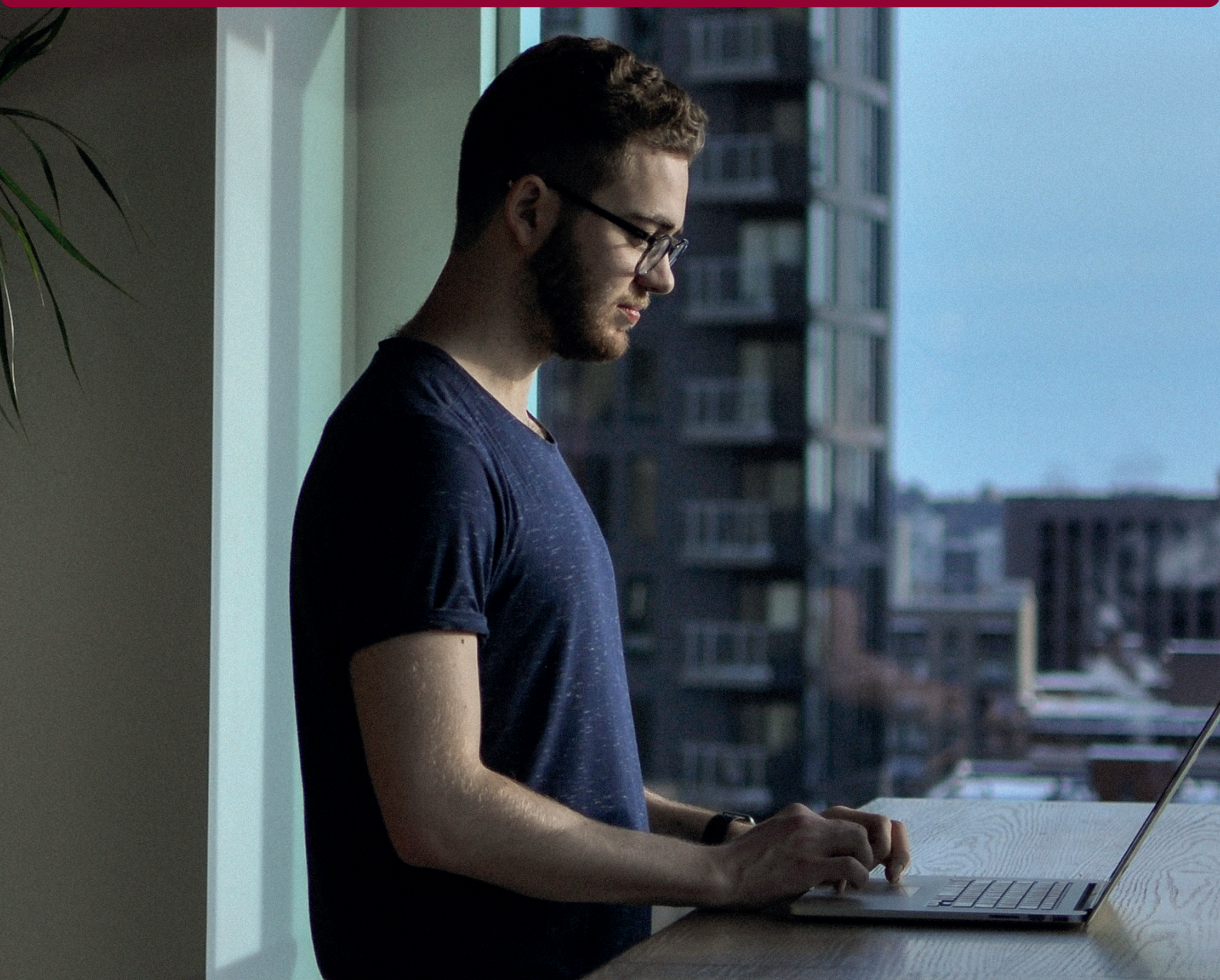
Dustin

Sikkerheds-udfordringer i digitaliseringens tidsalder



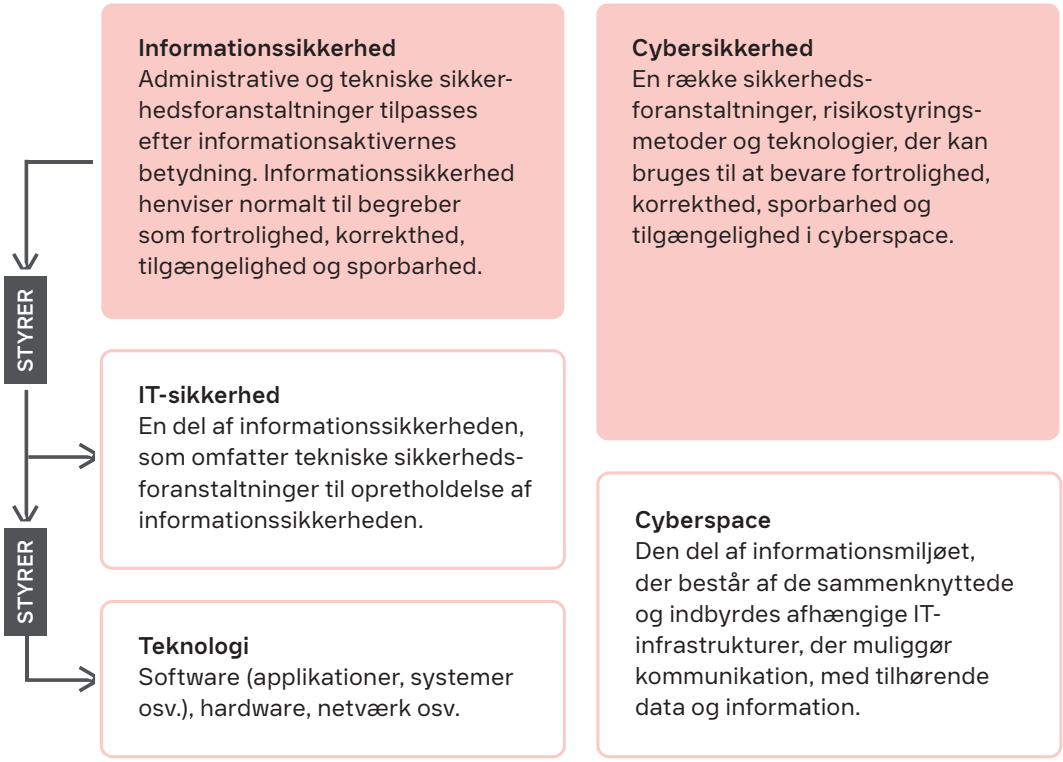
Indhold

1. Hvad betyder sikkerhed i dag?

I takt med, at digitaliseringen i stigende grad slår rod i alle dele af samfundet, forventes det af flere og flere, at man ikke kun forstår og reflekterer over digitaliseringen, men også at man bidrager til den. Til trods for den stigende aktualitet af cyber- og informationssikkerhedsspørgsmål er det nogle gange at afgrænse begreberne og adskille dem fra hinanden. Vi er vant til at sørge for vores fysiske sikkerhed med døre og låse, men med digitaliseringen har vi revet væggene ned og åbnet korridorer til andre virksomheder, og nogle gange meget hurtigt. Det har vi gjort bevidst for at håndtere øget konkurrence og stigende forventninger.

Med internettets globalisering bliver dele af den geografiske beskyttelse i den fysiske verden revet ned, og det øger efterspørgslen efter nye sikkerhedsmekanismer. Den øgede digitale kompleksitet skal håndteres med større klarhed, især når personer i stigende grad udsættes for risici, der tidligere kun ramte IT-organisationen. Hermed bliver sikkerhedsspørgsmål relevante for næste alle og enhver, selvom man ikke arbejder regelmæssigt med sikkerhed. Selv for den indviede er det nogle gange svært at skelne mellem fysisk sikkerhed, informationssikkerhed, IT-sikkerhed og cybersikkerhed.

Nøjagtige definitioner er ikke altafgørende, men hvis man ønsker at følge med i de daglige nyheder, kan man som læser med fordel anvende den forenklede begrebsmodel, som Radar bruger i sine analyser og rapporter.



IT-sikkerhed har som primært formål at beskytte data, der allerede har eller kan forædles til information. Datasikkerhed er den del af IT-sikkerheden, der omhandler teknisk beskyttelse af selve systemerne og dataene. Den omfatter bl.a. metoder til kryptering, godkendelse og beskyttelse mod overbelastningsangreb. Informationssikkerhed omfatter IT-sikkerhed samt processer og procedurer til at opretholde den nødvendige integritet, fortrolighed og tilgængelighed for informationen. En tommelfingerregel er, at arbejdet med informationssikkerhed beskriver, hvad der skal gøres, mens arbejdet med IT-sikkerhed snarere beskriver, hvordan dette skal gøres med teknologi og værktøjer.

Informationssikkerhed omfatter ikke kun IT-sikkerhed, men har også relationer til cybersikkerhed, der forener sikkerheden i forbindelse med forbundne informationsaktiver (især forbundet til internettet). Det er dette aspekt, der især berører den forbundne verden, vi har i dag.

2. Sikkerhed i en bølge af digitalisering

Fortsat digitalisering og optimering af digitale processer i svenske virksomheder er en nødvendighed. Ifølge Radars data har øget digitaliserings- (64 %) og automatiseringsgrad (46 %)1 samt indførelse af nye applikationer (44 %)1 således den højeste prioritet inden for IT.

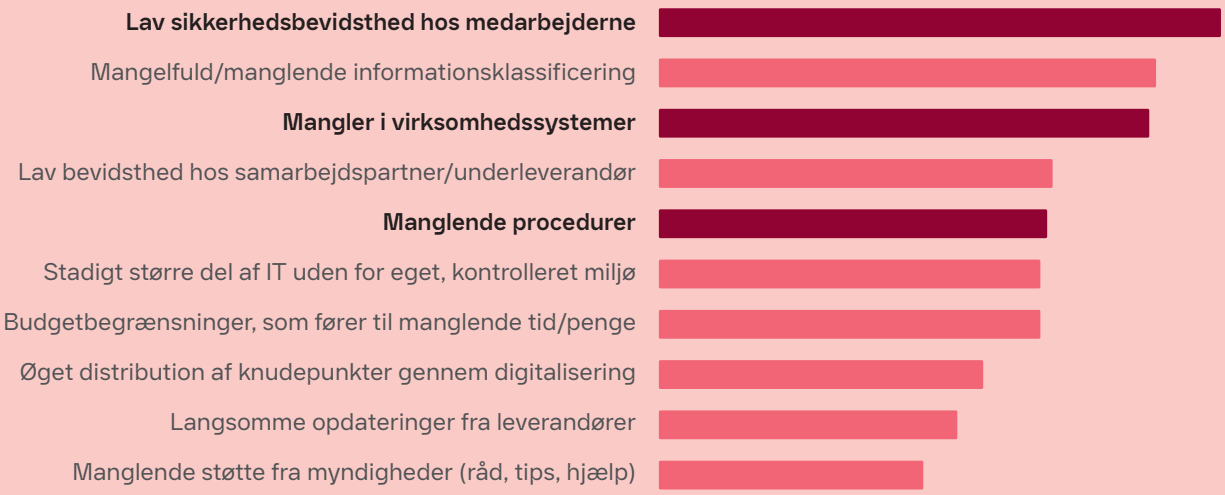
Samtidig genererer alt dette stadigt stigende datamængder, blandt andet på grund af øget brug af cloud-tjenester og IoT. Det giver mere intensive (kvantitet) og mere anvendelige (kvalitet) datastrømme. Gennem komplekse kæder skabes der værdi fra information, der tidligere har været uinteressant og ikke-målbar. Udviklingen har bredt sig, og man stræber i stigende grad efter mere fleksible forretnings- og virksomhedsmodeller, hvor datastrømmene kan udnyttes bedre.

De længere kæder bliver dog mere komplekse og dermed vanskelige at overskue ud fra et sikkerhedsperspektiv. I dag ser mere udviklede virksomheder i høj grad digitaliseringens øgede distribution af knudepunkter som en hindring i sikkerhedsarbejdet. Hos mindre udviklede virksomheder er der langt mindre bevidsthed om dette spørgsmål.

Udfordringen ligger i at forstå, hvordan information lever gennem hele den lange kæde. Med andre ord en forståelse af, hvornår informationen er i hvile, hvornår den bevæger sig eller er under brug, og hvem eller hvad, der har adgang til den. Svagheder i kæden kan føre til mistet forretningsinformation, effektivitetstab, kvalitetsmangler og/eller mindsket tillid. Det kan igen føre til øgede omkostninger, forringet konkurrenceevne eller i værste fald en risiko for samfundet som helhed.

Et realistisk udgangspunkt er, at intet sikkerhedsarbejde er perfekt. Radars mest almindelige anbefaling for udførelsen af sikkerhedsarbejdet er, at det skal være forsvarligt ikke bare juridisk, men frem for alt operationelt. Det skal fungere i praksis. Digitalisering uden at give afkald på sikkerhed, både for ens egen virksomhed, partnere og borgere, er en stor udfordring. En overset programrettelse, en utilsigtet åbning af en vedhæftet fil i en mail eller indtrængen hos en IT-leverandør kan få ødelæggende konsekvenser i dag. Ud over sikkerhedsforståelsen hos virksomhedens egne medarbejdere er mangel på procedurer og sikkerhedsbrister i virksomhedens systemer nogle af de vigtigste barrierer i dag.

10 største oplevede barrierer for sikkerhed i 2020



[1] Andel af svenske virksomheder, der ifølge rapporten IT-Radar 2020 prioriterer hvert enkelt område.
[2] Kortlægning af svensk cybersikkerhed 2020, Radar

Udveksling af information kræver, at den sikkerheds-fremmende indsats er afbalanceret og motiveret, hvilket er en udfordring i sig selv. En vurdering af den nuværende situation med fokus på behov og forudsætninger giver som regel et bedre udgangspunkt for fremtidige investeringer og ændringsprocesser, herunder arbejdet med overholdelse og opfyldelse af nye krav. Her er indsatser, der sigter mod at styrke virksomheden gennem kompetenceforbedrende tiltag på individuelt niveau, af stor betydning. Ikke mindst fordi lav sikkerhedsbevidsthed hos eget personale anses for at være en stor forhindring for at opretholde tilfredsstillende sikkerhed.

Et højt ændringstempo betyder stigende forventninger og krav om hurtig adgang til nye tjenester med øget effektivitet. Arbejdet med cyber- og informationssikkerhed retter sig dermed ikke kun mod ressourcer i form af penge, tid og evner, men nogle gange også mod faktorer som bekvemmelighed og frihed. Når stadigt kortere cyklustider belønnes, risikerer dynamikken at ændre sig fra en forsigtig tilgang til, at man tager højere risici. Det giver risiko for, at sikkerhedsarbejdet forsømmes på et tidligt tidspunkt. Ud fra et sikkerhedsmæssigt perspektiv er det problematisk, at stadigt kortere cyklustider fører til belønning af styringsmodeller og arbejdsmetoder, der er tænkt til at lette digitaliseringen af de offentlige myndigheders skatteinddrivelse.

Vores almindeligt udbredte ITIL-rammesystemer og agile metoder giver ikke IT-organisationen og resten af virksomheden tilstrækkelig støtte til håndtering af informations- og cybersikkerheden. ITIL dækker området bedre end agile metoder ved at referere til andre rammesystemer og standarder inden for området, men historisk set har man primært set på sikkerheden i forbindelse med brugernes adgang til information snarere end at skabe (eller anskaffe) et robust teknisk design. Agile rammesystemer beskæftiger sig ikke særlig meget med informations- og cybersikkerheden, men forventer i stedet, at f.eks. DevOps tager sig af dette. Selv traditionelle metoder som vandfaldsmodellen har deres begrænsninger og udfordringer, så løsningen er ikke nødvendigvis at vende tilbage til traditionelle udviklingsprincipper.

Uanset metoderne i vores organisationer er vi nødt til at sørge for, at sikkerhedsinteresserne også varetages under korte iterationer, hvor kun det højest prioriterede bliver udviklet. Sikkerhed skal have høj prioritet for at minimere fremtidige risici.

Hurtige transformationsprocesser bliver problematiske på grund af risikoen for, at man opbygger et IT-landskab, der er så komplekst, at det efterhånden bliver meget dyrt at finde ud af, hvilke risici organisationen udsætter sig selv for. Ofte er der stort fokus på funktionaliteten og mindre opmærksomhed på den proaktive sikkerhed, herunder dokumenterede informationsstrømme, risikovurderinger, uddannelse og hændelseshåndtering i forbindelse med informationssikkerheden.

Nylige og meget omtalte "fejlkonfigurationer" af standardtjenester, som har ført til, at der åbnes for følsom information, som kræver beskyttelse, viser med al tydelighed effekterne fra et opskruet tempo og mangler i metoderne. Problemerne stammer kun sjældent fra fejl i produktet eller løsningen. Som regel skyldes de mangelfuld håndtering. Der bliver ikke brugt tid til eftertanke, og man glemmer de mest fundamentale elementer som f.eks. konfiguration. Dette er endnu et af de mange elementer, der øger friktionen mellem hurtig udvikling og vedligeholdelse af stabile systemer, som har plaget IT-organisationerne i årevis.

Som sikkerheds- eller IT-ansvarlig risikerer man nogle gange at blive opfattet som bagstræberisk, som en forhindring for produktivitet og fleksibilitet. Hele virksomheden er nødt til at arbejde proaktivt for at øge forståelsen for den nødvendige risikominimering, selvom den skulle påvirke produktionen negativt. IT-funktionen skal definere, forankre og sikre sikkerhedsniveauerne, både med hensyn til infrastruktur og applikationer.

Som allerede beskrevet kræves der en indsats, der styrker passende og nødvendige adfærdsændringer hos alle IT-brugere i virksomheden. Et veldefineret og proaktivt arbejde for øget bevidsthed, bedre krisestyring og verificeret overholdelse giver virksomheden konkurrencefordele, fordi arbejdet både beskytter vigtige aktiver og virksomhedens omdømme. Fra et driftsmæssigt perspektiv betyder dette, at man skal vurdere allerede implementerede løsninger, sikre at det eksisterende vidensniveau opfylder kravene og forventningerne, og at fremtidige investeringer i innovation og transformation ikke går på kompromis med sikkerheden.

I denne sammenhæng er det afgørende, at ledelsesgrupperne og beslutningstagerne deltager aktivt i arbejdet, og at dette engagement gøres synligt. Radars data viser, at flere beslutningsroller end tidligere deltager ved aktivt at påvirke, drive og træffe beslutninger om spørgsmål i forbindelse med cybersikkerhed. Det er et tegn på, at udviklingen går i den rigtige retning. Samtidig er der udfordringer med at kommunikere internt, hvem der faktisk har ansvaret for spørgsmål om cybersikkerhed. Intet mindre end 27 procent af medarbejdere, som ikke er ledere, oplyser, at de ikke ved dette.

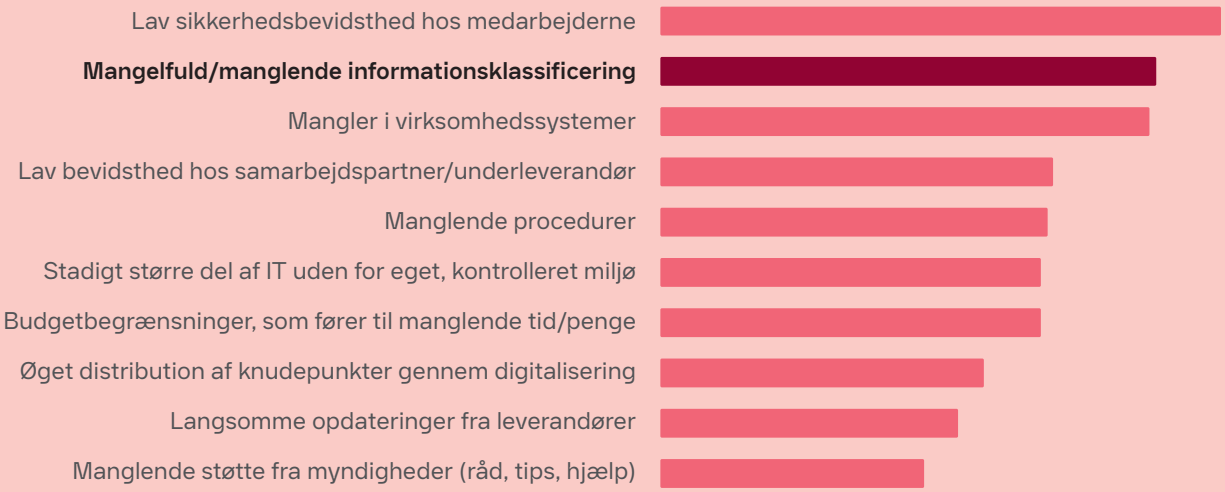
Radars anbefaling er at fokusere mere på virksomhedens viden om og kendskab til risici og udfordringer gennem indsatser på individuelt niveau.

2.1. Debatten om cloud-tjenester og sikkerhed

Sikkerhed fremstilles ofte som en af de større barrierer for væksten af cloud-tjenester og også generelt med hensyn til ekstern IT-drift. Imidlertid viser Radars data, at det ikke er sikkerheden, der er problemet, men derimod IT-organisationens modenhedsniveau.

Hvis man skal sige det lidt groft, handler det i høj grad om, at man ikke er nået så langt i sit grundlæggende arbejde, at man ved hvilke oplysninger, der er vigtige eller følsomme, og dermed hvordan de skal håndteres.

10 største oplevede barrierer for sikkerhed i 2020



En af cloud-tjenesternes vigtigste styrker er muligheden for at optimere de funktioner, der kræver skalerbarhed og fleksibilitet. For de fleste virksomheder handler det ikke om cloud-tjeneste eller ikke cloud-tjeneste, men om at finde den rigtige balance mellem offentlige cloud-tjenester og eksisterende intern produktion. Det handler om at kunne afbalancere IT-leverancerne i takt med ændringerne i virksomhedens krav.

På trods af cloud-tjenesternes mange positive egenskaber opleves sikkerhed desværre som en af de fem største barrierer, og for næsten 11 procent af nordiske virksomheder som den afgørende barriere, der forhindrer brug af cloud-tjenester. Radars data viser dog, at det snarere er et spørgsmål om modenhed end om sikkerhed. Modne virksomheder vælger i stigende grad produktions- og leveringsmetoder baseret på strategiske principper. Sikkerheden bliver en udfordring for disse virksomheder i forbindelse med tilføjelse af cloud-tjenester, og det skyldes ikke cloud-tjenesterne i sig selv. Forklaringen er, at de tjenester, der er egnede til levering i eller gennem skyen, allerede er i brug i disse virksomheder. Derfor er det måske teoretisk korrekt at beskrive sikkerheden som den største barriere, men uden nogen underliggende årsag bliver dette meget misvisende.

Hvis man som virksomhed ikke allerede har gennemført sit interne arbejde med informationsklassificering, så ved man heller ikke, hvordan informationen kan og skal håndteres i tjenesterne. Når det i dag er denne form for tjenester, man vender sig mod, så er det et naturligt resultat af hele industrialiseringen af IT-landskabet, og sikkerhedsproblematikkerne havde været de samme uanset outsourcing, cloud-tjeneste eller anden eksternalisering af IT.

Sikkerheden er ikke pr. definition lavere i en cloud-tjeneste. Den påvirkes i høj grad negativt af organisationens manglende regler og overholdelse, hvor hele 41 procent af alle svenske virksomheder faktisk mangler en strategi, der tager hensyn til cloud-tjenester.

[3] Radar Security Maturity Index
[4] Ifølge definition af Radars Maturity Index.

3. Situationen i den offentlige sektor

I de senere år har arbejdet med sikkerhedsspørgsmål i den offentlige sektor gennemgået en positiv udvikling. Sikkerhedsperspektivet får større plads i forbindelse med strategiske IT-projekter og implementering af ny teknologi. Samtidig har man øget støtten til samfundet og erhvervslivet, og kommunikationen er blevet tydeligere. Gennem strengere lovgivning, både på nationalt plan og på EU-plan, har forskellige regulerende myndigheder fået flere beføjelser og større ansvar.

Det har nogle gange ført til vanskelige diskussioner om ansvar og ansvarsfordeling, blandt andet omkring korrekt håndtering af data under og efter indkøb, løbende overholdelseskontrol og selve den måde, man anvender cloud-tjenester på.

Der er stigende opmærksomhed på denne problematik i både den offentlige og private sektor, og i dag ser mange større virksomheder på digitaliseringsrisikoen som mere end et branchespecifikt problem. Fra offentlig side er man i Sverige opmærksom på den samlede forsvarsevne og gråzoneproblemet i forbindelse med forskellige nationale sikkerhedsdebatter, f.eks. det fremtidige 5G-netværk, og det nye nationale cybersecuritycenter har bidraget til større konsensus på området.

I Radars netop gennemførte målinger af barrierer for sikkerhedsarbejdet betragtede private aktører støtte fra nationale myndigheder (råd, tip og hjælp) som den mindste forhindring. Mangler hos udbydere af sikkerhedsløsninger og forsinkede applikationsopdateringer blev i denne sammenhæng oplevet som mere problematiske. Mange statslige aktører og institutioner har hermed fået en stærkere profil i denne sammenhæng.

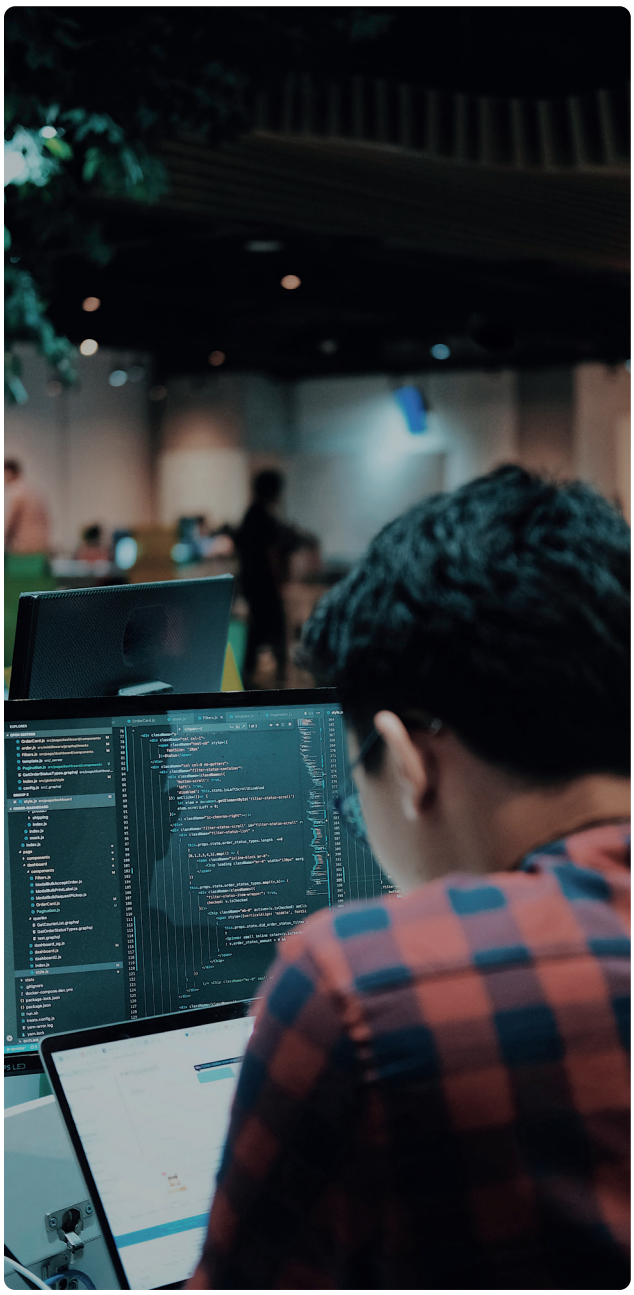
[5] I Radars seneste undersøgelse, der blev gennemført ved årsskiftet 2019/2020, blev respondenterne bedt om at rangordne elleve barrierer. Manglende statslig støtte blev opfattet som den mindste barriere for sikkerhedsarbejdet af private aktører.

3.1. Udfordringer

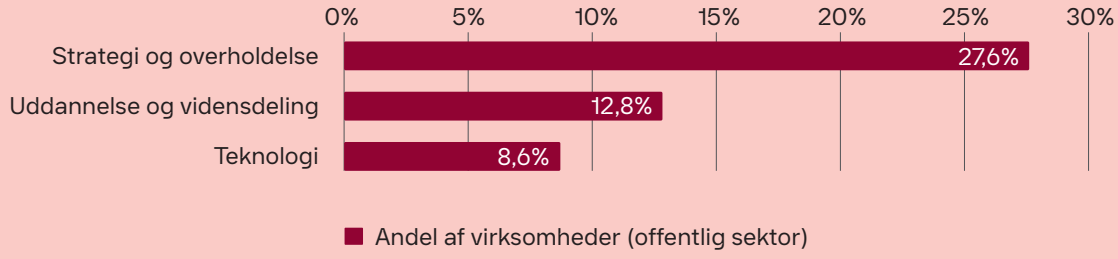
Selvom informations- og cybersikkerhed er kommet højere op på dagsordenen, viser Radars data relativt store forskelle på, hvordan IT-organisationen oplever, at man måler og vurderer sit eget arbejde sammenlignet med, hvordan andre områder i virksomheden vurderer det samme.

Driftsstabilitet, målt i antal problemer/sager og tilgængelighed, er et vigtigt målepunkt for 71 procent af IT-organisationerne, mens kun 19 procent af den resterende del af virksomheden bruger den til at måle sin IT. I stedet bruger man i højere grad budgetopfyldelse samt kunde- og brugertilfredshed ved vurderingen af sin egen IT-organisation. Forskellene kan delvis forklares med, at drøftelser om budgetter og projektomkostninger foretages regelmæssigt og bredt, og det samme gælder brugertilfredshed og kundetilfredshed. Driftsforstyrrelser og afbrydelser bliver først vigtige variabler for virksomheden uden for IT-organisationen, når forretningen bliver ramt, eller sandsynligheden for dette øges, for eksempel i forbindelse med ændringsprocesser.

Ifølge IT-organisationerne i den offentlige sektor findes de største sikkerhedsudfordringer på det strategiske og driftsmæssige område. Det omfatter bl.a. etableringen af en struktur med procedurer for overholdelse samt uddannelse og øget viden med henblik på en styrkelse af informationssikkerheden. Radars data viser, at flere forskellige forebyggende foranstaltninger enten er ved at blive indført eller allerede foretages løbende. Cirka 44 procent i den offentlige sektor oplyser, at øvelser inden for krise- og hændelsesstyring er i gang med at blive indført, og næsten en lige så stor andel arbejder kontinuerligt med overholdelsesspørgsmål. Det er en stor forskel i forhold til tidligere og kan sammenlignes med den aktuelle oprustning af vores samlede forsvarsevne helt ned til de offentlige organer, der er kritiske for samfundet.



Sikkerhedsudfordringer for IT-organisationer i den offentlige sektor 2020



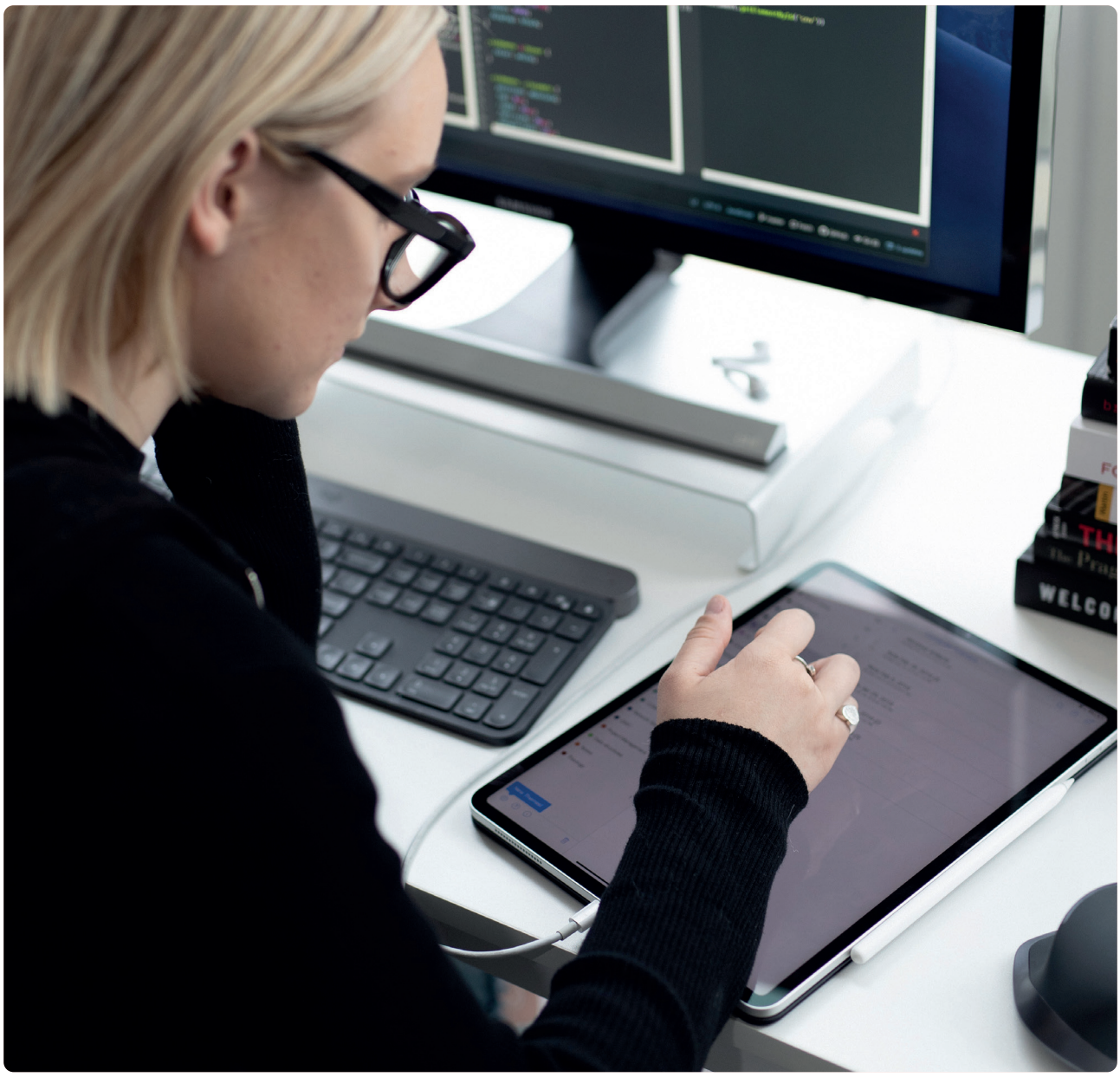
Satsninger inden for det strategiske og operationelle sikkerhedsarbejde ses ikke kun i den offentlige sektor. De kan også aflæses i den generelle markedsudvikling for cybersikkerhedsrelaterede produkter og tjenester. Særligt bemærkelsesværdig er tendensen hos de virksomheder, som Radar anser for at have en høj sikkerhedsforståelse. Relativt set er investeringen i tekniske sikkerhedsløsninger hos disse virksomheder faldende, mens man investerer mere i driftsmæssige sikkerhedsløsninger.

De øgede ressourcekrav til strategi og overholdelse er til en vis grad en reaktion på den øgede kompleksitet. I nogle tilfælde har denne kompleksitet givet anledning til stor usikkerhed, f.eks. anvendelsen af visse cloud-tjenester, i lyset af den amerikanske Cloud Act. Usikkerheden skyldes til en vis grad en ubalanceret FUD-retorik (Fear, Uncertainty, Doubt) i kombination med forholdsvis nye hændelser i den offentlige sektor.

Tydeligere retningslinjer styrker forudsætningerne for en vellykket digitalisering og mindsker samtidig risikoen for problemer. Derfor er det positivt, at man fra statslig side har valgt at undersøge spørgsmålet. Uanset om det gælder implementering af AI-løsninger i mindre skala eller informationslagring i større skala, så efterspørges der retningslinjer og afklaring omkring brugen af cloud-tjenester i den offentlige sektor.

I Radars seneste dataindsamling fra både den offentlige og den private sektor ser man en stor støtte fra IT-beslutningstagere i den offentlige sektor til en løsning, som kan føre til statslige cloud-tjenester. Hele 54 procent er positive, og kun 7 procent er negative over for en statsligt drevet sky. At de resterende 39 procent er neutrale eller negative er ikke overraskende på grund af den udbredte usikkerhed. Selvom en stor del af cyber- og informationssikkerhedsarbejdet i den offentlige sektor har en politisk dimension, ser det ud til, at styring og initiativer driver udviklingen fremad. Oprettelsen af et cybersikkerhedscenter og indførelsen af en cyberværnepligt er tegn på, at cybersikkerheden har fået en fortjent højere placering på dagsordenen.

Vi vil med stor sandsynlighed se hårdt tiltrængte ændringer på centralt plan, hvad angår strategi og retningslinjer. Men indtil da er det vigtigt ikke at blive for passiv og defensiv, da det kan føre til øget risiko og en mindsket generel sikkerhed.

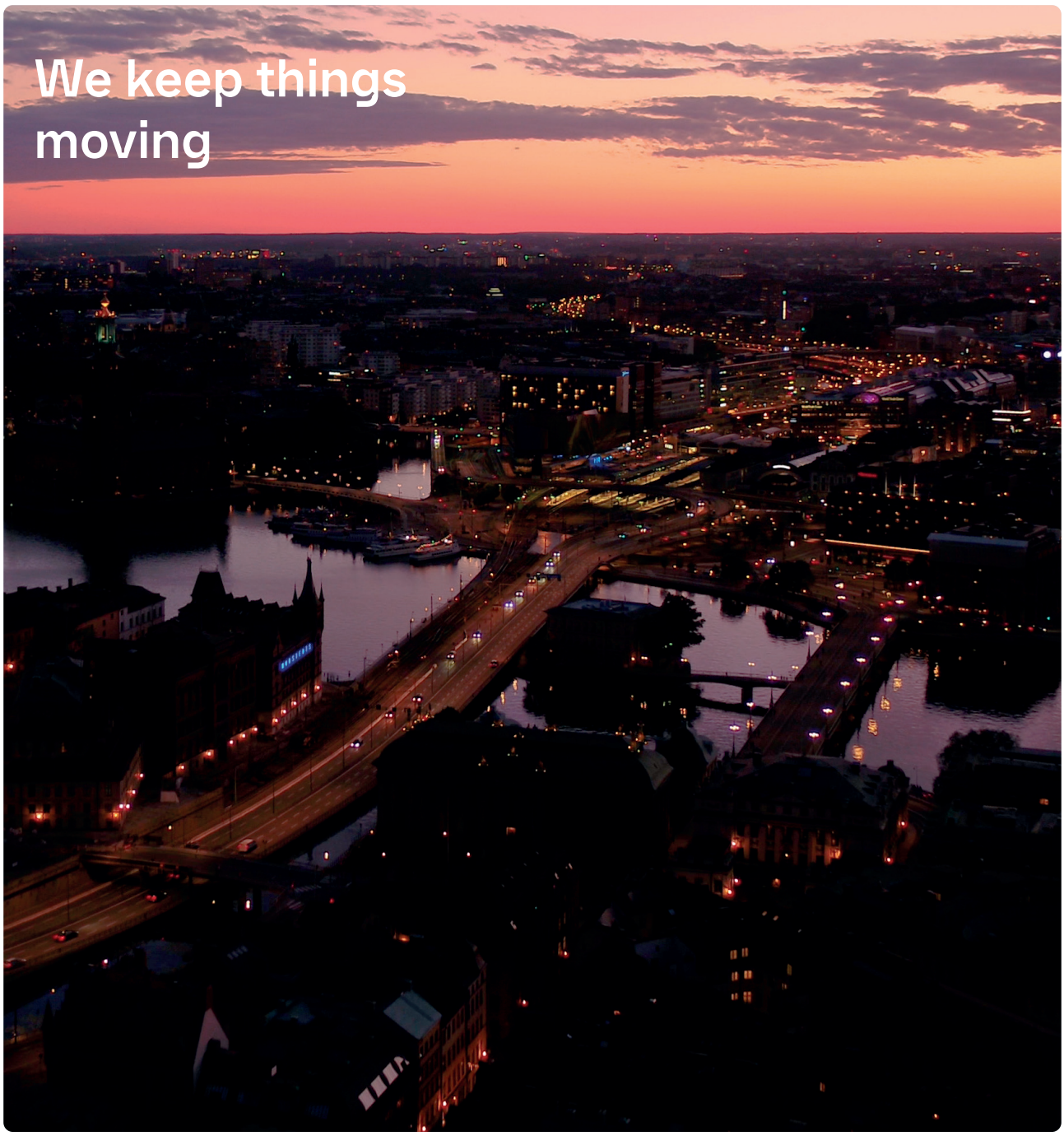


Om rapporten

Rapporten er udarbejdet af Radar på vegne af Dustin. Radar har uafhængigt udført analyser inden for givne områder ved hjælp af objektive metoder. Det betyder, at al dataindsamling og eventuelle interviews er udført af Radar under eget navn inden for rammerne af normal indsamling. Der er ikke indsamlet særlige data udelukkende til denne rapport. Derved sikres neutralitet i det statistiske grundlag. Radar er selv ansvarlig for indholdet og konklusionerne i denne rapport.

Rådgiver
Richard Werner
richard-werner@radareco.com

Analytiker
Patrik Mernissi Granlind
patrik.granlind@radareco.com



Dustin er en førende onlinebaseret IT-partner i Norden og Nederlandene. Vi sørger for, at vores kunder er på forkant ved at levere den rette IT-løsning på det rette tidspunkt og til den rette pris.

Vi tilbyder cirka 255.000 produkter med tilhørende tjenester til virksomheder, den offentlige sektor og privatpersoner.

Omsætningen i virksomhedsåret 2018/19 endte på ca. 12,5 mia. SEK, og ca. 90 procent af indtægterne kom fra erhvervsmarkedet.

Dustin Group har mere end 1800 medarbejdere og har været børsnoteret på Nasdaq Stockholm siden 2015 med hovedkontor i Nacka Strand lige uden for det centrale Stockholm.

dustin.dk

Dustin