KOCHCONSULTANCY
Security- & Privacy Awareness

Prijsinformatie

Awareness presentatie
1,5 - 2 uur

Security Awareness

Per 1-1-2025

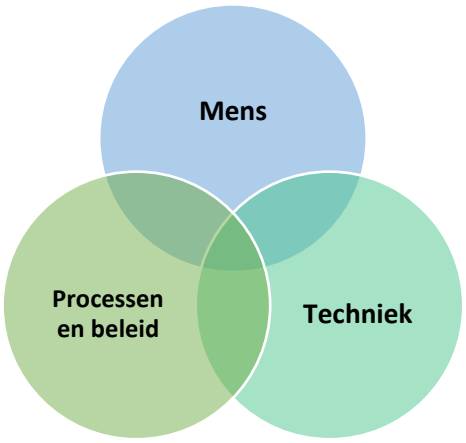
Waarom is Awareness belangrijk?

Meer dan 70% van de incidenten op het gebied van security en privacy wordt veroorzaakt door menselijk handelen. Dit komt doordat mensen in een bedrijf vaak niet bewust zijn van de risico's waaraan ze blootstaan en daardoor erg kwetsbaar zijn. Cybercriminelen richten zich tegenwoordig voor hun aanvallen voornamelijk op de medewerk(st)ers van bedrijven. In het bijzonder bij een hoge werkdruk is een medewerk(st)er die niet bewust is van die digitale gevaren extra kwetsbaar.

Mens, proces, techniek

Als je risico's wilt verlagen op het gebied van security en privacy is het niet genoeg om alleen te kijken naar mogelijke technische maatregelen. Er zijn drie belangrijke "Pijlers" waar aandacht aan gegeven moet worden:

- Mens: het gedrag van de mensen in de organisatie,
- Processen: de gebruikte processen (beleid, afspraken, richtlijnen, gedragscodes, "Code of Conduct", etc.)
- Techniek: De genomen technische maatregelen (in de meeste gevallen door de IT- of security mensen.



Het komt helaas erg vaak voor dat bedrijven bij het nemen van securitymaatregelen zich beperken tot het nemen van uitsluitend **technische** maatregelen zoals antivirus, firewalls, spamfilters, monitoring systemen, etc. Deze maatregelen zijn uiteraard nuttig, maar niet voldoende.

Als er geen goed **beleid** is opgesteld met processen/procedures en afspraken over hoe er met ICT-middelen en bedrijfsgegevens wordt omgegaan blijft het risico op een incident of een datalek nadrukkelijk aanwezig.

En dan is er natuurlijk het **menselijk gedrag**. Een bedrijf blijft kwetsbaar als medewerk(st)ers onveilig omgaan met bedrijfsinformatie en de beschikbaar gestelde ICT-middelen (computers, tablets, laptops, smartphones). Als de medewerk(st)ers bewust zijn van de risico's en gevaren waaraan ze (op het werk én thuis!) blootstaan verlaag je de kans om slachtoffer te worden van cybercriminelen door bijvoorbeeld phishing e-mails, fraude en/of onveilig gebruik van wachtwoorden. Maak de mensen daarom de sterkste schakel! Ze zijn immers de "First line of defense".

Bewust personeel maakt een bedrijf weerbaar en verlaagt het aantal incidenten en datalekken.

Awareness vergroting

Om medewerk(st)ers van een organisatie bewust te maken van cyber-risico's zijn er verschillende activiteiten mogelijk. Het organiseren van awareness presentaties is hierbij een veel gekozen activiteit.

Klassikale awareness presentaties

De awareness presentaties worden bij uw bedrijf aan huis of op een door u gekozen externe locatie verzorgd. De awareness presentatie duurt 1,5 - 2 uur.
Zie ook: https://www.kochconsultancy.nl/voorlichting-training/awareness-presentaties

De onderwerpen die in deze presentatie besproken worden zijn:

- Inleiding (Internet, cybercriminaliteit)
- Social Engineering - Phishing (Wat is het, hoe werkt het, hoe herken je het, wat te doen)
- Veilig gebruik van wachtwoorden (wat is wel/niet veilig, hoe worden ze gestolen, hoe onthoud je ze, MFA)
- Internet-Fraude (CEO-fraude, salarisfraude, leveranciersfraude, whatsapp-fraude, nepfacturen, QR-fraude)

De presentatie geeft op een leuke, interactieve (niet-technische) manier inzicht in de internet-risico's waaraan de mensen blootstaan. Het zijn informele presentaties met veel sprekende voorbeelden uit de (Nederlandse) praktijk. Er is voldoende gelegenheid om vragen te stellen en ervaringen te delen. De presentaties krijgen goede referenties en hebben voor veel mensen de ogen geopend met betrekking tot veilig gedrag met ICT-middelen en bedrijfsinformatie. In verband met de interactie is het maximaal aantal deelnemers gesteld op 25 per sessie.

Ruimte voor input

Bij de presentatie-sessie is er ruimte om bepaalde bedrijfsspecifieke onderwerpen "mee te laten nemen" in het programma. Denk hierbij aan eventuele afspraken/richtlijnen/procedures die in gebruik zijn op het gebied van ICT, security of privacy, clean desk policy, wachtwoord beleid, opslag van gegevens, toegang tot systemen, etc.
Het is daarom ook goed denkbaar om dergelijke presentaties te gebruiken voor nieuwe medewerkers gedurende hun introductieperiode.

Prijsinformatie awareness presentaties

Hieronder een overzicht van de benodigde investering voor het laten verzorgen van klassikale (in-house) awareness presentaties.

Omschrijving	Prijs
Security Awareness presentatie (1,5 - 2 uur)	€ 895,00

Omschrijving	Prijs 1-5 sessies	Korting > 5 sessies	Korting >10 sessies	Korting >25 sessies
Security Awareness presentatie (1,5 - 2 uur)	€ 895,00	15%	20%	25%

De genoemde prijzen zijn per sessie, excl. reiskosten (45 cent per km).

Contact informatie

Koch Consultancy BV
Beetzlaan 5
3762 CA Soest

Tel: 06-53233269

Website: www.kochconsultancy.nl
E-mail: rob.koch@kochconsultancy.nl

KOCHCONSULTANCY
Security- & Privacy Awareness