NORSK SOSIOLOGISK TIDSSKRIFT
Norwegian Journal of Sociology
VITENSKAPELIG PUBLIKASJON

UNIVERSITETSFORLAGET

Årgang 3, nr. 3-2019, s. 173–190
ISSN online: 2535-2512
https://doi.org/10.18261/issn.2535-2512-2019-03-02

Leaving the windows open – økt mangel på IKT-sikkerhetskompetanse i Norge

Leaving the windows open – increased lack of ICT security competence in Norway

Michael Spjelkavik Mark
Forskningsleder

NIFU – Nordisk institutt for studier av innovasjon, forskning og utdanning
michael.mark@nifu.no

Cathrine Edelhard Tømte
Forsker I

NIFU – Nordisk institutt for studier av innovasjon, forskning og utdanning
cathrine.tomte@nifu.no

Terje Næss
Fagkonsulent

NIFU – Nordisk institutt for studier av innovasjon, forskning og utdanning
terje.nass@nifu.no

Trude Røsdal
Forsker II

NIFU – Nordisk institutt for studier av innovasjon, forskning og utdanning
trude.rosdal@nifu.no

SAMMENDRAG

IKT-sikkerhet berører enkeltindivider, næringsliv, offentlig sektor, nasjonal infrastruktur og samfunnssikkerhet generelt. IKT-sikkerhet defineres vanligvis som evnen til å forebygge, oppdage og håndtere tre typer hendelser: brudd på konfidensialitet, det vil si at uvedkommende får innsyn i beskyttelsesverdig informasjon, brudd på integritet, det vil si at informasjon og/eller systemer endres, skades eller slettes på uautoriserte eller utilsiktede måter, og brudd på tilgjengelighet, det vil si at informasjon og/eller systemer går tapt eller er utilgjengelige når behovet er der (UNINETT, 2017). De siste årene har vi vært vitne til mange slike hendelser der IKT-sikkerheten har vært utfordret, og det er grunn til å tro at omfanget av slike utfordringer øker. I tillegg ser vi at utfordringer knyttet til IKT-sikkerhet

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Idunn
Nordiske tidsskrifter på nett

ved utbredelse av Internet of Things (IoT) øker, og trolig vil kreve styrking av kompetansen innen IKT-sikkerhet.

Selv om myndighetene har iverksatt tiltak for å styrke kompetanse- og kunnskapsnivået innen IKT-sikkerhet i Norge, er det grunn til å spørre om det gjøres nok: er innsatsen ambisiøs nok, og er mengden ressurser til å styrke kompetanse- og kunnskapsnivået tilstrekkelig? Utdanner vi kandidater med adekvat kompetanse?

Formålet med studien er å frambringe oppdatert kunnskap om tilgangen på IKT-sikkerhetskompetanse, høyere utdanning/spesialistkompetanse, sett i forhold til arbeidslivets framtidige behov. Studien bygger på en kvantitativ framskrivning og kvalitative intervjuer med ulike aktører knyttet til feltet IKT-sikkerhet.

Et hovedfunn er at det i årene framover vil utdannes for få med adekvat kompetanse innen IKT-sikkerhet, og at vi får et økende gap mellom tilgang på og behov for personer med IKT-sikkerhetskompetanse, med en underdekning på 4100 personer med IKT-sikkerhetskompetanse (i 2030). Bekymringen for mangelfull adekvat IKT-sikkerhetskompetanse nå og i framtiden blir også bekreftet gjennom intervjuene.

Nøkkelord

IKT-sikkerhet, kompetansebehov, digitalisering av samfunnet, Tingenes internett

ABSTRACT

Cybersecurity affects society at all levels. It affects individuals, businesses, the public sector, infrastructure and national security. The purpose of this paper is to assess whether Norway now and, in the future, has enough persons with an adequate level of cyber security skills. To illustrate the future increasing demand for cyber security skills, this paper investigates existing research on the IoT and cyber security, showing a much stronger focus on future positive possibilities and a lack of focus on cyber security challenges. By deploying dynamic simulation models developed by Statistics Norway we estimate the future deficit of people with adequate cybersecurity skills to be 4 100 persons in year 2030. Thus, to meet future demand, the supply side must increase by 40 per cent in addition to what current projections suggest. The relatively high deficit of cyber security skills follows the findings from national and international surveys and was further confirmed by in depth interviews with national cyber security experts in Norway.

Keywords

Cybersecurity skills, Internet of Things (IoT), Competence demand, digitalization

INTRODUKSJON

Da Etterretningstjenesten våren 2018 la fram sin årlige trusselvurdering, ble terror i det digitale rom framhevet (Etterretningstjenesten, 2018). Det har de senere årene vært økt oppmerksomhet rundt trusler og risiko knyttet til IKT-sikkerhet, både fra myndigheter

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Idunn
Nordiske tidsskrifter på nett

og media. I tillegg utføres IKT-kriminalitet stadig mer profesjonelt (Broadhurst, Grabosky, Alazab & Chon, 2014). Forskere peker på at mangel på kompetanse og manglende forståelse av hva IKT-sikkerhet innebærer kan være en mulig forklaring på slike uønskede hendelser. (Malmedal & Røislien, 2016; Taylor, Fritsch & Liederbach, 2015).

IKT-sikkerhet defineres vanligvis som evnen til å forebygge, oppdage og håndtere tre typer hendelser: *brudd på konfidensialitet*, det vil si at uvedkommende får innsyn i beskyttelsesverdig informasjon, *brudd på integritet*, det vil si at informasjon og/eller systemer endres, skades eller slettes på uautoriserte eller utilsiktede måter, og *brudd på tilgjengelighet*, det vil si at informasjon og/eller systemer går tapt eller er utilgjengelige når behovet er der (Uninett, 2017). IKT-sikkerhet blir slik et ganske vidt definert begrep, og herunder finnes igjen mange ulike forståelser og definisjoner. Ofte er disse knyttet til teknologiutviklingen i seg selv, som for eksempel kunstig intelligens og maskinlæring (Brundage et al., 2018). Kunstig intelligens og maskinlæring kan i et sikkerhetsperspektiv bety at tilgang på informasjon blokkeres eller ødelegges, at analyser av store mengder data om enheter eller enkeltpersoner samles inn og systematiseres for videre manipulering, eller at teknologien lager kunstige tilganger inn i systemer for å hente ut datatrafikk hos samfunnsaktører, i næringsliv og hos enkeltpersoner (Allen & Chan, 2017). I tillegg kan bruk av kunstig intelligens i verste fall bidra til sikkerhetsrisiko knyttet til krigføring, for eksempel ved ikke kontrollerte droneangrep (Scharre, 2016). Som vist omfatter IKT-sikkerhet enkeltindivider, næringsliv, offentlig sektor og samfunnssikkerhet generelt. IKT-sikkerhet innebærer derfor at ulike utfordringer må håndteres på ulike måter av ulike aktører og med ulike kompetanser. En NIFU-rapport fra 2017 fastslo at det finnes et gap mellom dagens kompetansetilfang og framtidens kompetansebehov innen IKT-sikkerhet (Mark et al., 2017).

I denne artikkelen skal vi ta for oss et tema der dette gapet er spesielt kritisk og sosiologisk interessant, nemlig innenfor det som kalles for «Tingenes internett», Internet of Things, eller kun forkortelsen IoT. «Tingenes internett» ble introdusert allerede i 1999 av Kevin Asthon (Razzaq, Gill, Qureshi & Ullah, 2017). I 2017 ble det identifisert 433 000 søkbare enheter tilkoblet Internett bare i Oslo. Slike enheter omfattet overvåkningsutstyr, databaser, babymonitorer, medisinsk utstyr og husholdningsapparater (Hellberg & Vosseler, 2017). Tingenes internett er med andre ord blitt en del av livene våre, både som privatpersoner, som samfunnsaktører og preger det samfunnet vi lever i. Og utviklingen har gått veldig raskt og kanskje uten at vi helt har klart å ta inn over oss hva en slik utvikling kan bety. I artikkelen stiller vi følgende spørsmål: Hva betyr teknologisk utvikling og digitalisering her forstått som IoT for framtidens behov for kompetanse innen IKT-sikkerhet? Og utdanner Norge nok personer med adekvat IKT-sikkerhetskompetanse? Mens det første forskningsspørsmålet er ganske vidtfavnende og har som mål å undersøke hvordan digitalisering og teknologiutvikling i økende grad krever ulik kompetanse knyttet til sikkerhet, vil det andre spørsmålet utdype om vi utdanner nok personer med slike kompetanser. I vår studie mener vi med «adekvat» kompetanse den som tilbys av landets læresteder innenfor høyere utdanning. Det er da naturlig å spørre om hvordan status er i Norge. Så vidt vi vet, mangler vi kunnskap om disse høyst samfunnsrelevante spørsmålene, og vi håper denne artikkelen kan bidra til ny innsikt.

Del 2 redegjør for hvorfor IoT er et relevant felt å konsentrere seg om når det gjelder å fylle kompetansebehovet innen IKT-sikkerhet. Del 3 presenterer metode og datagrunnlag.

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Idunn
Nordiske tidsskrifter på nett

I del 4 skal vi med utgangspunkt i kvantitative data, framskrivninger og kvalitative intervjuer undersøke om det er et kompetansegap innen IKT-sikkerhet. I tillegg skal vi gjennom de kvalitative intervjuene fra IKT-sikkerhetssektoren undersøke hvilke tiltak som egner seg best når det gjelder å styrke sikkerhetskompetansen innen IoT, med fokus på utdanning, bedre kjønnsbalanse og befolkningens sikkerhetskultur. Vår analyse og diskusjon i del 5 viser at dersom ikke utdanningen økes og styrkes, vil det medføre sikkerhetsutfordringer på grunn av den økende utbredelsen av IoT. se.

TIDLIGERE STUDIER

I denne delen redegjør vi for hvorfor IoT er et relevant utgangspunkt for å forstå kompetansebehovet innen IKT-sikkerhet.

IoT omtales ofte som at de fysiske grensene mellom Cyber Space og den virkelige verden brytes ned, noe som leder til at vi får et såkalt cyberfysisk samfunn, der hverdagen er integrert med digitale enheter på nett (de Bruijn & Janssen, 2017; Kobara, 2016). Det gjelder for individer som omgir seg med såkalt smarte enheter, for eksempel smarte hus, selvkjørende biler, smarte TV-er, smarte klokker (Shackelford et al., 2017; Chifor, Bica, Patriciu & Pop, 2018; Devi, Rohini & Suganya, 2016). Men det gjelder også for virksomheter (Wu et al., 2018) og handel (Razzaq et al., 2017), og på samfunnsnivå innen transport, helse og smarte byer (Razzaq et al., 2017; Chifor, Bica & Patriciu, 2017). Felles for disse er den kontinuerlige interaksjonen mellom menneske og enhet, fra enhet til enheter samt fra enhet til enhet (Abdul-Ghan, Konstantas & Mahyoub, 2018). Spørsmålet blir da om samfunnet ikke bare teknisk sett, men også sosiologisk sett, er rigget til å håndtere en utvikling der hverdagen i økende grad blir integrert med digitale enheter.

Ofte blir muligheter framfor begrensninger knyttet til IoT trukket fram i litteraturen, blant annet innenfor matvaresikkerhet (Ellis, Muhamadali, Haughey, Elliott & Goodacre, 2015), potensialet i smarte hjem (Devi, Rohini & Suganya, 2016), intelligente helsesystemer, (Feng, 2016) til å utvikle nye forretningsmodeller (Elter, Gooderham, Dasi & Pedersen, 2018), eller knyttet til offentlig transport hvor IoT kan bidra til større miljømessig, økonomisk og sosial bærekraft (Davidsson, Hajinasab, Holmgren, Jevinger & Persson, 2016). Påfallende er det likevel at sikkerhetsutfordringene så vidt nevnes, som i ovennevnte studier.

Samtidig har vi sett at når enheter er koblet sammen i større nettverk, kan dette utgjøre en sikkerhetsrisiko. Sannsynligvis var det slike koblinger som lå bak to større angrep på ulike nett-tjenester, som for eksempel Mirai-angrepet i 2016[1] og Wannacry i 2017.[2] Trådløse enheter er ikke nødvendigvis designet til å håndtere sikkerhet (Razzaq et al., 2017). I tillegg finnes det et mangfold av ulike standarder og antall oppkoblinger som igjen gjør det vanskelig å følge tradisjonelle sikkerhetsforanstaltninger (Sicari, Rizzardi, Grieco &

1. Mirai-angrepet er det første globale angrepet på enheter koblet til nettet. Ved å angripe tjenestene som Facebook, Netflix og Amazon, sørget Mirai for å krasje store deler av Internett en hel dag.
2. Wannacry fikk mye medieomtale da det lyktes i å sette mange store institusjoner ut av spill, herunder det britiske helsevesenet, FedEx, MIT og jernbaneverkene i Tyskland og Russland. Wannacry låser infiserte maskiner og krever løsepenger for å gi brukere adgang til enhetene deres igjen.

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Coen-Porisini, 2015). Paquet-Clouston et al. (2018) peker dessuten på at sentrale aktører, for eksempel de som styrer sosiale nettverk og produsenter av IoT-enheter, klarer å unngå å ta ansvaret for eventuelle sikkerhetsbrudd, se og Mizhari (2018). Andre peker på at kommersialisering av IoT-enheter leder til sikkerhetsutfordringer med større risiko for cyberangrep (Mosenia & Jha, 2017).

For å imøtekomme sikkerhetsutfordringer for IoT-enheter, stilles en rekke basale sikkerhetskrav. Slike sikkerhetskrav gjelder for både individer (Weber, 2010). Slike nye krav og det økte fokuset på IKT-sikkerhet vil bidra til å øke framtidens etterspørsel etter IKT-sikkerhetskompetanse.

Vi har her beskrevet noen utfordringer knyttet til sikkerhet ved IoT. Vi har vist at IoT er gjennomgripende på alle nivåer i samfunnet, samtidig som at sikkerhet knyttet til IoT er en utfordring. Forskning peker også på at samfunnet ikke er rigget til å håndtere en fortsatt kraftig vekst i IoT-enheter, og at det mangler incentiver for utviklere av IoT-enheter til å fokusere på sikkerhet. I tillegg kan et endret trusselsbilde for individer, bedrifter og samfunnet drive fram et økt fokus på IKT-sikkerhet, noe som igjen vil øke etterspørselen etter IKT-sikkerhetskompetanse.

OMSTILLING OG BEHOV FOR NY KOMPETANSE

Når samfunnet digitaliseres, er det også behov for mer generiske IKT-kompetanser i både arbeidsliv og hverdagsliv, i tillegg til fagspesifikk IKT-kompetanse. Det vil også være behov for å kunne kombinere IKT-kompetanser med andre ferdigheter, som lederskap, kommunikasjon og samarbeid (OECD, 2015; OECD, 2016; Grundke, Squicciarini, Jamet & Kalamova, 2017). Ferrari med kollegaer advarer mot mangel på digital kompetanse i befolkningen generelt. Med digital kompetanse menes da evnen til å samle inn, håndtere og vurdere informasjon, evnen til å kommunisere digitalt, evnen til å skape nytt digitalt innhold, evnen til å håndtere det å være på nett på en sikker måte, samt evnen til å løse problemer ved hjelp av digital teknologi (Ferrari, 2013).

Det er gjort en rekke studier av arbeidsmarkedet for det som kalles IKT-spesialister, og for personer med IKT-sikkerhetskompetanse (Frost & Sullivan, 2017; Samfunnsøkonomisk Analyse , 2014; IT&Telekomföretagen, 2017; Højbjerre Brauer Schultz, 2017). Personer med IKT-sikkerhetskompetanse antas i denne sammenheng å være en del av gruppen «IKT-spesialister». Studiene peker på at det har vært en stigende etterspørsel etter IKT-spesialister og personer med IKT-sikkerhetskompetanse de seneste ti årene (Eurostat, 2016a). I Eurostat (2016a) konkluderes det med at sysselsettingsveksten for IKT-spesialister stort sett har vært upåvirket av finanskrisen og at veksten i sysselsetting fra 2006 til 2016 har vært på tre prosent per år, noe som er åtte ganger høyere enn sysselsettingsveksten generelt.

Høy sysselsetting bidrar likevel ikke nevneverdig til å dekke behovet. Eurostat viser i sine analyser at så mye som 41 prosent av europeiske bedrifter i 2015 opplevde utfordringer med å rekruttere IKT-spesialister (Eurostat, 2016b). Arbeids- og sosialdepartementet i USA estimerer veksten i IKT-sikkerhetsjobber til å være 28 prosent fram mot år 2026, noe som er betydelig mer enn den gjennomsnittlige jobbveksten (Bureau of Labor Statistics, U.S. Department of Labor, 2018). Global Information Security Workforce Study (Frost & Sullivan, 2017) gjennomførte en omfattende global survey med 19 641 respondenter.

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Her pekes det på at det allerede i år 2022 vil mangle 1 800 000 IKT-sikkerhetsmedarbeidere på verdensbasis. I Sverige estimerer en studie at det vil bli en betydelig underdekning av behovet for IKT-sikkerhetsmedarbeidere i landet fram mot år 2022 (IT&Telekomföretagen, 2017).

METODE OG DATAGRUNNLAG

Vår studie har tatt utgangspunkt i en kvantitativ framskrivning basert på ulike datakilder: MOSART, MODAG, registerdata og opplysninger om opptak og gjennomføring fra NSDs Database for statistikk om høgre utdanning (DBH). I tillegg har vi gjennomført intervjuer med representanter for privat og offentlig næringsliv, for myndighetene og for høyere utdanning. Data fra intervjuene bidrar til å utdype funnene fra den kvantitative framskrivningen.[3]

Kvantitativ framskrivning av tilbud og etterspørsel

Analysen bygger på Statistisk sentralbyrås (SSB) framskrivninger av tilbud på og etterspørsel etter samtlige utdanningsgrupper i Norge. Følgelig er framskrivningene i tråd med andre framskrivninger med fokus på tilbud på og etterspørsel etter kompetanse målt etter utdanningsnivå og utdanningsretning i det norske arbeidsmarkedet.

MODAG er Statistisk sentralbyrås makroøkonomiske modell for framskrivninger av norsk økonomi. Modellen er bygget opp rundt det norske nasjonalregnskapet, og beskriver hvordan agenter forventes å agere gitt forskjellige trender i økonomien. Adferden på lang sikt er basert på neoklassisk økonomisk teori. Modellen er relativt ensartet når det gjelder beskrivelsen av arbeidskraften, siden arbeidsmarkedet kun er delt i fem utdanningskategorier. Imidlertid beskriver modellen norsk næringsstruktur relativt detaljert, der man skiller mellom 45 produkter og 22 næringer. Videre har produktene forskjellige priser, avhengig av tilgang (norsk eller utenlandsk produsert) og anvendelse (eksport- eller hjemmemarkedet). Dette gir til sammen en omfattende beskrivelse av utvikling i næringsstrukturer i Norge, og hvordan endringene i næringsstrukturen påvirker den samlede arbeidskraftetterspørselen.[4]

For å beregne endringer i etterspørselen etter arbeidskraft på detaljert utdanningsnivå, har SSB utviklet en såkalt ettermodell som beregner sammensetningen av kompetanseetterspørselen fordelt på 28 forskjellige utdanningsgrupper. Ved å beregne andeler av sysselsettingen i hver enkelt næring og for hver av de fem utdanningskategoriene historisk og etterpå framskrive andelene trendmessig og fordele etterspørselen etter arbeidskraft på de 28 utdanningsgruppene, har man kunnet lage anslag for sysselsettingen etter detaljerte utdanningsretninger, se Cappelen et al. (2013) og Samfunnsøkonomisk analyse (2014).

MOSART brukes til en rekke formål, blant annet til framskrivninger av pensjoner og befolkningens utdanningsnivå. MOSART benytter individuelle kjennetegn for det enkelte

3. En mer utførlig beskrivelse av metode og datagrunnlag finnes i Mark et al. (2017).
4. Se kapittel 4 i Cappelen et al. (2013) for mer detaljert beskrivelse av MODAG.

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

individ, og på bakgrunn av dette beregnes sannsynlige valg knyttet til utdanning og arbeidsmarkedstilknytning. År for år estimeres sannsynligheten for (for eksempel med utgangspunkt i individets kjønn og alder) at et individ starter en utdanning. Videre vil MOSART også kunne si noe om individets sannsynlige valg av utdanningsnivå og -retning og sannsynligheten for om hun/han fullfører utdanningen.

Vår beregning av tilbud på og etterspørsel etter arbeidskraft med kompetanse i IKT-sikkerhet er basert på estimater av andelen som har kompetanse i IKT-sikkerhet i utdanningsgruppene som benyttes i SSBs framskrivninger av tilbud på og etterspørsel etter arbeidskraft i MOSART og MODAG. Det er et relativt stort antall IKT-studier som gir noe kompetanse i IKT-sikkerhet, men likevel få spesialiserte utdanninger i IKT-sikkerhet som kan identifiseres av utdanningskodene som benyttes i MOSART og MODAG (NUS2000). Det finnes derfor ingen fullstendig oversikt over hvor mange som har utdanning i IKT-sikkerhet.

Opplysninger fra NSDs Database for statistikk om høgre utdanning (DBH) har imidlertid gjort det mulig å framskaffe et relativt godt bilde av aktuelle studieprogram. DBH inneholder et bredt spekter av informasjon om universiteter, høgskoler og fagskoler, oversikt over alle studieprogram og hvilke emner som inngår i disse, og antall studenter og kandidater som fullfører studieprogrammene. Med utgangspunkt i disse opplysningene har vi forsøkt å identifisere flest mulig studieprogram som gir formell kompetanse i IKT-sikkerhet. Vi har inkludert studieprogram som har sikkerhet eller security i studieprogramnavnet eller emner forbundet med sikkerhet/sikring/security, kryptografi/kryptologi eller «intrusion detection».

Gjennomgangen av informasjon fra DBH har gitt oss oversikt over de siste års utvikling i antall studenter og uteksaminerte kandidater på minimum bachelornivå med utdanning i IKT-sikkerhet. Denne oversikten er så innarbeidet i estimatene av andelene med utdanning i IKT-sikkerhet i utdanningsgruppene som benyttes i framskrivningene i MOSART og MODAG. Beregningene for disse modellene strekker seg fram til 2030.

Kvalitative intervjuer

For å belyse ulike samfunnsaktørers vurdering av utfordringene rundt kompetansemangel hva gjelder IKT-sikkerhet, har vi gjennomført 18 intervjuer. Vi ønsket å treffe et bredt utvalg som omfattet UoH-sektor, enkeltstående forskningsmiljøer, myndigheter, interesseorganisasjoner og næringsliv. Slik omfattet utvalget representanter for både meso- og makronivået. Makronivået omfatter myndighetsnivået og inkluderer informanter fra departement og forvaltning. På mesonivået har vi intervjuet personer tilknyttet universitets- og høgskolesektoren, herunder personer tilknyttet studieprogram om IKT-sikkerhet og informanter tilknyttet særskilte kompetansemiljø innenfor IKT-sikkerhet. Mesonivået omfatter også private selskaper og organisasjoner. Oversikt over informantene er gjengitt i tabell 1.

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Tabell 1 Datakilder og informanter

Nivå	Enhet	Informantgruppe
Makro	Justis- og beredskapsdepartementet	Myndighet
	Kunnskapsdepartementet	Myndighet
	Kommunal- og moderniseringsdepartementet	Myndighet
	Difi	Myndighet
	Helsedirektoratet	Myndighet
	Uninett	Myndighet
	Oslo kommune	Lokal myndighet
Meso	Telenor	Bedrift
	Atea	Bedrift
	IKT Norge	Bransje- og interesseorganisasjoner
	Abelia	Bransje- og interesseorganisasjoner
	LO	Bransje- og interesseorganisasjoner
	TEKNA	Bransje- og interesseorganisasjoner
	SIMULA senter IKT sikkerhet	U&H, Forskningssenter
	CCIS	U&H
	Sintef-Digital	U&H
	Utdannings- og forskningssenter for digitalisering, OsloMet	U&H
	NTNU, Institutt for datateknologi og informatikk	U&H

Vi utviklet intervjuguider tilpasset de ulike informantgruppene, men samtlige informantgrupper ble bedt om å reflektere over temaene IKT-sikkerhetskompetanse, arbeidslivets behov for – og rekruttering av – personer med adekvat IKT-sikkerhetskompetanse og perspektiver knyttet til etter- og videreutdanning. Informantene ble kontaktet med forespørsel om å delta via e-post**.** Vi oversendte tema for intervjuet i forkant. Intervjuene ble gjennomført på telefon, og det ble gjort lydopptak. Som hovedregel var det to forskere til stede under intervjuet hvor den ene intervjuet, mens den andre tok notater. En oppsummering av intervjuet ble oversendt informanten for verifisering. Intervjumaterialet ble i det videre analysearbeidet organisert ut fra temaene fra intervjuguiden.

Samlet vurdering av data

Studien bygger på en kvantitativ framskrivning og kvalitative intervjuer med ulike aktører knyttet til feltet IKT-sikkerhet. Ved å anvende MOSART og MODAG ser vi på det samlede norske arbeidsmarkedet, slik at man ikke får sektorresultater som er løsrevet fra alt annet, men som tar hensyn til andre forhold i samfunnet (som at ulike sektorer påvirker hverandre og at ikke alle sektorer kan vokse samtidig). Statistisk sentralbyrå benytter den makroøkonomiske modellen MODAG til å framskrive etterspørselen og mikrosimuler-

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

ingsmodellen MOSART til å beregne tilgangen på kompetanse, se eksempelvis Holmøy, Kjelvik & Strøm (2014) og Dapi et al. (2016).

De kvalitative intervjuene bidrar til å gi innblikk i ulike forståelser av hva IKT-sikkerhetskompetanse betyr innenfor ulike områder av samfunnet, og ikke minst ulike forståelser av framtidens behov for slike kompetanser. Herunder for eksempel hvordan utviklingen innen IoT øker framtidens behov. Samlet sett vil dataene slik bidra til et nyansert bilde av framtidens behov for IKT-sikkerhetskompetanse, samtidig som de også gir innblikk i noen dilemma og utfordringer knyttet til dette feltet.

UTDANNES MANGE NOK MED IKT-SIKKERHETSKOMPETANSE, OG HVORDAN FYLLE ET POTENSIELT GAP?

I perioden fra 2012 til 2016 ser vi en dobling i antall studenter og kandidater på studier der hovedfokus er på IKT-sikkerhet. I tillegg ser vi en tilsvarende økning i IKT-studieprogram med enkeltkurs i IKT-sikkerhet. Økningen er ikke like markant, men er på mer enn 40 prosent for antall studenter og mer enn 60 prosent for antall kandidater utdannet innenfor denne type studieprogram.

Tabell 2. Antall studenter og kandidater på studieprogram i IKT sikkerhet og IKT-studier med kurs i IKT-sikkerhet, bachelorgrad og mastergrad. Høstsemesteret

	2012	2013	2014	2015	2016
Antall studenter: Studieprogram i IKT-sikkerhet	163	198	207	224	358
Antall studenter: Studieprogram med kurs i IKT-sikkerhet	1945	2222	2378	2579	2736
Antall kandidater: Studieprogram i IKT-sikkerhet	26	39	51	29	49
Antall kandidater: Studieprogram med kurs i IKT-sikkerhet	278	350	391	403	456

Kilde: DBH og studieprogram fra lærestedenes egne hjemmesider.

Andelen studenter og uteksaminerte kandidater på studieprogram spesielt innrettet mot IKT-sikkerhet er imidlertid lav. Andelen ligger på rundt 8–11 prosent av alle som tar utdanning som inneholder minimum et enkeltfag i IKT-sikkerhet i perioden 2012–2016. Hvorvidt dette er en utfordring med hensyn til framtidens kompetanseetterspørsel, klarer vi ikke å svare på i denne studien. Det vil avhenge av i hvor høy grad framtidig etterspørsel knytter seg til henholdsvis bredde- eller spisskompetanse innen IKT-sikkerhet. Vil det være et stort behov for spesialister, eller blir det slik at alle relevante yrker må ha litt mer IKT-sikkerhetskompetanse? Svaret ligger nok midt imellom og blir derfor et slags «både/og».

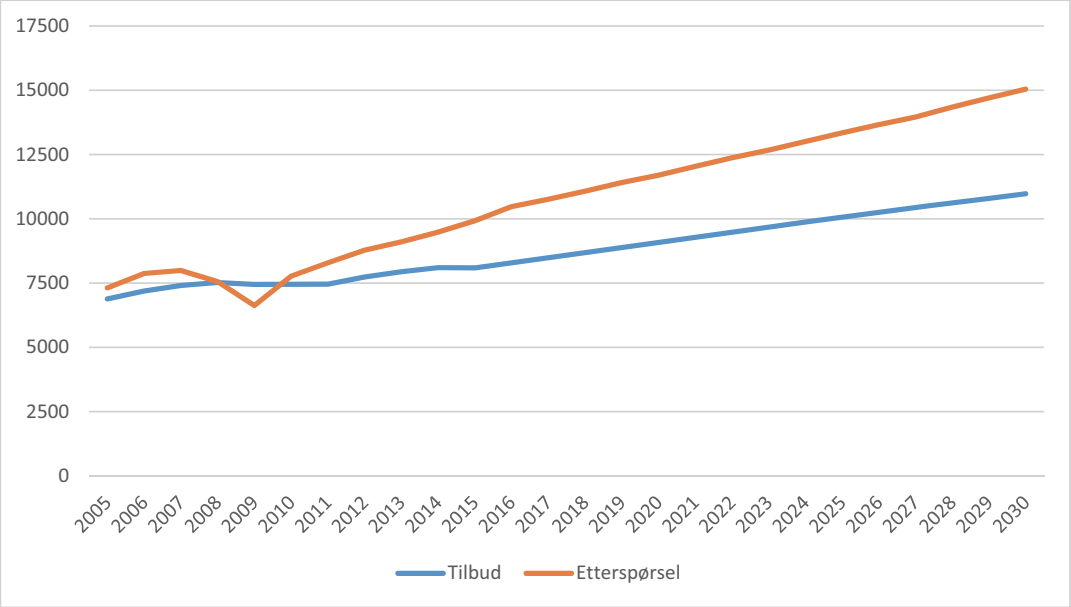
Til tross for den betydelige veksten i studenter og uteksaminerte kandidater, er gapet mellom tilgang og behov økende. Våre framskrivninger peker på at det allerede per i dag er et gap mellom tilgang og behov, og dette gapet vil øke fram mot år 2030. Våre esti-

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

mater peker på en underdekning på 4100 personer med IKT-sikkerhetskompetanse i år 2030.

Figur 1 viser at til tross for en forventet stabil økning av personer med IKT-sikkerhetskompetanse, øker gapet. Det skyldes en enda kraftigere økning i etterspørselen. I år 2030 passerer etterspørselen 15 000 personer. Dette svarer til at tilbudssiden må økes med 37 prosent for å kunne møte framtidens etterspørsel. Slik tallene fra den svenske undersøkelsen (IT&Telekomföretagen, 2017) pekte på, er det et behov for å øke å øke antallet medarbeidere med IKT-sikkerhetskompetanse med 35,7 prosent fram mot år 2022.

Tallene i figur 1 viser et fall i etterspørselen i årene 2008 og 2009. Dette er konsekvensen av finanskrisen i annen halvdel av år 2007. Krisen begynte for alvor i år 2008 og kulminerte i august 2008. Etterspørselen etter personer med IKT-sikkerhetskompetanse er imidlertid så sterk at fallet i etterspørselen er utjevnet allerede i år 2011.



Figur 1. Tilbud på og etterspørsel etter personell med IKT-sikkerhetskompetanse

Kilde: NIFU 2017.

Figur 1 beskriver det man kan kalle en nøytral utviklingsbane, der framskrivningene er basert på dagens status og trender. Det er mulig å gjøre forskjellige antagelser om utviklingsbanene fra i dag og framover, se Roksvaag og Texmon (2012) og Samfunnsøkonomisk analyse (2014). Slike antagelser kunne eksempelvis være at det framover vil være et avtagende fokus på IKT-sikkerhet; da vil etterspørselskurven få en avtagende positiv helning, og kompetansegapet vil bli mindre enn det figur 1 viser. Et annet eksempel kunne være at IKT og IKT-sikkerhet år for år blir satt enda høyere på den utdanningspolitiske dagsordenen. I tillegg ønsker flere unge å ta en utdanning innen IKT-sikkerhet, noe som vil bety at tilbudskurven i figur 1 vil få en økende postiv helning fra midten av 2020-årene, og dermed blir kompetansegapet mindre i år 2030. Man kan også se for seg at graden av digitaliser-

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

ing øker parallelt med kompleksiteten i cyberkriminaliteten, noe som vil føre til en økende positiv helning på etterspørselskurven allerede fra i dag og økt kompetansegap i år 2030.[5]

Det er ikke bare innen IKT-sikkerhet at det framover antas å bli et kompetansegap. Siden år 2000 har den relative andelen av akademikere økt fra 5,7 til 10,4 prosent i 2015. Målt i antall sysselsatte personer svarer det til en økning fra 130 000 til 268 000 (Eggen & Røtnes, 2017), tall som kan tolkes som økt etterspørsel. En annen undersøkelse peker på at det blir et kompetansegap innen IKT generelt, og at det i år 2030 vil være et udekket behov for personer med IKT-kompetanse på minimum bachelornivå på rundt 11 000 personer. Dette svarer til at tilbudssiden må øke med rundt 25 prosent for å kunne møte framtidens etterspørsel (Samfunnsøkonomisk Analyse , 2014). SSB har via HELSEMOD[6] estimert underdekningen av helse- og sosialpersonell fram mot 2035 til å være på 76 200 personer, noe som betyr at tilbudssiden må økes med 20,4 prosent (Roksvaag & Texmon, 2012). Vår analyse peker på et gap på knappe 40 prosent; relativt sett blir da kompetansegapet innen IKT-sikkerhet størst av de nevnte eksemplene.

Det kan pekes på flere årsaker til den kraftig økende etterspørselen etter personell med IKT-sikkerhetskompetanse, som også må antas å fortsette i årene som kommer. Norge har vært langt framme i å utvikle digitale løsninger for offentlig sektor, bredbåndsinfrastruktur og integrering av digitale løsninger, og landets innbyggere er i forkant når det gjelder bruk av IKT i hverdagen. Selv om Norge ikke er helt i tet – vi blir blant annet slått av land som Estland og Danmark, som skårer noe høyere på det som omtales som «gode» og «generelle» digitale ferdigheter (Europakommisjonen , 2016) – er Norge like fullt blant de mest digitaliserte landene i EU og EØS (Capgemini Consulting, 2016). Et uttalt ønske om effektivisering av offentlige og private tjenester, som på sikt kan skape konkurransefortrinn i en internasjonal sammenheng, har på mange måter vært en sentral motivasjon for digitaliseringsprosessene vi har vært vitne til her til lands og i land det er naturlig å sammenligne oss med. Men samtidig skaper dette også en bekymring for om digitaliseringsprosessen faktisk har gått for raskt, og at man ikke i tilstrekkelig grad har klart å identifisere og ivareta utfordringer knyttet til sikkerhet når tidligere analoge tjenester og systemer har blitt digitalisert.

På bakgrunn av denne kunnskapen, vår innledningsvise presentasjon av det omfattende omfanget av risikomomenter og vår analyse, mener vi at vi med rimelig stor sikkerhet kan si at det utdannes for få med IKT-sikkerhetskompetanse, og at det 10–20 år fram i tid har utviklet seg et relativt stort kompetansegap.

Hvordan fylle kompetansegapet?

For å få bedre innsikt i de utfordringene dette kompetansegapet potensielt kan bidra til, intervjuet vi representanter fra flere av de viktigste samfunnsaktørene.

5. Den eksakte tallfesting av det ovenstående krever en grundig gjennomgang av hvert scenario med vurderinger av graden av påvirkning på både tilbuds- og etterspørselssiden. Det ligger utenfor denne artikkelens mulighet å gjøre noe slikt, men det kan være utgangspunkt for ny forskning på feltet.
6. HELSEMOD er et planleggingsverktøy som benyttes til framskrivninger av tilbud av og etterspørsel etter helse- og sosialpersonell.

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

De følgende avsnittene består slik av presentasjon av synspunkter fra informantene knyttet til ovennevnte tema. Sammen med våre egne betraktninger, basert på våre analyser, fungerer disse som innspill i diskusjonen vi som forskere fører med utgangspunkt i funnene fra den kvantitative framskrivningen.

Uavhengig av tilknytning var informantene samstemte i at det er et behov for at flere utdanner seg innen IKT-sikkerhet – en utvikling som i betydelig grad er drevet av den teknologiske utvikling, eksempelvis via IoT. Våre informanter peker på betydningen av å tenke IKT-sikkerhet som en integrert del av produktutvikling, enten det er helsesystemer, smartklokker eller integrerte kameraer i leketøy. Ikke bare er dette viktig for den aktuelle målgruppen designet er laget for; like viktig er det at produkter over tid kan endres og bli brukt i nye sammenhenger. Dersom sikkerheten ikke er tilstrekkelig ivaretatt i designet, kan nye sårbarhetssituasjoner oppstå. Våre informanter framførte bekymringer for at digitaliseringsprosessen og den teknologiske utviklingen eksempelvis innen IoT faktisk har gått for raskt, og at man ikke i tilstrekkelig grad har klart å identifisere og ivareta utfordringer knyttet til sikkerhet.

For å få flere til å utdanne seg innen IKT-sikkerhet, mente flere av informantene at det må allokeres flere ressurser til utdanninger innen IKT og IKT-sikkerhet, samt at det også stilles krav til utdanningsinstitusjonene om at ressursene går til å øke utdanningskapasiteten innen IKT-sikkerhet. Våre informanter fra UoH-sektoren ga for øvrig uttrykk for at dette i noen grad kan innskrenke UoH-sektorens autonomi. Likevel påpekte disse informantene at når det er snakk om en samfunnskritisk utfordring, må det komme tydelige føringer på hva ekstra ressurser skal anvendes til.

Våre informanter peker også på betydningen av å styrke eksisterende fagmiljøer. I første omgang er det sannsynligvis økte ressurser som kan bidra til en styrking av disse miljøene. Noen informanter foreslo blant annet å åpne opp for flere stipendiatstillinger innen fagfeltet. De peker på at dersom man klarer å gjøre det mer attraktivt å ta en forskerutdanning innen IKT eller helst IKT-sikkerhet, vil dette bidra til å både styrke fagmiljø og utdanninger. En styrking av eksisterende fagmiljøer vil igjen være avgjørende for å klare å rekruttere både forskertalenter og allerede etablerte fagpersoner og forskere – altså en slags selvforsterkende effekt. Det er selvfølgelig utfordrende å trekke unge, dyktige studenter til en forskerutdanning. Forskningsmiljøene er i konkurranse med både offentlig sektor og privat næringsliv, som kan tilby høyere lønninger og også interessante fagmiljøer. I konkurranse med høye lønninger utenfor UoH-sektoren, mener våre informanter imidlertid at et sterkt fagmiljø er UoH-sektorens viktigste konkurransefortrinn. Vi mener at dette kan være et viktig satsingsfelt for UoH-sektoren og myndighetene framover.

En annen viktig faktor for å tette kompetansegapet, og som flere av våre informanter var opptatt av, handler om å utjevne kjønnsforskjellene innen fagfeltet. Vi fant bl.a. at tall fra DBH viser at antall kvinnelige studenter innen IKT-sikkerhet har gått ned de siste fem år. I 2017 var kun 13,4 prosent av studentene innen IKT-sikkerhet kvinner mot 17,8 prosent i år 2012. Dette er ikke enestående for Norge; globalt framheves det at kun 11 prosent av de som jobber med cybersikkerhet i verden er kvinner (Frost & Sullivan, 2017). Nielsen (2002) finner at kvinneandelen blant norske kandidater som avla embetseksamen eller hovedfag i IKT-fag generelt i perioden 1981–1996, var 19 prosent – noe som indikerer at kvinneandelen har blitt lavere innen IKT-fag de siste 20 år. Det er tydelig at utdanningene

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

innen IKT og IKT-sikkerhet må gjøres mer attraktive for kvinner spesielt, men også generelt. Imidlertid mente våre informanter at det i deres organisasjoner ikke nødvendigvis var en skjevfordeling mellom kjønnene hva gjaldt stillinger knyttet til IKT. Informantene våre pekte likevel på at kvinner i mindre grad var representert i de mest «tekniske» stillingene, men fantes i større grad i stillinger hvor juss, HR og ledelse utgjør en sentral del av stillingen.

Sannsynligvis er det en mangelfull forståelse i befolkningen for det komplekse teknologiske samspillet mellom sosiale og organisatoriske dimensjoner som åpner for at IKT-kriminalitet skjer i stadig større omfang. Ofte er det menneskelige feil heller enn teknologi som er avgjørende for at kriminelle handlinger på nett finner sted. Våre informanter peker på at også her vil forskning og utdanning være avgjørende.

Flere av informantene foreslo å innføre IKT-sikkerhet tidlig i utdanningsløpet. Informantene pekte på betydningen av å skape en «kultur» for sikkerhet – at barn automatisk tenker «sikkerhet» når de bruker internettet. IKT-sikkerhet bør bli en del av hver enkelts hverdag, mente en annen informant. En økt bevisstgjøring vil kanskje kunne bidra til en økt interesse for å utdanne seg innen feltet. Disse synspunktene finner vi også gjenklang av hos Malmedal og Røislien, som kartla forståelsen av sikkerhetskultur blant norske borgere (Malmedal & Røislien, 2016).

VINDUET STÅR ÅPENT – ØKT MANGEL PÅ IKT-SIKKERHETSKOMPETANSE

Målet med artikkelen har vært å bidra med oppdatert kunnskap om behovet for og tilbud på kompetanse innen IKT-sikkerhet i Norge. Innledningsvis stilte vi to spørsmål, nemlig: Hva betyr teknologisk utvikling og digitalisering, her forstått som IoT for framtidens behov for kompetanse innen IKT-sikkerhet? Og utdanner Norge nok personer med adekvat IKT-sikkerhetskompetanse?

Den teknologiske utviklingen åpner for svært mange muligheter. Spørsmålet er da om fokus på IKT-sikkerhet følger med. Selvkjørende biler er spennende, men er de godt nok sikret mot cyberangrep? Kan man forestille seg at IKT-kriminelle overtar kontrollen på biler og bruker dem i en terrorhandling? Smarthus-teknologi kan være god løsning for for eldre og funksjonshemmede, men er husene godt nok sikret mot cyberangrep? Kan for eksempel uvedkommende ta kontroll over huset og på den bakgrunn kreve løsepenger? Andre eksempler kan være å overta personers bankkonti eller identitetstyveri. Vi konkluderer med at den teknologiske utviklingen, eksemplifisert ved IoT, vil gi et økt behov for kompetanse innen IKT-sikkerhet.

Det andre spørsmålet blir da om Norge utdanner tilstrekkelig med personer med adekvat IKT-sikkerhetskompetanse. Vi finner at det er en betydelig underdekning av personer med adekvat kompetanse innen IKT-sikkerhet. Underdekningen estimeres til 4100 personer i år 2030. Det absolutte tallet i seg selv er mindre interessant. Det som er interessant, er at gapet mellom tilbud og etterspørsel øker, selv om det de seneste fem år har vært en økning i antall studenter og kandidater med høyere utdanning innen IKT-sikkerhet (ref. tabell 2).

Våre analyser tok utgangspunkt i de personene som har tatt utdanning på høyere nivå, hvor IKT-sikkerhet er en større eller mindre del av utdanningen, og det er ikke gjort noen

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

distinksjoner mellom forskjellige typer IKT-sikkerhetskompetanse. En opplagt kritikk til vår analyse vil dermed kunne være at vi ser de forskjellige retningene innenfor IKT-sikkerhetskompetanse, enten det dreier seg om teknologi, sosiologi, kultur, ledelse eller juss, under ett. Det vil sannsynligvis være forskjellige framtidige kompetansebehov knyttet til IKT-sikkerhet avhengig av tiltenkte arbeidsoppgaver og ansvarsområde.

Generelt sett er treffsikkerheten i våre valgte modeller usikker, noe som også avspeiler en generell usikkerhet på samfunnsnivå om hva som trengs og hva som tilbys. Det finnes ingen modeller som med stor presisjon vil treffe tilbud og etterspørsel 20 år fram i tid. Allikevel har modellene til SSB bedre treffsikkerhet enn andre, og vant Samfunnsøkonomenes prognosepris i perioden 2005–2014, se Samfunnsøkonomene (2017).

De økonomiske modellene til SSB bygger på en rekke antagelser, og framskrivningene har nå-situasjonen som utgangspunkt og forutsetter at betingelsene for nå-situasjonen vil opprettholdes. MODAG er basert på tall over faktisk sysselsetting, og ikke et underliggende behov som finnes i næringslivet og offentlig sektor. MOSART bygger tallene på observerte personer med en gitt utdanning. Beregningene er gjort med utgangspunkt i formelt utdanningsnivå, og inkluderer ikke etter- og videreutdanning, kompetanse tilegnet i arbeidslivet eller selvlært kompetanse. Som MODAG bygger MOSART på historiske data, og derfor vil store endringer som for eksempel en stor økning i tallet på studieplasser og derav flere som gjennomfører utdanning, påvirke validiteten i framskrivningen når de opprinnelige forutsetningene endres.

Våre data viser at det kan være grunn til bekymring hva gjelder det framtidige behovet for og den faktiske tilgangen til IKT-sikkerhetskompetanse. Samtidig peker internasjonale og nasjonale studier på at det er en betydelig mangel på personer med adekvat IKT-sikkerhetskompetanse (Eurostat, 2016b; Bureau of Labor Statistics, U.S. Department of Labor, 2018; IT&Telekomföretagen, 2017). Vi anser med andre ord at våre funn er på linje med andre, surveybaserte kartlegginger – noe som igjen understreker bekymringen.

Det finnes ingen «quick fix» for å dekke dagens behov eller fremtidens behov for personer med IKT-sikkerhetskompetanse. I artikkelen peker vi imidlertid på enkelte tiltak som vil kunne imøtekomme deler av dette behovet – eksempelvis å øke antallet av studieplasser, noe som igjen vil kreve flere personer med undervisningskompetanse på høyere nivå. Når få tar doktorgrader innen IKT-sikkerhet, blir dette en utfordring. Økt fokus på etter- og videreutdanning er et annet tiltak, men dette vil kreve finansiering og utdanningskapasitet.

Konsekvensene av manglende IKT-sikkerhetskompetanse og manglende innsats innen IKT-sikkerhet er mange. For samfunnet på overordnet nivå betyr det at det potensielt blir stadig vanskeligere å beskytte seg mot cyberangrep. Det kan gå ut over kritisk infrastruktur som vannforsyning og elektrisitet, noe som igjen potensielt kan lamme store deler av samfunnet og dermed ha enorme kostnader. Det kan ramme vitale samfunnsinstitusjoner, for eksempel sykehus. Vi så hvordan store deler av det britiske helsevesenet ble lammet av et hackerangrep.

Manglende IKT-sikkerhetskompetanse kan også bli en stor utfordring for næringslivet. Cyberangrep på bedrifter kan for eksempel sette interne styringssystemer ut av drift. Forrige år ble danske Mærsk utsatt for et slikt angrep, noe som satte logistikken ut i et par døgn. Det kostet Mærsk mer enn 2 mrd. kroner. Det er enkelt å forestille seg at Mærsk vil si seg villig til å betale løsepenger. 40 prosent av norske virksomheter med mer enn 500

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

ansatte er helt eller delvis villige til å vurdere å betale løsepenger (Vanson Bourne, 2018). Betaling av løsepenger eller store tap som følge av hackerangrep vil gå ut over lønnsomheten til bedrifter, noe som igjen vil påvirke sysselsettingsnivået. Med andre ord: hvis ikke bedrifter tar IKT-sikkerhet på alvor og ikke har tilgang på den riktige kompetansen til å motstå angrep, vil det kunne gå ut over sysselsettingen, noe som igjen vil påvirke samfunnet.

En annen utfordring for næringslivet er at man utvikler produkter som er nettbasert. IoT gir utrolige muligheter, men IKT-sikkerhet må tenkes inn i den digitale transformasjonen. Når kjøleskapet, leker på barnerommet, smart-TV og annet er nettbasert, er dette mulige innganger for cyberkriminelle. Om ikke bedriftene klarer å gjøre disse produktene sikre, gjør de potensielle kjøpere sårbare for cyberkriminalitet. Enkeltindivider blir også utfordret av den manglende IKT-sikkerhetskompetansen. Som vi så i eksemplet over, er de mange mulighetene i IoT en trussel for privatpersoner. Det kan tenkes å bli en stor påkjenning for enkeltpersoner å bli utsatt for den typen kriminalitet.

Manglende kompetanse innenfor IKT-sikkerhet rammer med andre ord samfunnet som helhet, bedrifter og den enkelte. Vi har i artikkelen forsøkt å synliggjøre behovet for ulike typer IKT-sikkerhetskompetanse, knyttet både til teknologibaserte fagdisipliner og til mer generiske kompetanser.

Vinduet står fremdeles åpent, og det krever betydelig innsats på flere områder for å få lukket det godt igjen.

REFERANSER

Abdul-Ghan, H. A., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *International Journal of Advanced Computer Science and Applications*, 355-373. DOI: https://doi.org/10.14569/IJACSA.2018.090349

Abromhara, M., & Køien, G. M. (2014). Security and privacy in the internet of things: Current status and open issues. *Privacy and Security in Mobilie Systems (PRISMS)* (ss. 1-8). San Jose: IEEE. DOI: https://doi.org/10.1109/PRISMS.2014.6970594

Allen, G., & Chan, T. (2017). *Artificial Intelligence and National Security.* Cambridge: Harvard Kennedy School, Belfer Center.

Broadhurst, R., Grabosky, P., Alazab, M., & Chon, S. (2014). Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology*, 1-20.

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., . . . Flynn, C. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation.* Oxford: University of Oxford.

Bureau of Labor Statistics, U.S. Department of Labor. (2018). Occupational Outlook Handbook Information Security Analysts. I U. D. Bureau of Labor Statistics, *Occupational Outlook Handbook*. Washington, DC: U.S. Bureau of Labor Statistics.

Capgemini Consulting. (2016). *International Digital Economy and Society Index (I-DESI).* Brussels: Europakommisjonen - Directorate-General of Communications Networks, Content & Technology.

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Idunn
Nordiske tidsskrifter på nett

Cappelen, Å., Gjefsen, H., Gjelsvik, M., Holm, I., & Stølen, N. (2013). *Forecasting demand and supply of labour by education.* Oslo: Statistisk sentralbyrå.

Chifor, B., Bica, I., & Patriciu, V. (2017). Sensing service architecture for smart cities using social network platforms. *Soft Computing*, 4513-4522. DOI: https://doi.org/10.1007/s00500-016-2053-x

Chifor, B., Bica, I., Patriciu, V., & Pop, F. (2018). A security authorization scheme for smart home Internet of Things devices. *Future Generation Computer Systems-the International Journal of Escience*, 740-749. DOI: https://doi.org/10.1016/j.future.2017.05.048

Dapi, B., Gjefsen, H. M., Sparrman, V., & Stølen, N. M. (2016). *Education-specific labour force and demand in Norway in times of transition.* Oslo–Kongsvinger: Statistisk sentralbyrå.

Davidsson, P., Hajinasab, B., Holmgren, J., Jevinger, A., & Persson, J. A. (2016). The Fourth Wave of Digitalization and Public Transport: Opportunities and Challenges. *Sustainability*. DOI: https://doi.org/10.3390/su8121248

de Bruijn, H., & Janssen, M. (2017). Building cybersecurity awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 1-7. DOI: https://doi.org/10.1016/j.giq.2017.02.007

Devi, G., Rohini, R., & Suganya, P. (2016). Internet of things: A survey on privacy and security for smart homes. *Iioab Journal* , 667-674.

Eggen, F. W., & Røtnes, R. (2017). *Framtidens behov for akademikere.* Oslo: Samfunnsøkonomisk Analyse.

Ellis, D. I., Muhamadali, H., Haughey, S. A., Elliott, C. T., & Goodacre, R. (2015). Point-and-shoot: rapid quantitative detection methods for on-site food fraud analysis - moving out of the laboratory and into the food supply chain. *Analytical Methods*, 9401-9414. DOI: https://doi.org/10.1039/C5AY02048D

Elter, F., Gooderham, P., Dasi, A., & Pedersen, T. (2018). The digital future of Telcos: Dumb pipes or crucial partners in innovation of new business models. *Beta*, 131-147. DOI: https://doi.org/10.18261/issn.1504-3134-2018-02-01

Etterretningstjenesten. (2018). *Fokus.* Oslo: Etterretningstjenesten.

Europakommisjonen . (2016). *A new comprehensive Digital Skills Indicator.* Brussels: Europakommisjonen .

Eurostat. (2016a, Oktober). *ICT specialists in employment.* Hentet fra Eurostat Web site: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_in_employment

Eurostat. (2016b, November). *ICT specialists - statistics on hard-to-fill vacancies in enterprises.* Hentet fra Eurostat Web site: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises

Feng, N. (2016). Research on the Modern Intelligent Healthcare Platform from the Perspectives of Grid based Cloud Computing and Information Management System Assisted Internet of Things Technology. *International Journal of Grid and Distributed Computing*, 35-47.

Ferrari, A. (2013). *DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe.* Seville: Joint Reserach Center, European Comission.

Frost, & Sullivan. (2017). *Global Information Security Workforce Study.*

Grundke, R., Squicciarini, M., Jamet, S., & Kalamova, M. (2017). Having the right mix: the role of skills bundles comparative advantage and industry performance in GVCs. *OECD Science,*

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Idunn
Nordiske tidsskrifter på nett

Technology and Industry Working Papers, No 134. DOI: https://doi.org/10.1787/892a4787-en

Hellberg, N., & Vosseler, R. (2017). *Western European Cities Exposed - A Shodan-based Security Study on Exposed Cyber Assets in Western Europe.* Trend Micro.

Holmøy, E., Kjelvik, J., & Strøm, B. (2014). *Behovet for arbeidskraft i helse- og omsorgssektoren fremover.* Oslo–Kongsvinger: Statistisk sentralbyrå.

Højbjerre Brauer Schultz. (2017). *Efterspørgslen efter IT-sikkerhedsmedarbejdere i Hovedstadsområdet.* København: Højbjerre Brauer Schultz.

IT&Telekomföretagen. (2017). *IT-kompetensbristen - Den svenska digitala sektorns behov av spetskompetens.* Stockholm: IT&Telekomföretagen.

Kobara, K. (2016). Cyber Physical Security for Industrial Control Systems and IoT. *Ieice Transactions on Information and Systems*, 787-795. DOI: https://doi.org/10.1587/transinf.2015ICI0001

Malmedal, B., & Røislien, H. E. (2016). *The Norwegian Cyber Security Culture.* Gjørvik: NORSIS.

Mark, M. S., Tømte, C., Næss, T., & Røsdal, T. (2017). *IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud.* Oslo: Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU).

Mizhari, S. K. (2018). Ontario's New Invasion of Privacy Torts: Do They Offer Monetary Redress for Violations Suffered via the Internet of Things. *Western Journal of Legal Studies.*

Mosenia, A., & Jha, N. K. (2017). A Comprehensive Study of Security of Internet-of-Things. *Ieee Transactions on Emerging Topics in Computing*, 586-602. DOI: https://doi.org/10.1109/TETC.2016.2606384

Nielsen, R. A. (2002). *Kjønn, alder og prestasjoner Om karakterforskjeller i høyere utdanning.* Oslo: Universitetet i Oslo.

OECD. (2015). *OECD Science, Technology and Industry Scoreboard 2015.* Paris: OECD Publishing. DOI: https://doi.org/10.1787/sti_scoreboard-2015-en

OECD. (2016). *Skills for a Digital World: 2016 Ministerial Meeting on the Digital Economy Background Report.* Paris: OECD Publishing. DOI: https://doi.org/10.1787/5jlwz83z3wnw-en

Paquet-Clouston, M., Decary-Hetu, D., & Bilodeau, O. (2018). Cybercrime is whose responsibility? A case study of an online behaviour system in crime. *Global Crime*, 1-21. DOI: https://doi.org/10.1080/17440572.2017.1411807

Razzaq, M. A., Gill, S. H., Qureshi, M. A., & Ullah, S. (2017). Security Issues in the Internet of Things (IoT): A Comprehensive Study. *International Journal of Advanced Computer Science and Application*, 383-388. DOI: https://doi.org/10.14569/IJACSA.2017.080650

Roksvaag, K., & Texmon, I. (2012). *Arbeidsmarkedet for sosial- og helsepersonell fram mot 2035.* Oslo: SSB.

Samfunnsøkonomene. (2017). *Samfunnsøkonomenes prognosepris.* Oslo: Samfunnsøkonomene.

Samfunnsøkonomisk Analyse . (2014). *Dimensjonering av avansert IKT-kompetanse.* Oslo: Kommunal- og moderniseringsdepartementet.

Scharre, P. (2016). *Autonomous Weapons and Operational Risk.* Washington: Center for a New American Security.

Shackelford, S. J., Raymond, A., Charoen, D., Balakrishnan, R., Dixit, P., Gjonaj, J., & Kavi, R. (2017). When toasters attack: A polycentric approach to enhancing the "security of things". *University of Illinois Law Review*, 415-473.

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Idunn
Nordiske tidsskrifter på nett

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security privacy and trust in Internet of Things: The Road Ahead. *Compunter Networks*, 146-164. DOI: https://doi.org/10.1016/j.comnet.2014.11.008

Taylor, R. E., Fritsch, E. J., & Liederbach, J. (2015). *Digital Crime and Digital Terrorism, 3rd Edition.* Dallas: Pearson.

Uninett AS. (2017). *Informasjonssikkerhet - IKT-strategi for norsk universitets- og høgskolesektor.* Oslo: Kunnskapsdepartementets arbeidsgruppe for IKT-strategi og helhetlige løsninger.

Vanson Bourne. (2018). *Risk Value Report.* Global: NTT Security.

Weber, R. H. (2010). Internet of Things - New security and privacy challenges. *Computer Law and Security Review*, 23-30. DOI: https://doi.org/10.1016/j.clsr.2009.11.008

Wu, D., Ren, A., Zhang, W., Fan, F., Liu, P., Fu, X., & Terpenny, J. (2018). Cybersecurity for digital manufacturing. *Journal of Manufacturing Systems*, 3-12. DOI: https://doi.org/10.1016/j.jmsy.2018.03.006

This article is downloaded from www.idunn.no. © 2019 Author(s).
This is an open access article distributed under the terms of the Creative Commons CC-BY-NC 4.0 License (http://creativecommons.org/licenses/by-nc/4.0/).

Idunn
Nordiske tidsskrifter på nett