Governance, Risk & Compliance

Säkerhet i varje beslut - för en tryggare digital framtid

orange™ Cyberdefense

Innehåll

We build a safer digital society

Cyberförsvar – från risk till robusthet

Digitaliseringen skapar enorma möjligheter, men den öppnar också dörren för nya risker. I takt med att komplexiteten ökar och vi blir mer och mer beroende av teknik, ökar också attackytan.

Det handlar inte längre om att undvika cyberattacker, utan om att vara redo när de inträffar. Eftersom IT är ryggraden i alla organisationer är det viktigt att tänka på IT-säkerheten redan från början och integrera den som en viktig del av verksamheten. Det övergripande ansvaret för att skapa en robust och holistisk försvarsstrategi ligger alltid hos ledningen.

Attackytan har aldrig varit större

Ju mer digitaliserat ett samhälle blir, desto större blir attackyta som cyberbrottslingar har att kapitalisera på. Därför ser vi varje år fler och fler allvarliga exempel på hur DDoS-attacker och ransomware-attacker, liksom olika typer av cyberaktivism, drabbar företag och organisationer med förödande kraft.
Idag har cyberbrottsligheten redan nått en omfattning som gör den till en av världens största ekonomier.
Och i takt med att cyberbrottslingarna blir allt skickligare på att använda ny teknik i sina attackmetoder förändras hot- och riskbilden. Nu måste vi tänka mer på när vi kommer att drabbas - inte om vi kommer att drabbas.

Tänk säkerhet, gällande allt

För att bekämpa den ökande volymen av cyberattacker behöver vi nya kraftfulla motåtgärder. Det kräver att vi utvecklar ett mer holistiskt synsätt på hur vi traditionellt uppfattar cybersäkerhet. Idag måste säkerheten beaktas från början i allt vi gör för att bygga upp ett tillräckligt robust cyberförsvar. Detta är ett paradigmskifte jämfört med tidigare, då cybersäkerhet sågs som en fråga för IT-avdelningen. En supportfunktion som förstod sig på brandväggar och perimetersäkerhet och som man i värsta fall kunde driva sin verksamhet utan.
För de flesta organisationer har detta förändrats radikalt. I dag spelar IT en central och avgörande roll i alla organisationer. Den har blivit ryggraden i verksamheten: Ingen IT, ingen verksamhet.

Ett robust försvar kräver en strategi

I takt med att IT blir allt viktigare och hotbilden utvecklas har det blivit hela organisationens ansvar att upprätthålla det skydd som behövs för att hålla kärnverksamheten igång i vardagen. Ett robust cyberförsvar kräver dock mer än så. Utan en övergripande strategi och en kompetent styrning kommer man inte att nå dit. Allt detta måste vara förankrat i en ansvarsfull ledningsgrupp som kan genomdriva och verkställa strategin och planerna tillsammans med medarbetarna.

Ledningen har det övergripande ansvaret

Det övergripande ansvaret för din organisations cybersäkerhet ligger alltid hos den verkställande ledningen och styrelsen. Tanken att detta ansvar kan läggas ut externt hör till det förflutna. Ur ett Governance, Risk & Compliance-perspektiv är det därför avgörande att den högsta ledningen har en djup förståelse för hur viktigt ett starkt cyberförsvar är för företagets överlevnad. Detta säkerställer att ledningen - baserat på kvalificerade råd från både interna specialister och externa experter - kan fatta välgrundade, dokumenterade och välinformerade beslut om cybersäkerhet och riskhantering innan det är för sent och skadan är skedd.

Det är här Orange Cyberdefense's expertis inom Governance, Risk och Compliance kommer in i bilden.

Vårt arbete handlar om att skydda verksamhetens kronjuveler, det vill säga den mest verksamhetskritiska informationen. Men ofta måste vi hjälpa till att gräva fram dessa juveler först, eftersom ledningen själv inte vet vilken information som är mest verksamhetskritisk.

Det är viktigt att ha ett systematiskt arbete för informationssäkerhet på plats som både är tillräckligt stabilt för att verksamheten ska kunna följa det, men också tillräckligt agilt för att tillåta ständiga förändringar och förbättringar.

Sigrid Öberg | Team Lead GRC
Orange Cyberdefense

Varför är Governance, Risk & Compliance relevant i förhållande till cybersäkerhet?

GRC står för Governance, Risk & Compliance, och tillsammans gör dessa tre fokusområden att du kan uppnå dina cybersäkerhetsmål på ett tillförlitligt och effektivt sätt.

Governance fokuserar på de regler, processer och strukturer som styr din organisations beslutsprocesser för cybersäkerhet. Den ska säkerställa att de är transparenta, involverar alla relevanta intressenter och passar din verksamhet.

Risk Management hjälper dig att identifiera de risker som hindrar dig från att uppnå dina mål. Utifrån en genomtänkt riskprofil kan du bedöma sannolikheten för att de inträffar och möjliga konsekvenser samt välja de bästa strategierna för din cybersäkerhet.

Compliance säkerställer att din organisation hela tiden följer all tillämplig lagstiftning och alla branschstandarder, så att du kan undvika juridiska problem, böter och eventuell skada på organisationens rykte.

Implementeringen av en GRC-strategi bygger på best praxis från standarder som COSO, ISO och NIST. Genom att kombinera dem med väl valda säkerhetslösningar och en stark säkerhetskultur kan du utrusta din organisation för att för att stå emot även storskaliga cyberattacker.

Kraften i GRC

GRC handlar inte bara om att bedöma risker, lägga upp strategier och fatta de bästa besluten. Det är också nyckeln till att skapa en helhetssyn på IT-säkerhet i hela organisationen.

Att ta sig an cybersäkerhet genom ett holistiskt GRC-perspektiv gör att man greppar mer än bara affärskritiska data, nätverk och system. Det handlar också om att skydda människor, våra relationer och vårt förtroende för varandra och det samhälle som vi alla är en del av.

Med andra ord skapar en stark GRC-strategi i enskilda organisationer och företag inte bara en betydande ökning av förmågan att stå emot cyberattacker och undvika de värsta hoten. Det gör också den värld vi lever i säkrare och tryggare.

Ett kraftfullt ledningsverktyg

Cybersäkerhet var tidigare en teknisk uppgift för IT-avdelningen, men i dag har det blivit en viktig fråga för alla ledningsgrupper och styrelser.

En bra GRC-strategi kan skapa ryggraden i ditt cyberförsvar, och här spelar ledarskapet en avgörande roll. Medvetenheten om cybersäkerhet bör alltid börja - och vara ständigt närvarande - i ledningsgruppen och styrelserummet, eftersom det är här som ramarna och riktlinjerna för en effektiv säkerhetskultur sätts.

Detta är ofta kopplat till ett behov av förändring och ett nödvändigt kulturellt skifte som behöver genomsyra hela organisationen om företagets motståndskraft mot cyberattacker ska kunna stärkas.

Med GRC som ramverk kan ledningen sända en tydlig signal om att cybersäkerhet är en högprioriterad fråga som inte ska behandlas som en eftertanke, utan som en affärskritisk riskfaktor som kräver full uppmärksamhet från alla avdelningar och medarbetare.

Våra erfarenheter visar att styrkan ligger i samarbetet mellan informationssäkerhet och IT-säkerhet. Genom att hjälpa våra kunder att förstå deras unika förutsättningar kan vi tillsammans skapa en verksamhetsanpassad strategi som möter deras specifika behov.

Det handlar inte bara om att implementera tekniska lösningar, vilka såklart är kritiska, utan också om att etablera ett riskbaserat arbetssätt och en gemensam säkerhetsgrund som sträcker sig över hela organisationen.

Christian Kyller | GRC Consultant
Orange Cyberdefense

Fem tips för implementering av GRC

”Hur kommer vi igång?”
Detta är en av de frågor våra GRC-specialister ofta får.

1 Definiera tydliga riktlinjer för Governance

Upprätta styrningspolicyer som tydligt beskriver roller, ansvar och beslutsprocesser relaterade till cybersäkerhet. Se till att riktlinjerna är i linje med organisationens strategiska mål. Involvera alla relevanta intressenter - inklusive ledningen, IT-team och jurister.

2 Genomför en cybersäkerhetsrisk-bedömning

Börja med att identifiera din organisations unika cybersäkerhetsrisker. Förstå vilka hot ni står inför, vilka sårbarheter som finns i era system och hur intrång kan påverka er, så att ni vet vad ni har råd att förlora och vad ni inte har råd att förlora kontrollen över.

3 Fokusera på compliance

Utvärdera kontinuerligt hur ni följer alla relevanta lagar, förordningar och branschstandarder. Genomför regelbundna revisioner. Håll dig uppdaterad om regeländ-ringar som kan påverka din organisation.

4 Skapa en sund säkerhetskultur

Gör medvetenhet om cybersäkerhet och ansvarstagande till en av organisationens gemensamma kärnvärden. Till exempel genom att belöna bra säkerhetsbeteende.
Utbilda dina medarbetare i att känna igen och reagera effektivt på hot. Alla bör kontinuerligt uppmuntras att rapportera säkerhetsöver-trädelser utan rädsla för negativa reaktioner.

5 Inför en cirkulär arbetsmodell

Cybersäkerhet är ett område som alltid bör vara högsta prioritet i alla dina beslut och i allt du gör som har en direkt eller indirekt inver-kan på din organisation och kärnverksamhet. Utvärdera därför regelbundet effektiviteten i dina cybersäkerhetsinitiativ och investeringar mot dina GRC-principer och gör justeringar efter behov.

“

Ju mer komplexa era IT-system blir, desto viktigare är det att bedöma de risker som är förknippade med dem - och det är här som professionell rådgivning, erfarenhetsutbyte och hjälp från ett starkt GRC-team behövs.

Ett team som kan sätta in dina kritiska utmaningar och affärsbehov i ett IT-säkerhetssammanhang gör en värdefull skillnad.

Mats Lindblad | Business Area Manager - GRC & Advisory
Orange Cyberdefense

Strategisk, taktisk och operativ nivå

En effektiv GRC-hantering kräver ett angreppssätt på tre nivåer: strategisk, taktisk och operativ. Var och en av dessa nivåer spelar en avgörande roll för att säkerställa att du inte bara svarar på hot, utan också proaktivt skyddar affärskritiska tillgångar, uppfyller lagstadgade krav och stöder organisationens långsiktiga mål.

Den strategiska nivån:

På strategisk nivå handlar GRC om att definiera den övergripande inriktningen och målen för organisationens cybersäkerhet. Här fastställs styrningsstrukturer, policyer och ramverk som reglerar hur risker identifieras, bedöms och hanteras inom hela organisationen. Denna nivå säkerställer att cybersäkerheten är integrerad i organisationens övergripande strategi och stöder affärsmålen. Det ger ledningen en tydlig förståelse för hur cybersäkerhetsinitiativ bidrar till att skydda både företagets tillgångar och rykte.

Strategisk GRC gör det möjligt för ledningen att fatta välgrundade beslut baserat på riskbedömningar och efterlevnadsbehov. Det skapar en stark grund för att stå emot cyberhot och säkerställer att resurser fördelas effektivt till de mest kritiska riskerna.

Den taktiska nivån:

På den taktiska nivån omsätts de strategiska målen i konkreta handlingsplaner och rutiner. Denna nivå fokuserar på att implementera kontroller, riskhantering och efterlevnadsaktiviteter som stödjer den övergripande strategin. Taktisk GRC innebär också att skapa standarder och riktlinjer som ska följas av medarbetare och avdelningar inom organisationen för att säkerställa att cybersäkerhetsåtgärderna är konsekventa och effektiva.

Taktisk GRC säkerställer att strategiska beslut kan verkställas i den operativa verkligheten. Det bidrar till att minimera riskerna genom att implementera rätt kontroller och rutiner som är anpassade till verksamhetens specifika behov.

Den operativa nivån:

Den operativa nivån är den nivå där den dagliga verksamheten äger rum. Detta inkluderar övervakning av säkerhetssystem, hantering av säkerhetsincidenter och upprätthållande av efterlevnad. Operativ GRC säkerställer att taktiska planer genomförs på ett effektivt sätt och att organisationen kan reagera snabbt och effektivt på säkerhetsincidenter.

Operativ GRC ger skydd i realtid för företagets tillgångar och bidrar till att säkerställa att cybersäkerhetskontrollerna fungerar som de ska och att organisationen kan reagera snabbt på nya hot. Den operativa nivån är avgörande för att upprätthålla den dagliga verksamheten utan avbrott.

Därför är alla nivåer viktiga

En effektiv GRC-struktur kräver att alla tre nivåerna arbetar i harmoni. Utan en strategisk inriktning kan taktiska och operativa aktiviteter bli okoordinerade och ineffektiva. Omvänt kommer en stark strategi utan effektivt genomförande och operativ implementering att göra organisationen sårbar för hot och överträdelser av efterlevnaden. Därför är det viktigt att du investerar i alla tre nivåerna av GRC för att skapa ett robust försvar mot cyberhot.

Vi har en unik strategi

Där många konsultföretag fokuserar enbart på att leverera rapporter och rekommendationer går Orange Cyberdefense GRC-konsulter ett steg längre eftersom. Vi vill gärna stötta er i att implementera och övervaka lösningarna.

Vår strategi för GRC omfattar:

- **Djupgående teknisk expertis:** Vi förstår dina komplexa tekniska utmaningar och levererar lösningar som integreras sömlöst med din organisations befintliga system.
- **Praktiskt genomförande:** Vi hjälper dig inte bara att utveckla strategier, utan också att förverkliga dem genom taktiskt och operativt stöd.
- **Kontinuerlig övervakning och förbättring:** Vi erbjuder inte bara enstaka lösningar, utan ser till att din övergripande cybersäkerhetsstrategi kontinuerligt anpassas och optimeras i takt med att hotbilden utvecklas.

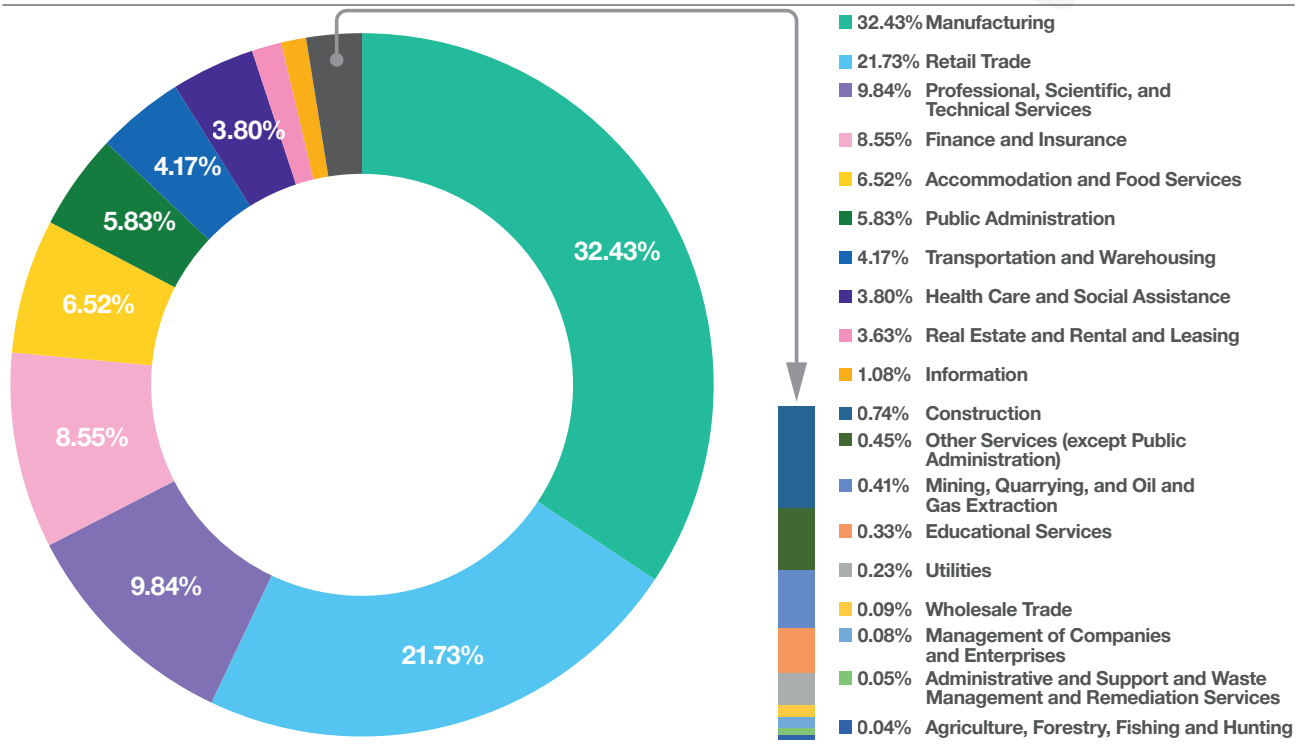
Genom att välja Orange Cyberdefense som din GRC-partner får du inte bara råd om hur du skapar en stark strategi för styrning, risk och efterlevnad. Vi hjälper dig också att implementera effektiv GRC i hela organisationen genom en praktisk, hands-on metod som säkerställer att din cybersäkerhet ligger steget före de senaste hoten, teknologierna och reglerna.

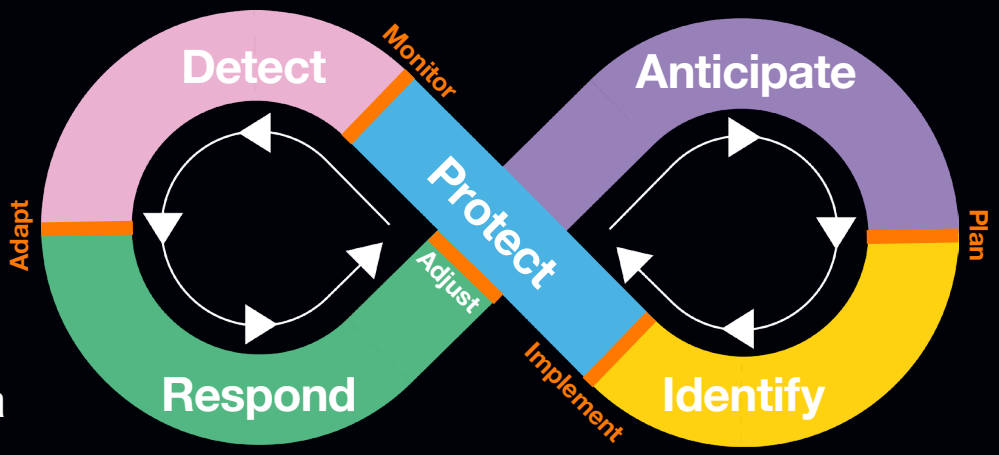
Vårt team av utredare och analytiska experter övervakar kontinuerligt det globala hotlandskapet och identifierar både aktuella och nya hot 24/7/365. Det innebär att vi ger dig konkreta rekommendationer om hur du bäst anpassar din säkerhetsstrategi så att du inte bara är skyddad mot befintliga hot, utan också är förberedd för framtida utmaningar.

Vi ser också till att dina system alltid är uppdaterade med de senaste säkerhetsuppdateringarna, att din compliance-struktur uppfyller de senaste lagstadgade kraven och att din riskhantering är proaktiv snarare än reaktiv. Genom att ligga steget före både teknik och hot kan du minimera riskerna, optimera säkerhetsresurserna och säkerställa kontinuitet i verksamheten, även i en dynamisk och komplex cybersäkerhetsmiljö.

Hur ser den aktuella hotbilden ut?

Vilka branscher drabbas oftast av cyberattacker?





Orange Cyberdefense hjälper dig hela vägen in i mål

Det nuvarande hotlandskapet är komplext och antalet cyberattacker ökar. Som en erkänd säkerhetsrådgivare och ledande Managed Security Service Provider kan Orange Cyberdefense ge dig råd om hur du säkrar ditt företag, hanterar sårbarheter och bygger den nödvändiga motståndskraften mot de faror som hotar ditt företag.

Som GRC-partner har vi inte bara ett strategiskt ledningsfokus - den operativa delen av GRC är lika viktig för oss.
Vi har djup IT-teknisk kunskap och insikt och hjälper till med implementering och drift av din operativa säkerhet. Vi ger rekommendationer och levererar rapporter som täcker alla aspekter av din cybersäkerhet. Från att utveckla en stark GRC-strategi med fokus på att optimera ert cyberförsvar hjälper vi er att hitta rätt säkerhetslösningar som passar just era behov, er riskprofil och era resurser.

Så ser en typisk GRC-process ut

Ingen organisation är den andra lik, och därför kommer GRC-processen att variera. Men det finns vanligtvis olika varianter av den här modellen.

Många ledande befattningshavare känner sig stressade av att de i allt högre grad måste ta ett direkt ansvar för hela organisationens cybersäkerhet - det gäller inte minst i ledningsgrupper och styrelser för bolag som arbetar med samhällskritiska områden. Men ur ett ledningsperspektiv gäller samma princip för alla organisationer: grunden för ett starkt cyberförsvar handlar om att skapa maximal synergi mellan övergripande strategiska affärsbeslut och riktlinjer, dagliga arbetsrutiner och processer samt operativ säkerhet.

Skarpt fokus på dina risker

Tidigt i GRC-processen hjälper Orange Cyberdefence GRC-team dig att fokusera på dina risker och identifiera vilka affärsdata, applikationer och infrastrukturer som du bäst bör skydda. Målet är att identifiera vad som är mest kritiskt för din organisation så att verksamheten kan fortsätta att fungera oavsett vad som händer. Det är alltid din riskprofil som avgör hur ditt specifika cyberförsvar ska utformas och byggas upp. Över tid bör bedömningen upprepas och justeras när nya behov uppstår, eftersom världen inte står stilla. Utvecklingen medför alltid förändringar, vilket gör det nödvändigt att kontinuerligt kalibrera dina cybersäkerhetslösningar och initiativ. Det är en cirkulär process.

Ansvaret för cybersäkerhet börjar i ledningen och verksamheten. Förståelsen föverksamhetsprocesser och roller i organisationen blir därför viktig för att säkerställa ansvaret och integrera cybersäkerhet som en naturlig och värdeskapande del. I den snabbt föränderliga världen med digitalisering behöver verksamheter snabbfotat kunna anpassa sig till förändringar.
En bra struktur behövs för att systematisk arbeta med verksamhetsutveckling där cybersäkerhet är en naturlig del i den utvecklingen.

Lisa Sjölund | GRC Team Lead
Orange Cyberdefense

GRC-tjänster för alla era behov

Governance-tjänster

Säkerhetsstrategi
Vi hjälper till att bedöma din organisations risker och säkerhetsmognad och arbetar sedan nära din CISO och andra ledare för att utveckla en operativ säkerhetsstrategi.

CISO-as-a-Service
Behöver ni en operativ CISO som tjänst, som ger dig råd om ditt företags riskprofil i förhållande till den aktuella hotbilden? Vi hjälper dig och leder dina strategiska och taktiska cybersäkerhetsprojekt, tar det dagliga ansvaret för din säkerhetsstyrning och informationssäkerhet (ISMS), hjälper till att implementera den operativa delen av din riskhantering i hela organisationen och hanterar dina utbildningsprogram för cybersäkerhet.

ISMS Implementation
Vi hjälper dig att bygga upp ett ledningssystem för informationssäkerhet (ISMS) för att säkerställa en systematisk samverkan mellan processer, teknik och människor. Hanteringen av din information baseras på en effektiv riskbedömning och erkända standarder som ISO27001, NIST och NSM.

Medvetenhet & utbildning
Baserat på affärsdrivna risk- och hotbedömningar hjälper vi dig att organisera och genomföra utbildning av medarbetare. Det kan gälla alla anställda och utvalda högriskgrupper. Vid behov kan vi också hjälpa till med att välja ut och implementera de bästa verktygen för medvetenhet och utbildning.

Risk & Reselins-tjänster

Risk- och hotbedömning
Tillsammans med din ledningsgrupp genomför vi en omfattande riskbedömning för att identifiera dina mest kritiska affärsfunktioner och tillhörande tillgångar. Resultatet sammanställs till ett beslutsunderlag som omfattar processbeskrivningar, riskhantering och en risk-matris som ger ledningen en fullständig överblick över alla relevanta risker och möjliga lösningar.

Krishantering
Efter risk- och hotbedömning hjälper vi er att organisera en effektiv krishantering. Detta inkluderar tydliga beskrivningar av vilka som ska involveras, vilka roller de ska ha och vilka uppgifter de har i en krissituation. De utvalda medarbetarna utbildas med jämna mellanrum genom realistiska övningsscenarier.

Hantering av verksamhetens kontinuitet
Genom omvärldsbevakning och tillhörande riskbedömningar hjälper vi dig att skapa, testa och kontinuerligt uppdatera beredskapsplaner för att säkerställa att din verksamhet kan fortsätta att fungera även om du utsätts för cyberattacker.

Planering och testning av katastrofåterställning
Här utvecklar och testar våra specialister effektiva återställningsplaner för dina mest kritiska digitala tillgångar. Alla berörda medarbetare utbildas i metodik, ramverk och operativ återställning av dina affärskritiska system.

Säkerhetsarkitektur
Här definierar vi en riskdriven säkerhetsarkitektur som omfattar applikationer, nätverk och infrastruktur. Den speglar dina kritiska affärsrisker på alla nivåer och utvecklas i nära samarbete med intressenter från din IT-organisation så att rutiner och underhåll är väl förankrade.

Compliance-tjänster

Cyber Maturity Assessment
Med hjälp av ett kraftfullt CMA-ramverk (Cyber Maturity Assessment) kartlägger vi mognadsgraden för er cybersäkerhet inom alla relevanta områden och i förhållande till er verksamhet. Detta inkluderar dokumentanalys och intervjuer med nyckelpersoner. Resultatet presenteras i en tydlig rapport där vi även beskriver rekommenderade, konkreta åtgärder som successivt ökar er cybersäkerhet med så lite resurser som möjligt.

Bedömningar av regelefterlevnad
Baserat på regulatoriska krav som NIS2, DORA, GDPR eller CRA genomför vi en bedömning av er efterlevnad. Rapporten omfattar observationer och rekommenderade konkreta åtgärder för att säkerställa efterlevnad - både nu och i framtiden.

Vad säger våra kunder?

Det arbete som vi genomfört tillsammans med GRC-teamet på Orange Cyberdefence med CMA:n har varit av stort värde för oss på Biometria. Dels utifrån den dialog vi haft vid genomförandet, där vi internt fått kalibrera oss utifrån de olika fokusområden som finns i CMA:n. Men vi har också utifrån slutresultat som togs fram fått ett nuläge och beskrivning av vår cybersäkerhetshygien. Vill rikta ett stort tack till teamet inom GRC som tryggt lotsat oss fram!

Om Biometria

Biometria är en medlemsägd och central aktör inom svensk skogsnäring. De mäter det virke som flödar mellan skog och industri och som opartisk säkerställer att Sveriges skogsägare är trygga i sina virkesaffärer. Deras uppdrag är att stödja och utveckla virkeshandel, logistik och produktion på virkesmarknaden.

BIOMETRIA

Destination Gotland

Vi fick en tydlig bild över våra styrkor och svagheter inom cybersäkerhet både på teknisk och organisatorisk nivå, vilket hjälper oss att prioritera rätt åtgärder och planera resurser. Den har gett oss en värdefull insikt och en konkret plan för att börja stärka våra säkerhetsrutiner och minska riskerna från externa hot efter att vi gjort prioriteringen. Nästa steg är att förbättra hela koncernens säkerhetsmedvetenhet genom att fortsätta utbilda och prata om cyberhygien. Det kräver små steg och disciplinerad förändringsledning då det mer är en kulturfråga i organisationen för att lyfta blicken från att det tidigare varit en IT-fråga enbart.

Om Destination Gotland

Destination Gotland AB driver ett av Europas mest moderna sjötransportsystem. Flottan består av tre höghastighetsfartyg, varav två drivs med flytande naturgas (LNG) och biogas (LBG). År 2023 transporterade bolaget cirka 1,7 miljoner passagerare, 540.000 bilar och 760.000 löpmeter gods. Under sommarsäsongen har vi upp till 18 avgångar per dag.

Vad säger våra kunder?

Orange Cyberdefense bistår oss med riskbedömningar, managementkonsultation och operativ implementering av stärkt säkerhetsarkitektur och skydd i våra lösningar - baserat på myndigheternas minimikrav, NIS2 och ISO 27001. Med deras hjälp kan vi fokusera och stärka vår förmåga att möta det ökade cyberhotet på ett resurseffektivt sätt.

Om Klimadatastyrelsen

Klimatdatastyrelsen arbetar för ett klimattåligt, grönt och säkert Danmark genom digitala lösningar, databaserad kartläggning och framtidssäkrad infrastruktur. Den danska klimatdatamyndigheten säkerställer att de mest relevanta uppgifterna är lättillgängliga och kan kombineras på tvärs - till förmån för det danska samhället. Myndigheten är en del av klimat-, energi- och försörjningsministeriet, som bland annat leder arbetet mot en 70-procentig minskning av växthusgaser i Danmark till 2030.

Klimadatastyrelsen

MILLUM®

Orange Cyberdefense har varit en värdefull partner som hjälpt oss att navigera i det alltmer komplexa säkerhetslandskapet. Genom CISO-as-a-Service och andra uppdrag har de gett råd till högsta ledningen i säkerhetsrelaterade affärsfrågor. Dessutom har de hjälpt oss att skapa och implementera ett ISMS, implementera en riskhanteringsprocess och utveckla beredskapsplaner för cybersäkerhet (ISO 22301). Genom vårt partnerskap har vi stärkt vårt arbete med informationssäkerhet.

Om Millum

Millum är den största upphandlingsplattformen för hotell-, restaurang- och cateringbranschen i Norden. Millum grundades 2002 och kopplar samman köpare och leverantörer genom en digital marknadsplats som underlättar effektiva upphandlingsprocesser för över 90 kunder och 2 500 leverantörer. Genom att tillhandahålla lösningar som främjar transparens, hållbarhet och operativ effektivitet spelar Millum en central roll i att förenkla upphandlings-processen. Med dagliga användare i Norge, Sverige och Danmark är Millum engagerat i att stödja företag i deras strävan efter hållbara metoder genom innovativ teknik.

> **På Orange Cyberdefense lämnar vi dig inte bara med en säkerhetsrapport. Vi analyserar din verksamhet och tar fram lösningar som matchar din riskprofil och dina resurser - och vi finns vid din sida hela vägen för att se till att du lyckas.**
>
> **Mats Lindblad | GRC Manager**
> **Orange Cyberdefense**

Därför ska du välja oss som din GRC-partner

I en värld där IT spelar en avgörande roll för kärnverksamheten behövs starka partners inom cybersäkerhet som inte bara levererar rapporter och sedan tar ett steg tillbaka.

Cybersäkerhet är komplext och kräver stor teknisk insikt och specifika kompetenser. Det är knappa resurser som det råder stor efterfrågan på. Kraven på säkerhet ökar ständigt och i många organisationer räcker inte resurserna till. Allt fler företag upplever att det är mycket svårt att omsätta komplicerade analyser och rekommendationer till konkret säkerhet som möter deras växande behov av ett starkt cyberförsvar.

De bästa rapporterna är de som man gör något åt, medan dyra rapporter som bara ligger i en byrålåda och samlar damm inte har något verkligt värde. Detta är kärnan i vår inställning till de råd vi ger genom vårt GRC-team.
På Orange Cyberdefense står vi bakom våra råd och vi är redo att omsätta dem i praktiken för våra kunder.
Det innebär att vi hjälper dig hela vägen - från inledande risk- och mognadsanalys till effektiv implementering och drift av de arkitekturer och säkerhetssystem som bäst passar dina säkerhetsbehov.

Vår GRC-tjänst bygger på professionell kunskap och djup teknisk insikt i de bästa och mest konkurrenskraftiga säkerhetsprodukterna, metoderna och tjänsterna på marknaden. Våra skickliga GRC-konsulter samarbetar - både i Norden och globalt. Samtidigt har vårt GRC-team erfarenheten att förstå din verksamhet, avkoda dina unika utmaningar och behov, så att de kan hjälpa dig att skapa det cyberförsvar som ger dig den absolut bästa säkerheten för dina investeringar.

Välj Orange Cyberdefense för att:

- Du vill ha en säkerhetspartner som kan förena din affärs- och säkerhetsstrategi.
- Vi talar både ledningens och IT:s språk.
- Vi står för vår rådgivning - från inledande analys till implementering och drift av dina operativa lösningar.
- Vi ser till att ditt företag kan fortsätta att fungera under en cyberattack.

Möt några av våra specialister

På Orange Cyberdefense arbetar vi med GRC-projekt av alla storlekar i hela Norden. Våra specialister kan ge fullständig rådgivning från initial analys till drift av implementerade säkerhetslösningar eller delta i delar av din GRC-process efter behov.

Mats Lindblad | Business Area Manager - GRC & Advisory

Orange Cyberdefense

Mats Lindblad har mer än 25 års erfarenhet av att arbeta med säkerhet i olika former. Han har arbetat med ledarskap och management på strategisk, taktisk och operativ nivå inom både offentlig sektor och privata företag, bland annat som CISO och CSO. Han har också arbetat som strategisk managementkonsult inom olika sektorer som bank, försäkring, detaljhandel och myndigheter.
Han är specialiserad på resiliensfrågor och hjälper kunder att bygga upp och upprätthålla sin förmåga att hantera olika typer av incidenter som kan inträffa.

Sigrid Öberg | GRC Team Lead

Orange Cyberdefense

Sigrid har mångårig erfarenhet i att arbeta med risk och efterlevnad av lagar och bästa praxis inom IT och informationssäkerhet. Som projektledare, förändringsledare och rådgivare leder hon resurser från flera delar av organisationen för att implementera och driva hållbara ramverk som både tar hänsyn till verksamhetens mål och omgivningens regulatoriska krav.

Christian Kyller | GRC Consultant

Orange Cyberdefense

Christian är en GRC-konsult och strategisk rådgivare. Hans roll innefattar ofta att identifiera och analysera kundernas risker och säkerhetsbehov samt översätta dem till genomförbara strategier och kontroller för att uppnå organisatoriska mål.

Lisa Sjölund | Team Lead GRC

Orange Cyberdefense

Lisa har flera års erfarenhet inom informationssäkerhet och hjälper företag att ta nästa steg i deras cybersäkerhetsresa med enkelhet som en nyckelparameter. Uppnå en god cybersäkerhet handlar om att säkerställa en symbios av processer, människor och teknik. Detta kräver tid och engagemang från hela organisationen, inte minst ledningen för att lyckas.

Cyberdefense - Vilka är vi?

Global förankring

Orange Cyberdefense är en ledande europeisk leverantör av cybersäkerhet och Managed Security Services med över 25 års erfarenhet. Vi är specialiserade på att tillhandahålla konsulttjänster, lösningar och tjänster och är erkända som en ledande MSS-leverantör av Gartner, Forrester och IDC.

Vi har en global Threat Intelligence-avdelning och 250 analytiker på **18 SOCs, 14 CyberSOCs och 4 CERTs,** som samlar in och analyserar globala data från över **500 informationskällor 24/7.**

Lokal närvaro

I Norden består vårt team av cirka **500 medarbetare** i Danmark, Norge och Sverige. I Sverige har vi cirka 400 medarbetare som arbetar från våra kontor i Stockholm, Göteborg, Malmö och Sundsvall. Våra kunder består främst av multinationella företag, offentliga organisationer och myndigheter.

Vår tillväxtresa

Vi har över **3.000 medarbetare** globalt och fler än 8.700 kunder i 160 länder.

Vi har haft flera år av stadig ekonomisk tillväxt. År 2023 uppgick våra globala intäkter till **€1,072 miljarder.**

En del av Orange Group

Orange Cyberdefense är en del av den globala franska telekommunikationskoncernen Orange Group, som har 137.000 anställda och över **296 millioner kunder** över hela världen.

År 2023 hade Orange Group en global omsättning på **€44 miljarder.**

Läs mer på:
orangecyberdefense.com/se

Kontakta oss:
info@se.orangecyberdefense.com
+46 10 202 20 13