Trusler og trender 2016

Bildet: Maria Nyheim

NorSIS

2016

Evolusjonen innen trådløs teknologi og digitale produkter de siste tyve årene har vært makeløs sett i historisk perspektiv. Førerløse biler og tilnærmet kontantløse samfunn har kommet raskere enn mange har våget å spå. Konkurransesituasjonen i næringslivet endres som følge av nye digitale produkter og tjenester. Det kreves innsikt, evne og vilje til å følge med og utnytte fortrinnene dette gir.

Det digitale livet er ikke en adskilt del av hverdagen, men en naturlig del av livet som gjør det vanskelig å skille mellom digitale og fysiske aktiviteter og handlinger. Internett og trådløs teknologi har gitt store muligheter til gevinstrealisering og effektivisering. Dagens mindreårige vil ikke huske noe annet enn at internett er overalt og at produkter og mennesker kommuniserer digitalt. Streaming av filmer, bildedeling, netthandel og annonsering har i mange år vært en naturlig del av hverdagen. Tilbud, omfang og tilpasning til hver enkelt er imidlertid nye elementer som eskalerer. Sammenstilling av stordata kan være til ulempe for den enkeltes personvern.

Et raskt utviklingstempo og teknologisultne forbrukere gjør at man omgir seg med og sprer informasjon om seg og sine vaner i «øst og vest». Informasjonen har blitt en kapitalvare i seg selv. En gjennomsnittlig bruker på nettet har en estimert markedsføringsverdi på 0,004 norske kroner. Tilgang til sensitive personopplysninger som bidrar til enda mer målrettet reklame høyner verdien. For eksempel har

Bilder: Maria Nyheim

markedsverdien for en gravid kvinne i 6. måned en estimert verdi på 90 øre. Persontilpasset reklame på nett er ikke nytt, men innen kort tid vil dette også gjelde TV[1].

Nyhetsbildet viser daglig til hendelser om nettkrenkelser og datakriminalitet. Det er en kjensgjerning at endringer i samfunnet og økonomi generelt også vil påvirke og endre kriminalitetsbildet. De kriminelle ferdes der økonomien er i sterk vekst og risiko for straff og konsekvenser er lav. Den digitale arena har nærmest ført til en frisone å ferdes i for mange kriminelle. Kun 13 % av de som har opplevd datakriminalitet eller kriminalitet på internett har anmeldt forholdet[2]. Det er viktig for enkeltindividet og samfunnet som helhet at politiet har evne og vilje til å etterforske og bidra til at datakriminelle blir tatt og straffet. Datakriminalitet krever annen kompetanse enn etterforskning av tradisjonelle lovbrudd. Det vil også virke preventivt om datakriminelle blir straffedømt og at risikoen for å bli tatt er høyere enn i dag.

I årets utgave av Trusler og trender vil vi trekke frem særlig to tema. Det ene er hvordan vi selv frivillig sprer informasjon om oss og våre gjøremål, det andre tema er hvordan kriminelle lurer fra enkeltpersoner og ansatte informasjon og benytter dette til å gjennomføre kriminelle handlinger. Formålet er i de aller fleste tilfellene økonomisk vinning. Det kan være vanskelig å forstå hvor mye verdi det ligger i ens personlige informasjon og det kan være veldig vanskelig å skille mellom personer med «urent mel i posen» og de seriøse aktørene.

---

[1] *Datatilsynet; Det store datakappløpet, 2015*

[2] *Politiets innbyggerundersøkelse 2015*

Bildet: iStockphoto.com


Norsk senter fo
informasjonssi

Direktørens ord

Digitaliseringen påvirker i økende grad arbeidslivet, næringslivet og hverdagen vår. Teknologien har eksistert ganske lenge, men endringer i økonomien tvinger oss nå til å sette ideene ut i live. Vi trenger nye løsninger når etterspørsel etter tradisjonelle varer og tjenester, miljøutfordringene og ikke minst forretningsmodellene endres. Samtidig oppstår helt nye muligheter for verdiskaping og kriminalitet. Etter hvert som myndighetene og næringslivet ser gevinstene som ligger i digitalisering vil verdiskapingen øke og kriminaliteten tilpasse seg umiddelbart.

Staten har avsatt betydelige midler for å forsterke digitaliseringen og flere offentlig tjenester blir tilgjengelig fra smarttelefonene våre. Delingsøkonomien tar fart og livene våre blir mer digitalisert. I økende omfang foretrekker vi å bruke tjenester som Airbnb og Uber. Netthandel brer seg til nye områder og nettbutikkene blir bedre tilpasset våre individuelle ønsker og behov. Nye aktører tilbyr dagligvarer på nett og vi gir terningkast til de som leverer varene til oss. De forbrukerne er fornøyde med øker sin omsetning og de som leverer dårlig kvalitet forsvinner. Kabel-TV utfordres sterkt av strømmetjenester og underholdning forventes å være tilgjengelig på alle digitale flater.

Samtidig legger stadig bedre sikkerhetsløsninger grunnlaget for at vi også får helsetjenester og annen sensitiv informasjon tilgjengelig på nettet. Helserådgivning på nettet vil finne sin naturlige plass. Bruken av velferdsteknologi vil også øke. Fokus på livskvalitet og økonomi vil stå sentralt når vi tar i bruk slike løsninger. Eldre og mennesker med funksjonsnedsettelser vil dermed få bedre forutsetninger for å ta del i arbeidsliv, sosiale aktiviteter og utføre daglige gjøremål.

Bilder: Maria Nyheim

Trenden med at app'er tar over for web forsterkes. Skreddersydde, enkle og underholdende vil disse programmene imøtekomme stadig flere av våre behov i hverdagen. App'ene vi har på smarttelefonene våre er i ferd med å bli koblingen mellom oss selv og huset, bilen, innkjøpene og vennene våre. Tilgjengelighet over alt har blitt en realitet og vi vet hvor alle våre venner er og hva de gjør, uten at de har postet meldinger om det.

Samtidig kobles barnas leker til internett og levendegjør deres lek og utforskertrang på helt nye måter. Dukkene er ikke lenger passive, men husker hva barnet fortalte den i går og deltar aktivt i samtaler og lek. Plenklipperen og støvsugeren vet ikke bare hvordan hagen og huset vårt ser ut, men vil i stadig større grad selv velge når jobben skal gjøres. 2016 vil bli året hvor grensene mellom internett og de fysiske aktivitetene våre for alvor viskes ut.

Men er vi forberedt på å håndtere de etiske og sikkerhetsmessige utfordringene dette fører med seg? Er våre verdier, ideer og holdninger tilpasset en verden hvor de teknologiske mulighetene utvikler seg så raskt som de gjør i dag?

Politiet opplyser at samtidig som den tradisjonelle kriminaliteten reduseres, øker datakriminaliteten[3]. Omfanget og konsekvensene er store. Datakriminalitet koster det norske samfunnet omtrent 19 milliarder kroner årlig[4]. Denne formen for kriminaliteten er godt organisert, med sin egen logikk og egne verdier. Datakriminalitet selges som tjenester og data-innbruddsverktøy omsettes som om det skulle være ordinære varer. Arenaen er «Darknet», et undergrunns-nett, med et enormt utbud av ulovlige varer og tjenester. Både selger og kjøper opptrer med skjult identitet og alle forsøk på å stanse aktiviteten har så langt mislyktes.

Tekniske IKT-sikkerhetstiltak har derimot blitt bedre, men etter hvert som antivirus og sikrere datasystemer har gjort hacking vanskeligere, så har de kriminelle tilpasset sine metoder. Arbeidsmåtene til cyber-kriminelle har endret seg fra å angripe datamaskinen din til å angripe deg. Spesielt ser vi en framvekst av nett-svindel og ID-tyveri hvor de kriminelle utgir seg for å være fra kjente bedrifter, venner eller noen man dater på nettet. Dine og mine penger er uansett målet. Internett og mobiltelefonen er bare måter å nå oss på.

Vi opplever daglig at mobbing og ulike former for krenkelser på nett rammer enkeltpersoner hardt. I løpet av de to siste årene har antallet

---

[3] *Kriminalstatistikken 2015*

[4] *NSR, Mørketallsundersøkelsen*

henvendelser til slettmeg.no økt med nesten 30%. Hvor bør de sosiale og juridiske grensene for slike ytringer gå? Spenningsforholdet mellom retten til å ytre seg fritt på den ene siden, og retten til vern mot krenkelser, hatytringer og forfølgelse på den andre har kanskje aldri vært viktigere å ta tak i[5].

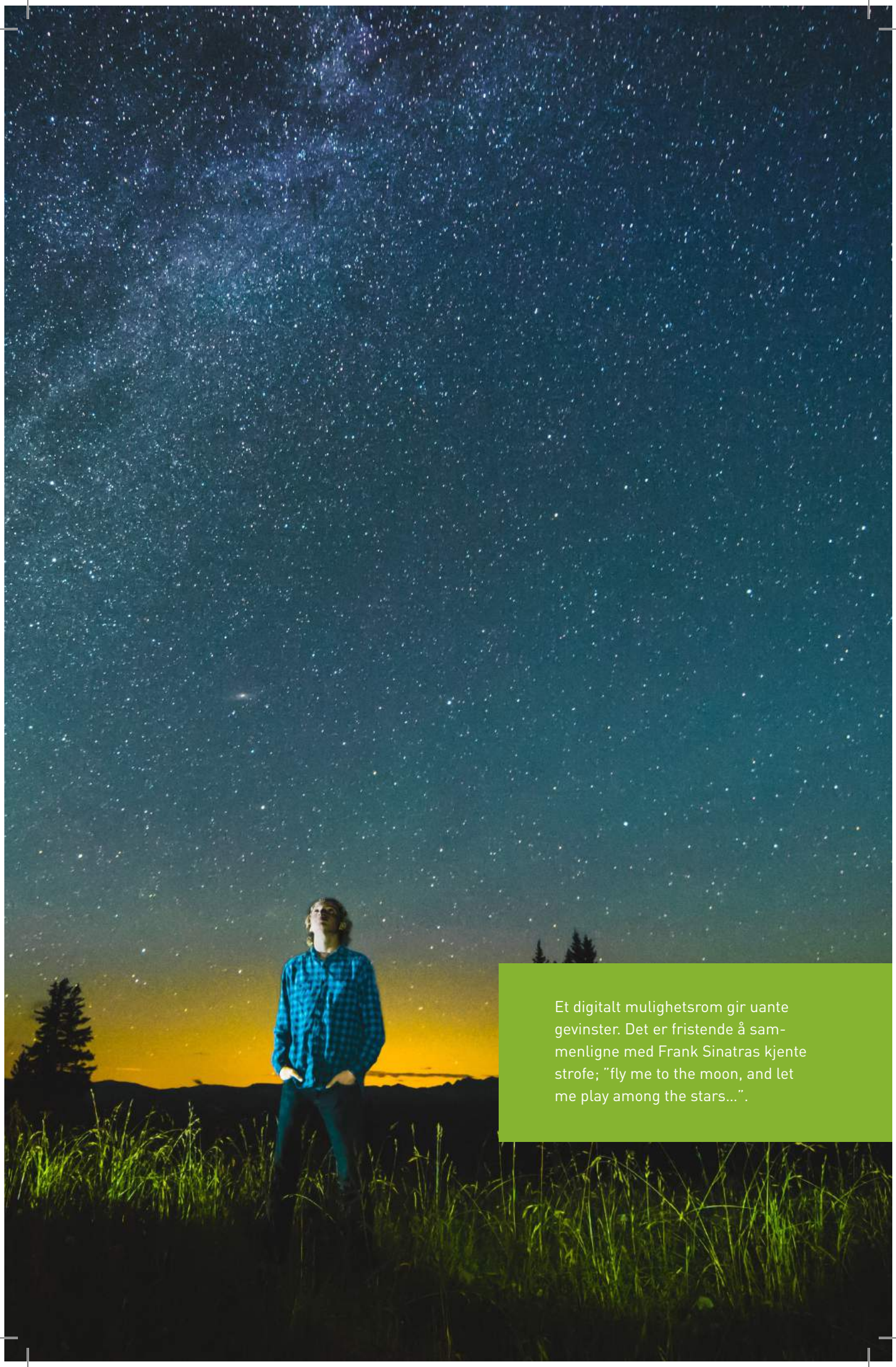
Vi ser dessverre en tendens til at mange skyver ansvaret for at vi skal være trygge på nett fra seg. Politiet skylder på manglende kapasitet og at gjerningspersonene er umulig å få tak i. Universitetene tilbyr avanserte IKT-studier uten en time datasikkerhet. Skolen forklarer at mobbing på nett er umulig å oppdage. Foreldre forstår ikke den nye teknologien og overlater barna til seg selv på nett. Alle er ikke slik, men vi hører så alt for ofte slike historier.

Vår anbefaling er samarbeid og åpenhet. Samarbeid på tvers av offentlig og privat sektor om de store spørsmålene og de praktiske løsningene. Åpenhet om datakriminalitet, slik at alle får mulighet til å forberede seg og utveksle ideer om gode løsninger. Spørsmålet om norske virksomheter bør være lovpålagt å informere eiere, kunder og samarbeidspartnere når de rammes av alvorlig datakriminalitet bør derfor på den politiske dagsorden.

Roger Johnsen
Administrerende direktør
Norsk senter for informasjonssikring

---

[5] *http://ytringsfrihet.no/status-for-ytringsfriheten-i-norge/ytringsfrihetens-grenser*



Et digitalt mulighetsrom gir uante gevinster. Det er fristende å sammenligne med Frank Sinatras kjente strofe; "fly me to the moon, and let me play among the stars...".

Et samfunn i endring - ”The sky is the limit...”

Bedrifter i 2016 har helt endrede forutsetninger enn for bare noen få år siden. Digitaliseringen av samfunnet har medført fordeler og innovative løsninger har bidratt til økt verdiskapning og effektivisering. Velferdsteknologi har gitt helsetjenesten helt andre muligheter til å utføre sitt virke. Forbrukerne har med IoT helt andre muligheter til å styre hjem, bil og sosialt liv enn tidligere. Mobiltelefonen har med alle sine app-er blitt «fjernkontroll i hverdagen».

Via mobiltelefonen har man tilgang til e-post, bildedeling, sosiale medier og app-er som kontrollerer og gir informasjon om og til trådløse produkter. Våre forbrukervaner på nett benyttes til å skreddersy løsninger og annonsemateriell. Tingenes internett er ikke lenger noe nytt, men bruk av roboter og kunstig intelligens er det som i forlengelsen av digitale tjenester og produkter er under utvikling til bruk i hverdagen.

Det totale bildet på verden er i radikal forandring hvis man ser på det globale samfunnet med «databriller». Cyberspace er ikke lenger en adskilt arena, den er luften vi puster og lever i. Vi etterlater oss elektroniske spor og kobler oss sammen digitalt ved mange av våre hverdagsaktiviteter. Derav begrepet «Internet in Everything».

Nordmenn er i særstilling kontra mange andre land i forhold til bruk av digital teknologi. I 2014 var 95% av norske husholdninger på nett[6].

[6] *http://www.bloomberg.com/visualdata/bestandworst/mostwiredintheworldcountries*

Bildet: unsplash.com

Mens gjennomsnittet for Europa[7] ligger på 73,5%. Endrede forutsetninger gir samfunnet utfordringer ved at spilleregler, etikk og handling ikke er etablerte og «gjengs» oppfatning er forskjellig.

Bedrifter må endre sine oppfatninger av hva samfunnet og næringsliv og forbrukere forventer og forlanger. Det digitale samfunnet må ivaretas i produkter og tjenester ellers kan man risikere å bli akterutseilt med fare for videre drift. 3D-printing vil komme for fullt og materialene som benyttes og smeltes sammen vil spenne seg fra karbon, plast og metaller til biologiske materialer.

Alt i det digitale nettet produserer, bruker og overfører informasjon. Informasjon har alltid eksistert overalt, men har ofte vært isolert, ufullstendig, utilgjengelig eller uforståelig. Fremskritt i semantiske verktøy som klassifiserer og analyserer enorme mengder data vil bringe mening til en ofte kaotisk flom av informasjon. Verdien av slik informasjon kan være enorm i de rette hender.

Grensen mellom det fysiske liv og det digitale liv viskes ut. Smarte maskiner vil overta for klassisk databehandling og informasjonshåndtering og lage systemer som autonomt kan lære å oppfatte verden på egen hånd. Eksplosjonen av datakilder og kompleksiteten av informasjon gjør manuell klassifisering og analyse umulig og uøkonomisk. Bruk av «intelligente» systemer utvikler seg «raskt» og organisasjoner må vurdere hvordan de kan bruke disse teknologiene for å oppnå konkurransefortrinn.

Smarte maskiner som roboter, autonome kjøretøy, virtuelle personlige assistenter og smarte rådgivere vil utvikle seg i året som kommer. Virtuelle personlige assistenter som Google Now, Microsoft Cortana og Apple Siri blir smartere og er forløpere til neste generasjon autonome agenter. I stedet for å kommunisere med menyer, skjemaer og knapper på en smarttelefon, snakker brukeren til en app, som er en virkelig intelligent agent[8]. Sikkerhet har ikke alltid fulgt utvikling av funksjonalitet. Hewlett Pachard gjennomførte i 2014 en undersøkelse som viste at 70 % av IoT har sårbarheter som kunne vært håndtert med programvareoppdatering[9].

En Oxfordstudie fra 2013 gjennomført av Carl Frey og Michael Osborn konkluderte med at 47 prosent av alle arbeidsplasser står i fare for

---

[7] *http://www.internetworldstats.com/stats.htm*

[8] *Gartner/Symposium ITxpo 2015 ; Top 10 Strategic Technology Trends 2016*

[9] *Hewlett-Packard Development Company, Internet of Things Research Study, USA 2014*

Bildet: iStockphoto.com

å bli automatisert. Duoen beregnet sannsynligheter for at yrker blir overtatt av datamaskiner. Blant de mest utrydningstruede yrkene pekte forskerne på de dårligste betalte, eller de med lavest kompetanse, slik som butikkansatte og maskinoperatører[10].

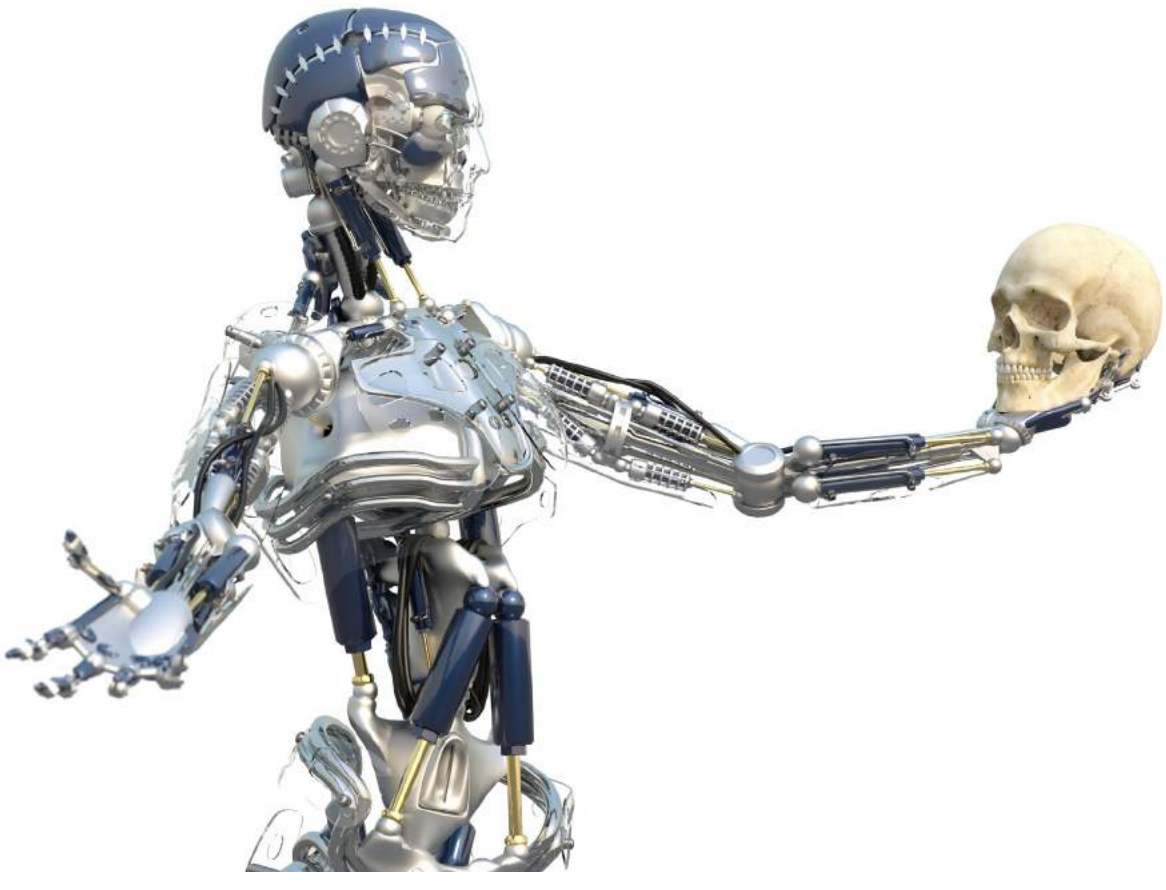
Geografiske grenser viskes ut, men samtidig har grensene betydning når det gjelder bruk av skytjenester og juridiske forskjeller og avtaler landene i mellom. En vesentlig endring i 2015 var EU-domstolens bestemmelse om datalagringsavtalen mellom USA og Europa (Safe Harbor) var ugyldig. EU-domstolen konkluderte med at amerikanske selskaper ikke ivaretar europeiske borgeres personvernrettigheter i sin behandling av europeiske borgeres personopplysninger[11]. I stedet er det ved inngangen til 2016 etablert en avtale kalt «Privacy Shield»-med formål å sette rammer for hva amerikanske myndigheter kan kreve av tilgang til europeisk persondata[12]. Det er viktig at virksomheter tar slike fakta som hvor lagres data, hvem behandler data og hvem får tilgang til hvilke data, i sin vurdering av skytjenester.

---

[10] *http://www.aftenposten.no/meninger/kronikker/Arbeidsliv-i-den-nye-robothverdagen--Camilla-Grana-8299608.html*

[11] *https://www.datatilsynet.no/Global/04_planer_rapporter/personvernrapporten-2016.pdf*

[12] *http://www.datatilsynet.no/Nyheter/2016/Enighet-mellom-EU-og-USA-om-nytt-rammeverk-for-hvordan-personopplysninger-kan-overfores-/*




BURTON

Hvem møter man på nett

Det er vanskelig å bedømme en person man møter på gaten. Man kan kanskje si litt om utseende, klesstil og i noen grad personlighet, mens personer man treffer kun digitalt har man ingen forutsetninger for å kunne si noe om. Ikke engang om de er hvem de utgir seg for å være.

Nettet florerer av hatefulle ytringer, svindelforsøk og dataangrep. Utfordringen blir hvordan man beskytter seg mot alle disse truslene. I utgangspunktet er det ikke noen forskjell fra det fysiske liv, men i det fysiske liv har man erfaring fra egen kultur og nedarvede beskyttelsesmønstre. På nett møter man alle kulturer og alle typer personligheter og den endrede måten å kommunisere og arbeide på har skjedd på veldig kort tid historisk sett. Det er nødvendig å finne nye måter å beskytte seg på og ha en forståelse for hvem man kan og vil møte på nett. Dette gjelder uavhengig av om man er privatperson eller næringsdrivende.

Hvordan kan man bli lurt

I 2010 opplevde en fjerdedel av alle internett-brukere i Norge tap av tid eller informasjon som følge av datavirus. Statistisk sentralbyrås undersøkelse om IKT-bruk i husholdningene[13] viser at etter 5 år er omfanget av virushendelser halvert. Etter hvert som antivirus og sikrere datasystemer har gjort hacking vanskeligere, så har de kriminelle tilpasset sin taktikk. Statistikken viser at samtidig som skadene som oppstår etter virus-hendelser går ned, øker andelen som har lidd økonomisk tap som følge av falske nettsider og falsk informa-

[13] *http://www.ssb.no/teknologi-og-innovasjon/artikler-og-publikasjoner/faerre-problemer-med-datavirus?tabell=249761*

Bilder: Maria Nyheim

Nettfisking, såkalt phishing, er når man fisker etter informasjon som direkte eller indirekte gir økonomisk vinning. Ofte gjennomført via e-post. Phishing er en måte å gjennomføre sosial manipulering.
Sosial manipulering er å lure offeret til selv å installere programvare, gi fra seg informasjon eller gjennomføre transaksjoner.

sjon. Spesielt ser vi en framvekst av nettsvindel og ID-tyveri hvor de kriminelle utgir seg for å være fra kjente bedrifter, venner eller noen man dater på nettet. ID-svindel rammet i fjor i overkant av 150 000 nordmenn[14]. Arbeidsmåtene til cyber-kriminelle har endret seg fra å angripe datamaskinen din til å angripe deg. Dine og mine penger er uansett målet. Internett og mobiltelefonen er bare måter å nå oss på.

E-post med vedlegg eller lenker man kan trykke på er den vanligste formen for angrep mot norske bedrifter[15]. Informasjonen en angriper er ute etter kan være personsensitiv eller bedriftssensitiv informasjon, kredittkortinformasjon eller man lurer offeret til å betale for falske varer og tjenester. Flere eksempler på dette er falske e-poster fra banker hvor man ber om brukernavn, passord og kredittkortinformasjon. Denne informasjonen er salgsvare for kriminelle. Det har også vært tilfeller hvor offeret har blitt oppringt i ettertid og benyttet informasjonen for å gjennomføre nettbanksvindel. En kombinasjon av metoder vil gi svindelforsøkene større legitimitet og bedre sjanser for å lykkes.

Kjente merkenavn utnyttes

Norske telefonnumre til intetanende politikamre eller enkeltpersoner blir utnyttet og benyttet av «Microsoft»-svindlere. Vilkårlige personer blir oppringt og får beskjed om at deres PC er infisert og at man via fjerntilkobling kan reparere dette. Gir man svindlerne tilgang til PC-en og nekter å betale har flere ofre fått sine dokumenter og bilder sperret. Det beste rådet er å legge på hvis man blir oppringt av svindlere.

Kjente virksomheter blir utnyttet og misbrukt av svindlere ved at de benytter deres merkenavn for å oppnå tillit hos ofrene. Ikea, Coop, Expert og Elkjøp er virksomheter som har blitt utnyttet av slik svindel. De har alle blitt benyttet som avsender til konkurranser som har til formål å sanke personlig informasjon eller har fått tilsendt ekstremt gode tilbud på varer. Varene vil ikke dukke opp, men man har intetanende betalt for ulike typer abonnement.

Hensikten med innsamling av personinformasjon er trolig for videresalg til markedsføringsbedrifter. Det er derfor vanskelig å ha fasiten på hvem man kan stole på og anse som en trygg og seriøs aktør. Det beste i slike tilfeller er å sjekke om konkurransen eller quizen faktisk

[14] *Id-tyveri undersøkelsen 2015, gjennomført av NorSIS og Skatteetaten*

[15] *http://www.digi.no/sikkerhet/2015/10/01/avslorer-farre-alvorlige-dataangrep-mot-norge*

kommer fra rett virksomhet. Avsenderadressen eller URL kan gi spor som viser at dette ikke er legitime kilder.

Flere av deg?

Å utgi seg for å være andre med formål å begå kriminelle handlinger eller med formål å krenke andre er identitetsvindel. Utgangspunktet for ID-svindel kan være informasjon man har sanket på nettet, stjålet post eller at man er i nær relasjon med offeret. Ofre for ID-tyveri opplever ofte at det er vanskelig å nøste opp svindelaktivitetene og enkelte bruker mye tid og ressurser på å bevise sin uskyld. Selv om ofrene ikke lider økonomiske tap vil de i lang tid etter å ha blitt utsatt for ID-tyveri være engstelige for når svindelaktiviteter kan starte igjen. Informasjon om dem er fortsatt ute på nett eller blant kriminelle som kan selge informasjonen videre som føre til flere svindelforsøk. Ved å sperre seg for kredittvurdering kan man unngå de mest opplagte svindelforsøkene.

Kjærestesvindel, eller datingsvindel er når man blir utsatt for svindlere som utgir seg for å venn, kjæreste eller fremtidig ektefelle. Svindlerne benytter falske profiler, ofte med bilder fra militære offiserer for å inngi tillit. Det brukes utspekulerte metoder for å overbevise ofrene om hvorfor de trenger penger. Sykdom i familien og reisekostnader er utgiftsposter som går igjen.

Med følelser som våpen

Datingsvindel hvor man benytter navn og bilder av reelle personer er kjente «agn» når kriminelle søker etter ofre. Formålet er fremdeles økonomisk vinning og «beileren» ber som regel om finansiell bistand til sykehusregninger, flyreiser eller advokatutgifter. Historiene er ofte tåredryppende fremstillinger av behovet for å låne penger. Det blir ofte gitt lovnader om å få tilbakebetalt lånebeløpet så snart arven blir utbetalt eller utenlandsoppholdet er over. Militære offiserer blir ofte benyttet som agn i datingsvindel, da disse inngir tillit i befolkningen. Svindlerne skaper ofte tette følelsesmessige bånd til ofrene. Studier fra University of Leceister viser til at ofrene for datingsvindel føler at tapet av en «sjelefrende» er større enn de økonomisk tap de er blitt påført. Ofrene har gjerne mistet ektefellen, er ensomme eller har et stort ønske om å møte den store kjærligheten. De har gjerne gått gjennom en sårbar fase i livet og kan slik bli et lett offer når de får stor omsorg og mye kjærlighet. Økokrim oppgir at 209 personer ble ofre for slik svindel i 2015, hvor disse har betalt til sammen 280 millioner kroner til svindlere. Slettmeg fikk i 2015 40 henvendelser relatert til datingsvindel. Dette er i hovedsak henvendelser fra familie og venner som er bekymret for at deres nære sannsynligvis er utsatt for datingsvindel.

Honningfeller

Lettkledde kvinner som ønsker å bli venner på sosiale medier har eskalert den senere tid. Formålet med disse lokkeduene er å spre annonsering av datingtjenester eller tjenester fra prostituerte. Kjøper

man tjenester av disse tilbyderne kan man bli presset for penger i ettertid via video-opptak, eller man blir presset på grunn av at man har begått kriminelle handlinger ved å kjøpe tjenester fra prostituerte. Det kan tyde på at flere av tilbyderne tilbyr andre tjenester i etterkant, eksempelvis at de skal rydde opp i utpressingen eller rense PC-en. Mange av ofrene vil ikke kontakte politiet på grunn av utpressingens art og svindlerne utnytter dette til sin fordel.

På jakt etter storfangsten

Norske bedrifter og deres ansatte blir utsatt for flere typer av sosial manipulering. En metode som er omtalt er e-post med lenke eller vedlegg som installerer ondsinnet kode på maskinen eller serveren. En annen type sosial manipulering som fikk et oppsving i 2014 og som Økokrim rapporterer har vært økende siden er såkalt ledelses-svindel. Dette betyr at man utgir seg for å være lederen i en virksomhet og ber økonomiansvarlig om overføring av penger til utlandet og at det haster med å gjennomføre betalingen. Leder er enten ikke tilgjengelig for kvalitetssjekk etter at e-post er sendt over, eller så utgir de kriminelle seg for å være daglig leder. Svindel av denne typen kan kun gjennomføres etter grundige undersøkelser av rutiner og ansatte. De kriminelle aktørene benytter tidsrom hvor leder av virksomheten er fraværende og utnytter dette tidsrommet til å gjennomføre svindelen. De som har vært utsatt for denne type svindel melder om voldsomt press for å få gjennomført betalingen[16].

Tjenestenektangrep (DDoS)
Det sendes massiv trafikk eller skadelige datapakker til en webside. Websiden takler ikke trafikken og bryter sammen. Hendelsen medfører at man ikke kan betjene kunder og man får ikke tilgang til data. Slike angrep kan skje vilkårlig eller være målrettet.

Utpressing og krav om løsepenger

Virksomheter blir utsatt for kriminelle som tar kontroll over lagret informasjon og krever løsepenger for å frigi lagret materiale. Informasjonen blir kryptert og dermed blokkert for tilgang av andre enn de kriminelle. De har nøkkelen som kan frigi informasjonen. Informasjonen som blir tatt som gissel kan være lagret på en PC, en server eller i skyen. Den vanligste formen for slike er angrep er der ofrene gir de kriminelle tilgang til virksomhetens systemer ved å klikke på lenker i en e-post. Betaling ønskes gjerne gjennomført i digital valuta, som Bitcoin.

Andre metoder kan være trusler om tjenestenektangrep hvis man ikke betaler beskyttelsespenger. Privat kan man utsettes for samme trussel-metoder. Andre betalingsformer kan være krav om seksuelle

[16] *http://www.okokrim.no/artikler/social-engineering-fraud-ceo 29.01.16*

[17] *https://norsis.no/assets/Trusler_og_trender_WEB_endelig_18022015.pdf*

handlinger eller kjæresteforhold, hvor trusselfaktoren er publisering av intime bilder eller videoer[17].

Samfunnets utvikling av autonome systemer som gressklippere, støvsugere, roboter, biler og droner kan utnyttes av kriminelle. Trådløs kommunikasjon og svakheter i systemene kan i mange tilfeller oppfattes av kriminelle som en ressurs. Et eksempel på dette er medisinsk utstyr som har trådløs tilkobling. En pacemaker kan hackes og kriminelle og terrorister kan utnytte dette til utpressing eller i verste fall drap. USAs visepresident Dick Cheney fikk i 2007 fjernet den trådløse enheten i sin implanterte hjertestarter[18], nettopp på grunn av fare for terrorhandlinger.

Løsepengevirus, eller ransomeware holder datafiler og bilder som gissel ved å kryptere dem. For å låse opp filene, dekryptering, blir offeret krevd for penger, gjerne i Bitcoin, en digital valuta. Betaler man løsepenger er man ikke garantert at filene blir gjort tilgjengelige igjen, og man risikerer å finansiere kriminell virksomhet.

Det frie ord

Nett-troll og mobbere kan skjule seg bak anonyme app-er og sende hatefulle og ondskapsfulle ytringer uten å vise ansikt eller navn. Fri ytring og spredning av bilder og videoer er en menneskerett. Medaljens bakside er nett-troll, mobbere og kriminelle, for eksempel pedofile, som utnytter og bruker informasjonen som deles. I dagens nett-samfunn må alle være sin egen redaktør for det som publiseres på nett.

Informasjon som betalingsmiddel

Falske konkurranser på nett eller underholdende oppstilling og tester av vennelista på Facebook innhenter personlig informasjon om den som deltar og vedkommendes venneliste. En leverandør av slike tester har som formål å innhente personlig informasjon som kan selges videre til markedsføringstiltak. Det er viktig å huske at slike underholdende tester ikke blir utviklet for å være gratis underholdning, men at man betaler med egen og venners personlige informasjon.

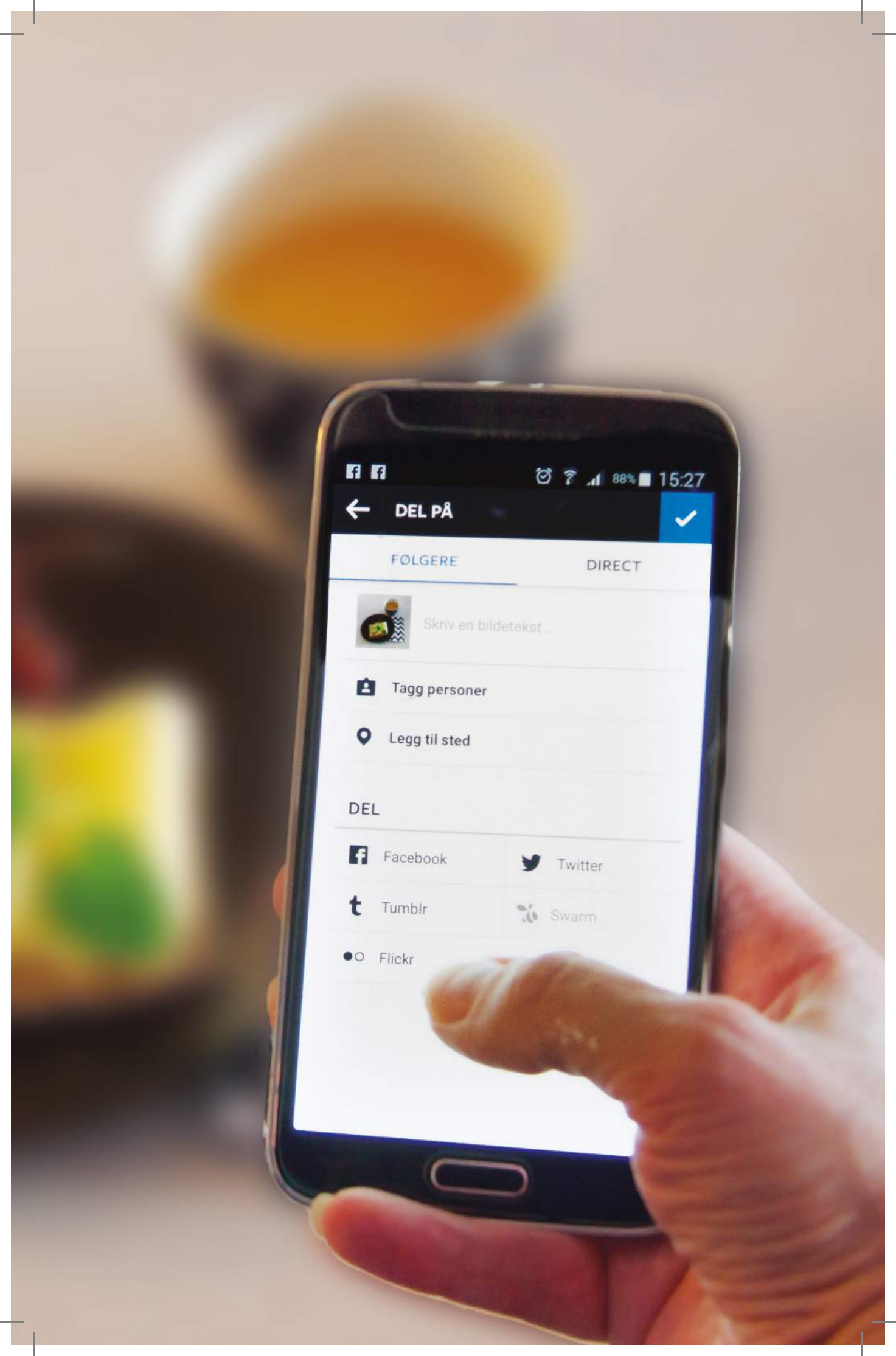
Darknet - det perfekte skjulested

Deler av internett er skjult for søkemotorer og åpne besøk. Dette kalles det mørke nettet. På slike plasser er man helt anonym og man vet ikke hvem andre man møter. Det mørke nettet gir beskyttelse mot personforfølgelse. Opprørere mot diktatur og terror har benyttet nettet til å samle folk og spre politisk agenda. Kilder til journalister sikres personvern når varsling kan være fare for liv og helse.

Den anonyme muligheten gir også kriminelle fritt spillerom. Våpen og narkotika omsettes og betaling skjer ofte i digital valuta. Overgripere har også sett muligheten det mørke nettet gir til å spre materiale til andre overgripere.

---

[18] *http://www.dn.no/magasinet/2016/01/08/2128/Teknologi/de-medisinske-hackerne*


88% 15:27
DEL PÅ
FØLGERE
DIRECT
Skriv en bildetekst ...
Tagg personer
Legg til sted
DEL
Facebook
Twitter
Tumblr
Swarm
Flickr

En digital hverdag

Ola og Kari Nordmann sine hverdagsvaner er fylt med digital samhandling og informasjonsutveksling. De digitale verktøyene som man benytter til daglig sender mye informasjon om hvor vi er, hva vi gjør og hvem vi kommuniserer med. Dette gir mange muligheter for en enklere hverdag, flere funksjoner foregår automatisk og man kan samhandle på tvers av landegrenser. Det kan imidlertid være noen «skjær i sjøen». Et eksempel på hva vi omgir oss med informasjon er å illustrere en familiehverdag som blir mer og mer vanlig.

Morgen

Smarthuset våkner til liv og øker til dagtemperatur. Dette er forhåndsprogrammert og familien styrer huset via kontrollpanel og app på telefonen. Familien benytter mobilen som vekkerklokke. Stedsangivelser er på og «finn venner»- appen er installert. Via app-en kan venner og familie se hvor de enkelte familiemedlemmene befinner seg og kollegaene kan se om man er på vei til arbeid. Svigermor har fått installert velferdsteknologi og har sensor i sengebunnen, slik at familien kan kontrollere om hun er våken og har stått opp. Hennes puls blir registrert av et armbånd og kan avleses via en app. Leverandørene av teknologien har samme data lagret på sine servere i et gitt tidsrom. Familiens tenåring står lenge i dusjen og gir sitt bidrag til økt strømforbruk. Hvor og hvem som bruker mest energi kan avleses via den smarte strømmåleren. Måleren gir også beskjed til energileverandøren og de kan tilpasse strømproduksjonen. Huseier kan via kontrollpanel

Bilder: Maria Nyheim

avlese hvem og hvor i huset man bruker mest energi. Strømleverandøren kan på sin side se når familiens morgen starter ved økt strømforbruk. Vaskemaskinen settes på og programmeres til automatisk å starte den innebygde tørketrommelen. Forløpet kan følges via app på mobilen.

Frokost

Kaffetrakteren er programmert til å være ferdig så snart morgendusjen er unnagjort. Bilde av hundens bedende blikk under frokosten publiseres på sosiale medier med et titalls hashtags. Bildet blir distribuert i flere kanaler og eierrettighetene til bildet overdras til flere virksomheter. Bildet blir benyttet i en reklame for dyrefôr uten familiens vitende. Under frokosten sjekkes det via smartbrett hvor det er oppkjørte skiløyper og ettermiddagens skitur planlegges. Dagens første videosamtale gjennomføres via app på nettbrettet med husets andre tenåring som er på utveksling i utlandet.

På vei ut døra...

Døren låses automatisk med den digitale dørlåsen. Familiens medlemmer har egen kode og vaskehjelpen har en annen kode som kun fungerer hver fredag mellom kl. 12 og 16. Døren kan også låses opp ved behov via app på mobilen. Lyset i huset slukkes via kontrollpanelet eller app på mobilen.

På vei til jobb og skole

Tenåringen tar buss til skolen. Holdeplassen har digital oversikt over avgangstider. De minste barna blir kjørt til barnehage og skole med familiens elbil. Bilens forbruk og hvor den befinner seg kan man også lese via app. Service og beskjeder fra verkstedet kommer via bilens skjerm. På vinterstid kan brøytebilens GPS viser hvilke veier som er ferdigbrøytet og hvor lang tid det tar før skiftet er ferdig.

På jobb

Dagens andre videokonferanse gjennomføres, denne gang med deltakere fra hele verden. Håndverkeren som skulle snekre kommer en dag for tidlig og hun slippes inn ved å taste inn kode i dørlås-appen. I virksomhetens produksjonsavdeling er det roboter som utfører arbeidet. Innstilling og programmering gjøres i et kontrollrom geografisk adskilt fra produksjonen. I lunsjen sjekkes det via app på mobilen om klesvasken er ferdig vasket og tørret. Den er OK. Plenroboten som er programmert til å starte om morgenen har ikke startet og må sjekkes etter arbeid. Etter et oppslag i en søkemotor dukker det opp målrettet reklame og forslag til artikler om parkettgulv som det ble søkt på dagen før. En e-post mottas med innbydelse til en konferanse i

utlandet. Programmet er et vedlegg å klikkes på. Vedlegget kan ikke åpnes, men filene blir kryptert med beskjed om at de kan låses opp igjen ved å betale løsepenger i Bitcoin. Virksomhetens IT-avdeling blir tilkalt og data må legges inn igjen fra back-up enheten.

På vei hjem

Minstejenta skal hentes i barnehagen og via mobilapp kan det avleses at ektefelle er i bilen og på vei for henting. Gjennom dagen har begge foreldrene fått beskjeder og bilder av minstemann på mobilen. I tillegg har minstejenta sensor i utetøyet sitt, slik at foreldrene kan se at det har vært høyt aktivitetsnivå hele dagen. Mobilappen viser dette. Ettermiddagens besøk i matvareforretningen betales med mobilen via en installert betalingstjeneste.

Om ettermiddagen

En telefonoppringning mottas fra en person som presenterer seg fra Microsoft. Vedkommende påstår at familiens PC er infisert av virus. Samtales brytes, da familien har blitt advart om svindelforsøk av denne typen fra NorSIS. Minstejenta i huset har fått interaktiv dukke og snakker med denne. Dukken kan besvare enkle spørsmål og ”samtalene” blir lagret på produsentens server i utlandet.

Om kvelden

En nyskilt tante ringer og er fortvilet over en opprettet dating-profil hun ikke får slettet. Hun tipses om å ringe Slettmeg for å få veiledning. Husets tenåring har lagt ut film på internett og må trøstes da de anonyme kommentarene er hatske og spottende. Dagligvarer til resten av uka bestilles via nettet og blir tilkjørt av butikken. Kveldens TV-titting skjer via film-delingstjeneste. Tjenesten kommer med forslag til filmer som er i samme sjargong man har sett på tidligere. Familiens medlemmer har hver sine mapper for best mulig tilpasning.

Nettkriminalitet - hva er truslene

Utfordringene forbundet med cyber-sikkerhet synes å ligge i grense-snittet mellom oss mennesker og teknologien. Skal vi holde tritt med datakriminaliteten må vi bli minst like gode som de kriminelle til å forstå menneskene som bruker internett. Det holder ikke lenger å anta at cyber-sikkerhet dreier seg kun om teknologi.

Datakriminalitet kostet Norge 19 milliarder kroner i 2014 viser Mørketallsundersøkelsen fra Datakrimutvalget. Det er grunn til å tro at tallet faktisk er så høyt når man ser at kun 13 % av de som ble utsatt for datakriminalitet anmeldte dette i 2015[19]. Anmeldelse alene vil ikke bidra til at datakriminalitet reduseres. Samfunnet som helhet må være rustet til å håndtere økt datakriminalitet i årene som kommer. Politiets rolle endres og det er viktig at kompetanse og ressurser blir tilført slik at dette blir ivaretatt.

Alle nettbaserte enheter med sårbar programvare kan utnyttes som redskap for kriminelle til data-angrep. Det er derfor viktig å oppdatere programvare, ikke bare til egen beskyttelse, men også som et bidrag i samfunnets beskyttelse mot kriminelle.

[19] *Politiets Innbyggerundersøkelse 2015*

Bilde: Nora Birgithe

Spionasje

Norge har virksomheter som er i toppsjiktet når det gjelder teknologiske løsninger og produkter. Informasjon om Norge som nasjon kan være interessant for andre statsmakter. Fremmede stater kan bruke sine etterretningstjenester på måter som kan undergrave eller svekke våre nasjonale interesser[20]. Informasjonen kan hentes via spionasjeprogrammer direkte rettet mot målet eller via tredje-parter som har tilknytning til målet. Cybervåpen benyttes aktivt og målbevisst i internasjonale konflikter.

Terrorisme

PST vurderer det som mulig at ekstreme islamister vil forsøke å gjennomføre terroraksjoner mot Norge i løpet av året som kommer. Dette kan være fysiske aksjoner eller det kan foregå via nettet. Frankrike har vært utsatt for nett-aksjoner i forbindelse med eller i etterkant av fysiske terroraksjoner. Ofte blir sårbarheter i systemer vilkårlige mål for slike handlinger og det kan ramme alle i samfunnet.

Aktivisme

Aktivister benytter nettet til å spre et politisk budskap og rekruttere sympatisører og medlemmer. Den meste kjente aktivistgruppen på nettet er Anonymous. De har blant annet erklært cyberkrig mot den Islamske stat (ISIL). Anonymous har samlet inn og rapportert Twitterkontoer de antar benyttes til rekruttering og planlegging av terror. De har også gjennomført tjenestenektangrep mot nettsteder de mistenker for å huse ISIL. Uskyldige har av Anonymous blitt hengt ut for å være ISIL sympatisører og uskyldige privatpersoner og uvitende bedrifter har fått stengt sine nettsteder. Anonymous jakter også på pedofile. De har utgitt seg for å være mindreårige, sanket inn og spredt informasjon om personer de antar er pedofile[21]. Det er umulig å forutsi hvem som er målet for aktivister. Aktivister kan ved feilgrep angripe eller navngi feil personer eller virksomheter, noe som kan være skadelidende for de som blir utpekt.

Vinningskriminalitet

Kriminelle på nettet har som formål å tjene penger på informasjon som er tilgjengelig på nettet. Informasjonen kan være åpen eller den kan stjeles via nettangrep. Utpressing og gisseltaking av data er metoder som har blitt mye benyttet den senere tid. En utvikling som kjennetegner kriminalitetsbildet på nettet er at denne typen kriminalitet er økende, mer målrettet og har større omfang og konsekvenser enn tidligere. Mennesket er et lettere mål for angrep enn via tek-

---

[20] *PST Trusselvurdering 2016*

[21] *http://www.nrk.no/sorlandet/xl/krigen-fra-gutterommet-1.12806737*

niske sikkerhetsløsninger. Industrispionasje og ID-tyveri skjer gjerne på bakgrunn av manuelle handlinger ved at offeret trykker på en lenke eller åpner vedlegg i e-post. Målrettede angrep mot ledere og ansatte med privilegerte rettigheter gir oftest størst gevinst og konsekvensene for virksomhetene vil bli større.

En tilbyder av tjenestenektangrep har gitt lokketilbud med tre minutters gratis tjenestenektangrep mot konkrete mål. Norske skoler har blitt rammet av dette.

Vandalisme

Vandalisme kan være målrettet eller vilkårlig. Angrep utføres fordi man tester egne ferdigheter på nettet, eller man ønsker å sabotere, gjøre hærverk eller stenge nettsider for moroskyld. Verktøyet er ondsinnet programvare som enkelt kan hentes på nettet eller bestilles for en «femtilapp». Flere skoler har vært utsatt for tjenestenektangrep av skoleelever.

Overgripere

Overgripere kan utnytte mulighetene som finnes i anonyme nettsteder. De kan utgi seg for å være ungdom eller barn og slik komme i kontakt med potensielle ofre. Barn og unge kan bli overtalt til å ta bilder og video av seg selv i intime situasjoner som overgriper får tilgang til. Materialet kan dermed distribueres i pedofile nettverk som eksisterer på det mørke nettet. Materialet kan også benyttes til å presse ofrene og deres familie for penger.

Hatefulle ytringer og krenkelser

Hatefulle ytringer kan være målrettet mot enkeltpersoner eller det kan være mot folkegrupper, politiske partier eller religioner. App-er gir skoleelever adgang til å mobbe medelever uten å tilkjennegi hvem som står bak. Ondsinnede kommentarer og krenkelser på nettet har økt i forbindelse med flyktningestrømmen i Europa.

Norsk senter for informasjonssikring er en uavhengig ekspert-organisasjon, som vier all sin innsats til å skape bevissthet om cyber truslene og til å spre kunnskap om effektive sikkerhetstiltak, god sikkerhetspraksis og trygge retningslinjer.

Vår målgruppe er norske virksomheter og innbyggere. Vi har et spesielt fokus på de små og mellomstore bedriftene, kommunene og hver og en som bor i Norge. Framtidig verdiskaping og velferd er avhengig av at vi lykkes med digitaliseringen både i offentlig sektor og i næringslivet. Innbyggernes evne til å forstå de digitale truslene er en forutsetning for at vi som nasjon skal kunne høste gevinstene og mulighetene digitaliseringen gir oss.

NorSIS er en samarbeidspartner og brobygger. Vi tilbyr kunnskap og opplæring. Vi organiserer konferanser og holder foredrag. For oss er det viktig at myndighetene forstår innbyggernes behov og at næringslivet og offentlige myndigheter samarbeider godt. NorSIS er også en pådriver. Når vi ser mangler eller nye muligheter så varsler vi de som kan gjøre noe med det. Vi ønsker dialog om utfordringene og tror at samarbeid bygger de beste løsningene.

Teknologivn. 22
Bygg A
2815 Gjøvik
Org.nr: 995 195 003

Telefon: 40 00 58 99
Nett: www.norsis.no
E-post: post@norsis.no

NorSIS
Norsk senter for informasjonssikring

slettmeg.no idtyveri.info sikkert.no nettvett.no