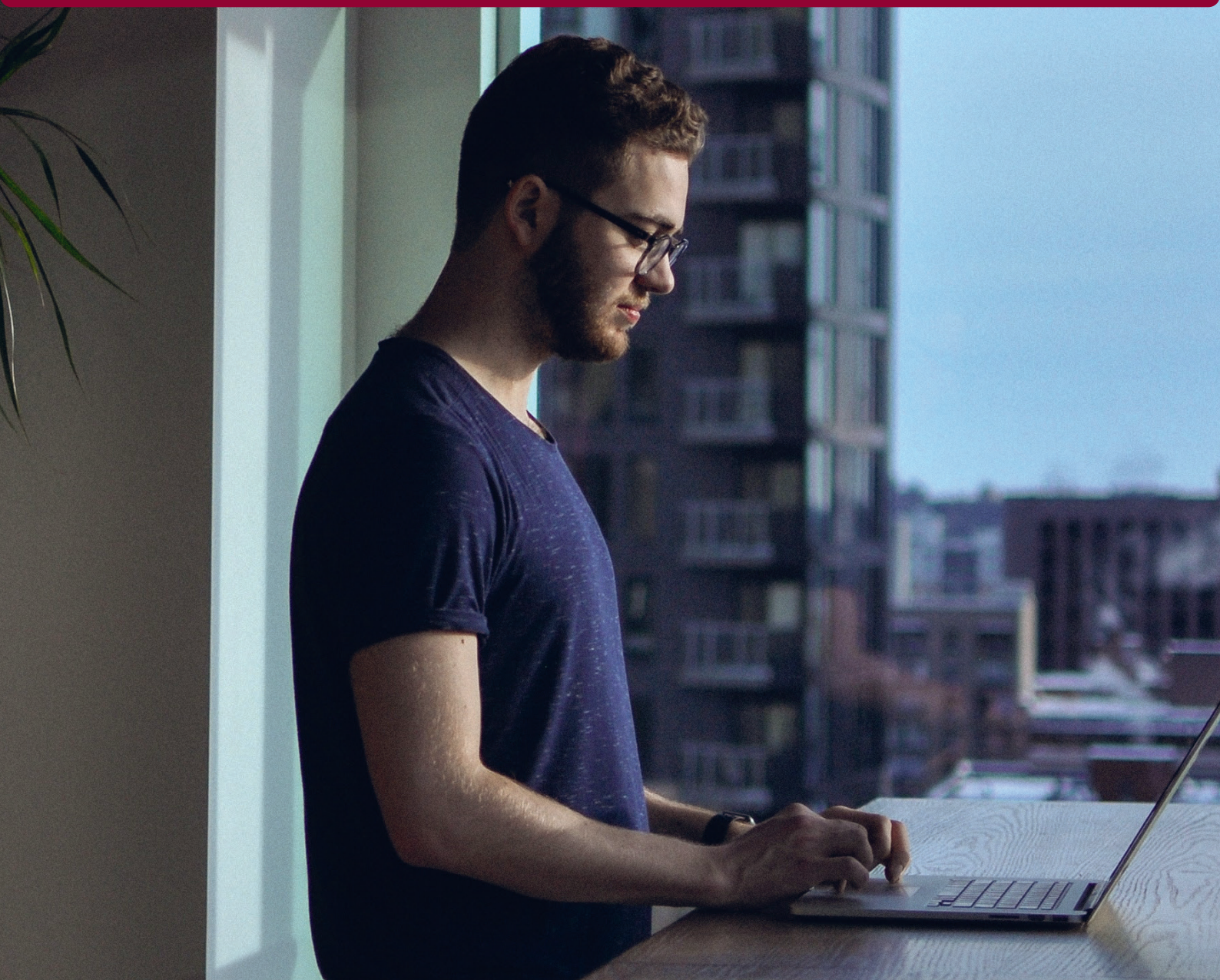
Dustin

Sikkerhetsutfordringer i digitaliseringstider



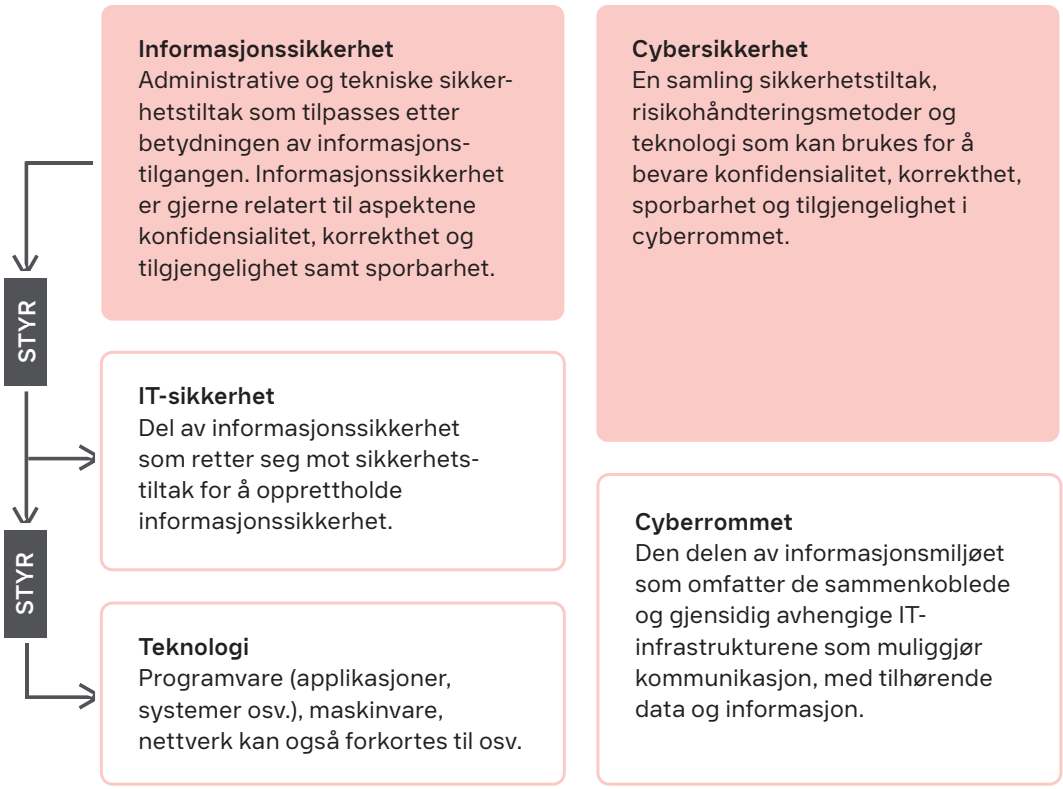
Innhold

1. Hva betyr sikkerhet i dag?

I takt med at digitaliseringen får stadig bedre fotfeste i alle deler av samfunnet blir sikkerhet noe det forventes at alle ikke bare forstår, men også bidrar til. Men til tross for at cyber- og informasjonssikkerhet blir stadig mer aktuelt, kan det av og til være vanskelig å avgrense og holde begrepene fra hverandre. Vi er vant til å vokte over vår fysiske sikkerhet med dører og låser, men med digitaliseringen har vi revet vegger og åpnet ganger til andre virksomheter gjennom iblant hastige prosesser. Det har vi også gjort bevisst for å møte økt konkurranse og høyere forventninger.

Med Internetts globalisering har også de geografiske vernene som finnes i den fysiske verden, blitt revet samtidig som det er etterspørsel etter nye sikkerhetsmekanismer. Økt digital kompleksitet må møtes med større tydelighet, særlig når personer stadig lengre inn i virksomhetene nå utsettes for risikoene som tidligere bare rammet IT-organisasjonen. Nå omfattes så å si alle, også de som ikke jobber regelmessig med sikkerhet. Også for den innvidde er det noen ganger vanskelig å skille mellom fysisk sikkerhet, informasjonssikkerhet, IT-sikkerhet og cybersikkerhet.

Nøyaktige definisjoner er ikke avgjørende, men for å kunne følge med i daglige rapporteringer kan man som leser gjerne benytte den forenklede begrepsmodellen som Radar tar utgangspunkt i i sine analyser og rapporter.



IT-sikkerhet har hovedsakelig som mål å beskytte data som allerede er eller kan bli foredlet til informasjon. Datasikkerhet er den delen av IT-sikkerheten som handler om teknisk beskyttelse av selve systemene og dataene. Det omfatter blant annet metoder for kryptering, autentisering og beskyttelse mot overbelastningsangrep. Informasjonssikkerhet omfatter så vel IT-sikkerhet som prosesser og rutiner for å opprettholde nødvendig integritet, konfidensialitet og tilgjengelighet av informasjon. En forenklet huskeregel er at informasjonssikkerhet beskriver det som skal gjøres, mens IT-sikkerhetsarbeidet mer beskriver hvordan det skal gjøres ved hjelp av teknologi og verktøy.

Informasjonssikkerhet omfatter ikke bare IT-sikkerhet, men er også knyttet til cybersikkerhet, som forener sikkerheten med hensyn til oppkoblet (hovedsakelig mot Internett) informasjonstilgang, som er det som i første rekke rammer oss i dagens oppkoblede verden.

2. Sikkerhet i en digitaliseringsbølge

Fortsatt digitalisering og optimalisering av digitale prosesser i svenske virksomheter er nødvendig. Ifølge Radars data er økt digitaliserings- (64 %) og automatiseringsgrad (46 %)[1], samt innføring av nye applikasjoner (44 %)[1] nettopp det som prioriteres høyest innen IT.

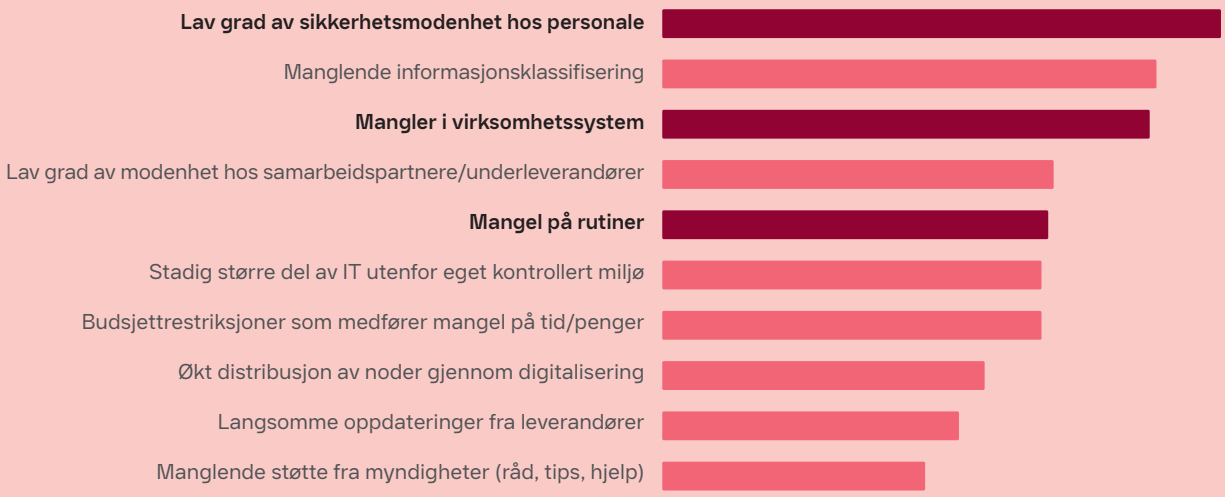
Samtidig genererer dette stadig større datavolumer, blant annet som følge av økt bruk av skytjenester og IoT, noe som medfører mer intensive (kvantitet) og mer anvendelige (kvalitet) datastrømmer. Gjennom komplekse kjeder skapes det verdi fra informasjon som tidligere har vært uinteressant og ikke-målbar. Utviklingen har gått fremover, og stadig flere etterstreber mer fleksible forretnings- og virksomhetsmodeller der datastrømmene utnyttes i større grad.

Lengre kjeder er imidlertid mer komplekse og dermed vanskelige å holde oversikt over fra et sikkerhetsperspektiv. Økt distribusjon av noder i forbindelse med digitalisering oppleves som et hinder i sikkerhetsarbeidet for de fleste modne virksomheter.

I mindre modne virksomheter er denne bevisstheten fremdeles liten. Utfordringen er å forstå hvordan informasjonen lever gjennom hele den lange kjeden. Det vil si å forstå når informasjonen ligger i ro, er i bevegelse eller i bruk samt hvem som har tilgang til den. Brudd i kjeden kan innebære tapt forretningsinformasjon, effektivitetstap, kvalitetsbrist og/eller redusert tillit, som igjen kan medføre økte kostnader, nedsatt konkurranseevne eller i verste fall risiko for samfunnet.

Et realistisk utgangspunkt er at ikke noe sikkerhetsarbeid er perfekt. Radars vanligste anbefaling for hvordan arbeidet med sikkerhet bør drives, er at det må kunne forsvares juridisk, men fremfor alt også operasjonelt. Det må fungere i praksis. Det er en stor utfordring å digitalisere uten å gi avkall på sikkerhet for egen virksomhet, samarbeidspartnere og medborgere. En glemt patch, en uforsiktig åpning av et vedlegg i en e-post eller et inngrep hos valgt IT-leverandør kan i dag få katastrofale følger. I tillegg til intern sikkerhetsmodenhet hos eget personale er manglende rutiner og brudd på sikkerheten i virksomhetssystemer i dag blant de største hindrene.

De 10 største opplevde hindrene for sikkerhet i 2020



[1] Andel av svenske virksomheter som ifølge rapporten IT-Radar 2020 prioriterer respektive område.
[2] Kartlegging av svensk cybersikkerhet 2020, Radar

For å få utbytte av tiltak som gir økt sikkerhet må disse være veloverveide og begrunnede, noe som er en stor utfordring i seg selv. En evaluering av nåværende situasjon med fokus på behov og forutsetninger gir gjerne et bedre utgangspunkt for fremtidige investeringer og endringsprosesser, blant annet arbeidet med overholdelse og oppfyllelse av nye krav. Arbeid som har til formål å styrke virksomhetens prestasjonsevne gjennom kompetansehevende tiltak på individnivå, er viktig i denne sammenheng. Særlig ettersom lav grad av sikkerhetsmodenhet blant eget personale betraktes som et stort hinder for å holde sikkerheten på et tilfredsstillende nivå.

Et høyt endringstempo innebærer stigende forventninger og krav om rask tilgang til nye tjenester som gir økt effektivitet. Cyber- og informasjonssikkerhetsarbeidet settes dermed ikke bare opp mot ressurser i form av penger, tid og kompetanse, men ofte også mot faktorene bekvemmelighet og frihet. Når stadig kortere virksomhetssykluser premieres, risikerer dynamikken å bli endret fra en forsiktig satsing til en med høyere risiko, noe som gir større fare for at sikkerhetsarbeidet havner på etterskudd allerede i en tidlig fase.

Fra et sikkerhetsperspektiv er det et problem at stadig kortere virksomhetssykluser medfører premiering av visse styringsmodeller og arbeidsmetoder som har til formål å lette tollvirksomhetens digitalisering.

De vanligste ITIL-rammeverkene og agile metodene gir ikke IT-organisasjonen og virksomheten for øvrig tilstrekkelig støtte i håndteringen av informasjons- og cybersikkerhet. ITIL dekker inn området mer enn agile metoder ved å henvise til andre rammeverk og standarder på området, men historisk sett har sikkerhet hovedsakelig tatt utgangspunkt i brukerens tilgang til informasjon fremfor å skape (eller anskaffe) en robust teknisk design. Agile rammeverk tar ikke opp informasjons- og cybersikkerhet i større utstrekning, men setter sin lit til blant annet DevOps. Også tradisjonelle metoder som fossefallmetoden har sine begrensninger og problemer, så løsningen er ikke nødvendigvis å gå tilbake til tradisjonelle utviklingsprinsipper.

Uansett metodikk i egen organisasjon må man sørge for at sikkerhetsinteressen overvåkes også i korte iterasjoner der bare det som er høyest prioritert, blir utviklet. Sikkerhet må gis høy prioritet for å minimere fremtidig risiko.

Hastige transformasjonsprosesser blir problematisk, da det er fare for at man bygger seg inn i et IT-landskap som er så komplisert at det senere blir svært kostbart å finne ut hvilke risikoer organisasjonen utsetter seg for. Ofte legges det stor vekt på funksjon, mens proaktiv sikkerhet som for eksempel dokumenterte informasjonsstrømmer, risikovurderinger, opplæring og håndtering av informasjonssikkerhetshendelser blir viet mindre oppmerksomhet.

Den siste tidens fokus på "feilkonfigureringer" av standardtjenester som har medført at følsom og beskyttelsesverdig informasjon har ligget åpen, viser med all tydelighet virkningene av et oppskrudd tempo og mangelfull metodikk. Det er sjelden feil på produktet eller løsningen - som oftest er det håndteringen som er mangelfull. Det gis ikke tid til ettertanke, og man glemmer de mest grunnleggende delene som for eksempel konfigurering. Dette er ytterligere en av de mange tingene som øker friksjonen mellom rask utvikling og bevaring av stabile systemer, som i mange år har vært en hodepine for IT-organisasjoner.

Som sikkerhets- eller IT-ansvarlig risikerer man iblant å bli oppfattet som bakstreversk og en bremsekloss for produktivitet og fleksibilitet. Hele virksomheten er nødt til å jobbe proaktivt for å øke forståelsen for nødvendig risikominimering, selv om det medfører produksjonstap. IT er nødt til å definere, forankre og trygge sikkerhetsnivåer, både når det gjelder infrastruktur og applikasjoner. Som allerede påpekt er det viktig med tiltak som styrker hensiktsmessige og nødvendige atferdsendringer hos alle IT-brukere. Et godt definert proaktivt arbeid for økt bevissthet, økt krisehåndtering og verifisert etterlevelse gir virksomheten et konkurransefortrinn gjennom å beskytte både nøkkelressurser og virksomhetens anseelse. Fra et virksomhetsperspektiv innebærer dette at man må evaluere allerede implementerte løsninger, sørge for at eksisterende kunnskapsnivå tilsvarer krav og forventninger samt at man i forbindelse med fremtidige investeringer i innovasjon og transformasjon ikke går på kompromiss med sikkerheten.

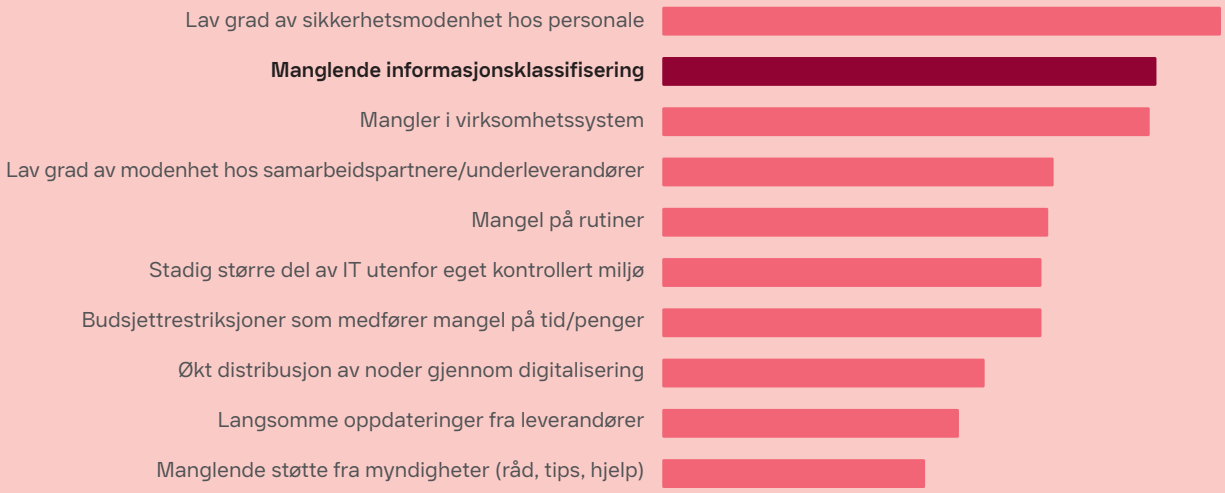
Aktiv deltakelse og synliggjøring av engasjement fra ledergrupper og beslutningstakere er sentralt i denne sammenheng. Radars data viser at flere beslutningstakende roller enn tidligere bidrar aktivt med å påvirke og ta beslutninger i spørsmål vedrørende cybersikkerhet, noe som tyder på at utviklingen går i riktig retning. Samtidig er det mangel på intern kommunikasjon om hvor ansvaret for cybersikkerhet ligger: Hele 27 prosent av medarbeidere som ikke har en lederstilling, oppgir at de ikke vet dette.

Radars anbefaling er å fokusere mer på virksomhetens kunnskap om og kjennskap til risikoer og utfordringer gjennom tiltak på individnivå.

2.1. Debatten om skytjenester og sikkerhet

Sikkerhet fremheves ofte som et av de største hindrene for veksten i skytjenester og ofte også generelt når det gjelder ekstern IT-drift. Radars data viser imidlertid at det ikke er sikkerheten som er problemet, men snarere IT-organisasjonens modenhet. Skal man være krass, handler det mye om at man ikke har kommet så langt i det grunnleggende arbeidet at man vet hvilken informasjon som er viktig eller følsom og dermed hvordan den kan håndteres.

De 10 største opplevde hindrene for sikkerhet i 2020



En av de grunnleggende styrkene ved skytjenester er muligheten til å optimalisere for funksjonene som krever skalerbarhet og fleksibilitet. For de fleste virksomheter er det ikke et spørsmål om skytjeneste eller ikke skytjeneste, men om å finne den riktige balansen mellom offentlige skytjenester og eksisterende intern produksjon. Alt for å kunne balansere IT-leveransen i takt med endringer i virksomhetens krav.

Til tross for mange positive egenskaper ved skytjenester oppleves dessverre sikkerhet som et av de fem største hindrene, og for nærmere 11 prosent av alle nordiske virksomheter er sikkerhet barrieren som gjør at de ikke kan benytte skytjenster. Radars data viser derimot at det heller er et spørsmål om modenhet enn sikkerhet. Modne virksomheter velger i stadig større grad produksjons- og leveranseform på grunnlag av strategiske prinsipper. Sikkerhet blir et problem for disse virksomhetene ved ytterligere skytjenester og ikke på grunn av skytjenester i seg selv. Forklaringen ligger i at tjenestene som egner seg for levering i eller gjennom skyen, allerede er i bruk i disse virksomhetene. Derfor er det å hevde at sikkerhet er den største barrieren muligens riktig i teorien, men svært misvisende uten noen bakenforliggende årsak.

Hvis man som virksomhet ikke allerede har gjort det interne arbeidet med informasjonsklassifisering, vet man heller ikke hvordan informasjonen i tjenestene får og kan håndteres. At det i dagens situasjon er denne typen tjenester man vender seg til er et naturlig resultat av hele IT-landskapets industrialisering, og sikkerhetsproblematikken hadde vært den samme uansett outsourcing, skytjeneste eller annen eksternalisering av IT.

Sikkerheten er ikke per definisjon dårligere i en skytjeneste, men rammes i større grad av organisasjonens egen mangel på regelverk og etterlevelse når hele 41 prosent av alle svenske virksomheter faktisk mangler en strategi som tar hensyn til skytjenester.

[3] Radar Security Maturity Index
[4] Ifølge definisjon av Radars Maturity Index.

3. Situasjonen i offentlig sektor

Arbeidet med sikkerhetsspørsmål i offentlig sektor har i de senere årene gjennomgått en positiv utvikling. Sikkerhetsperspektivet har fått større plass i forbindelse med strategiske IT-prosjekter og ved implementering av ny teknologi, samtidig som kommunikasjon og støtte til samfunn og næringsliv både er blitt tydeliggjort og mer omfattende. Gjennom skjerpet lovgivning både på nasjonalt og EU-plan har ulike tilsynsmyndigheter fått mer myndighet og større ansvar.

Iblant har dette imidlertid gitt opphav til harde debatter om ansvar og ansvarsfordeling, blant annet med hensyn til korrekt håndtering av data under og etter anskaffelser, kontroller av etterlevelse over tid og i hvilke former skytjenester kan benyttes.

I både offentlig og privat sektor er blikkene løftet, og mange større virksomheter ser i dag bortenfor bransjespesifikke oppfatninger rundt risikoer i forbindelse med digitalisering. Fra offentlig hold har opprustingen av svensk totalforsvarsevne og den gråsoneproblematikken som er blitt gjenstand for oppmerksomhet i forbindelse med ulike nasjonale sikkerhetsdebatter, for eksempel fremtidens 5G-nett og det nye nasjonale cybersikkerhetssenteret, bidratt til større enighet.

I Radars nylig gjennomførte målinger av hindre i sikkerhetsarbeidet, betraktet private aktører støtten (råd, tips, hjelp) fra nasjonale myndigheter som det minste hinderet. Mangler hos leverandører av sikkerhetsløsninger og forsinkede oppdateringer av applikasjoner opplevdes som mer problematisk i denne sammenheng. Dette har dermed gitt mange statlige aktører og institusjoner en stadig sterkere profil.

[5] I Radars siste undersøkelse, som fant sted ved årsskiftet 2019/2020, ble respondentene bedt om å rangere elleve hinder. Blant private aktører ble manglende statlig støtte opplevd som det minste hinderet i sikkerhetsarbeidet.

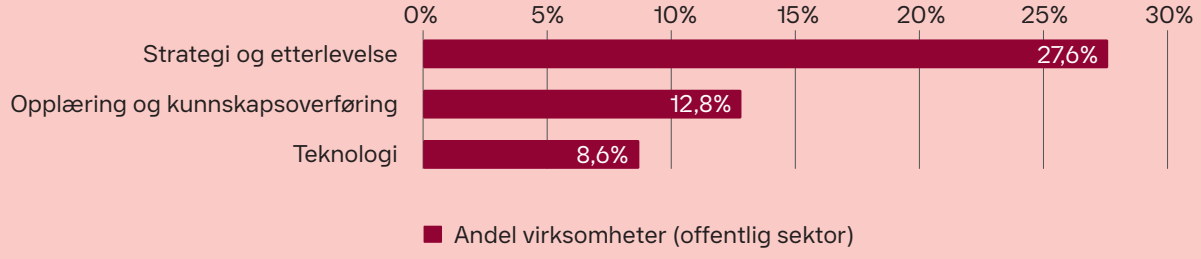
3.1. Utfordringer

Selv om informasjons- og cybersikkerhet står høyt på dagsorden, antyder Radars data relativt store forskjeller i hvordan IT-organisasjonen opplever at man måler og evaluerer eget arbeid sammenlignet med hvordan virksomheten for øvrig evaluerer det samme.

Driftsstabilitet målt i antall problemer/hendelser samt tilgjengelighet er et sentralt målepunkt hos 71 prosent av IT-organisasjonene, mens bare 19 prosent av virksomheten for øvrig bruker dette for å måle sin IT. I stedet er kostnader uttrykt som budsjettoppfyllelse samt kunde- og brukertilfredshet vanligere når virksomheter i offentlig sektor evaluerer sin IT-organisasjon. Forskjellene kan delvis forklares med at diskusjoner om budsjetter og prosjektkostnader skjer regelmessig og bredt, noe som også gjelder for bruker- og kundetilfredshet. Driftsforstyrrelser og avbrudd blir først viktige variabler for virksomheten utenfor IT-organisasjonen når virksomheten blir rammet eller sannsynligheten for det øker, for eksempel i forbindelse med endringsprosesser.

Ifølge IT-organisasjoner i offentlig sektor ligger de største sikkerhetsutfordringene innen det strategiske og operative området. Dette omfatter blant annet etablering av en struktur med rutiner for etterlevelse samt opplæring og kompetanseheving for styrket informasjonssikkerhet. Radars data viser at de fleste forebyggende tiltak er under innføring eller allerede på plass. Rundt 44 prosent i offentlig sektor oppgir at øvelser i krise- og ulykkeshåndtering er under innføring, og en nesten like stor andel jobber kontinuerlig med etterlevelsesspørsmål. Det er en stor forskjell i forhold til tidligere og kan sammenlignes med den aktuelle opprustingen av vår totalforsvarsevne ned til samfunnskritiske instanser.

Sikkerhetsutfordringer for IT-organisasjoner i offentlig sektor i 2020



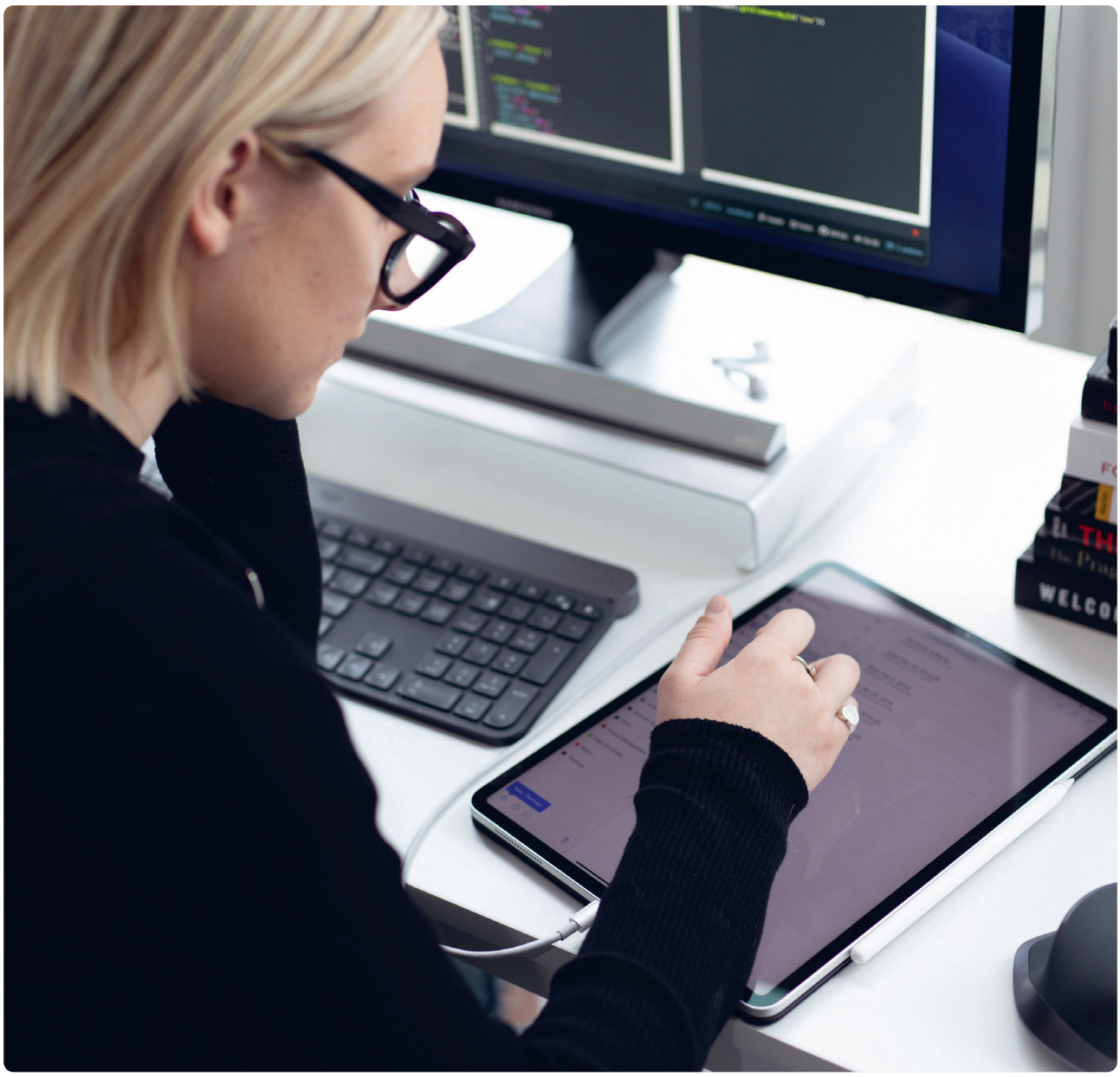
Satsinger på det strategiske og operative sikkerhetsarbeidet er ikke unikt for offentlig sektor, men kan også leses ut av den generelle markedsutviklingen for produkter og tjenester knyttet til cybersikkerhet. Særlig merkbar er trenden hos virksomhetene som Radar vurderer som sikkerhetsmodne. Disse virksomhetene investerer en mindre andel i tekniske sikkerhetsløsninger og stadig mer i operative sikkerhetsløsninger.

At strategi og etterlevelse har blitt mer ressurskrevende er delvis en reaksjon på økt kompleksitet. I noen tilfeller har denne kompleksiteten gitt opphav til stor usikkerhet. Et eksempel på det er bruken av visse skytjenester sett i lys av den amerikanske Cloud Act. Usikkerheten skyldes til en viss grad en ubalansert FUD-retorikk (Fear, Uncertainty, Doubt) kombinert med relativt ferske hendelser i offentlig sektor.

Det er positivt at man har valgt å granske spørsmålet fra statlig hold, siden klarere retningslinjer gir bedre forutsetninger for en vellykket digitalisering samtidig som det foreligger mindre risiko for problemer. Enten det gjelder implementering av AI i mindre skala eller lagring av informasjon i større skala, er retningslinjer og tydelighet vedrørende bruken av skytjenester etterspurt.

Radars siste datainnsamling, innen både offentlig og privat sektor, viste massiv støtte blant IT-beslutningstakere i offentlig sektor for en løsning som vil innebære statlige skytjenester. Hele 54 prosent er positivt innstilt, mens kun 7 prosent er negative til en statlig sky. Det at de øvrige 39 prosent er nøytrale er heller ikke overraskende, ettersom omfattende usikkerhet til en stor del ligger til grunn for granskingen. Selv om mye av arbeidet med cyber- og informasjonssikkerhet i offentlig sektor har en politisk dimensjon, virker det som om styringen og initiativene driver utviklingen fremover. Opprettelsen av et cybersikkerhetssenter og innføringen av en cyberverneplikt tyder på at cybersikkerhet har fått en riktigere plassering høyere på dagsorden.

I fremtiden vil vi høyst sannsynlig se nødvendige endringer på sentralt nivå når det gjelder strategi og retningslinjer. Men frem til da er det viktig å ikke bli for passiv og defensiv slik at effekten blir den motsatte, med økt risiko og lavere generell sikkerhet.

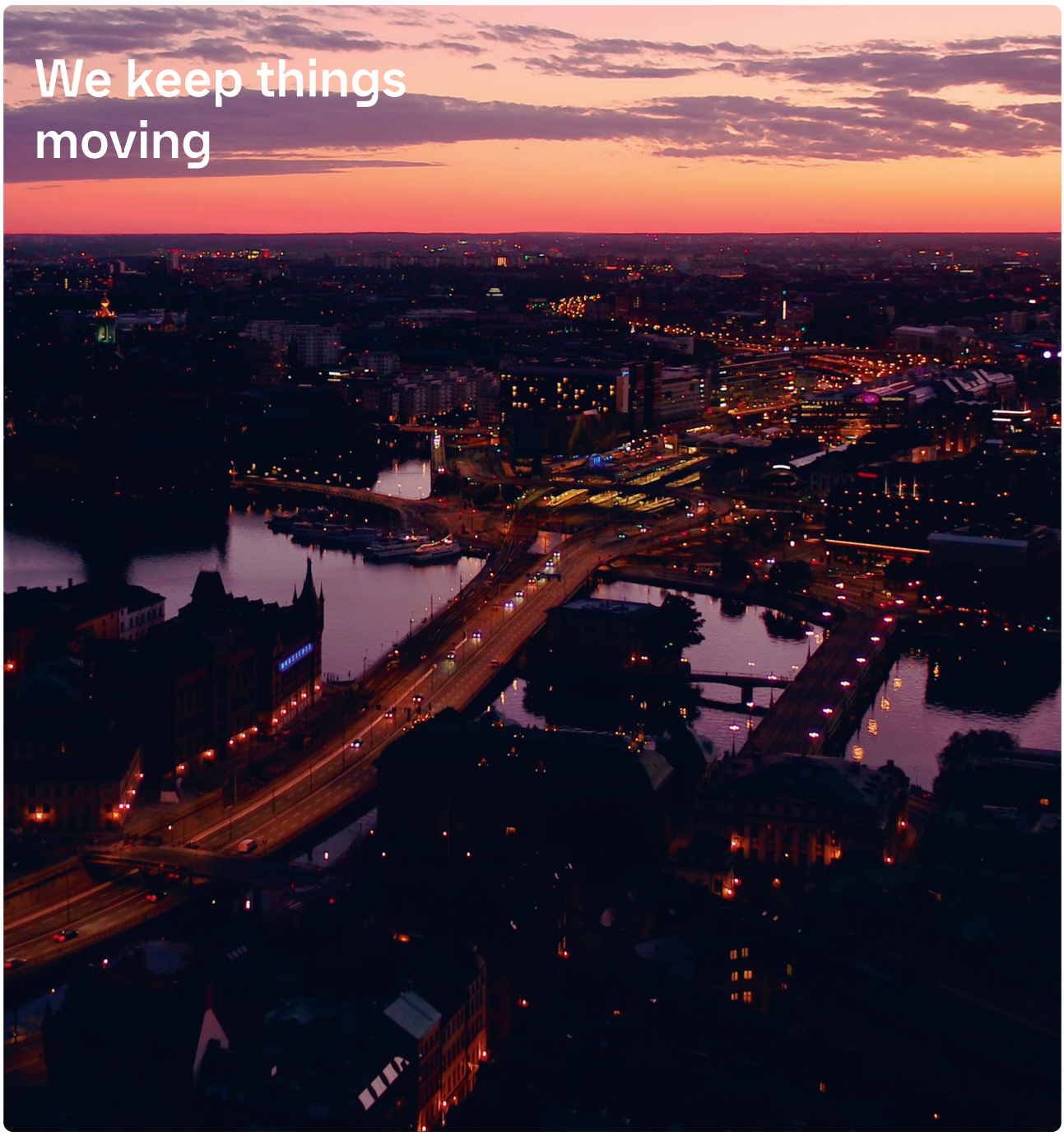


Om rapporten

Rapporten er utarbeidet av Radar på oppdrag av Dustin. Radar har foretatt en uavhengig analyse innen bestemte områder ved hjelp av objektive metoder. Det betyr at all datainnsamling og eventuelle intervjuer er gjennomført av Radar under eget navn innenfor rammene av normal innsamling. Det er ikke samlet inn spesielle data unikt for denne rapporten, noe som gjør at man unngår partiskhet i det statistiske underlaget. Radar er ene og alene ansvarlig for innhold og konklusjoner i denne rapporten.

Rådgiver
Richard Werner
richard-werner@radareco.com

Analytiker
Patrik Mernissi Granlind
patrik.granlind@radareco.com



Dustin er en ledende nettbasert IT-partner med virksomhet i Norden og i Nederland. Vi hjelper kundene våre med være i forkant ved å gi dem rett IT-løsning, til rett tid og rett pris.

Vi tilbyr ca. 255 000 produkter og tjenester for bedrifter, offentlig sektor og privatpersoner. Omsetningen for virksomhetsåret 2018/19 steg til ca. 12,5 millioner SEK, og rundt 90 prosent av inntektene kom fra bedriftsmarkedet.

Dustin Group har mer enn 1800 medarbeidere og har siden 2015 vært børsnotert på Nasdaq Stockholm med hovedkontor i Nacka Strand, like utenfor Stockholm sentrum.

dustin.no

Dustin