Myndigheten för samhällsskydd och beredskap

Rapport

Undersökning om OT-säkerhet

Hinder och utmaningar i OT-säkerhetsarbetet för samhällsviktig verksamhet

Undersökning om OT-säkerhet: Hinder och utmaningar i OT-säkerhetsarbetet för samhällsviktig verksamhet

Publikationsnummer: MSB2544 – februari 2025
ISBN-nummer: 978-91-7927-598-3

Förord

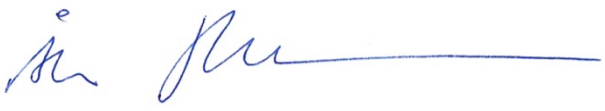
Med samhällsviktig verksamhet avses verksamhet, tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Stora delar av vad som utgör samhällsviktig verksamhet i dagens samhälle är beroende av OT-system. För att säkerställa samhällets funktionalitet i såväl vardag som kris eller krig är det nödvändigt att OT-system är skyddade på ett ändamålsenligt sätt.

Denna rapport är resultatet av en undersökning som MSB gjort i syfte att identifiera och dokumentera utmaningar och stödbehov avseende informations- och cybersäkerhet som berör OT-system och samhällsviktig verksamhet som är beroende av sådana system.

Undersökningen visar att det finns stora utmaningar rörande skyddet av och säkerheten i OT-system i samhällsviktig verksamhet. Några bidragande faktorer till detta är bland annat låg kunskap och medvetenhet om OT-säkerhet såväl inom den egna organisationen som hos externa kravställare, brister i organisationsledningens engagemang, bristande tillgång till kompetent personal samt avsaknad av OT-säkerhetsperspektivet i befintliga lagar, förordningar och föreskrifter inom cybersäkerhetsområdet.

Avsikten med denna rapport är tvåfaldigt: att synliggöra området OT-säkerhet, och att ta fram ett underlag som kan användas som utgångspunkt för diverse aktiviteter som syftar till att öka OT-säkerheten i samhället.

Solna, 2024-12-18



Åke Holmgren

Avdelningschef, Avdelningen för cybersäkerhet och säkra kommunikationer

Innehåll

Inledning

MSB har i uppdrag att samordna arbetet med samhällets informations- och cybersäkerhet. I detta ryms att MSB ska ge råd och stöd i det förebyggande arbetet inom området till berörda målgrupper.

Denna rapport är resultatet av en undersökning som MSB gjort i syfte att identifiera och dokumentera utmaningar och stödbehov avseende informations- och cybersäkerhet som berör OT-system och samhällsviktig verksamhet som är beroende av sådana system.

Vilka utmaningar och stödbehov som föreligger inom områden som informationssäkerhet och IT-säkerhet är både väldokumenterade och kända av många. Området OT-säkerhet har, i jämförelse med dessa områden, fallit i skymundan. Bakgrunden till och syftet med undersökningen är således tvåfaldigt: dels att synliggöra området OT-säkerhet, och dels att ta fram ett underlag som kan användas som utgångspunkt för diverse aktiviteter som syftar till att öka OT-säkerheten i samhället.

Undersökningen har genomförts av MSB med stöd av Attityd i Karlstad AB.

OT och cyberfysiska system – vad är det?

Cyberfysiska system är system där digitala och fysiska komponenter är tätt integrerade och samarbetar för att styra och övervaka processer i den fysiska världen. De kombinerar informationsteknologi (IT), såsom datorer och nätverk, med fysisk teknologi, som sensorer, maskiner och andra enheter, för att skapa avancerade, interaktiva system. Cyberfysiska system är vanligt förekommande i flera samhällsviktiga funktioner såsom produktion och distribution av el och energi, produktion och distribution av dricksvatten, i medicintekniska produkter inom hälso- och sjukvården samt inom transportsektorn.

Det är vanligt att begreppet cyberfysiska system delas upp i två olika huvudkategorier: Sakernas Internet/Internet of Things (IoT) och operativ teknik (OT).

IoT är fysiska objekt, som kan vara allt från hushållsapparater till industriella maskiner och bilar, som är utrustade med sensorer, programvara och nätverksanslutning. IoT-enheter inom industrin benämns Industrial Internet of Things (IIoT).

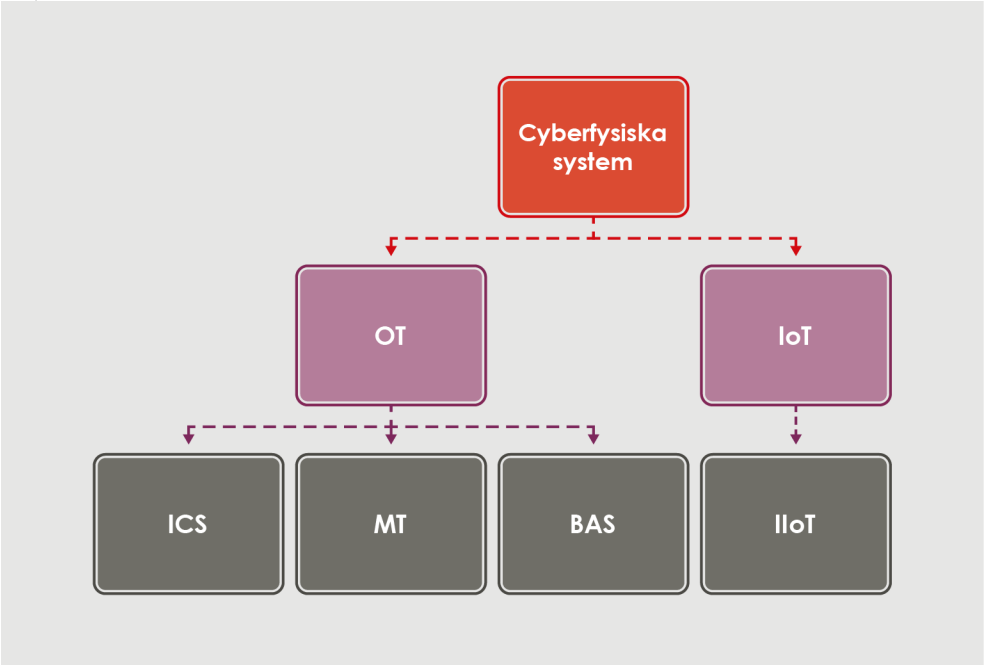
OT är ett samlingsbegrepp som innefattar bland annat industriella informations- och styrsystem (ICS), medicinteknik (MT) samt system för fastighetsautomation (BAS). Begreppet har etablerats för att särskilja och demonstrera de tekniska och funktionella skillnaderna mellan traditionella IT-system och primärt den industriella kontrollsystemmiljön. IT bearbetar och förädlar information,

och OT reglerar fysiska processer, ofta med direkt påverkan på människa eller omgivning. Det är vanligt att OT-system är optimerade för få eller inga oplanerade driftavbrott samt för att minimera risken för personskada, medan IT oftare är optimerat för att prioritera konfidentialitet hos den information som hanteras.

OT-system kan inte alltid hanteras på samma sätt som vanliga IT-system. Detta beror bland annat på att:

- OT-system är byggda för att vara ständigt tillgängliga och stabila under en lång tid, ofta 20 år eller längre. Detta innebär att det är sannolikt att systemleverantören kommer att sluta ge ut nya versioner och säkerhets-uppdateringar för systemet långt innan det planeras att tas ur drift. Därför kan OT-system inte uppdateras på samma sätt som vanliga IT-system. Faktum är att vissa OT-system inte kan uppdateras alls när de väl tagits i drift. Det är därför svårt att åtgärda upptäckta sårbarheter i OT-system, varför dessa system ofta behöver skyddas genom särskilda skyddsåtgärder.
- System som används för att övervaka och styra processer i realtid inte får störas ut eller förändras på ett sätt som innebär att systemet beter sig felaktigt.
- OT-system oftast är isolerade från internet.

Figur 1 Illustration över förhållandet mellan begreppen Cyberfysiska system, OT, IoT, ICS, MT, BAS samt IIoT.

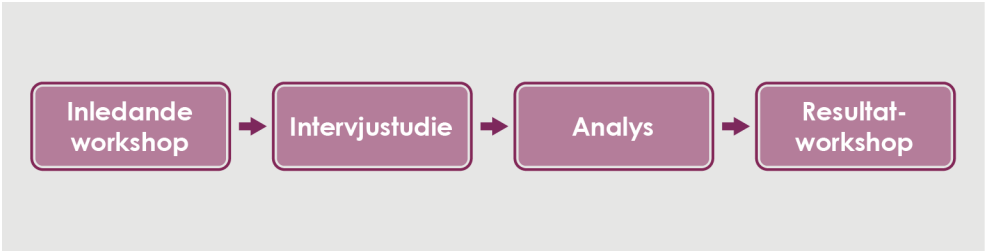


Om undersökningen

Detta kapitel beskriver undersökningens ingångsvärden, genomförande och hur resultatet omhändertagits.

Undersökningen är genomförd utifrån en kvalitativ ansats där de olika delmomenten har följt en sekventiell process:

Figur 2 Undersökningsprocessens delmoment



Inledande workshop

Ett av syftena med undersökningen var att ta fram ett underlag som kan användas som utgångspunkt för aktiviteter som syftar till att öka OT-säkerheten i samhället. Undersökningen behövde därför vara utformad på ett sätt som skulle säkerställa ett så brett omfång som möjligt.

För att säkerställa detta breda omfång arrangerades en inledande workshop tillsammans med olika centrala organisationer inom sakområdet i syfte att samla in information och eventuella medskick till undersökningsdesignen. Representanter från utvalda organisationer bjöds in till att delta i workshoppen och den slutliga deltagarlistan täckte de samhällsviktiga sektorerna energiförsörjning, transporter och hälso- och sjukvård inom såväl statlig som kommunal förvaltning.

Workshoppen genomfördes i form av ett öppet samtal utifrån tre frågeställningar:

- Vad vet vi i dagsläget om hur arbetet med OT-säkerhet ser ut i samhället?
- Vilka ytterligare kunskaper och insikter behövs för att kunna skapa bättre förutsättningar för arbetet med OT-säkerhet?
- Vilka förväntningar finns på slutresultatet och leveransen?

I diskussionerna framkom att det finns en rad roller med olika fokus och på olika nivåer som är eller borde vara involverade i OT-säkerhetsarbetet. Det finns roller som har ett djupt tekniskt fokus, och roller som är av mer strategisk natur. Likaså finns det individer som är väl insatta i området och individer som sannolikt ännu inte ens hört talas om begreppet OT. Slutligen finns det organisationer som kommit långt i sitt arbete och har en hög mognadsgrad inom området, samtidigt som det finns organisationer som fortfarande har en lång resa framför sig.

Under workshoppen fördes resonemang om att alla dessa faktorer påverkar vilka behov som finns. Exempelvis upplever en organisation med hög mognadsgrad inom OT inte samma utmaningar som en organisation med låg mognadsgrad (alt som inte kommit lika långt i sitt arbetet med OT-säkerhet) och en organisationsledning har inte samma behov som en tekniker.

Det framkom vidare att resursfrågan är viktig att beakta; mindre organisationer har ofta större utmaningar än större organisationer, vilket följer av att mindre organisationer har mer begränsade resurser. Detta innebär inte att större organisationer nödvändigtvis har det lättare än mindre organisationer, utan är endast ett konstaterande att det finns skillnader i förutsättningar. Samtidigt diskuterades även skillnader i förutsättningar för statlig, regional, kommunal och privat verksamhet samt hybrider av dessa kategorier.

Baserat på diskussionerna blev det klart att den vidare undersökningen behövde förstå målgrupperna både på ett brett och djupt plan. Undersökningen behövde säkerställa att följande aspekter och perspektiv omhändertogs:

- Förståelse för hur OT-säkerhetsarbetet bedrivs och fungerar;
- Kunskap om OT-arbetet är organiserat i olika organisationer.
- Identifiera de utmaningar som upplevs av olika roller; samt
- Utforska behov utifrån organisationernas olika förutsättningar (till exempel bransch, storlek, resurser, kompetenser).

Undersökningen konkretiserades till att utforska och förstå fyra övergripande teman:

Figur 3 Övergripande teman som inriktat undersökningens utformning och analys

Intervjuer som metod

För att få insikter på ett djupare plan krävs en kvalitativ ansats, varför undersökningen har genomförts som en intervjustudie. Djupintervjuer är en metod som erbjuder flera fördelar vad gäller att komma underfund med och förstå komplexa behov och problembilder.

En av de främsta fördelarna med att använda djupintervjuer som metod är att de möjliggör en djupare insikt i respondenternas perspektiv och erfarenheter. Genom att ställa öppna frågor kan respondenten själv välja hur de ska tolkas. När respondenten kan svara fritt uppnås två värdefulla mål:

- Varje intervju blir särskilt anpassad till varje respondents specifika situation och behov vilket medför att samtalet automatiskt förs in på de ämnen som är viktigast för varje respondent.
- Eftersom djupintervjuer är en mer personlig och flexibel interaktionsform känner sig respondenterna ofta mer bekväma vilket bidrar till att de lämnar mer ärliga och utförliga svar.

Intervju som metod erbjuder dessutom möjligheten att vid behov kunna stanna upp och gräva djupare i en specifik fråga eller område. På detta sätt kan detaljerad information erhållas som sannolikt inte skulle framkomma genom ett annat metodval, exempelvis enkäter.

Genomförande av undersökningen

En frågeguide, som återfinns i Bilaga 1, designades för att möta upp mot behovet av information.

Målgruppen för undersökningen avgränsades till personer som arbetar med OT-säkerhet i en organisation som anses utföra samhällsviktig verksamhet. Undersökningen fokuserade på organisationer verksamma inom någon av följande samhällsviktiga sektorer: energiförsörjning, dricksvattenförsörjning, transporter och hälso- och sjukvård.

Potentiella respondenter identifierades och kontaktades på olika sätt. Ett urval av MSB:s befintliga nätverk samt några branschorganisationer användes för att sprida information om undersökningen. Några kontakter förmedlades genom Nationellt cybersäkerhetscenter.

Intervjuperioden varade från maj till och med augusti 2024. Totalt genomfördes 18 intervjuer med följande fördelning per sektor:

Tabell 1 Antal respondenter per sektor

Energiförsörjning	Dricksvatten-försörjning	Transporter	Hälso- och sjukvård
7	3	3	5

För att säkerställa att så mycket information som möjligt skulle tas omhand från intervjuerna var alltid två personer närvarande vid varje intervju. Av dessa två interagerade den ena med respondenten och den andra dokumenterade diskussionen.

Omhändertagande av resultat

När samtliga intervjuer genomförts sammanställdes dokumentationen för att underlätta analys av materialet.

En uppföljande workshop arrangerades och genomfördes i syfte att stämma av resultatet av analysen, till vilken bland annat respondenterna var inbjudna till att delta.

Denna workshop hade två syften: dels att bekräfta och nyansera de insikter och slutsatser som identifierats i analysen, dels att närmare undersöka två av de områden som mest frekvent lyftes som utmaningar av respondenterna under intervjuerna.

Workshoppen delades in i två delar. I den första delen presenterades de identifierade storheterna i intervjuresultatet vilket följdes upp med samtal där deltagarna fick tillfälle att reflektera över analysen och ge sin feedback. I detta samtal bekräftade deltagarna slutsatserna och analysen. Den andra delen av workshoppen fokuserade på deltagarnas tankar avseende två områden, tillika tydliga utmaningar i arbetet med OT-säkerhet, som ofta var föremål för diskussion under intervjuerna:

- Hur kan vi få ledningen att förstå behovet av insatser inom OT-området?
- Hur kan vi få stöd för tolkning och efterlevnad av juridiska krav?

Resultaten från undersökningens samtliga delmoment har bearbetats och sammanfattats till denna slutrapport. Nedan följer en presentation av resultatet från intervjuerna och den uppföljande workshoppen samt ett avslutande kapitel innehållande MSB:s reflektioner kring resultatet.

Resultat

Detta kapitel redogör för sammanställningen av enskilda respondenters upplevelser och åsikter som framkommit under intervjuerna. Resultatet presenteras tematiskt utefter de fyra övergripande teman som togs fram för undersökningen:

- Organisationen kring OT-säkerhet;
- Kunskap och förståelse för OT-säkerhet;
- Utmaningar i OT-säkerhetsarbetet; och
- Vad skulle underlätta i OT-säkerhetsarbetet?

1 Organisationen kring OT-säkerhet

Det finns stora och tydliga variationer vad gäller hur samhällsviktiga organisationer har byggt upp sina respektive OT-säkerhetsfunktioner samt hur respektive organisation resonerat kring gränsdragningen mellan IT och OT. Detta avsnitt handlar om och beskriver dessa skillnader.

1.1 Tre typorganisationer

Baserat på respondenternas beskrivningar av hur deras respektive organisationer har resonerat kring gränsdragningen mellan IT och OT, så har tre huvudsakliga ”typorganisationer” utkristalliserats.

Typorganisation 1 ser IT och OT som två helt separata områden. Detta tar sig uttryck i organisationens struktur. I de flesta fall har separata grupperingar byggts upp för IT respektive OT med mer eller mindre vattentäta skott däremellan. De av respondenterna som arbetar vid organisationer som organiserat sig på detta vis beskriver att uppdelningen får negativa konsekvenser för organisationen och säkerhetsarbetet i stort, det vill säga inklusive men inte enbart för OT-säkerheten. Den silokultur som skapas av organisationsformen leder till att varje gruppering betraktar sitt eget område som viktigare än andras, vilket resulterar i att grupperingarna börjar konkurrera med varandra och konflikter uppstår. Bristen på samordning och kommunikation över grupperingsgränser leder till att vidtagna säkerhetsåtgärder inte är konsekventa över hela organisationen. I vissa fall initieras till och med säkerhetsåtgärder från en gruppering som direkt motverkar andra säkerhetsåtgärder från andra grupperingar.

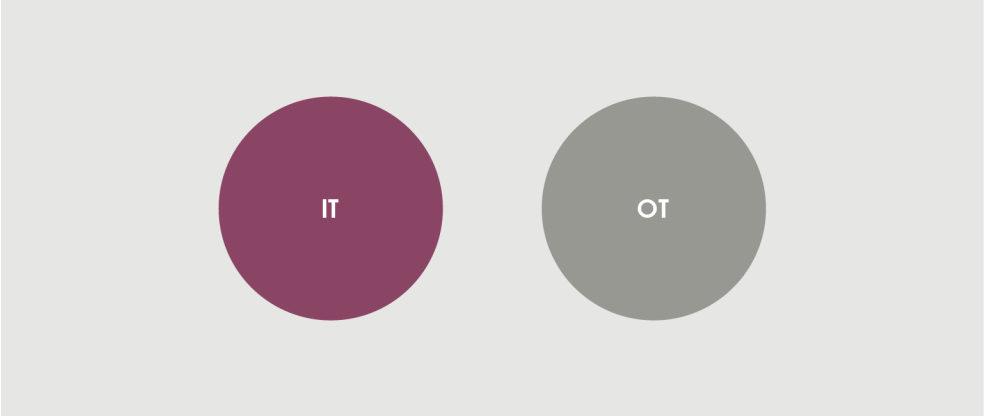
Konsekvensen av att dra hårda gränser mellan IT och OT blir således att kontrollen över organisationens säkerhet urholkas eftersom det blir omöjligt att skapa en komplett helhetsbild. Detta försvårar i sin tur arbetet med att såväl identifiera som hantera säkerhetsrisker i organisationen. Sådana försvårande omständigheter kan

anses innebära sårbarheter i sig eftersom organisationens förmåga att anpassa sig till nya säkerhetshot och utmaningar hindras.

Ytterligare en konsekvens av en mer eller mindre total separation av IT och OT är att arbetsmiljön för de individer som arbetar inom respektive område påverkas. En betydande andel av respondenterna från denna typorganisation beskriver att de mår dåligt över sin arbetssituation och de konflikter som uppstår till följd av det konstanta tävlandet inom organisationen.

De förhållanden som beskrivs ovan har beskrivits av respondenter från organisationer där IT och OT separerats antingen som olika enheter inom samma avdelning eller som olika avdelningar. *Hur* områdena separeras inom organisationen är alltså, baserat på respondenternas beskrivningar, irrelevant. Vad som är relevant är *graden av integrering och samarbete* mellan de olika grupperingarna.

Figur 4 Illustration av Typorganisation 1



Typorganisation 2 ser IT och OT som två sidor av samma mynt, det vill säga att organisationen aktivt arbetar för att de båda områdena ska samspela med varandra. I vissa av dessa organisationer hanteras både IT och OT inom ramen för samma gruppering oaktat om detta är på avdelnings- eller enhetsnivå. I de flesta fall är det dock olika grupperingar som fokuserar på IT respektive OT, men till skillnad från den föregående typorganisationen arbetar dessa grupperingar tillsammans med varandra.

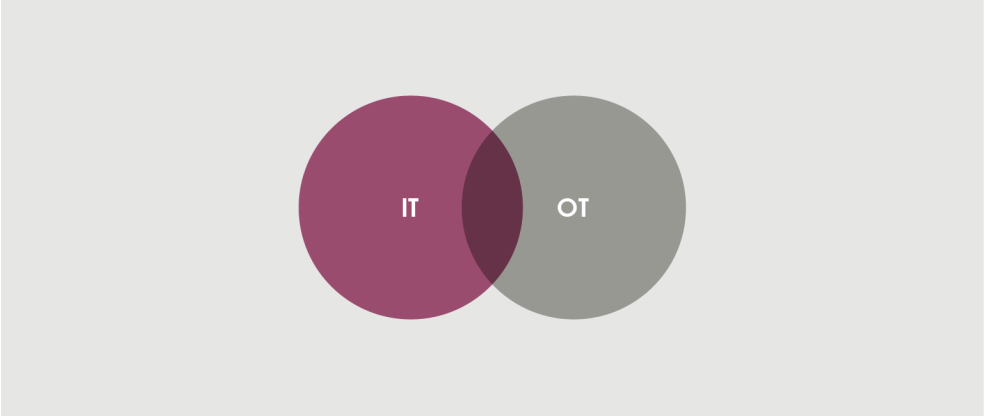
Att arbeta tillsammans beskrivs som mycket mer än kontinuerliga dialoger och avstämningar mellan grupperingarna. Det handlar snarare om en djup förståelse hos samtliga berörda för hur IT och OT relaterar till varandra och en gemensam insikt om att de två områdena kompletterar varandra och därmed måste samspela för att helheten ska fungera som önskat. Detta tar sig uttryck i att IT och OT-grupperingarna såväl planerar som utför stora delar av verksamheten tillsammans.

Organisationer med en hög grad av integration mellan IT och OT beskrivs uppnå ett effektivare säkerhetsarbete. Denna ökade effektivitet uppges ha sitt ursprung i tre huvudsakliga faktorer:

- Genom att IT och OT-grupperingarna i hög grad samplanerar och synkroniserar det arbete som ska bedrivas så säkerställs att de mest kritiska säkerhetsåtgärderna prioriteras samt att befintliga och planerade säkerhetsåtgärder kompletterar istället för att motverka varandra.
- Eventuella hinder i arbetet identifieras i tidigt skede vilket bidrar till att tid och resurser inte spenderas på uppgifter som inte går att genomföra.
- När personalen har god förståelse för flera områden utöver det som den enskilde primärt arbetar med läggs mer arbetstid på att faktiskt utföra de på att faktiskt utföra de nödvändiga arbetsuppgifterna och mindre tid och mindre arbetstid på att utbilda och övertyga kollegor om varför en viss uppgift är viktig och behöver utföras.

Utöver ökad effektivitet beskrivs denna typorganisation bidra till en mer hälsosam arbetsmiljö och bättre mående för personalen. Det faktum att den enskilda individen får utrymme att fokusera på ”sitt” område utan att behöva känna stress över intern konkurrens, i kombination med vetskapen att det egna området och perspektivet kommer att hörsammas, lyfts som bidragande faktorer till detta.

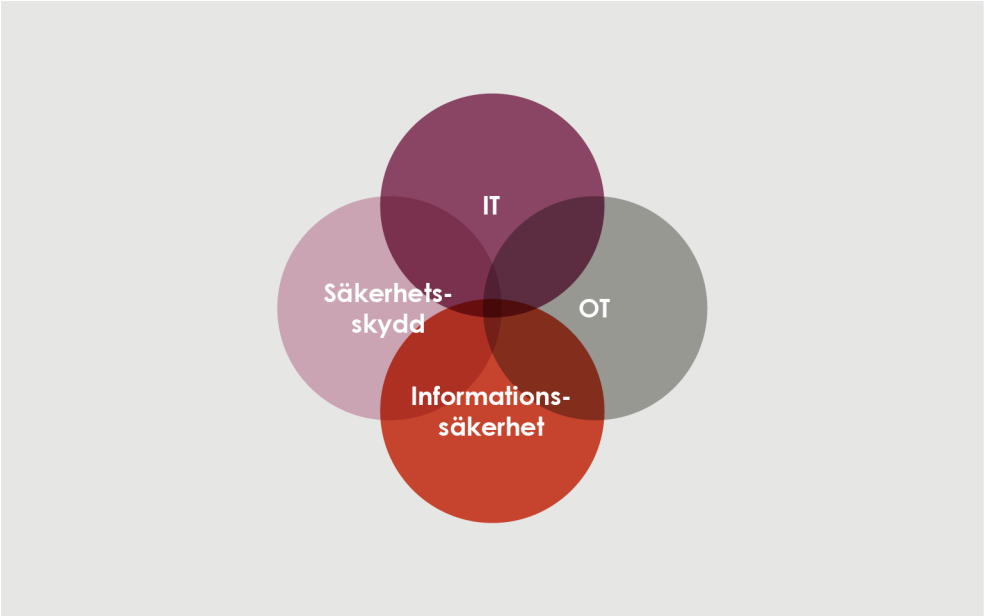
Figur 5 Illustration av Typorganisation 2



Typorganisation 3 är snarlik den närmast föregående och kan beskrivas som en utvidgad version av den. Denna tredje variant kännetecknas av att organisationen har ett ännu mer holistiskt förhållningssätt till säkerhet. Detta bredare förhållningssätt ser olika ut från organisation till organisation, men kännetecknas av att organisationens samtliga säkerhetsområden är samlade inom en och samma funktion eller gruppering. Vanliga områden är utöver IT och OT även informationssäkerhet och säkerhetsskydd.

Överlag beskrivs denna typorganisation i samma positiva anda som typorganisation 2. Några respondenter anser dock att det är lätt hänt att ett område försvinner bland övriga eller glöms bort när för många områden när för många områden integreras.

Figur 6 Illustration av Typorganisation 3



1.2 Roller, ansvar och arbetsuppgifter

Till skillnad från informationssäkerhetsområdet och dess yrkesroller som CISO, informationssäkerhetssamordnare och informationssäkerhetsspecialist, är det få personer inom OT-säkerhet som har en yrkesroll som tydligt fokuserar på just OT-säkerhet. Istället är det vanligt att arbetet med OT-säkerhet faller under roller med fokus på andra säkerhetsområden, eller som en del av ett bredare säkerhetsansvar. Av de totalt 18 respondenterna har endast sex en yrkesroll som anspelar på området OT-säkerhet. Endast tre av dessa sex har roller som är renodlade inom OT-säkerhet. Detta indikerar att en majoritet av de som arbetar med OT-säkerhet har yrkesroller som inte återspeglar återspeglar arbetets fokus (eller huvudinriktning). En stor majoritet av respondenterna beskriver vidare att de har så kallade tillikaroller där minst två men ofta fler säkerhetsområden ryms i samma roll.

Tillikarollerna beskrivs ha en procentuell uppdelning mellan de olika ingående områdena. Exakt hur uppdelningen ser ut mellan olika områden och vilka procent det handlar om skiljer sig från organisation till organisation. Den vanligaste kombinationen bland respondenterna är att halva arbetstiden fokuseras mot OT-säkerhet och andra halvan mot informationssäkerhet, men respondenterna uppger att denna uppdelning mycket sällan stämmer överens med verkligheten. Ofta läggs en betydande del av arbetstiden i praktiken endast på ett säkerhetsområde. Detta uppges delvis bero på att vissa områden traditionellt är mer eftersatta än andra, men även på respondenternas egna intressen och erfarenheter.

Exempel på yrkestitlar hos respondenterna

- Informationssäkerhetsspecialist
- IT-säkerhetsarkitekt
- Systemdesigner
- Cybersäkerhetsansvarig
- Strateg
- Projektledare
- Automationsingenjör
- Systemingenjör
- IT-chef
- Processledare
- IT-säkerhetsansvarig
- Samordnare

Flera av respondenterna beskriver att de inom ramen för sina respektive tjänster ansvarar för både strategiska och operativa/tekniska uppgifter rörande OT-säkerhet. Hur det strategiska och det operativa/tekniska viktas skiljer sig åt från organisation till organisation. Vilka konkreta uppgifter som bakas in under respektive kategori är däremot överlag detsamma i alla organisationer.

Strategiska arbetsuppgifter inom OT-säkerhet innefattar bland annat bevakning av externa hotbilder, interna planerade medvetandehöjande aktiviteter, hantering av upphandlingsfrågor och kravspecifikationer, säkerställande av lag- och regelefterlevnad samt genomförande av riskanalyser.

Operativa/tekniska arbetsuppgifter inom samma säkerhetsområde inkluderar bland annat att säkerställa säkerheten i nya system, genomförande av uppdateringar, implementering av åtkomstbegränsningar, konfiguration av brandväggar, nätverkssegmentering, klassificering av system, virtualisering, patchhantering och simuleringar.

Vidare beskrivs omvärldsbevakning och nätverkande som en viktig del i både det strategiska operativa/tekniska för att följa med i utvecklingen och dra lärdom av andra.

Respondenter från flera olika organisationer beskriver att en betydande mängd av deras arbetstid måste ägnas åt att oplanerat medvetandegöra och utbilda andra inom organisationen om vikten av säkerhetsarbete. Det kan exempelvis handla om att övertyga andra avdelningar som inte arbetar med säkerhetsfrågor om att ”godkänna” att en särskild säkerhetsåtgärd införs. Konsekvensen av detta beskrivs vara att uppmärksamheten till viss del avleds från kärnverksamheten inom OT-området, såsom genomförande av riskanalyser och implementering av säkerhetsåtgärder. Detta leder i sin tur till att vidtagande av nödvändiga säkerhetsåtgärder ofta tar betydligt längre tid att realisera än vad som egentligen hade behövts. Detta beskrivs närmare i närmast efterföljande tema.

2 Kunskap och förståelse för OT-säkerhet

Detta avsnitt handlar om kunskap och förståelse för OT-säkerhet i organisationen i stort, det vill säga hos personer som inte specifikt arbetar inom området.

Det finns betydande skillnader i säkerhetsmognad och förståelse för OT-säkerhetsarbetet både mellan olika organisationer och inom enskilda organisationer. När mognaden och förståelsen är låg får det negativa konsekvenser för säkerhetsarbetet. Vice versa, underlättas säkerhetsarbetet när mognadsgraden är hög. Ledningens kunskap och förhållningssätt har också betydelse för organisationens mognad, liksom erfarenhetsutbyte är viktigt för att höja kunskapen och förståelsen.

2.1 Säkerhetskultur

Att det finns en grundläggande säkerhetskultur i organisationen beskrivs av respondenterna som en förutsättning för hela organisationens förståelse för OT-säkerhet. Med säkerhetskultur menas här en organisatorisk säkerhetsmedvetenhet oberoende av sakområde som genomsyrar såväl personal som arbetssätt. Detta innebär att det inom organisationer med svag eller obefintlig säkerhetskultur heller inte kommer att finnas en förståelse för OT-säkerhet. Säkerhetskultur är därför något som kan anses skapa förutsättningar för OT-säkerhetsarbetet utan att OT-perspektivet för den sakens skull behöver vara centralt.

Respondenterna uppger att generellt sett är kunskapen om, och förståelsen för, OT och OT-säkerhet begränsad inom den egna organisationen hos individer som inte specifikt arbetar inom området. Flera beskriver att övriga kollegor inte har någon som helst uppfattning om att OT över huvud taget existerar. En del beskriver att övriga kollegor nog känner till begreppet OT, men att de inte skulle kunna förklara vad det är, vilken funktion det fyller eller vad som särskiljer OT från exempelvis IT. Endast en ytterst liten minoritet beskriver att övriga kollegor har en god uppfattning om vad OT är och varför det är viktigt att skydda.

Under intervjuerna blev det tydligt att de som arbetar med OT och OT-säkerhet gör starka kopplingar mellan OT-systemen och organisationens kärnverksamhet. OT-system är centrala i exempelvis produktionen och distributionen av energi och dricksvatten. Av den anledningen menar respondenterna att personer som arbetar i organisationen utan kunskap eller förståelse för OT därmed inte förstår organisationens verksamhet. Detta ska inte tolkas som att all personal förväntas ha någon form av expertis rörande OT, men däremot finns det en förväntan om att all personal ska ha någon form av grundläggande förståelse kring organisationens kärnverksamhet, vad denna består och är beroende av, och därmed varför det är viktigt att centrala beståndsdelar och beroenden skyddas. Budskapet är att konsekvenserna för samhället sannolikt blir betydligt större när OT-system är otillgängliga jämfört med IT-system; att en organisation tillfälligt inte kan hantera fakturor eller skicka e-post är omständligt och besvärligt, men det är värre om organisationen inte längre kan producera el eller dricksvatten, om sjukvården inte kan behandla vårdbehövande, eller om trafiken blir stillastående.

Tidigare nämndes att respondenterna beskriver att de behöver spendera betydande delar av sin arbetstid på att få andra avdelningar som inte arbetar med säkerhetsfrågor att ”godkänna” olika saker, exempelvis justeringar i befintliga system eller införandet av nya säkerhetsåtgärder. Ett konkret exempel kan vara ett förslag om att införa en ny behörighetsstyrning för tillgång till OT-miljön som skulle innebära en minskning av antalet medarbetare i organisationen som har behörighet till miljön. Sådana och liknande förslag beskrivs ofta resultera i konflikter inom organisationen. Detta uppges bero på att kollegor känner sig ifrågasatta och opålitliga när deras behörigheter begränsas. Konflikterna kan även handla om att övriga kollegor anser att deras egna arbetsuppgifter blir alltför omständliga utan egna behörigheter. Respondenterna å sin sida menar att behörigheter till system ska vara behovsstyrda och att det därmed är naturligt att personer med arbetsuppgifter som inte kräver direkt tillgång till OT-systemen heller inte har den behörigheten. Vidare menar de att negativa effekter på övriga kollegors förmåga att utföra sina arbetsuppgifter är mycket ovanliga eftersom det nästintill alltid går att hitta nya arbetssätt där alla parter fortfarande är nöjda. En respondent uttryckte det på detta vis: ”Många gånger är administrativ personal särskilt negativt inställda till förändringar då de tror att deras eget arbete kommer att hindras genom implementeringen av nya säkerhetsåtgärder, men de brukar till slut acceptera förändringarna när de inser att deras eget arbete kan fortgå som tidigare.” Att få kollegor att ”godkänna” saker handlar alltså om att bygga upp en acceptans för förändringar ur ett säkerhetsperspektiv inom organisationen, eller uttryckt i andra ord, att främja en säkerhetskultur.

Respondenterna menar att en bristande eller obefintlig säkerhetskultur inom organisationen medför att personal som inte arbetar med säkerhetsfrågor varken utvecklar kunskap eller förståelse för säkerhet över huvud taget, och än mindre för OT-säkerhet. En god säkerhetskultur och kunskap om OT-säkerhetens betydelse för kärnverksamheten beskrivs som grundförutsättningar för effektivt säkerhetsarbete. Detta eftersom en god säkerhetskultur medför att det finns en acceptans för förändringar i arbetssätt och behörighet till system ur säkerhetssynpunkt, vilket innebär att de som arbetar med säkerhet kan fokusera på på att förbättra säkerheten istället för att behöva motivera för andra delar av organisationen om varför en viss åtgärd är nödvändig.

Inom organisationer med en god säkerhetskultur och där övriga kollegor har en uppfattning om vad OT är och varför det är viktigt att skydda, beskrivs att arbetet med OT-säkerhet upplevs både effektivt och tillfredsställande. Respondenterna från dessa organisationer uppger att de ifrågasätts i liten utsträckning eller inte alls, och beskriver att de upplever det som lätt att få gehör i form av stöd och resurser för sina förslag.

2.2 Ledningens roll

Enligt respondenterna finns det en tydlig koppling mellan ledningens förhållningssätt till säkerhetsfrågor och nivån och kvaliteten på organisationens säkerhet. Två typer av ledningar beskrivs: den som betraktar säkerhet som en kostnad, och den som ser det som en investering.

Ledningar som ser säkerhet som en kostnad upplevs av respondenterna ofta sakna förståelse och kunskap för frågan. Konsekvensen av detta är att det blir svårt, om inte omöjligt, för de som arbetar med säkerhet att utföra sitt arbete. Respondenterna beskriver att de resurser som tilldelas säkerhetsområdet sällan är tillräckliga för att bibehålla befintliga säkerhetsnivåer, än mindre tillräckliga för att organisationen ska kunna följa med i utvecklingen och kunna skydda sig mot samtida och framtida hot och risker. Denna sortens ledningar beskrivs bland annat som ovilliga till att byta ut föråldrad utrustning och system, och förespråkar istället fortsatt underhåll. Motiveringen är ofta att det är för dyrt att köpa in och gå över till ny utrustning och "nya" (nya system).

I den efterföljande workshoppen fördes en diskussion med deltagarna kring just föråldrad utrustning och utbyten av sådan. Diskussionen landade slutligen i att det i OT-sammanhang inte går att undvika föråldrade system, men att varje organisation har ett eget ansvar i att säkerställa att föråldrade system skyddas av lämpliga säkerhetsåtgärder så länge de är i drift och att de så snart som möjligt byts ut mot modernare system. Det är således inte önskvärt att hålla liv i ett föråldrat system längre än vad som verkligen är nödvändigt.

Ett fåtal respondenter beskriver att deras respektive ledningar är personligt engagerade i säkerhetsfrågorna, att de förstår att säkerhetsarbetet behöver ske kontinuerligt och att detta arbete får lov att kosta pengar eftersom kostnaden efter en allvarlig incident kraftigt överstiger kostnaden för förebyggande av incidenter. Nya regleringar på området (i synnerhet NIS2), liksom inträffade incidenter, beskrivs vara bidragande faktorer till ledningens ökade medvetenhet och intresse för säkerhetsfrågor.

Närheten mellan verksamheten och ledningen beskrivs vara en nyckelfaktor för ett effektivt säkerhetsarbete. Organisationer där säkerhetsfrågorna finns representerade i ledningsgruppen är, enligt respondenterna, betydligt mer välfungerade ur säkerhetssynpunkt än organisationer där säkerhet inte anses vara en ledningsfråga.

2.3 Vikten av erfarenhetsutbyte

Såväl internt som externt erfarenhethetsutbyte beskrivs av respondenterna som en viktig del för att sprida kunskapen och förståelsen för OT-säkerhetsarbetet.

Internt erfarenhetsutbyte syftar till att tillmötesgå det behov som finns av att dela erfarenheter och kunskap mellan olika avdelningar och enheter inom den egna organisationen. Det beskrivs som viktigt att säkerställa att samtliga delar av organisationen har en gemensam förståelse för säkerhetskrav och bästa praxis samt att säkerställa att det säkerhetsarbete som bedrivs inom organisationen är konsekvent.

Hur det interna erfarenhetsutbytet ser ut skiljer sig från organisation till organisation. Inom vissa organisationer ligger tonvikten vid enstaka interna kommunikationsinsatser som syftar till att höja den allmänna säkerhetsmedvetenheten. I andra organisationer har särskilda forum etablerats med regelbunden mötesfrekvens där medarbetare på en mer detaljerad nivå kan diskutera och utbyta erfarenheter om säkerhetsutmaningar och lösningar. Internt erfarenhetsutbyte är särskilt framträdande i organisationer som har en högre mognadsgrad och en mer etablerad säkerhetskultur.

Externt erfarenhetsutbyte sker primärt genom deltagande i olika forum eller nätverk, omvärldsbevakning på olika sätt, samt genom deltagande på konferenser och mässor. Flera respondenter beskriver vidare att de har stort utbyte genom personliga nätverk, det vill säga personliga kontakter med andra individer med kunskap om OT-säkerhet.

Såväl under intervjuerna som under den efterföljande workshoppen blev det tydligt att de som arbetar med OT har behov av samordning och kunskapslyftande aktiviteter. Detta beror bland annat på att det finns ett begränsat antal personer som arbetar med och har kompetens inom OT samt att det finns särskilda utmaningar kopplat till säkerhet och hanteringen av OT-system som inte förekommer rörande andra sorters system. Eftersom det finns en begränsad skara av personer som alla sannolikt har upplevt liknande utmaningar är det viktigt att dessa personer kan träffas och utbyta erfarenheter och kunskaper med varandra. Respondenterna uttrycker att det finns stora behov av nätverk, konferenser och utbildningar med särskilt fokus på OT för att få insikter och inspiration i arbetet. Vidare ser respondenterna stora fördelar med att flera av de nätverk, konferenser och utbildningar som finns inte riktas specifikt mot enskilda branscher eftersom de flesta utmaningarna kring OT-säkerhet inte är branschspecifika.

En majoritet av respondenterna uppger att de deltar aktivt och regelbundet i externa erfarenhetsutbyten. Ett fåtal gör det dock inte och beskriver att detta primärt beror på att de inte känner till vilka nätverk som finns. Generellt är en övervägande majoritet av respondenterna av åsikten att det behövs fler OT-specifika aktiviteter i alla kategorier.

3 Utmaningar i OT-säkerhetsarbetet

Detta avsnitt sammanfattar de huvudsakliga utmaningarna som framkom under intervjuerna. De fem som listas är inte en uttömmande lista över upplevda utmaningar, men redogör för det som lyftes av en majoritet av respondenterna. Unika tillika organisationsspecifika utmaningar utelämnas denna rapport i syfte att skydda berörda respondenters anonymitet och/eller organisation.

3.1 Intern förståelse och arbetssätt

Den interna förståelsen för OT och OT-säkerhet hos personer som inte specifikt arbetar inom området, samt hur organisationen är organiserad upplevs av en majoritet av respondenterna som en stor utmaning och ett hinder för effektivt säkerhetsarbete. En mer uttömmande beskrivning av detta finns under rubriken *Organisationen kring OT-säkerhet* ovan.

Utmaningen ligger i att OT-säkerhetsarbetet ofta hanteras som ett eget avgränsat område inom många organisationer. Konsekvensen blir att övriga delar av organisationen som inte specifikt arbetar med OT eller säkerhet har en begränsad förståelse för frågorna vilket har en försvårande effekt på arbetet. Det innebär vidare att de som arbetar med OT-säkerhet får ägna merparten av sin arbetstid åt att motivera och förklara sitt arbete för resterande delar av organisationen istället för att ägna sig åt att faktiskt utföra sina egna uppgifter. Dessutom får det lätt negativa följder när OT-säkerheten hanteras separat från andra säkerhetsområden eftersom organisationen då förlorar det holistiska säkerhetsperspektivet. Exempel på negativa följder av olika organisationsstrukturer finns under rubriken *Organisationen kring OT-säkerhet* ovan.

3.2 Ledningens engagemang

Samtliga respondenter beskriver hur viktigt det är att ledningen har en förståelse för varför OT-säkerhetsarbetet är viktigt för att tillräckligt med resurser ska tilldelas arbetet. Samtidigt beskriver en stor majoritet att just detta inte är fallet i sina respektive organisationer. En mer uttömmande beskrivning av detta finns under rubriken *Kunskap och förståelse för OT-säkerhet* ovan.

Utmaningen ligger i att en övervägande majoritet av ledningar ser säkerhetsfrågan som något kostsamt och besvärligt, vilket medför att organisationen mer eller mindre duckar för säkerhetsarbetet. Medarbetarna upplever att de har svårt att få gehör för sina behov vilket leder till att värdefull arbetstid spenderas på annat än att faktiskt förbättra organisationens OT-säkerhet. Flera respondenter uppger att de känner en stor hjälplöshet med anledning av detta; de vet vilka sårbarheter som organisationen har och vilka åtgärder som behöver vidtas för att hantera sårbarheterna, men får inte möjlighet till att utföra åtgärderna.

3.3 Kompetensbrist

I stort sett samtliga respondenter vittnar om att deras respektive organisationer upplever stora svårigheter med att hitta personer med rätt kompetenser till

OT-säkerhetsarbetet. Akademin anses inte matcha de behov av bred grundkompetens som behövs inom samhällsviktig verksamhet avseende OT-säkerhet. De utbildningsprogram som finns anses inte beröra relevanta områden i tillräcklig utsträckning för att nyutexaminerade ska vara attraktiva på arbetsmarknaden för roller inom OT-säkerhet.

Respondenterna efterfrågar generella kunskaper inom flera säkerhetsområden parallellt. Allra helst bör kandidater ha en delad bakgrund inom både IT och OT med grundläggande kunskaper inom informationssäkerhet och säkerhetsskydd. Det handlar om att organisationerna söker efter personer som kan hantera den tekniska komplexiteten och diversiteten inom OT-systemen och som har förmåga att engagera och samordna hela organisationen i säkerhetsarbetet.

Eftersom tillgången på kompetent personal är betydligt mindre än efterfrågan blir många organisationer tvungna att anställa personal som egentligen inte lever upp till ställda krav. Istället behöver organisationen investera betydande resurser för att själva utbilda kandidaterna i de kunskapsområden som de saknar. Det är dock vanligt att dessa personer, så snart de erhållit dessa kunskaper, väljer att snart lämna organisationen för att söka sig vidare. Detta eftersom de nu besitter högt åtråvärda kompetenser som andra organisationer kan betala mer för. Respondenterna uppger att deras organisationer lägger betydande resurser på att agera lärosäten bara för att nästan omedelbart förlora den nybyggda kompetensen. Effekten blir alltså att samhällsviktig verksamhet inom OT-området befinner sig i ett näst intill kroniskt underbemannat tillstånd.

3.4 Juridiska krav

Inom juridiken är OT-säkerhet ett område som hamnat i skuggan av andra säkerhetsområden; de regleringar som finns på cybersäkerhetsområdet är skrivna med IT- och informationssäkerhet i fokus. Detta innebär inte nödvändigtvis att regleringarna inte alls är applicerbara även på OT-säkerhetsområdet, men respondenterna menar att det ligger en utmaning i att det uppstår otydligheter och tolkningssvårigheter när det inte är uttryckligen specificerat att även OT omfattas av regleringarna.

Efterfrågan på individer med juridisk kompetens och teknisk förståelse är hög och överstiger kraftigt tillgången. Inom OT-säkerhetsområdet är denna diskrepans mellan tillgång och efterfrågan ännu större än inom informationssäkerhets- och IT-säkerhetsområdet. Effekten av detta blir att respondenterna själva tvingas till att tolka juridiska material och väva in OT-säkerhetsperspektivet - trots att de inte är juridiskt utbildade. En majoritet av respondenterna menar vidare att deras respektive tillsynsmyndigheter saknar nödvändiga kompetenser för att kunna agera rådgivande på OT-säkerhetsområdet.

Ytterligare en utmaning som lyfts är att effekten av befintliga regleringar medför att OT-säkerhetsarbetet lätt nedprioriteras till fördel för IT- och informationssäkerhet. Detta beror på att ledningen tenderar att prioritera IT- och informationssäkerhetsåtgärder, eftersom dessa åtgärder specificeras i regleringarna och då kan vara föremål för tillsyn.

3.5 Hinder för erfarenhetsutbyte

Såväl internt som externt erfarenhetsutbyte är något som respondenterna värdesätter mycket högt. Det finns dock flera utmaningar som uppges hindra det önskvärda erfarenhetsutbytet.

Respondenterna beskriver att det interna erfarenhetsutbytet, om något sådant över huvud taget finns, försvåras av att medarbetare från andra delar av organisationen inte prioriterar säkerhetsfrågor eller ser värdet i att dela med sig av sina erfarenheter. En del respondenter beskriver även att det kan finnas organisatoriska hinder, såsom brist på tid och resurser, som gör det svårt att genomföra regelbundna erfarenhetsutbyten.

Det externa erfarenhetsutbytet försvåras bland annat av sekretess och GDPR, vilket skapar osäkerhet kring vilken information som kan delas. Flera av respondenterna trycker på att värdet med att delta i nätverk och forum är att utbyta information med andra, men att det ändå ofta uppstår en obalans bland deltagare i nätverk och forum. Obalansen består i att vissa organisationer och individer aldrig delar med sig av information till andra, men förväntar sig samtidigt att andra ska dela med sig av information till dem. Ett sådant ensidigt förhållningssätt tenderar att skada förtroendet och tilliten som deltagarna har till varandra.

4 Vad skulle underlätta i OT-säkerhetsarbetet?

Detta avsnitt sammanfattar faktorer som respondenterna anser är viktiga för att förbättra förutsättningarna för att bedriva ett systematiskt och resurseffektivt OT-säkerhetsarbete inom såväl det strategiska som operativa/tekniska. De fem faktorerna som beskrivs nedan är inte en uttömmande lista över framgångsfaktorer, men redogör för det som lyftes av en majoritet av respondenterna. Övriga medskick och önskemål utelämnas denna rapport i syfte att skydda berörda respondenters anonymitet och/eller organisation.

4.1 Ökad förståelse, resurser och samordning i den egna organisationen

Respondenterna uttrycker ett stort behov av stöttning i att höja medvetenheten kring och förståelsen för OT generellt i den egna organisationen. Detta anses vara en nödvändighet för att underlätta den interna samordningen och för att få gehör från såväl ledningen som från övriga kollegor för olika typer av initiativ som syftar till att förbättra organisationens säkerhet, både i allmänhet men i synnerhet avseende OT.

Särskilt angeläget framstår en grundläggande utbildning kring OT-säkerhet för ledningen för att öka kunskapen om OT. Även målgruppsanpassad och kontinuerlig extern information lyfts som förslag på åtgärder som skulle kunna hjälpa till med att väcka nyfikenhet och få upp frågorna på ledningens agenda. Att ledningen engagerar sig i OT-säkerhetsfrågan anses av respondenterna vara en förutsättning

för att arbetet ska prioriteras och tilldelas nödvändiga resurser. Det anses även viktigt att ledningen bidrar till att fostra en säkerhetskultur inom organisationen för att säkerhetsfrågorna ska integreras i samtliga led i verksamheten.

4.2 Bättre förutsättningar för erfarenhetsutbyte

Det finns stora behov av forum och nätverk där olika organisationer kan mötas. Erfarenhetsutbyte förutsätter dock att utbytet är ömsesidigt och att det finns förtroende mellan deltagande parter. Givet ämnesområdets natur är detta inte en självklarhet.

Det upplevs som negativt om ett ömsesidigt utbyte saknas. Respondenterna misstänker att oviljan att dela information oftast beror på att det finns en osäkerhet kring huruvida det är lämpligt eller ej att dela viss information samt att tilliten mellan deltagare ännu inte infunnit sig. Respondenterna menar att digitala möten inte är önskvärt eftersom många digitala mötesverktyg upplevs som osäkra vilket påverkar viljan att dela information; Fysiska möten och träffar är enligt respondenterna den bästa mötesformen. I de fall digitala träffar är nödvändigt underlättar det erfarenhetsutbytet om ordförande har valt ett säkert mötesverktyg för mötet i vilket det är möjligt att verifiera deltagarnas identiteter.

Respondenterna påpekar att det finns bra nätverk där det råder stort förtroende och en öppenhet mellan deltagarna. Samtidigt känner inte alla respondenter och organisationer till dessa. Således skulle informationsinsatser om vilka nätverk som redan finns tillgängliga kunna öppna upp för ett bredare och mer omfattande erfarenhetsutbyte inom befintliga nätverk.

4.3 Juridiskt stöd

Att inte veta hur organisationen ska förhålla sig till befintliga regleringar inom cybersäkerhetsområdet från ett OT-perspektiv lyfts som en av de största utmaningarna som respondenternas respektive organisationer står inför. Det finns således ett stort behov av jurister som kan tolka de regelverk som finns inom cybersäkerhetsområdet utifrån hur de påverkar OT-verksamheten, vilka säkerhetsåtgärder som är rimliga att vidta, och hur organisationen bör förhålla sig till olika regelverk som går in i varandra och gränsdragning mellan dem.

Utöver jurister utrycker respondenterna önskemål om mer juridiskt stödmaterial. Referensarkitekturer, vägledningar till föreskrifter som etablerar tydliga miniminivåer för åtgärder, och grundmallar för kravställning vid upphandlingar är exempel på stödmaterial som respondenterna själva har föreslagit.

4.4 Tillgänglig kompetens på arbetsmarknaden

Respondenterna upplever att den kompetens som de är i behov av inte finns tillgänglig på arbetsmarknaden. Detta leder till att organisationerna själva känner sig tvungna att agera lärosäte eller utbildningsanordnare.

Respondenterna menar att det behövs fler instanser där personer kan utbildas inom OT-säkerhet. De menar att akademin behöver bli bättre på att säkerställa att det finns universitetsutbildningar som möter de behov som finns av kompetens inom samhällsviktig verksamhet och kritisk infrastruktur.

4.5 Tillsyn och sanktioner

Tydligare juridiska regleringar avseende OT-säkerhet, tillsyn och sanktioner välkomnas av respondenterna eftersom detta ställer krav på att ledningen ger prioritet till OT-säkerhetsfrågan. Tillsyn efterfrågas för att få återkoppling på det utförda arbetet, säkerställa korrekta tolkningar av regler och förordningar samt för att bedöma huruvida organisationens vidtagna åtgärder är tillräckliga. Respondenterna menar att tillsyn, i kombination med sanktioner och personligt ansvar, är nödvändigt för att säkerställa att regleringar får önskad effekt. Detta utifrån ett upplevt gap mellan lagstiftning och efterlevnad, när sanktioner saknas.

Avslutande reflektioner

I detta kapitel görs några sammanfattande reflektioner kring intervjuresultatet. Reflektionerna presenteras tematiskt utifrån samma struktur som föregående kapitel.

På en övergripande nivå kan det konstateras att deltagande organisationer i undersökningen skiljer sig åt; de har kommit olika långt i sitt arbete med OT-säkerhet och de har olika förutsättningar att förhålla sig till vilket påverkar arbetet.

Trots att en medveten insats gjordes för att få en bra spridning av deltagande organisationer i undersökningen avseende sektor, storlek, bransch och geografisk spridning är det inte möjligt att garantera att resultatet av undersökningen är representativt på nationell nivå. Trots detta ger resultatet indikationer på vad som upplevs som utmanande och svårt; en majoritet av respondenterna målar upp liknande eller identiska problembilder oaktat vilken sektor de är verksamma i. Resultatet indikerar därför att det finns vissa förutsättningar som behöver vara på plats för att OT-säkerhetsarbetet ska kunna bedrivas resurseffektivt och fokuserat, liksom det finns utvecklingspotential inom flera områden för att underlätta arbetet med OT-säkerhet.

Organisationen kring OT-säkerhet

Undersökningen visar att organisationer bör sträva mot ett holistiskt säkerhetsarbete, i stället för att varje avdelning arbetar isolerat. Vidare bör i synnerhet grupperingar som arbetar med IT respektive OT vara samordnade och föra kontinuerlig dialog med varandra för att säkerställa effektivare resursanvändning och en enhetlig strategi för säkerheten i stort. En integrering av IT och OT underlättar samarbete, kommunikation och informationsdelning samt ger en bättre översikt över hela organisationens säkerhetsbehov och risker. Vidare bidrar en sådan integrering till en bättre arbetsmiljö, för de som arbetar med OT-säkerhet. För att uppnå detta krävs en ökad och kontinuerlig kommunikation mellan enheterna.

En majoritet av deltagande organisationer beskriver att OT-arbetet utförs inom ramen för roller med ett annat säkerhetsområde i fokus. Den renodlade tydligheten som finns inom exempelvis informationssäkerhet, säkerhetsskydd och dataskydd saknas på OT-området. Tillikaroller behöver inte vara något negativt; den som har flera säkerhetsområden i sin portfölj har en möjlighet att se synergier och arbeta med flera säkerhetsområden på ett mer integrerat och effektivt sätt. Det kan dock vara svårt att upprätthålla en hög nivå av expertis och framdrift inom flera säkerhetsområden samtidigt. Med andra ord finns det en risk för att vissa områden blir eftersatta när inbördes prioriteringar behöver göras mellan olika säkerhetsfrågor. Tillikaroller och breda portföljer innebär per definition att varje ingående område endast kan tillägnas begränsat med tid vilket kan medföra en lägre effekt.

Bristen på OT-specifika roller kan vara en bidragande faktor till att organisationerna upplever det så svårt att hitta de kompetenser som de eftersöker. När det inte finns tydliga områden och kompetenser är det svårt för framtida högskole- och universitetsstudenter att intressera sig för och rikta in sig på dessa områden.

Det är viktigt att organisationer låter de som har i uppgift att skydda kärnverksamheten besluta om vilka säkerhetsåtgärder som är nödvändiga. Det är viktigt att säkerhetsåtgärder är rimliga i sin omfattning för att inte ha en alltför negativ inverkan på förmågan att utföra sitt arbete. Det är däremot inte rimligt att övriga delar av organisationen mer eller mindre kan lägga veto på föreslagna säkerhetsåtgärder som läggs fram av säkerhetspersonalen.

Kunskap och förståelse för OT-säkerhet

Det är tydligt att en grundförutsättning för att kunna arbeta effektivt med sakområdet är att det finns en grundförståelse för OT i organisationen, hos såväl ledning som hos annan personal. I nuläget har personer som inte specifikt arbetar med OT generellt dålig kunskap om OT och varför det behöver skyddas. Det får till konsekvens att värdefull tid går förlorad i och med att åtgärder behöver förklaras och motiveras.

Utmaningar i OT-säkerhetsarbetet

Utbildningssystemet tycks inte vara anpassat för att tillgodose arbetsmarknadens behov av rätt kompetenser. Det finns behov av utbildningar som ger en bred grund att stå på för att intressera OT-arbetsmarknaden. De flesta organisationer eftersträvar personal med expertis inom både IT och OT, samt gärna ytterligare kunskaper inom i synnerhet informationssäkerhet och säkerhetsskydd. Detta ligger i linje med att olika säkerhetsområden behöver integreras i organisationerna för att säkerställa ett konsekvent och effektivt säkerhetsarbete.

Det finns stora behov av tolkningsstöd och tydliggörande av regleringar inom cybersäkerhetsområdet från ett OT-säkerhetsperspektiv. Befintliga regleringar saknar detta perspektiv vilket innebär osäkerhet och otydlighet för samhällsviktig verksamhet. Det är även bekymmersamt att flera av de deltagande organisationerna i denna undersökning upplever att de inte får tillräckligt stöd från sina respektive tillsynsmyndigheter. Önskemål om att bli föremål för tillsyn för att få klarhet och inriktning förutsätter att den instans som utför tillsynen har nödvändig kompetens för att kunna göra detta. Respondenternas beskrivningar indikerar att så inte är fallet.

Vad skulle underlätta i OT-säkerhetsarbetet?

Eftersom OT-säkerhet är ett område med särskilda förutsättningar är det viktigt att det finns möjligheter till erfarenhetsutbyte med andra och att det finns forum för detta. Det har framkommit att det finns några bra forum, men det är osäkert om de är kända bland relevanta aktörer. Detta antyder att det kanske inte endast handlar om att skapa nya forum, utan även att de som driver dessa forum bör förbättra sin informationsspridning. Det handlar också om att säkerställa att informationskanaler och forum är säkra, så att det känns tryggt att dela information. Bra nätverk för erfarenhetsutbyte karaktäriseras av ett ömsesidigt utbyte och att det finns ett förtroende mellan parterna, vilket ställer höga krav på att information kan delas på ett tryggt och säkert sätt.

Övriga reflektioner

- MSB gör bedömningen att hälso- och sjukvårdssektorn är den sektor som är i störst behov av stöd under den närmaste tiden. Historiskt har denna sektor fått mindre uppmärksamhet än övriga samhällsviktiga sektorer som varit representerade i undersökningen, vilket innebär att OT-säkerheten ligger långt efter övriga sektorer. MSB gör här en bred tolkning av begreppet OT och inkluderar såväl fastighetsautomation och medicinteknik i detta. Hälso- och sjukvårdssektorn har särskilda förutsättningar att förhålla sig till, exempelvis krav på certifiering av medicintekniska produkter samt vårdpersonalens behov av snabba och enkla lösningar, vilka försvårar arbetet med OT-säkerhet och även introducerar nya säkerhetsrisker.
- Vidare gör MSB bedömningen att de behov och önskemål som framkommit i denna undersökning kan inte tillmötesgås av en enskild aktör. MSB, liksom näringslivet, har stora och viktiga roller att spela, men uppmuntrar samtidigt andra instanser att bidra med vad de kan. God OT-säkerhet i samhällsviktig verksamhet bidrar till att säkerställa samhällets funktionalitet i såväl vardag som kris eller krig.

Bilaga 1 – Intervjuguide

Område 1: Inledande frågor

1. Vad är din arbetstitel och vad innebär den?
2. Hur mycket tid i din tjänst lägger du på säkerhetsarbete?
3. Hur skulle du beskriva organisationen som du arbetar på? Hur många ”kunder” servar organisationen?

Område 2: Organisationen kring OT-säkerhet

4. Vad innebär det att arbeta med OT-säkerhet hos organisationen? Vad gör ni i det arbetet?
5. Hur ser organisationen ut avseende OT-säkerhet? Vilka rutiner och arbetssätt finns? Vilka roller eller funktioner är delaktiga? Hur prioriteras resurser till arbetet i jämförelse med andra områden?

Område 3: Kunskap och förståelse för OT-säkerhet

6. Hur ser förståelsen för OT-säkerhet ut i organisationen? Hos kollegor inom andra områden? Hos din chef? På ledningsnivå utöver din chef?
7. Får du träffa och utbyta tankar och erfarenheter med andra som också arbetar med OT-säkerhet? Inom organisationen? Med andra organisationer inom samma bransch eller branschöverskridande?

Område 4: Utmaningar i OT-säkerhetsarbetet

8. Vilka är de största utmaningarna som du möter i arbetet med OT-säkerhet?
9. Hur hanterar ni de utmaningar som finns i arbetet idag?
10. Har ni några goda exempel att dela med er av där ni lyckats särskilt bra i ert arbete med OT-säkerhet?

Område 5: Vad skulle underlätta i OT-säkerhetsarbetet?

11. Vad skulle underlätta för dig i din vardag när det gäller OT-säkerhet? Finns det några särskilda interna förändringar som skulle underlätta? Finns det någon särskild extern hjälp och stöttning som skulle underlätta?

Område 6: Övriga frågor

12. Vart vänder ni er när ni har problem eller behöver stöd (ex. personliga kontakter, konsulter, löser problemet själva, etc.)?
13. Använder ni något metodstöd eller några andra former av stöd i ert arbete? Om ja, vilka avsändare har det stöd som ni använder er av? Vilka former har det stöd som ni använder er av? Varför använder ni just detta stöd och inte något annat? Om nej, hur kommer det sig att ni inte använder några stödmaterial?
14. Övrigt.

Myndigheten för
samhällsskydd
och beredskap

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publikationsnummer MSB2544 – februari 2025 ISBN-nummer 978-91-7927-598-3