Dediko A/S
Your Security is our Passion

Awarenessmodenhedsmodel

Kategori	Relevans	Svar	Spørgsmål	Bemærkninger
Hvorfor (ledelsen)	✓		**Udspringer awareness programmet fra ledelsen**	
	✓		**Har awareness programmet ledelsens fulde sponsorship**	
	✓		Har ledelsen sat organisationens awareness mål efter SANS.org modenhedsmodel	
	✓		Er ledelsesforankringen målbar	
	✓		Er awareness programmet et mandat fra et compliance krav	
	✓		**Kommunikeres resultaterne af awareness programmet regelmæssigt tilbage til ledelsen**	
Hvordan (metoden)	✓		**Er der udpeget en eller flere personer som har ansvar for awareness programmet**	
	✓		Har de awareness ansvarlige fornøden viden om awareness (fx SANS MGT 433)	
	✓		Er der udpeget frivillige awareness ambassadører for awareness programmet	
	✓		**Er emnerne i awareness programmet udvalgt på baggrund af en risikoanalyse**	
	✓		Er rækkefølgen i awareness programmet baseret på risiko	
	✓		**Er aktiviteterne i awareness programmet målbare hvor det er muligt (metrisk)**	
	✓		Er der fastsat et mål for aktiviteterne så organisationen ved hvornår målet er nået	
	✓		Er horisonten for awareness programmet flerårig	
	✓		Er organisationens clear-desk-policy understøttet af awareness programmet	
	✓		Er forståelsen af It-sikkerhedspolitikken målbar gennem årlige spørgeskemaer	
	✓		**Indgår regelmæssige tilfredshedsundersøgelser i korrigering af awareness programmet**	
	✓		Udføres der kun et (eller få relaterede) undervisningsforløb ad gangen	
	✓		Efterfølges alle undervisningsforløb af tests efter bedste praksis	
	✓		**Indtænkes adfærdsændringerne med respekt for A=M*E*I**	
	✓		Indtænkes undersøgelser og iterationer på basis af Hermann Ebbinghaus	
	✓		**Gennemføres regelmæssige phishing tests (fx månedlige)**	
	✓		Måles resultatet af phishing tests med et rullende gennemsnit af de sidste 3-5 målinger	
	✓		Er awareness programmet differentieret efter medarbejder roller	
	✓		**Korrigeres awareness programmet på basis af målinger og ledelseskommunikation**	
	✓		Er undervisningsmetoderne bevidst varierede og komplimentære	
	✓		Er der valgt en awareness maskot som går igen på alt awareness materiale	
Hvad (udførelsen)	✓		Kan CBT programmet håndtere valgfri målbare spørgeskemaer	
	✓		**Har CBT programmet interaktive undervisningsforløb som er engagerende**	
	✓		Kan CBT programmets undervisningsforløb tilpasses organisationen	
	✓		Er CBT programmets undervisingsforløb på flere relevante sprog	
	✓		**Indeholder CBT programmet valgfri målbare phishing tests**	
	✓		**Leverer CBT programmets leverandør regelmæssigt nye relevante undervisningsforløb**	
	✓		**Samles alle CBT målinger centralt i et fleksibelt centralt interface**	
	✓		Kan CBT programmet håndtere måling af brugernes identifikation af phishing mails	
	✓		Kan CBT programmet håndtere automatisk import af brugere	
	✓		Kan CBT programmet tilpasses medarbejder roller	
	✓		Kan sværhedsgraden af undervisningsforløbet varieres efter medarbejder roller	

Resultat

Hvorfor	Hvordan	Hvad
0%	0%	0%

Afvikles awareness programmet efter bedste praksis?

0%

Udfyldt af:	*Christian Schmidt*
Dato:	*27. maj 2021*
Virksomhed:	*Dediko*
Ledelsesgodkendt:	*Forhåbentlig ikke…*

Deloitte. | **Awareness checkliste. Resultat [0%]** | **Resultat** | **0%**

>>> Angiv om denne aktivitet er gennemført i kolonne F "Gennemført": 0=nej, 1=delvist og 2=Ja. Er spørgsmålet ikke relevant skrives 0 i kolonne E "Relevans"

Prioritet	Kategori	Relevans	Gennemført	Anbefaling	Forklaring	Dine bemærkninger
#01	Hvorfor	✓		Awareness programmet skal udspringe fra og ejes af ledelsen	Awareness programmets formål er risikoreduktion og det er ledelsen som ultimativt er ansvarlig for organisationens risikoappetit. Derfor skal awareness programmet initieres og ejes fuldt ud af ledelsen, men drives af andre afdelinger som fx IT og HR. Det er vigtigt at alle aktiviteter i awareness programmet kommunikativt udspringer fra ledelsen og ikke fra fx IT afdelingen	
#02		✓		Ledelsen skal sponsorere awareness programmet fuldt ud baseret på ønskede mål	Det er ledelsens opgave at få en teknisk vurdering af behovet for awareness træning (typisk fra HR, IT og DPO / Compliance afdelingen) og på basis af det vurderede niveau for risik reduktion fastsætte en tidsramme for at opnå de ønskede mål. Dertil bør ledelsen naturligvis bevilge de nødvendige ressourcer (medarbejdere, tid, budget, kompetencer m.fl.) og forlange status rapportering for at vurdere om planen bliver fulgt og resultaterne bliver opnået og vedligeholdt indenfor den afsatte tidsramme	
#03		✓		Resultaterne af awareness programmet skal regelmæssigt kommunikeres til ledelsen	Ledelsen skal sikre de nødvendige KPI'er med at de ansvarlige for at awareness programmet kan rapportere status til ledelsen regelmæssigt - typisk som et punkt på hvert bestyrelsesmøde. Afviger resultaterne fra planen, skal ledelsen iværksætte korrigering af awareness programmet så risikoreduktionen opnås indenfor den fastlagte	
#04	Hvordan	✓		En eller flere medarbejdere skal være ansvarlige for awareness programmet	Der bør afsættes en eller flere fuldtidsmedarbejdere til at være ansvarlige for awareness programmet. Denne funktion kan efter nøje overvejelse også outsources. Uden medarbejdere med ansvar og tilsvarede ressourcer til at gennemføre awareness programmet opnås den ønskede risiko reduktion næppe.	
#05		✓		De emner, der er en del af awareness programmet, skal være baseret på en risikoanalyse	Der skal ikke vælges træningsemner på basis af hvad CBT programmet tilbyder, men på basis af en risikoanalyse af relevante cyber sikkerhedsemner. Analysen vurderes fx på en klassisk kombination af sandsynlighed x konsekvens og gerne krydret med resultaterne fra en GAP analyse på it-sikkerhed. Træningsemner bør afvikles i rækkefølge efter faldende risiko med mindre andre faktorer som fx	
#06		✓		Aktiviteterne i awareness programmet skal være målbare overalt hvor det er muligt	Alle aktiviteter gennemføres ved først at lave en baseline måling og derefter fastsættes det ønskede målbare mål for adfærdsændringen. Fra baseline til det opnåede gentages et antal målinger for at vise, at adfærdsændringen er implementeret og accepteret. Målet for risikoreduktionen fastsættes efter trusselsbilledet og organisationens ønskede it-sikkerhedsprofil.	
#07		✓		Regelmæssige undersøgelser blandt brugerne skal danne grundlag for revidering af awareness programmet	Der bør gennemføres spørgeskemaundersøgelser eller interviews blandt relevante medarbejdere som har gennemført dele af awareness programmet for at vurdere brugernes opfattelse af programmet (kværhedsgrad, relevans, engagement osv). Resultaterne af disse undersøgelser skal indgå i den løbende revision af	
#08		✓		Den videnskabelige baggrund for awareness træning bør indtænkes: Adfærd=Motivation*Evne*Incitament	BJ Foggs behaviour model bør indgå som et element i alle træningsaktiviteter (hvor det er muligt) for at sikre den maksimale effekt af awareness programmet på en videnskabelig basis. Hvis adfærdsændringen er vanskelig skal produktet af motivation, evne og incitament være højt. Hvis nogen af de 3 faktorer er nul (eller tæt på nul) bliver det meget vanskeligt at gennemføre en adfærdsændring. Se mere på https://www.behaviormodel.org/	
#09		✓		Der skal gennemføres regelmæssige phishing tests (fx månedligt eller oftere)	Resultatet af en phishing simulering vil næppe ikke signifikant. Der bør gennemføres løbende phishing simuleringer (fx månedligt) og resultatet bør vurderes som gennemsnittet af de sidste 3-5 målinger. Husk at blive ved med disse målinger for at vurdere om resultatet af awareness initiativet er aftagende på grund af manglende	
#10		✓		Awareness programmet skal revideres baseret på de opnåede målinger (KPI) og ledelseskommunikationen	Hvis de observerede målinger af resultaterne af awareness programmet peger på at træningen ikke er effektiv nok til at opnå den ønskede risikoreduktion indenfor den fastsatte tidsramme skal awareness aktivteteme revideres tilsvarende. Det er vigtigt at kommunikere både succes og fejl i awareness programmet med ledelsen!	
#11	Hvad	✓		Awareness programmet skal være varieret og engagerende med korte undervisningsmoduler	Hvis brugerne har lyst til at gennemføre awareness træningen er der langt større chance for at programmet bliver en succes. Det er derfor meget vigtigt at programmet er varieret og engagerende (læs underholdende).	
#12		✓		Awareness CBT programmet/service skal indeholde muligheden for at afvikle valgfrie phishing tests	Det er en stor fordel hvis selveste CBT awareness programmet indeholder muligheden for selv at designe phishing tests på basis af skabeloner og afvikle dem lige så til det ønskes. Det giver den største fleksibilitet og de bedste målinger / resultater. Husk at det formodentligt skal afklares med ledelsen hvor mange phishing tests der skal/kan	
#13		✓		Awareness CBT programmet skal opdateres hyppigt med nye og relevante moduler	Det er meget vigtigt at servicen eller awareness programmets leverandør regelmæssigt leverer nye træningsmoduler som gør at programmet holder trit med trusselsbilledet og særlige nye forhold (som fx COVID-19 baserede trusler). Det er meget tidsrævende at lave disse træningsmoduler selv og derfor risikerer awareness	
#14		✓		Resultaterne fra aktiviteterne i CBT programmet skal samles i et intuitivt og fleksibelt centralt interface	Alle målbare aktiviteter i awareness programmet skal opsamles i ét centralt interface i CBT programmet. Der skal være mulighed for at sammenligne resultater, vise tendenser og eksportere data til fx Microsoft Excel for videre bearbejdelse og ledelsesrapportering og kommunikation.	