Innspill til ny nasjonal digitaliseringsstrategi

Vi blir daglig minnet på risiko knyttet til digitalisering, samfunnet er i dag mer sårbart enn noen gang tidligere. “Cyberangrep har blitt hverdagskost (NSM, 2023)” starter kapitelet som beskriver Cybersituasjonsbildet i Norge i “Nasjonal digitalt risikobilde 2023” rapporten fra nasjonal sikkerhetsmyndighet (NSM). I samme rapport blir det også nevnt at pro-russiske aktører, i løpet av det siste året, har forsøkt å utføre tjenestenektangrep mot nye sektorer NSM tidligere ikke har sett på som typiske mål (NSM, 2023). Angrepsflaten mot norske virksomheter og sektorer utvides og teknologien brukt i både norske virksomheter, men også teknologi brukt av angripere utvikler seg. Gapet mellom digitaliseringshastigheten, kompetanse, vår evne til å beskytte verdier og respondere trues i en sammensatt og kompleks global trusselsituasjon, som endres raskt, og som går på tvers av det offentlige og private.

Noen av utfordringene vi i Netsecurity møter i dag, hos stadig flere virksomheter, er en manglende evne til å håndtere kriser om en uønsket endring eller hendelse skulle inntreffe. Dette reduserer tryggheten og svekker tilliten knyttet til digitalisering. Mangel på kompetanse og interesse for informasjonssikkerhet blant ledere og ansatte i både det offentlige og private forhindrer norske virksomheter i å styrke forsvarsevnen nok til å kunne håndtere en hendelse om den skulle oppstå.

Den geopolitiske situasjonen gjør det vanskelig å ha kontroll på tillitsforhold. Store norske virksomheter og delvis statlige har konkurranseutsatt drift av både IT og IT sikkerhet til lavkost land med bånd til land vi er i konflikt med. Dette burde vært regulert, også med tanke på det reelle kompetansegapet vi møter ved å utføre arbeidet utenfor Norge. Manglende reguleringer gjør det enklere å nedprioritere informasjonssikkerhetsarbeidet, samtidig som både manglende regulereringer, krav og incentiver fører til at informasjonsdeling og samarbeid mellom det private og offentlig sektor i dag går for sakte.

Digitaliseringen av kraftsektoren og annen kritisk infrastruktur tar nå et stort skritt. Operasjonell IT skal utnytte Kunstig intelligens for økt forutsigbarhet for vedlikehold, redusere kostnader og mer, men skaper med det også økt risiko for både utilsiktet og bevisste hendelser som kan skape kritiske situasjoner.

Nasjonal kontroll

Norge bør i størst mulig grad være selvforsynte innen kritisk infrastruktur, digital sikkerhet og beredskap. Dette bør gjøres ved å stille krav til digital sikkerhet og beredskap til virksomheter i det private og i det offentlige. NIS2-direktivet er ett godt eksempel på ett initiativ som vil innføre skjerpede krav innen informasjons- og cybersikkerhet. Vi ser på slike krav som viktige steg for å sikre norske virksomheter

og Norges interesser. Ved innføring av nye krav ser vi også behovet for å oppmuntre norske virksomheter til å etterleve kravene og innføre sikkerhet utover kravene.

Når nye direktiver og krav blir innført så bør det derfor være et fokus på forenkling og bistand til etterlevelse av disse. For å få dette til må vi ikke bare skape mer effektivt samarbeid på tvers av det offentlige og private, men også på tvers av private aktører. Det offentlige bør arbeide for å legge til rette for slikt samarbeid gjennom ulike krav, incentivordninger og koordinering.

Virksomheter må føle trygghet og må være i stand til å samarbeide effektivt på tvers av ulike siloer mellom det offentlige og private. NSMs kvalitetsordning for leverandører som håndterer IKT-hendelser er et eksempel på en ordning hvor det offentlige stiller krav til private aktører, men hvor insentiver til å bidra til økt samarbeid og koordinering mangler.

Kompetanseunderskudd

Vi har i dag et stort underskudd på fagpersoner med rett kompetansenivå innen informasjonssikkerhet. Kampen om de få som utdannes innen cybersikkerhet er knallhard og bransjen kannibaliseres, som følge av hard konkurranse om fagressurser. Fremtiden ser foreløpig ikke lysere ut da det rapporteres ett forventet underskudd av 4100 fagressurser innen it-sikkerhet i 2030 (NIFU, 2023). For å dekke det fremtidige behovet må vi opprette flere spesialiserte studier og studieplasser innen informasjonssikkerhet med fokus og insentiver som gjør det attraktivt å utdanne seg og arbeide med it-sikkerhet. Vi bør også oppfordre til samarbeid mellom næringslivet og studier for å gi studentene praktisk erfaring før endt studie og øke relevansen fra eksisterende studier opp mot fremtidige arbeidsmarkedet studentene beveger seg mot.

Manglende risikoforståelse

Manglende risikoforståelse i virksomheter og i det offentlige gjør oss sårbare. Konkurranseutsetting og overgang til skytjenester grunnet økende krav til digitalisering og effektivisering uten å tenke risiko i tilstrekkelig grad gjør oss eksponert for trusselaktører. Krav, samarbeid og incentivordninger fra det offentlig burde ha til hensikt å påvirke virksomheter sin ledergruppe i arbeidet rundt sikkerhet.

Manglende kompetanse og risikoforståelse for it-sikkerhet blant ledelsen i norske virksomheter svekker organisasjonen evne til å iverksette beskyttende tiltak både for å forhindre cyberangrep mot sin egen virksomhet og mot tredjepart ved å bli brukt for å angripe en tredjepart, uvitende på vegne av angriperen. Når ledergruppen ikke involveres og engasjeres i sikkerhetsarbeidet i virksomheten de styrer, så økes risikoen for at riktige tiltak ikke blir innført i veien mot å bli sikrere.

Om Netsecurity

Netsecurity jobber med sikkerhet i alt vi gjør, fra rene sikkerhetstjenester til å tenke sikkerhet i andre it- tjenester, for å ivareta sikkerhet i hele verdikjeden til våre kunder. Våre it og ot-eksperter er tilgjengelig 24/7 – 365 dager i året. Netsecurity tilbyr ekspertise, løsninger og innovative tjenester innen it-sikkerhet i det norske markedet. Med over 150 ansatte plassert rundt på fem kontorer i Norge og ett kontor i Sverige utgjør vi ett av Norges største selskap innen it-sikkerhet.

Kilder:

Nasjonalt digitalt risikobilde 2023.(n.d.).Hentet 14. november 2023 fra: https://nsm.no/getfile.php/1313382-1697777843/NSM/Filer/Dokumenter/Rapporter/Nasjonalt%20digitalt%20risikobilde%202023.pdf

Arbeidslivets behov for digital sikkerhetskompetanse frem mot 2030. (n.d.). Hentet 14. november 2023, fra https://nifu.brage.unit.no/nifu-xmlui/bitstream/handle/11250/3069233/NIFUrapport2023-4.pdf?sequence=1&isAllowed=y