NÄR TVÅ VÄRLDAR MÖTS

UTMANINGAR OCH PRIORITERINGAR INOM OT-SÄKERHET I EN ALLTMER SAMMANKOPPLAD VERKLIGHET

Radar. EXCLUSIVE NETWORKS FORTINET NOZOMI NETWORKS

FÖRORD

Syftet med denna rapport är att bidra till en ökad medvetenhet för säkerhet av vår operativa teknik. Genom förklaringar och även praktiska råd hoppas vi kunna ge dig som läsare idéer, verktyg och en förståelse för hur olika delar av verksamheten kan ha helt olika perspektiv på samma fråga. Genom att öka intern kompetens, stärka ledarskapet och använda rätt verktyg kan vi alla förbättra vår säkerhetsposition.

För att minska Sveriges sårbarhet inom OT-säkerhet krävs ett holistiskt angreppssätt som adresserar både mänskliga och tekniska faktorer. Samarbete mellan avdelningar och anpassning till nya regulatoriska krav som lagen om cybersäkerhet hoppas vi efter att du läst denna rapport ser som möjligheter snarare än krävande måsten.

Denna rapport är framtagen av Radar Group, i samarbete med Exclusive Networks, Fortinet och Nozomi Networks. Studien som rapporten bygger på har utförts enligt Radars metodik, med Radars data och med ett oberoende förhållningssätt till de deltagande parterna. Radar ansvarar självständigt för de fakta och de slutsatser som redovisas.

Studien som rapporten bygger på har genomförts mellan juni-september 2024 och innefattar både en kvantitativ och en kvalitativ undersökning. En enkätundersökning har genomförts med ett brett underlag av svenska verksamheter för att möjliggöra analys och jämförelser mellan olika branscher, storlek på verksamheter och mellan olika roller. För att komplettera och möjliggöra djupare resonemang kring studiens frågeställningar har även djupintervjuer genomförts. Ett centralt fokus för rapporten är hur olika roller och funktioner ser på frågan om OT-säkerhet, varpå studien inkluderar respondenter från såväl IT-organisationer, OT-organisationer som ledningsgrupper.

SAMMANFATTNING

De senaste åren har vi sett en ökad integrering av IT och OT för att möjliggöra ett bredare nyttjande av data för ökat värdeskapande och effektivitet i verksamheter. Denna utveckling har både skapat möjligheter, men även nya sårbarheter som behöver hanteras. Denna rapport belyser hotbilden och cybersäkerhets-mognaden runt den operativa tekniken, vilka utmaningar som hindrar säkerhetsarbetet och lämnar rekommendationer för åtgärder som kan bidra till att överkomma dessa.

SVERIGES OT-MILJÖER STÅR INFÖR BETYDANDE SÄKERHETSUTMANINGAR

Medan vi gör framsteg i vissa områden, såsom att öka medvetenheten om OT-säkerhetsbehov, är vi fortfarande flera gånger mer sårbara än våra nordiska grannar. Rapporten kan påvisa att hela 71 procent av svenska verksamheter bedömer att deras OT-säkerhet är otillräcklig.

KUNSKAPSBRIST OM OT-SÄKERHET DET STÖRSTA HINDRET

Den främsta barriären för förbättrad OT-säkerhet är den interna kunskapsbristen, vilket tydligt framgår i samma dataunderlag. Bristen på kompetens, särskilt inom OT-specifika säkerhetsåtgärder, är ett centralt problem. Många organisationer försöker fortfarande hantera OT-säkerheten med IT-verktyg, som inte alltid är anpassade till OT-specifika krav. Vidare utmanas säkerheten av föråldrade system som inte är byggda för att möta moderna säkerhetshot.

ETT DELAT ANSVAR FÖR OT KRÄVER NÄRMARE SAMARBETE

Säkerhetsarbetet påverkas även tydligt av det delade ansvaret mellan IT och OT. Medan OT-avdelningar vanligtvis ansvarar för drift och inköp av system, faller säkerhetsansvaret ofta på IT. Detta skapar en klyfta när IT och OT har olika prioriteringar och saknar förståelse för varandras perspektiv. Utmaningen förstärks av ett bristande ledarskap och avsaknad av strategi och styrning där ledningen i många fall inte tar ett tillräckligt aktivt ansvar för risk eller säkerhet. En förutsättning för att höja säkerhetsnivån är att främja bättre samarbete mellan dessa avdelningar, vilket visat sig ha positiv effekt på säkerheten. Det är tydligt att mycket av säkerhetsutmaningarna hänger ihop med organisatoriska faktorer, snarare än att endast härröra från teknisk komplexitet. Därmed påverkas OT-säkerheten tydligt av organisatoriska förutsättningar som storlek på verksamhet, ledningens engagemang, samt ansvarsfördelning och organisering av IT och OT.

NYA REGULATORISKA KRAV KAN STÄRKA ELLER UTMANA SÄKERHETSARBETET

Vi noterar även de regulatoriska krav som kommer, där den nya lagen om cybersäkerhet (NIS2) nämns som en både utmanande och möjliggörande faktor. De nya cybersäkerhetskraven kan driva fram förbättringar, men de kan också skapa utmaningar för verksamheter som ännu inte är tillräckligt förberedda. Många verksamheter ligger efter i arbetet med att implementera de nya kraven och 69 procent uppger att de saknar nödvändig kompetens, vilket kan leda till att man försöker implementera åtgärder som kan vara opassande eller skadliga ur ett OT-perspektiv.

TILLÄMPA HOLISTISKA SÄKERHETSÅTGÄRDER BASERADE PÅ ER RISKANALYS

För att möta kraven på dagens OT-säkerhet samt förbereda organisationen för framtida hot är det viktigt att jobba holistiskt och tydligt koppla cyberrisk och cybersäkerhet till andra verksamhetsrisker och verksamhetsmål. Annars blir arbetet dåligt samordnat och silobaserat. Höj medvetenheten och kunskapen med regelbundna utbildningar och säkerhetsövningar för såväl IT- som OT-personal, samt ledning och styrelse.

Varje åtgärd som vidtas bör grunda sig på en noggrant genomförd riskanalys. Det är viktigt att identifiera sårbara områden i OT-miljön och utveckla åtgärder som är proportionerliga mot de specifika riskerna. Denna strategi minskar risken för att överinvestera i säkerhetsprodukter som kanske inte ger tillräckligt värde för verksamheten. Många organisationer försöker lösa sina OT-säkerhetsutmaningar genom att använda samma tänk som finns inom IT, vilket inte alltid är optimalt. Investeringar kan dock exempelvis göras i teknik som är anpassningsbar till OT-miljöer, som nätverkssegmentering för att säkerställa skydd och kontroll.

För att stärka säkerheten och minska risken för cyberincidenter bör IT- och OT-avdelningar integreras bättre. Genom att inrätta samverkansforum med representanter från både IT och OT kan samarbetet förbättras och ansvar delas på ett mer strukturerat sätt. Detta stärker också den övergripande säkerhetsstrategin genom att identifiera och åtgärda gemensamma sårbarheter och risker.

INNEHÅLLSFÖRTECKNING

Rapportförfattare:

Daniella Gustafsson, Rådgivare
E-post: daniella.gustafsson@radargrp.com

Elienor Werner, Rådgivare
E-post: elienor.werner@radargrp.com

Richard Werner, Head of Research & Analytics
E-post: richard.werner@radargrp.com

Research:

Iván Araque Cristóbal, Research Data Analyst
E-mail: ivan.ac@radargrp.com

Del 1

OT-SÄKERHET ÄR EN NATIONELL ANGELÄGENHET

En stark tradition av digitalisering och industrialisering har lett till en ökad sammankoppling av IT- och OT-tekniker. Utvecklingen har skapat massor av möjligheter för en mängd branscher, men även säkerhetsutmaningar som behöver hanteras. Sverige befinner sig i ett särskilt sårbart läge, och det är avgörande att vi skyddar vår operativa teknik för att skydda människor, stärka motståndskraften mot hot och säkra vår välfärd och konkurrenskraft.

MÖJLIGHETER OCH SÅRBARHETER NÄR IT & OT INTEGRERAS

Före IT:s intåg krävdes det ofta att en person fysiskt skulle närvara vid maskiner och system för att övervaka eller styra. Inledningsvis hade OT-system liten likhet med IT-system eftersom de var isolerade och körde proprietära kontrollprotokoll med hjälp av specialiserad hårdvara och mjukvara. Med IT-integration har detta förändrats radikalt. OT liknar i allt större utsträckning IT-system då IT-teknik införts för att främja integration mot verksamhetssystem samt fjärrövervakning och hantering. Nu kan operatörer övervaka och styra system på avstånd. Detta är särskilt viktigt i geografiskt spridda anläggningar, såsom oljeplattformar eller avlägsna gruvor, där fjärrstyrning minskar behovet av att skicka personal till svåråtkomliga, eller rentav farliga platser.

Med andra termer skulle vi kunna säga att vi i stora drag nu har ”IT-fierat” vår operativa teknik. På köpet har vi fått några negativa konsekvenser men också ett antal positiva. Det har funnits en drivkraft från verksamheten för att ena processer runt data, vilket till stor del är varför vi överhuvudtaget kopplar upp vår OT. Vi vill ha dess data för att ta bättre verksamhetsbeslut.

Med integrationen av IT har våra OT-system inte bara blivit sammankopplade utan också uppkopplade genom bland annat trådlösa tekniker, vilket möjliggjort insamling av stora mängder data från maskiner och sensorer. Som exempel kan data om maskinprestanda, energiförbrukning och produktionsutbyten samlas in och analyseras med hjälp av IT-baserade verktyg för att optimera produktionsprocesser, förutse underhållsbehov och minska driftskostnader. Det kan göra det lättare för verksamheter att exempelvis identifiera när en maskin börjar visa tidiga tecken på slitage, vilket gör att underhåll kan planeras innan ett kostsamt haveri inträffar. Möjligheterna är många inom en rad olika branscher, men utvecklingen har samtidigt bidragit till att introducera nya sårbarheter som behöver hanteras.

Denna integration stöder nya IT-funktioner men ger betydligt mindre isolering för OT från omvärlden jämfört med systemen från förr. Allmänt tillgängliga kommunikationsprotokoll och trådlös teknik ersätter äldre proprietär teknik, vilket ökar exponeringen för sårbarheter och incidenter inom cyberområdet. Även om säkerhetslösningar har utformats för att hantera dessa problem i typiska IT-system, måste särskilda försiktighetsåtgärder vidtas när dessa lösningar introduceras i OT-miljöer. I vissa fall krävs nya säkerhetslösningar som är anpassade till OT-miljön.

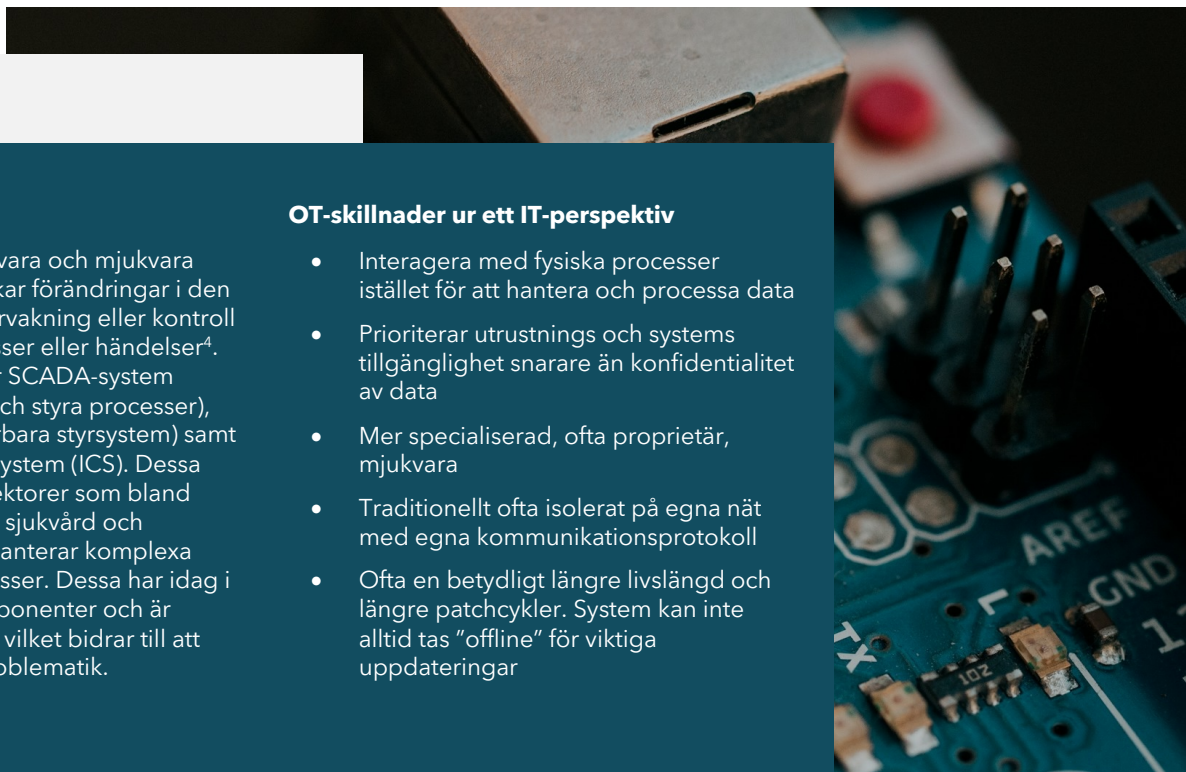
Definition

Operativ Teknik – OT

Med OT menas den hårdvara och mjukvara som upptäcker eller orsakar förändringar i den fysiska miljön genom övervakning eller kontroll av fysiska enheter, processer eller händelser[4]. Exempel på OT-system är SCADA-system (system för att övervaka och styra processer), PLC-system (programmerbara styrsystem) samt olika industriella kontrollsystem (ICS). Dessa system är kritiska i flera sektorer som bland annat tillverkning, energi, sjukvård och transportsektorn där de hanterar komplexa fysiska verksamhetsprocesser. Dessa har idag i olika utsträckning IT-komponenter och är anledning till konvergens vilket bidrar till att skapa både värde och problematik.

OT-skillnader ur ett IT-perspektiv

- Interagera med fysiska processer istället för att hantera och processa data
- Prioriterar utrustnings och systems tillgänglighet snarare än konfidentialitet av data
- Mer specialiserad, ofta proprietär, mjukvara
- Traditionellt ofta isolerat på egna nät med egna kommunikationsprotokoll
- Ofta en betydligt längre livslängd och längre patchcykler. System kan inte alltid tas ”offline” för viktiga uppdateringar



DET ÄR SKILLNAD MELLAN IT OCH OT

Även om likheterna idag är flera så har OT många egenskaper som skiljer sig från traditionella IT-system, främst olika typer och syn på såväl risker som prioriteringar. Några av dessa innefattar allvarliga risker för människors hälsa, miljö och ekonomi såsom produktionsförlust. OT har olika prestanda- och tillförlitlighetskrav och använder operativsystem och applikationer som kan anses vara okonventionella i en typisk IT-nätverksmiljö. Säkerhetsskydd måste implementeras på ett sätt som upprätthåller systemets integritet under normal drift såväl som under cyberattacker.

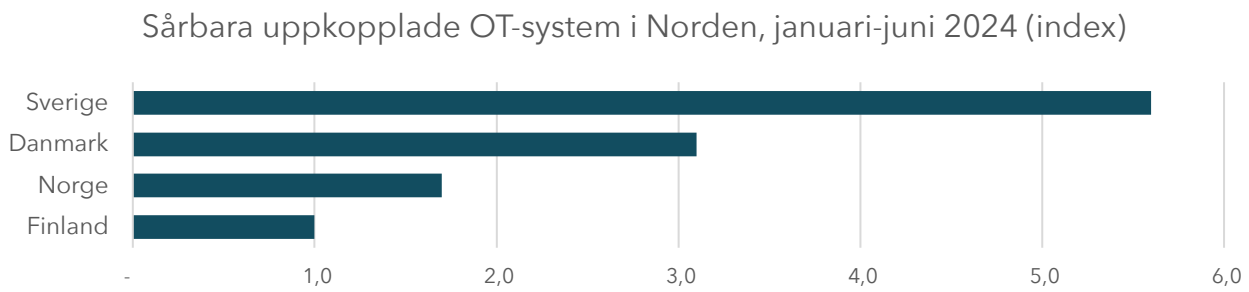
Kategori	IT	OT	Likheter
Syfte och användning	Hanterar, lagrar och bearbetar information för affärsfunktioner	Styr och övervakar fysiska processer och utrustning	Båda hanterar och bearbetar data, men för olika ändamål
Säkerhetsprioritering	Datasäkerhet, konfidentialitet och integritet	Kontinuerlig drift, säkerhet och tillförlitlighet	Båda kräver hög säkerhet för att skydda sina respektive system
Säkerhetsfokus	Skydda data mot obehörig åtkomst och cyberattacker	Skydda fysiska processer och maskiner mot störningar och sabotage	Båda kräver robusta säkerhetsåtgärder för att skydda mot cyberhot
Arkitektur	Bygger på standardiserade plattformar och protokoll, flexibla och skalbara	Blandning av äldre och ny teknik, specialiserad hårdvara och mjukvara	Båda använder digitala system som bygger på hårdvara och mjukvara
Livscykler	Kortare livscykler, regelbundna uppdateringar och patchar	Längre livscykler, längre mellan uppdateringar för att undvika driftstopp	Båda behöver regelbundna uppdateringar, även om frekvensen skiljer sig
Driftmiljö	Kontorsmiljöer eller datacenter med stabila förhållanden	Krävande industriella miljöer med extrema förhållanden	Båda kräver övervakning och kontroll i kontrollerade miljöer
Kommunikationsteknik	Använder standardiserad nätverksteknik som Ethernet och TCP/IP	Använder ibland proprietära nätverksprotokoll och isolerade system	Båda är nätverksberoende för kommunikation och dataöverföring
Ökande konvergens	Integrerar OT för bättre integration av företagsprocesser	Använder IT-teknik för att förbättra effektivitet och tillgänglighet av data	Både IT- och OT-system konvergerar alltmer och delar teknologier som molnlagring och virtualisering

Det är viktigt att förstå både det som särskiljer och det som förenar IT- och OT-system. Att enbart fokusera på olikheterna riskerar att försvåra samarbete och minska förståelsen mellan de olika organisatoriska funktionerna som ansvarar för respektive område. Samtidigt är det viktigt att förstå att det också finns centrala skillnader som gör att systemen kräver olika hantering. Att enbart utgå ifrån likheterna och behandla det ena området exakt som det andra riskerar att leda till lösningar som är dåligt anpassade efter verklighetens förutsättningar.

VARFÖR HOTAS VÅR OT NU?

Hotet mot OT har ökat markant under de senaste åren, och det finns flera skäl till varför detta sker nu snarare än tidigare. För det första har den tidigare utvecklingen att digitalisera och ansluta OT-system till IT-nätverk dramatiskt ökat den möjliga attackytan. Medan OT tidigare ofta var isolerat från externa nätverk, har Industrial Internet of Things (IIoT) och Industry 4.0-strategier under årens lopp kopplat samman OT och IT på ett sätt som inte bara möjliggör effektivare drift och skapande av data, utan också öppnar upp för mer IT-traditionella attacker.

En annan faktor som bidrar till det ökade hotet är den långa livslängden på många OT-system. Många av dessa system har varit i drift under decennier och designades inte med dagens säkerhetshot i åtanke. Längre livscykler har ofta följts av längre utvecklingscykler och vikt har lagts vid operativ stabilitet. Att då komma med snabba ändringar i system har alltid tidigare rimmat väldigt dåligt med stabilitetskraven. IT-området har krävt snabba cykler tack vare snabbfotade angripare samtidigt som OT-sidan inte har fått utså samma historiska prövning. IT och OT har därmed länge gått i otakt.



Figur 1. Sårbara uppkopplade OT-system i Norden, januari-juni 2024. Indexerat med Finland som referensland

Att vi kopplat upp allt fler OT-system syns inte minst i statistiken där vi i Sverige har flest OT-system öppna mot Internet. Sett till vår egen storlek, oavsett om vi mäter i antal människor, antal företag, BNP eller någon annan variabel, så sticker vi ut i Sverige i hur många öppna OT-system vi har.

BETYDELSEN FÖR SVERIGE

Sverige har en lång historia av digitalisering och industrialisering vilket bidrar till den OT-säkerhetsutmaning vi nu möter med mycket gammal utrustning och system som är utmanande att säkra. Att Sverige befinner sig i ett betydligt sämre läge än bland annat vår industrialiserade granne Finland kan vara ett resultat av en svagare koppling mellan digitalisering och säkerhet. Sverige och svenska verksamheter har länge varit duktiga på att digitalisera och dra nytta av fördelarna med ny teknik, men där säkerhetsarbetet inte har hängt med i samma tempo. Givet sin historia har Finland i kontrast haft en starkare säkerhets- och beredskapskultur. Därtill så har Sverige en lång tradition av decentraliserad styrning inom offentlig sektor som stundtals skapar utmaningar kring att enas runt en gemensam nationell strategi, och där bristen på tydligt ägarskap saktar ner viktig utveckling.

Som ett välutvecklat land med en stark ekonomi och teknologisk infrastruktur kan Sverige vara ett attraktivt mål för cyberangrepp från både statliga och icke-statliga aktörer. Som land utmanas vi idag cybersäkerhetsmässigt med över 2,5 miljoner registrerade attacker per år. Dessa aktörer kan ha som mål att störa kritisk infrastruktur eller stjäla känslig information med syfte att skada tillit i samhället men också skada Sverige, verksamheter och individer ekonomiskt. Vårt nya NATO-medlemskap adderar till den hotbilden. Sveriges beroende av branscher med hög grad av OT, landets höga grad av digitalisering och uppkoppling, användning av äldre OT-system, och brist på integrerad säkerhet gör landet mer sårbart för OT-säkerhetsproblem. Den tydliga sårbarheten kombinerat med den ökande hotbilden mot Sverige som land gör OT-säkerhet till en viktig fråga att hantera.

Tillverkningsindustrin är ett exempel på en sektor med mycket OT. Sektorns andel av svensk BNP uppgår till ungefär 20% eller **900 miljarder**, och den står för **16% av den totala sysselsättningen**. Att skydda OT är viktigt både för att säkra mänsklig hälsa och ekonomiska värden som är kritiska för vår välfärd och konkurrenskraft.

ETT HOTLANDSKAP UNDER UTVECKLING

Under de senaste åren har hotlandskapet blivit mer sofistikerat, målinriktat och har mycket lägre trösklar för att kunna tillgodose sig med ny teknik. Angripare har tillgång till avancerade verktyg och teknik i samma hyrmodeller som vilken modern IT-avdelning som helst, till exempel genom ransomware-as-a-service (RaaS) som erbjuds på dark web. Dessa verktyg gör det enkelt även för mindre kompetenta kriminella att utföra avancerade attacker i den digitala världen.

Just nu upplever vi även en geopolitisk situation med inslag av extremism som har påverkat den svenska situationen negativt. Det tidigare så ofta neutrala Sverige har allt tydligare valt sida och vår egen naivitet kring demokrati, extremism och religion har tyvärr satt oss i skottgluggen vid ett flertal tillfällen. Säkerhetspolisen rapporterar att främmande makt blivit alltmer offensiv och de tydligaste hoten uppges komma från Ryssland, Kina och Iran[7].

"Det största hotet är om de med illvilja inser potentialen. Det finns stora luckor när det kommer till OT-säkerhet."

- Chief Information Officer (CIO)

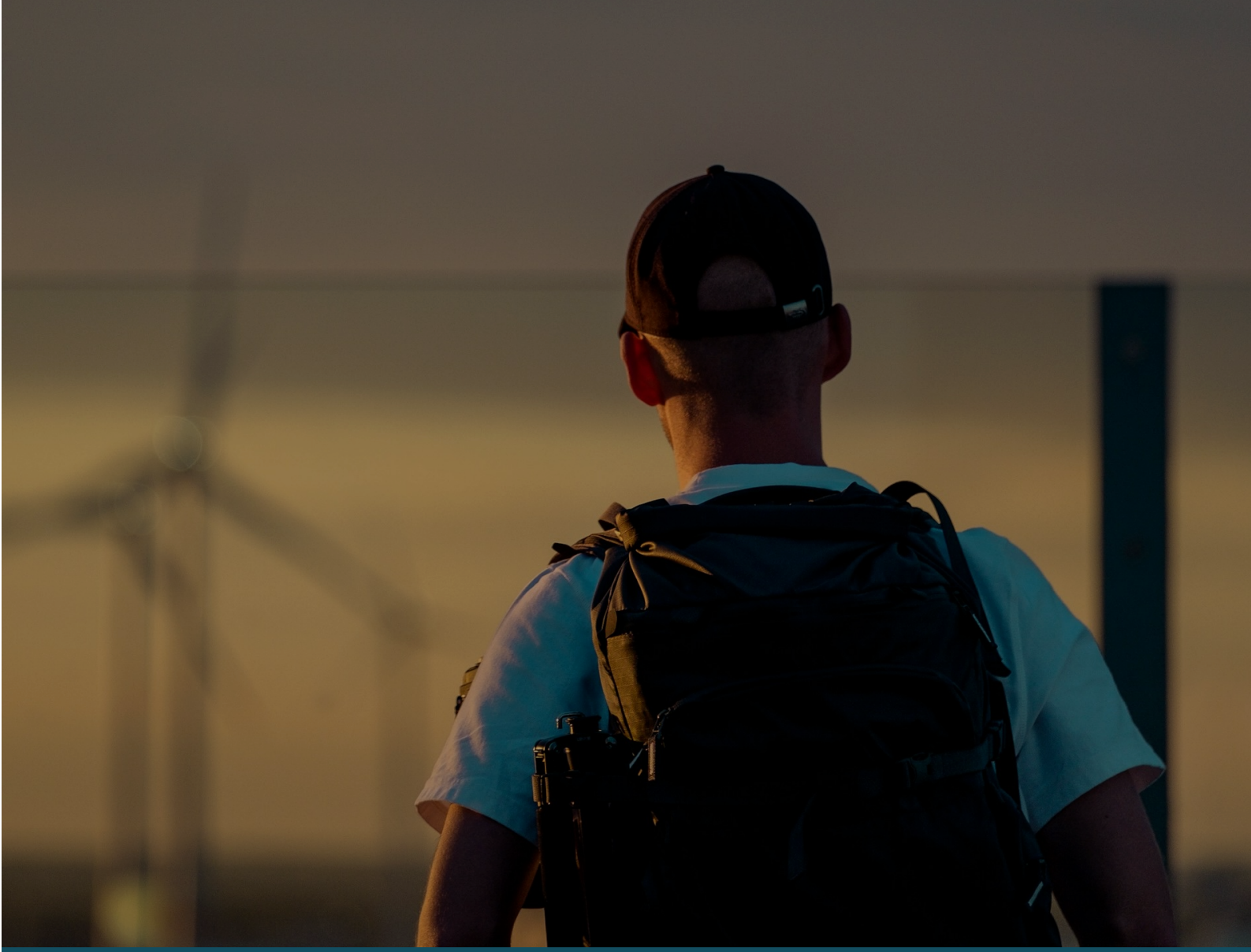
Från det pågående kriget i Ukraina kan vi även dra lärdomar från hur systematiska attacker mot kritisk infrastruktur använts som en strategisk spelbricka[2]. Kriget inleddes med massiva cyberattacker mot energiförsörjningen vilket har följts av fortsatta attacker och sabotage mot kritisk infrastruktur i landet. I händelse av krig eller kris är det helt avgörande att kunna upprätthålla samhällskritiska funktioner som el-, vatten- och matförsörjning, kommunikations- och transportinfrastruktur samt sjukvård. Det gör dessa sektorer till viktiga måltavlor och samtliga av dessa sektorer är även starkt beroende av operativ teknik för att kunna leverera sina tjänster. Med en otillräcklig nivå av OT-säkerhet lämnar vi ett sårbarhetsgap som kraftigt kan reducera vår motståndskraft när vi behöver den som mest. Denna insikt är även en anledning till att dessa sektorer nu omfattas av tuffare cybersäkerhetsregleringar.

HOTET MOT OT ÄR INTE ENDIMENSIONELLT

Även om vi har sett uppmärksammade cyberattacker riktade mot OT-miljöer är det betydligt fler attacker som utförs mot IT. Den högre graden av standardisering inom IT gör det enklare att designa och distribuera effektiva attackmetoder. I takt med att IT och OT blir närmare sammankopplat påverkas även OT:n av dessa hot. De taktiker, tekniker och procedurer (TTP) som tillämpas av angriparna kan skilja sig åt och cyberattackerna kan både ha en direkt och indirekt påverkan på OT.

Metod	Måltavla	Möjlig konsekvens för OT
IT-baserade TTP	IT	Indirekt påverkan på OT-miljön. Exempelvis att produktionen stannas som en säkerhetsåtgärd, eller en tillfällig nedstängning till följd av ett drabbat IT-system som OT har ett beroende till i sin processkedja
IT-baserade TTP	IT/OT	Attack utförs mot IT, men angriparen kan röra sig lateralt genom nätverken och även komma åt OT-system. Detta kan exempelvis möjliggöra dataexfiltrering och dubbel utpressning av hotaktören
IT-baserade TTP	OT	En hotaktör med begränsad förmåga och kapacitet runt OT kan tillämpa IT-baserade metoder för att rikta in sig mot eventuella IT-komponenter inom OT-tillgångarna. OT är den tilltänkta måltavlan, men metoden är inte den mest sofistikerade utifrån ett OT-perspektiv
OT-baserade TTP	OT	Direkt och potentiellt kritisk påverkan på OT-miljön. Hotaktören tillämpar OT-specifika metoder och kan uppnå en högre grad av sofistikering och precision för att åsamka skada på verksamheten

Detta belyser vikten av att jobba med en holistisk säkerhet, även när vi "bara" pratar om OT-säkerhet. OT-säkerhet kan sägas innefatta det som utgör en risk för OT-systemen, alltså inte bara säkerhet i den operativa tekniken i sig utan även andra system eller tillgångar som kan utgöra sårbarheter för vår OT.



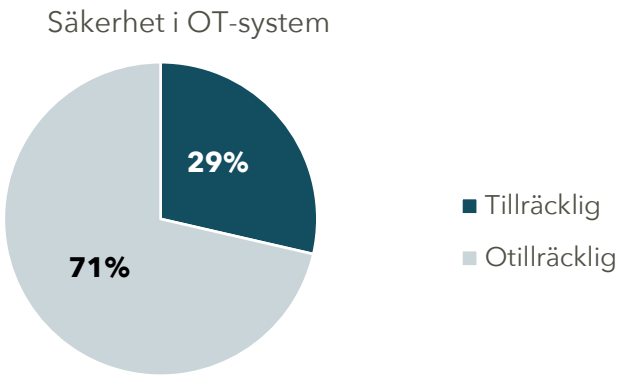
Del 2

FÖRUTSÄTTNINGAR OCH UTMANINGAR FÖR ATT SÄKRA OT

Vi upplever ett ökande hot, ett sårbart läge och med allvarliga konsekvenser om vi drabbas. Hur väl rustade är våra svenska verksamheter för att hantera utmaningen med att säkra OT-systemen? Vilka hinder upplevs som störst och har vi de verktyg som behövs för att hantera situationen?

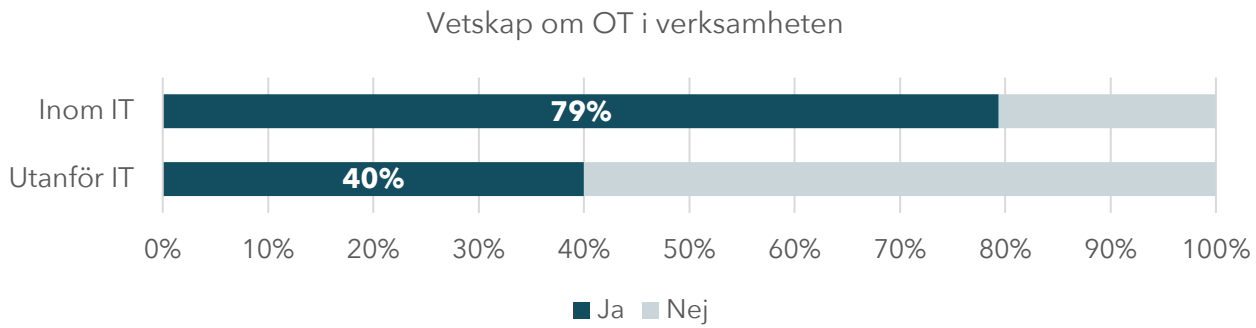
VÅR BEREDSKAP FÖR HOTET

Det är tydligt att en majoritet upplever nivån av cybersäkerhet i OT-system som otillräcklig. Bara en dryg tredjedel upplever att säkerhetsnivån är tillräckligt hög givet den hotbild man anser sig möta. Detta skiljer sig till viss del mellan verksamheter i olika storlekar, där stora verksamheter i högre grad uppger att säkerheten är otillräcklig (83 procent), kontra små och medelstora verksamheter (67 procent otillräcklig). Detta skulle kunna bero på att större verksamheter har en mer komplex miljö med fler system och utrustning som ska säkras. Det är även möjligt att stora verksamheter, som oftare har dedikerade resurser och team för att arbeta med detta, har en bättre överblick och förståelse för problematiken och därmed svarar mer "negativt" på grund av det.



Figur 2. Upplevd säkerhet i OT-system

Frågan om säkerhet i OT-system förutsätter en förståelse för vad som utgör OT i ens verksamhet, vilket inte är lika tydligt för alla. Framförallt skiljer sig detta mellan roller som befinner sig inom IT och utanför IT (roller utanför IT innefattar roller inom linjeverksamheten som bland annat sälj, HR eller ekonomi, samt ledningsgrupp).

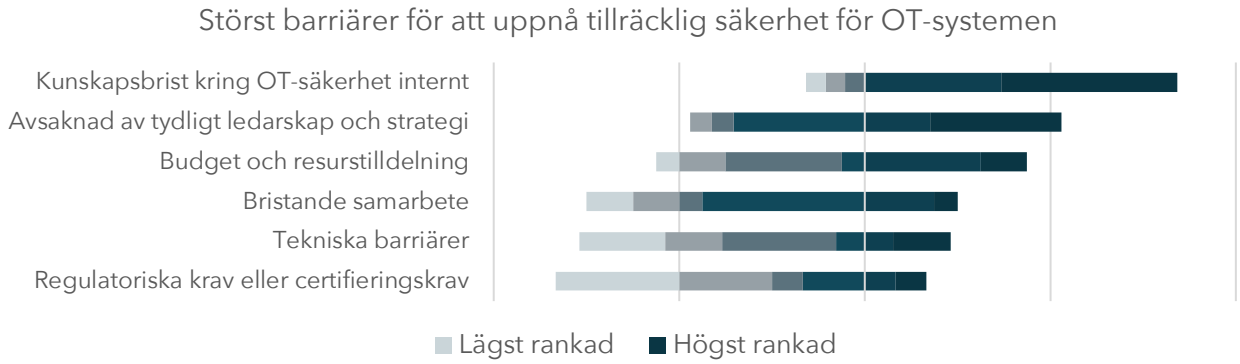


Figur 3. Olika rollers bedömning om huruvida verksamheten har OT eller inte

Att endast 40 procent av personerna utanför IT är medvetna om OT i verksamheten tyder på att det finns en betydande kunskapslucka utanför IT-avdelningen, borträknat OT-ansvariges domän. Det kan bero på att OT traditionellt har betraktats som en separat funktion, främst hanterad av ingenjörer och tekniker inom specifika operativa områden i linjeverksamheten snarare än av verksamhetsledning. Denna skillnad i medvetenhet kan innebära en potentiell risk då det kan vara svårt att få nödvändigt stöd och resurser från andra delar av organisationen för att säkra och optimera dessa system.

BARRIÄRER FÖR SÄKERHET I OT

När vi ser på de främsta hindren för att uppnå tillräcklig säkerhet i OT-system framträder flera kritiska problem. De mest betydande hindren är bristen på intern kunskap om OT-säkerhet, samt otillräcklig budget och resursallokering. Dessutom bidrar bristande samarbete, otydligt ledarskap och avsaknaden av en sammanhållen strategi till problemen med att säkerställa effektiv OT-säkerhet.



Figur 4. Största barriärerna för OT-säkerhet

KUNSKAPSBRIST

En av de största utmaningarna är bristen på kunskap inom organisationer om de specifika säkerhetsbehoven och hoten som är förknippade med OT-system. Till skillnad från IT-system, som ofta hanteras av experter inom cybersäkerhet, kräver OT-system specialiserad kunskap som kombinerar teknik och säkerhet. Denna kunskapslucka gör att OT-miljöer ofta är otillräckligt skyddade eftersom de ansvariga inte fullt ut förstår de unika utmaningarna med att säkra industriella styrsystem. Vid djupare resonemang uppges kunskapsbristen vara närvarande på olika sätt bland olika roller och funktioner, som alla behöver närma sig varandra för att få till ett effektivt säkerhetsarbete.

"Det är viktigt att höja kunskapsnivån på den faktiska ägaren. Tillgången ligger inte hos IT, utan där har verksamheten större beslutsmandat. Då måste vi jobba tillsammans för att hitta en bra lösning."

- Chief Information Officer (CIO)

BEGRÄNSAD BUDGET OCH RESURSER

En annan betydande begränsning är den otillräckliga budgeten och resursallokeringen. För att säkerställa robust säkerhet i OT-system krävs investeringar i avancerad säkerhetsteknik, kontinuerlig övervakning och regelbundna uppdateringar. Ofta förlitar sig OT på delade budgetar med IT, vilket kan leda till underfinansiering av nödvändiga säkerhetsåtgärder, vilket gör OT-systemen sårbara. Det finns en generell brist på experter inom säkerhet och inom OT-säkerhet i synnerhet. Många som arbetar med OT-system har stor teknisk kompetens inom sina områden men saknar specifik utbildning inom cybersäkerhet, vilket kan leda till sårbarheter.

BRISTANDE LEDARSKAP

Slutligen är avsaknaden av tydligt ledarskap och en sammanhållen strategi ett stort hinder för OT-säkerhet. Ledarskap är avgörande för att sätta prioriteringar, fördela resurser och driva implementeringen av säkerhetspolicyer. I många organisationer är ansvaret för OT-säkerhet splittrat, utan en tydlig ansvarsfördelning. Detta leder till en fragmenterad och reaktiv säkerhetsstrategi istället för en strategisk och proaktiv metod. Ledningen behöver även ta ansvar för värdering av digitala risker.

"Säkerhet måste tas på allvar på högsta nivån i verksamheten, annars blir det inte bra samordnat. Om ingen tar ansvar för helheten så blir det stuprör. Att ledningen visar att de prioriterar säkerhet skickar signaler till resten av verksamheten. Då blir det viktigt för alla."

- Verkställande Direktör (VD)

OLIKA PRIORITERINGAR OCH TEKNISKA UTMANINGAR

OT-system har traditionellt designats med primärt fokus på att säkerställa hög tillgänglighet och prestanda, där cybersäkerhet varit sekundärt då dessa system har isolerats på egna nät. Det innebär att flera av de OT-system som nu kopplas upp saknar många av de säkerhetsåtgärder som vi ofta tar för givet i IT-miljöer. Detta kan leda till sårbarheter när säkerheten inte är inbyggd från början. De olika prioriteringarna och särskilda tekniska kraven kan även bidra till att förstärka de organisatoriska utmaningarna som framhävts, då de kräver såväl relevant kompetens som resurser och samarbete för att hanteras effektivt.

BRISTANDE VISIBILITET

Kombinationen av mycket äldre teknik, långa livscykler och stor variation av system och leverantörer gör bristande visibilitet och följaktligen övervakning (monitorering) till en stor utmaning. Utan att fullt ut veta vilka tillgångar och system som finns i verksamheten är det svårt att skydda dem. Givet den långa livslängden av vissa system så kan informationen vara svår att samla då den kan finnas i pärmar, och medarbetare som lämnar verksamheten kan göra att viktig kompetens går förlorad.

"IT-säkerheten är bättre än OT-säkerheten. Det finns mer omogen teknik, stor variationsrikedom, många olika standarder och olika leverantörer. Monitorering är den högsta barriären för säkerhet. Det är lättare inom IT, där har vi koll på alla tillgångar och kan se till att allting är uppdaterat. Inom OT kan vi inte garantera det på samma sätt."

- Chief Information Officer (CIO)

En bristande visibilitet kan leda till en bristande insikt om vilka sårbarheter verksamheten faktiskt möter. Andra studier visar på hur andelen som upplever sig ha full visibilitet över OT kan minska när mognadsgraden ökar[1]. Det kan helt enkelt vara så att en ökad mognad gör att verksamheten får en större förståelse för problemet och blir medveten om sina blinda fläckar. Utan visibilitet över alla OT-system kan kritiska sårbarheter förbli oupptäckta och nödvändiga uppdateringar eller patchar missas.

MER OMOGEN OCH ÄLDRE TEKNIK

Utmaningar med utdaterade system (legacy) kan förekomma både inom IT och OT, men är en tydligare utmaning inom OT på grund av bland annat längre livscykler, högre kostnader och risker vid uppgraderingar, samt kritiska säkerhets- och kompatibilitetsutmaningar. OT-miljöer kan dessutom vara beroende av infrastruktur som är dåligt anpassad för dagens komplexa säkerhetshot och som kan vara svår eller omöjlig att integrera med moderna säkerhetslösningar. Gamla OT-system kan exempelvis sakna stöd för kryptering, multifaktorautentisering eller avancerade detekteringsverktyg. Dessutom är dessa system ofta sammankopplade med andra OT-system för att öka effektiviteten och optimera processer. Sammankopplingen av olika system kan underlätta för angrepp att spridas över hela nätverket utan tillräcklig segmentering som kan begränsa angreppets räckvidd.

UTMANANDE ÅTKOMSTHANTERING

Det är vanligt att många olika individer och roller såsom operatörer, ingenjörer och underhållspersonal behöver ha tillgång till OT-systemen i sitt dagliga arbete. En bred tillgång med många konton och användare kan innebära en sårbarhet för säkerhetshot om det inte hanteras på ett bra sätt. Utmaningen förstärks av användningen av standardlösenord, bristande autentisering och otillräcklig övervakning.

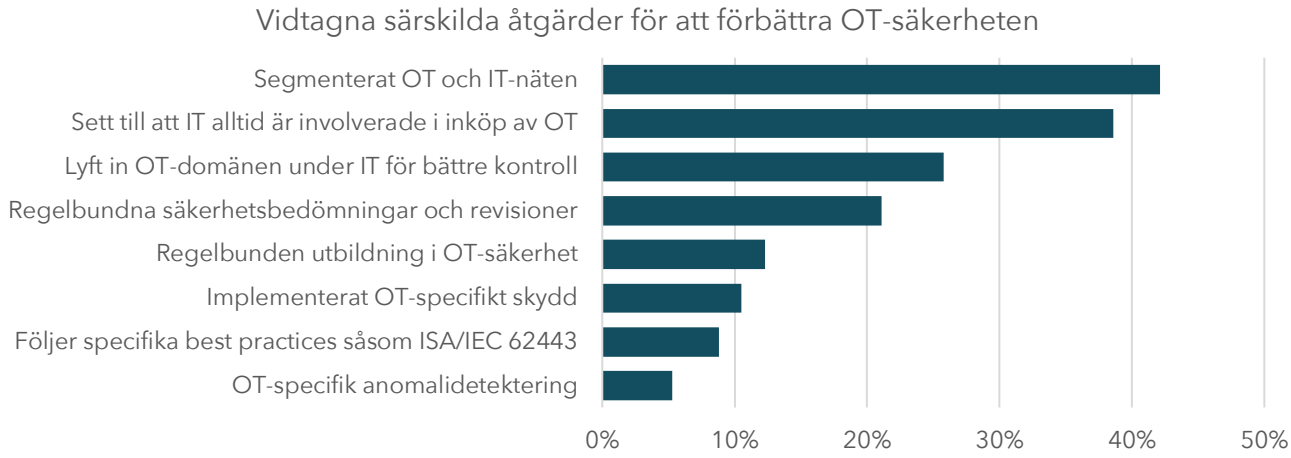
"Vi måste förflytta både kunskap och attityder. Man kommer inte kunna göra det man alltid har gjort. Säkerhet kostar, och det kan vara svårt att acceptera att det plötsligt blir dyrare. Saker som har varit lätta blir svårare för att det ska bli säkrare."

- Chief Information Officer (CIO)

VIKTIGT ATT ANVÄNDA RÄTT VERKTYG

IT-säkerhetsverktyg är ofta utformade med ett starkt fokus på dataskydd och integritet, vilket är kärnan i IT-säkerhet. OT-säkerhet, däremot, prioriterar robusthet och tillgänglighet för att säkerställa kontinuerlig drift av kritiska system. Verktyg som inte förstår eller tar hänsyn till OT:s operativa krav kan skapa konflikter, där säkerhetsåtgärder leder till oönskade driftsstopp eller störningar, vilket underminerar både säkerhet och effektivitet i OT-miljön. Att lösa säkerheten i OT-systemen enbart genom traditionella IT-verktyg blir helt enkelt fel verktyg för jobbet.

Till exempel behöver OT-system ofta skyddas mot hot som kommer från både fysiska och digitala källor, och de måste kunna övervakas och hanteras på sätt som är specifika för industriprocesser. Många IT-verktyg är inte utformade för att upptäcka eller hantera dessa typer av hot, vilket leder till att OT-system blir sårbara även när säkerhetsverktyg är implementerade. Många system är utmärkta för att övervaka IT-nätverk, men de är ofta inställda på att upptäcka hot som är vanliga i IT-miljöer, snarare än de specifika hot som OT-nätverk står inför. De kan också generera stora mängder falska positiva resultat i en OT-miljö, där trafikmönstren ofta är mycket olika de i ett traditionellt IT-nätverk. Detta kan leda till att viktiga varningar missas eller att systemadministratörer överväldigas av onödiga larm.



Figur 5. Vidtagna åtgärder för att förbättra OT-säkerheten

Att använda fel verktyg för att hantera OT-säkerhet innebär därmed stora risker. Verktyg som är utvecklade för IT-miljöer är ofta inte tillräckligt anpassade för de unika krav och utmaningar som finns inom OT. För att effektivt säkra OT-system behöver vi ofta investera i specialiserade säkerhetsverktyg som är designade eller anpassade för att hantera OT:s specifika behov, såsom realtidsstöd, kompatibilitet med äldre system, och en djup förståelse för de operativa krav som dessa system ställer. Utan sådana specialiserade verktyg riskerar organisationer att utsätta sina OT-miljöer för onödiga säkerhetsrisker och operativa störningar.

”Det gäller att hitta en bra balans mellan säkerhet och robusthet i systemen. Det är lätt att tänka att man ska implementera massa säkerhetsprodukter i ett system, men vilken nytta gör dem och hur många potentiella felkällor har vi introducerat. Det är många typiska IT-produkter som vill in i OT-branschen. Det gäller att hålla huvudet kallt när leverantörer ringer.”

- Automationsingenjör

Del 3

REGULATORISKA KRAV EN UTMANING OCH MÖJLIGHET

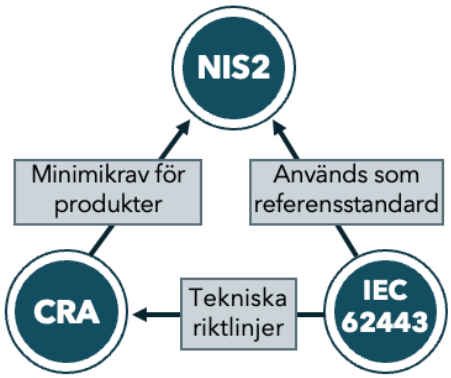
För att hantera det ökande cyberhotet och stärka den kollektiva motståndskraften introduceras nya regulatoriska krav. När nya krav och säkerhetsåtgärder ska implementeras är det kritiskt att bedöma de särskilda förutsättningar som finns för OT-systemen så att arbetet inte riskerar att förstärka befintliga utmaningar.

REGULATORISKA KRAV SOM PÅVERKAR OT

Vikten av ett stärkt och systematiskt säkerhetsarbete är en tydlig prioritering från EU som introducerar en rad nya cybersäkerhetsregleringar (se bilaga A för mer detaljer). Stort fokus i diskussionerna kring dessa regleringar har legat på IT-systemen och hur de ska skyddas, men för att uppnå en tillräcklig skyddsnivå är i många fall även OT-systemen en viktig del av arbetet för att kunna säkerställa ett skydd mot angrepp och störningar i verksamheten. Det är många sektorer och verksamheter som omfattas där man är ovan vid att jobba med denna typ av regleringar. Det kan även upplevas svårt att förstå hur olika regelverk hänger ihop.

NIS2, CRA, och IEC 62443 är ramverk och standarder som bidrar till att stärka cybersäkerheten, särskilt inom kritiska infrastrukturer och operativ teknik. De är kopplade genom sina mål att skydda digitala och industriella system från cyberhot, men de gör det genom olika tillvägagångssätt och i olika sammanhang.

- **NIS2** säkerställer att operatörer av samhällskritiska tjänster upprätthåller höga säkerhetsnivåer och rapporterar incidenter.
- **CRA** kompletterar genom att säkerställa att produkter med digitala komponenter som används i dessa sektorer är säkra från början.
- **IEC 62443** överbryggar klyftan genom att erbjuda tekniska standarder som gäller för OT-systemens specifika behov samt ger en gemensam terminologi och praxis.



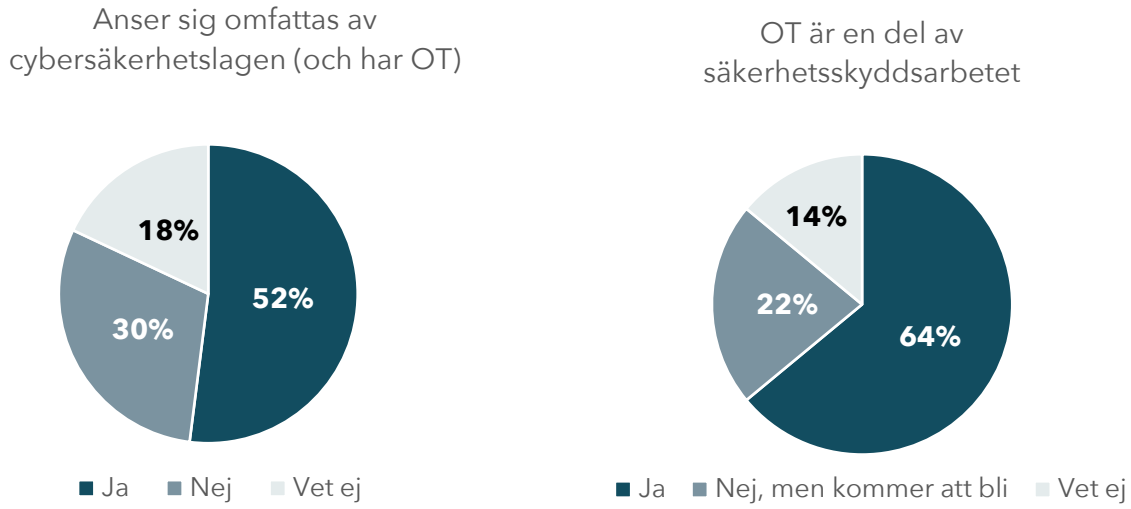
Genom att förstå relationen mellan olika regelverk eller standarder som är relevanta för er verksamhet så är det också möjligt att samordna arbetet runt riskanalys och kravställning bättre. Bygg en förmåga att hantera regelverk på ett strukturerat och systematisk sätt snarare än att hantera det i silos. Annars riskerar samma system eller process att mötas av olika kravställningar baserade på olika riskperspektiv från olika delar av verksamheten som blir svåra att hantera, eller till och med står i konflikt till varandra. Många verksamheter har dessutom erfarenheter av att implementera andra regulatoriska ramverk och kan då bygga på det arbetet snarare än att ”uppfinna hjulet” gång på gång.

	Syfte	Relation
NIS2	Att säkerställa att sektorer som energi, transport och hälso- och sjukvård har robusta cybersäkerhetsåtgärder på plats.	NIS2-direktivet kräver att organisationer implementerar säkerhetsåtgärder som ofta kan referera till standarder som IEC 62443 för att säkerställa att deras OT-system är tillräckligt skyddade. CRA stödjer NIS2 genom att rikta sig till cybersäkerheten för produkter med digitala element som också kan påverka nätverkssäkerheten.
CRA	Att säkerställa att produkter som säljs i Europa är säkra och uppfyller minimala säkerhetskrav.	CRA kompletterar NIS2 genom att fokusera på säkerheten för produkter som kan utgöra en risk för nätverks- och informationssystem inom NIS2 tillämpningsområde. Standarder som IEC 62443 kan tillämpas för att säkerställa att industriella produkter som omfattas av CRA också är skyddade mot cyberhot.
IEC 62443	Att ge riktlinjer för att utveckla säkerhetsprogram för OT-miljöer och skydda industriella system mot cyberattacker.	IEC 62443 ger detaljerade tekniska och organisatoriska riktlinjer som kan användas av organisationer för att uppfylla kraven i både NIS2 och CRA. När verksamheter implementerar IEC 62443-standarder säkerställer de att deras OT-system uppfyller de höga säkerhetskrav som ställs enligt NIS2-direktivet och de kommande kraven i CRA.

OT SOM EN DEL AV ARBETET MED DEN NYA CYBERSÄKERHETSLAGEN

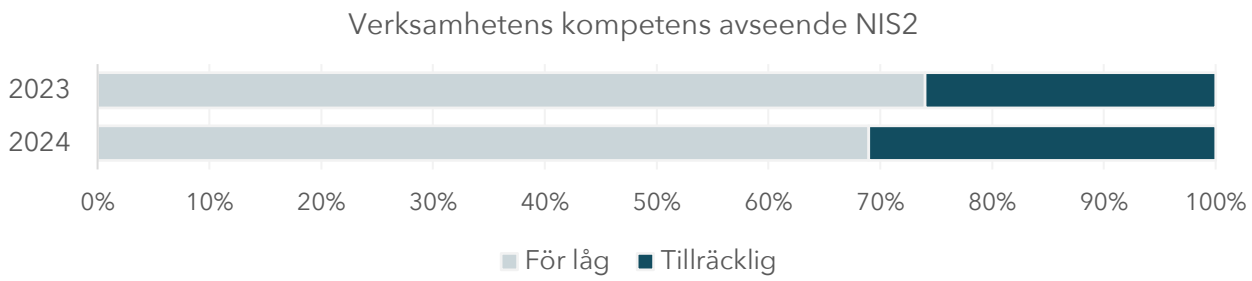
Den nya lagen om cybersäkerhet är den svenska tillämpningen av NIS2-direktivet, medan CER-direktivet regleras i lagen om motståndskraft hos kritiska verksamhetsutövare. De är båda relevanta utifrån ett OT-perspektiv. De handlar i slutändan om att stärka verksamheters motståndskraft genom att både skydda mot incidenter men även stärka förmågan att hantera dem när de väl inträffar.

NIS2 fokuserar på säkerhet i nätverk och informationssystem och handlar om att stärka verksamheters motståndskraft genom att hantera risker kopplade till cybersäkerhet. CER kompletterar NIS2 genom att fokusera på kontinuitet inom samhällsviktig verksamhet även kopplat till andra typer av potentiella störningar eller avbrott såsom olyckor, naturkatastrofer eller sabotage. Men när vi pratar om digitala risker och hot om cyberattacker mot OT är det alltså framförallt NIS2 som tar fasta på detta och ställer krav på verksamheter att skärpa sitt cybersäkerhetsarbete.



Figur 6. Verksamheter med OT som omfattas av lagen om cybersäkerhet, och Figur 7. Andel av dessa som inkluderat OT i arbetet

Tidigare analyser har visat att det finns en stor osäkerhet runt om verksamheten omfattas av NIS2 (lagen om cybersäkerhet) eller inte. Andelen som förstår att de behöver implementera de nya reglerna ökar över tid, men det har satt oss i ett läge där vi ligger efter och många verksamheter kämpar nu för att hinna klart i tid tills lagen börjar gälla. I denna studie är det en majoritet av verksamheterna med OT som uppger att man träffas av den nya lagen, och en majoritet av dessa som också inkluderat OT i säkerhetsarbetet. Bland de som menar att man inte omfattas hittar vi dock verksamheter inom såväl tillverkningsindustri, offentlig sektor och transportsektorn, så det finns en möjlighet att det även här råder en underskattning av lagens tillämpningsområde. Otydligheter kring vilka som omfattas, en upplevelse av otillräcklig kompetens om NIS2 och en tidsram som minskar varje dag sätter verksamheter i ett utmanande läge.



Figur 8. Bedömning av verksamhetens kompetens runt NIS2. Besvarat under hösten 2023 och våren 2024

De riskhanteringsåtgärder som ska tillämpas ska vara tekniska, driftsrelaterade och organisatoriska och utgå ifrån en riskanalys[5]. I en ansats att snabbt komma upp på banan så är det en del verksamheter som letar efter tekniska lösningar, men enbart ny teknik kommer inte att räcka för att efterleva kraven. Många sneglar även på varandra eller inväntar tydligare besked från myndigheterna, men verksamhetens handlingsplan måste utgå ifrån en egen riskanalys. Vissa riskhanteringsåtgärder som specificeras i den nya lagen om cybersäkerhet måste bedömas utifrån ett OT-perspektiv för att förstå hur de kan tillämpas.

"Jämför man i direktivet och förslaget som har kommit så har man tagit bort ett viktigt ord – lämpliga. Säkerhetsåtgärderna ska vara proportionerliga mot risken och 'lämpliga'. Ordet lämpliga är jätteviktigt ur ett OT-sammanhang. Vi kan inte ta en IT-lösning och köra på med, det är helt andra förutsättningar. Tillsynsmyndigheternas riktlinjer måste komma ikapp."

- OT-säkerhetsexpert

Den allmänt dåliga beredskapen för den nya lagen riskerar att förstärka befintliga utmaningar i verksamheten runt cybersäkerhet i IT och OT-systemen och bli en möjlig konfliktyta.

- Att implementera säkerhetsåtgärder i OT-miljöer är komplext och kan ta tid. Om tidsramen för att efterleva kraven minskat på grund av att verksamheter avvaktat eller varit omedvetna om att man omfattas riskerar det stressiga läget att leda till utmaningar och jobbiga diskussioner.
- Låg kunskap om NIS2 och även kring cybersäkerhet för OT internt gör det svårt att tolka och förstå kraven utifrån OT:s särskilda förutsättningar och krav. Det finns en risk att man försöker implementera åtgärder på OT-system som kan vara opassande eller rent skadliga.
- De hinder som uppgetts för att nå en högre cybersäkerhet inom OT (kunskapsbrist, brist på budget och resurser, bristande samarbete och avsaknad av ledarskap och strategier) riskerar att förstärkas i ett pressat läge där man försöker springa ikapp arbetet med att efterleva NIS2.
- För de som ligger efter med NIS2-arbetet kan det innebära att man behöver prioritera om eller allokera om budget och resurser från annat för att efterleva kraven. Vilket kan innebära att andra planerade investeringar eller projekt kan behöva stå tillbaka.

UTGÅ IFRÅN RISKANALYSEN
Olika verksamheter har olika förutsättningar, miljöer, sårbarheter, och så vidare. Därför kan man inte bara kolla hur andra gör eller följa generiska checklistor. Ni måste göra jobbet själva. Riskanalysen utgör grunden för er handlingsplan. Identifiera och bedöm era risker för att sedan definiera de säkerhetsåtgärder som är *proportionerliga* och *lämpliga*

Del 4

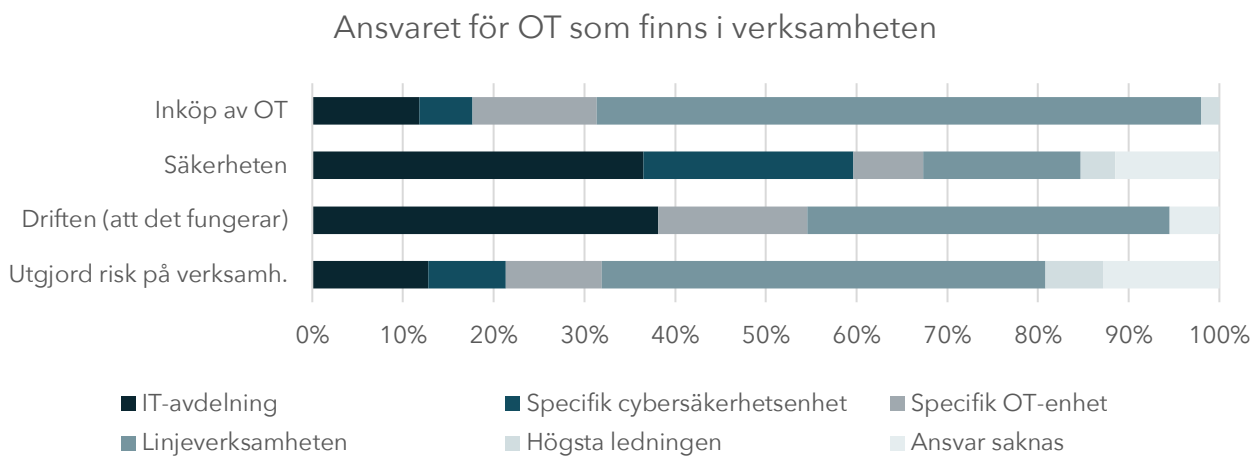
ANSVAR, SAMARBETE OCH LEDARSKAP

Mycket av utmaningarna med OT-säkerhet är kopplade till organisatoriska faktorer. I denna del tittar vi närmre på vad som bidrar till att skapa de utmaningarna och som behöver hanteras för att överkomma dem. Det handlar mycket om ansvarsfrågan, hur samarbetet runt OT ser ut och vilken roll ledning och styrelse behöver ta.

ANSVARET FÖR OT ÄR DELAT

Vår undersökning visar att ansvaret för olika aktiviteter rörande OT är uppdelat. Mycket av ansvaret faller på IT-avdelningen, med ett tydligt undantag för OT-relaterade inköp vilka utförs av linjeverksamheten. Som tidigare nämnts är säkerhet en av de största utmaningarna som OT nu står inför, vilket är ett ansvar som tydligt faller på IT-avdelningen. Detta indikerar att organisationer tenderar att centralisera säkerhetsfrågorna inom IT, vilket är rimligt med tanke på den ökade digitaliseringen och de cyberhot som riktas mot både IT och OT. IT-avdelningen har den expertis som krävs för att hantera komplexa säkerhetsutmaningar, särskilt i cyberdomänen, vilket förklarar deras ledande roll i detta avseende.

Detta beroende till IT-avdelningen kan till viss del förklaras av att OT inte alltid har en egen budget, utan den är ofta delad mellan IT och produktionsbudgeten. Denna brist på en dedikerad OT-budget och beroendet av andra avdelningsmedel gör OT-utmaningar svåra att hantera, eftersom prioriteringarna för IT och produktionsverksamhet kan skilja sig åt och kräver ett effektivt samarbete mellan flera olika parter och delar av organisationen.



Figur 9. Ansvar för OT i verksamheten

Linjeverksamheten ansvarar huvudsakligen för driften av OT-system samt för inköpen. Detta reflekterar ett traditionellt synsätt där de som är närmast den dagliga verksamheten bäst förstår de operativa behoven och därmed tar ansvar för att säkerställa att utrustningen fungerar som den ska. Att linjeverksamheten hanterar både inköp och drift visar att organisationerna fortfarande förlitar sig på specialistkunskaper inom sina produktionsavdelningar för dessa uppgifter. Specifika OT-enheter och cybersäkerhetsenheter tar på sig viktiga, men sekundära roller i drift och säkerhet. Det indikerar att vissa organisationer har valt att skapa dedikerade team eller enheter för att hantera de unika utmaningar som OT medför. Dessa enheter fungerar som experter inom sina områden för att säkerställa att OT-systemen inte bara är säkra, utan också optimerade för verksamheten.

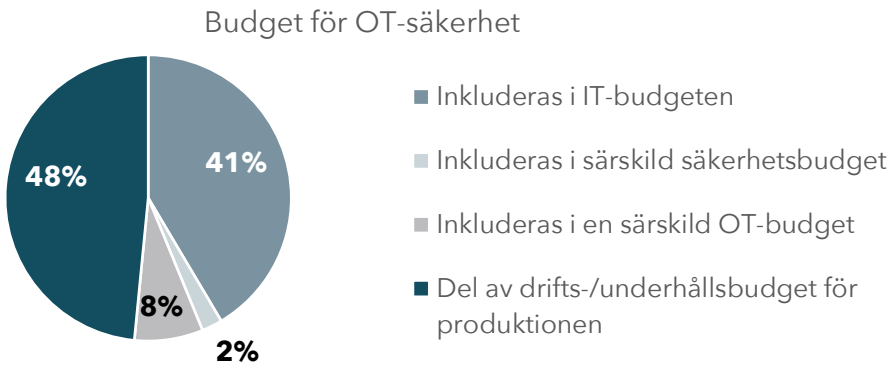
”Vi vill att produktionen ska höra av sig till oss innan de investerar i OT, men det händer inte alltid. Vi blir kontaktade efteråt när de vill ha hjälp med anslutning och då är det för sent. Problemet är att OT-investeringar är så dyra, så då får vi försöka få det att fungera”.

- Chief Information Security Officer (CISO)

Tillgängliga data pekar på att det finns en viss grad av otydlighet eller brist på ansvar i vissa områden, vilket kan indikera att vissa organisationer fortfarande kämpar med att fullt ut definiera vem som ansvarar för specifika aspekter av OT. Detta kan leda till ineffektivitet eller förhöjda risker om inte roller och ansvar klargörs och fördelas tydligt i verksamheten. När inköpsbeslut, budget, driftsansvar och säkerhetsansvar är fördelat mellan olika funktioner krävs samarbete och tydlig kommunikation.

VEM BETALAR FÖR OT-SÄKERHETEN?

Traditionellt sett har OT-system hanterats som en del av produktionens infrastruktur, vilket innebär att säkerheten kring dessa system ofta ses som en naturlig del av det dagliga underhållet och driften. Eftersom OT-system ofta är nära kopplade till maskiner och produktionsutrustning, kan det vara logiskt att säkerhetsbudgeten för dessa system inkluderas i drifts- och underhållsbudgeten för att kunna ta hänsyn till säkerhetsåtgärder när det gäller underhåll och reparationer. Det är också här vi återfinner den största andelen av OT-säkerhetsbudgeten, 48 procent. Detta innebär att säkerheten i många organisationer ses som en del av det dagliga underhållet av produktionsutrustningen. Det kan indikera att OT-säkerhet i dessa organisationer integreras direkt med den fysiska infrastrukturen, där underhåll och säkerhet behandlas som sammanflätade processer.



Figur 10. Fördelning av budget för OT-säkerhet

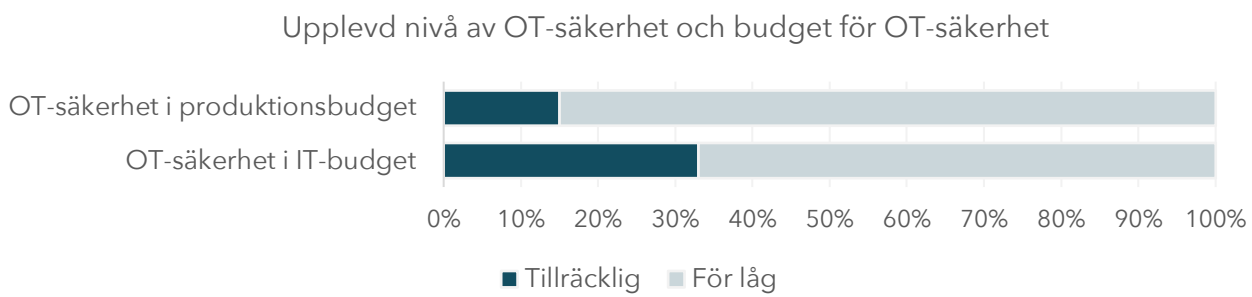
41 procent av verksamheter har OT-säkerhetsbudgeten inkluderad i IT-budgeten. Detta tyder på en ökad integration mellan IT och OT, där IT-avdelningen har ansvar för att hantera säkerheten för OT-systemen. Det kan såklart bero på vilka typer av system det gäller, men det speglar den moderna trenden att sammanföra IT- och OT-säkerhet under en gemensam paraplystrategi för att bättre kunna hantera hot som påverkar hela organisationen, vilket idag till stor del är cyberhot.

En mindre andel, 8 procent, av verksamheterna har specifikt avsatt medel inom en särskild OT-budget. Detta kan indikera att vissa organisationer har särskilda behov eller utmaningar som kräver att OT-säkerhet hanteras separat från andra budgetar. Det kan också tyda på en önskan att hålla OT-säkerheten isolerad från IT-budgeten för att säkerställa dedikerade resurser till dessa system.

BUDGET OCH ANSVARSFÖRDELNING

Hur organisationer strukturerar sina budgetar kan också återspegla interna ansvarsfördelningar. I vissa fall kan OT-säkerhet administreras av drift- och underhållsteam, vilket förklarar varför den största delen av budgeten hamnar där. I andra organisationer kan IT-avdelningen ha övertagit ansvaret för OT-säkerhet, varpå budgeten ligger under IT. Denna uppdelning kan vara resultatet av organisatoriska beslut om var ansvaret för OT-säkerhet bäst hanteras för att säkerställa effektivitet och säkerhet.

Utmaningar kan uppstå oavsett om budgeten för OT-säkerhet finns inom IT-budgeten eller drifts- och underhållsbudgeten. IT-budgetar behöver ofta täcka ett brett spektrum av behov, från uppdateringar av infrastruktur till licenskostnader och cybersäkerhet. När OT-säkerhet ingår i denna redan ansträngda budget kanske den inte får de medel som behövs för att fullt ut kunna åtgärda sårbarheter på ett adekvat sätt. På liknande sätt kan produktionsbudgeten vara fokuserad på att underhålla och optimera fysiska processer, vilket lämnar lite utrymme för att investera i avancerade cybersäkerhetsåtgärder, särskilt om säkerhet är underordnat andra prioriteringar.



Figur 11. Upplevd OT-säkerhet kombinerat med budgettillhörighet för OT-säkerhet

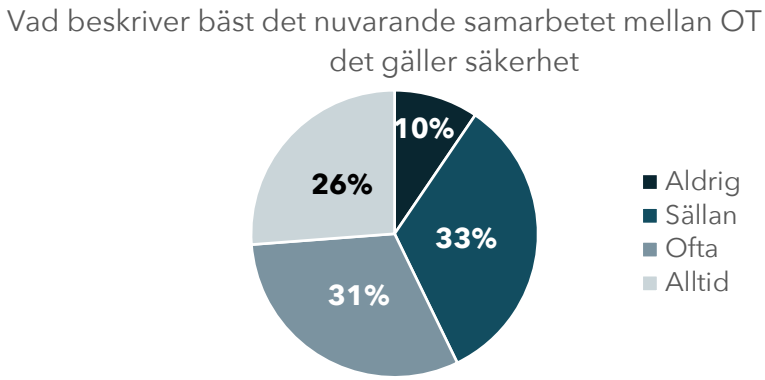
En vidare analys av de organisationer som deltagit i studien visar att de som inkluderat OT-säkerheten i IT-budgeten upplever en högre nivå av cybersäkerhet för OT-system än de som har OT-säkerhet inom drifts- och underhållsbudgeten. De organisationer som inkluderar OT-säkerhet i IT-budgeten uppger samtidigt en större ansvarsfördelning mellan IT-avdelningen och linjeverksamheten inom såväl inköp, säkerhet och riskhantering samt en högre grad av samarbete. När OT-säkerheten är en del av drifts- och underhållsbudgeten tycks området i sin helhet hanteras mer separerat från IT. Det skulle kunna innebära en säkerhetsutmaning när vi i högre grad sammankopplar IT- och OT-system och behöver ha en helhetsbild över de cyberhot och sårbarheter som hotar dessa för att kunna utforma lämpliga skyddsåtgärder. Oavsett var budgeten för OT-säkerhet återfinns behöver IT- och OT-teamen få till ett samarbete inom säkerhetsdomänen för att förena sina olika perspektiv, prioriteringar och kompetenser.

SAMVERKA RUNT INKÖP

Låt exempelvis större investeringar passera genom samverkansforum med representanter från olika funktioner i verksamheten. Där IT kan säkerställa bland annat kompatibilitet med arkitektur och att säkerhetskrav efterlevs. Inköpsprocessen är en central process att få till samarbete inom. Hänger inte kravställning från IT och OT ihop kan det uppstå problem senare i ledet som kan vara både komplext och kostsamt att försöka lösa, både driftsmässigt och säkerhetsmässigt.

SAMARBETE EN NYCKEL TILL HÖGRE OT-SÄKERHET

Samarbetet mellan OT och IT varierar kraftigt mellan organisationer. De två största kategorierna är "sällan" och "ofta", vilket visar att det finns en splittrad bild när det gäller samarbete mellan OT och IT inom säkerhet. En del av organisationerna verkar ha ett relativt frekvent samarbete, medan andra bara samarbetar sporadiskt. Denna delade bild kan bero på olika faktorer såsom organisatoriska strukturer, prioriteringar eller kanske bristande kommunikation och samordning mellan avdelningarna.

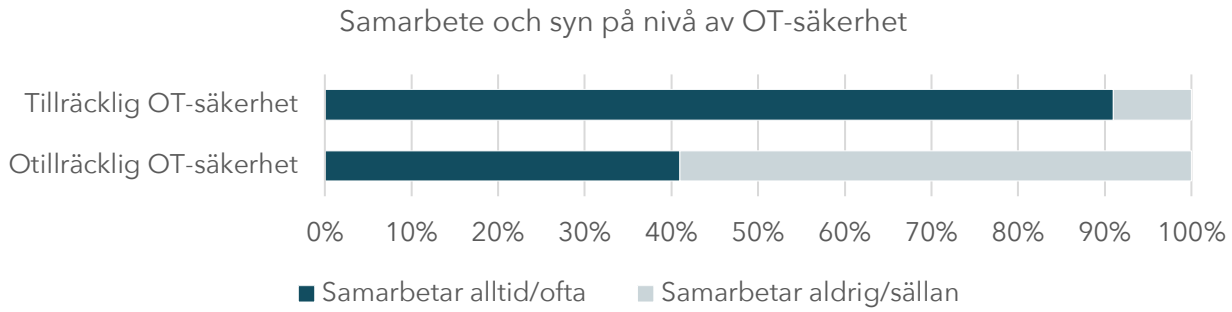


Figur 12. IT- och OT-enheters samarbete runt cybersäkerhet

Det är dock oroande att mer än en tredjedel av organisationerna rapporterar att samarbete sker "sällan" eller "aldrig", vilket indikerar brist på samordning och potentiellt säkerhetsrisker. Samtidigt är det uppmuntrande att en majoritet av organisationerna uppger att de "ofta" eller "alltid" samarbetar, vilket är ett steg i rätt riktning för att säkerställa en stark och integrerad säkerhetsstrategi.

"Det finns en brist på ödmjukhet från båda håll. Man vill inte dela med sig eller lära sig. Man förstår sitt område, men har dålig förståelse för att det är andra förutsättningar på andra sidan."

- OT-säkerhetsexpert



Figur 13. Relation mellan upplevd OT-säkerhet och frekvens av samarbete

En djupare analys påvisar ett tydligt samband mellan graden av förtroende för säkerhetsnivån i OT-system och samarbete mellan IT- och OT-avdelningarna. De som upplever sig ha en tillräckligt hög nivå av OT-säkerhet uppger samtidigt att de samarbetar ofta eller alltid runt säkerhetsfrågor. De som å andra sidan menar att deras säkerhetsnivå är otillräcklig uppger samtidigt en betydligt lägre grad av samarbete. Detta skulle kunna indikera att en högre grad av samarbete mellan IT och OT-enheterna leder till en förbättrad säkerhet, men även att ett högre förtroende för OT-säkerheten bidrar till en närmare integrerad och samarbetsvillig arbetsmiljö mellan dessa kritiska avdelningar.

"Samarbete mellan IT och OT är en nyckelfaktor. Det går inte att hålla isär."

- Chief Information Officer (CIO)

LEDARSKAP NÖDVÄNDIGT FÖR ATT HANTERA UTMANINGARNA

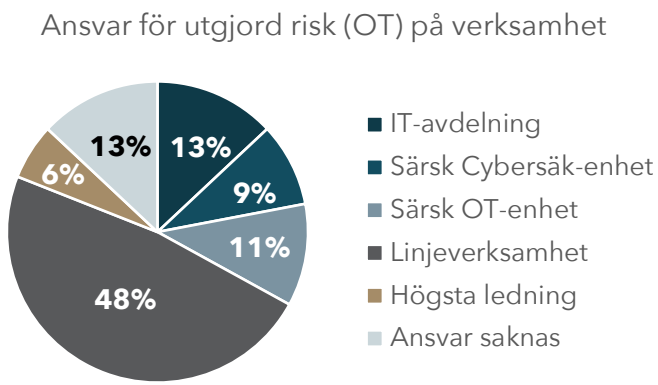
Flera av de utmaningar som nämnts; bristande samarbete, svårigheter att balansera prioriteringar, otydliga roller och ansvar, kompetens- och resursbrist, är alla områden med en tydlig koppling till behovet av ledarskap. I avsaknad av en sammanhållen strategi blir det upp till de olika funktionerna att själva försöka enas kring olika prioriteringar, vilket kan leda till jobbiga diskussioner och försämrade relationer. Utan ett ledarskap som tar ansvar för helheten riskerar arbetet att bli splittrat och ineffektivt.

Respondenterna i denna studie uttrycker att ledning och styrelse ofta har en insikt om att cybersäkerhet är viktigt, men saknar kunskap för att faktiskt kunna hantera frågan, och där styrelsen befinner sig ännu längre bort än ledningen. Vanligt är ett passivt förhållningssätt, där man förlitar sig på att IT-ansvariga gör bedömningar och rapporterar uppåt. Styrelsen har ett ansvar att övervaka och bedöma verksamhetsrisker, där digitala risker är en viktig del. Ledning är å andra sidan ansvariga för de strategiska insatser som krävs för att hantera denna risk och styra verksamheten mot gemensamma mål. Ledning och styrelse måste ta sitt ansvar och visa för verksamheten att säkerhet är prioriterat.

"Det är viktigt att ledningen tar sitt ansvar. Annars tvingas medarbetare längre ner i organisationen ta ansvar för beslut som de inte borde behöva fatta. Cybersäkerhet och verksamhetens risk är i grund och botten en lednings- och styrelsefråga."

- Verkställande Direktör (VD)

Vad gäller ansvaret för risker kopplade till OT-säkerhet är det tydligt att den högsta ledningen inte tar ett tillräckligt stort ansvar. Mycket av ansvaret faller på verksamheten själva som har den tekniska och operativa förståelsen för tillgångarna. Verksamhetens riskaptit är dock inte något som linjeverksamheten eller IT-avdelningen själva bör besluta om utan måste bedömas tillsammans med andra verksamhetsrisker i de styrande instanserna. Oroväckande är att många verksamheter dessutom tycks sakna en funktion som tar ansvar för denna affärskritiska fråga.



Figur 14. Ansvar över OT: Utgjord risk på verksamheten

För att cybersäkerhetsarbetet runt IT och OT ska bli bra samordnat krävs dels en övergripande strategi, men även att ledningen jobbar med styrning på rätt parametrar. Det som ledningen väljer att mäta och styra påverkar prioriteringar och arbetssätt i verksamhetsleden. Om den centrala ledningen formulerar mätvärden som är fokuserade på effektivitet i produktionen till en låg kostnad, och inte inkluderar risk eller säkerhet så är det naturligt att det påverkar hur verksamheten prioriterar sin budget och sina insatser. Om ledningen dessutom saknar förståelse för de OT-specifika förutsättningarna och upprättar mål och mätvärden som fungerar dåligt i praktiken kan detta skapa frustration och påverka förtroendet för verksamhetens ledning negativt.

SKAPA FÖRSTÅELSE FÖR DIGITALA RISKER

Styrelse och ledning måste ta ansvar för risk och riskhanteringsåtgärder, men IT- och OT-enheterna behöver även stötta och underlätta detta genom att inte basera riskdiskussioner på ett alltför tekniskt perspektiv utan tydligt koppla det till verksamheten. Det är viktigt att prata samma språk.

Ett tips kan vara att jobba med scenarion. Koppla hotbild till verksamheten och beskriv möjliga konsekvenser. Kvantifiera risker om möjligt och försök att hitta ett sätt att göra IT- och OT-risker jämförbara så att de kan hanteras ihop, och även värderas mot andra verksamhetsrisker.

ORGANISERING SOM HINDRAR ELLER STÖTTAR SAMARBETE

En stor utmaning för många verksamheter är balansen mellan en centraliserad styrning av IT och OT, och att samtidigt bibehålla ägarskap och ansvar för säkerheten ute i verksamheten. För att kunna arbeta med risk och säkerhet så är det kritiskt att krav och rutiner faktiskt funkar i den praktiska verkligheten. IT och OT har olika krav, processer, styrning och kräver olika kompetenser. Därför är det viktigt att de som förstår behoven, har mandaten att påverka och "pratar samma språk" också tar ansvar för säkerheten, men att det är samordnat under en övergripande strategi.

"IT är inte samma sak som OT. Det kräver andra kompetenser, teknik, processer, styrning, och så vidare. Man kan vara duktig på IT, men man kan inte tillgodogöra sig det inom OT riktigt, det är helt olika aspekter och prioriteringar. Inom OT så behöver vi jobba med cybersäkerhet på ett annat sätt så det inte påverkar tillgängligheten."

- IT-säkerhetschef

När IT och OT som tekniska domäner blir närmare sammankopplade blir det nödvändigt att integrationen även sker på det organisatoriska planet. De flesta respondenter är överens om att det är positivt att lägga ansvaret för OT-säkerhet under IT, men att bara samla ansvaret under en central stab är inte hela lösningen. Den som ansvarar över helheten måste ha en djup förståelse för verksamheten och stötta enheterna att röra sig i samma riktning. Det kan vara en utmaning i en IT-avdelning som befinner sig långt ifrån produktionen. Därför betonas vikten av att kombinera en central styrning med ett decentraliserat ansvar. Där man exempelvis kombinerar en central och sammanhållande IT-avdelning med lokala produktionsnära IT-enheter, eller cybersäkerhetsteam inom produktionen som kan etablera instruktioner och ramverk utifrån centrala mål och mätvärden.

ORGANISERINGEN AV IT KAN PÅVERKA

Den industriella utvecklingen inom IT har lett till en förflyttning från stora egna IT-avdelningar och egenproduktion till att alltmer organisera IT-avdelningen som en beställarorganisation. Industrialiseringen har lett till en ökad standardisering där IT i allt högre grad konsumeras som tjänst. Att outsourca IT har historiskt skapat stora effektivitets- och kostnadsvinningar. Baksidan av denna utveckling är att verksamheten tappat kontroll över sin egen miljö, det går inte lika snabbt och flexibelt att genomföra ändringar och verksamheten tappar egen teknisk (operativ) kompetens. Outsourcing av IT har lett till att vi måste hantera en mer komplex leverantörskedja. Denna fragmentering kan skapa utmaningar när det gäller att upprätthålla vår kontinuitet och säkerhet.

Denna utveckling och outsourcingtrend har inte sett likadan ut på OT-sidan där den ofta betydligt mer varierade och verksamhetsnära tekniken fortsatt har krävt en operativ förmåga i egen verksamhet för att jobba med den. I flera producerande verksamheter utgör OT dessutom en kritisk del av kärnverksamheten och det har varit nödvändigt att behålla en högre grad av kontroll över den operativa teknik som utgör grunden för värdeskapandet.

"En tydlig skillnad är att IT går att utveckla och jobba med på ett bra sätt utan att nödvändigtvis förstå allting i verksamheten. På OT-sidan är det svårare för tekniken ÄR verksamheten. Det kan vara svårt att hantera bra om man sitter långt bort i en konsoliderad IT-avdelning."

- OT-säkerhetsexpert

Outsourcingen hos IT har påverkat OT, eftersom OT-system ofta integreras med IT-system för övervakning, analys och styrning. Industrialiseringen av IT har gjort det möjligt att snabbt integrera nya OT-lösningar som kan köras på standardiserad IT-infrastruktur, vilket minskat beroendet av att helt skräddarsy lösningar från grunden. Det är dock värt att fundera över hur organiseringen av IT-avdelningen och syftesförflyttningen från egenproduktion till beställarfunktion påverkar synen på och samarbetet med OT-team. Särskilt då ansvaret för OT-säkerheten gärna även förläggs på den som är ansvarig över IT. Problem uppstår framförallt om inte samordningen fungerar effektivt, vilket kan vara särskilt problematisk när outsourcade kompetensdomäner måste samverka effektivt.

Del 5

ETT BRANSCHPERSPEKTIV PÅ OT-SÄKERHET

Många verksamheter i olika branscher har ett starkt beroende av OT för att producera och leverera sina tjänster, och behöver därmed jobba med att uppnå en hög OT-säkerhet. Denna del tittar närmre på tre olika branscher där OT-säkerhet är särskilt relevant: hälso- och sjukvårdssektorn, tillverkningsindustrin, samt energisektorn. Var och en av dessa branscher har unika prioriteringar, utmaningar och krav när det gäller att skydda sina OT-miljöer.

BETYDELSEN AV STORLEK

Trots de unika krav och utmaningar som varje bransch står inför, så är det framförallt verksamhetens storlek som spelar en avgörande roll när det kommer till mognadsgraden inom OT-säkerhet. Större organisationer har ofta råd att anställa dedikerad personal för att stötta och driva säkerhetsarbetet framåt och tillgång till mer resurser för genomförande. I mindre organisationer, som en liten kommun, är resurserna mer begränsade och säkerhetsarbetet betydligt mer personberoende. Det är vanligt att vissa roller får axla ett brett ansvar och även inneha dubbla roller för att organisationens storlek gör det orealistiskt att bryta upp den i många olika enheter. Dessa mindre verksamheter har därmed tuffare förutsättningar för att hantera säkerheten på ett effektivt sätt.

Betydelsen av storlek blir också tydlig i ljuset av de centrala utmaningar som tidigare diskuterats. De största utmaningarna som har lyfts fram är i huvudsak organisatoriska, som brist på kompetens, samarbete och avsaknad av ledarskap och strategier. Det är rimligt att anta att dessa organisatoriska utmaningar påverkas av hur stor eller liten verksamheten är. Exempel på skillnader som framkommit mellan mindre (små och medelstora) och stora verksamheter är:

- I mindre verksamheter är säkerhetsbudgeten för OT i högre grad en del av IT-budgeten
- Större verksamheter gör en mer negativ uppskattning av sin OT-säkerhetsnivå, vilket troligen hör ihop med en mer komplex miljö, men även en större insikt om problemen
- I mindre verksamheter samarbetar man mer frekvent runt IT och OT och det är inte lika stor variation i ansvarsfördelning av olika aktiviteter
- Mindre verksamheter ligger efter med att integrera OT i arbetet med NIS2 (lagen om cybersäkerhet)
- Större verksamheter har en större vana vid att arbeta med regulatoriska krav och jobbar oftare med standarder som IEC 62443
- Större verksamheter har i högre grad tillämpat OT-specifika säkerhetsåtgärder

Flera av skillnaderna kan förklaras av olikheter i resurser och förutsättningar som följd av storlek. Att mindre verksamheter med färre resurser exempelvis har enklare att få till ett effektivt samarbete är naturligt, men där samarbetet inte nödvändigtvis löser hela problemet när det i högre grad saknas nödvändig kompetens, budget och andra resurser för att jobba med OT-säkerhet i praktiken.

> ***"Alla tar säkerhetsfrågan på allvar, men det är svårare för mindre verksamheter. Vi har helt olika förutsättningar men möter samma krav. Som en liten organisation är svårt hinna hålla oss patchade och uppdaterade och kunna agera på nya sårbarheter som dyker upp tillräckligt snabbt"***
>
> - Verkställande Direktör (VD)

BRANSCHANALYS

HÄLSO- OCH SJUKVÅRDSSEKTORN

Inom hälso- och sjukvårdssektorn används OT-system på flera kritiska områden för att förbättra både patientvård och operativ effektivitet. De styr till exempel medicinska apparater som respiratorer och patientövervakningssystem, automatiserar laboratorieinstrument som blodanalysatorer och kemiska analysmaskiner, samt hanterar byggnadsautomation för HVAC-system och belysning med mera.

MOGNADSGRAD

Trots den omfattande användningen av OT-system så är den generella mognadsnivån inom hälso- och sjukvården relativt låg, vilket kan tillskrivas bristande vana och kompetens kring att cybersäkerhetsfrågor. Dessutom är dessa organisationer ofta ekonomiskt pressade, vilket ytterligare försvårar möjligheten att prioritera och investera i säkerhetsåtgärder. Samtidigt har sektorn en relativt hög IT-säkerhetsmognad på grund av den kritiska patientdata som hanteras. Trots den höga säkerhetsnivån i IT-system är det viktigt att beakta hela säkerhetskedjan, inklusive OT-system. Annars finns risken att sårbarheter i OT-system underminerar den uppnådda säkerheten i IT-systemen. Sektorn är van vid stränga lagkrav, men inte lika bred vana vid att tänka och jobba med cybersäkerhet.

”Hälso- och sjukvårdssektorn har en viktig roll i totalförsvaret. Det finns många olika typer av OT-system inom vården förutom de rent medicintekniska. Som olika försörjningssystem som ska kunna hållas uppe vid krig eller kris. Det är tufft för vilken verksamhet som helst att klara”

- OT-säkerhetsexpert

UTMANINGAR OCH RISKER

Många system måste vara tillgängliga och pålitliga för kontinuerlig vård eftersom OT-system här ofta används för att driva livskritiska apparater som pacemakers och andra medicinska enheter. Samtidigt är säkerhet och integritet för patientdata är en annan viktig utmaning. Cyberattacker som riktar sig mot patientdata eller medicinsk utrustning kan få direkta konsekvenser för patienters hälsa och liv. Hälso- och sjukvårdssektorn är en av de mest utsatta för cyberattacker, både från aktörer som vill tjäna pengar men även för att störa och destabilisera samhället. En utmaning ligger i att samordna arbetet så det inte hanteras i silos och hjälpa verksamheten att jobba riskmedvetet i en ofta väldigt stressig och pressad miljö.

IT PÅVERKAN PÅ OT

Sektorn är starkt beroende av fortsatt digitalisering för att klara sitt uppdrag mot en åldrande befolkning. Samtidigt riskerar budgetbegränsningar att påverka styrning och prioritering av cybersäkerhet vilket kan leda till att digitalisering och säkerhetsarbetet går i otakt. Det är viktigt att implementera robusta säkerhetsåtgärder som funkar i det dagliga arbetet och gör det ”lätt att göra rätt” för personalen.

Regulatoriska direktiv i fokus

Patientdatalagen (2008:355)

Dataskyddsförordningen (GDPR)

NIS/NIS2/CER-direktivet
(Lag om cybersäkerhet)
(Lag om motståndskraft hos kritiska verksamhetsutövare)

Prioriteringar från IT 2024

1. Strategisk säkerhet och efterlevnad av regelverk
2. Styrning för att minska IT-kostnader
3. Effektiv styrning av IT-organisationen

Utmaningar från IT 2024

1. Digitalisering (förändra verksamhetsmodeller)
2. Införande av nya applikationer
3. Strategisk säkerhet och efterlevnad av regelverk

BRANSCHANALYS

TILLVERKNINGSINDUSTRIN

Inom tillverkningsindustrin används OT-system för den övergripande produktiviteten, såsom produktionslinjer, maskiner och automationssystem. OT omfattar allt från sensorer och styrsystem till robotar och industriella nätverk, som tillsammans möjliggör effektiv och exakt drift av tillverkningsprocesser.

MOGNADSGRAD

Trots omfattningen av automatiseringen är den generella säkerhetsmognaden inom tillverkningssektorn ofta ojämn och beror mycket på storlek. Företag kan sakna den nödvändiga erfarenheten av att hantera säkerhetsfrågor i samband med OT-system, och resursbegränsningar kan försvåra investeringar i nödvändiga säkerhetsåtgärder. I ett land som Sverige, där tillverkningsindustrin är betydande för vår ekonomi och en stor del av exporten, kan dessa cybersäkerhetshot utgöra risker för den nationella ekonomin.

"Hotet har ökat de senaste åren och det absolut största hotet är ransomware. Vi har inte så mycket information som vi är oroliga för ska läcka, men däremot att någon ska ta sig in och påverka vital produktionsutrustning."

- Chief Information Officer (CIO)

UTMANINGAR OCH RISKER

Integrationen av både nya och äldre system breddar attackytan och skapar sårbarheter som kan utnyttjas av skadliga aktörer. Tillverkningssektorn är ett attraktivt mål och en av de mest utsatta för cyberattacker[3]. Åldrande OT-infrastruktur är särskilt utsatt för ransomware-attacker, vilket kan leda till allvarliga produktionsstopp och stora ekonomiska förluster.

Till följd av sektorns strategiska betydelse kommer delar av den att påverkas av det nya NIS2-direktivet. Samtidigt är tillverkningsindustrin generellt sett mindre vana vid att arbeta med regulatoriska ramverk, såsom NIS2. Detta beror dels på att tillverkningssektorn traditionellt har fokuserat mer på produktionsoptimering och effektivitet. Därför kan övergången till att implementera och följa cybersäkerhetslagstiftningen innebära en utmaning för många företag inom branschen.

IT PÅVERKAN PÅ OT

Ett starkt fokus på digitalisering och automatisering innebär ett fortsatt närmande mellan IT och OT och följaktligen höga krav på säkerhet. För de verksamheter som träffas av cybersäkerhetslagen kommer det att krävas resurser i form av tid och pengar från IT-avdelningen för att efterleva de nya kraven, och diskussioner kan uppstå kring hur de ska implementeras på ett effektivt sätt i OT-miljön.

Regulatoriska direktiv i fokus

Säkerhetsskyddslagen (2018:585)

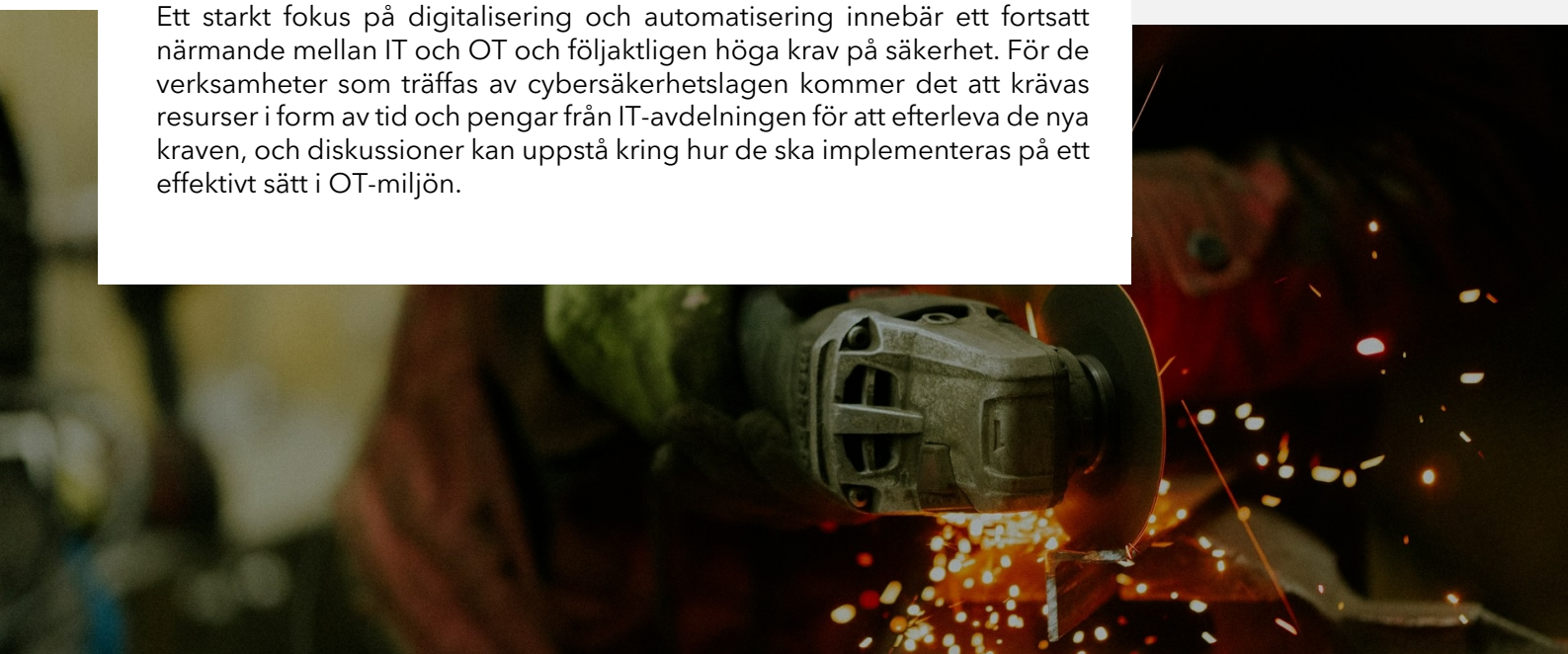
NIS2-direktivet (Lag om cybersäkerhet) *(Viss tillverkning)*

Prioriteringar från IT 2024

1. Strategisk säkerhet och efterlevnad av regelverk
2. Säkerhetsutbildningar och kunskapsöverföring
3. Automatisering för ökad effektivitet

Utmaningar från IT 2024

1. Förvaltning av befintliga applikationer
2. Effektiv styrning av IT-organisationen
3. Digitalisering (förändra verksamhetsmodeller)



BRANSCHANALYS
ENERGISEKTORN

Inom energisektorn används OT-system för att övervaka och styra kritiska infrastrukturer som elnät, kraftverk och energilagringssystem. Dessa system inkluderar sensorer, styrsystem och automatiseringsverktyg som säkerställer effektiv drift och stabilitet genom att reglera kraftproduktion, distribuera energi och hantera systemövervakning i realtid.

MOGNADSGRAD

Trots de utmaningar sektorn står inför, är den bland de mest mogna när det gäller säkerhet. Denna mognad kommer från sektorns strategiska betydelse, som länge inneburit tuffa krav inom säkerhet och gjort det till en prioriterad fråga. Energisektorn har även starka beroenden och sammankopplingar till andra verksamheter inom branschen och även till andra länder inom Norden och Europa vilket banat väg för samarbeten inom exempelvis säkerhetsområdet. Ett aktuellt exempel är nystartade EnergiCERT som ska stötta med att förebygga och hantera cyberincidenter.

"Vi kopplar ihop mer och mer vilket skapar nya hotvektorer och gör oss mer sårbara. Det skapar en ny typ av komplexitet. Men det är den vägen vi måste vandra för att lyckas med vårt uppdrag."

- IT-säkerhetschef

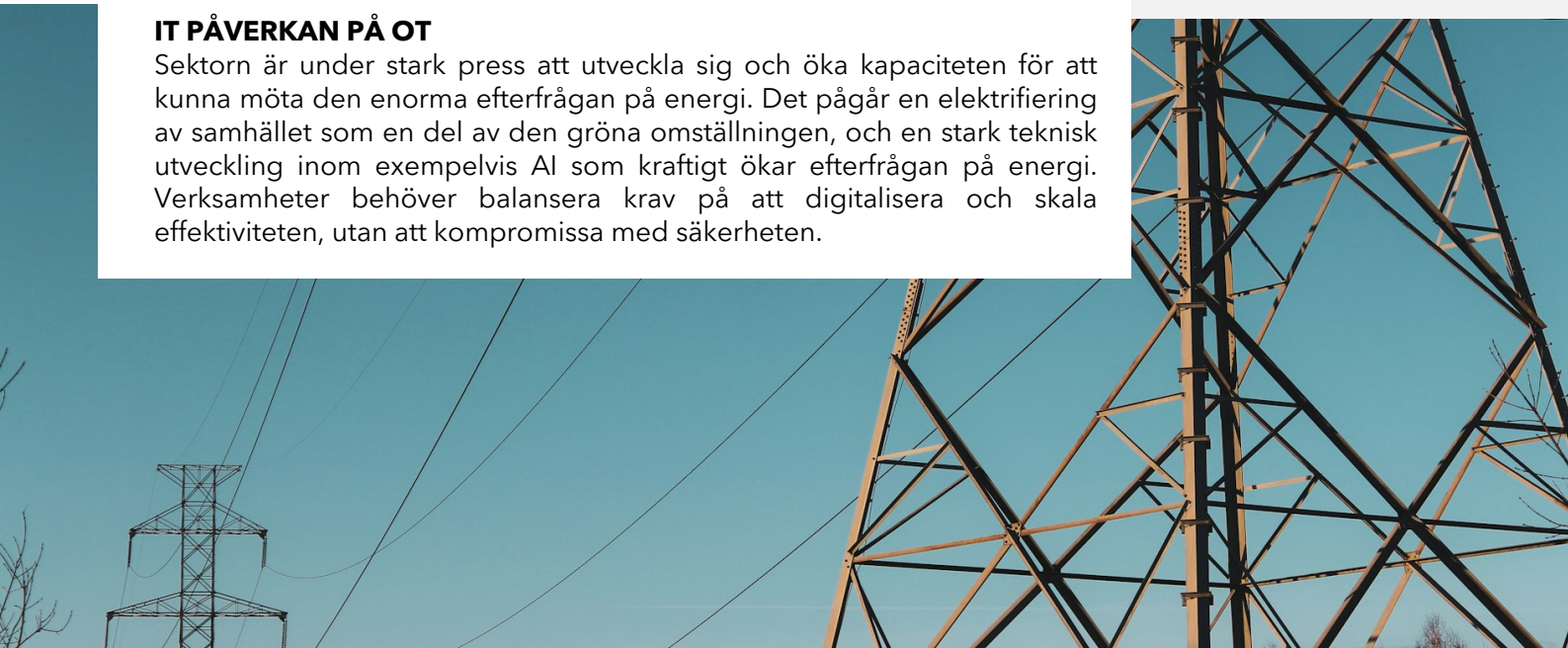
UTMANINGAR OCH RISKER

Kontinuitet och tillförlitlighet är av största vikt inom energisektorn, då denna sektor är grundläggande för nationell säkerhet. Cyberattacker mot SCADA-system, som styr och övervakar kritiska infrastrukturer, utgör en särskild risk eftersom dessa system är centrala för att upprätthålla stabiliteten i energinätet. Dessutom kan fysiska attacker kombineras med cyberangrepp för att maximera störningar och skada. Denna dubbla risk kräver omfattande säkerhetsåtgärder för att skydda mot både cyberhot och fysiska attacker, och för att säkerställa att energiförsörjningen förblir stabil.

Sektorns betydelse innebär en hög hotbild, där vi under det senaste året bland annat tagit del av larm om misstänkt kartläggning av energiinfrastruktur och elberedskap[6]. Från kriget i Ukraina ser vi hur energisektorn är under ständiga attacker från Ryssland vilket har förödande konsekvenser. Även NATO har genomfört övningar specifikt fokuserade på cyberhot mot förnybara energikällor som en reaktion på det växande hotet[8].

IT PÅVERKAN PÅ OT

Sektorn är under stark press att utveckla sig och öka kapaciteten för att kunna möta den enorma efterfrågan på energi. Det pågår en elektrifiering av samhället som en del av den gröna omställningen, och en stark teknisk utveckling inom exempelvis AI som kraftigt ökar efterfrågan på energi. Verksamheter behöver balansera krav på att digitalisera och skala effektiviteten, utan att kompromissa med säkerheten.



Regulatoriska direktiv i fokus

Ellagen (1997:857)

Säkerhetsskyddslagen (2018:585)

NIS/NIS2/CER-direktivet
(Lag om cybersäkerhet)
(Lag om motståndskraft hos kritiska verksamhetsutövare)

Prioriteringar från IT 2024

1. Strategisk säkerhet och efterlevnad av regelverk
2. Förvaltning av befintliga applikationer
3. Automatisering för ökad effektivitet

Utmaningar från IT 2024

1. Digitalisering (förändra verksamhetsmodeller)
2. Industrialisering och nyttja IT i större skala
3. Effektiv styrning av IT-organisationen

Del 6

REKOMMENDATIONER FÖR ATT STÄRKA OT-SÄKERHETEN

Från olika funktioner och roller inom olika verksamheter framgår det tydligt att en ökad förståelse och närmare samarbete är nödvändigt för att lyckas med säkerhetsarbetet. Nedan följer rekommendationer som syftar till att stötta en verksamhet som vill förbättra sin OT-säkerhet fördelat mellan mer tekniska och mer organisatoriska åtgärder. Se detta som inspiration och dra nytta av de rekommendationer eller åtgärder som är tillämpbara för er verksamhet.

KOSTNADSEFFEKTIVA ÅTGÄRDER

För den som känner att verksamhetens nivå av OT-säkerhet inte är tillräckligt hög så finns det ett antal säkerhetsåtgärder som ni kan tillämpa som ger god effekt, som generellt sett inte är alltför resurskrävande. De säkerhetsåtgärder ni väljer att implementera bör alltid grunda sig på er egen riskanalys, men kan exempelvis innefatta:

Område	Beskrivning
Nätverkssegmentering	Segmentera OT-nätverket från IT-nätverket och inom OT-miljön för att begränsa rörelse av hot och potentiella intrång i befintlig infrastruktur.
Använd befintliga verktyg för visibilitet	Utvidga användningen av befintliga IT-säkerhetsverktyg för att täcka OT-miljöer med OT-specifika moduler eller funktioner. Många övervakningsverktyg kan konfigureras för att fungera med befintlig infrastruktur, vilket ger förbättrad säkerhet utan stora nya investeringar.
Hotdetektering med anomalidetektering	Implementera maskininlärningsverktyg för att upptäcka avvikelser i OT-system och identifiera misstänkt aktivitet. Kräver färre resurser och minskar behovet av ständiga uppdateringar, vilket gör dessa verktyg mer kostnadseffektiva över tid.
Patchhantering	Implementera en robust patchhanteringsprocess för att regelbundet uppdatera och patcha OT-system, särskilt de som är exponerade för internet. Patchhantering är en lågkostnadsprocess som förhindrar många typer av attacker, vilket minskar behovet av dyrare åtgärder senare.
Zero Trust-modell	Implementera en Zero Trust-arkitektur där ingen enhet, användare eller system är betrodda som standard, även om de är inom nätverksperimetern. Kan implementeras gradvis med befintlig säkerhetsinfrastruktur, vilket minskar behovet av omfattande säkerhetsöversyner över tid.
Regelbunden medarbetarutbildning	Utbildning för grundläggande medvetenhet är en lågkostnadsinvestering som avsevärt minskar sannolikheten för mänskliga fel och säkerhetsincidenter.
Riskbedömningar och revisioner	Regelbundna riskbedömningar och revisioner fokuserar säkerhetsutgifter på de mest kritiska områdena, vilket undviker onödiga kostnader på mindre viktiga system.
Grundläggande IT-cyberhygien	Säkerställ att grundläggande cybersäkerhetshygien följs, inklusive policys, multifaktorautentisering och regelbundna säkerhetskopieringar av data. Dessa metoder kräver minimal investering men förhindrar många vanliga ingångar till cyberincidenter.

ORGANISATORISKA REKOMMENDATIONER

Under genomförandet av denna studie har det blivit tydligt att mycket av utmaningen med att öka cybersäkerheten inom OT-miljöer härrör från organisatoriska hinder. Bristande kommunikation och otydliga ansvarsområden kan leda till ineffektivitet, säkerhetsrisker och frustration.

Trots att det är utmanande finns det verksamheter som på olika sätt har försökt tackla dessa utmaningar och har goda exempel på aktiviteter som gett positiv effekt. Nedan följer en sammanställning av rekommendationer för olika delar av verksamheten; IT, OT och ledning, för att främja ett bättre samarbete och en förbättrad cybersäkerhet. Reflektera över grafiken för att identifiera och övervinna de interna hinder som hindrar verksamhetens framsteg. Genom att främja bättre samarbete mellan IT, OT och ledning kan vi inte bara förbättra vår operativa effektivitet utan också stärka motståndskraft mot cyberhot och bättre anpassa oss till framtida utmaningar.

	KOMPETENS	RISK	STRATEGI	ANSVAR
LEDNING/ STYRELSE	**Digitala risker** Tillräcklig teknisk kompetens för att kunna förstå och bedöma digitala risker och säkerhetsåtgärder	**Riskaptit** Bedöm risker och definiera er riskaptit. Hitta ett systematiskt sätt att hantera cyberrisk ihop med andra risker. Följ upp kontinuerligt	**Verksamhetsstrategi** Baserad på digitala risker och med hänsyn till verksamhetens digitala beroende. Där IT och OT kopplas ihop med verksamhetsmål snarare än att hanteras som silos	**Helhetsansvar** Ta en mer aktiv roll inom säkerhetsfrågor. Håll ihop helheten och se till att verksamheten jobbar i samma riktning. Sätta prioriteringar och fördela resurser
			MÄTA OCH STYRA PÅ RISK & SÄKERHET	***TVÄRFUNKTIONELLA SAMVERKANSFORUM***
IT	**Verksamhets-förståelse** Säkra en djup förståelse för verksamheten eller produktionen. Förstå specifika krav och förutsättningar	**Gemensamt riskramverk** Hantera IT- och OT-risker ihop och försök göra dem jämförbara med varandra och andra risker. Kvantifiera om möjligt	**IT och OT-strategi** Bryter ner verksamhetsstrategin och definierar gemensamma mål för IT och OT kring säkerhetsarbetet	**Cybersäkerhet IT och OT** Samordna arbetet att cybersäkra IT och OT. Balansera krav och prioriteringar. Central styrning kombinerat med decentraliserat ansvar
			MÄTA OCH STYRA PÅ RISK & SÄKERHET	***TVÄRFUNKTIONELLA SAMVERKANSFORUM***
OT	**Cybersäkerhet** Förstå hur digitaliseringen av verksamhetsteknik påverkar säkerhet inom OT. Kunskap om den nya hotbilden och sårbarheter	**Riskbaserat arbete** Bedöm och hantera cyberrisker i det dagliga arbetet. Exempelvis att ta hänsyn till cyberrisker vid inköp. Rapportera om nya möjliga risker eller sårbarheter	**Riktlinjer** Omvandla krav till instruktioner och riktlinjer som jobbar mot målen samtidigt som de funkar i praktiken för OT-system	**Drift och säkerhet** Ansvarig över driften, samt det operativa säkerhetsarbetet för OT baserat på gemensamt definierade mål och krav

KÄNNER DU IGEN DIG?

IT

Vår produktionsenhet fattar beslut om att investera i ny utrustning som kommer att förbättra effektiviteten i produktionen, och IT-teamet är inte alls tillräckligt involverade i processen. Vi är oroade över säkerheten och hur den nya utrustningen kommer att integreras med våra befintliga processer och system. Det känns som om vi arbetar i silos och inte riktigt förstår varandras perspektiv, vilket leder till en hel del frustration och misstro. Det står klart att vi behöver bättre samordning, men hur når vi dit?

Det är vårt ansvar att försöka säkra verksamheten från cyberangrepp. Men det känns som att andra inte förstår att cybersäkerhet kan innebära att man måste acceptera en viss inflexibilitet och att man inte kan fortsätta göra som man alltid har gjort. Inom IT upplever vi att OT inte beaktar säkerhet i tillräcklig omfattning.

OT

Du är mitt i ett stort projekt som har potential att öka produktiviteten, effektivisera och faktiskt förbättra hela verksamheten. Projektet har fokuserat på att få teknik på plats, införande på tid och enligt budget. Samtidigt som ditt fokus varit starkt inriktat mot att få till en optimal verksamhetsdrift så har IT-avdelningen börjat lägga sig i runt införandet av nya säkerhetsprotokoll och uppdateringar. Du upplever att det bromsar framdriften och deras förslag funkar dessutom dåligt i verkligheten. Hur ska ni kunna säkerställa att produktionen flyter på, när ni ständigt måste jonglera med störningar?

Det blir alltmer uppenbart att gränserna mellan era och IT:s ansvarsområden är suddiga. Det är oklart vem som egentligen har sista ordet i viktiga beslut och hur vi kan förena våra olika perspektiv.

LEDNING OCH STYRELSE

Som styrelseledamot fattar du beslut om bolagets styrning och förvaltning. Alla vet att säkerhet blivit ett högt prioriterat område och intresset finns men kunskapen är låg. Riskansvaret ligger på styrelsen, men det är svårt att tolka de digitala riskerna och verksamhetens sakkunniga är alldeles för duktiga på att beskriva dem i tekniska termer.

Ledningen i samma bolag har det operativa ansvaret. Det är mycket som är prioriterat och måste hanteras. Cybersäkerhet är såklart viktigt, men det är även mycket annat. Vi litar på att IT-avdelningen har tillräcklig koll på denna tekniska fråga och delar den information som vi behöver ha.

Vi saknar kanske ett systematiskt arbetssätt runt cybersäkerhet för det börjar bli tungrott med lagkrav som drar igång olika interna projekt, all dokumentation som ska sammanställas och nya säkerhetsrutiner och investeringar som måste genomföras. Det känns inte som att den här situationen är hållbar över tid, men vi vet såklart att vi måste jobba med frågan.

FÖRSLAG PÅ ÅTGÄRDER

- *Skapa tydliga beslutsprocesser med väl definierade roller och ansvar*
- *Inrätta en tvärfunktionell styrgrupp för säkerhet med ledningsrepresentation*
- *Utbildningar för såväl IT, OT som ledning*
- *IT gör praktik i produktion/verksamhet*
- *Kvantifiera risker och lyft till ledningen på ett pedagogiskt sätt som utgår ifrån verksamhetens specifika förutsättningar*
- *Skapa ägarskap och fördela ansvar för säkerhet ute i verksamheten*
- *Skapa kontinuitetsplaner som inkluderar både IT- och verksamhet och krisöva ihop*

- *Involvera IT i OT-inköp tidigt i processen för att hitta lösningar som funkar bra för båda*
- *Jobba med kompetensutveckling kring cybersäkerhet och omvärldsbevakning för att förstå hur digitala hot och sårbarheter inom OT behöver hanteras*
- *Säkerställ att arbetet med incidenthantering i OT-miljöer också kommer med bland redovisade IT -incidenter*
- *OT-risker ska hanteras operativt i produktionen, men övergripande riskansvar ska ligga hos ledning och styrelse*

- *Styrelse och ledning måste öka sin kunskap inom cybersäkerhet och ta en mer aktiv roll*
- *Lösningen är inte försäkringar och teknik enbart, det måste till ett systematiskt säkerhetsarbete*
- *Skapa en säkerhetskultur som kan genomsyra rutiner och beslutsfattande*
- *Föregå med gott exempel och visa att säkerheten är prioriterad uppifrån*
- *Skapa eller delta i samverkansforum för att hålla ihop helheten och få till samarbete mellan olika funktioner*
- *Bedöm cyberrisker och kom ihåg att de kan kräva tätare bedömningar än andra risker*
- *Släpp inte frågor eller risker, följ upp*

Radar.

REFERENSLISTA

1. Fortinet (2024). 2024 State of Operational Technology and Cybersecurity Report. https://www.fortinet.com/resources/reports/state-of-ot-cybersecurity

2. MSB (2023). Building resilience for the future. Lessons from Ukraine. https://rib.msb.se/filer/pdf/30449.pdf

3. Nozomi Networks (2024). Assessing the Threat Landscape for OT & IoT Security. https://www.nozominetworks.com/resources/assessing-the-threat-landscape-for-ot-iot-security

4. NIST (2024). Definition Operational Technology. https://csrc.nist.gov/glossary/term/operational_technology. [2024-08-05]

5. Regeringen (2024). Nya regler om cybersäkerhet. SOU 2024:18. https://www.regeringen.se/contentassets/1e56bf5cad214fc78eb80d91c11cccb6/nya-regler-om-cybersakerhet-sou-202418.pdf [2024-08-07]

6. SVT (2024). Larm om misstänkt kartläggning av landets elberedskap. https://www.svt.se/nyheter/inrikes/larm-om-misstankt-kartlaggning-av-landets-elberedskap. [2024-08-07]

7. Säkerhetspolisen (2024). Lägesbild 2023–2024. https://sakerhetspolisen.se/download/18.5cb30b118d1e95affec37/1708502268494/Lägesbild%202023-2024.pdf

8. TT (2023). NATO övar hot mot förnybara energisystem. https://via.tt.se/pressmeddelande/3370925/nato-ovar-hot-mot-fornybara-energisystem?publisherId=3236761. [2024-08-07]

BILDKÄLLOR

Omslagsbild: Hans Ott, Unsplash
Sida 1: Manuel Keller, Unsplash
Sida 2: Harrison Broadbent, Unsplash
Sida 6: Hans Ott, Unsplash
Sida 11: Jonas Jacobsson, Unsplash
Sida 15: Charles Deluvio, Unsplash
Sida 22: Reproductive Health Supplies Coalition, Unsplash
Sida 23 & 33: Rob Lambert, Unsplash
Sida 24: Testalize, Usplash
Sida 25: Kato Blackmore, Unsplash
Sida 26: Rivage, Unsplash
Sida 27: Jonas Jacobsson, Unsplash
Sida 29: Hans Ott, Unsplash

BILAGA A: REGULATORISKA KRAV

EU REGLERINGAR INOM CYBERSÄKERHET

EU STRATEGI FÖR CYBERSÄKERHET	
Cyber Solidarity Act	Stärkt solidaritet och kapacitet i unionen att upptäcka, förbereda sig inför och hantera storskaliga cyberhot och incidenter. Innefattar upprättandet av ett europeiskt SOC-nätverk, en europeisk cyberkrismekanism och mekanism för incidentutvärdering
Cyber Security Act	Utökat mandat för ENISA, och uppgift att etablera ett ramverk för cybersäkerhetscertifieringar av IKT-produkter, tjänster och processer
NIS2-direktivet	Säkerhet i nätverks- och informationssystem som innefattar krav kring cybersäkerhetsåtgärder, incidenthantering och rapportering
Cyber Resilience Act (CRA)	Reglering av produkter med digitala element. Cybersäkerhetskrav vid design, utveckling och produktion, samt regler för att säkerställa en högre säkerhet under produktens livslängd
CER-direktivet	Säkerställa förmågan hos samhällsviktiga aktörer att förebygga, motstå och hantera störningar eller avbrott i verksamheten. Som exempelvis terrorattacker, sabotage, olyckor eller naturkatastrofer
DORA	Reglering för ökad motståndskraft och effektiv hantering av digitala risker inom bank- och finanssektorn

LAGEN OM CYBERSÄKERHET

NIS2-direktivet kommer att införlivas i svensk lag och den nya lagen om cybersäkerhet väntas träda i kraft 1 januari 2025. De verksamheter som omfattas är medelstora och stora verksamheter inom nedan sektorer. Som huvudregel gäller ett storlekskrav på minst 50 anställda eller en årsomsättning över 10 miljoner Euro. Undantag kan göras för att exempelvis inkludera mindre verksamheter som bedöms vara samhällskritiska. Nedan presenteras de sektorer som omfattas av lagen om cybersäkerhet[5].

VÄSENTLIG VERKSAMHET	VIKTIG VERKSAMHET
Energi	Post- och budtjänster
Transport	Avfallshantering
Digital infrastruktur	Digitala leverantörer
Förvaltning av IKT-tjänster	Produktion och distribution av livsmedel
Bankverksamhet	Produktion och distribution av kemikalier
Finansmarknadsinfrastruktur	Forskning
Hälso- och sjukvård	Tillverkningsindustrin *(medicinska apparater, datorer, elektroniska och optiska produkter, elektrisk utrustning, maskiner, motorfordon, släpvagnar, semitrailers och annan transportutrustning)*
Dricksvatten	
Avloppsvatten	
Offentlig förvaltning	
Rymdverksamhet	

Verksamhetsutövaren ska vidta tekniska, driftsrelaterade och organisatoriska riskhanteringsåtgärder för att skydda nätverks- och informationssystem och systemens fysiska miljö mot incidenter Åtgärderna ska utgå från ett allriskperspektiv och en riskanalys och vara proportionella i förhållande till risken. De ska utvärderas och särskilt innefatta följande[5]:

Incidenthantering	Kontinuitetshantering	Säkerhet i leveranskedjan
Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem	Strategier och metoder för användning av kryptografi och kryptering	Strategier för åtkomstkontroll och tillgångsförvaltning
Personalsäkerhet	Säkrade lösningar för kommunikation	Lösningar för autentisering

Illustrativa citat från svenska verksamheter

"Mognadsgraden är fortfarande för låg. Vi kommer från en situation där allt var frånkopplat, till att nu koppla upp allt för att förbättra produktion och bli mer effektiva. Men säkerheten är inte där den borde vara. Säkerhet kräver investeringar, och ansträngning. Vi måste höja mognadsgraden snabbt, utan att skapa rädsla i organisationen"

" Jag skulle vilja att styrelsen var mer krävande"

"I stora verksamheter gör man det ibland kanske lite enkelt för sig när man ger ansvaret för OT-säkerhet till en central stab och tror att det ska lösa allting. Men tanken om ett närmare samarbete är god"

"Cybersäkerhet kräver en viss inflexibilitet och tröghet. Det är inte alltid det finns en förståelse för det"

"OT-personerna är inte experter på allt. Säkerhetsarbetet kommer bli suboptimalt om de inte får hjälp. Det är den centralt ansvariges uppgift. Inte att påtvinga något som funkar dåligt i deras verklighet, utan hjälpa de som jobbar i verksamheten att röra sig åt samma håll"

"Vi jobbar med segmentering framför barriär. Man måste snarare förutsätta att hotaktörer tar sig in och förhindra att de tar sig vidare. Vi måste ha system som kan upptäcka intrång och människor som kan hantera dem när de händer"

"Det finns mycket förutfattade meningar och klassiska 'vi och dem'-uppdelningar. Vi behöver utbilda varandra, annars fortsätter glappet att öka. Samverkan är en nyckel. För båda vill ju komma framåt i sina verksamheter"

Radar. EXCLUSIVE NETWORKS FORTINET NOZOMI NETWORKS

OM RADAR

Radars verksamhet bygger på data, nyckeltal och analyser på respektive nordiska marknader vilket också är basen för den faktabaserade rådgivning inom IT-styrning, strategi och verksamhetsutveckling som bolaget driver. Fokus är att skapa värde och tack vare nöjda och lojala kunder har verksamheten växt till att idag vara den oberoende aktör som har flest kunder inom
rådgivning på den lokala marknaden.

Radars tjänster skapar möjlighet för dig som IT-beslutsfattare att styra verksamheten baserad på lokalt insamlade fakta hur svenska och nordiska IT-chefer levererar, planerar och genomför sin IT-verksamhet. Genom tusentals datapunkter i ekosystemet samt genom närhet och kunskap om den lokala marknaden, levererar Radar ett värdeskapande som är ledande på såväl operativ som strategisk nivå. Radar levererar produkter och tjänster till såväl leverantörer som köpare av IT, vilket skapar en unik position att kunna följa en krona genom ekosystemet. Radar kan därför erbjuda en unik detaljnivå för en IT-verksamhet som genom våra olika erbjudanden stärker Radars kunders förmåga, lönsamhet och effektivitet efter lokala förutsättningar.

Ledande leverantör av faktabaserad insikt
Radar levererar insikt som bygger på lokal information. Radars insikt byggs upp genom tusentals strategi-, prioriterings- och nyckeltalsjämförelser som såväl IT-beslutfattare som leverantörer låter Radar genomföra och analysera varje år på respektive marknad. Genom analyser av dessa datapunkter samt genom närhet och kunskap om den lokala marknaden levererar Radar ett värdeskapande som är ledande på såväl operativ som strategisk nivå. Radar följer många underliggande regulatoriska, marknadsmässiga och tekniktrender som förändrar förutsättningarna för en IT-verksamhet och arbetar med råd och insikter runt den förändring som är ofrånkomlig.

Databas av nyckeltal
Radar har sedan start byggt egen Intellektuell Property (IP) i form av databaser och modeller för olika typer av benchmark av IT-verksamhet, pris och kostnadsjämförelser samt olika kvalitetsparametrar. Databaserna utvecklas genom kundåtaganden samt genom löpande insamling av data från IT-beslutsfattare via bland annat online-modeller ingående i abonnemang, enkäter, kostnadsanalyser, avtalsanalyser samt djupintervjuer. Genom ständigt uppdaterade data och erfarna rådgivare så jämförs och optimeras kostnader, priser och effektivitet inom en IT-verksamhet. Till skillnad mot många andra aktörer behöver Radar inte starta om processen med faktainsamling eller komplettering då lokala relevanta jämförelsefakta ofta redan finns i våra databaser.

Rådgivning och beslutsstöd
Radar erbjuder avancerad rådgivning inom IT-styrning, sourcing och nyckeltal kopplade till IT-produktion och effekthemtagning. Radars rådgivare har referensuppdrag inom IT-strategi, CIO-stöd, kompetensförsörjning, sourcingstrategi, m.m., till kunder över hela Sverige inom både privat och offentlig sektor. All rådgivning bygger på faktabaserad insikt, d.v.s. Radars data och mätpunkter för kostnader och effekt på den nordiska IT-marknaden. Radar stödjer sina kunder med en unik kombination av erfarenhet och underbyggda fakta i alla rådgivningsuppdrag.

Kontakt
+46812208000
www.radargrp.com

Besöksadress
Hammarby allé 47
120 30, Stockholm, Sweden

Radar.