Rapport fra seminaret «Sikkerhet og samarbeid – slik takler vi de nye truslene»

Cyberdomenet er blitt den nye slagmarken i en stadig mer sammenknyttet verden. Vi må være beredt til å forsvare oss mot cyber- og informasjonsoperasjoner med mål om å påvirke og lamme kritisk IKT-infrastruktur, virksomheter og demokratiske prosesser.

Utfordringene er store, og krever samarbeid. I CyberLand samles Norges ledende fagmiljø innenfor cyber- og informasjonssikkerhet. Her jobber Cyberforsvaret, NTNU Gjøvik, CCIS, NorSiS, Kommune-CSIRT og IKT-bedrifter sammen for å møte trusler mot vår informasjonssikkerhet. Det har allerede begynt å vokse bedrifter ut fra NTNU-miljøet på Gjøvik, og etterspørselen etter løsninger for cyber- og informasjonssikkerhet er økende.

Vårt mål er å etablere et økosystem hvor vekstbedrifter og talenter trives. Resultatet vil ikke bare bli flere arbeidsplasser, men et samspill mellom aktører for et sterkere og bedre cyberforsvar og løsninger som samfunnet trenger for å trygge kritisk infrastruktur. Under seminaret som CyberLand arrangerte under Sikkerhetsfestivalen 2019 inviterte vi noen av de klokeste hodene i bransjen til å diskutere utfordringene vi står overfor og løsningene vi trenger. Her kan du lese vår oppsummering.

Hilsen Paul Erik Hattestad,
Prosjektleder for CyberLand, Oppland fylkeskommune

***Cyberland** arbeider for å koble næringsliv, akademia og Forsvaret i Mjøsregionen sammen til én næringsklynge innenfor cyber- og informasjonssikkerhet. Her får bedriftene tilgang på kunnskap og ideer, teknologi og kapital. Det unike innovasjonsmiljøet skaper nye arbeidsplasser og trygghet for folk og samfunn. Slik skaper vi sikkerhet gjennom samarbeid.*

De nye truslene

Det meste av vår infrastruktur kan oppfattes som samfunnskritisk. Samfunnets infrastruktur vil også være viktig for å kunne opprettholde Forsvarets operative evne. Det gjør det vanskelig å tydelig definere det som ikke er legitime militære mål i en mulig konflikt. Vår infrastruktur vil kunne bli utsatt for angrep, men eierskap og utvikling av den er endret.

– Siden det offentlige i mindre grad eier, forvalter og utvikler infrastruktur har de ikke lenger den fremste kunnskapen. Kunnskap må flyte bedre, det gjelder også for Forsvaret, sier Kjell-Olav Nystuen, sjefsforsker ved Forsvarets forskningsinstitutt (FFI).

Manglende bevissthet

Det er daglig 40 millioner triggere på cyberangrep i Norge. Selv om de fleste bedrifter sier de har backup-rutiner, er det langt fra sikkert at de regelmessig sjekker disse. Kartlegging utført av Atea viser at det også kun er blant de største virksomhetene i Norge at det er en stor andel som har beredskapsplaner og gir de ansatte opplæring i IT-sikkerhet. I de mindre bedriftene er det lite av dette, selv om kostnadene vil være små og gevinstene store ved et angrep på IKT-systemene.

– Det er en naiv tilnærming til det å gi folk innganger, adgang og informasjon. Folk forstår ikke at det kun finnes to typer virksomheter: De som vet de har blitt hacket, og de som ikke er klar over at de har blitt hacket, forteller leder for IT-sikkerhet i Atea, Thomas Tømmernes.

Utfordringer i samarbeid

Bærerne av data er private, og dataene som lagres er på private hender. Lave marginer tilsier store volum, og gjør også at det meste av det som lagres er på utenlandske hender. Det offentlige lager tjenester med dette som utgangspunkt, det gjør at sameksistens og samarbeid med bedrifter blir viktigere. Det gjelder også for Forsvaret, ifølge executive director i KPMG Hans Christian Pretorius.

– For å lykkes bedre bør offentlige aktører være tydelige på hva som er behovet, men la bedrifter få handlingsrom til å skape innovative løsninger. Kontrakter som utformes fanger ikke godt nok opp de endringsbehovene som eksisterer. Det gjør at de løsningene som lages ikke er godt tilpasset et samfunn hvor teknologi er i rask utvikling og endring.

Fra venstre møteleder Hanne Eggen Røislien, Thomas Tømmernes (Atea), Kjell Olav Nystuen (FFI), Erlend Dyrnes (ISF) og Hans Christian Pretorius (KPMG) diskuterer hvordan det offentlige og privat næringsliv skal samhandle for å håndtere de nye digitale truslene.

– Dette er ikke enkelt. De som mener det er trivielt å dele informasjon ser bort fra at en offentlige aktør som får informasjon, også inviteres til å handle basert mottatt informasjon. Og private bedrifter kan vanskelig dele informasjon om sikkerhetsbrudd uten først å ha tatt hensyn til eiere, tilsynsmyndigheter og lovverk om hva de skal fortelle markedet, sier Pretorius.

– Vi må spørre oss om det offentlige ikke aksepterer vilkår bedrifter trenger for å utvikle nye løsninger. På sett og vis kan det virke som om det offentlige invaderer bedriftenes handlingsrom for innovasjon gjennom de avtalene som inngås.

– På grunn av at både kunnskap og teknologi utviker seg så raskt, blir det i stadig større grad nødvendig for Forsvaret å arbeide tettere mot akademia og næringsliv, sier sjef Cyberforsvaret, generalmajor Inge Kampenes.

Forsvarets behov

– Situasjonen er endret for dem som arbeider med cyber- og informasjonssikkerhet i Forsvaret. Tidligere tenkte Forsvaret at vi skulle ha kontroll over utvikling, og gjøre det meste selv. Var det et behov for akademisk kompetanse, ble det etablert nye enheter. Var det behov for nytt materiell, ble det laget av selskaper hvor staten hadde stor grad av kontroll. Trengte vi kommunikasjon og samband var Televerket tett koblet på Forsvaret, forteller sjef Cyberforsvaret, generalmajor Inge Kampenes.

I dag må Forsvaret forholde seg til markedsaktører og globale kunnskapsaktører, innenfor et område hvor både kunnskaps- og teknologiutviklingen går raskt. Utviklingen i det sivile markedet går også raskt, og driver teknologiutviklingen også for Forsvaret.

– Erkjennelsen av dette gjør at Forsvaret må arbeide tettere med akademia og næringsliv. For Cyberforsvaret er samarbeidet med NTNU særlig viktig, og modellen med samarbeid om utdanning av cyberingeniører har fungert godt. Vi forventer at akademiske miljøer ved NTNU er i kunnskapsfronten, og kan presentere trender og muligheter for Forsvaret.

Forsvaret kan ikke inngå strategisk samarbeid med hvilket som helst selskap, og trenger derfor at norske selskaper er på høyde internasjonalt.

– Det er et behov for samarbeid basert på gjensidig gevinst. De som leverer til oss må forstå Forsvarets behov bedre, og vi må bli bedre til å fortelle hva vi trenger, sier Kampenes.

Akademias bidrag

NTNU har det klart største og mest internasjonalt orienterte miljøet innenfor cyber- og informasjonssikkerhet i Norge. Fagmiljøet samarbeider tett med Cyberforsvaret, og er utgangspunkt for flere bedriftsetableringer i og utenfor Mjøsregionen. Forventningene til NTNU innenfor cyber- og informasjonssikkerhet er store, men matches av de forventningene de har til seg selv som en viktig del av et europeisk og internasjonalt kunnskapsnettverk, ifølge Nils Kalstad, leder av Institutt for informasjonssikkerhet og kommunikasjonsteknologi ved NTNU Gjøvik.

– Vi skal pushe den internasjonale kunnskapsfronten og hente hjem nye kunnskap. Det gjør oss relevante for Forsvaret, og gjør det mulig å skape nye bedrifter som bidrar til samfunnssikkerhet og arbeidsplasser i regionen, sier Kalstad.

Samfunnets satsinger

Uten økning av innsatsen på studieplasser vil Norge mangle 4.000 årsverk innenfor digital sikkerhet frem mot 2030, viser tall fra Statistisk sentralbyrå. Tallet er et forsiktig anslag, for utviklingen av informasjonssystemer og behov for sikkerhet vil sannsynligvis gå hurtigere enn det vi ser i dag. Det tilsier også økt satsing på forskning. I dag utgjør midler til forskning innenfor cyber- og informasjonssikkerhet 14 prosent av Forskningsrådets midler innenfor IKT. I tillegg er cyber- og informasjonssikkerhet høyt prioritert i EUs neste, store forskningsprogram – Horizon Europe.

– I Norge er de to mest vesentlige programmene for cyber- og informasjonssikkerhet SAMRISK og IKTPLUSS. Disse skal knyttes tettere sammen, også for å kunne få frem tverrfaglige prosjekter som inkluderer bedrifter, offentlige virksomheter og organisasjoner – brukerne forskere skal jobbe for, sier områdedirektør for samfunn og helse i Forskningsrådet Jesper W. Simonsen.

– Det å ikke forstå skaper ikke bare usikkerhet, men også distanse. Vi må erkjenne problemene vi står overfor, for å kunne forstå og håndtere de nye truslene.