forhold til at reagere på trusler, den proaktive beskyttelse af forretningns kritiske aktiver og overholdelse af gældende lovkrav.

Det strategiske niveau:

På det strategiske niveau handler GRC om at definere den overordnede retning og mål for organisationens cybersikkerhed. Her fastlægges governance-strukturer, politikker og rammeværker, som styrer, hvordan risici identificeres, vurderes og håndteres på tværs af hele virksomheden. Dette niveau sikrer, at cybersikkerhed er integreret i virksomhedens overordnede strategi og understøtter forretningsmålene. Det giver ledelsen en klar forståelse af, hvordan cybersikkerhedsinitiativer både medvirker til at beskytte virksomhedens aktiver og omdømme

Strategisk GRC giver ledelsen mulighed for at træffe oplyste beslutninger baseret på risikovurderinger og compliance-behov. Det skaber et stærkt fundament for at modstå cybertrusler og sikrer, at ressourcer allokeres effektivt i forhold til de mest kritiske risici.

Det operationelle niveau:

Det operationelle niveau er, der hvor de daglige aktiviteter finder sted. Det inkluderer overvågning af sikkerhedssystemer, håndtering af sikkerhedshændelser og opretholdelse af compliance på tværs af organisationen. Operationel GRC sikrer, at de taktiske planer bliver udført effektivt, og at organisationen kan reagere hurtigt og på sikkerhedshændelser.

Operationel GRC giver realtidsbeskyttelse af virksomhedens aktiver. Den sikrer, at cybersikkerhedskontrollerne fungerer som de skal, og at der kan reageres hurtigt på nye trusler. Det operationelle niveau er således afgørende for at opretholde den daglige drift - uden afbrydelser.

Det taktiske niveau:

På det taktiske niveau bliver de strategiske mål omsat til konkrete handlingsplaner og procedurer. Dette niveau fokuserer på implementering af kontrolforanstaltninger, risikostyring og compliance-aktiviteter, der understøtter den overordnede strategi. Taktisk GRC involverer også udarbejdelse af standarder og retningslinjer, der skal følges af alle afdelinger og medarbejdere i organisationen for at sikre, at cybersikkerhedsforanstaltningerne er konsekvente og effektive.

Taktisk GRC sikrer, at strategiske beslutninger kan eksekveres i den operationelle virkelighed. Ved at implementere skræddersyede kontroller og procedurer som matcher virksomhedens specifikke behov, kan man minimere de forskellige risici.

Derfor er alle niveauer vigtige

En effektiv GRC-struktur kræver, at alle tre niveauer fungerer harmonisk. Uden en strategisk retning kan de taktiske og operationelle aktiviteter blive ukoordinerede og ineffektive. Omvendt vil en stærk strategi uden effektiv eksekvering og operationel implementering efterlade virksomheden sårbar overfor trusler og compliance-brud. Derfor er det afgørende, at I investerer i alle tre GRC-niveauer for at skabe et robust forsvarsværn mod cybertrusler.

Orange Cyberdefenses unikke tilgang

Orange Cyberdefenses GRC rådgivning bygger på en teknisk ekspertise kombineret med dyb forståelse for forretningsstrategier og compliancebehov. Vi leverer ikke alene stærk rådgivning, men kan også hjælpe med at implementere og overvåge de anbefalede løsninger. Det, der adskiller os fra andre er, at vi, udover at levere rapporter med vurderinger og anbefalinger, går skridtet videre og hjælper jer helt i mål.

Vores tilgang til GRC inkluderer:

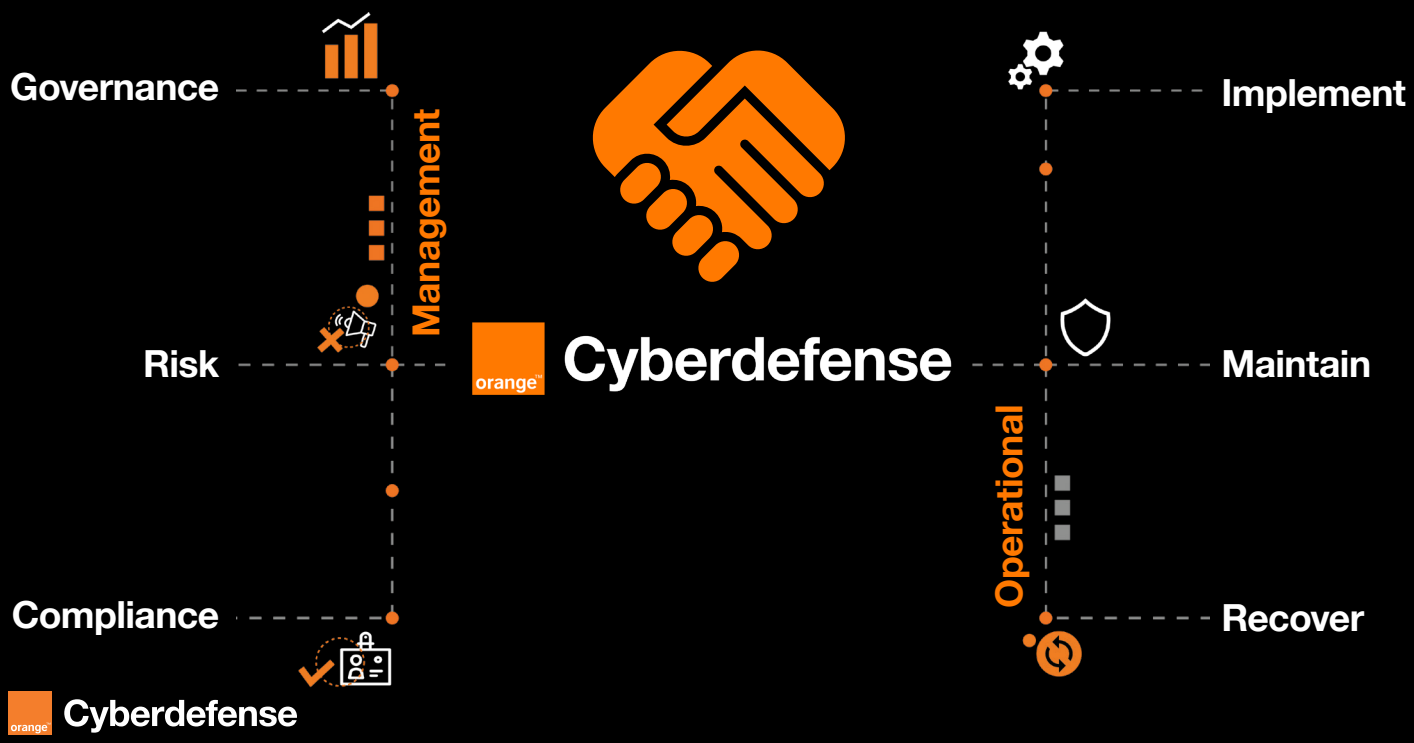
- **Indgående teknisk ekspertise:** Vi forstår jeres komplekse teknologiske udfordringer og leverer løsninger, der integrerer problemfrit med eksisterende systemer.
- **Praktisk implementering:** Vi hjælper jer ikke kun med at udvikle strategier, men tilbyder også taktisk og operationel støtte til at føre dem ud i livet.
- **Kontinuerlig overvågning og forbedring:** Vi tilbyder ikke kun "engangsløsninger", men sikre at jeres overordnede cybersikkerhedsstrategi tilpasses og optimeres løbende i takt med, at trusselsbilledet udvikler sig.

Ved at vælge Orange Cyberdefense som GRC-partner, får I ikke blot rådgivning i, hvordan I skaber en stærk Governance, Risk, og Compliance-strategi, og hvad det betyder for robustheden i jeres cyberforsvar.

Vi hjælper også med at implementere effektiv GRC i hele organisationen gennem en praktisk, hands-on tilgang, der sikrer, at jeres cybersikkerhed konstant er på forkant med de nyeste trusler, teknologier og reguleringer.

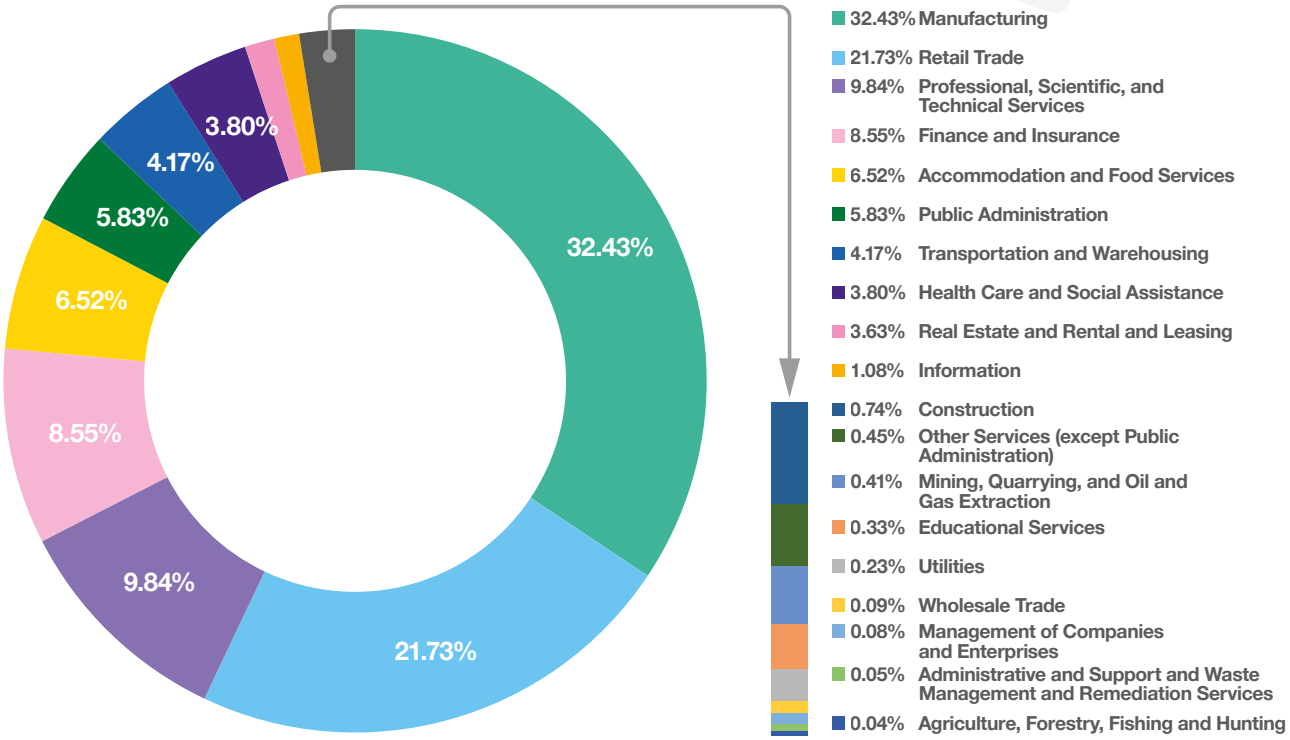
Orange Cyberdefense råder over et internationalt team af efterforskere og analytiske eksperter, som hele tiden overvåger det globale trussellandskab og identificerer nuværende og kommende trusler 24/7. Derfor er vi i stand til at give jer helt konkrete anbefalinger til, hvordan I bedst tilpasser jeres sikkerhedsstrategi, så I ikke kun er beskyttet mod eksisterende trusler, men også er forberedt på fremtidige udfordringer. Derudover sørger vi for, at jeres systemer altid er opdaterede med de nyeste sikkerhedspatches, at jeres compliancestruktur lever op til de nyeste lovgivningsmæssige krav, og at jeres risikostyring er proaktiv snarere end reaktiv.

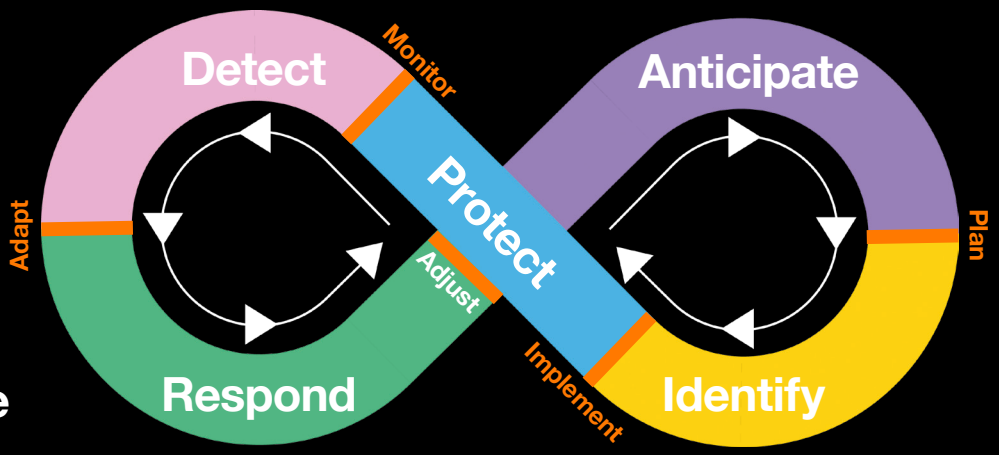
Ved at være på forkant med både teknologi og trusler, kan I minimere risici, optimere sikkerhedsressourcerne og sikre kontinuiteten i jeres forretningsdrift, selv i et dynamisk og komplekst cybersikkerhedsmiljø.



Hvordan ser det aktuelle trusselslandskab ud?

Hvilke brancher rammes oftest af cyberangreb?





Orange Cyberdefense hjælper jer hele vejen i mål

Det aktuelle trusselsbillede er komplekst og antallet af cyberangreb er stigende. Som en anerkendt sikkerhedsrådgiver og førende Managed Security Service Provider, kan Orange Cyberdefense både rådgive jer om, hvordan I sikrer jeres forretning, håndterer sårbarheder og opbygger den nødvendige modstandskraft mod de farer, der truer jeres forretning.

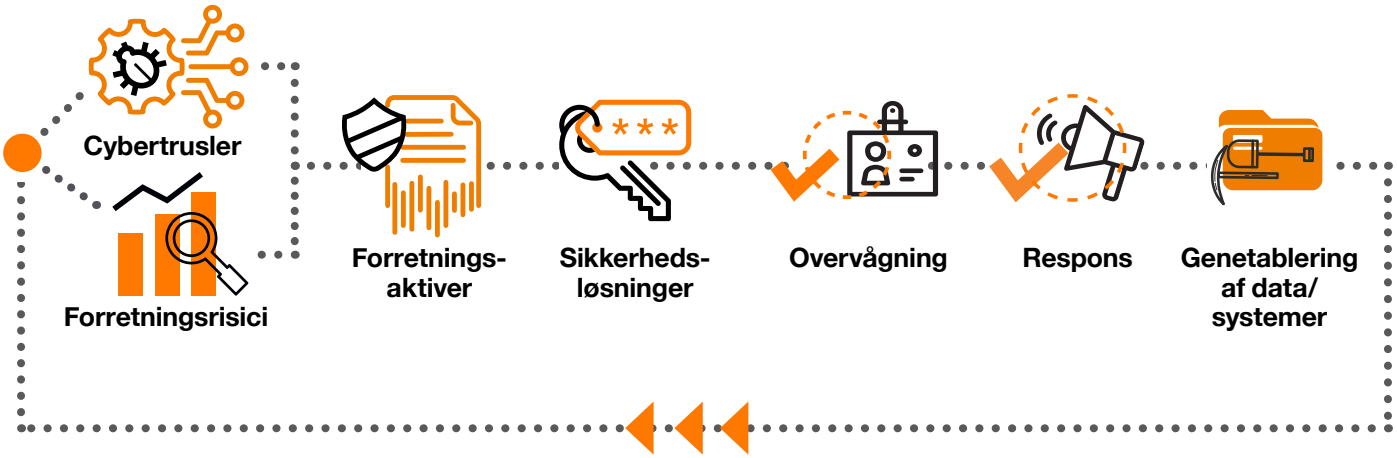
Som GRC-partner, har vi ikke kun et strategisk management fokus. Den operationelle del af GRC, er lige så vigtig for os. Vi har en dyb IT-teknisk viden og indsigt, som gør os i stand til at hjælpe med implementeringen og driften af jeres operationelle sikkerhed. Vi kommer med anbefalinger og leverer rapporter, der omfatter alle facetter af jeres cybersikkerhed. Vi hjælper jer hele vejen fra udviklingen af en stærk GRC-strategi med fokus på optimering af jeres cyberforsvar og assisterer med at finde de rigtige sikkerhedsløsninger, der passer nøjagtigt til jeres behov, risikoprofil og ressourcer.

orange Cyberdefense

Sådan ser en typisk GRC-proces ud

Ingen organisationer er helt ens, og derfor vil en GRC-proces variere. Men det er ofte forskellige udgaver af denne grundmodel.

Mange topledelser føler sig udfordret af, at de i stigende grad skal tage direkte ansvar for hele organisationens cybersikkerhed – det gælder især for direktioner og bestyrelser i de virksomheder, der beskæftiger sig med samfundskritiske områder. Men set fra et ledelsesperspektiv gælder det samme princip for alle organisationer: Fundamentet for et stærkt cyberforsvar handler om at skabe maksimal synergi mellem de overordnede forretningsstrategiske beslutninger og retningslinjer, de daglige arbejdsprocesser og den operationelle sikkerhed.



Skarpt fokus på jeres risici

Tidligt i GRC-arbejdet hjælper Orange Cyberdefense's GRC-team med at stille skarpt på jeres risici og udpege, hvilke forretningsdata, applikationer og infrastrukturer, I bør beskytte bedst. Målet er at identificere, hvad der er mest kritisk for jeres organisation, så jeres forretning kan køre videre, uanset hvad I bliver udsat for. Det er altid jeres risikoprofil, der bestemmer, hvordan jeres konkrete cyberforsvar skal designes og bygges op. Over tid bør vurderingen gentages og justeres, når nye behov opstår, for verden står ikke stille. Udviklingen fører altid forandringer med sig, som gør det nødvendigt at kalibrere jeres cybersikkerhedsløsninger -og initiativer løbende. Det er en cirkulær proces.

Når vi starter analysearbejdet, viser det sig tit, at de vigtigste forretningssystemer faktisk er nogle helt andre end vores kunde forventede. Det har naturligvis stor betydning for, hvordan hele arkitekturen omkring cyberforsvaret skal bygges op.

Bo Drejer | GRC Manager
Orange Cyberdefense

GRC-services til alle jeres behov

Governance Services

Governance er det strategiske kompas for jeres cybersikkerhed. Med disse services kan I opstille klare mål, politikker og strategier. F.eks. for beskyttelse af sensitive forretningsdata, kryptering og adgangskontrol som nøje afspejler jeres risikoprofil.

Sikkerhedsstrategi

Vi hjælper med at vurderere jeres organisations risici og sikkerhedsmæssige modenhed, hvorefter vi i tæt samarbejde med jeres CISO og forretningsansvarlige nøglepersoner udarbejder en operationel sikkerhedsstrategi.

CISO-as-a-Service

Vi stiller en fleksibel forretningsdrevet og operationel CISO-as-a-Service til rådighed, som er dedikeret til at rådgive jer omkring virksomhedens risikoprofil i forhold til det aktuelle trusselsbillede, lede jeres strategiske og taktiske cybersikkerhedsprojekter, varetage det daglige ansvar for jeres security governance og informationssikkerhed (ISMS), hjælpe med at implementere den operationelle del af jeres risikostyring i hele organisationen og administrere jeres cybersikkehedstræningsprogrammer.

implemtering

Vi hjælper jer med at opbygge et styringssystem for informationssikkerhed (ISMS), hvor formålet er at sikre et systematisk samspil mellem processer, teknologi og medarbejdere, så håndteringen af jeres information bygger på effektiv risikovurdering og anerkendte standarder som ISO27001, NIST og NSM.

Awarenes-stræning

Ud fra forretningsdrevne risiko- og trusselsvurderinger hjælper vi jer med at tilrettelægge og afvikle medarbejdertræning i god sikkerhedsadfærd. Det kan både være over for alle medarbejdere og udvalgte højrisiko-grupper. Efter behov kan vi også assistere med valg og implementering af de bedste awareness- og træningsværktøjer.

Risk & Resilience Services

Risikostyring er jeres cybersikkerhedsvagt, som proaktivt identificerer, vurderer og minimerer risici. Det er også ved hjælp af disse services, I kan lægge planer for, hvordan I bedst håndterer sikkerhedshændelser af alle størrelser.

Risiko- og trusselsvurdering

Sammen med jeres ledelse gennemfører vi en omfattende risikovurdering, hvor vi identificerer jeres mest kritiske forretningsfunktioner og tilhørende aktiver. Resultaterne samles i et beslutningsværktøj, som både omfatter procesbeskrivelser, risikohåndtering og en risikomatrice, som giver ledelsen fuldt overblik over alle relevante risici og mulige løsningsmodeller.

Krisehåndtering

Efter vi har foretaget en risiko- og trusselvurdering, hjælper vi jer med at lave en beredskabsplan og organisere en effektiv krisehåndtering med klare beskrivelser af hvem der bør deltage, hvad deres roller bør være og hvilke opgaver de har i en krisesituation. De udvalgte medarbejdere trænes med jævne mellemrum gennem realistiske øvelsesscenarier.

Business Continuity Management

Gennem en analyse, hvor vi afdækker jeres forretningsbehov med tilhørende risikovurderinger, assisterer vi jer løbende med at udarbejde, teste og opdatere de beredskabsplaner, som sikrer, at forretningen kan køre videre, selvom I bliver udsat for cyberangreb.

Disaster Recovery planlægning & test

Her udvikler og tester vores specialister effektive genetableringsplaner for jeres mest kritiske digitale aktiver. Alle relevante medarbejdere coaches i metodik, rammeværk og operationel genetablering af jeres forretningskritiske systemer.

Sikkerhedsarkitektur

Her definerer vi en risikodrevet sikkerhedsarkitektur, som både omfatter applikationer, netværk og infrastruktur. Den afspejler på alle niveauer jeres kritiske forretningsrisici og udvikles i tæt samarbejde med interessenter fra jeres IT-organisation, så praksis og vedligeholdelse forankres solidt.

Compliance Services

Compliance er det fyrtårn, der guider jeres organisation sikkert frem gennem lovgivning, regulativer og standarder, ved hjælp af regelmæssige audits. Når ny lovgivning træder i kraft, kræver compliance en gennemgang af prcesser, opdatering af politikker og udførelse af audits for at sikre, at I overholde gældende regler.

Cyber Maturity Assessment

Ved hjælp af et stærkt rammeværktøj for Cyber Maturity Assessment (CMA) kortlægger vi modenheden af jeres cybersikkerhed på alle relevante områder og i relation til jeres forretning. Herunder udfører vi også dokumentanalyse og interview af nøglepersoner. Resultaterne præsenteres i en overskuelig rapport, hvor vi også beskriver anbefalede, konkrete tiltag, som gradvist vil forstærke jeres cybersikkerhed for så få ressourcer som muligt.

Regulatoriske compliancevurderinger

Med udgangspunkt i regulatoriske krav såsom NIS2, DORA, GDPR eller CRA, gennemfører vi en vurdering af jeres compliance. Vurderingen omfatter observationer og anbefalede konkrete tiltag, for at sikre compliance – både nu og i fremtiden.

Det siger vores kunder om os

Orange Cyberdefense assisterer os med risikovurderinger, ledelsesrådgivning samt operationel implementering af styrket sikkerhedsarkitektur og beskyttelse af vores løsninger – med udgangspunkt i statens minimumskrav, NIS2 og ISO 27001. Med deres assistance er vi i stand til at fokusere og styrke vores evne til at imødekomme den øgede cybertrussel på en ressourceeffektiv måde.

Klimadatastyrelsen

Klimadatastyrelsen arbejder for et klimarobust, grønt og sikkert Danmark gennem digitale løsninger, databaseret kortlægning og fremtidssikret infrastruktur. Klimadatastyrelsen sikrer, at de mest relevante data er let tilgængelige og kan kombineres på tværs - til gavn for det danske samfund. Styrelsen er en del af Klima-, Energi- og Forsyningsministeriet, som bl.a. står i spidsen for arbejdet med 70 pct. reduktion af drivhusgasser i Danmark i 2030.

Klimadatastyrelsen

MILLUM®

Orange Cyberdefense har været en værdifuld partner, som har hjulpet os med at navigere i det stadig mere komplekse sikkerhedslandskab. Gennem CISO-as-a-Service og andre engagementer har de rådgivet topledelsen om sikkerhedsrelaterede forretningsanliggender. Desuden har de hjulpet os med at oprette og implementere et ISMS, implementere en risikostyringsproces og udvikle beredskabsplaner for cybersikkerhed (ISO 22301). Gennem vores partnerskab har vi styrket vores indsats inden for informationssikkerhed.

Millum

Millum er den største indkøbsplatform for hotel-, restaurant- og cateringbranchen i Norden. Etableret i 2002 forbinder Millum købere og leverandører gennem en digital markedsplads, der faciliterer effektiv indkøbsproces for over 90 kunder og 2.500 leverandører. Ved at levere løsninger, der fremmer gennemsigtighed, bæredygtighed og operationel effektivitet, spiller Millum en central rolle i at forenkle indkøbsprocessen. Med daglige brugere i Norge, Sverige og Danmark, understøtter Millum virksomheder i deres stræben efter bæredygtige praksisser gennem innovativ teknologi.

Det siger vores kunder om os

Det arbejde, vi har gennemført sammen med GRC-teamet hos Orange Cyberdefense med CMA'en, har været af stor værdi for os hos Biometria. Dels ud fra den dialog, vi har haft under gennemførelsen, hvor vi internt har kalibreret os ud fra de forskellige fokusområder, der er i CMA'en. Men vi har også ud fra det endelige resultat, der blev udarbejdet, fået en aktuel status og en beskrivelse af vores cybersikkerhedshygiejne. Vi vil rette en stor tak til GRC-teamet, som har ført os ikkert i mål!

Biometria

Biometria er en medlemsejet og central aktør i den svenske skovindustri, som måler det træ, der flyder mellem skov og industri. Det er en upartisk organisation, som sørger for, at Sveriges skovejere er sikre i deres træhandel. Biometria's mission er at støtte og udvikle træhandel, logistik og produktion på træmarkedet.

BIOMETRIA

Destination Gotland

Vi fik et klart billede af vores styrker og svagheder inden for cybersikkerhed, både på teknisk og organisatorisk niveau, hvilket hjælper os med at prioritere de rigtige tiltag og planlægge ressourcer. Det har givet os værdifuld indsigt og en konkret plan for at styrke vores sikkerhedsrutiner og reducere risici fra eksterne trusler, efter vi har lavet prioriteringen. Næste skridt er at forbedre hele koncernens sikkerhedsbevidsthed ved at fortsætte med at uddanne og tale om cyberhygiejne. Det kræver små skridt og disciplineret forandringsledelse, fordi det nu i lige så høj grad handler om kulturændringer som teknisk sikkerhed i organisationen.

Destination Gotland

Destination Gotland driver et af Europas mest moderne maritime transportsystemer. Flåden består af tre højhastighedsfartøjer, hvoraf to sejler på flydende naturgas (LNG) og biogas (LBG). I 2023 transporterede Destination Gotland har omkring 1,7 millioner passagerer, 540.000 biler og 760.000 enheder. I sommersæsonen har Destination Gotland op til 18 afgange om dagen.

> I Orange Cyberdefense efterlader vi ikke bare en sikkerhedsrapport. Vi analyserer jeres forretning og udvikler løsninger, der nøje matcher jeres risikoprofil og ressourcer – og vi står ved siden af jer hele vejen og sikrer, at I når godt i mål.
>
> **Bo Drejer**
> **GRC Manager**
> **Orange Cyberdefense Danmark**

Hvorfor vælge Orange Cyberdefense som GRC-partner?

I en verden, hvor IT spiller en afgørende rolle for kerneforretningen, er der behov for stærke cybersikkerhedspartnere, som ikke bare leverer rapporter og derefter trækker sig tilbage og overlader det fulde ansvar for at føre rapporternes konklusioner ud i livet til de enkelte organisationer og virksomheder.

Cybersikkerhed er en kompleks størrelse, som kræver en del teknisk indsigt og specifikke kompetencer. Det er knappe ressourcer, som der er stor efterspørgsel på. Kravene til cybersikkerhed øges konstant og i mange organisationer kan ressourcerne ikke følge med i samme tempo. Derfor oplever flere og flere virksomheder, at de har rigtig svært ved at omsætte komplicerede analyser og anbefalinger til konkret sikkerhed, som dækker deres voksende behov for et stærkt cyberforsvar.

De bedste rapporter er dem, der bliver eksekveret på, hvorimod dyre rapporter, der bare ligger og samler støv, ikke har nogen reel værdi. Det er kernen i den tilgang, vi har til GRC-rådgivning.

Hos Orange Cyberdefense står vi ved vores rådgivning fra A-Z, og vi er klar til at føre den ud i livet. Det betyder, at vi hjælper jer hele vejen i mål lige fra første risiko- og modenhedsanalyse til effektiv implementering og drift af de arkitekturer og sikkerhedssystemer, der passer bedst til jeres sikkerhedsbehov.

Vores GRC-service bygger på professionel viden og dyb teknisk indsigt i markedets bedste og mest konkurrencedygtige sikkerhedsprodukter, metoder og services. Vores dygtige GRC-konsulenter samarbejder – både på tværs af Norden og globalt. Samtidig har vores GRC-team en erfaring, som gør dem i stand til at forstå jeres forretning, afkode jeres unikke udfordringer og behov. Derfor er de i stand til at hjælpe jer med at skabe det cyberforsvar, som giver jer den absolut bedste sikkerhed for jeres investeringer.

Vælg Orange Cyberdefense fordi:

- I vil have en sikkerhedspartner, der kan forene jeres forretnings- og sikkerhedsstrategi.
- Vi kan tale både ledelsens og IT-afdelingens sprog.
- Vi står ved vores rådgivning – fra første analyse til implementering og drift af jeres operationelle løsninger.
- Vi sørger for, at jeres forretning kan køre videre under ethvert cyberangreb.

Mød nogle af vores erfarne GRC-specialister

I Orange Cyberdefense arbejder vi med GRC-projekter af alle størrelser på tværs af de nordiske lande. Vores specialister kan både levere totalrådgivning fra indledende analyse til drift af implementerede sikkerhedsløsninger eller indgå i dele af jeres GRC-forløb efter behov.

Kristine Reme | Security Manager

Orange Cyberdefense Norge

Kristine Reme er en erfaren sikkerhedskonsulent inden for GRC-området. Hun har solid erfaring med compliance i relation til forskellige rammeværk og reguleringer inden for informationssikkerhed samt etablering, implementering og drift af informationssikkerhedsstyringssystemer (ISMS). Dette omfatter blandt andet udarbejdelse af governance dokumenter, risikostyring, leverandørstyring, revisioner og meget mere. Hos Orange Cyberdefense har Kristine ydet væsentlige bidrag til en række GRC-projekter. Hun besidder stor indsigt og forståelse for vores kunders behov i arbejdet med at sikre, at sikkerhedsstrategien er i tråd med forretningsmålene.

Bo Drejer | GRC Manager

Orange Cyberdefense Danmark

Bo Drejer har mere end 20 års erfaring med operationel GRC i organisationer af alle størrelser. Han er vant til at kommunikere og facilitere samarbejdsprocesser på både ledelsesmæssigt og teknisk niveau. Bo's erfaringer spænder over flere sektorer såsom transport, tele, public service, detailhandel og finans. Han både været selvstændig konsulent og ansat hos blandt andre PwC, Microsoft, Oracle, IBM og nu i Orange Cyberdefense.

Katrine Krogedal | Team Lead GRC

Orange Cyberdefense Norge

Katrine Krogedal er senior sikkerhedsrådgiver inden for GRC. Hun har flere års erfaring med etablering af styresystemer for informationssikkerhed (ISMS). Herunder opbygning af rammeværktøj, struktur, risikostyring, leverandørstyring og effektiv håndtering af sikkerhedshændelser. Hun har også hjulpet en række virksomheder med at gennemføre ISO 27001-certificeringer. Desuden har Katrine stor erfaring med at udarbejde strategiske handleplaner for øget cybersikkerhed.

Mats Lindblad | GRC Manager

Orange Cyberdefense Sverige

Mats Lindblad har mere end 25 års erfaring med at arbejde med sikkerhed i forskellige former. Han har arbejdet med ledelse og styring på strategisk, taktisk og operationelt niveau både inden for den offentlige sektor og private virksomheder bl.a. som CISO og CSO. Han har også fungeret som strategisk ledelsesrådgiver i forskellige sektorer som banker, forsikringsselskaber, detailhandel og myndigheder. Han er specialiseret i spørgsmål vedrørende resiliens og hjælper kunder med at opbygge og opretholde deres evne til at håndtere de forskellige typer af hændelser, der kan opstå.

Cyberdefense - hvem er vi?

Global forankring

Orange Cyberdefense er en førende europæisk cybersikkerhedsleverandører og Managed Security Services Provider med over 25 års erfaring. Vi er specialister i at levere rådgivning, løsninger og services og er anerkendt som en ledende MSS-leverandør af både Gartner, Forrester og IDC.

Vi har en global Threat Intelligence afdeling og 250 analytikere fordelt på **17 SOCs, 15 CyberSOCs, 11 CERTs** og **4 scrubbing centers** som indsamler og analyserer globale data fra over **500 informationskilder 24/7.**

Lokal tilstedeværelse

I Norden består vores team af omkring **500 medarbejdere** fordelt på Danmark, Norge og Sverige. I Danmark har vi ca. 60 medarbejdere, som arbejder fra vores kontorer i København og Aarhus.

Vores kunder inkluderer primært multinationale virksomheder, offentlige organisationer og statslige myndigheder.

Vores vækstrejse

Vi har over **3.100 medarbejdere** globalt og 50.000 kunder i hele verden, hvoraf 6.000 er store internationale virksomheder.

Vi har igennem en årrække haft en stabil økonomisk vækst og fremgang. I 2024 var vores globale omsætning på **€1,2 milliarder.**

En del af Orange Group

Orange Cyberdefense er en del af den globale franske telekoncern **Orange Group**, som har 137.000 medarbejdere og **296 millioner kunder** i hele verden.

I 2024 havde Orange Group en global omsætning på **€40,3 milliarder.**

Læs mere på:
orangecyberdefense.com/dk

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