DIGITALISERINGSSTYRELSEN

Guide til awareness om informationssikkerhed

Marts 2013

Guide til awareness om informationssikkerhed

Udgivet marts 2013

Udgivet af Digitaliseringsstyrelsen

Publikationen er kun udgivet elektronisk

Henvendelse om publikationen
kan i øvrigt ske til:

Digitaliseringsstyrelsen
Landgreven 4
1017 København K
Tlf. 33 92 52 00

Publikationen kan hentes på
Digitaliseringsstyrelsens hjemmeside
www.digst.dk.

Foto Jeppe Gudmundsen

Elektronisk publikation
ISBN 978-87-995647-4-3

1. Hvorfor awareness – og hvad er det?

I dag bruges tekniske løsninger til at beskytte teknologiens komponenter. Men så snart mennesker involveres i teknologierne, stiger trusler, sårbarheder og risici, fordi der ikke er implementeret tilsvarende sikringsforanstaltninger til 'det menneskelige operativsystem'.

Vi har en tendens til at overvurdere risici, som vi kan se, men som vi ikke har direkte kontrol over. Af samme grund overvurderes risici typisk for flystyrt, hajangreb mv.

Samtidig undervurderes risici, der ikke er visuelle, og hvor vi selv har en vis grad af kontrol. Her er hacker-angreb, phishingangreb og læk af data gode eksempler. Det sker virtuelt ude af vores synsfelt, og selvom vi i teorien kan gøre en hel del for at undgå det, undervurderes den enkeltes betydning for sikkerhedshændelser.

Awareness betyder bevidsthed om et givent emne. Formålet med at etablere awarenessprogrammer er gennem information, kommunikation og træning at ændre vores adfærd.

Vi skal gøres opmærksomme på vores egen betydning for og påvirkning af informationssikkerheden. Og vi skal lære ikke at undervurdere de reelle sikkerhedstrusler.

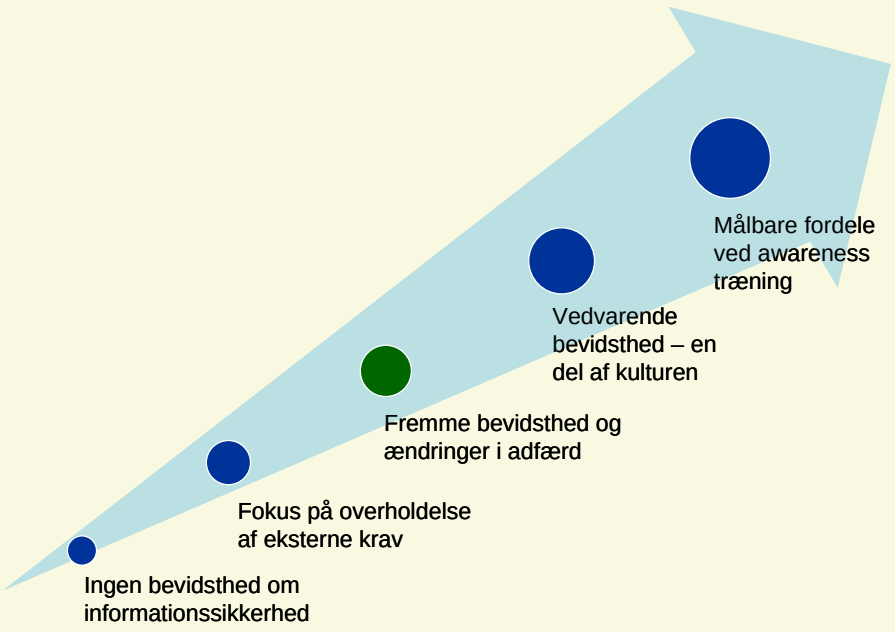
Ved awarenesstræning kan sikkerhedshændelserne ikke forhindres fuldstændigt, men som andre sikringsforanstaltninger som antivirusprogrammer, firewalls mm., kan det minimere sandsynligheden væsentligt.

Det forudsætter dog, at awarenessprogrammet og den træning, der følger med, ikke blot bliver en enkeltforestilling eller noget, der kun sker én gang om året. Det kræver en vedvarende og kontinuerlig indsats, som bør være lige så naturligt integreret i sikkerhedsarbejdet, som de tekniske foranstaltninger er i dag.

2. Modenhed

Nedenfor vises en modenhedsskala, som en organisation vil arbejde sig op ad, efterhånden som graden af awareness stiger.

Illustration af en modenhedsskala



Anbefalingen er, at der som minimum stræbes efter at fremme bevidstheden om informationssikkerhed blandt organisationens medarbejdere i en grad, at adfærden ændres i en positiv retning. Det vil sige, at politikker og regler på området efterleves.

Før der udarbejdes et egentlig program og plan for awarenessarbejdet i organisationen, bør det fastlægges, hvilket modenhedsniveau organisationen befinder sig på, og hvilket niveau der sigtes efter.

En vigtig del af forberedelserne og fastlæggelse af det nuværende modenhedsniveau er at kortlægge, hvilke konkrete awarenessaktiviteter organisationen gennemfører allerede, hvilke der fungerer effektivt i organisationen, og hvilke områder der eventuelt er særligt oversete.

3. Awarenessplan - step by step

Nedenfor foreslås en metode til, hvordan man kan iværksætte et awarenessprogram i organisationen. De enkelte trin gennemgås efterfølgende.

Illustration af metode til iværksættelse af awarenessprogram

Styringskomite
Der bør etableres en styringskomite bestående af frivillige ambassadører for informationssikkerhed og awareness. Disse skal skabe ejerskab på tværs af afdelinger og områder i organisationen.

Som udgangspunkt er det informationssikkerhedskoordinatoren, der tager initiativ til at etablere styringskomiteen. Medlemmerne i styringskomiteen bør repræsentere forskellige afdelinger i organisationen og forskellige roller i organisationens arbejde (jurister, HR, it, helpdesk, kommunikation m.m.). Herved sikres det, at awarenessprogrammet bliver effektivt spredt i forskellige grene i organisationen.

Hvis organisationen har en kommunikationsafdeling, bør der deltage en kommunikationsmedarbejder i styringskomiteen, så awarenessprogrammet koordineres med organisationens eksisterende kommunikationsstrategi- og arbejde.

Den optimale gruppe er på fem-ti personer, som skal hjælpe med at planlægge, eksekvere og vedligeholde programmet.

Gruppen bør mødes med faste mellemrum og med fast dagsorden, men kan indimellem møderne eventuelt koordinere virtuelt.

Hvem skal planen rettes mod?
Det skal besluttes, hvem der er målgruppen for awarenessprogrammet, og hvis adfærd man ønsker at påvirke. Målgruppen kan omfatte alle medarbejdere eller afgrænses til it-udviklings- eller driftsmedarbejdere, medarbejdere i en service- eller helpdeskfunktion, ledelsespersoner eller eksterne leverandører. Det skal tages forskellige budskaber og kommunikationsmidler i anvendelse over for de forskellige grupper. Derfor afgrænsning af målgruppen.

Hvad skal formidles?
Når træningen eller kommunikationen skal planlægges, kan det være en god idé at dele træningen op i forskellige moduler med fokus på hver deres specifikke sikkerhedsemne eller trusselsområde.

Der kan f.eks. være emner som:

- e-mail
- sociale netværk
- kodeord/passwords
- cloudløsninger
- brug af it-udstyr
- brug af kritiske it-systemer
- arbejdsopgaver med følsomme data.

Omfang og varighed af det enkelte træningsmodul kan være forskellig, og det er ikke sikkert, at alle medarbejdere skal bruge lige lang tid på træningen.

De er måske behov for, at visse dele af organisationen skal have en egentlig tilpasset uddannelse, mens andre kan få en pakke med information og en basisuddannelse.

Hvilke formidlingskanaler skal bruges?
I planlægningen af kommunikations- og formidlingsindsatsen skal der tages højde for organisationens kultur, eksisterende kommunikationstraditioner og målgruppens præferencer.

Når målgruppen er fastlagt, bør der gennemføres en målgruppeanalyse for at finde ud af, hvordan organisationens forskellige modtagere af awarenessprogrammet bedst modtager ny information.

Visse persongrupper vil måske overvejende drage fordel af meget faktuelle oplysninger baseret på tekst og tal. Andre vil være langt mere motiveret af visuelle illustrationer baseret på billeder eller film.

Det kan anbefales at bruge humor i kommunikation. Stilen skal lægges op ad den form for humor, som er gangbar i organisationens kultur. Pas dog på, at budskabet stadig fremstår seriøst. Fokuser på fordelene, frem for at awarenessprogrammet gøres til en skræmmekampagne. Det motiverer ingen.

Det er vigtigt, at målgruppen engageres mest muligt, og det kan derfor være en god idé, at budskaberne handler om pointer, der kan relateres til brugernes liv udenfor arbejdslivet. Benyt mindst tre forskellige kanaler til at supplere og repetere.

Nedenfor er opstillet nogle eksempler:

- Videoklip
- Plakater – fysiske eller digitale
- E-learning
- Intranet
- Nyhedsbreve
- Undervisning/træning
- Workshops
- Gå-hjem-møder
- Seminarer
- Kurser

Plakater, nyhedsbreve og videoklip mv.
Plakater, nyhedsbreve, intranetnyheder, videoklip mv. kan alle være gode supplementer til nogle af de andre mere uddybende kanaler. Fordelen er fleksibiliteten, da medarbejderne selv kan bestemme, hvor og hvornår de vil bruge tid på det. På den anden side kan risikoen være, at modtagerne aldrig får det læst.

- Budskaberne skal være enkle og fange målgruppens opmærksomhed
- Udfordringen er at gøre emnet interessant, vedrørende eller sjovt
- Vælg kun de vigtigste elementer i informationssikkerhedsarbejdet - og hold fokus.

E-learning, workshops, håndbøger mv.
E-learning, workshops, håndbøger, kurser og lignende træningsformer giver lejlighed til at give en mere uddybende forståelse for informationssikkerheden blandt medarbejderne.

Opdel træningen i forskellige moduler, f.eks.:

- Basistræning
- Brugeransvar
- Indenfor arbejdspladsen
- Udenfor arbejdspladsen.

Hvert modul kan så yderligere inddeles i tre dele:

- Teori
- Scenarie
- Test

Udarbejd selve awarenessprogrammet
Styringskomiteen gennemgår og opdaterer indholdet i "Hvem – Hvad – Hvordan" for awarenessprogrammet og sender evt. indholdet til godkendelse hos ledelsen.

Indholdet i programmet skal helst være så personneutralt og teknologineutralt som muligt, forstået på den måde at programmet kan implementeres, selvom organisationens persongalleri eller teknologi udskiftes løbende.

Implementering og opdatering
Når programmet er godkendt, skal planen implementeres i praksis, hvorefter det opdateres og gennemgås periodisk. Det anbefales, at opdateringen sker minimum én til to gange årligt.

Organisationen bør også gøre sig overvejelser om, hvem der skal stå for selve implementeringen af det awarenessprogram, der er blevet udarbejdet af styringskomiteen.

Det er vigtigt, at formidlingen ud til medarbejderne foretages af en person, der både har erfaringen og kompetencerne til formidling. Det kan også være en person, som modtagergruppen har tillid til, og som fungerer som respekteret rollemodel i organisationen.

Mål effekten af awarenessprogrammet
Ved måling af effekten er det vigtigt på forhånd at fastlægge, hvad der reelt skal måles på. Er det graden af bevidsthed, forståelse eller graden af efterlevelse af informationssikkerheden i organisationen? Det optimale ville være at måle på alle tre dele, men i praksis vil det afhænge af organisationens ambitionsniveau, og hvor stor en viden medarbejderne allerede har på området. Ved at foretage effektvurdering af awarenessprogrammet kan der samtidig også ændres på medarbejdernes adfærd i en positiv retning. Indsamlingen af medarbejdernes viden om sikkerhed vil nemlig ofte forbedre bevidstheden og interessen blandt de, der deltager i undersøgelsen.

Nedenfor er opstillet forslag til metoder til måling af effekten af awarenessprogrammet:

- Spørgeskemaundersøgelser
- Quiz med præmier
- Kryds og Tværs med præmier
- Konkurrencer/lodtrækninger
- Testresultater fra e-learning.


NØD