Veileder for informasjonssikkerhet **Grafisk bransjeforening**

Verden er i stadig endring. Krig, klimakatastrofer og uenigheter mellom stormaktene skaper mye usikkerhet. Samtidig har det skjedd mye på teknologifronten som sjeldent havner på fremsidene av de store avisene. Antall cyberangrep har økt, også i Norge. Angriperne forsøker ofte å finne minste motstands vei gjennom automasjon/AI og manuelle operasjoner, uavhengig av virksomhetens størrelse. Man trenger ikke ha «fiender», for å være et potensielt mål for cyberangrep.

Phishingangrep, fakturasvindel og tredjepartsangrep er noe som nå skjer daglig. Når teknologien blir mer avansert, så blir angrepsmetodene fra ondsinnet hackere også det. Selv med god intern informasjonssikkerhet kan trusselaktører utnytte dårlig sikrede underleverandører for å nå sine mål.

Tre viktige risikoreduserende tiltak for å forbedre informasjonssikkerheten:

1. **Forstå virksomhetens kontekst**
   For å beskytte seg mot digitale angrep er det viktig å forstå hva som er viktig for virksomheten, hvem som kan true den, og hvordan angrep kan skje. Dette inkluderer virksomhetens mål, strategier, verdier, aktører, systemer og prosesser. Ved å analysere dette kan man finne ut hvilke verdier som er mest sårbare for angrep, hvilke personer eller grupper som kan ha interesse av å angripe, og hvilke deler av systemene eller prosessene som kan utnyttes. På denne måten kan man redusere risikoen for digitale angrep ved å fokusere på sikkerhetstiltak som beskytter det som er viktigst for virksomheten.

2. **Risikoforståelse og viktigheten å ha en risikobasert tilnærming**
   Ledelsen må ha en felles oppfatning av hvilke risikoer virksomheten står ovenfor. Dette danner grunnlaget for å bestemme hvor mye risiko virksomheten kan tåle, som er en viktig del av å håndtere risiko. Når beslutninger tas, må de kontrollere om de er innenfor de grensene som er satt knyttet til akseptert risikonivå.

3. **Ha og øv på en krise- og beredskapsplan**

   Dersom en informasjonssikkerhetshendelse inntreffer er det avgjørende å vite hvem som gjør hva når hendelsen oppstår. En krise- og beredskapsplan sier hvem som har hvilke roller, ansvar og myndighet under håndteringen av krisesituasjonen. Ved å ha forhåndsdefinerte rolle- og tiltakskort vil det være mulig å øve på å håndtere en beredskapssituasjon, og konsekvensen av de iverksatte tiltakene kan vurderes før de blir tatt i bruk. Man må også sørge for å revidere eventuelle nåværende beredskapsplaner, slik at de er oppdaterte og relevante, med riktige kontaktpunkter etc. Her er det også viktig å tenke på hva slags kommunikasjonsmuligheter man har, om de primære metodene, ikke er tilgjengelige.

Reduser sannsynligheten for å oppleve digitale angrep ved å:

1. **Arbeide med opplæring og bevissthet:** Vær bevisst på hvilke verdier virksomheten din besitter. Dette kan være alt fra personlig eller sensitiv informasjon til informasjon om intervjuobjekter, kunder og samarbeids-partnere. Ha et bevisst forhold til hvordan dette blir behandlet og sikret etter kritikalitet.

2. **Ta i bruk et passord-hvelv og ha unike, komplekse passord på de systemene du bruker.** I en verden hvor mange passord allerede er tilgjengelige for uautorisert tilgang, er det kritisk å unngå den enkleste veien inn for trusselaktører. Aktiver multi-faktor autentisering på de systemene som har denne funksjonaliteten tilgjengelig.

3. **Ha oversikt over hvilke enheter virksomheten besitter.** Det er avgjørende å ha en fullstendig oversikt over datamaskiner, nettbrett, telefoner og andre enheter som finnes i virksomheten for å sikre at disse er innrullet og utrullet etter virksomhetens risikoaksept.

4. **Ha oversikt over systemene dine.** Oversikt over virksomhetens endepunkter og overvåking er avgjørende for å oppdage abnormal aktivitet på et tidlig stadium, og redusere skadeomfanget dersom det er en pågående informasjonssikkerhetshendelse.

5. **Revider leverandøravtaler.** Få en oppdatert oversikt over hva man har av leverandører og hva man får levert av disse. Bruker man det man har kjøpt, bruker man det riktig, og får man levert det man har krav på?

6. **Aktiv tilgangsstyring.** Sørg for at ansatte kun har tilgang til nødvendige deler av systemet, basert på hvilken rolle og funksjon de har i virksomheten, for å minimere risiko. Dette er særlig viktig ifm. bytte av stilling, eller avslutning av arbeidsforhold.