Den sikre kommune

Ciscos vejledning til sikre kommuner

Indholdsfortegnelse

Introduktion

En stor del af Danmarks kommuner har Cisco som leverandør til en del af deres it-miljø. Gennem disse kunderelationer har vi fået indblik i de sikkerhedsmæssige udfordringer danske kommuner står over for. I daglige dialoger med både beslutningstagere og it-ledere ser vi, at mange ønsker at prioritere it-sikkerhed, men også at mange efterspørger vejledning til, hvordan de skal håndtere de i mange tilfælde både nye og komplekse trusler, der findes.

Undervisningsmateriale med fokus på it-sikkerhed er ofte skrevet i et teknisk fagsprog og er ikke helt let at tage fat i. Vi har derfor lavet dette whitepaper, som indeholder en beskrivelse af, hvordan vi ser på it-sikkerhed i danske kommuner. Spørgsmål som vi vil give vores syn på, er f.eks. hvilke trusler og udfordringer er specifikke for den kommunale sektor og hvilke behov og foranstaltninger der kræves for at beskytte dig selv.

Vi mener, at materialet er brugbart for dig, der har rollen som CIO eller CISO, og har ansvaret for og koordinerer det i din kommune, men det skal også ses som en vigtig brik i puslespillet at bidrage med viden på området til kommunale beslutningstagere. Nedenfor ser du en oversigt over de forskellige afsnit og deres indhold.

IT-trusler og sårbarheder	Eksternt trusselsbillede mod danske kommuner Metoder og tilgange Hvor er sårbarhederne i det kommunale netværk?
Generelle kommunale IT-udfordringer	Generelle udfordringer i kommunernes it-sikkerhedsarbejde Udfordringer med at håndtere persondata i skyen
Kommunale IT-sikkerhedsbehov	Hvad er kommunernes IT-sikkerhedsbehov? Hele kommunens behov Forretningsspecifikke behov
Kapaciteter til at sikre IT-miljøet	Hvilke foranstaltninger kræves for at imødekomme de kommunale behov? Foranstaltninger for hele kommunen Erhvervsspecifikke foranstaltninger
Ciscos referencearkitektur	Eksempler på Ciscos referencearkitekturer til et sikkert IT-miljø

Om Ciscos vejledning til sikre kommuner

I et globalt perspektiv er Danmark nået langt på sin digitaliseringsrejse. Danske husstande og virksomheder er hurtige til at adoptere og bruge nye digitale tjenester og værktøjer. Den nødvendige IT-infrastruktur (både faste bredbåndsløsninger og trådløs teknologi) er blevet kraftigt udvidet, og selvom der stadig er meget at gøre, er der bred enighed blandt beslutningstagere om nødvendigheden og fordelen ved digitalisering. Alt dette er medvirkende til, at Danmark i de senere år har været blandt de fem bedste lande i EU's årlige digitaliseringsindeks, DESI[1].

Kommunal drift er fundamentet i det danske samfund og udgør en håndgribelig del af den offentlige sektor. Hver dag går hundredtusindvis af voksne og børn på arbejdspladser, skoler eller andre aktiviteter, der drives eller overvåges af kommuner. Landets kommuner har også foretaget store investeringer i digitale tjenester og it-systemer, der gradvist har gjort driften både mere effektiv og målgruppeorienteret.

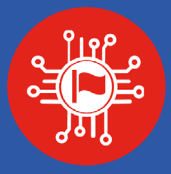
Men i takt med at flere og flere dele af den kommunale drift er blevet digitaliseret, er afhængigheden af, at medarbejdere og borgere har adgang til det rigtige system og den rigtige information også øget. Den øgede deling af information gennem digitale kanaler skaber også nye sikkerhedsudfordringer. Eksterne aktører med forskellige motiver har en interesse i enten at få adgang til information og systemer, de ikke har ret til, eller på anden måde at forstyrre forretningen. På grund af de brede og diversificerede aktiviteter, der udføres, har der længe været en god forståelse i Danmarks kommuner for behovet for et højt it-sikkerhedsniveau.

Ciscos erfaring er, at denne forståelse også er steget de seneste år, da større cyber angreb mod både kommunal drift og mod andre typer organisationer har fået stor opmærksomhed i medierne. En stor del af Danmarks kommuner har valgt Cisco som leverandør i IT-sikkerhedsområdet. Det betyder, at vi gennem årene har fået et unikt indblik i de it-sikkerhedsbehov, der findes i danske kommuner, og de udfordringer, de står over for. I de kontakter, vi har med kommunale repræsentanter både på beslutnings- og driftsniveau, har vi set et tydeligt krav om vejledning i spørgsmålet om, hvordan kommunerne skal agere for at beskytte deres systemer og informationer mod trusler udefra.

For at gøre det nemmere at skabe overblik over det typiske kommunale IT-miljø og hvilke behov og evner der kan knyttes til det, har vi i Cisco Danmark lavet Ciscos vejledning til sikre kommuner. Målgruppen for denne publikation er hovedsageligt it-chefer, it-sikkerhedschefer og CIO'er, der tænker it-sikkerhed i en kommunal sammenhæng. Vi mener også, at dette skriv kan have interesse for

kommunaldirektører og forvaltningschefer, der ønsker at danne sig en mening om, hvordan de kan ræsonnere i it-sikkerhedsspørgsmål. På den måde er vores håb, at materialet kan forenkle dialogen mellem drift og it på området. I dette dokument vil vi gennemgå, som vi ser som de største it-trusler lige nu, hvilke udfordringer der er specifikke for kommunale organisationer, hvilke behov der findes i kommuners forskellige aktiviteter, hvilke kapaciteter kommunen skal opbygge for at imødekomme disse behov og afsluttes med et kapitel, der beskriver mulige referencearkitekturer for fælles kommunale udfordringer. Materialet er baseret på Ciscos langvarige kundekontakt med en lang række danske kommuner, og vores ambition er her at italesætte både nutidens og morgendagens kommunale behov for it-sikkerhedsløsninger.

Eksternt trusselsbillede mod danske kommuner



Statslige aktører
Stater bruger hovedsageligt it-angreb til at sabotere og spionere. Deres omfattende ressourcer og ekspertise gør dem yderst dygtige og i stand til alvorligt at forstyrre og skade offentlige operationer.

Kriminelle organisationer
Kriminelle har primært økonomiske mål i forbindelse med it-angreb. De forsøger at få fat i følsomme data eller adgangskoder, der så kan bruges til afpresning.

Aktivister
Aktivister har i de senere år brugt it-angreb til at forstyrre eller sabotere stater og organisationer. Målene for angrebene varierer afhængigt af angriberen, men er ofte ideologisk motiverede.

Antallet af cyber angreb mod europæiske virksomheder og organisationer er steget markant de seneste år[2]. Det eksterne trusselsbillede er komplekst, og årsagerne til at angrebene stiger, har mange facetter. Men årsager, der højst sandsynligt har bidraget til stigningen, er blandt andet, at samfundet er blevet mere og mere afhængigt af digitale løsninger for at drive sin forretning. Tid er også en ressource, der er blevet stadig vigtigere for alle typer organisationer. For hver time en virksomhed eller virksomhed ikke har adgang til sine informationer eller systemer, går der penge tabt. For nordiske virksomheder, koster et hackerangreb i gennemsnit 16,5M kroner[3].

I virksomheder som kommunale plejeforvaltninger kan det endda i værste fald føre til døden. Som en konsekvens af denne sårbarhed øges virksomheders og organisationers betalingsvillighed for igen at få adgang til deres informationer, hvilket skaber yderligere incitamenter for fjendtlige aktører. Og hver gang en organisation betaler de aktører, der udfører angrebene, bliver de styrket, hvilket fører til en ond spiral. Endelig er de aktører, der engagerer sig i denne type aktiviteter, også blevet professionaliserede med tiden[4]. Det gælder både statslige aktører og kriminelle organisationer.

Der findes mange eksempler på rapporter om dette emne, men sikkerhedspolitiet i Sverige udgav i 2020 publikationen "Cybersikkerhed i Sverige - Trusler, metoder, mangler og afhængigheder". Dette viser en diversificeret og kompetent gruppe af trusselsaktører. Disse består hovedsageligt af statslige aktører og kriminelle grupper. Til en vis grad er der også ideologisk motiverede aktører, såsom hacktivister eller grupper med terrorforbindelser.

Statslige aktører

Statslige aktører udfører cyber-angreb mod Danmark til forskellige formål. Det kan fx dreje sig om at indhente information, der kan gavne eget lands udenrigs- og sikkerhedspolitiske interesser, styrke eget lands økonomi og virksomheder gennem virksomhedsspionage eller destabilisere ved at angribe samfundsvigtige tjenester og informationsveje. Der er en række statslige aktører, inden for demokratier såvel som mere autoritære stater, som har opbygget velorganiserede enheder med ansvar for cyber-angreb. Disse kan formelt være en del af statens nationale militær- eller sikkerhedstjeneste, men kan også have løsere forbindelser til staten. Også selvom Danmark ikke er i direkte konflikt med disse lande, kan statslige aktører forsøge at tvinge kommunale systemer til at placere malware, der så

ligger latent i systemerne. Ved et givet signal kan sådanne programmer så bruges til at forstyrre eller sabotere kommunal drift.

Kriminelle organisationer

Den mest almindelige cybertrussel mod alle typer organisationer er kriminelle. I langt de fleste tilfælde har cyberkriminalitet til formål at tjene penge. Også her sker professionaliseringen og eksemplerne på succesfulde it-angreb bliver flere og flere.

Antallet af bedragerier risikerer også at blive stort, da mange virksomheder betaler de kriminelle i stedet for at fortælle dem, at de er blevet afsløret. Offentlige organisationer kan være særligt følsomme over for angreb fra kriminelle organisationer, da de håndterer data, der kan være afgørende for folks sundhed og velvære (f.eks. patientjournaler).

Vi har allerede set eksempler på angreb, hvor sådanne data er krypteret, og kommuner eller myndigheder bliver afpresset til at købe dem tilbage fra angriberen[5]. Vi ser også en udvikling i verden, hvor flere og flere statslige aktører og kriminelle organisationer opererer i symbiose. I nogle lande fungerer kriminelle organisationer næsten præcis som virksomheder og kan så også udføre missioner for staten og købe kompetencer fra andre kriminelle. I sådanne miljøer der fungerer som "økosystemer", får kriminelle organisationer øget evne til at udføre sofistikerede og målrettede
angreb.

Aktivister

Online-aktivister, eller hacktivister, er en mindre almindelig trussel mod offentlige organisationer i Danmark. Onlineaktivister er ideologisk drevne og kan have forskellige motiver til at angribe offentlige organisationer.

Det kunne for eksempel handle om, at man ikke er enig i den politik, der føres på nationalt eller lokalt plan. Danmark har historisk (så vidt vi ved) ikke været udsat for omfattende hacktivistiske angreb. Men globalt set har det i de senere år været muligt at observere sådanne grupper udføre målrettede angreb mod statslige mål[6]. Ikke sjældent er der tale om ideologisk drevne personer, som ofte besidder stor viden om forskellige angrebsmetoder[7].

Metoder og angrebsmetoder

Uanset hvilke underliggende motiver fjendtlige aktører har for at ønske adgang til kommunale it-systemer, anvender de ofte relativt ens metoder. Fælles for mange af disse er, at de forsøger at narre medarbejdere eller brugere til at give angribere adgang til netværk og systemer. For at give et hurtigt overblik over de mest almindelige metoder vil vi præsentere nogle af dem her.

Phishing

En af de mest almindelige metoder til at starte et angreb er ved at sende e-mails, der ser legitime ud. Angriberen håber, at nogen med adgang til et system eller

netværk vil frigive den malware, der er indeholdt i e-mailen. Dette kan gøres ved at klikke på et link, åbne et vedhæftet dokument eller downloade et billede, der er vedhæftet mailen. Metoden kaldes phishing og er meget populær ved cyberangreb. Hele 90 % af alle angreb initieres af en bruger, der åbner en phishing-besked[8]. Et af de mest almindelige motiver bag phishing-angreb er at forsøge at få fat i login-detaljer til forretningssystemer, eller at forsøge at komme længere ind i organisationens netværk på anden måde.

Malware

En anden almindelig metode til it-angreb er malware. Malware er et fællesbegreb, der bruges til at beskrive flere typer programmer. Dette inkluderer spyware, ransomware, vira og orme. Også her er den mest almindelige angrebsmetode, at en bruger klikker på et link eller en vedhæftet e-mail, som derefter installerer softwaren på brugerens konto. Når først er inde i systemet, kan softwaren f.eks.:

- Blokere og kryptere adgang til væsentlig information i netværket med det formål at afpresse organisationen for penge for at få dem tilbage (ransomware)
- Installere yderligere ondsindet software
- Hemmeligt kopiere information til overførsel data fra centrale systemer eller harddiske (spyware)
- Skader eller afbryde visse tekniske komponenter, som kan gøre systemet ubrugeligt.

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

Man-in-the-middle (MitM)-angreb kendes også som f.eks. aflytningsangreb. Disse opstår, når en hacker får adgang til en to-parts transaktion (f.eks. når en bruger forbinder sin enhed til et netværk). Når først angriberne får adgang til datatrafikken, kan de analysere og stjæle data fra flowet.

To almindelige indgangspunkter for MitM-angreb er:

1. På offentlige Wi-Fi-netværk uden tilstrækkelig sikkerhed, hvor angriberen kan fungere som et link mellem en besøgendes enhed og netværket. Uden at vide det sender den besøgende alle oplysninger gennem angriberen.
2. Når først malware har brudt en enhed, kan en angriber installere yderligere software til at manipulere andre enheder, som brugeren opretter forbindelse til.

DDoS-angreb

Et DDoS-angreb (denial-of-service) oversvømmer systemer, servere eller netværk med datatrafik for at forbruge ressourcer og båndbredde. Som følge heraf kan systemet opleves som nedbrud, og dets rigtige brugere kan ikke få adgang.

Målet er normalt ikke at støde på specifikke data, men derimod at forstyrre vigtige funktioner såsom hjemmesider. Motiverne hertil kan være at skabe rod, men metoden kan også bruges til at maskere andre typer it-angreb.

Hvor er sårbarhederne i det kommunale netværk

Enheder tilsluttet netværket

Et netværk er normalt det mest følsomme over for angreb gennem de enheder (endepunkter), der er tilsluttet. Enheder er ethvert udstyr, der kan tilsluttes en organisations netværk (f.eks. mobiltelefoner, computere eller tablets). Sådanne enheder har ofte mindre avancerede sikkerhedsbeskyttelser end organisationens netværksudstyr, hvilket gør dem attraktive mål. Her ser vi, at ældre enheder, uden mere moderne former for indbygget beskyttelse, bliver særligt sårbare. Hvis en angriber får adgang til en enhed, der bruges af en medarbejder i en central position i organisationen, kan denne hurtigt blive udsat for tab af forretningskritisk information.

Mange brugere har også deres konto med brugerrettigheder knyttet til deres enhed. Et brud på enheden betyder derfor, at en hacker potentielt kan få adgang til følsomme oplysninger eller fortrolige systemer. Derudover, når en angriber overtager en enhed, kan de fortsætte med at forsøge at overtage andre enheder fra organisationens netværk. Sikring af enheder i kommunale netværk kompliceres af, at mange brugere medbringer deres egne enheder (f.eks. computere). Disse mangler beskyttelsessoftware eller indstillinger, som netværksejerens enheder har installeret og kan derfor repræsentere et potentielt svagt led i sikkerhedskæden.

Manglende autentificeringsprocedurer

Autentificering betyder, at en bruger bekræfter sin identitet over for et system for at få adgang. De fleste kommuner har et såkaldt Active Directory (AD), hvor en bruger får tildelt tilladelser. De løsninger, der findes til autentificering af informationer, udvikles løbende, og det er ikke ualmindeligt, at brugere bliver tvunget til at vælge et kodeord med en vis kompleksitet og til at skifte kodeord hyppigt.

Mange kommuner bestræber sig også på at etablere såkaldt Single Sign On (SSO), hvilket betyder, at man kun behøver at logge ind én gang for at få adgang til de styresystemer, man er autoriseret i. Det bliver i dag mere og mere almindeligt, at kommuner bruger to- faktorgodkendelse. Ligesom navnet antyder, betyder to-faktor autentificering, at brugere har adgang til to metoder til identifikation. Oftest handler det om en adgangskode og en enhed, f.eks. ved brug af mobilt MitID på en smartphone.

Hvis en kommune ikke har implementeret to-faktor autentificering, er der klare sårbarheder i det kommunale it-miljø. Det er relativt almindeligt, at brugere har samme adgangskode i flere forskellige sammenhænge og herigennem kan en person, hvis private konti er blevet hacket, også blive en belastning for de kommunale it-miljøer. Som vi tidligere har nævnt, udgør phishing-angreb 90 % af alle angrebsforsøg på organisationers netværk. Heraf er 83 % forsøg på at komme på at opsnappe legitimationsoplysninger som f.eks. adgangskode.

De alsidige og opdelte operationer

Kommuner er ekstremt diversificerede organisationer. Der er få virksomheder i Danmark, der inden for rammerne af deres serviceleverance har alt fra at tilbyde uddannelse, til at administrere kritisk infrastruktur og udlåne bøger.

Alt dette sker inden for rammerne af den samme organisation i danske kommuner. Det gør kommunen til en dynamisk organisation, men det gør det også sværere at beskytte ud fra et it-sikkerhedsperspektiv. Billedet kompliceres yderligere af, at mange kommuner deler it-relaterede indkøb op i en netværksdel og en driftsdel. Netværksinvesteringer sker næsten altid gennem centralt indkøb, mens virksomhederne i nogle tilfælde har tendens til at indkøbe enheder som computere eller smartphones lokalt. Det er ikke ualmindeligt, at forskellige virksomheder indkøber løsninger med forskellige tekniske standarder, der kræver særligt tilpassede integrationsløsninger. Dette skaber yderligere vanskeligheder i et allerede komplekst organisatorisk miljø.

Generelle udfordringer i kommunernes it-sikkerhedsarbejde

Ciscos erfaring er som tidligere nævnt, at arbejdet med it-sikkerhed i danske kommuner er blevet en stadig højere prioritet i de senere år. Samtidig ser vi også, at der er en række udfordringer med it-sikkerhedsarbejdet i kommunerne. Vi har valgt at samle det, vi ser som de største udfordringer på tre overordnede områder; økonomiske, kompetencemæssige og organisatoriske udfordringer. Derudover tilføjes en mere specifik udfordring, knyttet til usikkerheden omkring håndteringen af persondata i cloudmiljøer. Denne udfordring er hovedsageligt blevet aktualiseret gennem den højt profilerede Schrems II dom.

Økonomiske udfordringer

De økonomiske vilkår i mange danske kommuner er ofte relativt stramme. Danmarks kommuner og regioner har i en lang årrække taget fat på den demografiske udfordring, der indebærer, at andelen af ældre stiger hurtigere end befolkningen i den erhvervsaktive alder[9] (danmarks statistik). Samtidig er forskellene mellem danske kommuner meget store, og mange, hovedsageligt mindre, tyndt befolkede kommuner, har særligt anstrengte budgetter. Samtidig er velfungerende it-sikkerhedsarbejde ikke nødvendigvis billigt, hvilket bl.a. det faktum, at der er mangel på kompetence på området. Og som med alle beredskabsspørgsmål ser budgetposten kun ud til at koste penge, så længe den ikke bliver brugt.

Der er derfor en overhængende risiko for behov for større investeringer i sikkerhedskompetencer. Med sikkerhedsgæld henviser vi til situationer, hvor du er afhængig af systemer, der er forældede eller ikke korrekt vedligeholdt af budgetmæssige årsager. Denne gæld bliver i sidste ende en sikkerhedsrisiko. Sådanne sikkerhedsrisici bliver attraktive mål for eksterne angribere, hvis de ikke adresseres. Håndtering af disse risici kan omprioriteres ved budgettering, hvis der ikke er indtruffet en højprofileret hændelse i den nærmeste fremtid.

Derfor kan det være udfordrende for CIO'er og it-sikkerhedschefer at argumentere for, hvorfor it-sikkerhedsløsninger er "vigtigere" end flere lærere eller et nyt plejehjem. Man kan også argumentere for, at de lange

budgetcyklusser, der er aktuelle i kommunale organisationer, gør det særligt vanskeligt at styre en så hurtig proces som it-sikkerhed. Det der adskiller it-sikkerhedsområdet fra andre områder, er netop at hvis et angreb lykkes, koster det. Både på det personlige plan og på pengefronten, bliver det yderst håndgribeliget. Vores egen forskning viser, at 53 % af alle cyberangreb resulterer i omkostninger på 4 millioner DKK eller mere[10].

Kompetenceudfordringer

En håndgribelig udfordring, når det kommer til it-sikkerhed, er kompetenceniveauet. Denne udfordring er todelt; det handler dels om en ulige fordelt digital kompetence, dels om manglende spidskompetence Inden for rammerne af næsten alle typer organisationer er medarbejdernes digitale kompetence ulige fordelt.

Kommunale organisationer er ingen undtagelse. Der er medarbejdere, som er helt i front, når det kommer til brugen af digitale tjenester, men der er også medarbejdere, der sjældent eller aldrig bruger eller har brugt digitale tjenester. Dette bliver særligt udfordrende ud fra et it-sikkerhedsperspektiv, da et netværk potentielt ikke behøver at være stærkere end dets svageste led. Det kræver kun, at en medarbejder klikker på et link for at inficere et dårligt sikret netværk. Den anden del af kompetenceudfordringen, handler om manglen på spidskompetence på området.

Der er et skøn der siger, at der mangler 20 % af den arbejdsstyrke, der ville være påkrævet i området. Samtidig forventes behovet for kompetence inden for it-sikkerhed at stige yderligere på kort sigt[11]. Og med de budgetmæssige begrænsninger, der er i mange kommuner, kan det også være svært at stille sig op i konkurrencen om arbejdskraften. Dette kan igen føre til, at it-sikkerhedsroller er ubemandede i lang tid, hvilket i sig selv kan blive en sikkerhedsrisiko.

Organisatoriske udfordringer

I nogle kommuner er der også en række organisatoriske udfordringer. Det betyder i bund og grund, at de dele af organisationen, der har it-sikkerhedsrelaterede ansvar, ikke nødvendigvis er synkroniserede. Et tydeligt eksempel er, at den del af organisationen, der har ansvaret for medarbejdernes klienter, ikke nødvendigvis har et tæt samarbejde med dem, der arbejder med kommunens netværk. I et it-sikkerhedsperspektiv har dette den effekt, at der kan skabes sårbarheder, som igen kan bruges af fjendtlige aktører.

En klar risikofaktor, som vi har identificeret i forhold til kommunale aktører, er også, at der ofte er en del kommunale virksomheder knyttet til kommunen. I nogle tilfælde har vi også set, at disse ikke nødvendigvis håndteres på samme måde som resten af kommunen, hvilket kan medføre it-sikkerhedsmæssige udfordringer. Et fragmenteret it-miljø fører til udvidede processer til at opdage og imødegå trusler. Målet bør i stedet være integrerede sikkerhedsløsninger, hvor firewall, klientbeskyttelse og e-mail kan overvåges centralt. Sådanne platforme fører til bedre overblik og enklere og mere effektive muligheder for at stoppe forsøg på indtrængen.

Udfordringer ved håndtering af persondata i skyen (Schrems II)

I flere år har debatten om, hvordan persondata kan håndteres digitalt af danske myndigheder, kommuner og regioner, været i gang. Fokus har været på, om persondata kan placeres dels i cloudtjenester, dels i tjenester leveret af amerikanske leverandører. Baggrunden for diskussionen er den såkaldte Schrems II-dom. Det betød, at de regler, der tidligere regulerede dataoverførsel af personoplysninger (Privacy Shield) mellem USA og Europa, blev erklæret ugyldige. Dommen er til dels blevet fortolket således, at placeringen af persondata i amerikanske cloudtjenester ikke er forenelig med databeskyttelsesforordningen. Mange kommuner har valgt at bremse eller helt stoppe indførelsen af sådanne tjenester.

Skybaserede tjenester er samtidig et meget brugbart værktøj, der skaber gode betingelser for fjernarbejde og samarbejde i store organisationer med mange interessenter. Mange offentlige organisationer ser problemer med at balancere organisationens krav om digitalisering og omkostningseffektive løsninger mod krav om sikkerhed. Denne udfordring forventes heller ikke at blive mindre, i takt med at den offentlige drift også i fremtiden vil have behov for fleksible, skalerbare og tilgængelige it-løsninger.

Der er også et stigende behov for at kunne stille data til rådighed for forskellige interessenter, for at samarbejde med eksterne parter og for hurtigt at kunne justere driften ved ændrede forhold Blandt mange offentlige aktører er der usikkerhed om betingelserne for at udlicitere it-drift til private tjenesteudbydere. Fortolkningen af, hvornår en oplysning er forkert delt i henhold til gældende lovgivning, er svær at foretage. På grund af usikkerheden har nogle aktører ventet med at træffe beslutninger om IT-drift, hvilket også kan have negative konsekvenser for organisationernes udvikling, sikkerhed og omkostninger.

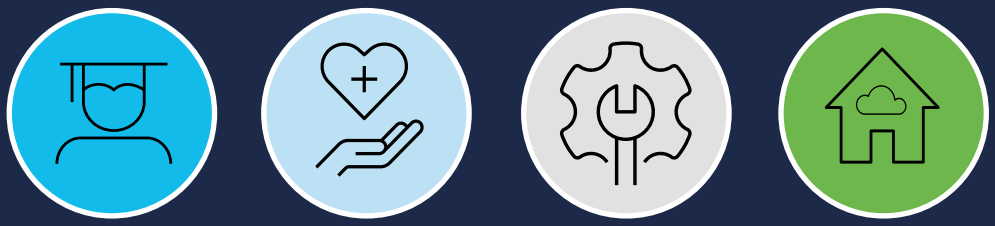
Ciscos tilgang til håndtering af personlige data i skyen

Vi mener, at Schrems II har øget behovet for at opbygge langsigtede relationer baseret på tillid mellem leverandører, kunder og partnere. At vise, at I beskytter hinandens privatliv og sikkerhed, vil være et højt prioriteret emne i nye forretningsforbindelser fremover.

Vi mener også, at tillid i høj grad bør være baseret på gennemsigtighed. At kunne vise i detaljer og på produktniveau, hvilke persondata der behandles, er en grundlæggende forudsætning for en sådan gennemsigtighed. Oplysningerne om, hvordan data behandles, bør være frit tilgængelige for kunder, partnere og offentligheden. På denne måde bliver også konsekvensvurdering og analyser af privatlivets fred muliggjort. Vi har arbejdet på dette hos Cisco i lang tid. Vi er gennemsigtige med, hvilke data der påvirkes ved brug af vores produkter og tjenester, om der er en international overførsel og hvilke risici der er forbundet med hvilken type data eller behandling der er berørt. Cisco behandler kun EU-personoplysninger på steder, hvor EU's databeskyttelsesstandarder kan opfyldes, og der kan ydes "i det væsentlige tilsvarende" beskyttelse.

Hvilke it-sikkerhedsbehov har kommunerne?

I dette kapitel vil vi beskrive vores syn på de it-sikkerhedsbehov, der er knyttet til det kommunale it-miljø. Selvom Danmarks 98 kommuner er organiseret på forskellige måder og har forskellige størrelser og forhold, så ser Cisco, at mange behov ligner hinanden. Vi indleder dette afsnit med at beskrive vores syn på fælles og basale kommunale behov. Vi præsenterer desuden en række virksomhedsspecifikke behov, der er opdelt i forretningsområderne skoler og daginstitutioner, omsorg og pleje, kritisk infrastruktur, fast ejendom og IoT. Grunden til, at vi har valgt at fremhæve netop disse områder, er, at vi har identificeret specifikke it-sikkerhedsudfordringer indenfor dem.



Hele kommunens behov

Behovsbeskrivelsen tager udgangspunkt i fire aktivitetsspecifikke kategorier. Det er uddannelse og børnepasning, omsorg og pleje, kritisk infrastruktur og fast ejendom og IoT. Udover erhvervskategorier har vi også identificeret en række overordnede IT-sikkerhedsbehov, som findes i store dele af den kommunale drift, og som er opsummeret i kategorien "Hele kommunens behov".

Hele kommunens behov

Den kommunale drift er yderst diversificeret, men vores erfaring er, at IT-sikkerhedsbehovet for store dele af driften stadig ser relativt ens ud, uanset hvilken drift det drejer sig om. Primært handler det om at stille værktøjer til rådighed på en sikker måde, der letter og understøtter hele kommunen i den daglige drift. IT-sikkerhed er efter vores mening et område, som helst ikke skal bemærkes af brugeren overhovedet.

I dette afsnit giver vi vores syn på seks grundlæggende behov, som ethvert kommunalt it-miljø skal opfylde.

At relevant lovgivning følges

I forhold til mange private organisationer, har kommuner en meget lovstyret drift. Et grundlæggende behov er derfor, at det kan garanteres, at al relevant lovgivning følges. Det lyder måske som en selvfølge – men i dag er der stor usikkerhed omkring mange problemstillinger knyttet til it-sikkerhed. I de senere år har EU's databeskyttelsesforordning (GDPR) fået stor opmærksomhed, men der er anden lovgivning (f.eks. Sundhedsloven, serviceloven og persondataloven), der regulerer hvordan en kommune må håndtere følsomme oplysninger. Fælles for alle disse love er, at de pålægger kommunen at håndtere data på en sådan måde, at det kun er personer, der skal have adgang til oplysninger, der får dem. Databeskyttelsesforordningens grundprincipper opsummerer det kommunale behov på en god måde[12].

Principperne betyder blandt andet, at en persondataansvarlig virksomhed:

- skal have opbakning i databeskyttelsesforordningen for at få lov til at behandle personoplysninger
- må kun indsamle personoplysninger til specifikke, specifikt specificerede og begrundede formål
- må ikke behandle flere personoplysninger, end der er behov for til formålene
- skal sikre, at personoplysningerne er korrekte
- skal slette personoplysningerne, når de ikke længere er nødvendige
- skal beskytte personoplysningerne, for eksempel så uvedkommende ikke får adgang til dem, og så de ikke går tabt eller tilintetgøres
- skal kunne påvise, at den overholder databeskyttelsesforordningen, og hvordan den gør det.

At den rette person har adgang til det rigtige system på det rigtige tidspunkt

I moderne virksomheder er digitale værktøjer og informationerne i disse værktøjer blevet en grundlæggende forudsætning for overhovedet at kunne udføre enhver virksomhed. Det forudsætter, at den rigtige person har adgang til det rigtige system og den rigtige mængde information på det rigtige tidspunkt. Det grundlæggende behov her er altså at sikre, at dette kan ske. Egentlig handler det om, at flere behov arbejder sammen.
Vi oplister disse nedenfor:

- Kommunen skal kunne stille information til rådighed mellem forskellige virksomheder (f.eks. skal virksomhedsledere have adgang til centrale økonomisystemer).

- For at relevant lovgivning kan følges, er der også behov for at sikre at kun autoriserede personer har adgang til følsomme oplysninger i de kommunale driftssystemer. Ud fra et it-sikkerhedsperspektiv er det derfor vigtigt at sikre, at brugerne har adgang til den rigtige information ved at garantere det modsatte – at den forkerte person ikke får adgang til information, som de ikke har krav på.

- For at ovenstående behov skal opfyldes, er det også nødvendigt for kommunen, at systemer og programmer kommunikerer med hinanden for at stille tilgængelige og sikre informationer i den rigtige rækkefølge. En person, der skifter stilling, skal f.eks. ikke kunne få adgang til samme styresystem som hidtil, medmindre det er nødvendigt for den nye faglige rolle

Stabil og sikker netadgang i kommunens lokaler

Mange kommunale aktiviteter har som tidligere nævnt gennemgået en omfattende digitalisering i de senere år. Vi ser, at denne tendens vil fortsætte og stige selv i den nærmeste fremtid.

Et stadigt voksende behov og brug af digitale funktioner, med flere brugere, øger behovet for sikre og stabile forbindelser i kommunens lokaler. Samtidig er der sket et skift mod et digitalt miljø, der i stigende grad fokuserer på bærbare enheder. I kommunal sammenhæng omfatter det alt fra at muliggøre netværksadgang for elever i skolerne til åbne netværk på biblioteker til at medarbejderne kan arbejde problemfrit.

Denne levering er således blevet en grundlæggende forudsætning for at muliggøre alle kommunens aktiviteter. Det handler dels om et behov for at sikre, at netadgangen ikke udgør et adgangspunkt til at trænge ind i kommunens infrastruktur. Derudover skal netværket klare en stadigt stigende mængde datatrafik, for at undgå overbelastning.

Tilstrækkelig kompetence inden for IT-sikkerhed blandt personalet

Som tidligere nævnt er et IT-miljø kun så sikkert, som brugerne gør det. Et flertal af alle cyberangreb initieres af, at en bruger i ens egen organisation klikker på et inficeret link eller åbner en fil sendt af en angriber. Når den ondsindede kode eller software, der er blevet indlejret, accepteres i systemet, kan det gøre meget skade på virksomheden. At være opmærksom på de mest almindelige metoder (f.eks. phishing) reducerer risikoen for vellykkede angreb. Samtidig er kendskabet til sådanne metoder generelt stadig lavt blandt mange it-brugere. I vores seneste trendrapport om IT-sikkerhed oplyser vi bl.a. at 86 % af alle organisationer har fået en medarbejder til at klikke på et inficeret link i et phishing-angreb[13].

At informationsaktiver og driftssystemer er beskyttet mod angreb

For at kommunen kan drive virksomhed i overensstemmelse med lovgivning og regler om fortrolighed, er det en grundlæggende forudsætning, at systemerne er tilgængelige og ikke penetreres af uvedkommende aktører. Der er derfor et klart behov inden for den kommunale drift for tilstrækkelig beskyttelse, så det ikke kan ske. Endvidere, skal kommunen sikre sig, at den har tilstrækkelig overvågning, mere eller mindre i realtid, så skaderne ved et eventuelt angreb kan minimeres. Behovet er egentlig ikke unikt for kommunal drift, men er ikke desto mindre relevant

Muliggør mobile arbejdsmetoder

Covid-19 pandemien har sat gang i en i forvejen stærk tendens til mere fleksibelt arbejde i store dele af arbejdslivet. I løbet af de seneste to år har både kommunalt ansatte og elever skullet udføre arbejde og skolearbejde på afstand. Selv i fremtiden forventes et stort antal kommunalt ansatte at arbejde på afstand i en vis periode. Det giver anledning til nye behov i kommunerne. For både studerende og ansatte er muligheden for at deltage i videomøder et krav. De skal desuden tilgå kommunens netværk på samme betingelser, som hvis de var på stedet i kommunens lokaler, og identificere sig over for dem for at opnå den korrekte brugerautorisation. Dette stiller nye krav ud fra et it-sikkerhedsperspektiv.

Når den traditionelle sikkerhed i forretningen har haft fokus på at sikre de miljøer, som medarbejderne indgår i, vil denne tendens betyde et væsentligt større fokus på at opretholde tilstrækkelig sikkerhed også i andre miljøer. Det har man også gjort før pandemien, men da skiftet er sket i, hvordan medarbejdere og arbejdsgivere ser på, hvad der er en egnet og attraktiv arbejdsplads, vil det stille helt nye krav til kommunens it-sikkerhedsløsninger.

Forretningsspecifikke behov

Ud over de behov, der er rapporteret ovenfor, har Cisco også identificeret en række virksomhedsspecifikke behov. Disse er baseret på særlige forretningsmæssige udfordringer knyttet til it-sikkerhed. Vi har organiseret disse

driftsbehov i de fire kategorier skoler og daginstitutioner, pleje og omsorg, kritisk infrastruktur og fast ejendom og IoT

Operationelle behov i skoler og daginstitutioner

Brug af computere og tablets er blevet mere reglen end undtagelsen i størstedelen af danske skoler. Fra børnehave og helt op til gymnasiet bruger danske elever digitale enheder i deres daglige skolearbejde. Mens eleverne skal have adgang til deres skolecomputere, er yngre brugere en mere udsat brugergruppe af digitale værktøjer. Dels i form af at de viser en større tilbøjelighed til at søge efter provokerende eller stødende materiale men også i den måde de bevidst forsøger at omgå de sikkerhedsprocedurer, der er opstillet på deres enheder. For at regulere og beskytte brugen af skolernes enheder, uden helt at lukke ned og mulighederne for at bruge internettet, ser vi derfor som to vigtige behov knyttet til uddannelses- og pasningsområdet.

Et flertal af alle kommuner bruger en form for skoleplatform. Disse bruges f.eks. at planlægge undervisning, stille arbejdsmaterialer til rådighed og kommunikere med elever og værger. Flere af disse platforme er cloud-baserede. Samtidig er store dele af den danske skolesektor skiftet til cloud-baserede løsninger til digitale undervisningsværktøjer. Disse er i det væsentlige Microsoft-baserede produkter eller produkter fra Google. Oplysninger om studerendes fremmøde og andre oplysninger, der behandles i sådanne cloudtjenester, skal være omgivet af en sådan beskyttelse, at alle parter kan være sikre på, at oplysningerne ikke kan tilgås af tredjeparter.

Driftsbehov i pleje og omsorg

Den kommunale pleje - både hvad angår ældrepleje og omsorg for mennesker med handicap - bruger i stigende grad digital driftsstøtte. Generelt er man ikke nået helt så langt her som i digitaliseringen af uddannelse og børnepasning, men der er taget vigtige skridt på vejen. Inden for forretningen har der historisk set været meget fokus på effektivitet og planlægning af forretningen. Det, der adskiller denne drift fra visse andre dele af kommunen, er, at driftssikkerhed og informationssikkerhed er af endnu større betydning givet de oplysninger, der håndteres. Dels ud fra hvor følsomme oplysningerne er, og dels ud fra hvor missionskritiske de er. Forenklet kan man sige, at en badevandstemperaturservice både kan gå ned og blotte alt sit data på nettet, uden at det påvirker kommunen væsentligt. Hvis det tilsvarende skulle ske i et system, der holder styr på en brugers medicinbehov, ville det være en alvorlig hændelse.

I takt med at flere produkter kommer på markedet, og graden af digitalisering er steget i virksomhederne, er velfærdsteknologi også begyndt at blive implementeret i virksomhederne. Dette kan omfatter alt fra digitale sikkerhedsalarmer og faldsensorer til natovervågningssystemer. Selv denne type løsninger stiller særligt høje krav til drifts- og IT-sikkerhed, givet de potentielle konsekvenser en afbrydelse vil have. Inden for pleje- og socialsektoren er der også en højere andel af personale med lav digital modenhed end i andre kommunale drifter. Det stiller også andre krav til it-sikkerhed end i andre virksomheder. Endelig er området også udliciteret til private entreprenører i en

højere andel end andre kommunale aktiviteter. Disse har dog i højere grad brug for adgang til de kommunale driftssystemer end fx friskoler. Der er derfor behov for at gøre disse systemer og denne information tilgængelige uden at udsætte systemerne for unødvendige risici.

Driftsbehov indenfor kritisk infrastruktur

Inden for rammerne af den kommunale serviceleverance indgår det at levere basale sociale funktioner til alle kommunens beboere. Hertil har vi valgt at medregne levering af rent vand, spildevand og energi. Alle kommuner har et ansvar for at sørge for vand og spildevand, mens det ikke er obligatorisk for kommunen at levere energiydelser. En række kommuner har valgt at samarbejde om vand- og spildevandsydelser enten gennem kommunalt samarbejde eller gennem virksomheder, der leverer ydelserne til flere kommuner. Ud fra et IT-sikkerhedsperspektiv stilles der andre krav til denne type drift ud fra de potentielt katastrofale effekter en afbrydelse i forsyningen ville have kunnet have. For at sikre, at driften opretholdes på en række samfundsvigtige områder, har EU vedtaget NIS og NIS2-direktivet[14]. Dette peger bl.a. energi og forsyning og distribution af drikkevand som regulerede områder. At en aktivitet er reguleret af NIS-direktivet betyder konkret, at kommunen er forpligtet til at opretholde et højt fælles sikkerhedsniveau i netværk og informationssystemer, der styrer aktiviteten.

Kommunerne har altid haft et særligt ansvar for, at sådanne fællesskabsfunktioner fungerer tilfredsstillende, men de seneste år er lovgivningen blevet yderligere strammet. Udover de krav, der er fastsat inden for rammerne af NIS-direktivet, der har til formål at sikre, at samfundsvigtig drift kan fortsætte, uanset hvordan kommunens øvrige IT-miljø påvirkes, er der også specifikke behov knyttet til området kritisk infrastruktur, som ikke er reguleret ved lov. Det handler blandt andet om at skabe en central styring af driftsteknologi (OT) enheder. OT-enheder kan ganske enkelt beskrives som hardware og software, der bruges til at overvåge eller kontrollere industrielt udstyr[15]. Mange af disse enheder er tæt forbundet med det udstyr, de skal kontrollere, og de er ofte relativt gamle og derfor sårbare over for it-angreb.

Erhvervsbehov inden vfor fast ejendom og IoT

Næsten alle kommuner har en eller anden form for egen fast ejendom. Det kan være idrætshaller, skoler og kommunale bygninger, hvori der drives kommunale aktiviteter. Et flertal af kommunerne har også kommunale boligselskaber, der har til formål at skaffe udlejningsejendomme til de kommunale beboere. Ejendomsbeholdningerne er ofte omfattende, og at få central kontrol til overblik og optimering kan derfor betyde store besparelser for kommunen. Tilsvarende som inden for VA og energi er der også behov for at skabe en central styring af de OT-enheder, der findes i sådanne ejendomme. Også her er mange af systemerne ældre og sårbare, og selvom det ikke er så driftskritisk som kritisk infrastrukturområdet, er der også her et stort behov for driftssikkerhed.

Behovet stiger i takt med, at kommunerne vælger at digitalisere og muliggøre central styring af produkter, der er af driftskritisk karakter, såsom låse eller styringsanlæg til ventilation Udover at sikre en smidig og sikker drift af ældre OT-

anlæg, er der også en voksende behov for at styre mængden af smarte enheder, der installeres i kommunerne med det formål at få intelligente ejendomme og Smart Cities. Der er ingen entydig definition af disse begreber, men fælles er at bruge IT til at forbedre ressourceanvendelsen, dele information med offentligheden og opnå højere kvalitet i det kommunale servicetilbud[16]. Konkret omfatter dette brug af enheder, der er baseret på tingenes internet (IoT) eller tingenes internet. Her handler det ofte om at indføre teknisk infrastruktur, der indsamler data eller agerer autonomt i bymiljøet.

Potentialet i sådan teknologi er stort, og i dag bruges enheder f.eks. i ejendomsbesiddelser til varme- og fugtmålere eller til luftmåling i bymiljøet. Ud fra et it-sikkerhedsperspektiv stiller det særlige krav. Alle disse enheder er placeret i et bymiljø, men har samtidig brug for netværksadgang. Ydermere har it-sikkerheden i IoT-enheder historisk set været relativt mangelfuld. Dette er dog blevet bedre, efterhånden som markedet er blevet modnet.

Hvilke funktioner kræves for at imødekomme de kommunale behov?

Præsentation af Ciscos kort over funktioner for sikre kommuner

I dette afsnit præsenterer vi Ciscos forslag til overblik over funktioner for sikre kommuner. Det er designet til at imødekomme de behov, der er kortlagt i det foregående afsnit, og til at gøre det på en sikker og omkostningseffektiv måde. Ligesom behovsafsnittet vhar vi valgt at præsentere disse funktioner fordelt på et overordnet niveau og på et aktivitetsspecifikt niveau.

Organisationsspecifikke funktioner

- Særligt omkostningseffektive løsninger for elever
- Overvågning af følsomme data i cloud-tjenester
- Mobile enheder som deles af flere brugere
- Imødekomme NIS-direktivets krav
- Webfilter til studerende
- Begrænset informationsdeling med private entreprenører
- Sikker styring af OT- og IoT-enheder

Funktioner for hele kommunen

- Beskyttet infrastruktur
- Sikker adgang til de rigtige applikationer og informationer
- Omkostningseffektivitet og automatisering
- Hurtig detektering og afhjælpning af indtrængen
- Sikkert fjernarbejde/hybridarbejde
- Beskyttede enheder/klienter
- Tilstrækkelig kompetence hos medarbejdere og brugere
- Udbyde netværk til tredjeparter

Kompetencer for hele kommunen

Visse it-kompetencer er grundlæggende og nødvendige i alle dele af den kommunale drift. Dette omfatter f.eks. grundlæggende evne til at beskytte infrastruktur og enheder og mulighed for at tilslutte medarbejderes og gæsters udstyr til kommunale netværk på en sikker måde. Nedenfor har Cisco listet otte væsentlige muligheder, som vi ser som afgørende for hele kommunens it-sikkerhed.

Funktion	Beskrivelse	Kategori
Beskyttet infrastruktur	At kunne beskytte dit netværk mod eksterne trusler er afgørende for kommunernes it-sikkerhed. Det drejer sig om firewalls, web- og e-mailfiltre, men også segmentering af det kommunale netværk.	
Sikkert fjernarbejde/ hybridarbejde	I takt med at kommunens medarbejdere i stigende grad arbejder på afstand, stilles der stadig højere krav til at tilbyde et beskyttet it-miljø også i medarbejdernes hjem. Det kræver, at kommunerne kan sørge for både sikre forbindelser til kommunens applikationer og systemer og tilstrækkelig beskyttelse af enheder også uden for den almindelige arbejdsplads. Fjernarbejde har også øget behovet for sikre forbindelser til cloud-baserede systemer.	
Sikker adgang til de rigtige applikationer og informationer	At kunne segmentere netværk, så brugerne kun får adgang til det, de har brug for i deres rolle, er vigtigt både for at opretholde kommunens overordnede krav til informationssikkerhed (GDPR, Persondataloven mv.). Det er også vigtigt at forhindre malware i at bevæge sig frit mellem forskellige enheder i det interne netværk.	
Beskyttede enheder/klienter	Beskyttelse af netværkets enheder/klienter (f.eks. computere og mobiltelefoner) er afgørende for muligheden for at stoppe ondsindet software, der vil ind på en kommunes netværk. Beskyttelse af enheder mod sådanne trusler stiller høje krav til både de anvendte tekniske produkter og brugernes viden (se nedenfor).	
Omkostningseffektivitet og automatisering	Mange kommuner har stramme budgetter og skal derfor effektivisere og automatisere driften i det omfang det er muligt. Stordriftsfordele og fælles standarder letter det arbejde og bidrager med lavere omkostninger, men også et mindre komplekst it-miljø (hvilket reducerer behovet for yderligere sikkerhedsforanstaltninger).	

Funktion	Beskrivelse	Kategori
Tilstrækkelig kompetence hos medarbejdere og brugere	At medarbejderne har en god forståelse for, hvordan man bruger kommunale it-systemer og digitale enheder på en sikker måde, er afgørende for den kommunale it-sikkerhed. Phishing, malware og andre angrebsmetoder, der forsøger at trænge ind i en kommunes netværk, kan ofte lykkes pga. af medarbejdere, der ubevidst lader angriberen komme ind ved f.eks. klik på et link. Løbende uddannelse af personalet er derfor en vigtig del af en kommunes it-sikkerhedsarbejde.	
Hurtig detektering og afhjælpning af indtrængen	For hvert sekund, der bruges skadelig software eller kode i en kommunes netværk, øges risikoen for storstilet datatab, sabotage eller andre negative forretningsmæssige effekter. Det er derfor af stor betydning, at kommuner hurtigt kan opdage og afhjælpe indbrud i deres egne systemer.	
Udbyde netværk til tredjeparter	Mange af brugerne af kommunernes netværk er ikke ansatte eller brugere af kommunens ydelser. Det kan f.eks. omhandle besøgende, der kobler deres egne computere til rådhusets Wi-Fi eller i lokalerne til den kommunale drift. Da kommuner dagligt har kontakt til en lang række virksomheder, kommunale beboere og andre repræsentanter, er det også nødvendigt at kunne tilbyde en sikker forbindelse til disse brugere.	

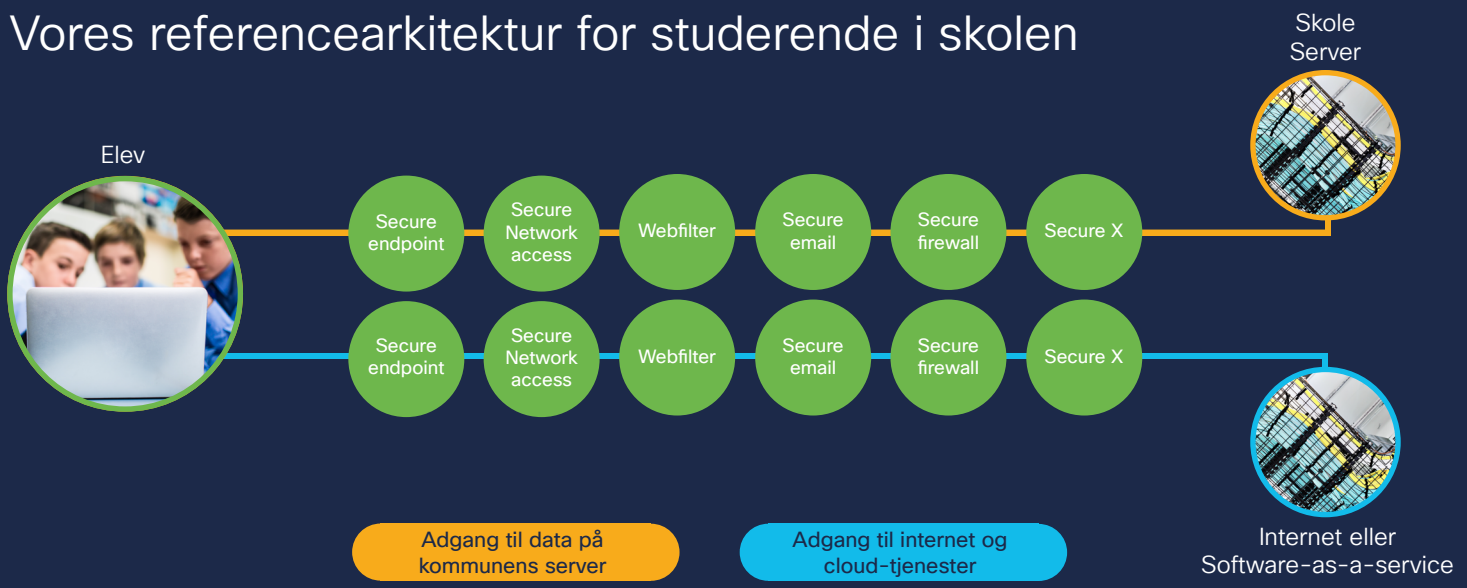
Forretningsspecifikke evner

Funktion	Beskrivelse	Kategori
Særligt omkostningseffektive løsninger for studerende	Mange kommuner har begrænsede ressourcer til investeringer i it-sikkerhed. Studerende udgør en stor gruppe af it-brugere, og kommuner skal derfor kunne tilbyde omkostningseffektive og skalerbare sikkerhedsløsninger. Generelt har eleverne også en højere risikoprofil end kommunalt ansatte, hvilket betyder, at sikkerhedsløsninger er særligt relevante.	
Overvågning af følsomme data i cloud-tjenester	Da cloud-baserede tjenester bruges til fjernundervisning og i kontakt mellem elever, lærere og værger, skal en kommune være i stand til at beskytte og overvåge potentielt følsomme data, der deles mellem dem.	

Funktion	Beskrivelse	Kategori
Webfilter til studerende	En vigtig evne for skolen er at kunne levere velfungerende webfiltre, der begrænser elevernes muligheder for at tilgå farligt eller upassende materiale på skolens enheder. Filteret skal virke både i og uden for skolens område.	
Mobile enheder, der kan deles af flere brugere	Inden for hjemmeplejen skal kommunen kunne rumme medarbejdere, der deler mobile enheder (mobiltelefoner, tablets) med kolleger, mens disse kun får adgang til personoplysninger om brugere, som de har brug for i deres daglige arbejde. At brugernes personlige integritet skal respekteres, er lovgivet i persondataloven.	
Begrænset informationsdeling med private entreprenører	Kommunerne skal kunne dele driftsrelevante oplysninger (persondata mv.) med private udbydere af velfærdsydelser (f.eks. hjemmeplejevirksomheder). Samtidig er det af stor betydning, at sådanne entreprenører ikke får større adgang, end det er begrundet i deres mission.	
Leve op til kravene i NIS-direktivet	Kommuner skal være i stand til særlige sikkerhedsløsninger i netværk, der kan kobles til samfundskritisk tjenester (fx digital infrastruktur, energi og forsyning/distribution af drikkevand) i henhold til NIS-direktivet.	
Sikker styring af OT- og IoT-enheder	Kommunerne skal kunne opretholde kommunikationen mellem centrale it-systemer og driftens OT- og IoT-enheder på en sikker og stabil måde. Centraliseret drift og sikkerhedsovervågning er en afgørende komponent i det arbejde.	

Reference-arkiteturer for en sikker kommune

Nu hvor vi har forklaret vigtige kommunale behov og muligheder, vil vi give nogle eksempler på, hvordan disse konkret kan håndteres gennem et sæt af vores løsninger. Vi kalder det Ciscos referencearkitekturer for en sikker kommune. Vi er klar over, at ingen kommuner har en blank tavle, og at der er mange måder at løse de sikkerhedsmæssige udfordringer på. Her giver vi dog vores bud på, hvordan Ciscos løsning kan struktureres fra bunden. I dette kapitel har vi valgt at visualisere og beskrive Ciscos referencearkitekturer til fire typiske kommunale behov. Disse demonstrerer også på en god måde, hvad vi ser som et formålstjenligt set-up for en tryg kommune. Hvis du er interesseret i at se yderligere eksempler på referencearkitekturer til andre forretningsbehov, bedes du kontakte din Cisco-sælger.



Referencearkitektur for studerende i skolen

Som beskrevet i færdighedskapitlet udgør eleverne en meget stor brugergruppe, der skal kunne koble sig på kommunens digitale miljø både hjemmefra og fra skolen. I næsten alle kommuner vil eleverne befinde sig forskellige steder, når de opretter forbindelse til skolens server eller cloud-tjenester. Nedenfor beskriver vi vores referencearkitektur for en elev i skolens lokaler.

- For at en elev kan få adgang til deres skolemateriale, skal elevens enhed (computer/mobil/tablet/chromebook) være tilsluttet et netværk (ofte skolens eget netværk). Uanset hvor eleven opretter forbindelse, har enheden allerede grundlæggende beskyttelse mod malware via det sikre slutpunkt. Denne løsning svarer til evnen Beskyttede enheder/klienter.

- Hvis eleven herefter ønsker at koble sig på kommunens netværk, anvendes Ciscos Secure netværksadgangsløsning til at sikre, at eleven reelt har ret til at få adgang til de efterspurgte informationer, gennem netværkssegmentering af brugerne. Løsningerne svarer til evnen Sikker adgang til de rigtige applikationer og informationer.

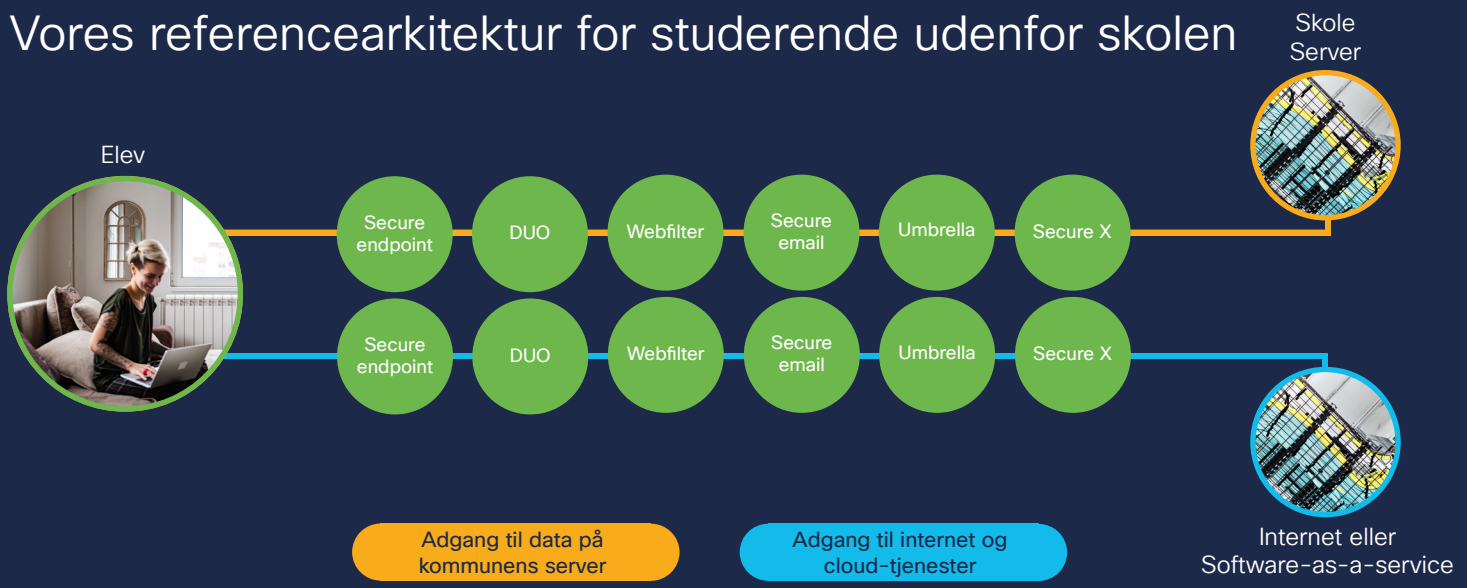
- Når eleven forbinder sin computer via skolens netværk, er Ciscos webfilter slået til, for at forhindre eleven i at besøge sider med skadeligt eller upassende indhold. Løsningen svarer til funktionen Web-filter i skoler og hjem.

- Til elevens mailprogram kræves et særligt værktøj, der beskytter mod ondsindede phishing-forsøg. Behovet kan udfyldes gennem de funktioner, der er tilgængelige i Ciscos Secure email og svarer til funktionen Beskyttede enheder.

- Hvis eleven opretter forbindelse via skolens netværk, bruges Ciscos Secure firewall til at beskytte elevens enhed mod skadeligt materiale eller programmer. Løsningerne svarer til evnen Beskyttede enheder/klienter og Overvågning af følsomme data i cloudtjenester.

- Kommunen bør desuden have en central mulighed for at overvåge webtrafik fra elevernes computere, for at sikre at der ikke kommer malware ind i skolens enheder. En sådan overvågning kan effektivt styres gennem Secure X, en cloud-baseret platform til overblik over hele kommunens it-sikkerhed. Løsningen svarer til evnen Hurtig detektering og håndtering af indtrængen

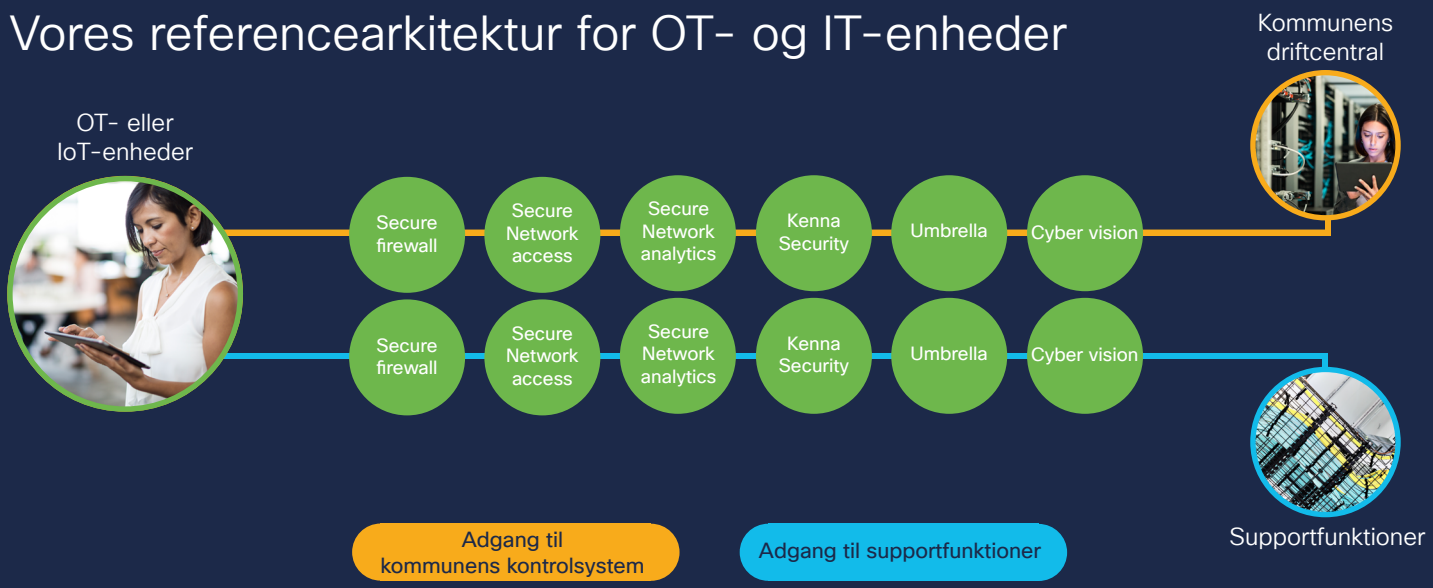
Cisco er opmærksom på det ofte pressede budget, der er indenfor kommuneskolen. Vores løsning til studerende kan derfor tilbydes til en meget konkurrencedygtig pris, uden at det går ud over sikkerhed eller brugervenlighed. Dette svarer til funktionen Særligt omkostningseffektive løsninger for studerende.



Referencearkitektur for elever uden for skolens netværk

Eleverne udfører en stor del af deres skolearbejde uden for skolens område. Uanset om eleven er på et bibliotek, på en café eller i hjemmet, skal skoleenheden forblive beskyttet. Her beskriver vi vores referencearkitektur for en elev uden for skolens område.

- For at en elev kan få adgang til sit skolemateriale, skal elevens enhed (computer/mobil/tablet/chromebook) være tilsluttet et netværk (ofte) elevens Wi-fi derhjemme). Uanset hvor eleven opretter forbindelse, har enheden allerede grundlæggende beskyttelse mod malware via det sikre slutpunkt. Denne løsning svarer til funktionen Beskyttede enheder/klienter-kapaciteten.
- Hvis eleven herefter ønsker at tilslutte sig kommunens netværk, anvendes Ciscos løsning til to-faktor login, DUO, der opfylder samme funktion som Sikker netværksadgangsløsning, for at sikre, at den studerende reelt har ret til at deltage i de ønskede oplysninger. Løsningerne svarer til funktionen Sikkert fjernarbejde/hybridarbejde og Sikker adgang til de rigtige applikationer og informationer.
- Hvis eleven tilslutter sin computer derhjemme, er Ciscos webfilter slået til, for at forhindre eleven i at besøge sider med skadeligt eller upassende indhold. Løsningen svarer til evnen Web-filter i skoler og hjem.
- Til elevens mailprogram kræves et særligt værktøj, der beskytter mod ondsindede phishing-forsøg. Behovet kan udfyldes gennem de funktioner, der er tilgængelige i Ciscos Secure email og svarer til funktionen Beskyttede enheder.
- Når forskellige cloud-baserede tjenester som f.eks. Google Classroom bruges, der er behov for kontinuerlig beskyttelse af datatrafikken, der bevæger sig mellem elevens enhed og cloud-tjenesten. Ciscos løsning Umbrella kan bruges til netop det behov. Løsningen svarer til funktionen Beskyttede enheder/klienter og Overvågning af følsomme data i cloud-tjenester.
- Kommunen bør desuden have en central mulighed for at overvåge webtrafik fra elevernes computere, for at sikre at der ikke kommer skadelig software ind i skolens enheder. En sådan overvågning kan effektivt styres gennem Secure X, en cloud-baseret platform til overblik over hele kommunens it-sikkerhed. Løsningen svarer til funktionen Hurtig detektion og afhjælpning af indtrængen.



Referencearkitektur for OT og IoT

Ved udvikling af en referencearkitektur til OT- og IoT-enheder bør den første prioritet være at adskille særligt følsomme enheder fra resten af netværket. Gennem en sådan segmentering kan der foretages individuelle risikovurderinger for at give internetadgang til systemer, hvor det vurderes at være risikofrit eller nødvendigt, såsom leverandørers servicesystemer eller kommunens betroede driftscenter. Nedenfor opsummerer vi vores overordnede referencearkitektur for OT- og IoT-enheder.

- For at forhindre forkert kommunikation mellem OT- eller IoT-enheder og netværket, sker der først en netværkssegmentering gennem Cisco sikker netværksadgang og Cisco firewall. Med disse værktøjer er adgangen til OT og IoT spærret for uautoriserede personer. Produkterne er vigtige komplementer til hinanden og svarer til funktionen Beskyttet infrastruktur og/eller Beskyttede enheder/klienter og Sikker adgang til de rigtige applikationer og informationer.

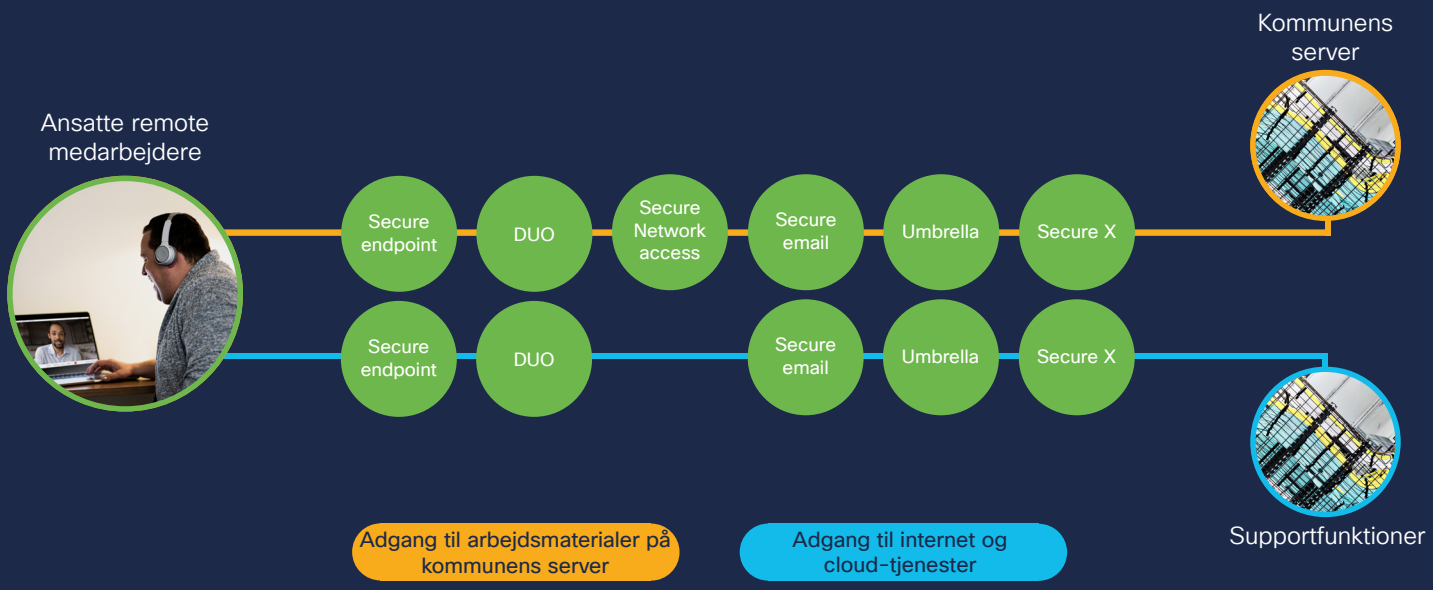
- For yderligere at sikre, at der ikke finder uautoriserede indtrængningsforsøg sted inden for den følsomme infrastruktur, er Ciscos værktøj Sikker netværksanalyse er en vigtig brik i et puslespil. Det bruges til at overvåge, hvad der sker udenfor i OT-miljøet. Denne løsning svarer til funktionen til hurtig indtrængningsdetektion og -afhjælpning.

- Et andet vigtigt supplement inden for driftsovervågning er Kenna, som er et værktøj til at evaluere og vurdere, hvilke trusler der bør prioriteres. Det er af særlig betydning ved styring af OT-ressourcer, da sådanne enheder (f.eks. vandværker) ikke på noget tidspunkt kan lukkes ned eller genstartes (og dermed opdatere drivere/installere ny software). Derfor, når en trussel er identificeret, skal den løbende overvåges, indtil den kan adresseres gennem softwareopdateringer. Denne løsning reagerer også på funktionen Hurtig detektion og afhjælpning af indtrængen.

- Efterhånden som it-systemer, cloud-tjenester og kontrolnetværk til OT-enheder er integreret, øges trusselsrisikoen mod OT- og IoT-enheder. Til kontinuerlig operationel overvågning af alle disse dele og effektiv trusselsdetektion og driftsinformation fra systemerne, har Cisco udviklet CyberVision-løsningen. Produktet er specielt udviklet, så medarbejdere med ansvar for OT-enheder kan sikre driftskontinuitet, robusthed og sikkerhed. Løsningen svarer til funktionen Hurtig detektion og afhjælpning af indtrængen og Sikker styring af OT- og IoT-enheder.

Løsningerne beskrevet ovenfor er alle vigtige puslespilsbrikker, der tilsammen bidrager til den kommunale funktion Sikker håndtering af OT- og IoT-enheder og kommuners mulighed for at leve op til kravene i NIS-lovgivningen.

Vores referencearkitektur remote kommunalt ansatte



Referencearkitektur for kommunale ansatte der arbejder decentralt

På samme måde som fjernarbejdende elever har kommunalt ansatte fjernarbejdere brug for sikker og stabil adgang til kommunens netværk. Dette svarer også til de kompetencer, der er specifikke for Pleje- og støtteområdet – nemlig Mobile enheder, der kan deles af flere brugere og Begrænset informationsdeling med private entreprenører.

- Også her en grundlæggende beskyttelse af den kommunalt ansattes enhed (computer/mobil/tablet) er påkrævet, når den tilsluttes et netværk, der ikke er kommunens (f.eks. medarbejderens hjemmenetværk). Behovet er sikret gennem Secure endpoint. Denne løsning svarer til funktionen Beskyttede enheder/klienter.
- For at medarbejderen kan få adgang til det fælles netværk, benyttes ofte en VPN-tunnel. Denne forbindelse er garanteret gennem Ciscos sikre fjernadgang. Ciscos løsning DUO bruges til at identificere sig selv og vise, at enheden lever op til kommunens krav til tilsluttede enheder. Løsningerne svarer til funktionen Sikkert fjernarbejde/hybridarbejde og Sikker adgang til de rigtige applikationer og informationer.
- Godt forbundet til det kommunale netværk, her bruges også Sikker netværksadgang. Dette er for at sikre, at den tilsluttede bruger modtager den rette autorisation til at få adgang til de ønskede oplysninger. Løsningen svarer til funktionen Sikker adgang til de rigtige applikationer og informationer.
- Da e-mail er et af de vigtigste arbejdsredskaber for medarbejderne, åbner mange mennesker deres e-mailklient med det samme, når arbejdsdagen begynder. Her kræves, ligesom for eleven, et godt forsvar mod ondsindede phishing-mails, gennem Cisco Secure-e-mail. Løsningen svarer til funktionen Beskyttede enheder/klienter.
- Da mange kommuner giver medarbejderne mulighed for at bruge deres computer til private anliggender, er der også behov for løbende overvågning af webtrafik, når fjernmedarbejderen er tilsluttet internettet. Ciscos Umbrella-løsning bruges her for at kunne vedligeholde funktionen Hurtig detektion og håndtering ved indtrængen og Sikkert fjernarbejde/hybridarbejde.
- Kommunen bør også her have en central mulighed for at overvåge webtrafik for at sikre, at ingen skadelig software får ind i kommunens enheder. En sådan overvågning kan effektivt styres gennem Secure X, en cloud-baseret platform til overblik over hele kommunens it-sikkerhed. Løsningen svarer til funktionen Hurtig detektion og afhjælpning af indtrængen.

Bilag

Sådan kan Cisco bidrage til at styrke de kommunale kompetencer

I dette bilag kan du selv se, hvilke løsninger vi i Cisco kan tilbyde din kommune ud fra de kompetencer, der er identificeret i tidligere afsnit.

Vil du vide mere om, hvordan Cisco kan hjælpe dig med at designe en sikker kommune?

Kontakt

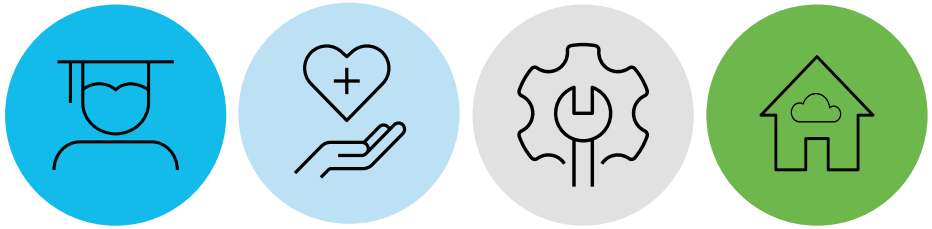
Kenneth Schwartz
Cyber Security Lead
keschwar@cisco.com
+4540490870

Rasmus Kamper Mathiasen
Sales Director, Public
rkamperm@cisco.com
+4540359677

Match mellem funktion og Ciscos tilbudte løsning – hele kommunen

Ciscos tilbudte løsning	Beskyttet infrastruktur	Sikker adgang til de rigtige applikationer og informationer	Omkostningseffektivitet og automatisering	Hurtig detektering og afhjælpning af indtrængen	Sikker fjernarbejde / Hybridt arbejde	Beskyttede enheder / Klienter	Tilstrækkelig kompetence hos medarbejdere	Udbyde netværk til tredjeparter
Cyber Vsion	●			●				
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	●	●	●	●	●	●	●	

Match mellem funktion og Ciscos tilbudte løsning – organisationsspecifikt



Ciscos tilbudte løsning	Særligt omkostnings-effektive løsninger	Overvågning af følsomme data i cloud-tjenester	Webfilter til studerende	Mobile enheder som deles af flere	Begrænset informationsdeling med private	Imødekomme NIS-direktivets krav	Sikker styring af OT- og IoT-enheder
Cyber Vsion							●
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	●	●	●			●	●

Referencer

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

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

3 Compouterworld 2020: Hackerangreb koster i gennemsnit de ramte virksomheder 16,5 millioner kroner
https://www.computerworld.dk/art/277667/hackerangreb-koster-i-gennemsnit-de-ramte-virksomheder-16-5-millioner-kroner

4 IT Branchen 2020: Nu er cyberkriminaliteten blevet personlig
https://itb.dk/nyheder/nu-er-cyberkriminaliteten-blevet-personlig/

5 To sygehuse i Region-syd udsat for hacker-angreb (2017)
https://www.dr.dk/nyheder/regionale/syd/sygehuse-i-region-syd-udsat-hacker-angreb

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

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

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

9 Folketal fra Danmarks Statistik
https://extranet.dst.dk/pyramide/pyramide.htm#!&t=1

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

11 Partier frygter mangel på IT-sikkerhedsfolk (2022) Version2
https://www.version2.dk/artikel/partier-frygter-akut-mangel-paa-it-sikkerhedsfolk-som-jeg-ser-det-kan-vi-ikke-goere-andet

12 Databeskyttelsesforordningen (2017) Datatilsynet
https://www.datatilsynet.dk/media/6559/generel-informationspjece-om-databeskyttelsesforordningen.pdf

13 2021 Cyber security threat trends (2021) Cisco
https://umbrella.cisco.com/info/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

14 NIS-directive (2023) The European Union Agency for Cybersecurity (ENISA)
https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

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

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