Oslo Militære Samfund 110126

”Cyberdomenet vinnes ikke med smalltalk”

- våre og samfunnets utfordringer -

Storm Jarl Landaasen, Head of Risk & Security, Telenor Business Norway
Telenor Business Norway (ca 1000 ansatte, omsetter for ca 10 mrd), divisjonen er del av Telenor Norge (ca 5000 ansatte, 30 lokasjoner inklusive Svalbard, omsetter for ca 25 mrd)

Vi er svært glade for denne anledningen til å bidra med utfordringer og muligheter i Cyberdomenet, sett fra vårt ståsted. Når vi inviteres for å snakke om cyberspace er det lett å be oss snakke om *”Telefoni og internett som en inngangsport til Cyberspace. Operatørens utfordringer og samfunnsmessige utfordringer.”*
Det vil jeg gjerne gjøre, men vi har altså ikke tro på at cyberspace vinnes med smalltalk, det må vilje, evne og handling til – nå – før det går galt.
Hensikten med denne konferansen er jo først og fremst å skape en bedre forståelse hos målgruppene for de utfordringer og muligheter som ligger i ”Cyberspace”. Jeg håper å kunne bidra til dette sett fra et operatørperspektiv.

Filosofien vår er:
Alt vi i Telenor gjør innenfor security, kan klassifiseres som samfunnsansvar. Telenor har et samfunnsansvar i form av vår størrelse og hva vi leverer til markedet. Det påligger oss et særskilt ansvar for å bidra med vår kompetanse og erfaring for å sikre landet i tilfelle nasjonalt cyberangrep. De valgene vi tar hver dag er viktige for at Telenor skal lykkes som selskap. Vi vet at informasjonsflyt er viktig, både hos oss selv og ovenfor våre samarbeidspartnere, kunder, entreprenører og leverandører.
Vi har ingen tro på å vinne Cyberdomenet ved å holde ting for oss selv. Samtidig må vi følge våre Etiske retningslinjer (Codes of Conduct). D ette betyr at vi må beskytte våre kunders og vår engen sensitive informasjon, men vi må dele og få informasjon som kan gjøre oss i stand til å håndtere et cybercrimeangrep eller et cyberangrep på nasjonen.
Jeg ønsker å ta for meg våre, altså operatørens, utfordring og det vi ser som samfunnets behov.

Forsvarsstatsråd GRETE FAREMO sa fra denne talerstolen 10. januar blant annet:
"Dataangrep utgjør en fjerde alvorlig trussel mot våre åpne samfunn. Nylige eksempler er hackingen av Nobelkomiteens nettsider forut for fredsprisutdelingen i 2010, samt de omfattende Wikileaks lekkasjene av sensitiv informasjon. Angrep mot IKT-systemer er en ny form for krigføring, som også kan ødelegge strømforsyninger, industriprosesser og andre samfunnskritiske virksomheter og funksjoner. Derfor må slike trusler møtes både med sivile og militære virkemidler."

Cybercrime kan for Telenors del grovt deles i to:
Det er kriminell handling mot våre kunder og det er kriminell handling mot oss – eventuelt en kombinasjon av disse to tingene.
Vi beskytter våre kunder i henhold til de tjenester, løsninger og serviceavtaler de har kjøpt for å beskytte seg. Vi beskytter oss selv for å beskytte vår virksomhet og vår forretning – men også fordi vi har et samfunnsansvar.

En digresjon: Allerede i 2007 var cybercrime større enn internasjonal narkotika - og prostitusjonstrafikk til sammen. I den forbindelse kan vi merke oss en artikkel i Wired i fjor der det blant annet sto: *“Why are hackers of this breed so “advanced” and “persistent? – Because somebody put them on a full-time salary.”*

Vi vet fra våre kundeundersøkelser at dersom brukerne ikke føler seg trygge på en løsning så vil dette begrense bruk av ny teknologi. Security og folk som arbeider med security må derfor skape tillit! Ikke ruge på hemmeligheter!
Dette må gjelde mellom oss og de vi har et grensesnitt mot også, men tillit er som dere vet noe man må fortjene, ikke noe man får.
Har politiet tilstrekkelige ressurser til å etterforske cybercrime effektivt i en verden uten nasjonale grenser?
Har politiet fått tilstrekkelig kapasitet og kapabilitet til å drive cyberetterretning og spre informasjon til oss som har bruk for det?
Telenor ønsker å dele med myndighetene, men skal dette ha noen hensikt må informasjonsdeling være toveis og tillitsbasert.

Det som bekymrer oss er mangel på koordinert deteksjon og manglende vilje til å dele informasjon.

Spørsmålet vårt er om samfunnet er skrudd sammen for å skulle detektere eller håndtere dette på en god måte – for eksempel i grensesnittet mellom Politiet, Forsvaret og sivile aktører.

Angrepet?
Hacking og angrep er trolig de mest misbrukte begreper innen security, både av securityfolk og i media.
Vi anser ikke et virusutbrudd, en trojaner eller annen malware for å være angrep, vi kaller ikke virusutbrudd på et sykehus for et angrep. Utbrudd av malware i en virksomhet kommer som regel av driftsfeil eller menneskelig svikt.
Et angrep har et mål og en ønsket sluttsituasjon og i cyberverden benytter man en spesialtilpasset malware designet for en spesifikk hensikt mot en spesifikk organisasjon, person eller nasjon.
«Targeted threat ... a class of malware destined for one specific organization...»
Eller fra den kjente analoge slagmarken:
«... a type of offensive action characterized by preplanned co-ordinated employement of firepower and manoeuvre to close with and destroy the enemy. »

Jeg kjenner bare til ett tilfelle der vi i Telenor har brukt begrepet målrettet angrep, det skjedde en gang mellom 24. og 25. oktober 2010, angrepet på Nobelinstituttet. NorCert uttalte på NSMs sikkerhetskonferanse at Nobelinstituttet hadde vært "kompromittert" helt siden 15. oktober.

Det som skjedde de døgnene var grovt sett at vi oppdaget unormal aktivitet 25. oktober, da vi så at dette var et angrep ved hjelp av en ukjent sårbarhet varslet vi NorCert. – Syv timer senere fikk vi bekreftelse fra NorCert om at "Nobelinstituttet var klar over dette".
Det er også på det rene at angrepet ikke ble utført av automatisert malware, dette er en av de viktigste indikasjonene vi har på at det var et målrettet angrep..

Om Telenor har blitt angrepet?
Senest for noen dager siden opplevde vi at en av våre websider var nede, men heller ikke det var et angrep mot Telenor.
Vi var offer for "colateral damage", vi var ikke målet.
Vi har ikke vært utsatt for et målrettet angrep oss bekjent.

Tillit – ikke "hemmelig nettverk
Jeg nevnte tillit, jeg vet at flere av dere har sett dette:
«Informasjonen kan deles med andre virksomheter eller personer innen informasjonssikkerhetsmiljøet, men skal ikke publiseres eller legges ut på websider/åpne mailinglister. Informasjonen er unntatt offentlighet. »

Vi kan ikke ha det slik som dette!
Hvis securitymennesker og securityorganisasjoner opptrer slik uten å tenke seg om så kan man spørre seg om avsender ikke forstår hva man holder på med.
Da jeg så disse formuleringen slo det meg: Hvem er personer og virksomheter i informasjonssikkerhetsmiljøet? Er dette et slags hemmelig brorskap?
Unntatt offentlighet? Når informasjonen man snakker om er public på Internet? –

Vi i Telenor kommuniserer med virksomheter og kan ikke ha kommunikasjon mellom enkeltpersoner i "hemmelige nettverk" som "får vite" men som "ikke får lov å fortelle videre".
I Telenor opptrer vi som selskap og på vegne av Telenor, det en ansatt får vite fordi han eller hun kjenner noen i en offentlig etat kan ikke vedkommende bruke i sitt arbeid.

Før 2000 snakket alle securitymennesker om " Need to know", derfra flyttet vi oss til "Need to share". I fjor høst fikk jeg gleden av å delta på NNEC-seminar (NNEC er som dere vet NATO Network Enabled Capabilities) på Lillehammer, der ble jeg presentert for begrepet "Responsibility to share" – jeg liker tanken og måten å dele på.

- Vi må slutte å tro at ting ikke kan hende oss
Samarbeidet for samfunnssikkerhet i Norge er sjokkerende dårlig, ifølge Riksrevisjonen. Ifølge riksrevisor Jørgen Kosmo står det ikke på penger, men på evne og vilje til å samordne på tvers av sektorer og avdelinger. Som eksempler trekker Kosmo blant annet frem at som følge av dette er informasjonssikkerheten i landet er mangelfull.
Jeg er enig med Kosmos uttalelser på den nasjonale konferansen om samfunnssikkerhet og nye trusselbilder.

RAND Corporation (http://www.rand.org/about/history.html) har i rapporten "Toward a Theroy of Intellicence" blant annet sagt:
"Historisk sett har etterretningstjenesten vært den mest nasjonale av statlige institusjoner. Mer enn hærer, har de vært utformet for å gi statene et forsprang på sine motstandere. Nå, som stater endres, hvor langt kan vi vente at etterretningstjenester vil gå for å oppnå samarbeid og åpenhet? Hva er grensen for etterretningsorganisasjoners evne til å strekke seg ut og dele, ikke bare deler og valgte godbiter med favorisert partnere, men engasjerende i felles problemløsning med selskaper og frivillige organisasjoner, stater og lokale myndigheter og utenlandske partnere? Kan slike nye mottakere bli mer enn tilfeldige mottakere av informasjon, og også kilder og forbrukere i et dynamisk nettverk der rollene endres fra en dag til den neste, og ett problem til neste?"

Jeg vil tro dette er spennende, men skremmende for etterretningsverden, både den sivile og den militære, men jeg tror etterretningsteori kan hjelpe mange å forstå grensene og mulighetene.

Jeg påstår etter å ha lest rapporten fra Rand Corporations:
Dette kan ikke lenger kun være et myndighetsanliggende.

Spillere som Telenor må med på en offisiell måte, men vi kan ikke operere i et "hemmelige brorskap".

Responsibility to share
Jeg likte umiddelbart "Responsibility to share"-tanken. Vi er i ferd med å implementere den selv, tenke nytt og det er fra oss i security det kommer! Det er vi som forteller organisasjonen hvordan vi kan dele informasjon og samtidig beskytte den riktig.

Major Bjarte Malmedal i Forsvarets Computer Network Defence-enhet sa på NNEC-seminaret i høst blant annet: *"Transformasjonen mot NNEC vil bli omfattende, og omfatter endringer i prosess, organisasasjon og teknologi. "*

Vi som arbeider med security i Telenor er overbevist om at "Responsibility to share" vil bedre informasjonskvalitet, samarbeid og felles situasjonsforståelse internt.
I forhold til "Cyberdomenet" forventer Telenor at myndigheter deler nyttig informasjon med oss. Vi vil dele informasjon, men da må vi ikke sende noe inn i et sort hull uten å få noe tilbake.

De som håndterer Cyberdomenet på offentlig side må være koordinert og kunne analysere mer enn malware, altså at man har en situasjonsforståelse og evne til å koordinere ressurser.
E-tjenesten, NorCert, PST altså de som håndterer Cyberdomenet må i tett og åpen dialog med oss som leverer kommunikasjonsinfrastruktur.

Det vi mangler for å være i stand til å dele og agere koordinert og riktig er tre ting:

- For det første: Formalistiske tiltak i lov og forskrift
- For det andre: Teknisk tilrettelegging
- For det tredje: Tillit mellom aktører som må skapes i fredstid

Det må tilrettelegges for å kunne opprettholde de viktigste samfunnskritiske funksjoner som er avhengig av vår infrastruktur.

Myndighetene bør i et samfunnssikkerhetsperspektiv sørge for at det blir tilrettelagt både formalia, tekniske løsninger og rutiner for å kunne utnytte kommunikasjonskapasiteter på tvers av Forsvaret og Telenor ved større hendelser/kriser, terror og krig.
Det er "for sent" å starte dette når behovet har inntruffet fordi både beslutningsprosesser og teknisk tilrettelegging vil ta lang tid.

Med gode forberedelser ville vi på kort tid kunne avhjelpe hverandre med å opprettholde de viktigste samfunnskritiske funksjoner som er avhengig av vår infrastruktur.

Kommandørkaptein Helge Arnli skrev i fjor en svært interessant masteroppgave ved Forsvarets Høyskole: "Intelligence sharing with host nations in multinational operations: Hurdles and dilemmas in Afghanistan".
Denne kan på svært mange felt overføres til det samarbeidet vi trenger for å vinne Cyberdomenet.
Min påstand er at Forsvaret kan dette. Cyberdomenet er ikke "noe nytt" om man ser på det som enhver annen operasjon, det nye er å dele og nyttiggjøre informasjon med andre aktører.

Formalia, tillit, tilrettelegging og trening er de viktigste bestanddelene for suksess.

Takk for oppmerksomheten.