KPMG

KPMG Cyber – “Halloween”

Agenda

Om meg☺

- Har tidligere jobbet for Norsk senter for Informasjonssikring (NorSIS), Telenor, Symantec og som selvstendig rådgiver innen strategisk kommunikasjon og forebyggende tiltak knyttet til digital sikkerhet, samt allianser, aktivering av sponsorater og ulike samarbeid innen sikkerhet m.m.
- Jobber i dag for KPMG innen prosjekter knyttet til «cyber communication» – herunder strategisk kommunikasjon, rådgivning, sikkerhetsledelse og kultur. Samarbeider med Næringslivets sikkerhetsråd (NSR) via KPMG i forbindelse med deres arbeid knyttet til Mørketallsundersøkelsen – 2018.
- **Hva jeg skal snakke om:**

- For ledere om digital sikkerhet – overordnet og ikke teknisk
- Belyse viktigheten av trusselvurderinger knyttet til sikkerhetsledelse/kultur og omdømme
- Eksempler på erfaringer knyttet til manglende sikkerhetsledelse (anonyme)
- Konkrete tiltak og inspirasjon til bedre sikkerhetsledelse & kultur
- Litt om utviklingen fremover – hva bør en leder være obs på.

Varsler vi må / bør forholde oss til

- Værvarsler: gir oss mulighet til å planlegge reisemuligheter og tilpasse bilkjøring etter ferdigheter/evne og bilens tekniske stand.

= felles er at det gir oss et beslutningsgrunnlag for vår egen og andres sikkerhet på veien.

- Men, hvilke varsler er det du som leder baserer deg på når du skal beslutte innen sikkerhetsledelse?

De åpne trusselvurderingene

Trusselvurderingene = værvarsel for det digitale rom for inneværende år og kommer i februar/mars.

Trusselvurderingene er en bestilling fra norske myndigheter til Nasjonal sikkerhetsmyndighet (NSM), PST, E-tjenesten og DSB.

Anbefaler fokus i hovedsak på trusselvurderingene fra NSM og PST – da de kan omsettes til handling i næringslivet.

De åpne trusselvurderingene skal være et grunnlag for sikkerhetsarbeidet til næringsliv og det offentlige. Det å dele nedgradert informasjon – er en vikling utvikling.

Husk at NSM og PST er hemmelige tjenester som bare har vært «åpne» de 2 siste årene – men som følge av bestilling/krav fra myndighetens er blitt åpnere. For som myndighetene sier – «vi kan ikke håndtere alt med cybersikkerhets alene – vi må ha samarbeid med næringslivet og alle må ta ansvar**».**

De åpne trusselvurderingene bidrar til at vi kan ta bedre ansvar for vår egen cybersikkerhet, men også melde i fra til myndigheten når hendelser oppdages.

Trusselvurderinger for døve ører?

- **Nesten 90 prosent av digital infrastruktur i Norge er i private hender.**
- **Samtidig er det få innen næringsliv og det offentlige som leser trusselvurderingene som utgis årlig av eksempelvis Nasjonal sikkerhetsmyndighet og PST (ref. KRISINO 2017 / NSR).**
- **De som har lest PSTs trusselvurdering:**
- **I privat sektor: 14%**
- **I offentlig sektor: 26%**
- **De som har lest NSMs trusselvurdering:**
- **I privat sektor: 8%**
- **I offentlig sektor: 21%**

- **Så hvilket beslutningsgrunnlag har da norske virksomheter når de skal planlegge sikkerhetsledelse av egen virksomhet?**

Trusselvurderingene = viktig beslutningsgrunnlag

- Få virksomheter har mulighet til å drive etterretning alene. Vi er avhengige av myndighetene og samarbeid.
- Trusselvurderingene er uavhengige og kvalitetssikret og koordinert mellom e-tjenestene. Altså ikke utformet med annet formål enn **å bevisstgjøre og forebygge**.
- Trusselvurderingene baserer seg på etterretning– og viser at trusselbildet blir stadig mer komplekst og er i utvikling med aktører som spenner seg fra kriminelle enkeltpersoner, til organisasjoner og stater. **Man kan se trender og forberede seg bedre. Herunder også se om enkelte bransjer er utsatt.**
- Formålet bak cyberkriminaliteten blir også tydeliggjort: ofte drevet av økonomisk vinning, stjele sensitiv bedriftsinformasjon for videresalg, spionere, ødelegge eller drive ulike former for utpressing.
- Informasjon om hvordan Cyber kriminaliteten utøves i form av generelle og spissede angrep – eller i kombinasjon.
- **Cyber er også en arena hvor den sikkerhetspolitiske situasjonen utspiller seg** – f. eks hacker angrep fra Russland med større mål i sikte, kan også ramme eller gå via små norske virksomheter. (Nato øvelsen)
- Å forstå trusselbildet og driverne bak trusselbildet gjør en også i bedre stand til **å forebygge og reagere** ved cyber hendelser når de rammer. Herunder interne og eksterne tiltak.
- Hva må på plass for å dokumentere hendelser – logg analyser. (viktig info til Politi/etterforskning)

En annen viktig utvikling ref. trusselvurderingene:

- De siste trusselvurderingene viser at vi **teknologisk sett har aldri vært sikrere**.
- Samtidig dokumenterer alle trusselvurderingene, at en av de største truslene er sosial manipulering og innside trusselen.
- **Menneske er det svake leddet** og faller for f. eks falske eposter eller konkurranser i sosiale medier som spiller på:

- Fristelser
- Frykt
- Tillit
- = behov for kontinuerlig bevisstgjøring, øvelse og rapportering er stort og et viktig forebyggende tiltak.
- = teknologien utvikler seg stadig – kunnskap blir ferskvare.

Erfaringer knyttet til manglende «forebyggende arbeid» innad i en virksomhet

- Ingen rapportering langs verdikjeden om cyberhendelser (f. eks på avdelingsmøter)
- Ingen pålagt opplæring om digital sikkerhet eller kompetanse mål (gammel teknologi vedvarer / ny teknologi dominerer)
- Ingen deling av informasjon internt om trussel/ sikkerhetssituasjonen – kun foreholdt noen få.
- Ulik modenhet innad i organisasjonen pga ulik arbeidshverdag – ulik oppfattelse av trusler.
- Sikkerhetstiltak oppleves som tidkrevende og hemmer arbeidsprosesser – konskevens?
- Ikke alle forstår – når eller hva er sensitiv informasjon? (eks info på avveie som kan hindre virksomheten i å levere tjenester som vanlig)
- «ikke mitt ansvar» - en gjenganger
- Dårlig informasjonsflyt om digital sikkerhet – dermed lav bevissthet
- Viktig lærdom: Blir du **ikke målt** på sikkerhet, rapporteres det heller ikke. (Mørketallsundersøkelsen fra NSR)

Hvordan styrke intern sikkerhetskultur

Mange virkemidler og ulikt utgangspunkt – men noen tips:

- Felles situasjonsforståelse - Forankre trusselbildet og tilhørende forventet adferd.
- «mitt ansvar/mine handlinger» - mine handlinger øker eller reduserer sikkerheten.
- Oppdatere trusselbildet internt i tråd med eksterne hendelser som f. eks nedetid hos BankID, men del også egne interne hendelser med fokus på læring. Ikke hold det hemmelig.
- Forebygging og formidling er et kontinuerlig arbeid og krever også interne arenaer for læring og god informasjonsflyt internt i virksomheten.(etabler egne eksperter)
- Innføringskurs om digital sikkerhet for alle nyansatte.
- Opplæring kan være f. eks med fokus på å lære «hva er sensitiv informasjon» og hvordan skal vi forvalte sensitiv informasjon?
- Info om lover og regler. Akkurat som trafikkregler – finnes også lover og regler for det digitale rom. (Sikkerhetsloven)
- Sikkerhetskultur – krever tettere samarbeid mellom IT/sikkerhets avd, HR, ledelse og marked/kom
- Rapportering – vi må bli målt på hvordan vi håndterer sikkerhet.

Sikre og styrke omdømmet knyttet til sikkerhet

- Ta eierskap til temaer innen digital sikkerhet med relevans for din virksomhet/bransje.
- Bygg relasjon/nettverk innen digital sikkerhet innad i egen bransje- f.eks med andre ledere – skap bransjearenaer for læring (ikke konkurrer på sikkerhet – se f. eks på bankene)
- Vurder alliansebygging med aktører som tilfører verdi – f. eks Næringslivets sikkerhetsråd.
- Etabler kjennskap internt til premissleverandørene innen digital sikkerhet – i hovedsak NSM, NSR, Næringslivskontaktene i POD/KRIPOS og andre arenaer som fronter kunnskap, forskning, læring m.m.
- Jo mer åpenhet og deling, jo mer robust blir vårt digitale samfunn - så det handler også om at dere tar et aktivt digital samfunns ansvar. Det må ledes.

Nye føringer som man bør være obs på

- I januar 2019 vil vi få en ny sikkerhetslov i Norge. I korte trekk vil den omfatte flere aktører og den vi medføre mer ansvar for de som blir underlagt sikkerhetsloven.
- Men ny sikkerhetslov vil også medføre en domino effekt som følge av at de som er leverandører inn til en aktør som er underlagt sikkerhetsloven – også må forholde seg til sikkerhetsloven og får krav som må tilfredsstilles (eksempelvis leverandørklarering).
- Ny sikkerhetslov vil fremtvinge mer bevissthet om hvorfor vi trenger digital sikkerhet og konsekvens forståelse for hva som kan skje om sikkerheten ikke blir ivaretatt.
- NIS direktivet (Network Information Security) fra EU – har kommet i bakgrunnen av GDPR – men vil også fremtvinge økt ansvar og krav til grunnsikring. (til behandling i EØS)
- Nye lover og føringer både nasjonalt og internasjonalt vil sette føringer for å tenke sikkerhet i de «digitale verdikjedene» vi alle er avhengige av.
- Nye lover og regler vil også medføre mer omtale i media om digital sikkerhet, politikere vil engasjere seg – som igjen vil kunne bidra til å skape forventninger til alle som forvalter digital informasjon.
- Hver enkelt virksomhet må ta mer tydelig ansvar for egen og dermed bidra til å styrke andres digitale sikkerhet.

Noen tips til bruk i hverdagen:

- Abonner på nyhetsmail fra Nasjonal sikkerhetsmyndighet eller Næringslivets sikkerhetsråd – det gir innblikk i de viktigste hendelsene som er på radaren til norske og internasjonale cyber - myndigheter. I tillegg får man info om konferanser og frokostseminarer som det kan være interessant å delta på. Mye effektiv læring som gjør det lettere for deg og din virksomhet å forstå og forebygge cyberhendelser.
- Nyhetsmailer fra NSR/NSM/NorSIS gir også bedre innsikt i ord og uttrykk som brukes, samt hvem som uttaler seg om hva.
- Også viktig å få oversikt over hvordan de ulike myndighetsorganisasjonene jobber og hvem har ansvar for hva – eksempelvis er NSM et direktoratet med makt/tilsyn og samarbeider med andre nasjonale/internasjonale aktører i utveksling av informasjon.
- Politiet er i ferd med å bygge opp et cybersenter Nc3 – følg med på det.
- Internasjonalt: Vær også obs på Europol sin cyber enhet som heter Europol Ec3. Der kan man også finne relevant og verifisert informasjon ved større hendelser + undersøkelser og trusselrapporter.
- Få inn eksterne foredragsholdere som er eksperter på de sikkerhetsområdene som er viktige for dere – bruk også gjerne om mulig demo.
- Vær ikke redd for å dele informasjon om hendelser – det er en del av det digitale samfunnsansvar. (lukket forum kan også etableres innad for bransje)
- Ved cyber hendelser - husk media sitter på spekulasjoner – ikke alltid med fakta ved større cyberhendelser. Og vi må «lære media» å respektere at det tar tid å få verifisert hendelser, omfang og konsekvens. Er du og din virksomhet rammet – så henvis og samarbeid også til myndighetene – dere skal ikke stå alene i en slik situasjon.

Vær føre var:

- Menneske kan ikke oppgraderes på digital sikkerhet så enkelt som en PC. Det tar tid å implementere en felles forståelse, behov for rapportering og vedlikehold av kunnskap. Forebyggende arbeid er evigvarende – men via kommunikasjonstiltak kan det bli spennende, givende og inspirerende. La IT/sikkerhet samarbeide med marked/kom – tenk nytt! Aktivisering skaper engasjement. Etab.er egen sikkerhetspris.
- Les trusselvurderingene fra myndighetene – trekk ut det som berører ditt lederskap og din virksomhet. Omsett til handling, innfør rapportering innad i egen virksomhet og jobb akivt med sikkerhet innen de rammer dere har. Husk at erfaringer dere gjør har betydning for myndigheten. Så hjelp PST og NSM i å bli bedre ved å si i fra hvilke hendelser dere opplever og hva dere trenger for å forebygge enda bedre.
- «When in peace, prepare for war»

Oppsummert

- «Vær og føreforhold» i det digitale rom – hvilke verdier har du og hva skal du beskytte deg mot og hvordan?
- Lær av andre – se hvordan Coop og Finn.no håndterer sikkerhets/svindelutfordringer.
- Lytt til trussel rapportene / vurderinger fra NSM / PST. Men gi også innspill til dem om hva din bransje trenger.
- Se via NSM/NSR/norsis.no hvordan du kan forebygge internt via enkle tiltak og veiledninger som allerede eksisterer.
- Innfør rapportering langs «verdikjeden» din virksomhet er avhengig av og sørg for at digital sikkerhet blir målt. Det er i seg selv bevisstgjørende, forebyggende og gir mulighet for bedre hendelses håndtering om noe skulle ramme virksomheten.

Takk for meg☺