Sikring mot IKT-trusler

Norske bedrifter henger ikke med i utviklingen når det gjelder IKT-sikkerhet. Gapet mellom trusselaktørene og vår evne til å hindre, oppdage og håndtere IKT-angrep er økende. Hvorfor er det sånn, og hva kan bedrifter gjøre for å redusere dette gapet?

Artikkelen er forfattet av:

Senior manager
Dagfinn Buset
Leder i BDO sikkerhet og beredskap

Senior manager
Andreas Vogt
Leder i BDO sikkerhet og beredskap

Risikoen for nettverksbasert spionasje og andre alvorlige dataangrep mot norske virksomheter er høy. Dette har landets sikkerhets- og etterretningstjenester påpekt i flere rapporter, senest i Nasjonal sikkerhetsmyndighets rapport «Helhetlig IKT-risikobilde 2015».[1] Om trusler i det digitale rom skriver også Etterretningstjenesten i sin åpne vurdering, FOKUS 2015, at «(n)ettverksbaserte etterretningsoperasjoner er en betydelig trussel mot norske interesser. Slike operasjoner utføres mot en rekke mål i Norge. Fremmed etterretning angriper løpende norske myndigheter og virksomheter».[2]

Trusselaktørenes evne og vilje til å innhente informasjon gjennom datanettverk blir stadig mer målrettet og sofistikert. Det kanaliseres milliarder av kroner hvert år til nettverksbasert etterretning. At trusselaktørenes kapasiteter øker, må bety at omfanget og aktiviteten øker tilsvarende. Budsjettene til etterretningsorganer som driver spionasje over datanettverk, eller i cyberspace, har blitt tidoblet. Cybersikkerhet, i betydningen både offensive og defensive aktiviteter for å sikre seg i det digitale rom, har førsteprioritet i det nasjonale sikkerhetsarbeidet i flere land.

Er det så viktig da?

Det er mange årsaker til at bedrifter ikke tar nødvendige grep om egen IKT-sikkerhet. En åpenbar årsak kan være at bedriften tror at den ikke er utsatt for dataangrep. Det blir ofte sagt at vi nordmenn er naive. Det stemmer. Holdninger som «det kommer aldri til å skje», «la oss ikke bli paranoide», «det skjer ikke her» og «vi har ingenting av verdi», er ganske utbredt i det daglige når alt er som normalt. Imidlertid kommer andre holdninger til overflaten når hendelsene først inntreffer: «Hvordan var det mulig at dette kunne skje?», «Hvorfor var vi ikke forberedt på dette?» osv. Når skaden har skjedd og tapet merkes på bedriftens bunnlinje, er det for sent å erkjenne at man kunne ha vært bedre forberedt – både når det gjelder forebyggende tiltak og skadebegrensende tiltak.

Det vil alltid finnes dem som mener at sikkerhetstiltak er unødvendige fordi de ikke har blitt påført noen tap ennå. Da er det viktig å se på sikkerhet som en langsiktig investering. Det er i flere rapporter gjort beregninger på hva bedrifter påføres av tap som følge av manglende IKT-sikkerhet. I en rapport fra McAfee anslås det et globalt tap på 400 milliarder dollar som følge av manglende IKT-sikkerhet.[3] Det er som sagt lett å være etterpåklok når skaden har skjedd. Og det kan ikke minst bli dyrt. Som Sven Ullring, tidligere konsernsjef i DnV og leder av det regjeringsoppnevnte utvalget for sikring av landets kritiske infrastruktur, har sagt: «Synes du sikkerhet er dyrt, prøv en katastrofe!»[4]

Behovet for risikoerkjennelse

Risikoerkjennelse er selve grunnlaget for å redusere vår sårbarhet. Dette er noe 22. juli-kommisjonen vektla i sin rapport, og som Nasjonal sikkerhetsmyndighet også har vektlagt i sine rapporter om sikkerhetstilstanden, første gang i 2011.[5] I 22. juli-kommisjonens utredning fremgår det at «Kommisjonens viktigste anbefaling er at ledere på alle nivåer i forvaltningen systematisk arbeider med å styrke sine egne og organisasjonenes grunnleggende holdninger og kultur knyttet til risikoerkjennelse, gjennomføringsevne, samhandling, IKT-utnyttelse, og resultatorientert lederskap».[6] Kommisjonens anbefalinger er selvsagt like relevante for privat sektor som for forvaltningen.

Risikoerkjennelse handler om å ha oversikt og forståelse for hvilke verdier virksomheten forvalter, hvilke trusler og farer disse verdiene må beskyttes mot, og hvilke sårbarheter som kan utnyttes og dermed medføre skade og tap.

Kjenn dine verdier!

For å kunne jobbe systematisk og ressurseffektivt med sikkerhet, må virksomheter ha et klart bilde av hvilke verdier de forvalter. Dette kan være verdier i form av informasjon, fysiske objekter, eller funksjoner og prosesser. Det er i denne sammenheng nedslående å lese Mørketallsundersøkelsen 2014, der det fremgår at norske virksomheter ikke har oversikt over hvilke verdier de besitter, og at under halvparten av de store virksomhetene har vurdert sine informasjonsverdier.[7] Dette kan ha alvorlige økonomiske og sikkerhetsmessige konsekvenser. Manglende oversikt over hvilke verdier en bedrift besitter, kan føre til at det brukes ressurser på sikkerhetstiltak som er helt unødvendige, eller at bedriften ikke beskytter det som har verdi med påfølgende risiko for at disse verdiene skades, forringes eller i verste fall går tapt.

Grunnleggende sikkerhetstiltak

Grunnleggende tiltak kan ha stor sikkerhetsmessig effekt. I 2014 håndterte NSM totalt 88 alvorlige dataangrep. Dette er

1 Kilde: «Helhetlig IKT-risikobilde», Nasjonal sikkerhetsmyndighet (2015).
2 Kilde: «*FOKUS 2015*», Etterretningstjenesten (2015).

3 Kilde: «*Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II.*» McAfee, Center for Strategic and International Studies (June 2014).
4 Kilde: «*Årsmelding 2011*», Nasjonal sikkerhetsmyndighet (mai 2012).

5 Kilde: «*Rapport om sikkerhetstilstanden 2011*», Nasjonal sikkerhetsmyndighet (juni 2012).
6 Kilde: «*NOU 2012: 14 Rapport fra 22. juli-kommisjonen*», 22. juli-kommisjonen (august 2012).
7 Kilde: «*Mørketallsundersøkelsen 2014*», Næringslivets sikkerhetsråd.

nesten en dobling fra året før. Nå skulle man kanskje tro at det ikke har nevneverdig effekt å etablere grunnleggende IKT-sikkerhetstiltak for å motvirke disse truslene. Det er ikke tilfelle. I sin rapport «Helhetlig IKT-risikobilde 2015» skriver Nasjonal sikkerhetsmyndighet at 90 prosent av alle dataangrep kan forhindres hvis virksomheter implementerer ti grunnleggende sikkerhetstiltak. Videre påpeker NSM at 100 prosent av de alvorlige dataangrepene de har sett de to siste årene, hadde blitt stoppet dersom virksomheten som var angrepet, hadde gjennomført fire av de enkle tiltakene NSM anbefaler.[8] Dette er tiltak som NSM har anbefalt gjentatte ganger. At mange bedrifter fremdeles unnlater å følge disse rådene, er overraskende. Men – det gir også en ganske enkel oppskrift på hva som må gjøres først. De fire grunnleggende tiltakene som anbefales er:[9]

1. Oppgrader program- og maskinvare.
2. Vær rask med å installere sikkerhetsoppdateringer.
3. Ikke tildel sluttbrukere administratorrettigheter.
4. Blokker kjøring av ikke-autoriserte programmer («hvitelisting»).

Helhetlig tilnærming til sikkerhet

Vi i BDO mener at alle virksomheter bør ha en helhetlig tilnærming til sikkerhetsrisiko. IKT-sikkerhet er ikke noe som skal styres løsrevet fra arbeidet med fysisk sikkerhet og personellsikkerhet i virksomheten. Dette er områder som har tette koblinger til hverandre, og som bør sees i sammenheng.

Dette er nødvendig for å utvikle et formålstjenlig system for sikkerhet og påfølgende balanserte tiltak som forbedrer sikkerhetstilstanden.

I denne sammenheng har britiske sikkerhetsmyndigheter gitt råd om hvordan bedrifter kan øke sin IKT-sikkerhet på en helhetlig måte gjennom de såkalte «10 Steps to Cyber Security»[10]. Disse stegene omfatter følgende områder:

1. Risikohåndtering
2. Sikker konfigurasjon
3. Nettverkssikkerhet
4. Styring av brukerrettigheter
5. Opplæring og bevisstgjøring av brukere
6. Hendelseshåndtering
7. Forebyggende tiltak mot skadevare
8. Overvåkning
9. Kontroll med flyttbare medier
10. Sikring av mobilt kontor

Etabler et styringssystem for sikkerhet

I likhet med annen risikostyring innebærer styring av sikkerhetsrisiko å identifisere og håndtere kravene som stilles til din virksomhet på området. Hvilke sikkerhetskrav og sikringsambisjoner en virksomhet har, avhenger av egne mål og arbeidsprosesser, sammen med de eksterne krav, lover og regler som stilles fra samfunnet.

Formålet med sikkerhetsstyring er at virksomheten når sine mål innenfor en bevisst akseptert margin av sikkerhetsrisiko. God sikkerhetsstyring vil si at ledelsen i virksomheten har erkjent hvilken sikkerhetsrisiko virksomheten står ovenfor, har en policy og strategi for hvordan sikkerhetsrisikoen håndteres, og fører kontroll med den faktiske etterlevelsen.

Bedriftens styre spiller en avgjørende rolle

Styret spiller en avgjørende rolle for å styrke IKT-sikkerheten i bedriften. Styret kan i større grad etterspørre status på IKT-sikkerheten i bedriften. Noen grunnleggende spørsmål som styret kan stille er:

1. Blir bedriftens sikkerhetsarbeid godt ivaretatt, og blir verdiene tilstrekkelig beskyttet mot uønskede hendelser?
2. Hvordan blir risiko håndtert?
3. Hvilken risiko aksepteres?

For å få brakt status på styrets bord, er det stadig flere styrer som etterspør kvalitetsrevisjoner av bedriftens sikkerhets- og beredskapsarbeid. Dette er bra!

God sikkerhet gir godt omdømme

Norsk næringsliv forvalter enorme verdier i intellektuell eiendom, avansert teknologi og unike produksjonsprosesser. Dette er verdier som gjør enkeltbedrifter konkurransedyktige i et internasjonalt marked, og som legger grunnlaget for videre økonomisk vekst. Det er nødvendig med økt forståelse for at dette er verdier som uvedkommende har interesse av å få tilgang til, og at manglende sikkerhet kan få alvorlige økonomiske konsekvenser. Det er god økonomi i å tenke sikkerhet. Vi kan regne med at antallet dataangrep mot norske bedrifter vil øke i årene fremover. Da gjelder det å redusere risikoen gjennom å styre sitt sikkerhetsarbeid på en fornuftig og balansert måte, etablere forebyggende tiltak som forhindrer potensielle tap, og etablere en operativ evne til å håndtere de hendelsene som vi likevel må regne med rammer oss. Helhetlig og godt sikkerhetsarbeid skaper god kvalitet i våre leveranser av varer og tjenester, som igjen gir tillit og godt omdømme i et stadig mer risikoutsatt samfunn.

8 Kilde: *«Helhetlig IKT-risikobilde»*, Nasjonal sikkerhetsmyndighet (2015).
9 Kilde: *«Fire effektive tiltak mot dataangrep»*, Nasjonal sikkerhetsmyndighet, (oppdatert 31.01.2014).
10 Kilde: *«10 Steps to Cyber Security»*, CESG, Cabinet Office, Centre for the Protection of National Infrastructure and Department for Business, Innovation & Skills (oppdatert 16. januar 2015).

Økonomisk styring og kontroll. Punktum.

FINALE

Kd110 REIBO Foto: Monkey Business

ÅRSOPPGJØR | RAPPORTERING | KONSOLIDERING | AVSTEMMING | SKATT | DRIFTSMIDLER | INVESTOR

Finales programmer tar over der økonomisystemene stopper, og hjelper deg videre med årsregnskap, noteopplysninger, ligningsoppgaver, skatteberegning, avstemming, dokumentasjon, analyse- og nøkkeltallrapporter, prognoser, grafer, perioderapporter, konsernregnskap, avskrivninger, driftsmiddeloversikt, aksjeoversikt, kontantstrømoppstilling m.m. I tillegg valideres dataene automatisk mens du arbeider, slik at feilføringer avsløres umiddelbart. Gratis demoversjoner finner du hos www.finale.no.

Finale Systemer as
SMS Finale til 26112

Tlf.: 4000 2215
www.finale.no

e-post: firmapost@finale.no

Et selskap i VISMA®