Säker region

Ciscos vägledning för cybersäkra regioner

Innehåll

Sammanfattning

Samtliga Sveriges regioner har Cisco som leverantör för någon del av sin it-miljö. Genom dessa kundrelationer har vi fått en unik inblick i vilka säkerhetsutmaningar svenska regioner står inför. I dagliga dialoger med både beslutsfattare och it-chefer ser vi att många vill prioritera it-säkerhet, men också att många efterfrågar vägledning i hur man ska gå till väga för att hantera den i många fall både nya och komplexa hotbild kopplat till it-säkerhet som finns. Utbildningsmaterial med fokus på it-säkerhet är ofta skrivet på ett tekniskt fackspråk och är inte helt lätt att ta till sig för personer som inte arbetar dagligen med frågan.

Vi har därför tagit fram denna vägledning som innehåller en beskrivning av hur vi ser på it-säkerhet i svenska regioner. Frågor som vi kommer ge vår syn på är till exempel vilka hot och utmaningar som är specifika för den regionala sektorn och vilka behov och förmågor som krävs för att skydda sig.

Vi tror att materialet är extra användarbart för dig som har rollen CIO eller CISO men det ska också ses som en viktig pusselbit för att bidra med kunskaper inom området it-säkerhet till regionala beslutsfattare. Här nedan ser du en summering av de olika avsnitten och dess innehåll.

It-hot och sårbarheter	Extern hotbild mot svenska regioner Metoder och angreppsätt
Generella regionala it-utmaningar	Generella utmaningar i regionernas it-säkerhetsarbete Utmaningar i hantering av personuppgifter i molnet
Regionala behov av it-säkerhet	Vilka behov har regioner av it-säkerhet? Hela regionens behov Verksamhetsspecifika behov
Nödvändiga säkerhetsförmågor för att trygga it-miljön	Vilka förmågor krävs för att möta de regionala behoven? Förmågor för hela regionen Verksamhetsspecifika förmågor
Användarfall och lösningar för en säker region	Exempel på användarfall och lösningar för en säker region

Om Ciscos vägledning för cybersäkra regioner

Cisco har som en av Sveriges ledande leverantörer av säkerhetslösningar en god inblick i de hot och utmaningar den svenska offentliga sektorn står inför inom cybersäkerhetsområdet. Vi gav under våren 2022 ut skriften **Cybersäker kommun**[1] som beskrev situationen för svenska kommuner. Nu går vi vidare i vårt arbete i att försöka stärka cybersäkerheten i den svenska offentliga sektorn genom denna skrift; **Cybersäker region**. Målsättningen med skriften är att försöka skapa en överblick över den typiska regionala it-miljön och vilka behov och förmågor som kan kopplas till denna.

Regionerna utgör en grundpelare i den svenska välfärden. Genom sitt ansvar för kollektivtrafik, regional utveckling, i viss mån kultur men särskilt hälso- och sjukvård har man ansvar för mycket av det som medborgarna ser som grundfunktioner i samhället. När medborgarna själv får ranka sina absolut viktigaste frågor återkommer sjukvården nästan alltid som den viktigaste[2]. Regioners överlägset största ansvar är också hälso- och sjukvård vilket påverkar innehållet i denna skrift. Avsikten är dock att täcka hela regionsektorn.

Precis som andra delar av samhället har regionsektorn under lång tid arbetat med att digitalisera sin verksamhet. Detta har i många fall lett till bättre och mer patientcentrerad vård, en smidigare resa för kollektivtrafikresenären och en förbättrad administration inom regionen. I många fall har verksamheterna blivit så beroende av digitala lösningar och verktyg att det blivit svårt att bibehålla samma kvalitet i servicen vid ett avbrott. Vi har i korthet varit så effektiva i vår digitalisering att vi gjort oss i stort sett helt beroende av att den fungerar.

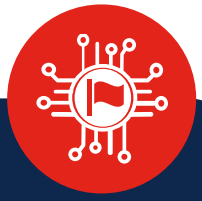
Det finns olika hot kopplat till it som en region behöver skydda sig mot. Denna skrift kommer att fokusera på **cybersäkerhetshot**. Det finns ingen vedertagen definition av cybersäkerhetshot men det kan beskrivas som en avsiktlig handling för att skada, störa eller på annat negativt sätt påverka nätverks- och informationssystem, användare av dessa system och andra personer.

För att komma till rätta med cybersäkerhetshot är en förutsättning att ha ett ändamålsenligt arbete med såväl **it-säkerhet** som **informationssäkerhet**. **Informationssäkerhet** är den samlade, övergripande säkerhet som ska se till att den information som finns i en organisation alltid är korrekt, tillgänglig och skyddad från obehörig åtkomst[3]. **It-säkerhet** är ett samlande begrepp för det en organisation gör för att skydda en verksamhets värdefulla tillgångar som information, hårdvara och mjukvara. Både informations- och it-säkerhet ingår som en del av en verksamhets totala säkerhetsarbete. I denna skrift kommer fokus ligga huvudsakligen på hot och skydd direkt kopplat till it.

Ciscos bedömning är att den regionala sektorn i många fall har ett relativt välfungerande arbete när det kommer till it- och informationssäkerhet. Men som nästan alla andra sektorer i samhället har man i flera regioner insett att man trots det är underinvesterade i säkerhetslösningar. Delvis har omvärlden blivit en osäkrare plats genom konflikter på global nivå. Delvis har hot-aktörerna blivit mer aktiva och professionella i sina angrepp. Fokuset har också stärkts genom ett antal vitt uppmärksammade framgångsrika attacker på svenska företag och offentliga institutioner.

Målgruppen för denna skrift är huvudsakligen it-chefer, it-säkerhetschefer och CIO:er som funderar över it-säkerhet i en regional kontext. Vi tror också att skriften kan vara av intresse för regiondirektörer och förvaltningschefer som vill bilda sig en uppfattning om hur de kan resonera i it-säkerhetsfrågor. På det sättet är vår förhoppning att materialet kan förenkla i dialogen mellan verksamhet och it inom området.

I denna skrift kommer vi att gå igenom vilka vi ser som de största it-hoten just nu, vilka generella utmaningar som är specifika för just regioner och vilka behov som finns ute i regioners olika verksamheter. Sedan fortsätter vi med att beskriva vilka säkerhetsförmågor regionen behöver bygga upp för att klara dessa behov och avslutar med ett kapitel som beskriver möjliga lösningar för vanliga regionala användarfall. Materialet är baserat på Ciscos långvariga kundkontakt med samtliga svenska regioner samt ett antal intervjuer med företrädare från målgrupperna. Vår ambition är här att fånga både dagens och morgondagens regionala behov av it-säkerhetslösningar.



Statliga aktörer

Stater använder sig av it-attacker främst för att sabotera och spionera. Deras omfattande resurser och expertis gör att de är mycket kapabla och har förmåga att allvarligt störa och skada offentlig verksamhet.

Kriminella organisationer

Kriminella har främst ekonomiska mål vid it-attacker. De försöker komma över känslig data eller lösenord som sedan kan användas i utpressningssyfte.

Aktivister

Aktivister har under senare år använt it-attacker för att störa eller sabotera för stater och organisationer. Målen med attackerna varierar beroende på angripare, men är ofta ideologiskt motiverade.

Extern hotbild mot svenska regioner

Antalet cyberattacker mot europeiska företag och organisationer har de senaste åren ökat påtagligt[4]. Den externa hotbilden är komplex och anledningarna till att angreppen ökar är mångfacetterade. Men en orsak som med stor sannolikhet bidragit till ökningen är bland annat att samhället i allt högre grad har gjort sig alltmer beroende av digitala lösningar för att kunna bedriva sin verksamhet.

Tid är också en resurs som blivit allt viktigare för alla typer av organisationer. För varje timme ett företag eller en verksamhet inte har tillgång till sin information eller sina system går pengar förlorade. En genomsnittlig datafil som förstörs eller förloras beräknas kosta ca 1600 kronor[5]. När det kommer till hälso- och sjukvården är frågan inte heller bara ekonomisk. Här är det bokstavligen en fråga om liv och död.

Denna sårbarhet får som konsekvens att företag och organisationers betalningsvilja för att få tillgång till sin information igen ökar, vilket skapar ytterligare incitament för fientliga aktörer. Och varje gång en organisation betalar de aktörer som utför angreppen stärks dessa, vilket leder till en ond spiral. Slutligen har också de aktörer som ägnar sig åt dessa typer av aktiviteter professionaliserats över tid[6]. Detta gäller såväl statliga aktörer som kriminella organisationer.

Under 2020 gav Säkerhetspolisen ut skriften ”Cybersäkerhet i Sverige – Hot, metoder brister och beroenden”. Denna visar på en diversifierad och kompetent grupp aktörer. I huvudsak utgörs dessa av statliga aktörer och kriminella grupper. I viss omfattning förekommer även ideologiskt motiverade aktörer, såsom hacktivister eller grupperingar med terrorkopplingar.

Statliga aktörer

Statliga aktörer genomför cyberangrepp mot Sverige i olika syften. Det kan exempelvis handla om att inhämta information som kan gynna det egna landets utrikes- och säkerhetspolitiska intressen, att stärka det egna landets ekonomi och företag genom företagsspionerи eller att destabilisera genom att angripa samhällsviktiga tjänster och informationsvägar. Det finns ett flertal statliga aktörer, inom såväl demokratier som mer auktoritära stater, som byggt upp välorganiserade enheter med ansvar för cyberangrepp. Dessa kan formellt vara en del av statens nationella militär eller säkerhetstjänst men kan också ha lösare kopplingar till staten. Även om Sverige inte är i direkt konflikt med dessa länder kan statliga aktörer försöka forcera regionens system för att placera skadlig programvara som sedan ligger latent i systemen. På en given signal kan sådana program sedan användas för att störa eller sabotera regionens verksamhet.

Kriminella organisationer

Det vanligaste cyberhotet mot alla typer av organisationer är kriminella. Cyberkriminalitet syftar i de allra flesta fall till att tjäna pengar. Även här sker en professionalisering och exemplen på framgångsrika it-attacker blir fler och fler. Mörkertalet riskerar också att vara stort då många bolag i stället för att berätta att de blivit utsatta betalar de kriminella. Offentliga organisationer kan vara särskilt känsliga för angrepp från kriminella organisationer, då man hanterar data som kan vara livsavgörande för människors hälsa och välmående (t.ex. patientjournaler). Vi har redan sett exempel på attacker där sådan data krypteras och vårdaktörer utpressas att köpa tillbaka den från angriparen[7]. Vi ser även en utveckling i världen där allt fler statliga aktörer och kriminella organisationer verkar i symbios. I vissa länder fungerar kriminella organisationer nästan precis som företag och kan då utföra uppdrag för stater och köpa kompetens av andra kriminella. I sådana ”entreprenöriella” miljöer får kriminella organisationer ökad förmåga att utföra sofistikerade och riktade attacker.

Aktivister

Nätaktivister, eller hacktivister, utgör ett mindre vanligt förekommande hot mot offentliga organisationer i Sverige. Nätaktivister är ideologiskt drivna och kan ha olika motiv till att angripa offentliga organisationer. Det kan exempelvis handla om att man inte är överens med den politik som förs på nationell eller lokal nivå. Sverige har historiskt sett (till vår kännedom) inte utsatts för några omfattande hacktivist-attacker. Men globalt har man under senare år kunnat observera sådana grupperingar utfört riktade attacker mot statliga mål[8]. Inte sällan rör det sig om ideologiskt drivna personer som ofta besitter stor kunskap om olika angreppsmetoder[9].

Metoder och angreppsätt

Oavsett vilka bakomliggande motiv fientliga aktörer har till att vilja få tillträde till de regionala it-systemen använder de ofta relativt likartade metoder. Gemensamt för många av dessa är att de försöker lura medarbetare eller användare att ge angripare tillträde till nätverk och system. För att ge en snabb överblick över de vanligaste metoderna kommer vi här presentera några av dem.

Nätfiske (phishing)

Ett av de vanligaste tillvägagångssätten för att påbörja ett angrepp är genom att skicka mejl som ser legitimt ut. Angriparen hoppas att en person med tillgång till ett system eller nätverk ska släppa in skadlig programvara som finns i mejlet. Det kan ske genom att man klickar på en länk, öppnar ett bifogat dokument eller laddar ned en bild som finns bifogad i mejlet.

Metoden kallas för nätfiske (phishing) och är mycket populär i cyberattacker. Hela 90% av alla attacker påbörjas genom att en användare öppnar ett phishing-meddelande[10]. Ett av de vanligaste motiven bakom

phishing-attacker är att försöka få tag i inloggningsuppgifter till verksamhets-system, eller att på annat sätt försöka ta sig vidare in i organisationens nätverk.

Skadlig programvara (malware)

En annan vanlig metod vid it-attacker är skadlig programvara (malware). Skadlig programvara är ett samlingsbegrepp som används för att beskriva flera typer av program. Här ingår bland annat spionprogram, ransomware, virus och datamaskar. Även här är den vanligaste angreppsmetoden att en användare klickar på en länk eller e-postbilaga som sedan installerar programvaran på användarens konto. Väl inne i systemet kan program-varan t.ex.:

- Blockera och kryptera åtkomst till väsentlig information i nätverket med syfte att sedan utpressa organisationen på pengar för att få tillbaka den (ransomware)
- Installera ytterligare skadlig programvara
- I hemlighet kopiera information genom att överföra data från centrala system eller hårddiskar (spionprogram)
- Skada eller avbryta vissa tekniska komponenter vilket kan göra systemet obrukbart.

Man-in-the-middle (MitM)-attacker

Man-in-the-middle (MitM)-attacker är även kända som avlyssningsattacker. Dessa inträffar när en angripare får tillträde till en tvåpartstransaktion (t.ex. när en användare ansluter sin enhet till ett nätverk). När angriparna väl får tillträde till datatrafiken kan de analysera och stjäla data från flödet.

Två vanliga ingångspunkter för MitM-attacker är:

1. På offentliga Wi-Fi-nätverk utan tillräcklig säkerhet där angriparen kan agera som en länk mellan en besökares enhet och nätverket. Utan att veta skickar då besökaren all information genom angriparen.
2. När skadlig programvara har gjort intrång i en enhet kan en angripare sedan installera ytterligare programvara för att bearbeta andra enheter som användaren ansluter till.

DDoS-attacker

En DDoS (denial-of-service)-attack översvämmar system, servrar eller nätverk med datatrafik för att förbruka resurser och bandbredd. Som ett resultat kan systemet upplevas gå ner och dess riktiga användare kan inte få tillgång. Målet är oftast inte att komma över specifika data, utan snarare att störa ut viktiga funktioner såsom webbplatser. Motiven till detta kan vara att skapa oreda men metoden kan också användas för att maskera andra typer av it-angrepp.

Generella utmaningar i regionernas it-säkerhetsarbete

Ciscos upplevelse är, som tidigare nämnts, att arbetet med it-säkerhet i svenska regioner under relativt lång tid varit prioriterat. Samtidigt ser vi också att det finns ett antal utmaningar med it-säkerhetsarbetet i regionerna. Vi har valt att sammanställa det som vi ser som de största utmaningarna under tre övergripande rubriker;

- En fragmenterad och omfattande organisation
- En digitalisering i otakt
- Brist på kompetens och en stark profession

Dessutom tillkommer en mer specifik utmaning kopplad till osäkerheten rörande hantering av personuppgifter i molnmiljöer. Denna utmaning har främst aktualiserats genom den uppmärksammade Schrems II-domen.

En fragmenterad och omfattande organisation

Till skillnad från kommuner är regioner huvudsakligen fokuserade kring en fråga – hälso- och sjukvården. Ca 82 procent av de regionala kostnaderna är hälso- och sjukvårdskopplade[11]. Detta kan utgöra en organisatorisk fördel för regioner som i mångt och mycket kan dimensionera och anpassa sina lösningar just utifrån vårdens behov. Samtidigt är hälso- och sjukvården ett komplext och omfattande system som leder till att cybersäkerhetsansvariga i regionerna får särskilda utmaningar. Mycket av komplexiteten handlar om att den information som hanteras är av känslig karaktär och att det därför är av särskild vikt att säkerställa att rätt verksamhet får tillgång till rätt information vid rätt tidpunkt, men inte mer. Däremot så är tillgången i många fall överordnad säkerheten. Om det är en fråga om liv och död finns det i ibland möjlighet att åsidosätta säkerhetsfunktioner för att säkerställa att vården ändå kan utföras.

Samtidigt finns ett antal tydliga beröringspunkter med den kommunala sektorn – särskilt inom vården och omsorgen. Möjligheten att dela information mellan regionernas hälso- och sjukvård, kommunernas hälso- och

sjukvård och den kommunala omsorgen är ofta avgörande för att kunna erbjuda patienter en sammanhållen vård, men innebär även informations- och cybersäkerhetsmässiga utmaningar för hur information kan delas på ett säkert sätt mellan aktörerna. Dessutom finns ofta en bred flora av privata och offentliga vård- och omsorgsutförare i både region och kommun, vilket ytterligare försvårar möjligheterna till säkert informationsutbyte. Utöver det finns också en central aktör i form av Inera som tillhandahåller de huvudsakliga vårdnära e-tjänster som riktar sig ut mot regioninvånarna. Även detta utgör en komplicerande faktor i termer av roller och ansvar inom it- och informationssäkerhetsarbetet.

Vi ser även att det är relativt vanligt förekommande att kollektivtrafiken är avknoppad och i stor utsträckning får sköta sig själv i många regioner och att centrala säkerhetsfunktioner tenderar att vara relativt fokuserade på de behov som finns inom hälso- och sjukvården. Detta ger kollektivtrafiken relativt stor handlingsfrihet att anpassa lösningar utifrån de behov som finns inom området. Samtidigt innebär det att man inte nödvändigtvis nyttjar de stordriftsfördelar som det innebär att vara en större aktör i termer av gemensamma resurser och kompetenser.

Här är det också värt att påtala att regionerna i stor utsträckning har ett ansvar för sin egen verksamhet. Även fast verksamheten innehållsmässigt är huvudsakligen densamma i samtliga 21 regioner så är det relativt ovanligt förekommande att regioner samverkar kring informations- och it-säkerhet. På central nivå finns Nationellt cybersäkerhetscenter med uppdrag att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot. Centret är under uppbyggnad och kan på sikt utgöra en viktig aktör i arbetet att främja den svenska cybersäkerheten även inom regionsektorn.

En digitalisering i otakt

Regionsektorn är, som stora delar av det övriga samhället, en sektor i förändring. Hälso- och sjukvården har under en lång tid varit ledande i att implementera digitala lösningar för en effektiv vård av god kvalitet. Det kan exempelvis handla om monitoreringsutrustning som låter diabetespatienter själva hålla koll på sina blodsockernivåer och rapportera in dem till vården, robotar som möjliggör för kirurger att utföra komplexa operationer på distans och hjärt- och lungmaskiner som är direkt livsuppehållande. All denna utrustning innehåller digitala beståndsdelar och mycket av utrustningen är också uppkopplad mot nätet på något sätt. Detta exempelvis för att överföra data mellan system eller för att möjliggöra support. Samtidigt finns en annan bild av it och digitalisering i regionerna. Precis som i många andra delar av offentlig sektor finns en stor mängd föråldrad programvara och medicinteknisk utrustning (MT), vilket ofta leder till att vårdens medarbetare upplever it-systemen som ett arbetsmiljöproblem snarare än ett stöd i vardagen. Ett exempel är de digitala verksamhetssystem som används för att möta de höga kraven på dokumentation som följer av bland annat patientdatalagen. Verksamhetssystemen har ofta implementerats med ett bristande grepp kring den samlade it-arkitekturen, vilket leder till att samma information måste skrivas flera gånger i olika verksamhets- och journalsystem.

Ytterligare en komplexitet kopplad till implementeringen av medicinteknisk utrustning i vården är att MT-produkter behöver CE-märkas av Läkemedelsverket för att godkännas. När produkten väl godkänts får den inte förändras utan ett nytt godkännande. I jämförelse med andra mer konventionella digitala produkter, som regelmässigt får uppdateringar eller så kallade ”patchar” för att åtgärda säkerhetsbrister, är detta inte möjligt när det kommer till medicintekniska produkter vilket leder till att de blir särskilt sårbara för angrepp. Medicintekniska produkter är dessutom ofta relativt hårt knutna till leverantören för såväl support som uppdateringar men även tekniska gränssnitt vilket också ställer till svårigheter om man vill standardisera sin it-miljö.

När det kommer till kollektivtrafikområdet ser vi inte samma utmaningar som med medicinteknisk utrustning men där är å andra sidan produkter av IoT-karaktär vanligt förekommande. Dessa ställer särskilda krav på it-säkerheten då de ofta har ett svagt skydd.

Den samlade bilden av digitaliseringen i regionen är att den går något i otakt. Samtidigt som det finns absolut spetsteknologi inom ett flertal områden finns det också sårbarheter och föråldrade system. Detta ställer särskilda krav när det kommer till arbetet med it- och informationssäkerhet.

Brist på kompetens och en stark profession

På samma sätt som i kommuner är kompetens en påtaglig utmaning när det kommer till arbetet med it- och informationssäkerhet. Här kan man också addera komplexiteten det innebär att ha ett antal starka professioner som påverkar innehållet i verksamheten.

Inom ramen för nästan alla typer av organisationer är den digitala kompetensen hos medarbetarna ojämnt fördelad. Regioner är inte något undantag. Det finns medarbetare som ligger i den absoluta framkanten när det kommer till nyttjandet av digitala tjänster men det finns också medarbetare som sällan eller aldrig använder digitala tjänster. Detta blir särskilt utmanande utifrån ett it-säkerhetsperspektiv då ett nätverk potentiellt inte behöver vara starkare än sin svagaste länk. Det krävs enbart att en medarbetare klickar på en länk för att infektera ett dåligt säkrat nätverk.

Den andra delen av kompetensutmaningen handlar om bristen på spetskompetens inom området. Det finns en uppskattning om att det redan i dagsläget saknas 20% av den arbetskraft som skulle krävas inom området. Samtidigt förväntas behovet av kompetens inom it-säkerhet öka ytterligare i närtid[12]. De budgetmässiga begränsningar som finns i många regioner kan också innebära att de har svårt att stå sig i konkurrensen om arbetskraften framför allt i konkurrens med den privata sektorn. Detta kan i sin tur leda till att it-säkerhetsroller står obemannade under lång tid eller att ansvar och arbetsuppgifter läggs på resurser som inte har it-säkerhetskompetens. Båda dessa faktum kan ge upphov till säkerhetsrisker. Gällande

rekrytering av kompetens ser vi också tendensen att om en region lyckas fylla en position så kommer ofta den individen från en annan region vilket leder till att det totala skyddsvärdet för hela den regionala sektorn är oförändrat.

Ytterligare en komplexitet inom området är att regionernas verksamheter – och särskilt hälso- och sjukvården – är en påtagligt professionsstyrd verksamhet. Det finns ett antal starka professioner som har ett stort inflytande i utformningen av vården. Det finns många positiva aspekter i detta, bland annat att de som har bäst förståelse för och närhet till patienten har stora möjligheter att påverka vårdens sakinnehåll. Utifrån ett it- och informationssäkerhetsperspektiv kan det dock leda till utmaningar. De frågor som tenderar att prioriteras är, enligt vår erfarenhet, de som direkt bidrar till bättre vård. Alla andra frågor tenderar att nedprioriteras eller ses som någon annans ansvar. Detta gör det utmanande att nå ut med frågor om it- och informationssäkerhet och då särskilt i termer av att låta säkerhetsfrågorna ta plats tidigt i alla förändringsprocesser.

Detta fokus på patientnära processer och den tidigare nämnda förekomsten av osmidiga och komplexa system kan också leda till att medarbetarna blir uppfinningsrika för att få till vad de ser som en patientsäker arbetsdag. Exempelvis kan medarbetare låta SITHS-kort sitta i avdelningsdatorer hela arbetspass för att det är det enda sättet att få patientflödet att fungera. Samtidigt innebär det såväl it-säkerhetsmässiga som informationssäkerhetsmässiga sårbarheter.

Utmaningar i hantering av personuppgifter i molnet (Schrems II)

I flera år har debatten om hur personuppgifter kan hanteras digitalt av svenska myndigheter, regioner och kommuner pågått. Fokus har legat på huruvida personuppgifter kan placeras dels i molntjänster, dels i tjänster som tillhandahålls av amerikanska leverantörer.

Bakgrunden till diskussionen är den s.k. Schrems II-domen. Denna innebar att det regelverk som tidigare reglerat dataöverföring av personuppgifter (Privacy Shield) mellan USA och Europa blev ogiltigförklarat. Domen har delvis tolkats som att placeringen av personuppgifter i amerikanska molntjänster inte är förenliga med dataskyddsförordningen. Många regioner har valt att bromsa eller helt stoppa införandet av sådana tjänster. Samtidigt är molnbaserade tjänster ett mycket användbart verktyg som skapar goda förutsättningar för distansarbete och samverkan i stora organisationer med många intressenter.

I en statlig utredning från 2021 konstateras det att många offentliga organisationer ser problem med att balansera verksamhetens krav på digitalisering och kostnadseffektiva lösningar mot krav på säkerhet.

Denna utmaning förväntas inte heller bli mindre, i takt med att offentliga verksamheter även i framtiden kommer ha ett behov av flexibla, skalbara och tillgängliga it-lösningar. Det finns dessutom ett växande behov av att kunna tillgängliggöra information till olika intressenter, samarbeta med externa parter och att snabbt kunna ställa om verksamheter vid förändrade förutsättningar[13].

Enligt utredningen råder det en osäkerhet bland många offentliga aktörer kring förutsättningarna för utkontraktering av it-drift till privata tjänsteleverantörer. Tolkningen av när en uppgift delas felaktigt enligt rådande lagstiftning är svår att göra. På grund av osäkerheten har vissa aktörer avvaktat att ta beslut om it-drift, vilket också det kan få negativa konsekvenser för organisationernas utveckling, säkerhet och kostnader[14].

Ciscos syn på hantering av personuppgifter i molnet

Vi tror att Schrems II har ökat behovet av att bygga långsiktiga relationer baserade på förtroende mellan leverantörer, kunder och partners. Att visa att man värnar om varandras integritet och säkerhet blir en högt prioriterad fråga i nya affärsrelationer framöver.

Vi tror också att förtroende i stor utsträckning bör bygga på transparens. Att i detalj och på produktnivå kunna visa vilken persondata som behandlas är en grundläggande förutsättning för sådan transparens. Informationen om hur data behandlas bör vara fritt tillgänglig för kunder, partners och allmänheten. På så sätt görs också integritetskonsekvensbedömning och analyser möjliga. Detta har vi arbetat med på Cisco under lång tid. Vi är transparenta med vilken data som berörs vid användning av våra produkter och tjänster, om det finns en internationell överföring och vilka risker som är förknippade med vilken typ av uppgifter eller behandling som berörs. Cisco behandlar endast EU-personuppgifter på platser där EU:s dataskyddsstandarder kan uppfyllas och ”i huvudsak likvärdigt” skydd kan tillhandahållas. Se även Ciscos Trust center för vidare information[15].

Vilka behov har regioner av it-säkerhet?

I detta kapitel kommer vi att beskriva vår syn på de it-säkerhetsmässiga behov som finns kopplade till den regionala it-miljön. Även om Sveriges 21 regioner är organiserade på olika sätt och har olika storlekar och förutsättningar ser Cisco att många behov liknar varandra. Vi inleder det här avsnittet med att beskriva vår syn på gemensamma och grundläggande regionala behov. Vi presenterar också ett antal verksamhetsspecifika behov som är uppdelade i verksamhetsområdena kollektivtrafik samt hälso- och sjukvård som vi delat in i kategorierna möjliggöra vård, som lägger grundförutsättningarna för att utföra vård, och utföra vård, där vi försöker fånga det med patientnära. Vi är medvetna om att detta inte täcker hela regionens ansvarsområde men vår bedömning är att övriga verksamheter som regionen ansvarar för täcks in av de behov som beskrivs under hela regionens behov.

Hela regionens behov

Trots att Sveriges 21 regioner valt att organisera sig på lite olika sätt och har olika mix av privata och offentliga utförare är vår bedömning att de övergripande behoven ser relativt likartade ut. Främst handlar det om att på ett säkert sätt tillhandahålla verktyg som underlättar och stödjer hela regionen i dess dagliga verksamhet. It-säkerhet är enligt vår uppfattning ett område som för användaren helst inte ska märkas över huvud taget.

I det här avsnittet ger vi vår syn på sex basbehov som varje regional it-miljö behöver tillgodose.

Att relevant lagstiftning följs

Regioner har i jämförelse med många privata organisationer en väldigt lagstyrd verksamhet. Ett grundläggande behov är alltså att det kan garanteras att all relevant lagstiftning följs. Detta kan låta som en självklarhet – men idag finns en stor osäkerhet kring många frågeställningar kopplade till it-säkerhet. På senare år har EU:s dataskyddsförordning (GDPR) varit mycket uppmärksammad, men det finns andra lagstiftningar (t.ex. OSL, patientdatalagen, hälso- och sjukvårdslagen samt NIS2-direktivet) som reglerar hur en region bör hantera känslig information.

Patientdatalagen reglerar bland annat:

- Vilken information som måste ingå i en patientjournal
- Vårdgivares möjlighet att ge patienten direktåtkomst till dess vårddokumentation.
- Sammanhållen journalföring, vilket innebär att flera vårdgivare kan ge och få direktåtkomst till varandras journalhandlingar om de uppfyller patientdatalagens krav.
- Inre sekretess – en reglering som innebär att bara den som behöver uppgifterna i sitt arbete inom hälso- och sjukvården får ta del av patientuppgifter. Detta förtydligas genom att det i lagen ställs krav på behörighetstilldelning och åtkomstkontroll.
- Patienten har rätt att spärra uppgifter både i vårdgivarens journalsystem och för andra vårdgivare vid sammanhållen journalföring.[16]

Relevant att påtala här är också vikten av det kommande NIS2-direktivet som från EU-nivå reglerar cybersäkerhetsnivåer avseende såväl hälso- och sjukvård som kollektivtrafik.

Att rätt person har tillgång till rätt system vid rätt tidpunkt

I moderna verksamheter har digitala verktyg och den information som finns i dessa verktyg blivit en grundförutsättning för att kunna utföra någon verksamhet överhuvudtaget. Det förutsätter att rätt person har tillgång till rätt system och rätt informationsmängd vid rätt tidpunkt. Grundbehovet här är således att säkerställa att så kan ske. Egentligen handlar det här om flera behov som samverkar. Vi listar dessa nedan:

- Regionen behöver kunna tillgängliggöra information mellan olika verksamheter.
- För att relevant lagstiftning ska följas finns även ett behov att säkerställa att bara behöriga personer har tillgång till känslig information i de regionala verksamhetssystemen. Utifrån ett it-säkerhetsperspektiv är det alltså av vikt att säkerställa att användarna har tillgång till rätt information genom att garantera sig om motsatsen – att inte fel person får tillgång till information som de inte har rätt till.
- För att ovanstående behov ska kunna uppfyllas är det också nödvändigt för regionen att system och program kommunicerar med varandra för att tillgängliggöra och säkra information i korrekt ordning. En person som byter befattning i regionen ska t.ex. inte kunna tillgå samma verksamhetssystem som tidigare, om inte det är nödvändigt för den nya yrkesrollen.

Stabil och säker nättillgång i regionens lokaler

Som tidigare nämnts har många regionala verksamheter genomgått en omfattande digitalisering under senare år. Vi ser att denna trend kommer att fortsätta och öka även i den närmaste framtiden. Ett ständigt växande behov och användning av digitala funktioner, med fler användare, ökar behoven av säkra och stabila anslutningar i regionens lokaler. Samtidigt har ett skifte skett mot en digital miljö som alltmer fokuserar på bärbara enheter. I en regional kontext innefattar det alltifrån att möjliggöra nättillgång för patienter på inlagda på sjukhusen till öppna nät på långdistansbussar till att medarbetarna på ett smidigt sätt kan arbeta. Denna leverans har således blivit en grundförutsättning för att möjliggöra regionens samtliga verksamheter. Det handlar dels om ett behov av att säkerställa att nättillgången inte utgör en accesspunkt för att penetrera regionens infrastruktur. Dessutom måste nätverket klara av en ständigt ökande mängd datatrafik, för att undvika överbelastning.

Denna vägledning fokuserar främst på it-säkerhet, men om du är intresserad av hur vi på Cisco jobbar med kapacitetsfrågor kopplade till Wi-Fi, så kan du läsa mer om vårt nationella program WiFi-lyftet[17] .

Tillräcklig kompetens inom it-säkerhetsområdet hos personalen

Som tidigare nämnts är en it-miljö bara så säker som användare gör den. En majoritet av alla cyberattacker påbörjas genom att en användare i den egna organisationen klickar på en smittad länk eller öppnar en fil som skickats av en angripare. När den skadliga kod eller programvara som legat inbäddad accepteras in i systemet så kan den göra mycket stor skada i verksamheten. Att vara medveten om de vanligaste metoderna (t.ex. nät-fiske) minskar risken för framgångsrika angrepp. Samtidigt är kunskapen om sådana metoder generellt sett fortfarande låg hos många it-användare. I vår senaste trendrapport om it-säkerhet, konstaterar vi t.ex. att 86% av alla organisationer har haft någon anställd som klickar på en infekterad länk i en nätfiske-attack[18].

Att informationstillgångar och verksamhetssystem skyddas från angrepp

För att regionen ska kunna bedriva sin verksamhet i linje med lagstiftning och regler kring sekretess är en grundförutsättning att systemen är tillgängliga och inte penetreras av obehöriga aktörer. Det finns därför ett tydligt behov inom regional verksamhet av tillräckliga skydd så att detta inte kan ske. Vidare behöver regionen säkerställa att den har tillräcklig övervakning, mer eller mindre i realtid, så att ett eventuellt angrepp kan upptäckas så tidigt som möjligt för att kunna minimera skadan. Behovet är inte unikt för den regionala verksamheten, men är inte desto mindre relevant.

Möjliggörande av mobila arbetssätt

Covid-19-pandemin har skyndat på en redan stark trend av mer flexibelt arbete i stora delar av arbetslivet. Här ser vi både de stora möjligheter till distansarbete som finns inom regionen och den potential som i allt större utsträckning börjar nyttjas gällande vård på distans.

Detta ger specifika behov; för anställda krävs möjlighet att kunna medverka i videomöten. De måste också komma åt regionens nätverk på samma villkor som om de var på plats i regionens lokaler, och identifiera sig mot dessa för att få rätt användarbehörighet. Detta ställer nya krav utifrån ett it-säkerhetsperspektiv. När den traditionella säkerheten i verksamheten har haft ett fokus på att säkra upp de miljöer inom vilka de anställda ansluter sig så kommer denna trend innebära ett betydligt större fokus på att upp-rätthålla tillräcklig säkerhet även i andra miljöer. Detta har även gjorts innan pandemin men i takt med att skiftet skett i hur medarbetare och arbetsgivare ser på vad som utgör en lämplig och attraktiv arbetsplats kommer det att ställa helt nya krav på regionens it-säkerhetslösningar.

Verksamhetsspecifika behov

Utöver de behov som redovisats ovan har Cisco också identifierat ett antal verksamhetsspecifika behov. Vi har organiserat dessa verksamhetsbehov i två övergripande kategorier; kollektivtrafik och hälso- och sjukvård. Vi har valt att segmentera hälso- och sjukvården i två underkategorier; möjliggöra och utföra vård för att spegla de olika behov som finns i verksamheten.

Verksamhetsbehov inom kollektivtrafik

Kollektivtrafiken tillhandahålls ofta av fristående bolag, så att verksamheterna sköts helt separat från övrig regional verksamhet. Detta ger dessa aktörer den snabbfotadhet som det innebär att vara en något mindre aktör. Det öppnar samtidigt upp för sårbarheter då man inte på samma sätt kan utnyttja stordriftsfördelarna det innebär att vara del av en större aktör.

Den verksamhet som bedrivs är centrerad kring att tillhandahålla kollektiva transporter till invånare och besökare till regionen. Detta går dock att bryta ner i ett antal beståndsdelar. De regionala kollektivtrafikmyndigheterna (RKM) har det övergripande ansvaret för tillhandahållandet av tjänsten men den absoluta majoriteten av utförandet åläggs privata bolag som upphandlas. Detta ställer särskilda krav utifrån ett informationssäkerhetsperspektiv då entreprenörerna behöver ha tillgång till information och i viss mån system som är gemensamma. På motsvarande sätt blir de också ansvariga för att tillhandahålla information till RKM:erna.

Hanteringen av trafikinformation är ytterligare ett kritiskt verksamhetsområde utifrån ett it- och informationssäkerhetsperspektiv. Denna samlas och tillhandahålls nästan uteslutande som öppna data via Samtrafiken. Att tillhandahålla informationen som öppna data innebär visserligen att samtliga intresserade har möjlighet att få tillgång till informationen men också bygga tjänster baserat på den. Samtidigt behöver alla aktörer som tillhandahåller öppna data vara medvetna om informationssäkerheten och överväga hur informationen kan användas i ett fientligt syfte exempelvis om den läggs samman med annan information. Utöver det behöver analyser ske vilka konsekvenserna skulle bli om informationen manipuleras eller om tillgången stryps.

Regionerna och RKM:erna har också ansvaret för att ta fram övergripande mål och göra prioriteringar inom kollektivtrafiken utifrån ett samhälls-, medborgar- och resenärsperspektiv. Detta görs genom regionala trafikförsörjningsprogram. Här är tillgången till tillförlitlig data en förutsättning för att kunna ta fram välgrundade planer.

När det kommer till den spårbundna trafiken finns särskilda behov. Det handlar bland annat om att i många fall samverka med Trafikverket kring deras trafikinformation. Utifrån ett beredskapsperspektiv är också spårbunden trafik extra sårbar då ett lyckosamt angrepp på denna skulle lamslå stora delar av ett samhälles persontransporter.

Verksamhetsbehov inom hälso- och sjukvård

Vi har valt att segmentera hälso- och sjukvården i två delar. Ett område där vi fokuserar på den tekniska och fysiska infrastrukturen som möjliggör vård och ett område där vi fokuserar på det vårdnära utförandet.

Verksamhetsbehov – möjliggöra vård

Samtliga regioner har någon typ av egna sjukvårdsfastigheter oftast i form av akutsjukhus, vårdcentraler och specialistkliniker. Ett grundläggande behov inom området att möjliggöra vård är således att säkerställa att sjukhusbyggnaderna är tillgängliga och fungerande vid alla tidpunkter. Detta beskrivs i bland annat MSB:s skrift Den robusta sjukhusbyggnaden[19]. Sjukhusbyggnader är ofta till sin natur relativt öppna miljöer vilket i förhållande till andra verksamheter ställer större krav på ett medvetet säkerhetsarbete.

Något som lyfts fram som en grundförutsättning för att möjliggöra vård är möjligheter att vid alla tidpunkter upprätthålla telefonin. Stora delar av verksamheterna är fortfarande beroende av att kunna kommunicera muntligt för att koordinera, planera och utföra verksamheten. Telefoni tillhandahålls oftast via ip-telefoni eller andra digitala lösningar och inte via traditionella kopparledningar.

Utifrån ett it-säkerhetsperspektiv ställs andra krav på denna typ av verksamhet utifrån de potentiellt katastrofala effekter ett driftsavbrott skulle kunna få. För att säkerställa att driften upprätthålls inom ett antal samhällsviktiga områden har som tidigare nämnts EU fattat beslut om NIS-direktivet[20]. Detta pekar ut bl.a. hälso- och sjukvård som ett område som regleras. Att en verksamhet regleras av NIS-direktivet innebär konkret att regionen är skyldig att hålla en hög gemensam nivå på säkerhet i nätverk och informationssystem. Regioner har alltid haft ett särskilt ansvar för att trygga att sådana samhällsfunktioner fungerar tillfredsställande, men under senare år har lagstiftningen skärpts ytterligare. Snart kommer också NIS2 som kommer skärpa kraven ytterligare[21].

I sjukhusbyggnaderna finns också ofta så kallad operational technology (OT). OT-enheter kan förenklat beskrivas som hård- och mjukvara som används för att övervaka eller styra industriell utrustning[22]. Exempel på OT-enheter i ett sjukhus kan exempelvis vara låssystem, styr- och reglersystem och hissar. Många av dessa enheter är tätt kopplade till den utrustning de ska styra och de är ofta relativt gamla och därav sårbara för it-angrepp. Ett tydligt behov inom området är att skapa en central och säker samordning av all OT.

Verksamhetsbehov – utföra vård

Det som särskiljer denna verksamhet från vissa andra delar av regionen är att driftsäkerheten och informationssäkerheten är av ännu större vikt givet den information som hanteras. Dels utifrån hur känslig informationen är, dels utifrån hur verksamhetskritisk den är.

I utförandet av vården är det utifrån ett informations- och it-säkerhetsperspektiv det påtagliga krav på dokumentation som ställs i huvudsakligen patientdatalagen (PDL) som påverkar verksamheten mest. Det ställer stora krav på regionerna bl.a. i termer av att säkerställa att all information registreras på ett korrekt sätt. För att få verksamheterna att fungera är det också centralt att data kan flöda mellan verksamhetssystem och journalsystem på ett smidigt sätt. Detta kräver i många fall integrationer systemen emellan. Patienterna äger också enligt patientdatalagen rätten till sin egen data. Ett flertal regioner har således gett möjligheter för patienter att få tillgång till sin information via 1177. Givet den känsliga karaktären på den data som hanteras i systemen blir den särskilt intressant för hotaktörer.

Utifrån ett verksamhetsperspektiv behöver också den potentiella problematiken med MT-utrustning ute i verksamheterna adresseras. I mycket högre grad än i andra typer av verksamheter utgör MT-utrustning en integrerad del av verksamheten inom hälso- och sjukvården. Den etablerade definitionen av medicintekniska produkter är relativt bred och avser alltifrån rullstolar till röntgenutrustning. När vi refererar till MT-utrustning avser vi enbart de produkter som har en digital komponent men inte enbart är digital. Exempelvis fångar vi med denna definition den fysiska utrustning som nyttjas ute i vården såsom röntgenapparater, hjärt-lungmaskiner, blodtrycksmätare och så vidare. Det vi inte fångar med definitionen är renodlade it-system och enbart fysiska produkter. Vi är medvetna om att det går ifrån den etablerade definitionen men utifrån ett it- och informationssäkerhetsperspektiv har de inte samma behovsbild som den utrustning vi avser med ovan definition. Som delvis beskrivits i utmaningskapitlet finns det specifika utmaningar kopplat till MT-utrustning. Den är definitionsmässigt en medicinteknisk produkt så möjligheterna att uppdatera den är lagstiftningsmässigt begränsad. Det är alltså inte ovanligt att medicintekniska produkter körs på gamla operativsystem som inte är uppdateringsbara. Det finns också ett behov att koppla upp den medicintekniska utrustningen mot nätverket. Detta delvis för att möjliggöra support på produkterna men också för att flöda information till andra verksamhetssystem. Detta behov skapar en sårbarhet utifrån ett cybersäkerhetsperspektiv, då det finns enheter som är svåra att skydda men som tekniskt och utifrån ett verksamhetsbehov behöver vara integrerade i den tekniska miljön.

I takt med att arbetet med kontinuitetsbaserad vård fortlöper och den digitalisering som pågår i samhället har också behovet av vård på distans eller fjärrvård också ökat. Detta kan handla om så enkla saker som att genom videokonsultation tala med vårdpersonal istället för att fysiskt förflytta sig till en mottagning. Men utifrån ett patientsäkerhetsperspektiv finns det också en tydlig rörelse mot att bedriva alltmer avancerad vård i patientens hem, det som ofta refereras till som Avancerad sjukvård i hemmet (ASIH). Där finns det alltså samma behov av driftsäkerhet och informationssäkerhet som i den vård som utförs på ett sjukhus men där vården istället utförs på en plats utanför regionens brandväggar. På motsvarande sätt behöver säkra tunnlar för överföring av informationen som samlas in av MT-utrustning ute i personernas hem etableras.

Slutligen finns det också i många regioner en stor andel privata utförare. Dessa har ett behov av tillgång till vissa gemensamma system och gemensam information. De har också på motsvarande sätt som övrig verksamhet inom hälso- och sjukvården krav på sig att registrera information i dessa system. Här finns således behov av att tillgängliggöra dessa system och denna information utan att exponera regionen för onödiga risker. Centralt är att i upphandlingar av denna typ av aktörer också ställa krav på tillräckliga säkerhetsnivåer i hanteringen av information och system.

Vilka förmågor krävs för att möta de regionala behoven?

Presentation av Ciscos förmågekarta för cybersäkra regioner

I det här avsnittet presenterarar vi Ciscos förslag till förmågekarta för cybersäkra regioner. Den har utformats så att de behov som kartlades i föregående avsnitt adresseras, och att det görs på ett säkert och kostnads-effektivt sätt. Likt behovsavsnittet har vi valt att presentera dessa förmågor fördelat på övergripande nivå och på verksamhetsspecifik nivå.

Säkerhetsförmågor

Exempel på verksamhetsspecifika förmågor

- Kontinuerlig övervakning av känslig data i molntjänster
- Patientdata tillgänglig för rätt roll eller person
- Begränsad informationstillgång till externa utförare
- Säker videokonsultaion
- Telefoni och larmtjänster med säkerställt hög tillgänglighet och redundans
- Säker och mobil medicinteknisk utrustning
- Säker vård på distans
- Tillgänglighet och riktighet på realtidsdata från trafiken

Exempel på förmågor för hela regionen

- Säkert distansarbete/ hybridarbete
- Skyddade enheter/ klienter
- Tillräcklig kompetens hos medarbetare och användare
- Snabb upptäckt och åtgärd av intrång
- Segmenterade och övervakade OT och IoT-enheter
- Skyddad infrastruktur
- Säker åtkomst till rätt applikationer och information
- Automatisering
- Tillhandahålla nätverk till tredje part
- Leva upp till NIS- samt PDL:s kravbild

Hela regionen

Hälso- och sjukvård
Möjliggöra vård

Hälso- och sjukvård
Utföra vård

Kollektivtrafik

Förmågor för hela regionen

Vissa säkerhetsförmågor är grundläggande och krävs i alla delar av den regionala verksamheten. Hit hör t.ex. grundläggande förmåga till skydd av infrastruktur och enheter och möjligheten att ansluta medarbetare och gästers utrustning till regionala nätverk på ett säkert sätt. Nedan har vi listat elva väsentliga förmågor som vi ser som avgörande för hela regionens it-säkerhet.

Förmåga	Beskrivning	Kategori
Skyddad infrastruktur	Den digitala infrastrukturen är skyddad mot hot både utifrån och inifrån av brandväggar, webb- och mejl-filter.	
Säkert distansarbete/hybridarbete	Regioner ska tillhandahålla både säkra anslutningar till regionens applikationer och system samt fullgoda skydd för enheter utanför den ordinarie arbetsplatsen. Distansarbete måste också kunna genomföras på ett säkert sätt via säkra anslutningar till molnbaserade system.	
Säker åtkomst till rätt applikationer och information	Oavsett hur man ansluter till nätet tilldelas användare automatiskt roller. Detta styrs av ett övergripande regelverk som bygger på information såsom plats, identitet, roll, utrustning etc. Säker åtkomst bör även säkerställas genom flerfaktorsautentisering.	
Skyddade enheter/klienter	Nätverkets enheter/klienter (t.ex. datorer och mobiltelefoner) måste skyddas för att hindra och hitta skadlig programvara. Om en klient blir infekterad behöver nätverket skyddas från vidare spridning.	
Automatisering	Automatisering av säkerhetslösningarna bidrar med effektivare processer och lägre kostnader. Automatisering kan också bidra till en mindre komplex it-miljö vilket minskar behovet av ytterligare säkerhetsåtgärder. Automatisering minskar också behovet av att nyttja kvalificerad personal för enklare arbete.	

Förmåga	Beskrivning	Kategori
	Är miljön automatiserad och standardiserad blir det också enklare att identifiera avvikelser i en it-miljö.	
Tillräcklig kompetens hos medarbetare och användare	Att kontinuerligt utbilda sin personal är en viktig del i en regions it-säkerhetsarbete för att undvika riskbeteenden hos personalen. Oftast lyckas phishing, malware och andra angreppsmetoder att penetrera ett nätverk då den anställda omedvetet släpper in angriparen genom att till exempel klicka på en länk. Detta innefattar också att säkerställa tillräcklig beredskap inför krissituationer hos medarbetare och chefer.	
Tillhandahålla nätverk till tredje part	När en region tillhandahåller nät till tredje part är den centrala förmågan att endast ge åtkomsten till det nät, system eller den information som tredje part ska ha tillgång till.	
Snabb upptäckt och åtgärd av intrång	Regionen behöver en förmåga att minska tiden mellan upptäckt och åtgärd av intrång. En förutsättning för att uppnå detta är automation och integration av centrala verksamhetskomponenter.	
Leva upp till NIS- samt PDL:s kravbild	NIS-direktivet är ett europeiskt direktiv som ställer krav på säkerhet i nätverk och informationssystem. Direktivet omfattar såväl hälso- och sjukvård som transporter. Att uppnå de högt ställda krav som finns i direktivet är således en nödvändig förmåga för hela regionen. Patientdatalagen, PDL, reglerar upprättande och korrekthet gällande patientdokumentation. Regleringen innebär strikta och höga krav på informationssäkerhet vilket i sin tur ställer stora krav på it-säkerheten.	

Förmåga	Beskrivning	Kategori
Segmenterade och övervakade OT och IoT-enheter	Regioner måste på ett säkert och stabilt sätt kunna upprätthålla kommunikation mellan centrala it-system och verksamheternas OT- och IoT-system. Den avgörande säkerhetsförmågan är att kunna segmentera OT-/IoT-systemen utan att störa verksamheten samt ha kontroll över vilka komponenter och beroenden som finns i verksamheten. En avgörande beståndsdel i det arbetet är en centraliserad drift- och säkerhetsövervakning.	

Verksamhetsspecifika förmågor

Förmåga	Beskrivning	Kategori
Telefoni och larmtjänster med säkerställt hög tillgänglighet och redundans	100% tillgänglighet i telefoni och larmtjänster behöver säkras med multipla mobila accesstjänster för att etablera fullständig redundans i anslutningarna.	
Kontinuerlig övervakning av känsliga data i molntjänster	Om molntjänster används behöver regionen ha detaljerad kontroll över vilken typ av uppgifter som placeras var. Det innebär bland annat att regionen kan förhindra att känsliga data placeras i tjänster som enligt regionens regelverk inte är tillåtna.	
Patientdata tillgänglig för rätt roll eller person	En förutsättning för att utföra vård är att rätt roll får tillgång till rätt information oavsett plats de befinner sig på. Detta styrs och regleras genom ett centralt regelverk.	
Säker och mobil medicinteknisk utrustning	MT-utrustning behöver hanteras inom segmenterade nätverk som kapslar in utrustningen. Dagens krav på mobilitet innebär att utrustningen ska kunna flyttas runt och bibehålla samma grad av segmentering.	

Förmåga	Beskrivning	Kategori
Begränsad informationsdelning med privata utförare	Oavsett hur användare ansluter till nätet ska tilldelning av roll ske automatiskt. Detta styrs av ett övergripande regelverk som bygger på information som till exempel plats, identitet, roll och utrustning. Detta gäller såväl privata utförare som de som befinner sig inom regionen. Anslutning bör dessutom kombineras med en flerfaktorsautentisering.	
Säker vård på distans (ASIH)	Vård på distans som till exempel monitorering, larm och avancerad medicinteknik behöver erhålla samma skydd som vård på en avdelning. Detta uppnås via en VPN-koppling med samma säkerhetsförmågor som på ett sjukhus. Ett exempel på en säkerhetsförmåga som behöver säkerställas även på distans är segmentering av MT-utrustning.	
Säker videokonsultation	Vid videokonsultation hanteras data enligt förutbestämda regler för att säkerställa efterlevnad av dataskyddsförordningen. Ur ett patientsäkerhetsperspektiv behöver tillräcklig kvalitet på video- och talkvaliteten säkras.	
Tillgänglighet och riktighet på realtidsdata från trafiken	Informationsöverföring sker via en krypterad tjänst som är mobil, tillgänglig och tillförlitlig. Tjänsten ska vara oberoende av extern aktör eller tjänst.	

Användarfall och lösningar för en säker region

När vi nu redogjort för viktiga regionala behov och förmågor, vill vi ge några exempel på hur dessa konkret kan hanteras genom en uppsättning av våra lösningar. Vi är medvetna om att ingen region är ett blankt papper och att det finns många sätt att adressera de säkerhetsutmaningar som finns. Här ger vi dock vår syn på hur Ciscos lösningar kan struktureras från grunden.

Vi har valt att i det här kapitlet visualisera och beskriva Ciscos lösningar för fyra typiska regionala behov. Dessa demonstrerar också på ett bra sätt vad vi ser som en ändamålsenlig uppsättning för en säker region.

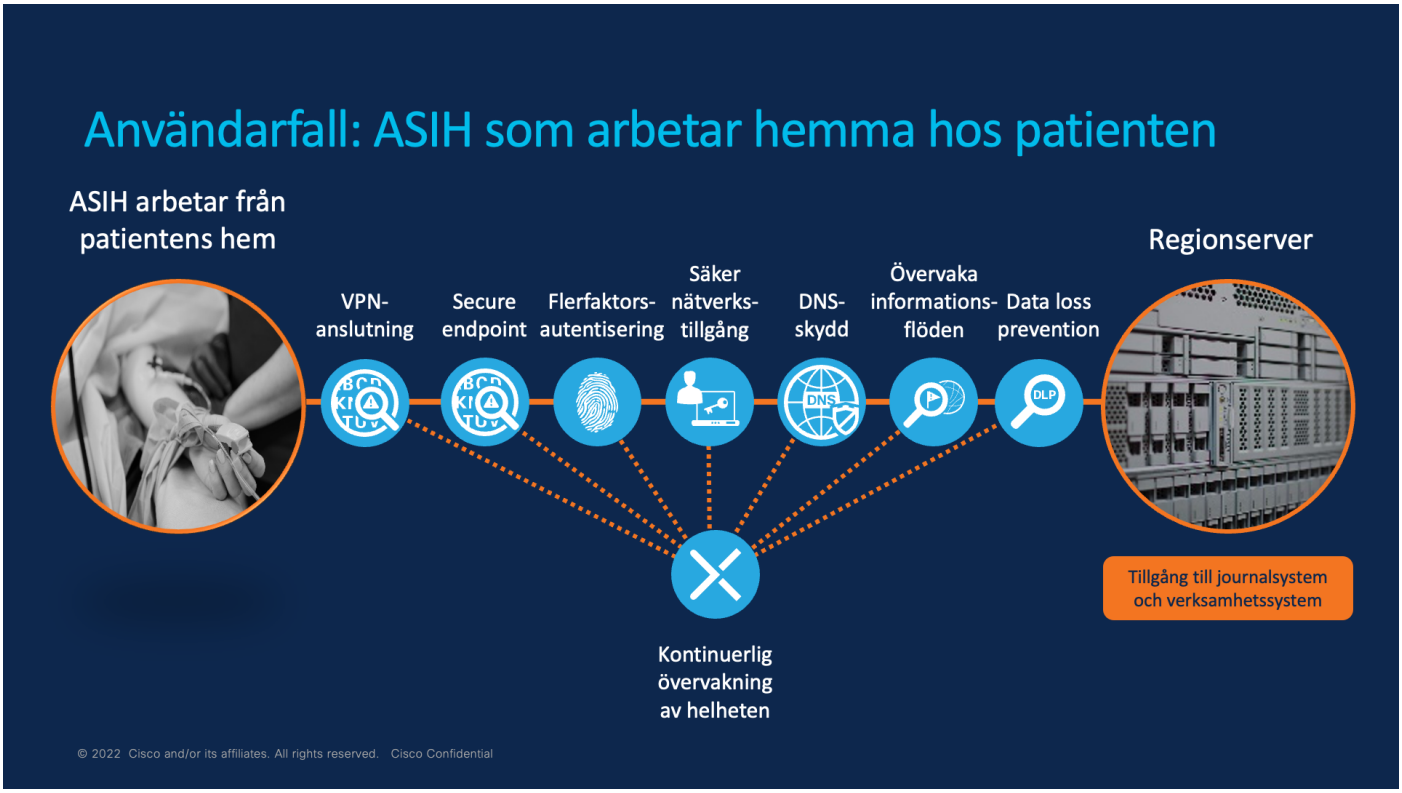
Användarfall och lösningar för vårdpersonalens vardag på ett sjukhus

Som beskrivits i behovs- och utmaningskapitlen är vårdpersonal helt och hållet beroende av en välfungerande och smidig tillgång till rätt system och medicinteknisk utrustning under sitt dagliga arbete. Detta behöver också ske på ett säkert sätt. Här beskriver vi ett användarfall för en vårdpersonals vardag på ett sjukhus. Vi särskiljer mellan system som ligger på insidan av den regionala it-miljön och utanför.

- För att vårdpersonalen ska kunna komma åt de verksamhetssystem och journalsystem som de behöver för sitt arbete måste deras enheter (dator/mobil/surfplatta) anslutas till ett nätverk (ofta sjukhusets egna nätverk). Oavsett var personalen ansluter sig har enheten redan ett grundskydd mot skadlig programvara, genom det som brukar benämnas som *Endpoint security*. Ciscos lösning för detta heter *Cisco Secure Endpoint*. Denna lösning svarar mot förmågan **Skyddade enheter/klienter**.
- För att få tillgång till den digitala miljön som innehåller patientinformation är det lagkrav på att detta ska föregås av stark autentisering[23]. Detta sköts vanligtvis inom vården genom multifaktorsautentiseringstjänsten SITHS som tillhandahålls av Inera men som är lätt integrerat i Ciscos lösningar. Lösningen svarar mot förmågan **Säker åtkomst till rätt applikationer och information**.
- För att sedan ansluta till regionens nätverk krävs säker nätverkstillgång. Ciscos lösning för detta heter *Cisco Identity service engine (ISE)*. Detta görs för att säkerställa att vårdpersonalen verkligen har rätt att ta del av den efterfrågade informationen, genom nätverkssegmentering av användarna. Lösningen svarar mot förmågan **Säker åtkomst till rätt applikationer och information**.
- För vårdpersonalens mail-program krävs särskilt skydd mot skadliga phishing-försök, alltså säker e-post. Behovet kan fyllas genom de funktioner som finns tillgängliga i Ciscos tjänst *Cisco Secure Email* och svarar mot förmågan **Skyddade enheter/klienter**.
- För att vårdpersonalen ska kunna ansluta säkert till internet krävs s.k. DNS-skydd. Genom att säkra DNS-lagret blockeras fientliga domäner, IP-adresser och moln-applikationer redan innan en uppkoppling skett. Ciscos lösning för detta heter *Cisco Umbrella*. *Umbrella* kan också användas för att övervaka att information inte

distribueras till olämpliga molntjänster. Lösningen svarar mot förmågorna **Säker åtkomst till rätt applikationer och information**, **skyddade enheter/klienter** och **Övervakning av känsliga data i molntjänster**.

- För att skydda nätverket och informationen ytterligare är det centralt att i realtid övervaka informationsflödena för att kunna agera på möjliga hot. Detta görs genom Ciscos lösning *Network detection and response (NDR)* som kontinuerligt monitorerar och analyserar alla flöden av data i nätverket för att generera en baslinje för normalt nätverksbeteende. När sedan misstänkta nätverksmönster som avviker från baslinjen identifieras så notifieras säkerhetspersonalen om möjliga säkerhetshot i it-miljön. Denna lösning svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.
- Information är som nämnts i behovskapitlet centralt för att kunna upprätthålla en fungerande hälso- och sjukvård. Mycket av den information som hanteras inom vården är också av känslig karaktär och får inte hamna i orätta händer. För att säkerställa att så inte sker rekommenderar Cisco sin lösning Cisco *Data loss prevention (DLP)*. DLP används för att identifiera känslig information som inkluderats i digital kommunikation såsom exempelvis e-post. Om exempelvis en journal exporteras och skickas via e-post till en okrypterad e-postadress kan DLP identifiera detta och hindra att så sker. Lösningen svarar mot förmågorna **Säker åtkomst till rätt applikationer och information** och **Patientdata tillgänglig för rätt roll eller person**.
- Regionen bör också ha en central förmåga för att övervaka helheten som kan användas exempelvis av ett Security operations center (SOC). För detta rekommenderas lösningen *Cisco SecureX* som ger organisationen en överblick av hela regionens it-säkerhetslösningar och it-infrastruktur. Lösningen svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.



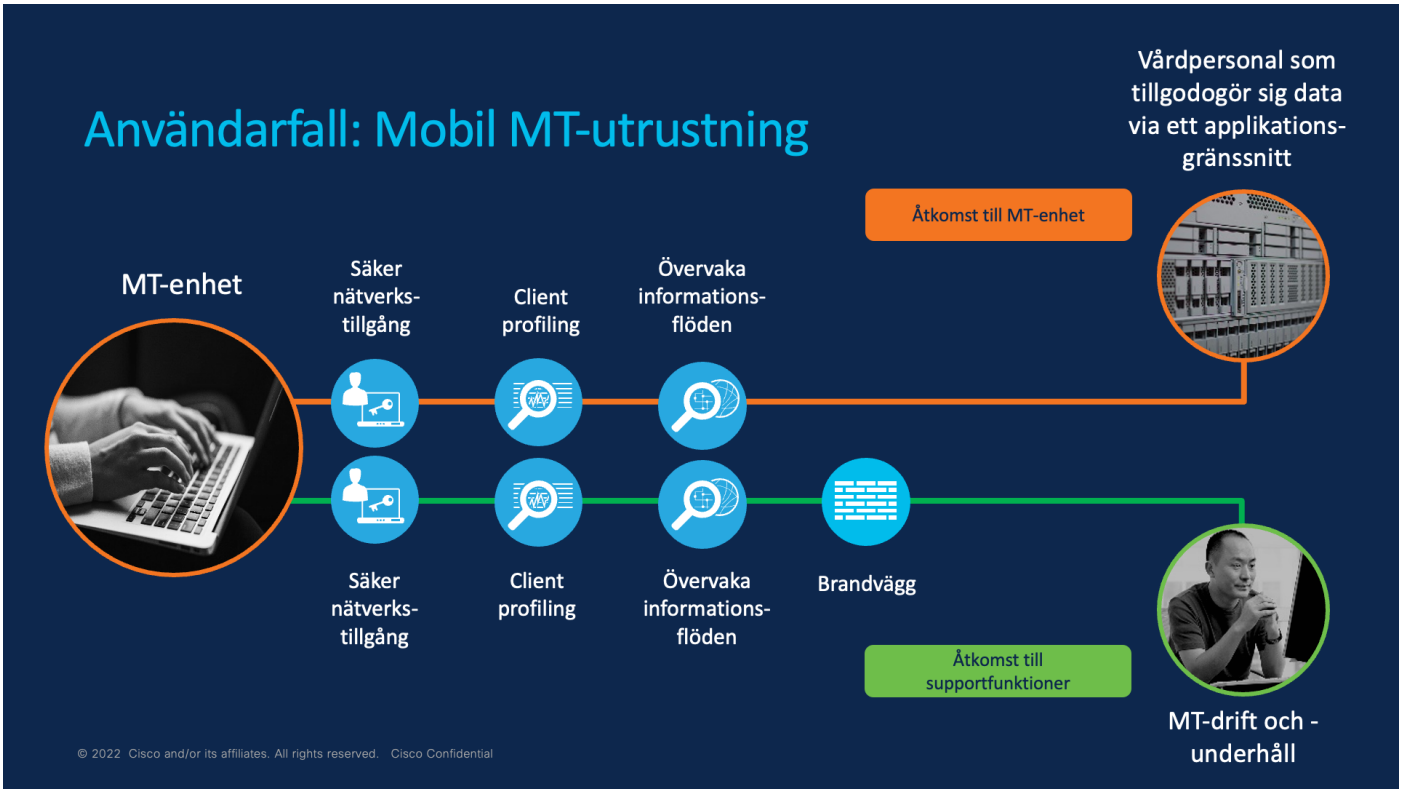
Användarfall och lösningar för ASIH som arbetar hemma hos patienten

Som beskrivits i behovskapitlet utförs alltmer vård utanför regionens lokaler. Genom att ASIH har blivit en alltmer vanligt förekommande vårdform behöver också it-säkerheten garanteras oavsett var vården utförs, som till exempel i patientens hem. I detta användarfall används ASIH som exempel, men där den tekniska lösning som beskrivs kan användas i all regional vård som sker i hemmet eller på annan plats.

- För att ASIH-personalen ska komma åt det regionala nätverket används ofta en VPN-tunnel. Denna uppkoppling garanteras genom lösningen *Cisco+ Secure Connect*. Detta ger personalen tillgång till de system och den information de behöver för att utföra sitt arbete även hemma hos patienten. Lösningen svarar mot förmågan **Säker vård på distans**, **Säkert distansarbete/hybridarbete** och **Säker åtkomst till rätt applikationer och information**.
- Också här krävs ett grundläggande skydd av ASIH-personalens enhet (dator/mobil/surfplatta/MT-enhet) när den ansluter till ett nätverk som inte är regionens. Oavsett var personalen ansluter sig har enheten redan ett grundskydd mot skadlig programvara, genom det som brukar benämnas som Endpoint security. Ciscos lösning för detta heter *Cisco Secure Endpoint*. Denna lösning svarar mot förmågan **Skyddade enheter/klienter**.
- På motsvarande sätt som för övrig vårdpersonal krävs också att ASIH-personalen identifierar sig med flerfaktorsautentisering. Även här görs detta med SITHS. Denna lösning svarar mot förmågan **Säker vård på distans** och **Säker åtkomst till rätt applikationer och information**.
- Väl ansluten till det regionala nätet rekommenderas också här *Cisco ISE*. Detta för att säkerställa att den anslutna användaren får rätt behörigheter. Lösningen svarar mot förmågan **Säker åtkomst till rätt applikationer och information**.
- För ASIH-personal rekommenderas också att lösningar för DNS-skydd implementeras. Även här rekommenderas lösningen *Cisco Umbrella*. Lösningen svarar mot förmågorna **Säker åtkomst till rätt applikationer och information**, **skyddade enheter/klienter** och **Övervakning av känsliga data i molntjänster**.
- När vårdpersonalen utför vård bortom sjukhusbyggnaderna blir det särskilt viktigt att i realtid övervaka informationsflödena för att kunna agera

på möjliga hot. Detta görs även här genom Ciscos lösning *Network detection and response (NDR)*. Denna lösning svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.

- När personalen är borta från regionens lokaler blir det ännu viktigare att säkerställa att säkra kommunikationsmetoder används. Så även här rekommenderas användning av *Cisco Data loss prevention (DLP)*. Lösningen svarar mot förmågorna **Säker vård på distans** och **Patientdata tillgänglig för rätt roll eller person**.
- Regionen bör också i relation till detta användarfall ha en central förmåga för att övervaka helheten som kan användas exempelvis av ett Security operations center (SOC). För detta rekommenderas lösningen *Cisco SecureX* som ger organisationen en överblick av hela regionens it-säkerhetslösningar och it-infrastruktur. Lösningen svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.



Användarfall och lösningar för mobil MT-utrustning på ett sjukhus

Som beskrivits i såväl utmanings- som behovskapitlen utgör MT-utrustning en av de mest riskabla attackvektorerna i ett sjukhus verksamhet. Således bör den första prioriteringen vara att avskilja särskilt känsliga enheter från resterande delar av det nätet. Genom sådan segmentering kan enskilda riskbedömningar göras, för att tillåta internetåtkomst åt system där det bedöms riskfritt eller nödvändigt, såsom leverantörers servicesystem eller regionens betrodda driftcentral.

- För att förhindra att felaktig kommunikation sker mellan MT-enheter och nätet sker först en nätverkssegmentering. Här rekommenderas användning Ciscos lösning *Cisco Identity service engine (ISE)*. Med detta verktyg spärras åtkomsten till MT-enheter för obehöriga och en kontroll över vilken typ av kommunikation MT-enheten får ägna sig åt med andra enheter och resten av nätverket etableras. När detta sker kan man också sätta upp så att MT-enheten på ett sömlöst sätt kan förflyttas i lokalerna utan att sluta fungera. Lösningen svarar mot förmågan **Skyddad infrastruktur**, **Säker åtkomst till rätt applikationer och information** och **Säker och mobil medicinteknisk utrustning**.
- För att ytterligare säkra att inga obehöriga intrångsförsök sker inom den känsliga infrastrukturen rekommenderas Ciscos lösning *AI endpoint analytics*. Den används för att detektera och klassificera MT-utrustning under olika rubriker såsom typ, modell, tillverkare och operativsystemstyp. På detta sätt kan man sedan använda dessa rubriker för att sätta upp regler och policies för sitt nätverk. Lösningen används också för att med hjälp av maskininlärning övervaka vad som händer ute i MT-miljön. Denna lösning svarar mot förmågan **Snabb upptäckt och åtgärd av intrång** och **Säker och mobil medicinteknisk utrustning**.
- När MT-enheter integreras med nätverk och andra system ökar konsekvenserna av ett eventuellt framgångsrikt angrepp. För kontinuerlig driftövervakning och effektiv hotdetektering rekommenderas lösningen *Cyber Vision*. Produkten är speciellt utvecklad för att anställda med ansvar för MT-enheter ska kunna säkerställa driftkontinuitet, motståndskraft och säkerhet. Lösningen svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.

- Slutligen behöver också utrustningen skyddas med en brandvägg. Vi rekommenderar i det här fallet *Cisco next generation firewall*. Lösningen svarar mot förmågan **Skyddad infrastruktur** och **säker och mobil MT-utrustning**.

Lösningarna som beskrivs ovan är alla viktiga pusselbitar som tillsammans bidrar till den regionala förmågan **Säker och mobil medicinteknisk utrustning** och regioners förmåga att **Leva upp till NIS samt PDL:s kravbild**.

Användarfall och lösningar för säker fordonskommunikation

Inom kollektivtrafiken har det blivit väldigt vanligt förekommande att nyttja olika IoT-lösningar i och kring fordonen. Detta innefattar bland annat lösningar för positionering, kameraövervakning och biljetthantering. All denna utrustning behöver alltså övervakas för att säkerställa såväl att den fungerar som att den är skyddad från angrepp.

- Den fordonsoptimerade routern ansluter flera åtskilda lokala nät som fordonskontroll, publik WiFi och betalfunktioner. Vi rekommenderar i detta fall *Cisco IR1800*.
- Den centrala utrustningen skyddas med en brandvägg. Vi rekommenderar i det här fallet *Cisco next generation firewall*. Lösningen svarar mot förmågan **Skyddad infrastruktur** och **säker och mobil MT-utrustning**.
- För att koppla upp utrustningen till regionens nätverk krävs säker nätverkstillgång. Ciscos lösning för detta heter *Cisco Identity service engine (ISE)*. Detta görs för att säkerställa att enheterna verkligen har rätt att ta del av den efterfrågade informationen, genom nätverkssegmentering. Lösningen svarar mot förmågan **Säker åtkomst till rätt applikationer och information**.
- För att skydda nätverket och informationen ytterligare är det centralt att i realtid övervaka informationsflödena för att kunna agera på möjliga hot. Detta görs genom Ciscos lösning *Network detection and response (NDR)* som kontinuerligt monitorerar och analyserar alla flöden av data i nätverket för att generera en baslinje för normalt nätverksbeteende. När sedan misstänkta nätverksmönster som avviker från baslinjen identifieras så notifieras säkerhetspersonalen om möjliga säkerhetshot i it-miljön. Denna lösning svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.
- För att ytterligare säkra att inga obehöriga intrångsförsök sker inom den känsliga infrastrukturen rekommenderas Ciscos lösning *AI endpoint analytics*. Den används för att detektera och klassificera IoT-utrustning under olika rubriker såsom typ, modell, tillverkare och operativsystemstyp. På detta sätt kan man sedan använda dessa rubriker för att sätta upp regler och policies för sitt nätverk. Lösningen används också för att med hjälp av maskininlärning övervaka vad som händer ute i MT-miljön. Denna lösning svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.

Lösningarna som beskrivs ovan är alla viktiga pusselbitar som tillsammans bidrar till den regionala förmågan **Tillgänglighet och riktighet på realtidsdata från trafiken** och regioners förmåga att **Leva upp till NIS samt PDL:s kravbild**.

Vill du veta mer?

Vi hoppas att den här skriften har bidragit till att informera och inspirera dig. Vill du veta mer om hur Cisco kan hjälpa dig i utformningen av en säker region?

Kontakta

Henrik Bergqvist
Sales Manager, Security
hbergqvi@cisco.com
070-544 96 22

Anders Johansson
Sales Manager, Public Sector
andjohan@cisco.com
070-530 08 50

Maria Lawestig
Sales Manager, Public Sector
mlawesti@cisco.com
070-279 7003

Referenser

1. Cisco – säker kommun
   Länk: https://www.cisco.com/c/dam/global/sv_se/home/pdf/saker-kommun-cisco.pdf

2. Vad tycker väljarna – Viktigaste politiska frågan
   Länk: https://novus.se/valjarforstaelse-arkiv/kategori/viktigaste-politiska-fragan/2022/

3. Informationssäkerhet vs it-säkerhet – vad är vad?
   Integritetsskyddsmyndigheten
   Länk: https://www.imy.se/blogg/informationssakerhet-vs-it-sakerhet--vad-ar-vad/

4. Future of Secure Remote Work Report (2021) Cisco.
   Länk: https://www.cisco.com/c/en/us/products/security/future-secure-remote-work-report.html

5. Hackers love retail. The average cost per lost or stolen item. (2018) Cisco
   Länk: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/retail-security-infographic.pdf

6. Om cyberkriget kommer (2020) P1 Konflikt
   Länk: https://sverigesradio.se/avsnitt/1428309

7. 187 regioner drabbade av utpressningsvirus (2017) SVT
   Länk: https://www.svt.se/nyheter/inrikes/187-regioner-drabbade-av-utpressningsvirus

8. Anonymous declared a ‘cyber war’ against Russia
   Länk: https://www.cnbc.com/2022/03/16/what-has-anonymous-done-to-russia-here-are-the-results-.html

9. Ideologically motivated computer hacking
   Länk: https://rusi.org/publication/ideologically-motivated-computer-hacking

10. 2021 Cyber security threat trends (2021) Cisco
    Länk: https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

11. Regionernas kostnader och intäkter Ekonomifakta
    Länk: https://www.ekonomifakta.se/Fakta/Offentlig-ekonomi/kommunal-ekonomi/landstingens-kostnader-och-intakter/

12. IT-kompetensbristen (2020) TechSverige
    Länk: https://www.techsverige.se/2020/12/it-kompetensbrist/

13. SOU 2021:1: Säker och kostnadseffektiv it-drift (2021) Regeringskansliet
    Länk: https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/01/sou-20211/

14. SOU 2021:1: Säker och kostnadseffektiv it-drift (2021) Regeringskansliet
    Länk: https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/01/sou-20211/

15. Cisco trust center
    Länk: https://www.cisco.com/c/en/us/about/trust-center.html

16. Hälso- och sjukvård på IMY.se
Länk: https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/vard/

17. Vad är WiFI-lyftet? (2021) Cisco
Länk: https://www.cisco.com/c/sv_se/solutions/industries/education.html

18. 2021 Cyber security threat trends (2021) Cisco
Länk: https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

19. Myndigheten för samhällsskydd och beredskap, Det robusta sjukhuset,
Länk: https://www.msb.se/sv/publikationer/den-robusta-sjukhusbyggnaden---2021--en-vagledning-for-driftsakra-sjukhusbyggnader/

20. Information om NIS-direktivet (2022) MSB
Länk: https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/

21. Inspektion för vård och omsorg, Det nya NIS 2-direktivet
Länk: https://www.ivo.se/yrkesverksamma/anmal-brister-och-risker/incidenter-i-informationssakerhetssystem-nis/det-nya-nis-2-direktivet/

22. Gartner Glossary
Länk: https://www.gartner.com/en/information-technology/glossary/operational-technology-ot

23. HSLF-FS 2016:40 Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården, Kapitel 4 §11


CISCO