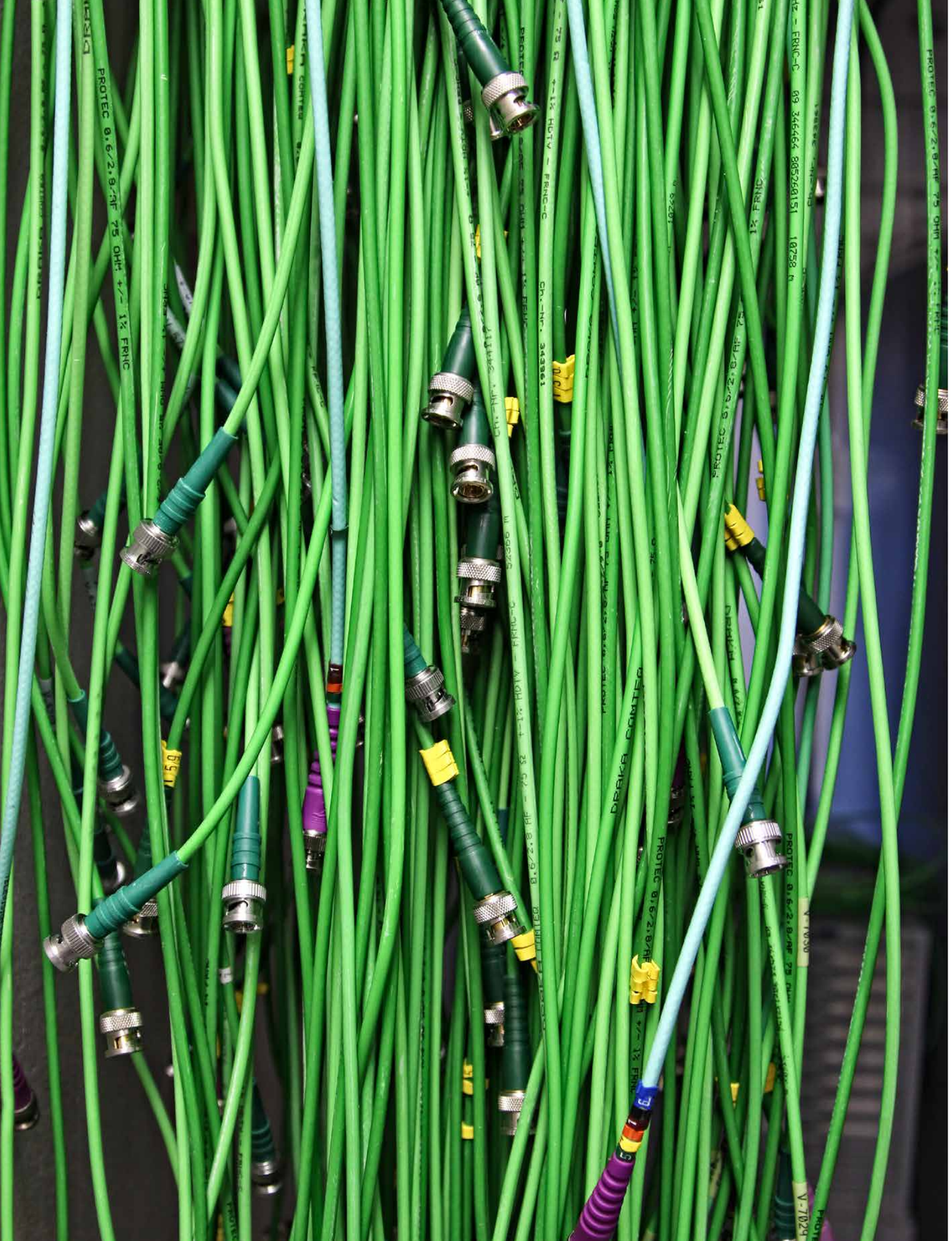
Et tryggere samfunn

Digital Sikkerhet 2017

telenor



Innhold

Innhold: Alle vurderinger, råd og fagkunnskap som presenteres i denne rapporten er en gjengivelse av kunnskap og erfaringer som Telenor Norge besitter, og da spesielt Telenor Norges sikkerhets-avdeling. Dette er et fagmiljø bestående av omtrent 50 rådgivere, analytikere og ingeniører med lang kompetanse og erfaring fra alle deler av sikkerhetsfaget. Avdelingen ledes av sikkerhetsdirektør Hanne Tangen Nilsen.
Trykkdato: 07.08.2017
Design: WergelandApenes/ Craft
Digital versjon: www.telenor.no/om/digital-sikkerhet

Ønsker du å komme i kontakt med oss?
Ønsker du å komme i kontakt med oss? Send en epost til caroline.lunde@telenor.com

Berit Svendsen
Konserndirektør i Telenor ASA
og adm.dir i Telenor Norge AS

> Denne rapporten skal bidra til større åpenhet rundt hva vi beskytter.

Et digitalisert samfunn er et tryggere samfunn

Vi er et av verdens mest digitaliserte samfunn, både på godt og vondt. Våre myndigheter, viktige samfunnsfunksjoner og hver enkelt av oss er avhengige av digitale tjenester. Tjenester og verktøy som forenkler kommunikasjon, arbeidsprosesser og tilgang til informasjon og kunnskap, men de kan også misbrukes til å utføre kriminalitet og aktivitet som truer staten Norge. Digitaliseringen har gjort cybersikkerhet til noe som angår oss alle.

> Vi eier og forvalter samfunnskritisk infrastruktur, som sammen med våre tjenester er kritiske for at samfunnet skal fungere. Det gir oss et betydelig samfunnsansvar.

For Telenor Norge er cybersikkerhet et strategisk kompetanse- og satsningsområde. Det er en kompetanse vi må ha, og evne å bruke.

Nesten 80 prosent av all datatrafikk i Norge går gjennom vår infrastruktur. Nasjonen Norge er avhengig av denne for å drifte alt fra vannforsyning, nødetater, økonomi, helse og strømforsyning, vi må være vårt ansvar bevisst.

Vi eier og forvalter samfunnskritisk infrastruktur, som sammen med våre tjenester er kritiske for at samfunnet skal fungere. Det gir oss et betydelig samfunnsansvar. Vi må beskytte og forsvare det vi eier og gjøre det motstandsdyktig for menneskelig feil og handlinger fra trusselaktører som har ulovlige hensikter.

Vi vet at det vi leverer er verdifullt for samfunnet, at vi må levere stabile og trygge tjenester og at vi er et mål for trusselaktørene. Trusselaktørene utvikler seg stadig. Det gjør at vi må bruke nye metoder både for å forebygge, detektere og håndtere hendelser i våre nett, systemer og tjenester.

Telenor Norge har de siste årene dedikert betydelige ressurser, mye oppmerksomhet og store investeringer på å forsterke vårt forsvar av den digitale samfunnskritiske infrastrukturen. Denne rapporten skal bidra til større åpenhet rundt hva vi beskytter nettverket mot, og hva vi mener skal til for å styrke beskyttelsen av Norges viktigste digitale nettverk i cyberspace.

I rapporten løftes det frem kunnskap som kan oppfattes som et noe dystert bilde av cyberspace. La meg derfor understreke at digitalisering skaper en bedre, tryggere og mer opplyst verden. Likevel må vi ta innover oss hvilke konsekvenser det har å flytte stadig flere samfunnskritiske og økonomiske verdier, i tillegg til personopplysninger, over i den digitale verden der stadig flere aktører forsøker å få uberettiget tilgang på systemer og informasjon.

Berit Svendsen

Hanne Tangen Nilsen
Sikkerhetsdirektør i Telenor Norge

Telenor Norge håndterer cyberangrep daglig.

Vi skal gjøre det vanskelig

Som eier av Norges viktigste digitale infrastruktur må vi ha solid kunnskap om hvilke utfordringer og trusselaktører som kan og vil påvirke den digitale sikkerheten. Denne innsikten deler vi med norske myndigheter, kunder og samarbeidspartnere. Gjennom denne rapporten ønsker vi å dele noe av vår kunnskap og tilnærming til sikkerhetsarbeid med flere.

Telenor Norge håndterer cyberangrep daglig; alt fra avanserte forsøk på spionasje, sosial manipulering og lammelse av tjenester til forsøk på innbrudd, tyveri og økonomisk bedrageri. I vår jobb med å designe, utvikle og operere Telenor Norges nett og tjenester skal vi gjøre det vanskelig for de som har uredelige hensikter å gjøre skade på vår infrastruktur, svindle, manipulere eller stjele informasjon.

> Myndigheter, kritiske samfunnsfunksjoner, infrastruktureiere, leverandører og enkeltmennesker har alle et ansvar for å sørge for et motstandsdyktig samfunn.

Som Berit nevner innledningsvis er cybersikkerhet en strategisk viktig kompetanse for oss. Det gjør jobben min som sikkerhetsansvarlig noe enklere. Ledelsens evne til å forstå sikkerhetsrisiko er avgjørende for hvordan god sikkerhetsledelse kan utøves. Å bygge kompetanse og forståelse tar tid. Kompetanse er nøkkelen til å endre holdninger og adferd. Derfor legger vi stor vekt på å bygge tilstrekkelig kompetanse i alle ledd av virksomheten.

Det krever også en tilnærming der risikostyring er en sentral del av virksomhetens styringsmodell, og hvor risiko og tiltak er noe som diskuteres, forankres og besluttes. Vi kan ikke redusere konsekvens til null, men et tydelig risikobilde gir ledelsen mulighet til å prioritere tiltak som reduserer handlingsrommet til trusselaktørene.

Myndigheter, kritiske samfunnsfunksjoner, infrastruktureiere, leverandører og enkeltmennesker har alle et ansvar for å sørge for et motstandsdyktig samfunn. Gjennom flere utvalg de senere årene, og nå senest *Stortingsmelding nr 38 (2016–2017) IKT-sikkerhet – Et felles ansvar*, setter myndighetene søkelyset på nødvendigheten av å styrke sikkerhetsarbeidet i alle ledd. Sett fra vår side er det mange gode tiltak som adresseres, spørsmålet vi allikevel tillater oss å stille er om myndighetene setter nok krefter bak sine tiltak. Det er fortsatt mange tiltak som skal utredes, vil vi reelt sett se handling fremover?

Tør myndighetene modernisere sin tilnærming til militært-sivilt samarbeid, herunder å gi private virksomheter en sentral rolle i Totalforsvaret? Når skal politiet får ansvaret for kriminalitet i cyberspace fra a til å - slik de har det i alle andre domener?

Rekken av spørsmål fra vår side er mange, mest av alt fordi dette engasjerer oss og fordi vi har et ansvar i fred, krise og krig. Vi leverer kritisk infrastruktur, og vi skal beskytte tjenester så vel som informasjon om enkeltindividers digitale liv. Vi er den som kan gjøre vår digitale infrastruktur motstandsdyktig, og vi er den som reelt sett håndterer hendelser når noe skjer.

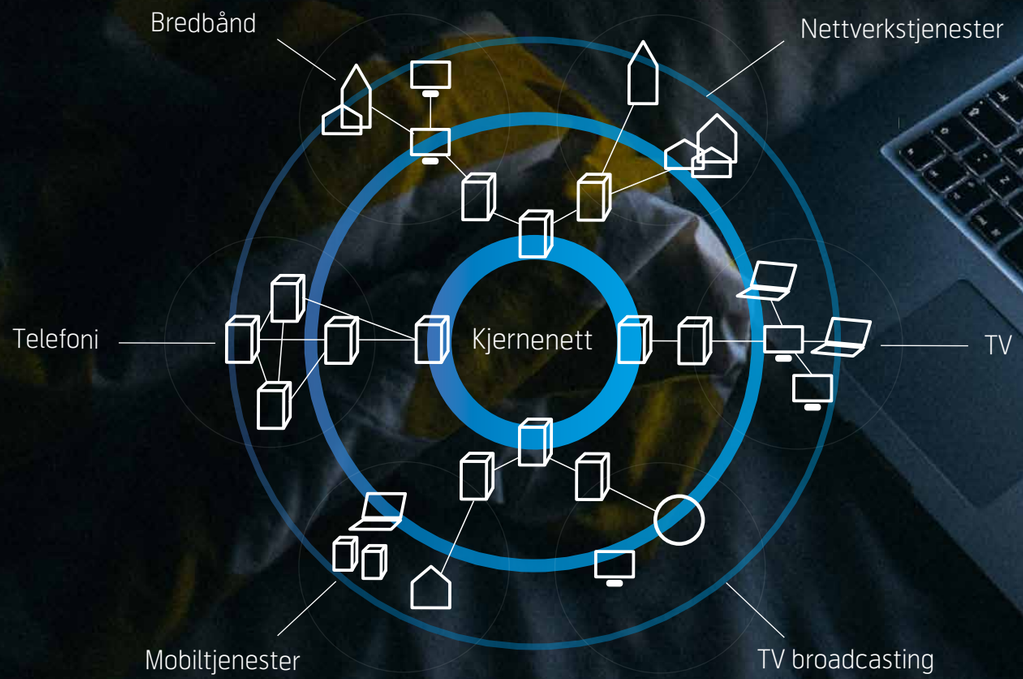
Heldigvis har vi i Norge (da denne rapporten gikk i trykken) ikke opplevd alvorlige cyberangrep som har slått ut samfunnskritiske funksjoner slik Ukraina opplevde da deler av strømforsyningen ble tatt ut i 2015, 2016 og 2017. Om det vil skje i Norge en dag kan ingen svare på, men vi må likevel være forberedt på det.

Norske myndigheter, infrastruktureiere og kritiske samfunnsaktører må ruste seg for å takle slike angrep, i fellesskap. Dette må vi jobbe sammen om. Det er vi alle tjent med.

Hanne Tangen Nilsen

Beskyttelse av det som er sårbart

> Den digitale revolusjonen har forandret samfunnet – og forventningene.



Digitaliseringen gjør det norske samfunnet tryggere, men samtidig sårbart på nye måter. Menneskelige og tekniske feil, så vel som bevisste handlinger utført av aktører som vil manipulere, paralysere eller på annen måte ramme samfunnet og borgerne, er noe vi må forholde oss til.

For mer enn 160 år siden kom telegrafen og der starter vår historie. Telekommunikasjon har revolusjonert nordmenns liv. Vi har en lang og stolt historie – men verden har forandret seg. Selv om målet vårt i all enkelhet fortsatt er det samme – sørge for at folk får kommunisert med hverandre – jobber vi under helt andre vilkår nå. Før var det risiko knyttet til manuelle operasjoner som bygging, montering, manuelle prosesser og pussing av kobberkabler i sentralen. Det var høyere toleranse for feil og lang rettetid. Samfunnet gikk rundt selv om man ikke fikk ringt.

Den digitale revolusjonen har forandret samfunnet – og forventningene. Digitalisering gjør samfunnet tryggere gjennom enklere tilgang til for eksempel varer og tjenester, transport, kunnskap, nyheter og helsetjenester. Samtidig setter det høyere krav til oppetid og rettetid, det skal ikke lange brudd til før det er krisestemning i norske hus og hytter – og enda verre; før samfunnskritiske funksjoner ikke virker.

Telenor Norges infrastruktur dekker hele Norgeskartet, og danner grunnlaget for at vi nordmenn har tilgang til et av verdens beste mobilnett, bredbånd, TV og telefonitjenester. Gjennom de siste 20 årene har vår infrastruktur vært gjennom store endringer. Hovedsakelig drevet av teknologiutviklingen som har gjort det mulig å levere TV, mobil og fasttelefoni over samme teknologi som internett. Det gjør oss som selskap mer effektive og robuste, men samtidig åpner det for nye sårbarheter som krever en helhetlig tilnærming til design og utvikling av styringssystemer, tjenesteproduksjon og den fysiske infrastrukturen.

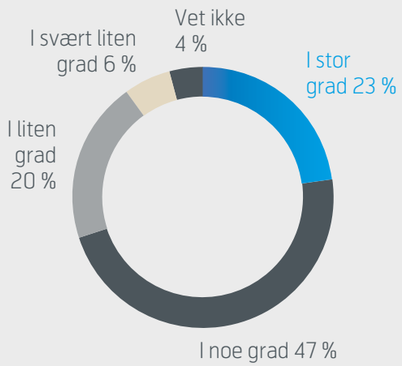
Bekymret
Norske myndigheter har uttrykt bekymring for samfunnets avhengighet til vår infrastruktur og har besluttet et pilotprogram som skal se på muligheten for en alternativ infrastruktur til Telenor Norges. Pilotprogrammet skal se på hvordan man gjennom markedsmekanismer kan drive sikkerhetsforståelsen til kritiske virksomheter og derigjennom bygge en alternativ infrastruktur eller mer robust infrastruktur. Vi vil delta og aktivt søke å adressere de tiltak som vi mener vil gjøre det norske samfunnet mer robust.

Mens dette arbeidet pågår, vil vi fortsette å sikre vår infrastruktur, vi vil fortsette å jobbe for at vi kan håndtere enhver hendelse. Dette gjør vi blant annet gjennom å ha en aktiv tilnærming til krise og beredskap. Vi er en beredskapsaktør som må kunne snu oss raskt når noe skjer, og vår bruk av kriseledelse som ledelsesverktøy er en viktig del av vår beredskap. Vi trener og øver jevnlig og er slik sett ganske lik nødetatene og Forsvaret og vi er aldri kun i en normalsituasjon.

Komplekse omgivelser påvirker oss
Globalisering, teknologiutvikling, endringer i lovverk og utvikling i trusselbildet påvirker oss som virksomhet på godt og vondt. Nye risikoer introduseres og det settes høyere krav og forventninger til at tjenestene vi leverer alltid skal virke.

Digital avhengighet gjør samfunnet sårbart på en ny måte. Samtidig må vi kunne stole på teknologien for at vi skal føle oss trygge. Utviklingen av nye digitale tjenester skjer raskt, og da må myndighetenes og næringslivets investeringer i kompetanse og evne til beskyttelse, følge teknologiutviklingen proporsjonalt.

70 prosent sier de i stor eller i noen grad er bekymret for at norske samfunns-kritiske funksjoner skal kunne slåes ut av et cyberangrep.

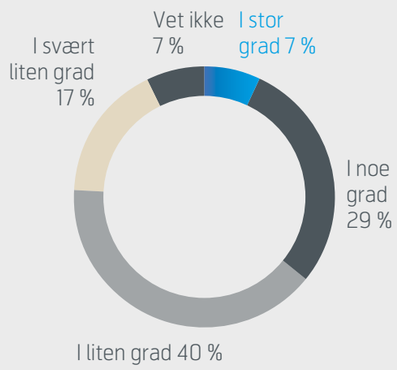


I en undersøkelse analysebyrået Kantar har gjennomført for Telenor Norge, svarer 70 prosent at de er bekymret for at norske samfunnskritiske funksjoner skal kunne slås ut av et cyberangrep. Vi tror at de siste årenes geopolitiske hendelser hvor internasjonal datakriminalitet har vært på agendaen, samt økt mediedekning og politisk fokus har bidratt til at folk i dag vet mer om cybertrusselen. Det er bra. Vi tar bekymringen på største alvor. Det skal ikke være lett å slå ut Telenor Norges infrastruktur.

Stortingsvalget
Telenor Norges undersøkelse viser også at mange begynner å se de svært alvorlige konsekvensene cyberoperasjoner kan få. Det potensielle skadeomfanget skaper bekymring, også sett opp mot det kommende valget i høst.

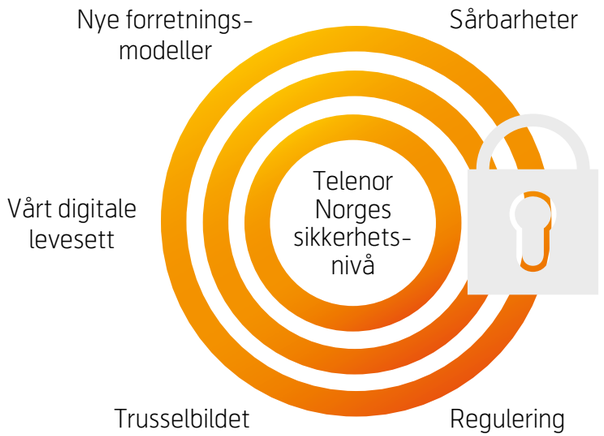
Mer enn én av tre nordmenn svarer at de i stor eller noe grad er bekymret for at den norske valgkampen skal bli manipulert via cyberspace.

36 prosent sier de i stor eller i noe grad er bekymret for at den norske valgkampen skal bli manipulert via cyberspace.



Spørreundersøkelsen er en landsrepresentativ undersøkelse gjennomført av analysebyrået Kantar TNS. Den nettbaserte undersøkelsen ble sendt til over 1000 respondenter i juni 2017.

Dette påvirker Telenor Norges sikkerhetsnivå



Telenor Norge tar høyde for sårbarheter, nye forretningsmodeller, vårt digitale levesett, trusselbildet og lovregulering når vi fastsetter vårt sikkerhetsnivå.

Det er mange faktorer som påvirker sikkerhetsnivået i Telenor Norge. De viktigste er:

1) Trusselbildet: Dette er i stadig endring og trusselaktørene får nye verktøy og metoder. Hvis en skal forstå hvordan man trues, må man først forstå hvem aktørene er, hvilke metoder de benytter, og hvilke mål de prioriterer å gå etter. Derfor utarbeider vi årlig vårt trusselbilde som brukes aktivt i risikostyring.

2) Sårbarheter: For å utøve god risikostyring må vi kjenne egne sårbarheter og svakheter. Logiske, fysiske og menneskelige svakheter kan utnyttes av trusselaktører, eller utløses av menneskelig svikt, tekniske feil eller miljøfaktorer. Dette er viktig innsikt på alle nivåer i organisasjonen. Alle i Telenor Norge er ansvarlig for å vurdere risiko innenfor sitt ansvarsområde.

3) Regulering: Myndighetene stiller krav til vårt sikkerhetsnivå gjennom lovkrav, som vi omsetter til sikkerhetskrav og prosedyrer som organisasjonen må forholde seg til. Dette påvirker oss organisatorisk og medfører både prosess- og systemendringer.

4) Nye forretningsmodeller: Vi leverer ikke telekommunikasjon alene. Vi er helt avhengige av internasjonale så vel som nasjonale leverandører. Vi sikrer at våre leverandører og entreprenører har god sikkerhetsstyring gjennom avtaler, krav og kontroller. I tillegg har vi samarbeidsarenaer for deling av kompetanse og utvikling av sikkerhets- og risikoforståelse. Våre leverandører må forstå Telenor Norges nasjonale rolle og derav vårt risikobilde.

5) Vårt digitale levesett: Vi, samfunnet og kundene tar i bruk ny teknologi, og gammel teknologi på nye måter. Forventningene til tilgjengelighet på digitale tjenester utvikler seg kontinuerlig og dette påvirker vår vurdering av risiko.

Tre ting er vi sikre på: Teknologi vil svikte, mennesker vil feile og ondsinnede aktører vil ønske å utnytte teknologi og mennesker til egen vinning. I vårt arbeid med risikostyring må vi legge dette til grunn og forberede organisasjonen på å håndtere hendelser, uavhengig av utløsende årsak.

Trussel-forståelse

Nesten daglig driver statlige aktører, kontraktører, organiserte kriminelle og politisk motiverte hackere, cyberoperasjoner mot eller i Telenor Norges infrastruktur og tjenester.

Telenor Norge anser ethvert forsøk på innbrudd i eller angrep på nett, tjenester, styringssystemer eller personell som en kriminell handling. Dette er helt uavhengig av om den som utfører handlingen er en enkeltkriminell eller en fremmed stat. Det er en etablert forståelse i vårt selskap om at selv de mest avanserte trusselaktørene nå driver cyberoperasjoner rettet mot samfunnskritisk infrastruktur.

Siden 2011 har vi arbeidet metodisk med selskapets egen trusselforståelse og eget trusselbilde. Det beskriver trusselaktørenes handlemåter, metoder og intensjoner, og benyttes som et vesentlig element i arbeidet med risikostyring.

Med utgangspunkt i de årlige trusselvurderingene fra Etterretningstjenesten (E) og Politiets Sikkerhetstjeneste (PST) bygges vårt trusselbilde. Vi må forstå hva myndighetenes vurderinger kan bety for oss, våre kunder og samfunnet.

I tillegg benyttes rapporter fra Kripos, Europol, de hemmelige tjenestene i Sverige, Danmark og Finland, og rapporter fra Nasjonal sikkerhetsmyndighet (NSM). På toppen av disse vurderingene legger vi vår kunnskap om svakheter og sårbarheter i egen infrastruktur, sammen med kunnskap om bransje, tjenester, samfunnets behov og endringer, informasjon fra åpne kilder, egne hendelser og dialog med ressurspersoner innen blant annet teknologi, geopolitikk og historie. Trusselvurderingene oppdateres minimum fire ganger årlig og produseres av et eget team i sikkerhetsavdelingen i Telenor Norge på oppdrag fra ledelsen.

Myndighetenes vurderinger

I 2017 er Etterretningstjenesten svært tydelige på at aggressiv og målrettet etterretningsvirksomhet pågår i Norge. I FOKUS 2017 står det blant annet:

«Russiske aktørar har i årevis freista trengje inn i datasystem som høyrer til norske styresmakter, og denne interessa vil halde fram. Ein annan kontinuerleg trussel mot norske verksemder er inntrenging og kompromittering for å etablere skjult infrastruktur med føremål å innhente informasjon. Også kinesiske aktørar har i 2016 gjennomført operasjonar mot norske styresmakter og teknologiselskap, og det er venta at kinesiske aktørar vil halde fram aktiviteten i 2017. Industrispionasje mot norske teknologiselskap vil framleis stå for ein betydeleg del av den forventa aktiviteten.»

PST peker i Trusselvurdering 2017 på kritisk infrastruktur:
«Norsk kritisk infrastruktur vil fortsatt være et utsatt etterretningsmål i 2017. Formålet med slike etterretningsoperasjoner vil både være å hente ut informasjon om selve infrastrukturen samt å legge til rette for å kunne manipulere data eller forberede sabotasje, dersom det oppstår en tilspisset utenriks- eller sikkerhetspolitisk situasjon. Systemer innenfor kraftsektoren og elektroniske kommunikasjonstjenester er å anse som spesielt etterretningsutsatt kritisk infrastruktur.»

Trusselaktørene

Figuren beskriver hierarkiet av trusselaktører: Høyere type entitet bruker sannsynlig underliggende nivåer som «service provider» der dette finnes formålstjenlig. Advanced Persistent Threat (APT) benyttes som begrep for å beskrive aktører som evner å drive sine operasjoner skjult og over tid med en tydelig intensjon og ønsket sluttsituasjon.

Målene som trusselaktørene ønsker å oppnå kan være:
- **Hindre bruk:** Gjøre tjenester utilgjengelige
- **Forme bruk:** Sørge for at tjenester bare virker når angriperen ønsker
- **Trenge inn:** Vise makt, tyveri av informasjon og/eller penger
- **Lekke stjålet informasjon:** Skade vårt eller kunders omdømme
- **Manipulere:** Påvirke mennesker og systemer for egen vinning eller senere operasjoner

Advanced Persistent Threat
På toppen av pyramiden er stater og kontraktører, ofte omtalt som Advanced Persistent Threat (APT), altså aktører som har kapasiteter og evne til å drive operasjoner skjult og over lang tid (i måneder og år). Slike aktører har tydelig intensjon og en vilje til å oppnå det de vil.

Kontraktører er oppdragsstyrt
De driver operasjoner som er betalt av andre etter spesifiserte oppdrag. De blir ofte omtalt som cyberverdens leiesoldater. De gjør oppdrag for stater (spionasje og sabotasje) og næringsvirksomhet (industrispionasje).

Organisert kriminalitet
Organisert kriminalitet i cyberspace er i ytterste konsekvens involvert i svært alvorlig kriminalitet slik som hvitvasking av penger fra narkotikaomsetning, menneskehandel og terrorfinansiering. I dette segmentet har nå enkelte av aktørene tilgang til både verktøy og metoder som tidligere bare har vært forbeholdt statlige aktører og kontraktører.

Hacktivisme
Dette er cyberkriminelle med en politisk intensjon, ofte omtalt som «hacktivister», og de angriper for å nå frem med sitt politiske budskap. Aktører av denne typen leter ofte etter svakheter som kan utnyttes for å få frem budskapet deres. Eksempler på dette har vært såkalt «defacing» av websider hvor innhold på nettsider blir endret.

Enkeltkriminelle og svindlere
Dette segmentet er kriminelle med en intensjon om å tjene penger til seg selv og i noen tilfeller å vise hvor dyktige de er for å få innpass høyere opp i hierarkiet.

Slik angriper de

Status Digital Sikkerhet 2017

Fra mai 2016 til mai 2017 håndterte Telenor Norge over 1800 forsøk på innbrudd på egne og kunders nettverk, og langt flere forsøk på å sabotere selskapets tjenester med tjenestenektangrep.

I takt med at stadig flere ting kobles til internett har også angriperne blitt stadig mer kompetente til å utnytte svakheter og sårbarheter i våre systemer, men det handler om mer enn teknologi. De menneskelige svakhetene er like viktige som de teknologiske når trusselaktørene går til digitalt angrep.

I Telenor Norges undersøkelse svarer nesten halvparten at de har blitt utsatt for «phishing», altså blitt forsøkt fralurt informasjon i privat sammenheng eller på jobb. 12 prosent har opplevd innbrudd i sin private e-post eller på private kontoer på sosiale nettverk. Fire prosent har blitt utsatt for løsepengevirus.

> I Telenor Norges undersøkelse svarer nesten halvparten at de har blitt utsatt for «phishing».

Krevende beskyttelse

Mange nordmenn synes det er krevende å beskytte seg mot kriminalitet i cyberspace. Mer enn 60 prosent av respondentene svarte at de syntes det i noe eller i stor grad er krevende å beskytte seg selv mot svindel og annen type kriminalitet. Det viser at denne typen kriminalitet er noe som angår oss alle, og vi er nødt til å bli mer kritiske til

Norsk senter for informasjonssikring (NorSIS) er en uavhengig organisasjon som arbeider for økt kunnskap om og forståelse for informasjonssikkerhet.

Kilde: norsis.no

henvendelser vi får digitalt, og hvordan vi passer på informasjon. Det dette viser er at denne type kriminalitet krever kompetanse og innsikt hos alle. Skal vi endre adferd og holdninger, må vi tilføres kompetanse. Fra vårt ståsted har NorSIS en viktig rolle i Norge i forhold til å formidle kunnskap om hva enkeltindividet kan gjøre selv.

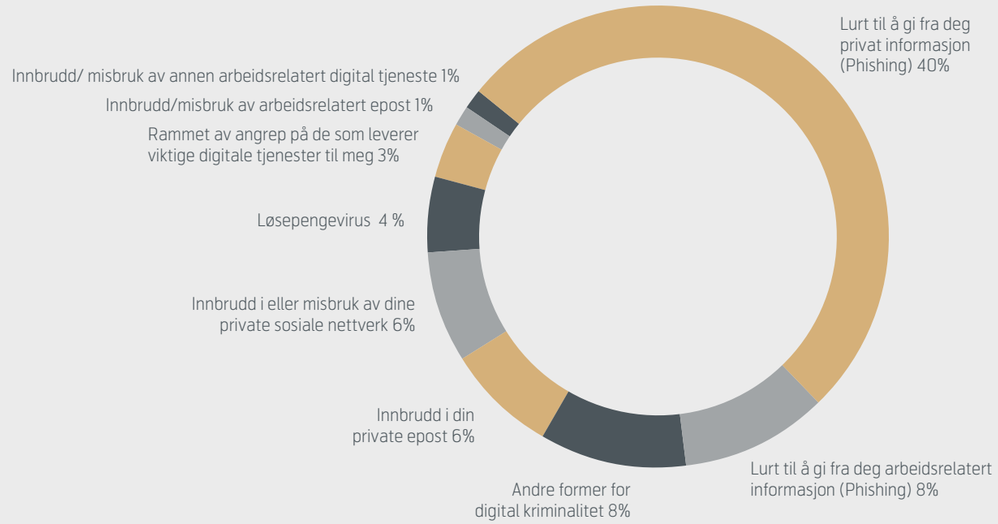
Som leverandør av meldingstjenester har Telenor et ansvar for å håndtere phishingangrep rettet mot våre kunder, og oppdage når tilgangen til våre tjenester har blitt kompromittert som følge av skadevare eller phishing. Det krever oppdatert kunnskap om trender og trusselbilde.

Telenors merkevare er attraktiv å misbruke for svindlere. Dette har vi sett eksempler på under kampanjer der det er sendt ut løsepengevirus forkledd som fakturaer fra Telenor. Vi må også forvente at vår posisjon som leverandør misbrukes av både statlige aktører, kontraktører og kriminelle med økonomisk motivasjon mot våre kunder i målrettede phishingkampanjer.

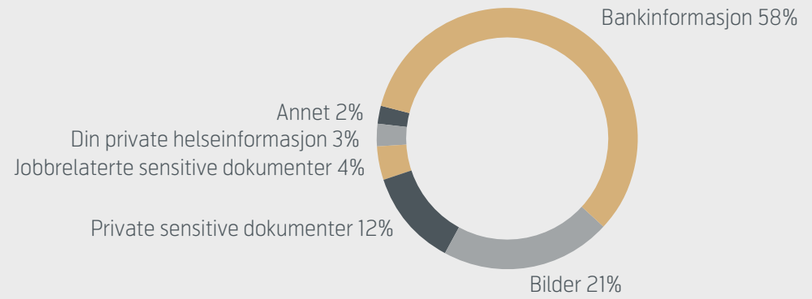
Vil ha varslingskanal

Vi jobber aktivt med håndtering av alle hendelser, og anmelder de store og viktige sakene til politiet. Omfanget av hendelser gjør det urealistisk å anmelde hver enkelt, også fordi mange hendelser i seg selv ser ut, for oss, å ha lite skadepotensiale. Det vi savner er en digital varslingskanal der vi og andre kan rapportere hendelser til politiet på en effektiv måte slik at politiet kan gjøre sine vurderinger om hendelser fra flere virksomheter og sette disse i sammenheng som en del av et større sakskompleks. For det vet jo ikke vi. Vi tror en slik løsning vil ha mye positivt ved seg, både for å få oversikt over omfang av hendelser, hyppighet og målgruppene det treffer, samt at politiet får et bedre bilde av hva som faktisk foregår av digitale kriminelle aktiviteter.

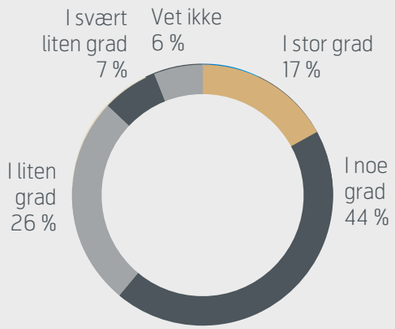
Har du blitt utsatt for eller forsøkt utsatt for noen av følgende?



Hva slags digital informasjon er du mest redd for å miste tilgangen til eller kontrollen på?



61 prosent synes det i noe eller i stor grad er krevende å beskytte seg mot ulike former for svindel og digital kriminalitet.



Ønsker tilgang

De aller fleste cyberoperasjoner benytter sosial manipulering, enten digitalt eller ved direkte menneskelig kontakt. Hensikten er uansett påvirkning. E-post er en yndet måte å gjøre det på, fordi det virker. De mest avanserte aktørene ønsker ikke å bruke ondsinnet kode, men vil skaffe seg tilganger ved å få ansatte til å gi fra seg påloggingsinformasjon og annen sensitiv jobbinformasjon. På denne måten ønsker slike aktører å kunne operere inne i virksomheters nett uten å bli oppdaget i lengst mulig tid.

> Vår vurdering er at det er grunn til å tro at vi vil se flere forsøk fremover.

Her er noen eksempler på sosial manipulering:

- Personer utgir seg for å være noen andre for å skape tillitt, som for eksempel driftsansvarlig, reparatør eller fra IT-avdeling.
- Noen spiller på frykt, av typen «Hvis du ikke fyller inn dette webskjemaet med kredittkortopplysninger eller brukernavn og passord, vil brukerprofilen eller mailkontoen din bli slettet.»

Vil tjene penger

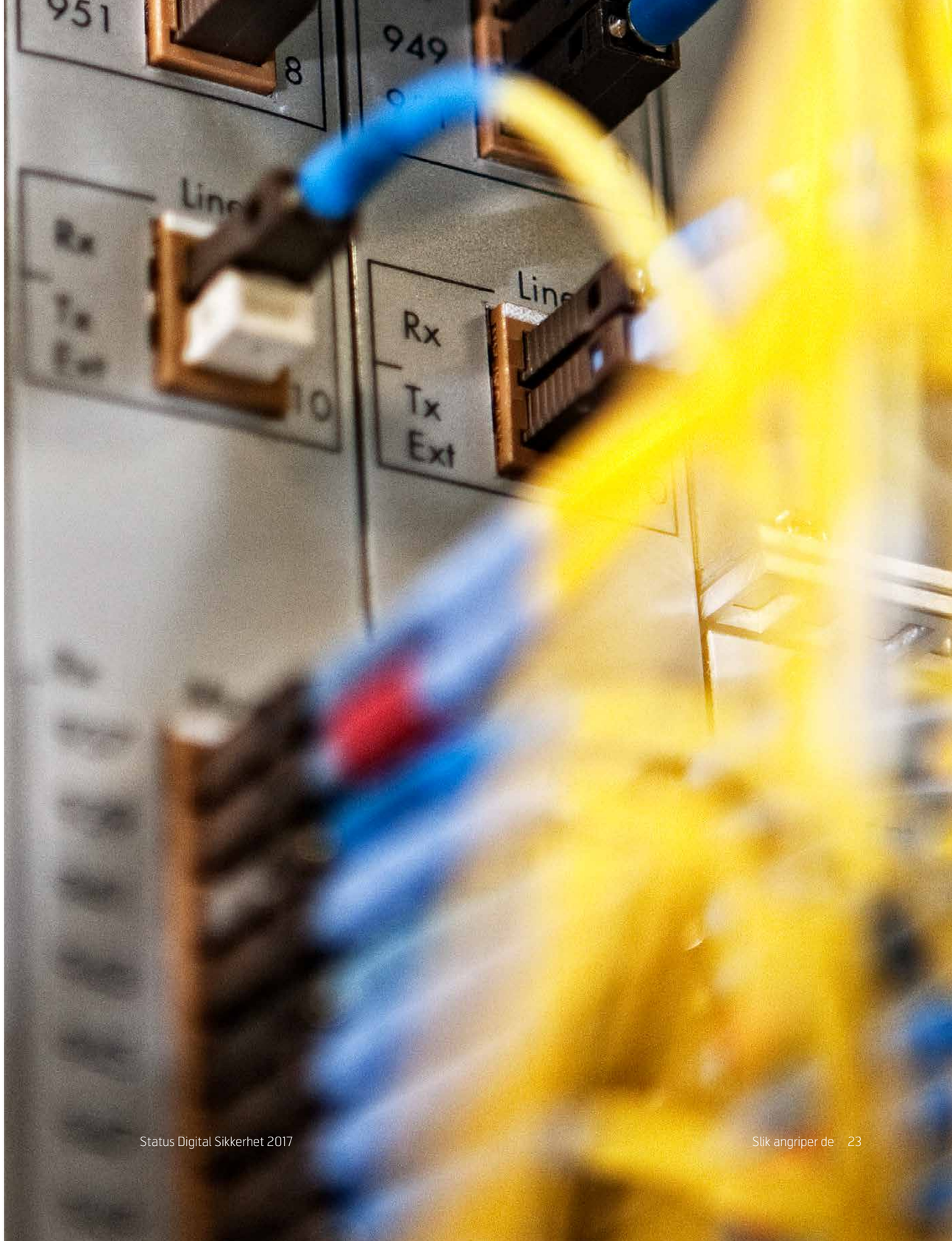
Når trusselaktørene har økonomisk vinning som mål er ransomware eller «løsepengevirus» en kjent metode. Du angripes gjerne via e-post med et infisert vedlegg, eller lurer deg til å klikke på en lenke som så fører til at du får servert en «cocktail» med ondsinnet kode som tar maskinen din som «gissel». Det vil si at alle dokumenter blir låst og utilgjengelig. Angriperen ønsker du skal betale for å få nøkkelen til å kunne låse opp igjen informasjonen din. Denne metoden har blitt mye brukt så langt i 2017.

I mai ble et større antall offentlige institusjoner og firmaer rammet av løsepengeviruset kalt «WannaCry», som spredde seg over hele verden. I Storbritannia ble blant annet mange helseforetak rammet. I Norge var spredningen heldigvis liten, og det ble kun meldt om et fåtall smittede maskiner. Skadevaren spredde seg som en orm fra maskin til maskin. Eldre versjoner av Windows uten de siste oppdateringene ble rammet.

WannaCry var forholdsvis amatørmessig laget, og manglet blant annet en god betalingsløsning. Både Nord-Korea og mindre dyktige cyberkriminelle aktører har vært lansert som mulige aktører bak angrepet. Teknikken for å spre skadevare har også endret seg jevnlig, for eksempel har det vært brukt filvedlegg i e-post, linker til nedlastning via Dropbox og Word-filer med makroer.

Hvis du skulle være uheldig å få dine data tatt som gissel er anbefalingen fra Telenor at du ikke betaler. Kriminelle holder sjelden hva de lover, og du har ingen garanti for at de virkelig har gått ut av systemet ditt. Samtidig vil enhver betaling bidra til videre kriminell virksomhet og at flere utsettes for liknende angrep. Kontakt heller IT-eksperter som kan bistå deg i å få informasjonen din tilbake. For å unngå større konsekvenser med løsepengevirus er det lurt å alltid ha oppdatert sikkerhetskopi av informasjon.

Som internettleverandør har Telenor Norge et ansvar for å redusere risikoen for spredning av skadevare i vårt nettverk, og gjøre det vi kan for å beskytte kundene fra å få utstyr infisert. I tillegg bistår vi bredbåndskunder som har fått infisert sine maskiner med skadevare, eller som har utstyr som er sårbart for misbrukes til skadevareangrep. Vi blokkerer også infrastruktur på internett som utelukkende benyttes til spredning av skadevare.



Mer direktørsvindel
Fra september 2016 opplever vi at flere kriminelle forsøker å lure til seg penger ved å svindle ledere og andre nøkkelpersoner som har myndighet til å utføre store utbetalinger i norske selskaper.

Direktørsvindel (også omtalt som CxO-svindel) er en metode der angriperen benytter sosial manipulering via e-post, ofte kombinert med telefonhenvendelse for å få utbetalt penger til seg selv. Telenors toppledere har også blitt utsatt for dette og trusselaktørene i slike saker er på jakt etter penger.

De som henvender seg har ofte gjort forundersøkelser som gjør at de har et språk og refererer til intern informasjon som får hele henvendelsen til å fremstå mer reell. I fjor ble et verdensomspennende norsk selskap forsøkt svindlet for 500 millioner norske kroner. De lyktes med å stoppe majoriteten av overføringen, men svindlerne slapp unna med over 100 millioner kroner.

Denne typen svindel har økt i omfang, og siden det er store penger å tjene her forventer vi at de kriminelle vil fortsette å bruke denne metoden også fremover. Vårt råd til virksomheter er å innføre krav om minimum to personers godkjenning før større pengeoverføringer kan gjennomføres.

Ønsker å lamme virksomheten
Tjenestenektangrep eller DDoS-angrep (Distributed Denial of Service) går ut på å lamme tilgangen til en nettside eller tjeneste, ofte ved å sende store mengder trafikk mot den. Tjenesten, for eksempel en nettbank, vil for kundene oppleves ikke å være tilgjengelig. Distributed betyr at angrepet skjer fra mange steder på Internett samtidig.

En utfordring er at det finnes tjenester der man enkelt kan betale for å få utført angrep til en billig penge. De som kjøper tjenestene er alt fra gutteroms-hackere til profesjonelle aktører. De har ulike hensikter, som hærverk og utpressing med trusler om slike angrep, dersom man ikke betaler.

I fjor høst så vi det første store DDoS-angrepet som ble utført ved hjelp av tingenes internett. Da ble den amerikanske nettleverandøren Dyn rammet av et DDoS-angrep fra et stort nettverk som har fått navnet Mirai. Angrepet førte til at nettsidene til en rekke store selskaper var utilgjengelig, deriblant Twitter, Spotify, Netflix og PayPal.

Hackede webkameraer fra det kinesiske firmaet Xiongmai var ett av systemene som ble brukt i disse DDoS-angrepene. Kameraene leveres med standard brukernavn og passord og lar seg ikke oppgradere. Firmaet endte opp med å tilbakekalle kameraene sine i USA.

I perioden mai 2016 – mai 2017 ble det gjennomført over 8000 DDoS-angrep mot Telenor Norge og virksomheter som kjøper sikkerhetstjenester av Telenor Norge. Telenor Norges sikkerhetssenter (Telenor Security Operations Centre – TSOC) er selskapets førstelinje mot cyberangrep. De håndterer hundrevis av tjenestenekt-angrep hver eneste måned.

Omtrent en tredjedel av angrepene var så store at Telenor Norges sikkerhetssenter måtte gjøre tiltak for at angrepene ikke skulle påvirke Telenor Norges eller våre kunders tjenester. Det største angrepet var på over 277 gigabits per sekund (Gbps) og varte i én time. Slike trafikkmengder kan ta ned enhver virksomhet i Norge. Vårt mål er at slik uønsket trafikk aldri skal treffe våre kunder. Vi bygger derfor ut vår evne til håndtering av denne type hendelser fortløpende.

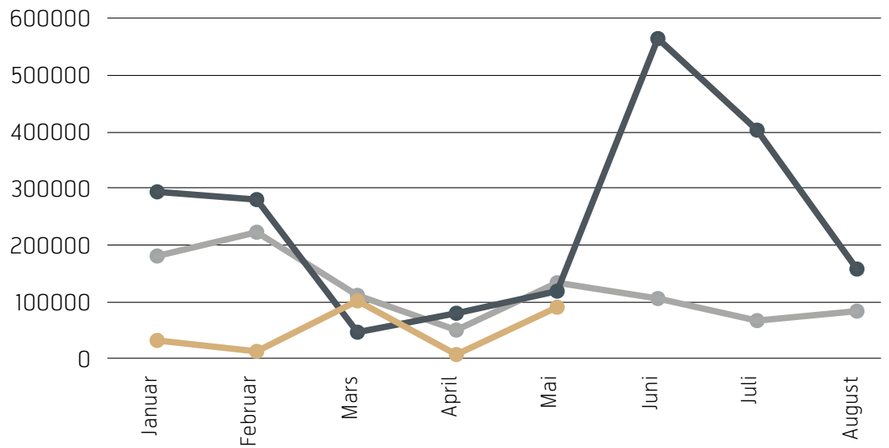
Telefonsvindel
Telefonsvindlere ringer ofte fra utenlandske nummer, og legger på med en gang det svares. Det kan være et tilfelle av et såkalt "wangiri"-anrop. Selve ordet "Wangiri" betyr "One and cut". Denne formen for svindel går ut på å få offeret til å ringe tilbake. Svindlere bruker en datamaskin som kan ringe opp flere tusen numre i minuttet, og lar det ringe kun en gang før samtalen automatisk avbrytes. Dette gjør at mottakeren får et tapt anrop på telefonen sin. Målet er å vekke nysgjerrighet og at offeret ringer tilbake for å finne ut av hvem som ringte. Det er da svindlerne tjener penger fordi nummeret som det ringes til er forskjellige typer teletorgnumre, med skyhøye takster.

Vi jobber løpende med å beskytte våre kunder mot de verste formene for One-ring, og redusere mulige tap for dem. Ringer våre kunder til et utenlandsnummer som er tilknyttet en teletorgløsning betaler kunden kun utenlandstaksten som er forhåndsdefinert, men det kan naturligvis fortsatt bli dyrt.

Vårt råd er; ikke ring tilbake når ukjente utenlandske numre har ringt deg. Det er for øvrig en myte at det kan takseres for innkommende anrop på mobilen. Så lenge kundene befinner seg i Norge vil man aldri bli belastet for innkommende anrop.

Sperrer anrop fra svindlere
Kriminelle som forsøker å fiske ut informasjon eller svindle til seg penger via telefonen, er fortsatt en utfordring. Selv om nordmenn generelt har blitt mer skeptiske til mistenkelige telefonoppringninger vil kriminelle fortsatt benytte metoden så lenge den er lønnsom. Telenor Norge har et anropsfilter som kan hindre at anrop fra verifiserte svindlere kommer gjennom vårt nettverk. Vi oppdaterer filteret løpende og straks vi blir klar over nye numre i omløp.

Antall sperrede anrop



2015
Totalt sperrede anrop 1.634.963

2016
Totalt sperrede anrop 2.417.336

2017
Totalt sperrede anrop 228.275

Teknologi som driver endring

Det tok over 75 år for fasttelefonen å nå 50 millioner kunder. For mobiltelefonen tok det 16 år, mens Facebook brukte litt over 4 år. Nå tar det kun dager før en ny digital tjeneste er spredd internasjonalt. Når alt skal på nett vil det også påvirke risikobildet vårt.

Den fjerde industrielle revolusjonen gir samfunnet store muligheter. Varer og tjenester kan lages og leveres med automatiserte prosesser, offentlig sektor kan effektiviseres, og velferdstilbudet forbedres. Behovet for økt bevissthet om hvilke sikkerhetsutfordringer som ligger i disse endringene er noe vi alle må ta inn over oss. Innovasjon omfatter å ta risiko, men risiko må også tas med utgangspunkt i forståelse av både svakheter og trusler.

Stordata
Telenor har over 7000 basestasjoner i Norge. Disse samler inn enorme mengder data fra trafikken i mobilnettet. Disse stordataene kan gi verdifull innsikt og analyser som aldri tidligere har vært mulig. Både politi, helsevesen, statlige etater, kommuner og private virksomheter vil dra nytte av innsikt fra stordata.

> Både politi, helsevesen, statlige etater, kommuner og private virksomheter vil dra nytte av innsikt fra stordata.

I 2016 begynte forskningsavdelingen i Telenor å dele mobilitetsdata for forskningsformål. Disse dataene inneholder ikke personopplysninger som kan identifisere enkeltindivider, men består av store mengder datamateriale fra basestasjonene som er anonymisert og slått sammen.

Datagrunnlaget fra aggregerte aktiviteter i mobilnettet er enormt. Etter hvert som vi har utforsket og gravd dypere i datamaterialet, finner vi stadig frem til nye bruksmuligheter som vi tror både offentlig og privat næringsliv vil ha stor nytte av å bruke for egen virksomhets analyser og planlegging. Vi planlegger å bruke stordataene i kommersielle produkter. Da vil eventuelle personopplysninger være anonymiserte og det er ikke mulig å identifisere individer eller enkelte mobiltelefoner ut fra de aggregerte resultatene.

Sterkere rett til egne personopplysninger
En personopplysning er en informasjon eller vurdering som kan knyttes til deg som enkeltperson, slik som for eksempel navn, adresse, telefonnummer, e-postadresse, bilnummer, bilder, fingeravtrykk, irismønster, hodeform (for ansiktsgjenkjenning) og fødselsnummer (både fødselsdato og personnummer).

I 2018 vil en ny personvernlovgivning tre i kraft i EU og EØS. General Data Protection Regulation (GDPR) erstatter eksisterende lovverk fra 1995 som oppleves som utdatert på flere områder og som ikke dekker godt nok opp hvordan data blir samlet inn, oppbevart og prosessert i vår digitale tidsalder.

Den nye lovgivningen vil ha stor innvirkning på den norske personvernloven og styrker enkeltpersoners personvern og kontroll over brukerdata. Samtidig vil det nye lovverket gi nye plikter til både private virksomheter og offentlige aktører som samler inn, lagrer og prosesserer personopplysninger for ansatte eller kunder.

Dette betyr de nye personvernreglene for private og offentlige organisasjoner:

1. Alle norske virksomheter får nye plikter
2. Alle skal gi god informasjon om hvordan de behandler personopplysninger
3. Alle skal vurdere risiko og personvernkonsekvenser
4. Alle skal bygge personvern inn i nye løsninger (Privacy by Design)
5. Mange virksomheter må opprette personvernombud (Telenor Norge har personvernombud)
6. Reglene gjelder også virksomheter utenfor Europa
7. Alle databehandlere får nye plikter
8. Alle får nye krav til avvikshåndtering
9. Alle må kunne oppfylle borgernes nye rettigheter

(Kilde: Datatilsynet)

Personvern som prioritet
Et sterkt personvern har alltid høy prioritet i Telenor Norge, og arbeidet for å sikre at den nye reguleringen blir ivaretatt er satt til en egen prosjektgruppe. Prosjektet skal ivareta disse områdene:

- Sørge for at alle våre produkter, tjenester, prosesser og IT-systemer håndterer personvern på en korrekt måte.
- Innføre "privacy by design" for å sikre at alle nye eller endrede produkter og tjenester håndterer personvern på en korrekt måte.
- Oppdatere eksisterende og innføre nye prosesser som overvåker og kontrollerer at Telenor Norge følger retningslinjer, lover og forskrifter for personvern.
- Opplæring av ansatte i riktig håndtering av personopplysninger.

Databeskyttelse og personopplysninger
Personvern dreier seg om ivaretakelsen av personlig integritet, enkeltindividers rett til privatliv, selvbestemmelse, selvutfoldelse og håndtering av personopplysninger. Digitale tjenesteleverandører sitter på enorme mengder informasjon om sine brukere, og brukerne deler informasjon som aldri før.

En av de nyere utfordringene for personvernet er at vi legger igjen mange digitale spor. Ny lovgivning som gjelder fra mai 2018 vil i større grad enn tidligere gi deg mulighet til å ha et aktivt forhold til hvordan dine personlige opplysninger blir brukt i tjenesteproduksjon.

Telenor Norge har store mengder personopplysninger om våre kunder. Det er snakk om telefonnummer, adresser, e-postadresser, adferdsmønster og bevegelsesmønster, bare for å nevne noe. Telenor Norge har konsesjon for innsamling, behandling og lagring av spesifikke type opplysninger til begrensede og spesifikke formål. Enhver ny eller endring i innsamling, behandling, lagring eller sletting av data må begrunnes i konsesjon eller i personvernlovgivningen.

Personopplysninger skal ikke komme på avveie, men dersom det skjer har Telenor Norge et ufravikelig krav om å varsle Datatilsynet.

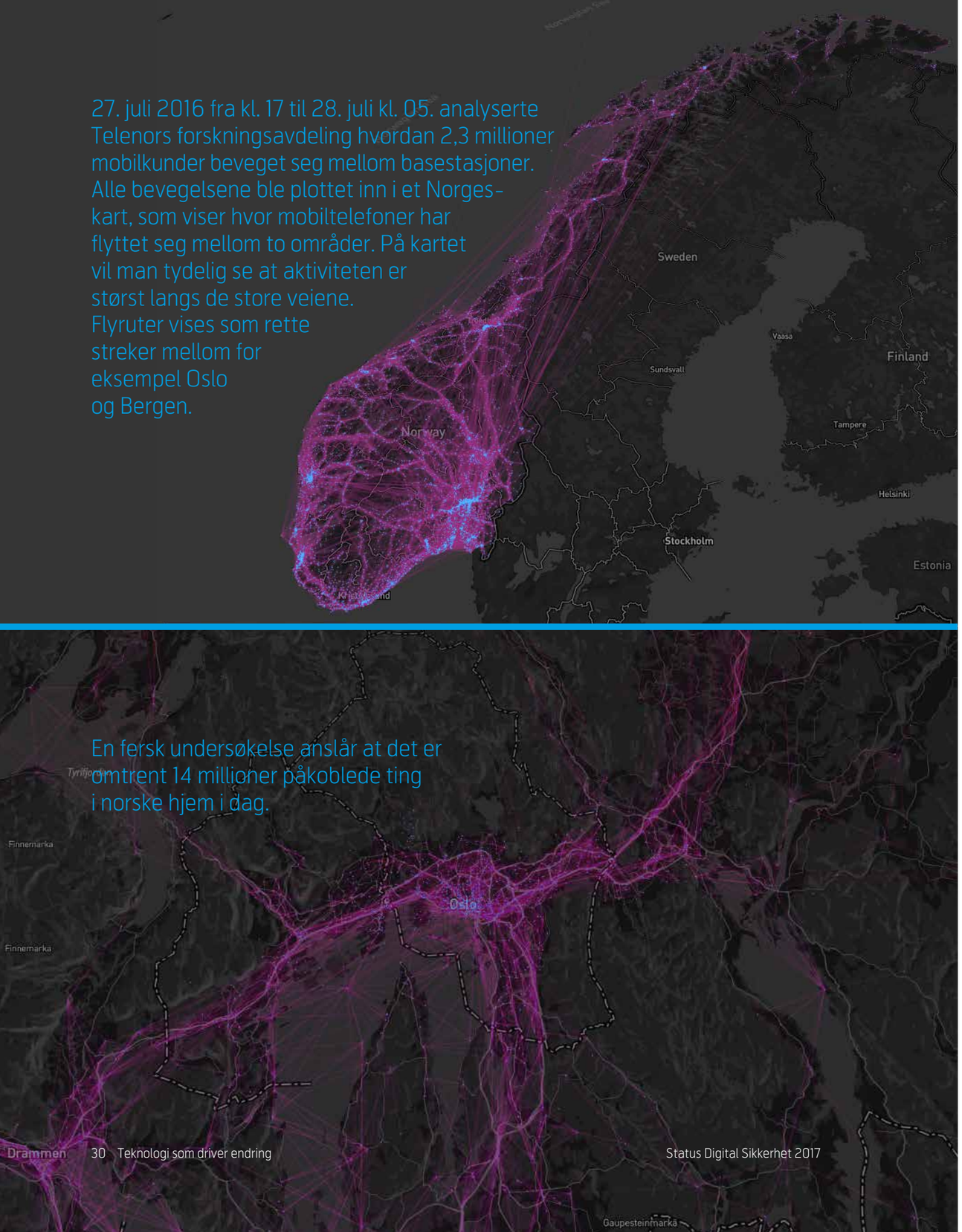
Utlevering av data til norske myndigheter
Alle Norges telekomselskaper utleverer kundedata til Politiet dersom det foreligger rettslig kjennelse eller Politiet påberoper seg nødrett. Hvert år rapporterer Telenorkonsernet tall fra antall utleveringer til lokale myndigheter i alle de landene selskapet opererer.

I Norge er det kun Politiet og Politiets sikkerhetstjeneste som kan gjennomføre avlyttinger av kommunikasjon for å etterforske alvorlig kriminalitet eller saker relatert til nasjonal sikkerhet. Slike operasjoner har Politiet og PST kun tillatelse til etter en rettslig kjennelse.

I 2016 mottok Telenor 7679 anmodninger om utlevering av historiske trafikkdata (metadata), signaleringsdata, terminaldata, bruk av IP-adresser, abonnementsinformasjon og kundeinformasjon. Tallet er en sum av ulike typer anmodninger.

I 2016 mottok Telenor 432 anmodninger om kommunikasjonskontroll og 667 anmodninger hvor hjemmel om nødrett er benyttet. Dette er antall anmodninger Telenor Norge har mottatt fra myndighetene og viser ikke antall berørte enkeltnummer.

27. juli 2016 fra kl. 17 til 28. juli kl. 05. analyserte Telenors forskningsavdeling hvordan 2,3 millioner mobilkunder beveget seg mellom basestasjoner. Alle bevegelsene ble plottet inn i et Norges-kart, som viser hvor mobiltelefoner har flyttet seg mellom to områder. På kartet vil man tydelig se at aktiviteten er størst langs de store veiene. Flyruter vises som rette streker mellom for eksempel Oslo og Bergen.



En fersk undersøkelse anslår at det er omtrent 14 millioner påkoblede ting i norske hjem i dag.

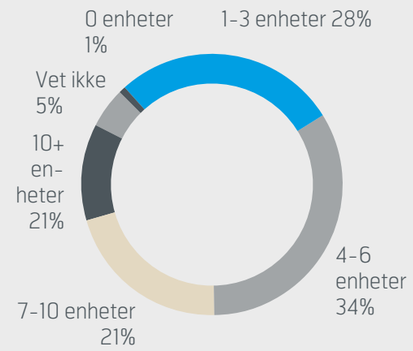
Tingenes internett
Smarte byer, tilkoblede ting, roboter og styring ved hjelp av kunstig intelligens er løsninger for fremtiden. Verdipotensialet antas å være betydelig; samfunnet vil spares for store summer fordi vi automatiserer og endrer hvordan jobber blir utført.

De som har besvart vår undersøkelse har i gjennomsnitt seks påkoblede enheter i hver husholdning. Hvis en legger Statistisk Sentralbyrå (SSB) sine tall på antall husholdninger til grunn, kan man lage et grovt anslag på totalt 14 millioner PCer, mobiltelefoner, treningsklokker, varmeovner, webkameraer, værstasjoner, husalarmer biler og annet som sender informasjon over internett her og nå.

Tingenes internett er et begrep som favner svært vidt, og det kan være alle mulige gjenstander, alt fra leketøy til droner. Det er i utgangspunktet ikke en ting som ikke kan kobles på internett. Selv enkeltindivider kan i dag kobles til internett via en pacemaker.

Tingenes internett bringer mange nye utfordringer, men aktualiserer dessverre også mange kjente utfordringer i ny kontekst.

Hvor mange ting har du koblet på nettet i din husholdning?



Seks sikkerhetsutfordringer rundt Tingenes internett

1. Dårlig sikkerhet
Det er mange aktører i denne bransjen som er flinke til å lage leketøy, biler eller kameraer, men som historisk sett ikke har trengt å ha særlig kompetanse på cybersikkerhet.

2. Misbruk
Kriminelle tenker utenfor boksen, og ser hvordan «tingen» kan utgjøre en trussel utenfor bruksområdet den er laget for. Det vanligste akkurat nå er at sårbare ting utnyttes til å lage botnet. De kan også brukes til å bryte seg inn i datanettverket på norske arbeidsplasser når tilsynelatende harmløse konsumentprodukter tas med på jobb og blir koblet til nettet. Da blir den nyttige dingsen et springbrett for å kompromittere bedriften og dens IT-systemer, for eksempel til å drive industrispionasje.

3. Produsenten av tingen har blitt et IT-selskap
«Tingene» blir ofte laget av tradisjonelle produksjonsbedrifter. Dette er selskaper som aldri har hatt høy IT-ekspertise, men produserer biler, leketøy eller kjøkkenutstyr. Disse selskapene har av naturlige årsaker ikke alltid har et våkent forhold til cybersikkerhet, fordi de aldri har drevet med IT tidligere – og ofte fortsatt ikke har forstått hva det innebærer at de nå gjør det.

4. Få incentiver
Ved fremveksten av IoT-baserte botnet har det blitt svært tydelig at det i tillegg til kunnskap og teknisk instrumentering for sikkerhet, også mangler incentiver og ansvarsplassering.

Eierne av IP-kameraer og videoopptakere som er innrullert i et botnet og misbrukes til DDoS-angrep, er ikke selv klar over at de har et problem, og produsentene har begrenset motivasjon for å foreta seg noe.

5. Sikkerhetsovervåkning
Fordi preventiv sikring ikke er nok, blir sikkerhetsovervåkning helt sentralt. Du må forvente at endepunkter i et nettverk, som tingene jo er, kan bli kompromittert, og bygge sikkerhetsovervåkning for å avdekke det. Trafikkovervåkning er særlig sentralt, da mange «ting» i seg selv har begrenset instrumentering for overvåkning.

6. Overeksponering til internett
Internett er overalt, og det er både enkelt og billig å etablere en kobling ved å eksponere tingen direkte til internett, men ikke alle ting bør eksponeres direkte til internett eller kommunisere i samme trafikkplan som «alt annet». Både segmentering og minimering av angrepsflate er veletablerte sikkerhetsprinsipper som vi også bør følge for IoT.

Det er mange sikkerhetsutfordring knyttet til tingenes internett, men det er ett ledd i verdikjeden som kan kontrolleres, og som automatisk vil gi bedre sikkerhet: En trygg og god kommunikasjonskanal.

I år kommer det to nye kommunikasjonsstandarder i 4G-nettet, som er bygget for IoT. Mobilnettbasert kommunikasjonskanal muliggjør både mindre eksponering til internett og bedre segregering av kommunikasjonen.

Botnet
Datamaskiner, nettbrett, smarttelefoner og «ting» kan bli kapret og bli en del av et botnet. Et botnett er et nettverk av datamaskiner infisert av datavirus eller trojanske hester. Disse maskinene kobler seg til en eller flere sentrale styrende noder der de får tildelt oppgaver.

Slik beskytter vi oss

For å være forberedt på å møte et stadig mer avansert trusselbildet investerer Telenor tungt i design, utvikling og drift av våre løsninger. I tillegg investerer vi i bedre evne til å forutse, oppdage og håndtere hendelser.

Telenor Norge er en beredskapsorganisasjon hvor driftssikkerhet og informasjonssikkerhet er en prioritet. Vi leverer tjenester i en tryggest mulig infrastruktur og bygger vår infrastruktur og tjenester slik at en eventuell hendelse skal ha begrenset skadeomfang. Vi har som mål å oppdage hendelser så tidlig som mulig og samtidig sørge for en effektiv håndtering av dem.

Risikostyring og sikkerhetsstyring er en del av våre virksomhetsprinsipper. Vi vurderer risiko i prosjekter, i prosesser og på alle ledelsesnivåer. Sikkerhetsstyring kommer i tillegg med tydelige krav og prosedyrer som organisasjonen skal forholde seg til.

> Risikostyring og sikkerhets-styring er en del av våre virksomhetsprinsipper. Vi vurderer risiko i pro-sjekter, i prosesser og på alle ledelsesnivåer.

En meget sentral del av vår styringsmodell er kravene til sikkerhetsarkitektur. Dette er prosedyrer som gir føringer for hvordan de forskjellige infrastrukturene for mobil, fastnett, datasenter, IT og sluttbruker, og systemene som produserer tjenester i dem, skal designes og implementeres. I all hovedsak kan føringene oppsummeres ved at alle som bygger nye eller fornyer eksisterende systemer og infrastruktur må:

1) Forstå hva som kan og skal eksponeres (informasjon, funksjoner, grensesnitt), til hvem, og hvordan
2) Etablere tilstrekkelige logiske og fysiske skiller, samt redusere avhengigheter på tvers
3) Sikre at tilstrekkelig sikkerhetsovervåkning er til stede – både som en del av infrastrukturen og i systemene som produserer og støtter tjenestene (f.eks. drift, overvåkning, tilgang).

Dette er en idealrepresentasjon av kravene, og vil ikke alltid passe med virkeligheten. Derfor har vi sikkerhetsarkitekter som bistår prosjekter, linjeorganisasjon og systemområder for å kvalitetssikre at design og implementasjon fører til så få avvik som mulig, og at eventuelle avvik håndteres i henhold til våre retningslinjer.

Vi beskytter infrastrukturen og kommunikasjonstjenestene våre, mens det en kunde har «i eget hus» utover dette må de selv beskytte. Vi leverer robust og trygg kommunikasjon, men hva slags passord som brukes, hva som kobles til nettverket og hvordan det brukes, påvirker også kundenes sikkerhet, og er den enkeltes ansvar.

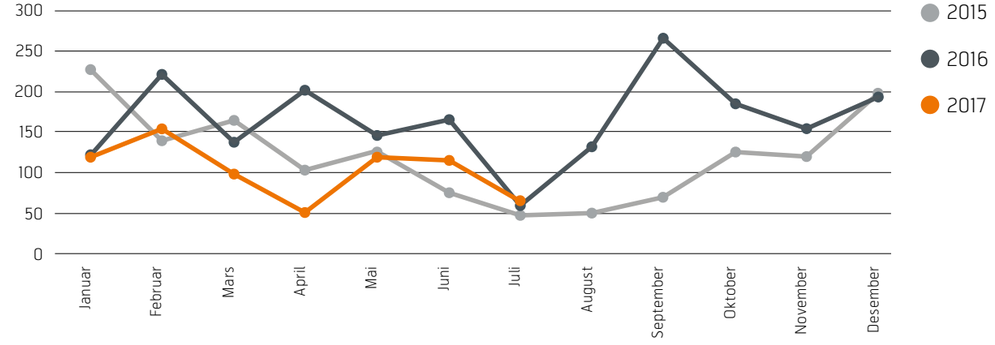
Slik oppdager vi angrep

Det er umulig å være hundre prosent beskyttet mot et nettverksangrep eller innbrudd. Derfor er det viktig å være i stand til å oppdage og begrense skadene et angrep kan skape.

Hvert år håndterer vårt sikkerhetssenter (TSOC) et tusentalls alvorlige hendelser. Dette er hendelser som har potensiale til å gjøre skade. I tillegg beskytter de mot tjenestenektangrep. Vi monitorerer både egen infrastruktur og leverer sikkerhetsovervåkning som tjeneste til bedriftskunder i inn- og utland.

Det skal være vanskelig for trusselaktører å trenge inn i, eller misbruke, våre tjenester og infrastruktur. Vi bygger våre kapabiliteter basert på lovkrav fra norske myndigheter, i tillegg til internasjonal god praksis og vår egen kunnskap og evne på området. Vi satser på innsamling av stordata, men ikke personopplysninger. For å kunne håndtere dette har vi blant annet en av Nordens største sentraliserte loggløsninger. Den tar imot flere terrabyte med data i døgnet, og innkomne data overvåkes kontinuerlig.

Alvorlige hendelser



Alvorlige hendelser er hendelser hvor en enhet (klient/server/»dings») er under kontroll av en tredjepart eller kan bli det dersom tiltak ikke treffes. Antallet går i bølger, men vi ser også at en del av de hendelser vi har jobbet med i senere tid har vært av mer alvorlig art enn tidligere.

> Alvorlige sikkerhets-hendelser er en del av hverdagen.

De vanskeligste angrepene

De mest profesjonelle trusselaktørene er krevende å håndtere. De gjør hva de kan for ikke å bli oppdaget og ønsker å drive sine operasjoner over tid. For å håndtere slike avanserte aktører må vi gjennomføre operasjonene slik at vi ikke røper kapasiteter og kapabiliteter. Dette er cyberoperasjoner som kan beskrives litt som «katt og mus». De kriminelle som står bak innbruddet må ikke få vite at de er oppdaget før de er stengt ute. Dette er komplekse operasjoner som krever spesialkompetanse og trusselforståelse i organisasjonen.

I takt med et mer utfordrende trusselbildet og sett i forhold til den ekspertkompetansen avanserte trusselaktører besitter, har vi valgt å bygge opp et eget fagmiljø med kompetanse og evne til å håndtere de vanskeligste angrepene; Telenor Norges Computer Emergency Response Team (CERT).
I tillegg til å håndtere hendelser i Norge støtter både Telenor Norges SOC og CERT Telenors operasjoner i Norden, Øst-Europa og Asia. Det betyr at vi er med på å yte støtte i beskyttelsen av over 36 000 ansatte, over 200 millioner kunder, og datasentre med titusenvis av servere og nettelementer. Med et slikt omfang er arbeid med alvorlige sikkerhetshendelser en del av hverdagen.

Angriper oss selv

Det er alltid en risiko for at det er noe vi ikke har tenkt på når vi designer våre systemer og nettverk. Derfor foretar vi sikkerhetstesting der kompetent personell gjør sitt beste for å kompromittere vår infrastruktur og tjenester. Målet er at de finner eventuelle sikkerhetshull før trusselaktører gjør det. For å få en best mulig test av egen teknologi kjøper Telenor Norge tjenesten fra eksterne leverandører som har sikkerhetstesting som sin kjernekompetanse.

Begrenser misbruk
Sikkerhetsavdelingen håndterer også misbruk av våre løsninger og tjenester, deriblant brudd på abonnementsvilkårene. Vi jobber aktivt med å avdekke sårbart utstyr i vår infrastruktur, eller kundeplassert utstyr, som blir misbrukt til ondsinnede formål. Eksempelvis å være avsender av angrepstrafikk rettet mot andre.

Telenor Norge driver ikke noen form for overvåking av enkeltindivider. Vi vurderer ikke lovligheten av innhold som formidles av andre, utover det som følger av gjeldende retts aktsomhetskrav. Vi utviser allikevel en proaktiv holdning i spesielle tilfeller overfor innhold som formidles, og spesielt ovenfor samfunnets mest sårbare – barn og unge.

For mer enn ti år siden utviklet vi i samarbeid med Kripos et eget overgrepsfilter. Formålet er å beskytte barn og unge fra overgrep. Hvis en Telenor-kunde forsøker å åpne en nettside som er registrert i forbindelse med spredning av overgrepsbilder, kommer det opp en sperreside med informasjon om filteret, samt en direktelink til Kripos sine sider. Det er Kripos som beslutter hvilke sider som har ulovlig innhold, og vår egenutviklede «Stoppside» skal hindre tilgang til ulovlig innhold og begrense lignende søk.

Overgrepsfilteret stoppet over 1 million besøk til registrerte sider fra august 2016 til og med juli 2017.

Telenor hverken lagrer eller logger hvem som faktisk treffer filteret.

Beredskapsorganisasjon
Vår krise- og beredskapsorganisasjon er et ledelsesverktøy som understøtter den organisasjonen som til daglig håndterer drift og feilretting. For oss handler kriseledelse om å gi linjeorganisasjonen vår støtte, sikre rett prioritering og entydig informasjon til kunder, myndigheter og media. Arbeid med hendelseshåndtering involverer både leverandører og entreprenører; både i beredskapsplanlegging, i daglig drift og under pågående hendelser.

Telenor Norge ser på samarbeid og samhandling som avgjørende for et godt sikkerhetsarbeid. Vi er ikke bedre enn summen av den sikkerhetskompetanse som sitter i hele vår verdikjede, og hos naturlige samarbeidspartnere som nasjonale samfunnskritiske aktører, sikkerhetsleverandører, andre virksomheters sikkerhetsavdelinger nasjonalt og internasjonalt, norske sikkerhetsmyndigheter, Forsvaret og politiet.

Vi jobber derfor aktivt med å forbedre både kompetanse og grensesnitt for samhandling. Vi samarbeider med en rekke høyskoler og underviser blant annet på Politihøgskolen og vi har avtale med Forsvaret om utvikling av cyberkompetanse. Telenor Norge har avtale med NSM/NorCERT om utvikling av en samarbeidsmodell mellom det nasjonale CERT'et og en eier av samfunnskritisk infrastruktur, intensjonen er at modellen skal kunne gjenbrukes av NSM/NorCERT overfor andre eiere av samfunnskritisk infrastruktur.

Et nasjonalt ansvar

Cyberspace kan ikke forsvares sektorvis

I juni 2017 kom stortingsmelding nr. 38 om IKT-sikkerhet som bærer tittelen «Et felles ansvar». Det er et godt prinsipp, men skal vi ta et felles ansvar må vi ha ett nasjonalt situasjonsrom for å skape felles situasjonsforståelse og en samlet evne til å håndtere hendelser. Vi kan ikke forsvare cyberspace sektorvis. Ei heller kan det gjøres uten private aktører.

I Telenor Norges undersøkelse svarer hele 70 prosent at de i stor grad (23 prosent) eller i noen grad (47 prosent) er redd for et cyberangrep skal lykkes i å slå ut vårt lands viktigste funksjoner. Samtidig svarer over halvparten at de har tillit til at norske myndigheter gjør hva de kan for å ruste samfunnet for den digitale trusselen.

Dette er tall som er illustrerende for situasjonen vi er i. Vi står ovenfor trusselaktører som kan skape store konsekvenser i samfunnet. Dette har blitt demonstrert blant annet gjennom påvirkningsoperasjoner som preget det amerikanske presidentvalget og cyberangrepene som har tatt ut deler av strømnettet i Ukraina.

Regjeringen har definert IKT-sikkerhet til å være et virksomhetsansvar. Det vil si at vi som selskap selv er ansvarlig for å foreta risikovurderinger og innføre tiltak. I tillegg har Justis- og beredskapsdepartementet et samordningsansvar for sivil sektor. Samordning og koordinering er to ord som går igjen i alle utredninger, men vi mener det mangler tydelig vilje til å peke ut hvem som har totalansvar for IKT-sikkerhet. Ingen myndighetsaktør leder håndteringen av hendelser i cyberspace i dag, det er kun koordinering og deling av informasjon som er formålet for hendelseshåndtering i cyberspace. Et lederdepartement må *lede*. Vi forstår at dette er krevende diskusjoner, men her trengs politisk vilje til å endre.

Må dele mer
Det er ikke deling av informasjon om sårbarheter hos for eksempel Microsoft og Adobe som skaper en koordinert evne til samhandling. Det er forståelsen av trusselaktørenes intensjon, kapasitet og kapabilitet som må deles mellom de som faktisk kan håndtere en avansert cyberoperasjon. Leverandører av samfunnskritisk infrastruktur må settes i stand til å forstå trusselaktørene slik at vi kan finne dem, og håndtere dem ut ifra én felles forståelse av mulige konsekvenser dette kan ha for samfunnet.

I en situasjon der Norge utsettes for cyberoperasjoner der det skapes ustabilitet eller kritisk informasjon kommer på avveie, er det myndighetenes oppgave å sikre prioritering av samfunnskritiske og nasjonale funksjoner. Hvis Norge utsettes for påvirkningsoperasjoner der nasjonal infrastruktur misbrukes for å påvirke demokratiske prosesser, er myndighetenes rolle å sikre sann og riktig informasjon.

Vi mener at dette først vil være mulig når vi har ett nasjonalt situasjonsrom. Vårt nasjonale CERT har ikke dette mandatet. Det er vesentlig for vår nasjonale beredskap at det nasjonale CERT-et har forståelsen av trafikken på internett i Norge. Det er ikke tilfelle i dag, da kun noen prosent er synlig gjennom VDI-sensorene til NorCERT.

Må behandles likt
Hendelser i cyberspace må håndteres etter de samme retningslinjer som hendelser i «den virkelige verden», men vi har ingen politimester i cyberspace.

Hvis noen fysisk bryter seg inn i Telenor Norges lokaler eller fysisk truer vår virksomhet eller ansatte så er vi ikke i tvil om at Politiet, de andre nødetatene, kanskje i de mest ekstreme situasjoner støttet av Forsvaret, ville håndtere hendelsen. Når Norge blir utsatt for en avansert cyberoperasjon via vår infrastruktur, så finnes ingen cyberberedskapstropp, det er kun Telenor Norge som reelt sett kan håndtere og normalisere situasjonen. Vi kjenner vår infrastruktur, og det er vi som må gjøre det som skal til for å normalisere situasjonen.

Det store problemet er at vi velger å gjøre ting annerledes når det handler om cyberspace. Politiet og Forsvaret utgjør statens to maktmonopoler for håndtering av ondsinnede handlinger og denne inndeling må derfor også gjelde for cyberspace. Telenor Norge mener at politiet bør bli gitt ansvaret, verktøyene og ressursene som skal til for å arbeide mot kriminalitet i cyberspace fra a til å, på samme måte som de håndterer kriminalitet i den fysiske verden. Det betyr å gi politiet et helhetlig ansvar for alt fra forebygging, håndtering og etterforskning av cyberkriminalitet. I flere år har behovet for et «nasjonalt cyber crime center» i politiet – et såkalt NC3 – vært etterspurt. Det har ikke blitt realisert ennå.

FCKS - Norges nye Felles Cyberkoordineringssenter skal koordinere de hemmelige tjenestenes innsats på cyberområdet. Det er positivt at de hemmelige tjenester skal koordinere sin innsats, men det er fortsatt infrastruktureierne og virksomhetene som må håndtere hendelser og redusere konsekvenser. Norge må ha en arena der informasjon blir delt og hendelser koordinert og ledet. Vi opplever at det fortsatt er et stykke igjen.

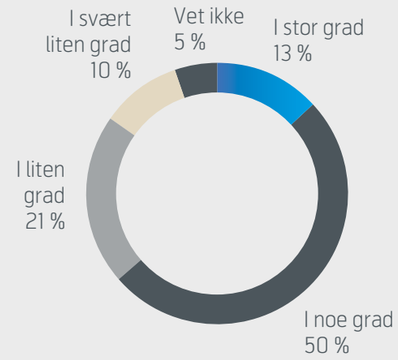
Nå må vi kraftsamle
Alle skal koordinere – ingen vil koordineres – nå må vi kraftsamle og bygge robusthet inn i den nasjonale hendelseshåndteringen.

I 2016 kom det første rammeverket for digital hendelseshåndtering, hvor ingen privat eier av samfunnskritisk infrastruktur er tegnet inn. Offentlig-privat samarbeid beskrives som viktig i samfunnssikkerhetsmeldingen, men det gjenspeiles ikke i rammeverket. Selve håndteringen kan ikke utføres av det offentlige alene, det erkjenner jo også myndighetene selv, så hvorfor holdes de private aktørene utenfor?

I et land med 5 millioner mennesker har vi fått et stort antall sektorvise responsmiljøer som ikke har egen evne til å håndtere hendelser, men kun informere om at noe har skjedd og formidle dette mellom ulike aktører eller innad i en sektor. Den operative effekten er lite synlig.

I enhver beredskapsorganisasjon står betydningen av å trene, utdanne og øve svært sentralt. Dette gjelder både militære, sivile, private og offentlige organisasjoner. Når NATO øver i Norge neste år er det den største øvelsen på flere tiår. Eiere av samfunnskritisk infrastruktur og andre samfunnskritiske aktører må få delta i slike øvelser. De operative beredskapskapasiteter som finnes i myndighetsapparatet må kunne understøtte håndteringen av cyberoperasjoner mot nasjonal infrastruktur. Dette må være forankret politisk. Når nasjonen skal beskyttes må det sivile samfunnet støtte Forsvaret; Totalforsvaret må fungere for at Forsvaret kan forsvare Norge. Vi må legge til rette for dette i fredstid for å sikre at det også virker når den nasjonale krisen kommer. Det betyr at private aktører må være en integrert del av Totalforsvaret.

63 prosent har i stor eller i noe grad tillit til at norske myndigheter gjør nok for å sikre samfunnet mot større cyberangrep.



Det har ikke gått galt – ennå
Cyberspace er ikke et mål i seg selv for en angriper, det er et middel for å oppnå en intensjon. Ukraina har de tre siste årene vært utsatt for en serie avanserte angrep fra Russland. Ukraina har blitt omtalt med ett russisk ord *polygon*; øvings- og treningsområde.

Professor Thomas Rid ved *War Studies department* ved King's College i London sier dette om Russlands operasjoner i Ukraina: «*De tester ut hvor den røde linjen går, og hva de kan slippe unna med.*» Et russisk ordtak går slik: «*Stikk med bajonetter. Når du treffer noe mykt, fortsett. Når du treffer stål, trekk deg ut.*» Vi aner ikke hvor eller hvem som er målet neste gang.

Norge er et langt mer digitalisert land enn Ukraina, og vi har ikke opplevd et alvorlig cyberangrep ennå - som vi er klar over. Når et angrep treffer samfunnskritiske funksjoner er vi i tvil om ressursene faktisk vil finne hverandre.