Digital beredskap

Innholdsfortegnelse

Innledning

Kunnskap om og forståelse for informasjonssikkerhet er helt avgjørende i en tid som preges av teknologisk utvikling. I tråd med den teknologiske utviklingen oppdages nye trusler og sårbarheter. Effektivisering av ulike deler i virksomheter, ved delvis eller omfattende digitalisering, kan gjøre virksomheten mer attraktiv og utsatt for blant annet cyberkriminalitet. Dermed er denne artikkelen høyest relevant og verdifull som et steg i å forbygge gjennom bevisstgjøring rundt metodikk og økt kunnskap om digital beredskap og datasikkerhet.

Man er ikke sterke enn det svakeste leddet, gjelder i like stor grad innen datasikkerhet som i konvensjonell militærtaktisk tankegang. Å identifisere svakheter og sårbarheter hos fienden for å kunne utnytte disse til egen fordel er en kjent analysemetode innen militære operasjoner. Til sammenligning gjelder også dette i en digitalisert verden. En angriper som har intensjoner om å hente ut sensitiv informasjon trenger ikke å rette sitt angrep direkte mot toppledelsen i en digital verden. Alle som har tilgang til samme informasjonen er potensielle innslagspunkt og således svakheter i systemet. Dermed er det, for en angriper, tilstrekkelig at én medarbeider ikke har fulgt med i timen når det kommer til datasikkerhet.

Denne oppgave består av to hoveddeler som er inndelt i kapittel 1- sosial manipulasjon og kapittel 2 – spill for bevisstgjøring omkring informasjonssikkerhet. I første kapittel defineres angrepsmetoden sosial manipulasjon (sosial engineering) etterfulgt av refleksjoner rundt hvorfor nettopp denne angrepsmåten blir mer og mer aktuell for angripere. I kapittel 2 vil det henvises til fire spill som omhandler informasjonssikkerhet og bevisstgjøring. Formålet er å vise til hvilke styrker og svakheter disse spillene har, for deretter å reflektere hvorvidt og på hvilken måte, disse spille kan øke bevisstheten om informasjonssikkerhet og cybertrusler. Avslutningsvis vil kapittelet ta for seg betraktninger om hvordan disse spillene kunne vært benyttet i Forsvarets for å øke bevisstheten om informasjonssikkerhet. Forsvaret er valgt som etat grunnet strenge krav om skjerming. Til slutt i artikkelen vil hovedargumentene fremstilles i en oppsummering, etterfulgt av en kort konklusjon.

1 Sosial manipulasjon

Angrepsmetoden som ikke baserer seg på direkte digital angrep mot en virksomhets datasystem kalles Sosial Engineering (SE) eller sosial manipulasjon på norsk (Nätt & Heide, 2017 s.28; NorSiS, 2019, s.36). Metoden handler om å få brukere til å kompromittere informasjon og informasjonssystemer. I motsetning til direkte digitale angrep som retter seg mot en virksomhets datasystemer, er målet med sosial manipulasjon å angripe mennesker som har aksess til informasjon (Krombholz, Hobel, Huber & Weippl, 2014). Hensikten er å manipulere mennesker til å røpe konfidensiell informasjon eller, gå så langt, at andre sier seg villig til å utføre ondsinnede angrep gjennom dårlig innflytelse og overtalelse (Ibid).

Nasjonal sikkerhetsmyndighet (NSM) (2019) er Norges ekspertorgan og det nasjonale fagmiljøet for digital sikkerhet og varslings- og koordineringsinstans for alvorlige digitale angrep og sikkerhetshendelser. Under inntrengningstester utnytter NSM menneskelige sårbarheter med stort hell (Ibid, s.18). I datasikkerhet sammenheng blir den menneskelige faktoren gang på gang ansett til å være sikkerhetens svakeste ledd (Nätt & Heide, 2017, s. 29). Alex Scroxton (2019) peker på forskning som hevder at nesten alle cyberangrep, på et eller annet tidspunkt, er avhengig av at mennesker blir lurt til å gjøre noe. Scroxton viser videre til visepresident for trussel operasjoner ved Proofpoint, som hevder at 99% av cyberangrep er avhengig av menneskelig interaksjon for å utnytte menneskelige feil gjennom skytjenester, e-post eller sosiale medier. Sosial manipulasjon anses dermed som et psykologisk angrep hvor en angriper forleder noen til å gjennomføre en handling som angriperen vil ha utført (NorSIS, 2019, s. 31; Nätt & Heide, 2017, s. 31).

1.1 Sosial manipulasjon blir mer og mer aktuelt

Det er flere ting som gjør sosial manipulasjon mer og mer aktuelt for angripere. Økt teknologisk utvikling gir ikke bare flere muligheter for angrep, det er også med på å vanskeliggjøre angrep ved å stadig forsterke og forbedre beskyttelsen på datamaskiner (NorSIS, 2019, s. 32). Ved å vanskeliggjøre direkte digitale angrep må angripere benytte seg av andre metoder for å lykkes med sine formål. BankID er et relevant eksempel i denne sammenheng siden det benyttes av over fire millioner nordmenn. Denne autentiseringsmetoden er ekstremt krevende for en angriper å trenge gjennom ved «klassiske» digitale angrep. Dermed rettes fokuset på andre sårbarheter som menneskene, der ulike metoder nyttes for å svindle til seg innloggingsdetaljer ved eksempelvis å dirigere brukere til falske sider som kontrolleres av angripere (Ibid).

Sosiale medier gir angripere bedre innsikt om attraktive mål for mer målrettede svindler. De fleste kjenner seg igjen i å bruke facebook eller andre lignende sosiale medier for å finne ut mer detaljer og informasjon om et nylig etablert bekjentskap. Det eneste man behøver er navnet på vedkommende for deretter å taste det inn på facebook og få et innblikk i hverdagen, interessene, hobbyer, nettverk osv. om en tilnærmet ukjent person. Spesielt er det enkelt å finne informasjon om personer som har profiler på internett som er åpen for alle. I tillegg har de aller fleste virksomheter en hjemmeside som gir en oversikt over ledelsen og nøkkelpersoner.

Bedrifter og andre institusjoner er avhengige av å nå sine kunder og forbrukere, dermed velger disse å markedsføre sine tjenester digitalt. Markedsføringen gir angripere den nødvendige informasjonstilgang og er med på å forenkle kartlegging og innhenting av sårbarheter som kan utnyttes. Det betyr at individene selv ikke trenger å publisere informasjonen på egenhånd. Sosial manipulasjon som metode foretrekkes i denne sammenheng fordi metoden blir vanskelig å stoppe, da god og omfattende innhenting gjør angrepene meget persontilpasset (NorSiS, 2019-2020, ss. 25-32; Nätt & Heide, 2017, s. 31-34).

Gode forberedelser kan gi dypere aksess mot en virksomhet, uten at angripere nødvendigvis må jobbe mot avanserte digitale sikkerhetstiltak. Alex Scroxton (2019) viser til Proofpoint sin *human factor* rapport der man har utført undersøkelser som tydeliggjør hvem som blir mål for angripere. I rapporten brukes benevnelsen «very attacked people» (VAP) om de menneskene i en virksomhet som er gjenstand for angrep. Det som skiller disse individene er at de, som regel, befinner seg dypt i en organisasjon, har tilgang til økonomi eller sensitiv data og har synlige profiler eller identiteter som er tilgjengelige på organisasjonens webside, sosiale medier, publiseringer eller til og med via google søkemotor (Ibid). I denne sammenheng blir sosial manipulasjon som metode foretrukket både fordi angripere kan få en dypere aksess, og fordi de unngår å jobbe mot avanserte sikkerhetstiltak.

Sosial manipulasjon må også ses opp mot faren for å bli avslørt. Datakriminalitet skiller seg ut fra generell kriminalitet på områder som *avstand, automatisering, teknologisk spredning, enkelt å skjule spor og distanse til offeret* (Nätt & Heide, 2017, s. 18-19). Datakriminelle kan nå sine ofre over hele verden, samtidig som maskinkraften muliggjør at programmer automatisk kan forsøke å svindle hundretusenvis av brukere samtidig. Teknologisk spredning gjør at det tar lengre tid for virksomheter å lage og distribuere sikkerhetsfikser til brukerne.

Digital informasjon legger ikke igjen fysiske spor. Selv om deteksjon av endringer ved eksempelvis logging er gjennomførbare, er dette noe dyktige angripere kan manipulere bort etter at angrepet er gjennomført. Den fysiske distansen til ofrene er også med på å lette samvittigheten til datakriminelle, det er lett å tenke at offeret «bare» er et dårlig sikret system (Ibid). Det sier seg selv at angripere foretrekker en angrepsmetode der risikoen for å bli avslørt er lavest mulig.

Manglende kunnskap om datasikkerhet og dårlig sikkerhetskultur er med på å aktualisere sosial manipulasjon. Manglende kunnskap er som oftest ikke et godt utgangspunkt. Når mennesker ikke kjenner til eller forstår hva datasikkerhet er, er det naturlig å anta at de blir usikre. Usikkerhet i kombinasjon med manglende kunnskap øker frykten for at noen skal ta over kontoen vår, eller installere løsepengevirus. Samtidig har folk en holdning om at det er vanskelig og nærmest en heldagsjobb å sikre seg i tilstrekkelig grad mot stadig nye trusler (NorSIS, 2019, s. 4; Nätt & Heide, 2017, s. 25-26). Ifølge NorSIS (2019, s. 39) benytter sosial manipulasjon seg av grep som tillit, frykt og fristelser. Angripere utnytter tillit ved å utgi seg til å være en avsender som vi kjenner eller stoler på, de er kapable til å skremme oss til å utføre en handling som å laste ned et program for å bli kvitt et påstått virus, og de frister med gratis programvarer eller spill som lurer oss til å oppgi personopplysninger.

Sosial manipulasjon kan utføres ved å ta i bruk flere ulike medier. Typiske medier for denne typen svindel kan være e-post, sosiale nettverk, nettprat-tjenester, nettsider (inkludert kopier), telefon, brev og fysisk oppmøte (Nätt & Heide, 2017, ss. 31-34). Som nevnt tidligere er formålet å utnytte og manipulere menneskers sårbarheter. Vi mennesker er sårbare for autoriteter, seksualdrift, økonomi og grådighet, frykt og krisesituasjoner, nysgjerrighet og tillit (Ibid). I neste kapittel skal vi se nærmere på hvordan bevisstgjøring, ved bruk av spill, omkring våre sårbarheter og informasjonssikkerhet kan være med på å redusere risikoen for at vi faktisk blir lurt eller svindlet.

2 Spill for bevisstgjøring omkring informasjonssikkerhet

I denne delen av besvarelsen er utgangspunktet fire spill som har til hensikt å bevisstgjøre og øke brukerens kunnskap innen informasjonssikkerhet. De fire spille er: 1) Nettfiske- test. Er du smartere enn en nettsvindler? 2) Hvor utsatt er du for ID-tyverie? 3) The Weakest Link: A User Security Game, og 4) Cyber Awerness Challenge 2019. I det følgende vil det vises til konkrete styrker og svakheter ved spillene, for deretter å reflektere hvorvidt og på hvilken måte disse spillene kan øke den enkeltes bevissthet om informasjonssikkerhet og cybertrusler.

Til slutt presenteres noen betraktninger om hvordan disse spillene kunne vært benyttet i Forsvaret.

2.1 Styrker og svakheter ved de fire spillene

Nettfiske-test, er du smartere enn en kriminell? De fleste har opplevd å få tilsendt en e-post som både inneholder noe vi ikke var forberedt på og i tillegg sendt fra en ukjent avsender eller henviser til en mistenkelig nettside. Dette spillet har tatt for seg phishing som svindlemetode. Phishing har som formål å lure brukeren til å oppgi brukernavn og passord, betalingsinformasjon o.l. gjennom forholdsvis troverdige kopier av e-post og nettsider (Nätt & Heide, 2017, s. 46). Spillet inneholder åtte eksempler med tilhørende forklaring til hva brukere skal se etter for å oppdag om innholdet er et forsøk på phishing eller ikke.

En av styrkene ved dette spillet er at det er laget med fokus på enkelhet og brukervennlighet. Etter at brukeren velger sitt foretrukne språk, blir han/hun bedt om å lage et fiktivt brukernavn og e-postadresse, ved å gå videre derfra starter man rett på første case. Brukerne kan ta den tiden de trenger for å finne ut om det de har foran seg er phishing eller legitimt. Når valget er tatt får brukeren umiddelbart svar på om det var korrekt eller feil. Uavhengig om svaret var rett eller galt blir viser spillet «fasiten» som fører til rett svar.

Informasjonen til brukerne i de ulike casene er også en styrke. Brukeren har ikke noe valg om å gå videre uten at fasiten blir presentert. Dermed vil selv de travleste av oss bli nødt til å klikke «neste» og faktisk få med seg verdifull informasjon. Gjennomgangen i hver case er detaljert og relevant for å lære hvordan en kan avsløre phishing. Spillet viser både den enkleste varianten av phishing, der brukeren får varsel om å endre passord fordi noen angivelig har forsøkt å logge seg inn et sted med brukerens passord. I tillegg en metode der e-posten inneholder en lenke til en nettside, opplysninger som gis på nettsiden blir sendt til svindleren. Spillet og dets innhold er dagsaktuelt og treffer dermed de aller fleste brukere.

Det er likevel en svakhet at spillet bare dekker et relativt snevert område innen informasjonssikkerhet. Her er fokuset utelukkende på phishing ved bruk av e-post. Med kun åtte eksempler tar det veldig kort tid å klikke gjennom spillet. Man kunne med fordel laget et noe lengre spill som dekket flere andre metoder enn phishing. Eksempelvis hadde det vært en fordel om spillet også tok for seg *nettsider* og hvordan lage gode *brukerkontoer og passord*. Det kunne tilført spillet noe mer substans og kunne muligens også vært et hjelpemiddel i undervisningssammenheng.

Når spillet kun har phishing som moment ville det vært en stor fordel med en oppsummering over læringsmålene, og en påminnelse om hva brukerne skal være oppmerksom på. Eksempelvis kunne sjekklisten for phishing blitt presentert slik som Nätt & Heide (2017, s. 49) har gjort det:

- Klikk aldri på lenker i en e-post. Gå heller til tjenestens nettside ved å skrive inn nettadressen i nettleseren.
- Ingen seriøse aktører ber deg oppgi kontoinformasjon eller utføre handlinger via e-post.
- Mistenker du at noen har svindlet deg på denne måten, sørg for å bytte passord alle steder der passordet er brukt.
- Benytt om mulig egne e-postadresser til kritiske tjenester. Dermed kan phishing-forsøk avsløres ved at de blir sendt til «feil adresse».

På denne måten ville brukerne blitt presentert en kort oppsummering etter endt spill, og har anledning til å reflektere over noen få hovedmoment mens eksemplene enda er ferskt i minne.

Hvor utsatt er du for ID-tyveri, kan vanskelig kalles et spill. Websiden NettVett.no bruker *quiz oversikt* i introduksjonen når brukeren trykker seg videre fra linken på canvas og velger *alle tester*. Går brukeren videre med «quizen» *hvor utsatt er du for ID-tyveri,* presenteres 11 ulike temaer: lommeboken, postkassen, spredning av personlig informasjon, PC-en, netthandel, mobiltelefonen, passord og koder, fødselsnummer, bank- og kredittkort, personlig informasjon, kredittverdighet og vurdering. Hvert tema inneholder alt fra tre til seks spørsmål. Når testen er avsluttet blir brukeren presentert med testresultatet med en oversikt over spørsmålene og valgt svaralternativ. Brukeren får også en score som forteller noe om avviket fra svarene i forhold til fasiten.

Testen er laget på en ryddig og strukturert måte. Fremstillingen er med på å styrke testen og sørger for at brukerne får en bevisstgjøring omkring sine handlinger, holdninger og kunnskaper, sett opp mot ID-tyveri. Årlige undersøkelser utført av NorSIS og Skatteetaten viser at over 100 000 nordmenn har vært utsatt for ID-tyveri (NorSIS, 2019, s. 19). Testen tar høyde for at ID-tyveri blir utført av personer som er i nær relasjon, samt kriminelle. I tillegg til at det kan ramme både virksomheter og privatpersoner (Ibid). Dermed egner denne testen seg for alle ferdighetsnivåer og oppnår målsettingen med økt bevisstgjøring, holdninger knyttet til personopplysninger og kunnskap om ID-tyveri.

Testen skiller i mindre grad mellom hva som er forhåndsregler og hvilke tiltak brukerne skal iverksette når de er rammet av ID-tyveri. Dette, samme med at spørsmålene og korrekt svar oppleves for enkle og ledende, er store svakheter med denne testen. Dersom brukerne er

forberedt på et spill vil de umiddelbart bli skuffet i møte med NettVett sin test for ID-tyveri. Ser man bort fra sistnevnte ville en tydeligere fremstilling av forholdsregler og tiltak når brukerne er rammet, styrket testen. Testresultatene til slutt kunne vært delt slik at temaene ble oppsummert med forholdsregler og tiltak. Alternativt hadde det vært en fordel om de viktigste læringsmålene brukerne skal ta med seg videre kom tydeligere frem. Som et eksempel vises det til NorSIS (2019, s.19) sine forholdsregler:

- Ikke oppgi personlig informasjon til ukjente over internett, på telefon eller e-post.
- Klikk aldri på lenker i e-poster for å legge inn personinformasjon. Skriv heller adressen til nettstedet rett inn i adressefeltet i nettleseren din.
- Sikre dine kontoer for e-post og nettsamfunn med totrinnsbekreftelse.
- Lås postkassen din for å hindre tyveri av personopplysninger.

På lik linje kunne testen tatt høyde for og presisert hvilke tiltak som kan og bør gjøres når brukerne er rammet. Igjen vises det til NorSIS som er konkret i sine anbefalte tiltak (Ibid):

- *Vær rask.* Hva er forsvunnet/misbrukt av informasjon og identitetsdokumenter?
- *Anmeld forholdet*
- *Ta kontakt med banken*
- *Be om frivillig sperring*
- *Følg nøye med på postgangen*
- *Bruk ID-tyveri forsikringen.*
- *ID-tyveri på nett*, reager umiddelbart dersom du mottar informasjon om at det er opprettet en konto i ditt navn eller at brukerrettighetene for din konto er endret.

The Weakest Link er tidlig ute med sitt budskap om at det svakeste leddet i en bedrift sitter mellom stolen og tastaturet. Med utgangspunkt i første arbeidsdag, i en ny jobb, blir brukeren eksponert for ulike scenarioer som det må tas stilling til. Spillet er laget med 23 arbeidsdager, der brukeren må ta stilling til ett nytt scenario for hver dag. Etter at svaret er avgitt får brukeren direkte tilbakemelding med symbolene tommel opp eller ned, etterfulgt av en grundig forklaring. I tillegg har brukeren valget om å lese mer for ytterligere utfyllende informasjon.

Styrken i dette spillet er måten det belyser og bevisstgjør utfordringene som kan ligge i medarbeidere som er opptatt av, og påpeker sikkerhetstrusler gjennom en arbeidsperiode. De fleste har kjent på en følelse av at sikkerhetstiltakene, til en viss grad, er tidkrevende og vanskeliggjør et ønske om fleksibilitet. Istedenfor å oppgi brukernavn og passord til en kollega man har tillit til, og som kan hjelpe med å få sendt en e-post mens man selv er sykt, er man nødt til å vente til en selv er tilbake på jobb. Innloggingsdetaljer skal aldri oppgis til noen selv om man anser at faren er minimal (Nätt & Heide, 2017, s. 103; NorSIS, 2019, s. 19). Det

kan friste og røpe det likevel fordi man tenker at passordet enkelt kan endres ved første anledning. Særlig utfordrende kan det være dersom det på en eller annen måte påvirker andre kolleger og venner på arbeidsplassen. Spillet bevisstgjør på en utmerket måte hvilke konsekvenser manglende sikkerhetsbevissthet og dårlig sikkerhetskultur kan ha for en bedrift. I så måte er dette et ypperlig spill for å få medarbeidere og kolleger til å tenke og handle helhetlig. En helhetlig tilnærming er essensielt i arbeidet med å utvikle en god sikkerhetskultur hos alle ansatte.

Fravær av oppsummering etter endt spill er en av svakhetene. Etter omfattelende scenarioer der brukerne tar stilling til forskjellige handlinger, sitter man til slutt igjen med en score og en kort kommentar som konkluderer i hvilken grad brukeren er tilstrekkelig sikkerhetsbevisst til å ikke være det svakeste leddet. Spillet er laget som en blanding mellom test og eksempler fra virkelige situasjoner man kan havne i, dermed burde det også følge en oversikt over hvilke handlinger eller fravær av disse, som utgjør en sikkerhetsrisiko for virksomheter generelt, eller spesielt for denne bedriften.

For mye tekst gjør det vanskelig å memorere eksemplene fra spillet. Det er også en svakhet at spillet ikke har klart å visualisere scenarioene ved eksempelvis å bruke enkle animasjoner eller skisser. Når brukeren leser de ulike scenarioene dannes det ulike bilder ut ifra erfaring fra tilsvarende situasjoner som spillet forsøker å sette brukeren inn i. Ved å anvende enkle animasjoner, skisser eller tegninger ville spillet i større grad lykkes med å gi brukerne samme utgangspunkt og referanse. Samtidig husker mennesker generelt mye bedre noe som er visualisert, kontra i tekstform.

Cyber Awareness Challenge er et gjennomført og omfattende spill, der hensikt er å gi en innføring i retningslinjer og tiltak (best practice) fra det amerikanske forsvarsdepartementet innen cybersikkerhet. Målgruppen for dette spillet er alle autoriserte brukere av det amerikanske forsvarsdepartementets informasjonssystemer, samt medlemmer av etterretningskomiteen. Gjennom spillet får brukerne en grundig og innholdsrik bevisstgjøring innen mange relevante temaer.

Det tar ikke lang tid å fullføre spillet dersom man går rett på de ulike temaene, uten å sette seg inn i bakgrunnsinformasjonen. Målsettingen med spillet er å bevisstgjøre brukerne i risikofylte handlinger og gi anbefalinger slik at departementet, etterretningskomiteen, personlig informasjon og informasjonssystemer er best mulig sikret. På spillets hjemmeside er følgende fire mål presentert (1, 2020):

- Identify cybersecurity and why it is important.
- Identify the different types of information and the requirements to protect each content type.
- Identify the different forms and methods of cyber attacks.
- Identify the types of technologies that are particularly vulnerable to attacks.

Med sine fem hovedkategorier og 12 underkategorier dekker spillet og bakgrunnsinformasjonen de ovennevnte målene på en god måte og anses derfor som en styrke ved dette spillet.

Svakheten med et såpass omfattende spill er den trege fremdriften. Dette kommer særlig frem når man svarer feil. Da går mye av tid til «loading» og innføring ved bruk av animasjoner som ikke gir noe særlig utbytte. Spesielt plagsomt er det i de tilfellene der introduksjonsvideoen ikke trengs for å besvare spørsmålene i etterkant. Man sitter igjen med en følelse av å ha gjennomført et tungt og trengt spill, der mye av tiden har gått med på venting.

Siden spillet er laget for en spesiell målgruppe oppfattes det akademiske nivået på språket som krevende. For noen som ikke behersker engelsk på et relativt høyt nivå vil det være veldig vanskelig å forstå alle fremmedordene. I tillegg er det mange forkortelser og spesielle benevnelser som antagelig benyttes på departementsnivå. Det kan skape forvirring og vil kreve at man setter seg inn i bakgrunnsinformasjonen. Samtidig kan man anse dekningsgraden som en svakhet. Altså at de som ikke forholder seg til gradering og graderte dokumenter ikke vil ha dirkete nytte av spillet.

2.1 Hvorvidt, og på hvilken måte, kan disse spillene øke den enkeltes bevissthet om informasjonssikkerhet og cybertrusler?

Disse spillene øker den enkeltes bevissthet ved å tilføre kunnskap og forståelse om informasjonssikkerhet og cybersikkerhet. Menneskers hukommelse er knyttet til både følelser og stedsorientering (Nordengen, 2017). Spill er med på å skape en virtuell verden der opplevelser på en måte virkeliggjøres. Et spill som er godt utviklet tillater brukeren å entre et virtuelt miljø som er tilnærmet lik virkeligheten. På den måten vil brukeren kunne overføre læring fra det virtuelle miljøet til den virkelige verden. I tillegg kan spill motivere brukere med å gi de mål som de må oppnå og se konsekvenser av sine handlinger uten at disse straffer seg i den virkelige verden (Alotaibi, Furnell, & Papadaki, 2016).

Dersom spillet er laget på en måte som øker hukommelsen og er virkelighetsnær vil brukeren sitte igjen med en mye høyere grad av læring, og dermed være i stand til å sikre seg bedre mot digitale angrep (Mayhorn & Nyeste, 2012). I studien til Mayhorn og Nyeste (2012) viser de til

sammenhengen mellom økt kognitiv kapasitet gjennom spill, sett opp mot økt bevissthet omkring informasjonssikkerhet og cybersikkerhet. Gjennom funnene i studien hevder de at selv enkle spill som fokuserer på bevisstgjøring har en positiv effekt, og er en god måte for å redusere risikoen for å bli lurt eller svindlet (Ibid).

Bevisstheten blir økt ved at spillet engasjerer og fenger oppmerksomhenen til den enkelte. Derfor må bevisstgjøringspillet lages på en slik måte at det møter behov som er i konstant endring, og tar i betrakting ulike livsstiler og kulturelle forhold (Alotaibi et.al, 2016). Seriøse spill har en klar hensikt og mål som brukeren skal oppnå. Slike spill er ikke kun ment som underholdning, og derfor kan man anta at disse spillene i mindre grad er fengende (Ibid). Rasjonale bak seriøse spill kan ses i sammenheng med at den enkeltes interesse for fagfeltet, samt økt bevissthet om digitale trusler utover i spillet ligger i bunn som motivasjon for å gjennomføre spillet. Det man søker å oppnå er en atferdsendring, av den grunn legges det som en forutsetning at motivasjon for å gjennomføre spillet er tilstede. Er motivasjonen og forståelsen av viktigheten med å søke kunnskap gjennom spillet tilstede, kan spillet med enklere grep fremstå som engasjerende, nettopp grunnet en underliggende interesse for digital sikkerhet.

Sammenlignet med 3D virtuelle spill og simulasjonstrening er disse spillene nokså svake. Selv om budskapet i spillene er relevant og har forankring i virkeligheten har formidlingen og bevisstgjøringen gjennom disse spillene et stykke å gå, sett i sammenheng med hva som finnes på markedet. Profesjonelle og seriøse spill som er tilgjengelighet 24/7 og er laget på en slik måte at brukeren kan få profesjonell veiledning underveis, med online simulasjonstrening som reflekterer en reel arbeidssituasjon gir best effekt (Ariyapperuma & Minhas, 2005). Spill som tar utgangspunkt i simulasjonstrening motiverer brukerne til å visualisere, eksperimentere og være kreative (Mitchell & Savill-Smith, 2004). Derigjennom øker effekten og bevisstgjøringen omkring informasjonssikkerhet og cybersikkerhet. Til tross for at spillene som denne artikkelen tar utgangspunkt i ikke nytter 3D virtuelle hjelpemidler, er det som tidligere nevnt flere andre elementer som øker bevisstheten gjennom spill. Kombinasjonen video, audio og tekst som nyttes i spillene er med på å gi god og verdifull kunnskap, samt øke forståelsen for informasjonssikkerhet og cybersikkerhet (Ibid).

2.3 Kan spill benyttes i Forsvaret for å øke bevisstheten om informasjonssikkerhet? På hvilken måte ville bevisstgjøringsopplegget vært organisert?

Arbeidet med økt bevissthet omkring informasjonssikkerhet og cybersikkerhet krever en helhetlig tilnærming. Digital sikkerhet er på agendaen også i regjeringen. Norge skal være i front med å utvikle og levere digitale tjenester til innbyggere og næringsliv. En forutsetning for vellykket digitalisering, er at det skjer innenfor rammen hvor digital sikkerhet og personvern ivaretas (Justis-, 2019). I januar 2019 la regjeringen fram en nasjonal strategi for digital sikkerhet og en nasjonal strategi for digital sikkerhetskompetanse (Ibid). Strategien beskriver tiltak for til sammen om lag 1,6 milliarder kroner. Av denne summen går nesten halvparten til kompetansetiltak. Slike kompetansehevende tiltak har truffet Forsvarsetaten på lik linje som mange andre bedrifter og virksomheter i Norge. Erfaringsmessig har forsvarsansatte et dårlig forhold til datasikkerhet. Årsaken til dette er, blant annet, en antagelse om at denne type forebyggende og bevisstgjørende arbeid er tidkrevende og begrenser aktiviteter og handlingsrom heller enn å gi muligheter.

Denne artikkelen har allerede belyst at det svakeste ledd i alt sikkerhetsarbeid, som regel, er et menneske. Noe datakriminelle vet å utnytte. Vår akilleshæl, som brukere av digitale verktøy er uoppmerksomhet, latskap, kunnskapsløshet og altfor stor tiltro til våre medmennesker (Godejord, 2019; Nätt & Heide, 2017, s. 31-34). I Forsvaret ser man tendenser til dårlig sikkerhetskultur. Bakgrunnen for dette er både manglende kunnskap, men i like stor grad en «dette skjer ikke oss» tankegang som kan være direkte farlig. Den økonomiske faktoren har i denne sammenheng, dessverre, også en stor betydning. Noe forenklet kan man fremstille økonomiforvaltningen som bra når det brukes midler til å skape kampkraft, og unødig når det skal brukes på forebyggende arbeid med «data-ting».

Spill som bevisstgjøringsmetode er billigere enn mange andre undervisningsmetoder som eksempelvis kurs og foredrag (Alotaibi et.al, 2016). Det er dessverre slik i Forsvaret, som i mange andre virksomheter, at det ikke alltid passer for absolutt alle å delta på foredrag eller kurs som gjerne avholdes i bestemte tidsperioder, og med en viss varighet. Dermed oppstår det «hull» i kompetansehevingen og bevisstgjøringen omkring forebyggende tiltak i datasikkerhet. Dersom Forsvaret i større grad kan nyttiggjøre seg av spill som bevisstgjøringsmetode, bør slike spill være tilgjengelig 24/7. Denne typen bruk av spill vil både redusere kostnadene knyttet til kompetanseheving, samtidig øke sannsynligheten for at informasjonen blir tilgjengelig for flere brukere og dermed ha en helhetlig bevisstgjøringsmetode.

I tillegg er spill mer engasjerende og gir dermed bedre effekt hos flere brukere (Mitchell & Savill-Smith, 2004). Særlig effektivt kan spillene være dersom disse skreddersys for å treffe på de områdene som er mest aktuell for forsvarsansatte (Ibid). I Forsvaret er det stor divergens i kunnskapsnivået omkring digital beredskap og informasjonssikkerhet. Forsvarsansatte som til daglig arbeider med digital sikkerhet har et annet bevisstgjøringsbehov, kontra de av oss som har andre ansvarsområder. Det er ikke dermed sagt at ikke alle kan dra nytte av spill som bevisstgjøringsmetode. Spill for bedrifter og virksomheter med høyere forståelse og kunnskap innen datasikkerhet omhandler i stort, forebygging av datatap og informasjonsbehandling (Alotaibi et.al, 2016). Forsvarsansatte som ikke direkte jobber med informasjonssikkerhet og ikke har den samme interessen for datasikkerhet, vil trenge, og ha god effekt av, spill som bevisstgjøringsmetode dersom spillet er laget på en fengende og kunnskapsrik måte. Det er også naturlig å anta at dersom spillet er skreddersydd til å bevisstgjøre omkring de farene som berører den enkeltes ansvarsområder, vil spillet ytterligere aktualiseres og motivasjonen for å fullføre spillet være forhøyet.

Den beste måten å bekjempe cyberkriminalitet på er å øke bevisstheten og forholde seg til informasjonssikkerhetsrutinene (Ibid). Er det noe Forsvaret, i fredstid, er gode på så er det etablering av rutiner. Ved å innføre spill som bevisstgjøringsmetode vil det erfaringsmessig ta kort tid før spillet etablerer seg som en rutine og krav for forsvarsansatte. Det som allikevel vil være vesentlig ved innføring av spill som undervisningsmetode for økt kunnskap og forståelse, er erkjennelsen av endringer som følge av den teknologiske utviklingen og hvilke ressurser som vil kreves for å opprettholde spillets relevans (Ibid). For dersom spillet mister sin relevans vil brukerne fort neglisjere trusselen datakriminalitet utgjør. Av den grunn må Forsvaret tilrettelegge og ha et system for oppdateringer, justeringer og validering av de spillene der formålet er å øke den enkeltes kunnskap og forståelse om datasikkerhet (Ibid).

Implementering av spill som bevisstgjøringsopplegg bør inneholde fire steg (SEORG, 2018). Første steget bør bestå av forberedelser, der målet er å kartlegge svakheter ved de systemene og rutinene som gjelder i dag. Manglende kunnskap er i denne sammenheng også ansett som en stor svakhet. Simulerte angrep er en god måte å kartlegge svakheter på. Slike angrep kan være rettet mot den enkelte eller mot systemene. Andre steget er å utvide rapporteringsrutinene for å danne et godt datagrunnlag for hvordan de ansatte responderer mot slike simulerte angrep. Tilbakemeldinger fra de ansatte vil være verdifull informasjons for å kunne skreddersy et solid spill. Tredje steget er å identifisere hvilke avdelinger eller grupper av ansatte som er mest utsatt. Eksempelvis vil de avdelingene som ikke behandler gradert

informasjon, være mindre sårbare og utsatt for tap av sensitiv informasjon. Fjerde steget vil, basert på resultatene fra simulerte angrep og tilbakemeldinger fra de ansatte, utvikle en kontinuerlig evaluering- og utviklingsprosess for å forebygge og vanskeliggjøre angrep gjennom økt bevisstgjøring.

Etter kartlegging av svakheter og identifisering av behov, bør bevisstgjøringsopplegget organiseres slik at det er tilgjengelig for både nye ansatte og de som allerede har en ansettelse. Det holder ikke å innføre et spill for alle nye dersom de av oss som, helt sikkert, har tillagt oss vaner og uvaner får lov til å holde på som vi «alltid» har gjort. Vi vil, i en kompetansehevende sammenheng, utgjøre store hull i sikkerhetsarbeidet og hindre at spillet blir dekkende for en helhetlig bevisstgjøring i Forsvarssektoren. Videre må spillet som bevisstgjøringsmetode forankres i ledelsen og pålegges utført av alle forsvarsansatte. Det kan ikke være opp til den enkelte avdelingssjef å avgjøre om det er behov for kompetanseheving eller ikke. I Forsvaret er allerede den nødvendige teknologien for å kommunisere med alle ansatte på plass gjennom tonivå intranett. Her gjelder det i teorien «kun» å finne det mest relevante spillet og trykke play.

Oppsummering og konklusjon

Sosial manipulasjon eller Sosial Engineering (SE) er en angrepsmetode som ikke baserer seg på direkte digital angrep mot en virksomhets datasystem. Denne angrepsmetoden blir stadig mer og mer aktuell for datakriminelle. Det har sammenheng med den teknologiske utviklingen, som på mange områder vanskeliggjør direkte digitale angrep ved å beskytte datasystemene til brukerne bedre. Dermed benytter angripere andre metoder, som sosiale medier. Gjennom sosiale medier klarer angripere å finne attraktive mål og være mer målrettede i sine angrep. Datakriminelle kan samtidig få en dypere aksess mot en virksomhet, uten å jobbe mot avanserte digitale sikkerhetstiltak. Dermed aktualiseres angrepsmetoden også ved at det kan være tidsbesparende, i tillegg mindre risikofullt. Angrepsmetoden gir muligheter for å utføre automatiserte angrep uavhengig av avstand til offeret, samt gode muligheter for å skjule egne spor. Typiske medier for sosial manipulasjon er e-post, sosiale nettverk, nettprat-tjenester, nettsider, telefon, brev og fysisk oppmøte. Lavt kunnskapsnivå om datasikkerhet og dårlig sikkerhetskultur hos brukerne er selvsagt medvirkende til valgt angrepsmetode.

I andre del av besvarelsen belyses styrker og svakheter ved fire spill som har til hensikt å bevisstgjøre og øke kunnskap innen informasjonssikkerhet.

1) *Nettfiske- test. Er du smartere enn en nettsvindler?* Styrkene i dette spillet er brukervennlighet, ved at det er veldig enkelt laget samtidig som brukeren sitter igjen med god og relevant informasjon innen tematikken. Dessverre tar spillet kun for seg phishing som sårbarhet. I tillegg ville en oppsummering av læringsmålene til slutt vært en fin huskeliste for brukeren.

2) *Hvor utsatt er du for ID-tyveri?* Allerede ved første øyekast oppleves dette som en test heller enn et spill. Likevel er det laget og fremstilt på en ryddig og strukturert måte. Testen belyser hvilken innvirkning handlinger, holdninger og kunnskaper har for ID-tyveri. Største svakheten er manglende skille mellom hva som er forhåndsregler og tiltak som kan iverksettes dersom man allerede er rammet av ID-tyveri.

3) *The Weakest Link: A User Security Game*. Spillet belyser utfordringer vi mennesker kan møte på når vi er på jobb. Det er en styrke at den mellommenneskelige faktoren blir belyst. Svakheten i dette spillet er den store mengden tekst som er benyttet. Omfattende bruk av tekst går på bekostning av virkemidler som kan visualisere temaet.

4) *Cyber Awareness Challenge 2019*. Dette spillet har en klar målgruppe og er skreddersydd for denne målgruppen. Jobber man derimot ikke med graderte dokumenter eller for det amerikanske forsvarsdepartementet, eller etterretningskomiteen kan informasjonen i spillet være av liten verdi. I tillegg oppleves fremdriften av spillet tregt, både fordi det bruker lang tid på å laste, men også språket som er brukt.

Artikkelen har belyst flere fordeler ved å anvende disse spillene som bevisstgjøringsmetode. Spill formidler kunnskap og forståelse om informasjonssikkerhet og cybersikkerhet på en engasjerende og fengende måte. Ved bruk av godt utviklede spill blir brukeren satt i en virtuell verden som er tilnærmet lik virkeligheten. Der forsterkes følelsene og stedsorienteringen og på den måten husker mennesker informasjonen bedre. Spill kan også lages på en slik måte at de møter den enkeltes endrede behov, livsstil og kulturelle forhold. Fordelen med spill, i motsetning til foredrag og kurs, er at disse kan være tilgjengelige 24/7, og lages slik at brukeren kan få veiledning av eksperter underveis, i tillegg kan spill simulere den enkeltes reelle arbeidsforhold og ha dette som utgangspunkt for spillet.

Forsvaret ville i stor grad kunne nyttiggjøre seg av spill som bevisstgjøringsmetode. Det er særlig to faktorer ved spill som aktualiserer metoden. Det første er økonomiske besparelser. I dag bruker Forsvaret mye tid, ressurser og penger på kompetanseheving innen datasikkerhet. Kunnskap om datasikkerhet formidles gjennom kurs, foredrag og avdelingenes egne rutiner

pålagt av sikkerhetsseksjonen. Spill som bevisstgjøringsmetode hadde hatt en umiddelbar effekt med å avlaste diverse kurs og foredrag. Den andre faktoren er at spill kan skreddersys til de ulike forsvarsansattes ansvarsområder. På denne måten ville spillene reflektere reelle forhold den enkelte kan bli utsatt for i sin nåværende stilling.

Organisering av spill som bevisstgjøringsmetode må ta høyde for og erkjenne endringer i angrepsmetodene som følge av teknologisk utvikling. Derfor må det identifiseres hvilke ressurser som vil kreves for å opprettholde spillets relevans. Forvaret må tilrettelegge og ha et system for oppdateringer, justeringer og validering av spillene der formålet er å øke den enkeltes kunnskap og forståelse om datasikkerhet.

Implementering av spill som bevisstgjøringsopplegg bør starte med å kartlegge svakheter ved de systemene og rutinene som eksisterer i dag. Dernest bør det utvikles rapporteringsrutiner for å danne et godt datagrunnlag for aktuelle områder spillene vil ha effekt. Når dette er på plass vil det være like viktig å identifisere hvilke avdelinger eller grupper som er mest utsatt. Som et eksempel vil det ha liten verdi å lage et spill som omhandler behandling av gradert informasjon, for personelle som ikke behandler denne type informasjon. Til slutt bør en implementering av spill først gjennomføres når det er utviklet et system som ivaretar kontinuerlig evaluering og utvikling av spillene.

Denne artikkelens konklusjon er at mennesket definitivt har en sentral rolle i datasikkerhetsarbeid. I tillegg til at mennesker har ulike sårbarheter, er kunnskap og forståelse omkring datasikkerhet avgjørende for en helhetlig tilnærming til bevisstgjøringsarbeid. Spill som bevisstgjøringsmetode er høyest aktuelt og bør bli en sentral del i undervisningssammenheng og metode for økt bevisstgjøring.

Litteraturliste

Alotaibi, F., Furnell, S., & Papadaki, M. (2016). A Review of Using Gaming Technology for Cyber-Security Awarness. *International Journal for Information Security Research (IJISR)*, 660-666.

Ariyapperuma, S., & Minhas, A. (2005). *Internet Security Games as a Pedagogic Tool for Teaching Network Security.* Indianapolis: IEEE Frontiers in Education Conference.

Godejord, P. A. (2019, mars 24). *Digital beredskap – et spørsmål om bevisstgjøring*. Hentet fra blogg.nord.no: https://blogg.nord.no/didaktiskebetraktninger/2019/03/24/digital-beredskap-et-sporsmal-om-bevisstgjoring/

Justis-, b. o. (2019, Februar 12). *Digital sikkerhet.* Hentet fra Regjeringen.no: https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/digital-sikkerhet/id2340011/

Katharina Krombholz, H. H. (2014). Advanced Social Engineering Attacks. *Journal of information Security and Aplications*, 11.

Leyden, J. (2004, September 3). *Old PCs are goldmine for data thieves.* Hentet fra The Register: https://www.theregister.co.uk/2004/09/03/old_pcs_not_wiped/

Mayhorn, C. B. (2012). *Training users to counteract phishing*. Hentet fra Department of Psychology: https://content.iospress.com/download/work/wor1054?id=work%2Fwor1054

Mitchell, A., & Savill-Smith, C. (2004). *The use of computer and video games for learning.* London: Learning and Skills Development Agency.

Nordengen, K. (2017). *Hjernen er stjernen.* Kagge.

NorSiS. (2019-2020). *Trusler og trender*. Hentet fra Flliphtml5. Få en tryggere digital hverdag: http://online.fliphtml5.com/uwwnn/fxil/#p=1

NSM, (. s. (2019). *Helhetlig digitalt risikobilde 2019.* Hentet fra Årets rapport: Nasjonal sikkerhetsmyndighet: https://www.nsm.stat.no/globalassets/rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf

Nätt, T. H., & Heide, C. F. (2017). *Datasikkerhet: Ikke bli svindlerens neste offer*. Oslo: Gyldendal.

SEORG. (2018, Desember 10). *Security through education.* Hentet fra Don’t Overlook the Human Element in Security Training and Awareness: https://www.social-engineer.org/general-blog/dont-overlook-the-human-element-in-security-training-and-awareness/

Scroxton, A. (2019, September 9). *Social engineering a factor in virtually all cyber attacks, report claims.* Hentet fra ComputerWeekly.com: https://www.computerweekly.com/news/252470384/Social-engineering-a-factor-in-virtually-all-cyber-attacks-report-claims

1, W. (2020, mai 3). *Cyber Awareness Challenge*. Hentet fra DoD: https://dl.dod.cyber.mil/wp-content/uploads/trn/online/cyber-awareness-challenge/index.html