Säker kommun

Ciscos vägledning för säkra kommuner

Innehåll

Sammanfattning

En stor del av Sveriges kommuner har Cisco som leverantör för någon del av sin it-miljö. Genom dessa kundrelationer har vi fått en unik inblick i vilka säkerhetsutmaningar svenska kommuner 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 som finns. Utbildningsmaterial med fokus på it-säkerhet är ofta skrivet på ett tekniskt fackspråk och är inte helt lätta att ta till sig.

Vi har därför tagit fram detta whitepaper som innehåller en beskrivning av hur vi ser på it-säkerhet i svenska kommuner. Frågor som vi kommer ge vår syn på är t.ex. vilka hot och utmaningar som är specifika för den kommunala 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, och ansvarar för och samordnar it hos er i kommunen, men det ska också ses som en viktig pusselbit för att bidra med kunskaper på området till kommunala beslutsfattare. Här nedan ser du en summering av de olika avsnitten och dess innehåll.

It-hot och sårbarheter	Extern hotbild mot svenska kommuner Metoder och angreppsätt Var finns sårbarheter i det kommunala nätverket?
Generella kommunala it-utmaningar	Generella utmaningar i kommunernas it-säkerhetsarbete Utmaningar i hantering av personuppgifter i molnet
Kommunala behov av it-säkerhet	Vilka behov har kommuner av it-säkerhet? Hela kommunens behov Verksamhetsspecifika behov
Förmågor för att trygga it-miljön	Vilka förmågor krävs för att möta de kommunala behoven? Förmågor för hela kommunen Verksamhetsspecifika förmågor
Ciscos referens-arkitektur	Exempel på Ciscos referensarkitekturer för en säker it-miljö

Om Ciscos vägledning för säkra kommuner

I ett globalt perspektiv har Sverige kommit mycket långt på sin digitaliseringsresa. Svenska hushåll och företag är snabba att ta till sig och använda nya digitala tjänster och verktyg. Den nödvändiga it-infrastrukturen som behövs (både fasta bredbandslösningar och trådlös teknik) har byggts ut kraftigt och även om mycket kvarstår att göra så finns en bred enighet hos beslutsfattare om digitaliseringens nödvändighet och nytta. Allt detta bidrar till att Sverige de senaste åren har rankats bland de fem bästa länderna i EU:s årliga digitaliseringsindex, DESI[1].

Den kommunala verksamheten är grunden i det svenska samhällsbygget och utgör en påtaglig del av den offentliga sektorn. Varje dag går hundratusentals vuxna och barn till arbetsplatser, skolor eller andra verksamheter som drivs eller överses av kommuner. Även landets kommuner har gjort stora satsningar på digitala tjänster och it-system som successivt har gjort verksamheterna både mer effektiva och målgruppsorienterade.

Men i takt med att allt större delar av den kommunala verksamheten digitaliserats har också beroendet av att medarbetarna och kommuninvånarna har tillgång till rätt system och rätt information ökat. Den ökade delningen av information genom digitala kanaler skapar också nya säkerhetsutmaningar. Externa aktörer med olika motiv har intresse av att antingen få tillgång till information och system de inte har rätt till eller på andra sätt störa verksamheten.

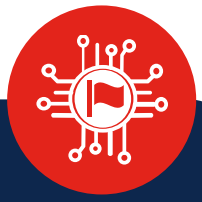
På grund av den breda och diversifierade verksamhet som bedrivs har det länge funnits en god förståelse ute i Sveriges kommuner för behovet av en hög it-säkerhet. Ciscos upplevelse är att denna förståelse också har ökat de senaste åren, i takt med att stora cyberattacker mot både kommunal verksamhet och mot andra typer av organisationer fått stor uppmärksamhet medialt.

En stor del av Sveriges kommuner har valt Cisco som leverantör inom it-säkerhetsområdet. Detta gör att vi över åren fått en unik inblick i de it-säkerhetsmässiga behov som finns ute i svenska kommuner och vilka utmaningar de står inför. I de kontakter vi har med kommunrepresentanter både på beslutsfattarnivå och operativ nivå, har vi sett en tydlig efterfrågan på vägledning i frågan om hur kommuner bör agera för att skydda sina system och sin information mot yttre hot.

För att göra det lättare att skapa en överblick över den typiska kommunala it-miljön och vilka behov och förmågor som kan kopplas till denna har vi på Cisco Sverige tagit fram **Ciscos vägledning för säkra kommuner**.

Målgruppen för denna skrift är huvudsakligen it-chefer, it-säkerhets-chefer och CIO:er som funderar över it-säkerhet i en kommunal kontext. Vi tror också att skriften kan vara av intresse för kommundirektörer 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 utmaningar som är specifika för just kommunala organisationer, vilka behov som finns ute i kommuners olika verksamheter, vilka förmågor kommunen behöver bygga upp för att klara dessa behov och avslutas med ett kapitel som beskriver möjliga referensarkitekturer för vanliga kommunala utmaningar. Materialet baseras på Ciscos långvariga kundkontakt med ett stort antal svenska kommuner och vår ambition är här att fånga både dagens och morgondagens kommunala 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 kommuner

Antalet cyberattacker mot europeiska företag och organisationer har de senaste åren ökat påtagligt[2]. Den externa hotbilden är komplex och anledningarna till att angreppen ökar är mångfacetterade. Men orsaker 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[3]. I verksamheter som kommunala omsorgsförvaltningar kan det till och med i värsta fall leda till dödsfall. 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[4]. 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 hotfulla 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 företagsspionerі 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 säkerhets-tjänst men kan också ha lösare kopplingar till staten. Även om Sverige inte

är i direkt konflikt med dessa länder kan statliga aktörer försöka forcera kommunala 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 den kommunala verksamheten.

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 kommuner eller myndigheter utpressas att köpa tillbaka den från angriparen[5]. 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 också utföra uppdrag för staten 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[6]. Inte sällan rör det sig om ideologiskt drivna personer som ofta besitter stor kunskap om olika angreppsmetoder[7].

Metoder och angreppsätt

Oavsett vilka bakomliggande motiv fientliga aktörer har till att vilja ha tillträde till kommunala it-system 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[8]. Ett av de vanligaste motiven bakom phishing-attacker är att försöka få tag i inloggningsuppgifter till verksamhetssystem, 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 programvaran 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.

Var finns sårbarheter i det kommunala nätverket?

Enheter anslutna till nätverket

Ett nätverk är oftast som allra känsligast för angrepp genom de enheter (endpoints) som ansluts. Med enheter menas all utrustning som kan anslutas till en organisations nätverk (t.ex. mobiltelefoner, datorer eller surfplattor). Sådana enheter har ofta mindre avancerade säkerhetsskydd än organisationens nätverksutrustning, vilket gör att de blir lockande måltavlor. Här ser vi att äldre enheter, utan modernare typer av inbyggda skydd, blir särskilt sårbara. Om en angripare får tillträde till en enhet som används av en medarbetare på en central position i organisationen kan denna snabbt vittjas på verksamhetskritisk information.

Många användare har även sitt konto med användarbehörighet kopplade till sin enhet. Ett intrång i enheten innebär därför att en angripare potentiellt kan få tillgång till känslig information eller sekretesskyddade system. När en angripare väl tagit över en enhet kan den dessutom fortsätta att försöka ta över andra enheter inifrån organisationens nätverk. Att skydda enheter i kommunala nätverk kompliceras av att många användare tar med sig egna enheter (t.ex. datorer). Dessa saknar skyddsprogram eller inställningar som nätverksägarens enheter har installerade och kan därför utgöra en potentiellt svag länk i säkerhetskedjan.

Bristande autentiseringsrutiner

Att en användare autentiserar sig innebär att den bekräftar sin identitet mot ett system för att beviljas åtkomst. De flesta kommuner har ett så kallat Active Directory (AD) i vilket en användare tilldelas behörigheter. De lösningar som finns för autentisering av uppgifter utvecklas ständigt och det är inte ovanligt att användare exempelvis tvingas välja ett lösenord med en viss komplexitet och att återkommande byta lösenord. Många kommuner strävar också efter att etablera så kallad Single Sign On (SSO) som innebär att du enbart behöver logga in en gång för att få tillgång till de verksamhetssystem du har behörighet till.

Det blir idag allt vanligare att kommuner använder sig av tvåfaktorsautentisering. Precis som namnet antyder innebär tvåfaktorsautentisering att användare har tillgång till två metoder för identifikation. Oftast handlar det om ett lösenord och en enhet, t.ex. som vid användandet av mobilt Bank-ID på en smartphone.

Om en kommun inte har implementerat tvåfaktorsautentisering finns tydliga sårbarheter i den kommunala it-miljön. Det är relativt vanligt förekommande att användare har samma lösenord i flera olika sammanhang och genom detta kan en person vars privata konton hackats även bli en belastning för de kommunala it-miljöerna. Som vi tidigare konstaterat utgör phishing-attacker 90 % av alla angreppsförsök på organisationers nätverk. Av dessa är 83% försök att komma över autentiseringsuppgifter som t.ex. lösenord.

Den mångsidiga och uppdelade verksamheten

Kommuner är oerhört diversifierade verksamheter. Det är få företag i Sverige som inom ramen för sin tjänsteleverans har alltifrån att tillhandahålla utbildning, till att förvalta kritisk infrastruktur och att låna ut böcker. Allt det sker inom ramen för samma organisation i svenska kommuner. Detta gör kommunen till en fantastisk organisation, men det gör också att den blir svårare att skydda utifrån ett it-säkerhetsperspektiv.

Bilden kompliceras ytterligare av att många kommuner delar upp it-relaterade inköp i en nätverksdel och en verksamhetsdel. Nätverksinvesteringar sker nästintill alltid genom centrala upphandlingar, medan verksamheterna i vissa fall tenderar att upphandla enheter som datorer eller smartphones lokalt. Det är inte ovanligt att olika verksamheter upphandlar lösningar med olika tekniska standarder som kräver specialanpassade integrationslösningar. Detta skapar ytterligare svårigheter i en redan komplex organisatorisk miljö.

Generella utmaningar i kommunernas it-säkerhetsarbete

Ciscos upplevelse är, som tidigare nämnts, att arbetet med it-säkerhet i svenska kommuner under de senaste åren blivit allt högre prioriterat. Samtidigt ser vi också att det finns ett antal utmaningar med it-säkerhetsarbetet ute i kommunerna. Vi har valt att sammanställa det som vi ser som de största utmaningarna i tre övergripande områden; ekonomiska, kompetensmässiga och organisatoriska utmaningar. 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.

Ekonomiska utmaningar

De ekonomiska förutsättningarna i många svenska kommuner är ofta relativt pressade. Sveriges kommuner och regioner (SKR) har under ett stort antal år påtalat den demografiska utmaningen som handlar om att andelen äldre ökar i snabbare takt än den arbetsföra befolkningen[9]. Samtidigt är skillnaderna mellan svenska kommuner väldigt stora och många, i huvudsak mindre glesbygdskommuner, har särskilt ansträngda budgetar.

Samtidigt är ett välfungerande it-säkerhetsarbete inte nödvändigtvis billigt vilket delvis har att göra med att kompetens inom området är en bristvara. Och som med alla frågor som handlar om beredskap ser budgetposten enbart ut att kosta pengar så länge den inte kommer till användning. Det finns därför en överhängande risk att man bygger upp en löpande säkerhetsskuld i verksamheten. Med säkerhetsskuld syftar vi på situationer där man förlitar sig på system som är föråldrade, avskrivna eller inte ordentligt underhållna av budgetskäl. Denna skuld blir med tiden en säkerhetsrisk. Sådana säkerhetsrisker blir lockande mål för externa angripare om de inte åtgärdas. Att åtgärda dessa risker kan nedprioriteras vid budgetering om ingen högprofilerad incident har inträffat i närtid.

Därav kan det vara utmanande för CIO:er och it-säkerhetsansvariga att argumentera för varför it-säkerhetslösningar är ”viktigare” än fler lärare eller ett nytt äldreboende. Det går också att argumentera för att de långa budgetcykler som är aktuella i kommunala organisationer gör det särskilt svårt att hantera en så pass snabbrörlig process som it-säkerhet.

Det som skiljer it-säkerhetsområdet från andra områden är just det att om ett angrepp lyckas kan kostnaderna såväl i pengar som i mänskligt lidande bli extremt påtagliga. Vår egen undersökning visar att 53% av alla cyber-attacker resulterar i kostnader på 5 miljoner kronor eller mer[10].

Kompetensmässiga utmaningar

En påtaglig utmaning när det kommer till it-säkerhet är graden av kompetens. Denna utmaning är tudelad; det handlar dels om en ojämnt fördelad digital kompetens, dels om bristen på spetskompetens.

Inom ramen för nästan alla typer av organisationer är den digitala kompetensen hos medarbetarna ojämnt fördelad. Kommunala organisationer 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 eller har använt 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[11]. Och givet de budgetmässiga begränsningar som finns i många kommuner kan man också ha svårt att stå sig i konkurrensen om arbetskraften. Detta kan i sin tur leda till att it-säkerhetsroller står obemannade under lång tid vilket i sig kan bli en säkerhetsrisk.

Organisatoriska utmaningar

I vissa kommuner finns också ett antal organisatoriska utmaningar. Detta handlar i huvudsak om att de delar av organisationen som har it-säkerhetsrelaterade ansvar inte nödvändigtvis är synkroniserade. Ett tydligt exempel är att den delen av organisationen som ansvarar för medarbetarnas klienter inte nödvändigtvis har ett tätt samarbete med de som arbetar med kommunens nät. Detta får utifrån ett it-säkerhetsperspektiv effekten att sårbarheter kan skapas som i sin tur kan nyttjas av fientliga aktörer.

En tydlig riskfaktor som vi identifierat i relation till kommunala aktörer är också att det ofta finns ett antal kommunala bolag kopplade till kommunen. I vissa fall har vi också sett att dessa inte nödvändigtvis hanteras på samma sätt som resten av kommunen vilket kan leda till it-säkerhetsmässiga utmaningar. En splittrad it-miljö leder till förlängda processer för att upptäcka och möta hot. Målbilden bör i stället vara integrerade säkerhetslösningar, där brandvägg, klientskydd och mail kan övervakas centralt. Sådana plattformar leder till bättre översyn och enklare och effektivare möjligheter att stoppa intrångsförsök.

Utmaningar i hantering av personuppgifter i molnet (Schrems II)

I flera år har debatten om hur personuppgifter kan hanteras digitalt av svenska myndigheter, kommuner och regioner 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 kommuner 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 data till olika intressenter, samarbeta med externa parter och att snabbt kunna ställa om verksamheter vid förändrade förutsättningar[12].

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[13].

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 data-skyddsstandarder kan uppfyllas och ”i huvudsak likvärdigt” skydd kan tillhandahållas.

Vilka behov har kommuner av it-säkerhet?

I detta kapitel kommer vi att beskriva vår syn på de it-säkerhetsmässiga behov som finns kopplade till den kommunala it-miljön. Även om Sveriges 290 kommuner 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 kommunala behov. Vi presenterar också ett antal verksamhetsspecifika behov som är uppdelade i verksamhetsområdena utbildning och barnomsorg, omsorg och stöd, VA och energi och fastigheter och IoT. Skälet till att vi valt att lyfta fram just dessa områden är att vi identifierat it-säkerhetsspecifika utmaningar inom dem.

Behovsbeskrivningen utgår ifrån fyra verksamhetsspecifika kategorier. Dessa är utbildning och barnomsorg, omsorg och stöd, VA och energi och fastigheter och IoT. Utöver verksamhetskategorier har vi även identifierat en rad övergripande it-säkerhetsbehov, som återfinns i stora delar av den kommunala verksamheten, och som summeras i kategorin hela kommunens behov.

Hela kommunens behov

Den kommunala verksamheten är oerhört diversifierad men vår erfarenhet är att de it-säkerhetsmässiga behoven för stora delar av verksamheten ändå ser relativt likartade ut oavsett vilken verksamhet som berörs. Främst handlar det om att på ett säkert sätt tillhandahålla verktyg som underlättar och stödjer hela kommunen 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 kommunal it-miljö behöver tillgodose.

Att relevant lagstiftning följs

Kommuner 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. patientdatalagen, hälso- och sjukvårdslagen, socialtjänstlagen och personuppgiftslagen) som reglerar hur en kommun får hantera känslig information. Gemensamt för samtliga av dessa lagstiftningar är att de ställer krav på kommunen att hantera data på ett sådant sätt att enbart personer som behöver ha tillgång till information, ska få det. Dataskyddsförordningens grundläggande principer summerar det kommunala behovet på ett bra sätt[14].

Principerna innebär bland annat att en personuppgiftsansvarig verksamhet:

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- ska se till att personuppgifterna är riktiga
- ska radera personuppgifterna när de inte längre behövs
- ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
- ska kunna visa att den lever upp till dataskyddsförordningen och hur den gör det.

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:

- Kommunen behöver kunna tillgängliggöra information mellan olika verksamheter (t.ex. måste verksamhetsansvariga kunna få tillgång till centrala ekonomisystem).
- För att relevant lagstiftning ska följas finns även ett behov att säkerställa att bara behöriga personer har tillgång till känslig information i de kommunala 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 kommunen att system och program kommunicerar med varandra för att tillgängliggöra och säkra information i korrekt ordning. En person som byter befattning i staden ska t.ex. inte kunna tillgå samma verksamhetssystem som tidigare, om inte det är nödvändigt för den nya yrkesrollen.

Stabil och säker nättillgång i kommunens lokaler

Som tidigare nämnts har många kommunala 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 kommunens lokaler. Samtidigt har ett skifte skett mot en digital miljö som alltmer fokuserar på bärbara enheter. I en kommunal kontext innefattar det alltifrån att möjliggöra nättillgång för elever i skolorna till öppna nät på biblioteken till att medarbetarna på ett smidigt sätt kan arbeta. Denna leverans har således blivit en grundförutsättning för att möjliggöra kommunens samtliga verksamheter. Det handlar dels om ett behov av att säkerställa att nättillgången inte utgör en accesspunkt för att penetrera kommunens infrastruktur. Dessutom måste nätverket klara av en ständigt ökande mängd datatrafik, för att undvika överbelastning.

Detta white paper 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[15].

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. nätfiske) 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[16].

Att informationstillgångar och verksamhetssystem skyddas från angrepp

För att kommunen 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 kommunal verksamhet av tillräckliga skydd så att detta inte kan ske. Vidare behöver kommunen säkerställa att den har tillräcklig övervakning, mer eller mindre i realtid, så att skadan av ett eventuellt angrepp kan minimeras. Behovet är egentligen inte unikt för den kommunala 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. Både kommunanställda och elever har under de senaste två åren behövt utföra arbete och skolarbete på distans. Även fortsättningsvis förväntas en stor del kommunanställda arbeta en viss tid på distans. Det ger upphov till nya behov i kommunerna. För både elever och anställda krävs möjlighet att kunna medverka i videomöten. De måste också komma åt kommunens nätverk på samma villkor som om de var på plats i kommunens 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 upprätthålla 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 kommunens it-säkerhetslösningar.

Verksamhetsspecifika behov

Utöver de behov som redovisats ovan har Cisco också identifierat ett antal verksamhetsspecifika behov. Dessa utgår från särskilda verksamhetsutmaningar kopplade till it-säkerhet. Vi har organiserat dessa verksamhetsbehov i de fyra kategorierna utbildning och barnomsorg, omsorg och stöd, VA och energi och fastigheter och IoT.

Verksamhetsbehov inom utbildning och barnomsorg

Att använda datorer och surfplattor har blivit mer regel än undantag i majoriteten av svenska skolor. Från förskolan hela vägen upp till gymnasiet använder svenska elever digitala enheter i sitt dagliga skolarbete. Samtidigt som elever behöver ha tillgång till sina skoldatorer, utgör yngre användare en mer riskbenägen användargrupp av digitala verktyg. Delvis i termer av att de i visar en större benägenhet att söka på provokativt eller stötande material men också på sättet att de medvetet försöker runda de säkerhetsrutiner som satts upp på deras enheter Att reglera och skydda användandet av skolornas enheter, utan att helt stänga ned möjligheterna till att använda internet, ser vi därför som två viktiga behov kopplade till utbildnings- och barnomsorgsområdet.

En majoritet av alla kommuner använder sig av någon sorts skolplattform. Dessa används bl.a. för att planera undervisningen, tillgängliggöra arbetsmaterial och kommunicera med elever och vårdnadshavare. Flera av dessa plattformar är molnbaserade. Samtidigt har stora delar av den svenska skolsektorn gått över till molnbaserade lösningar för digitala pedagogiska verktyg. Det är i huvudsak Microsoft-baserade produkter eller produkter från Google. Information om elevers skolgång och övrig information som bearbetas i sådana molntjänster måste omgärdas av sådant skydd att alla inblandade kan vara säkra på att informationen inte kan nås av tredje part.

Verksamhetsbehov inom omsorg och stöd

Den kommunala omsorgen – både i termer av äldreomsorg och omsorg för personer med funktionsnedsättning – nyttjar i allt högre andel digitala verksamhetsstöd. Generellt har man här inte kommit riktigt lika långt som i digitaliseringen av utbildning och barnomsorg men viktiga steg på vägen har tagits. Inom verksamheten har mycket fokus historiskt legat på effektivitet och planering av verksamheten.

Det som särskiljer denna verksamhet från vissa andra delar av kommunen 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. Förenklat kan man säga att en tjänst för badvattentemperatur såväl kan gå ner och exponera alla sina

data online utan att det skulle påverka kommunen nämnvärt. Om motsvarande skulle ske i ett system som håller reda på en brukares läkemedelsbehov skulle det vara en allvarlig incident.

I takt med att fler produkter når marknaden och att digitaliseringsgraden ökat i verksamheterna har också välfärdsteknologi börjat implementeras i verksamheterna. Detta kan innefatta alltifrån digitala trygghetslarm och fallsensorer till system för nattövervakning. Även denna typ av lösningar ställer särskilt stora krav på drifts- och it-säkerhet givet de potentiella konsekvenserna ett avbrott skulle få.

Inom vård- och omsorgsområdet finns också i högre andel än i andra kommunala verksamheter personal med låg digital mognad. Även detta ställer andra krav på it-säkerhet än inom andra verksamheter.

Slutligen är området också i högre andel än andra kommunala verksamheter utlagd på privata utförare. Dessa har dock i högre utsträckning än till exempel friskolor behov av tillgång till de kommunala verksamhetssystemen. Här finns således behov av att tillgängliggöra dessa system och denna information utan att exponera systemen för onödiga risker.

Verksamhetsbehov inom VA och energi

Inom ramen för den kommunala tjänsteleveransen ingår att tillhandahålla grundläggande samhällsfunktioner till samtliga kommuninvånare. Till detta har vi valt att räkna tillhandahållandet av rent vatten, avlopp och energi. Samtliga kommuner har ett ansvar att tillhandahålla vatten och avlopp medan det inte är obligatoriskt för kommunen att tillhandahålla energitjänster. Ett flertal kommuner har valt att samverka kring vatten- och avloppstjänster antingen genom kommunsamverkan eller genom bolag som tillhandahåller tjänsterna till flera kommuner.

Utifrån ett it-säkerhetsperspektiv ställs andra krav på denna typ av verksamhet utifrån de potentiellt katastrofala effekter ett avbrott i leveransen skulle kunna få. För att säkerställa att driften upprätthålls inom ett antal samhällsviktiga områden har EU fattat beslut om NIS-direktivet[17]. Detta pekar ut bl.a. energi och leverans- och distribution av dricksvatten som områden som regleras. Att en verksamhet regleras av NIS-direktivet innebär konkret att kommunen är skyldig att hålla en hög gemensam nivå på säkerhet i nätverk och informationssystem som hanterar verksamheten. Kommuner har alltid haft ett särskilt ansvar för att trygga att sådana samhällsfunktioner fungerar tillfredsställande, men under senare år har lagstiftningen skärpts ytterligare.

Utöver de krav som etableras inom ramen för NIS-direktivet som syftar till att säkerställa att samhällsviktig verksamhet kan fortsätta oavsett hur kommunens övriga it-miljö är påverkad finns det också specifika behov kopplade till området VA och energi som inte är lagreglerade. Detta handlar bland annat om att skapa en central kontroll av operational technology

(OT)-enheter. OT-enheter kan förenklat beskrivas som hård- och mjukvara som används för att övervaka eller styra industriell utrustning[18]. 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.

Verksamhetsbehov inom fastigheter och IoT

Nästan alla kommuner har någon typ av egna fastigheter. Det kan vara idrottshallar, skolor och kommunhus inom vilka kommunal verksamhet bedrivs. En majoritet av kommunerna har också kommunala bostadsbolag vars syfte är att tillhandahålla hyresrätter till kommuninvånarna. Fastighetsbestånden är ofta omfattande, och att få central kontroll för överblick och optimering kan därför innebära stora besparingar för kommunen.

På motsvarande sätt som inom området VA och energi finns också ett behov av att skapa en central kontroll av de OT-enheter som finns i sådana fastigheter. Även här är många av systemen äldre och sårbara, och trots att det inte är lika verksamhetskritiskt som VA- och energi-området finns det också här ett stort behov av driftsäkerhet. Behovet ökar i takt med att kommuner väljer att digitalisera och möjliggöra central kontroll av produkter som är av verksamhetskritisk karaktär såsom exempelvis lås eller kontrollsystem för ventilation.

Utöver att säkra en välfungerande och säker drift av äldre OT-system, finns också ett växande behov av att hantera den mängd smarta enheter som installeras i kommunerna i syfte att få intelligenta fastigheter och smarta städer. Det finns ingen entydig definition av dessa begrepp men gemensamt är att använda it för att förbättra resursanvändningen, att dela information med allmänheten och få högre kvalitet på det kommunala tjänsteutbudet[19]. Detta innefattar rent konkret att använda sig av enheter som bygger på internet of things (IoT) eller sakernas internet. Här handlar det ofta om att införa teknisk infrastruktur som samlar in data eller agerar autonomt i stadsmiljön. Potentialen i sådan teknik är stor, och idag används enheter t.ex. i fastighetsbestånd för värme- och fuktmätare eller för luftmätning i stadsmiljön.

Utifrån ett it-säkerhetsperspektiv ställer det särskilda krav. Samtliga dessa enheter finns i stadsmiljö men har samtidigt behov av nättillgång. Vidare har it-säkerhet i IoT-enheter historiskt varit relativt bristfällig. Detta har dock blivit bättre i takt med att marknaden mognat.

Vilka förmågor krävs för att möta de kommunala behoven?

Presentation av Ciscos förmågekarta för säkra kommuner

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

Verksamhetsspecifika förmågor

- Särskilt kostnadseffektiva lösningar åt elever
- Övervakning av känslig data i molntjänster
- Mobila enheter som kan delas av flera användare
- Leva upp till NIS-lagstiftningens kravbild
- Webbfilter i skolor och hem
- Begränsad info-delning med privata utförare
- Säker hantering av OT- och IoT-enheter

Förmågor för hela kommunen

- Skyddad infrastruktur
- Säker åtkomst till rätt applikationer och information
- Kostnads-effektivitet och automatisering
- Snabb upptäckt och åtgärd av intrång
- Säkert distansarbete/ hybridarbete
- Skyddade enheter/ klienter
- Tillräcklig kompetens hos medarbetare och användare
- Tillhandahålla nätverk till tredje part

Utbildning och barnomsorg

Omsorg och stöd

VA och energi

Fastigheter och IoT

Hela kommunens behov

Förmågor för hela kommunen

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

Förmåga	Beskrivning	Kategori
Skyddad infrastruktur	Att kunna skydda sitt nätverk mot externa hot är avgörande för kommuners it-säkerhet. Det rör sig dels om brandväggar, webb- och mejl-filter, men också segmentering av det kommunala nätverket.	
Säkert distansarbete/hybridarbete	I takt med att kommunens medarbetare jobbar alltmer på distans ställs allt högre krav på att erbjuda en skyddad it-miljö även i medarbetarnas hem. För detta krävs att kommuner kan tillhandahålla både säkra anslutningar till kommunens applikationer och system, och fullgoda skydd för enheter även utanför den ordinarie arbetsplatsen. Distansarbete har också ökat behovet av säkra anslutningar till molnbaserade system.	
Säker åtkomst till rätt applikationer och information	Att kunna segmentera nätverk, så att användare enbart får tillgång till det som denna har behov av i sin roll är viktigt både för att upprätthålla kommunens övergripande krav på informationssäkerhet (GDPR, patientdatalagen etc.). Det är även viktigt för att förhindra att skadlig programvara kan röra sig fritt mellan olika enheter i det interna nätverket.	
Skyddade enheter/ klienter	Att skydda nätverkets enheter/klienter (t.ex. datorer och mobiltelefoner) är avgörande för möjligheten att stoppa skadlig programvara som vill ta sig in i en kommuns nätverk. Att skydda enheter från sådana hot ställer höga krav både på de tekniska produkter som används, och kunskap hos användare (se nedan).	

Förmåga	Beskrivning	Kategori
Kostnadseffektivitet och automatisering	Många kommuner har pressade budgetramar och behöver därför effektivisera och automatisera verksamheten i den utsträckning det är möjligt. Stordriftsfördelar och gemensamma standarder underlättar i det arbetet, och bidrar med lägre kostnader, men också en mindre komplex it-miljö (vilket minskar behoven av ytterligare säkerhetsåtgärder).	
Tillräcklig kompetens hos medarbetare och användare	Att anställda har god förståelse för hur man använder kommunala it-system och digitala enheter på ett säkert sätt är kritiskt för den kommunala it-säkerheten. Phishing, malware och andra angreppsmetoder som försöker penetrera en kommuns nätverk kan ofta lyckas pga. av att anställda omedvetet släpper in angriparen genom att t.ex. klicka på en länk. Att kontinuerligt utbilda sin personal är därmed en viktig del i en kommuns it-säkerhetsarbete.	
Snabb upptäckt och åtgärd av intrång	För varje sekund som en skadlig programvara eller kod används i en kommuns nätverk ökar riskerna för storskaliga dataförluster, sabotage eller andra negativa verksamhetseffekter. Det är därför av stor vikt att kommuner snabbt kan upptäcka och åtgärda intrång i de egna systemen.	
Tillhandahålla nätverk till tredje part	Många av användarna av kommuners nätverk är inte anställda eller brukare av kommunens tjänster. Det kan t.ex. röra sig om besökare som ansluter egna datorer till kommunhusets Wi-Fi eller i de kommunala verksamheternas lokaler. Eftersom kommuner dagligen har kontakt med ett stort antal företag, kommuninvånare och andra representanter behöver man även för dessa användare kunna erbjuda en säker anslutning.	

Verksamhetsspecifika förmågor

Förmåga	Beskrivning	Kategori
Särskilt kostnadseffektiva lösningar åt elever	Många kommuner har begränsade resurser för investeringar i it-säkerhet. Elever utgör en stor grupp it-användare och kommuner måste därför kunna erbjudas kostnads-effektiva och skalbara säkerhetslösningar. Generellt har elever också en högre risk-profil än kommunanställda, vilket gör att säkerhetslösningar blir särskilt aktuella.	
Övervakning av känsliga data i molntjänster	Eftersom molnbaserade tjänster används för distansundervisning och i kontakt mellan elev, lärare och vårdnadshavare, måste en kommun kunna skydda och övervaka potentiellt känsliga data som delas mellan dessa.	
Webbfilter åt elever	En viktig förmåga för skolan är att kunna tillhandahålla välfungerande webbfilter som begränsar elevers möjligheter att nå farligt eller opassande material på skolans enheter. Filtret måste fungera både i och utanför skolans lokaler.	
Mobila enheter som kan delas av flera användare	Inom hemtjänsten måste kommunen kunna tillgodose att anställda delar mobila enheter (mobiltelefoner, surfplattor) med kollegor, samtidigt som dessa enbart får ha tillgång till personlig information om brukare som de behöver i sitt dagliga arbete. Att den personliga integriteten hos brukare ska respekteras är lagstiftat i patientdatalagen. Där står det; ”Den som arbetar hos en vårdgivare får ta del av dokumenterade uppgifter om en patient endast om han eller hon deltar i vården av patienten eller av annat skäl behöver uppgifterna för sitt arbete inom hälso- och sjukvården[20].	

Förmåga	Beskrivning	Kategori
Begränsad informationsdelning med privata utförare	Kommuner behöver kunna dela verksamhetsrelevant information (personuppgifter m.m.) med privata utförare av välfärdstjänster (t.ex. hemtjänstföretag). Samtidigt är det av stor vikt att sådana utförare inte får större tillgång än vad som är motiverat utifrån deras uppdrag.	
Leva upp till NIS-lagstiftningens kravbild	Kommuner måste ha förmåga till särskilda säkerhetslösningar i nätverk som kan kopplas till samhällsviktiga tjänster (t.ex. digital infrastruktur, energi och leverans /distribution av dricksvatten) enligt NIS-direktivet.	
Säker hantering av OT- och IoT-enheter	Kommuner måste på ett säkert och stabilt sätt kunna upprätthålla kommunikation mellan centrala it-system och verksamheternas OT- och IoT-enheter. Centraliserad drift- och säkerhetsövervakning är en avgörande komponent i det arbetet.	

Referens-arkitekturer för en säker kommun

När vi nu redogjort för viktiga kommunala behov och förmågor, vill ge några exempel på hur dessa konkret kan hanteras genom en uppsättning av våra lösningar. Vi kallar det, Ciscos referensarkitekturer för en säker kommun. Vi är medvetna om att ingen kommun 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 lösning kan struktureras från grunden.

Vi har valt att i det här kapitlet visualisera och beskriva Ciscos referens-arkitekturer för fyra typiska kommunala behov. Dessa demonstrerar också på ett bra sätt vad vi ser som en ändamålsenlig uppsättning för en säker kommun. Om ni har intresse av att se ytterligare exempel på referensarki-tekturer för andra verksamhetsbehov, vänligen kontakta er Cisco-säljare.

Referensarkitektur för elever i skolan

Som beskrivits i förmågekapitlet utgör elever en mycket stor användargrupp som har behov av att kunna ansluta till kommunens digitala miljö både från hemmet och från skolan. I nästan samtliga kommuner kommer elever befinna sig på olika platser när de ansluter sig till skolans server eller molntjänster. Här nedan beskriver vi vår referens-arkitektur för en elev i skolans lokaler.

- För att en elev ska kunna komma åt sitt skol-material behöver elevens enhet (dator/mobil/surfplatta/chromebook) anslutas till ett nätverk (ofta skolans egna nätverk). Oavsett var eleven ansluter sig har enheten redan ett grundskydd mot skadlig programvara, genom **Secure endpoint**. Denna lösning svarar mot förmågan **Skyddade enheter/klienter**.
- Om eleven sedan vill ansluta till kommunens nätverk används Ciscos lösning **Secure network access** för att säkerställa att eleven verkligen har rätt att ta del av den efterfrågade informationen, genom nätverkssegmentering av användarna. Lösningarna svarar mot förmågan **Säker åtkomst till rätt applikationer och information**.
- När eleven ansluter sin dator via skolans nätverk finns **Ciscos webbfilter** påslaget, för att förhindra att eleven besöker sidor med skadligt eller olämpligt innehåll. Lösningen svarar mot förmågan **Webbfilter i skolor och hem**.
- För elevens mail-program krävs ett särskilt verktyg som skyddar mot skadliga phishing-försök. Behovet kan fyllas genom de funktioner som finns tillgängliga i Ciscos **Secure email** och svarar mot förmågan **Skyddade enheter**.
- Om eleven ansluter sig via skolans nätverk används Ciscos **Secure firewall** för att skydda elevens enhet mot skadligt material eller program. Lösningarna svarar mot förmågan **Skyddade enheter/klienter** och **Övervakning av känsliga data i molntjänster**.
- Kommunen bör också ha en central förmåga att övervaka webbtrafik från elevdatorer, för att säkerställa att ingen skadlig programvara tar sig in i skolenheter. Sådan övervakning kan effektivt skötas genom **Secure X**, en molnbaserad platt-form för överblick av hela kommunens it-säkerhet. Lösningen svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.

Cisco är medvetna om den ofta pressade budget som finns inom den kommunala skolan. Vår lösning för elever kan därför erbjudas till ett mycket konkur-renskraftigt pris, utan att säkerhet eller användar-barhet offras. Detta svarar mot förmågan **Särskilt kostnadseffektiva lösningar åt elever**.

Referensarkitektur för elever utanför skolans nätverk

Elever utför en stor del av sitt skolarbete utanför skolans lokaler. Oavsett om eleven befinner sig på ett bibliotek, på café eller i hemmet så behöver dock skolans enhet förbli skyddad. Här beskriver vi vår referensarkitektur för en elev utanför skolans lokaler.

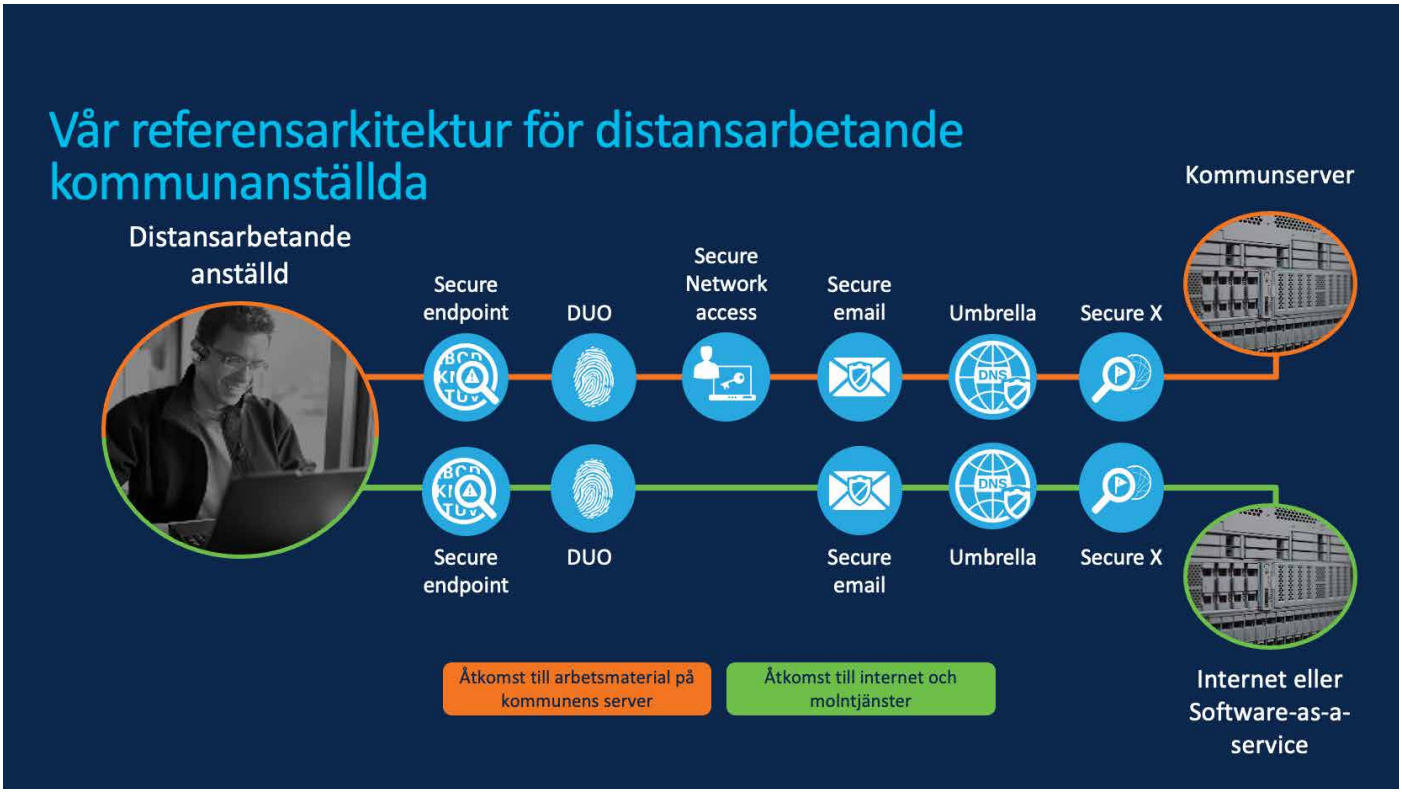
- För att en elev ska kunna komma åt sitt skolmaterial behöver elevens enhet (dator/mobil/surfplatta/ chromebook) anslutas till ett nätverk (ofta elevens Wi-fi i hemmet). Oavsett var eleven ansluter sig har enheten redan ett grundskydd mot skadlig programvara, genom **Secure endpoint**. Denna lösning svarar mot förmågan **Skyddade enheter/klienter**.
- Om eleven sedan vill ansluta till kommunens nätverk används Ciscos lösning för tvåfaktorsinloggning, **DUO**, som fyller samma funktion som lösningen **Secure network access**, för att säkerställa att eleven verkligen har rätt att ta del av den efterfrågade informationen. Lösningarna svarar mot förmågan **Säkert distansarbete/ hybridarbete** och **Säker åtkomst till rätt applikationer och information**.
- Om eleven ansluter sin dator i hemmet finns **Ciscos webbfilter** påslaget, för att förhindra att eleven besöker sidor med skadligt eller olämpligt innehåll. Lösningen svarar mot förmågan **Webbfilter i skolor och hem**.
- För elevens mail-program krävs ett särskilt verktyg som skyddar mot skadliga phishing-försök. Behovet kan fyllas genom de funktioner som finns tillgängliga i Ciscos **Secure email** och svarar mot förmågan **Skyddade enheter**.
- När olika molnbaserade tjänster som t.ex. Google Classroom används behövs kontinuerligt skydd av den datatrafik som rör sig mellan elevens enhet och molntjänsten. Ciscos lösning **Umbrella** kan nyttjas för just det behovet. Lösningen svarar mot förmågan **Skyddade enheter/klienter** och **Övervakning av känsliga data i molntjänster**.
- Kommunen bör också ha en central förmåga att övervaka webbtrafik från elevdatorer, för att säkerställa att ingen skadlig programvara tar sig in i skolenheter. Sådan övervakning kan effektivt skötas genom **Secure X**, en molnbaserad plattform för överblick av hela kommunens it-säkerhet. Lösningen svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.

Referensarkitektur för OT och IoT

I framtagandet av en referensarkitektur för OT- och IoT-enheter 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 kommunens betrodda driftcentral. Nedan summerar vi vår övergripande referensarkitektur för OT- och IoT-enheter.

- För att förhindra att felaktig kommunikation sker mellan OT- eller IoT-enheter och nätet sker först en nätverkssegmentering genom **Cisco secure network access** och **Cisco firewall**. Med dessa verktyg spärras åtkomsten till OT- och IoT för obehöriga. Produkterna är viktiga komplement till varandra och svarar mot förmågan **Skyddad infrastruktur** och/eller **Skyddade enheter/klienter** och **Säker åtkomst till rätt applikationer och information**.
- För att ytterligare säkra att inga obehöriga intrångsförsök sker inom den känsliga infrastrukturen utgör Ciscos verktyg **Secure network analytics** en viktig pusselbit. Det används för att övervaka vad som händer ute i OT-miljön. Denna lösning svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.
- Ett annat viktigt komplement i driftövervakningen är **Kenna**, som är ett verktyg för att utvärdera och bedöma vilka hot som bör prioriteras. Det är av särskild vikt inom hantering av OT-resurser, eftersom sådana enheter (t.ex. vattenverk) inte kan stängas eller startas om (och på så sätt uppdatera drivrutiner/installera ny programvara) närsomhelst. När ett hot väl identifierats måste det därför kontinuerligt övervakas tills det kan bemötas genom mjukvaruuppdateringar. Denna lösning svarar också mot förmågan **Snabb upptäckt och åtgärd av intrång**.
- I takt med att it-system, molntjänster och kontrollnätverk för OT-enheter integreras ökar hotrisken mot OT- och IoT-enheter. För kontinuerlig driftövervakning av alla dessa delar, och effektiv hotdetektering och driftinformation från systemen har Cisco tagit fram lösningen **Cyber Vision**. Produkten är speciellt utvecklad för att anställda med ansvar för OT-enheter ska kunna säkerställa driftkontinuitet, motståndskraft och säkerhet. Lösningen svarar mot förmågan **Snabb upptäckt och åtgärd av intrång** och **Säker hantering av OT- och IoT-enheter**.

Lösningarna som beskrivs ovan är alla viktiga pusselbitar som tillsammans bidrar till den kommunala förmågan **Säker hantering av OT- och IoT-enheter** och kommuners förmåga att **leva upp till NIS-lagstiftningens kravbild**.



Referensarkitektur för distansarbetande kommunanställda

På samma sätt som distansarbetande elever behöver distansarbetande kommunanställda ha säker och stabil åtkomst till kommunens nätverk. Detta svarar också mot de förmågor som är specifika för området Omsorg och stöd – nämligen **Mobila enheter som kan delas av flera användare** och **Begränsad informationsdelning med privata utförare**.

- Också här krävs ett grundläggande skydd av den kommunanställdas enhet (dator/mobil/surfplatta) när den ansluter till ett nätverk som inte är kommunens (t.ex. den anställdes hemnätverk). Behovet tryggas genom **Secure endpoint**. Denna lösning svarar mot förmågan **Skyddade enheter/klienter**.
- För att den anställda ska komma åt det kommunala nätverket används ofta en VPN-tunnel. Denna uppkoppling garanteras genom Ciscos **Secure remote access**. För att identifiera sig och visa att enheten lever upp till kommunens krav för ansluta enheter används Ciscos lösning **DUO**. Lösningarna svarar mot förmågan **Säkert distansarbete/hybridarbete** och **Säker åtkomst till rätt applikationer och information**.
- Väl ansluten till det kommunala nätet används också här **Secure network access**. Detta för att säkerställa att den anslutna användaren får rätt behörighet att ta del av efterfrågad informationen. Lösningen svarar mot förmågan **Säker åtkomst till rätt applikationer och information**.
- Eftersom mailen är ett av de viktigaste arbetsverktygen för anställda är det många som öppnar sin mail-klient direkt när arbetsdagen börjar. Här krävs precis som för eleven ett bra försvar mot skadliga phishing-mail, genom Cisco **Secure email**. Lösningen svarar mot förmågan **Skyddade enheter/klienter**.
- Eftersom många kommuner ger anställda möjlighet att använda sin dator för privata ärenden krävs också en kontinuerlig övervakning av webbtrafiken när distansarbetaren väl är ansluten till internet. Här används Ciscos lösning **Umbrella** för att kunna upprätthålla förmågan **Snabb upptäckt och åtgärd vid intrång** och **Säkert distansarbete/hybridarbete**.
- Kommunen bör också här ha en central förmåga att övervaka webbtrafik för att säkerställa att ingen skadlig programvara tar sig in i kommunens enheter. Sådan övervakning kan effektivt skötas genom **Secure X**, en molnbaserad plattform för överblick hela kommunens it-säkerhet. Lösningen svarar mot förmågan **Snabb upptäckt och åtgärd av intrång**.

Bilaga

Hur Cisco kan bidra till att stärka de kommunala förmågorna

I den här bilagan kan du själv se vilka lösningar som vi på Cisco kan erbjuda er kommun utifrån de förmågor som identifierats i tidigare avsnitt. Vill du veta mer om hur Cisco kan hjälpa dig i utformningen av säker kommun?

Kontakta

Henrik Bergqvist
Sales Manager, Security
hbergqvi@cisco.com
070-544 9622

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

Matchning mellan förmågor och Ciscos erbjudna lösningar – hela kommunen

Ciscos erbjudna lösningar	Skyddad infrastruktur	Säker åtkomst till rätt app-likationer och information	Kostnads-effektivitet och automatisering	Snabb upptäckt och åtgärd av intrång	Säkert distansarbete/ hybridarbete	Skyddade enheter/klienter	Tillräcklig kompetens hos medarbetare och användare	Tillhandahålla nätverk till tredje part
Cyber Vision	✓			✓				
DUO		✓	✓	✓	✓		✓	✓
KENNA security			✓	✓				
Secure endpoint			✓	✓	✓	✓		
Secure email			✓	✓	✓	✓	✓	
Secure firewall	✓	✓	✓	✓	✓	✓		✓
Secure net-work access	✓	✓	✓			✓		✓
Secure net-work analytics	✓	✓	✓	✓				✓
Secure remote access		✓	✓		✓	✓		✓
Secure web		✓	✓	✓		✓	✓	
Secure workload	✓	✓	✓	✓				✓
Secure X			✓	✓				
Security Awareness training							✓	
Umbrella	✓	✓	✓	✓	✓	✓	✓	

Matchning mellan förmågor och Ciscos erbjudna lösningar – verksamhetsspecifikt

Ciscos erbjudna lösningar	Särskilt k ostnadseffektiva lösningar åt elever	Övervakning av känslig data i molntjänster	Webbfilter i skolor och/eller hem	Mobila enheter som kan delas av flera användare	Begränsad informations-delning med privata utförare	Leva upp till NIS-lagstift-ningens kravbild	Säker hantering av OT-enheter och smarta enheter
Cyber Vision							✓
DUO				✓	✓	✓	
KENNA security						✓	✓
Secure endpoint						✓	
Secure email	✓					✓	
Secure firewall	✓	✓	✓		✓	✓	✓
Secure network access	✓				✓	✓	✓
Secure network analytics						✓	✓
Secure remote access			✓		✓	✓	✓
Secure web		✓	✓			✓	✓
Secure workload						✓	
Secure X	✓					✓	✓
Security Awareness training						✓	
Umbrella	✓	✓	✓			✓	✓

Referenser

[1]DESI, The Digital Economy and Society Index (2021) EU-kommissionen
Länk: https://digital-strategy.ec.europa.eu/en/policies/desi

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

[3]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

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

[5]187 kommuner drabbade av utpressningsvirus (2017) SVT
Länk: https://www.svt.se/nyheter/inrikes/187-kommuner-drabbade-av-utpressningsvirus

[6]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

[7]Ideologically motivated computer hacking
Länk: https://rusi.org/publication/ideologically-motivated-computer-hacking

[8]2021 Cyber security threat trends (2021) Cisco
Länk: https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

[9]Ekonomiskt andrum, men framtiden kräver långsiktighet (2021) SKR
Länk: https://skr.se/skr/tjanster/press/vdskronika/aldrevdskronika/ekonomisktandrummenframtidenkraverlangsiktighet.54368.html

[10]What is a Cyberattack? (2021) Cisco
Länk: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

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

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

[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]Det här gäller enligt dataskyddsförordningen - grundläggande principer (2022) Integritetsskyddsmyndigheten
Länk: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/grundlaggande-principer/

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

[16]2021 Cyber security threat trends (2021) Cisco
Länk: https://umbrella.cisco.com/
info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

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

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

[19]TWI - What is a smart city?
Länk: https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city

[20]Patientdatalag (2008:355)
Länk: https://www.riksdagen.se/sv/dokument-lagar/dokument/
svensk-forfattningssamling/patientdatalag-2008355_sfs-2008-355


CISCO