KOCHCONSULTANCY
Security- & Privacy Awareness

Awareness

Security
Privacy

Wat is het belang en hoe zet je een awareness campagne op?

- Waarom is Awareness belangrijk?
- Vergroting van de Awareness. Hoe dan?
    - Verandering van gedrag
- Acties binnen een awareness campagne
    - Nulmeting
    - Leren
    - Meten
    - Rapportage
- Voorbeelden van een Awareness campagne

feb 2023

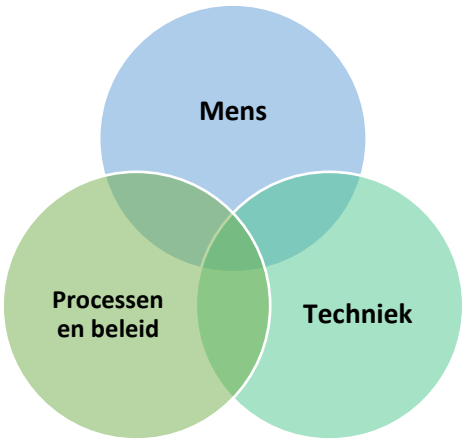
Waarom is Awareness belangrijk?

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.

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 security-maatregelen niet verder gaan dan alleen het nemen van technische maatregelen zoals antivirus, firewalls, spamfilters, monitoringsystemen, etc. Deze maatregelen zijn uiteraard noodzakelijk, 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 mensen binnen de organisatie bewust zijn van de gevaren waaraan ze blootstaan verlaag je de kans om slachtoffer te worden van cybercriminelen door bijvoorbeeld phishing e-mails, fraude en/of onveilig gebruik van wachtwoorden.

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

Medewerk(st)ers van bedrijven zijn het doelwit van cybercriminelen
Cyber-criminelen richten zich tegenwoordig voor hun aanvallen voornamelijk op de medewerk(st)ers van bedrijven en in veel mindere mate op de infrastructuur (netwerk, computers, servers, etc.).
In het bijzonder bij een hoge werkdruk is een medewerk(st)er die niet bewust is van de digitale gevaren extra kwetsbaar.

Aanvallers zijn vaak gericht op het verkrijgen van usernames en wachtwoorden van medewerk(st)ers waarmee ze kunnen inloggen in het bedrijfsnetwerk en de systemen. Hiervoor maken ze gebruik van verschillende "Social Engineering" technieken zoals bijvoorbeeld phishing. Als ze eenmaal toegang hebben tot het bedrijfsnetwerk kunnen ze "van binnenuit" verdere aanvallen uitvoeren zoals het versturen van nep-mails of nep-facturen of binnen de systemen verder zoeken naar interessante informatie zoals documenten, inloggegevens, bank/betaalgegevens en financiële data.

Alle medewerk(st)ers dragen verantwoordelijkheid voor de informatiebescherming
Om het gedrag van medewerk(st)ers veilig(er) te maken is het daarom van groot belang dat ze bewust zijn van de risico's op het gebied van security en privacy waaraan ze dagelijks blootstaan, zowel op het werk als 's avonds thuis op de bank met hun tablet, telefoon of laptop.

Zijn de medewerk(st)ers bewust van het feit dat ze voor hun dagelijkse werkzaamheden toegang hebben tot zeer vertrouwelijke gegevens? Medewerk(st)ers van de financiële afdeling hebben bijvoorbeeld toegang tot de financiële gegevens van het bedrijf en wellicht verrichten ze ook betalingen. Een productmanager heeft informatie over nieuwe productontwikkelingen en een financieel manager is betrokken bij de besprekingen over een overname.

Patiëntgegevens, Leveranciersgegevens, prijsinformatie, HR-dossiers van het personeel, bank/betaalgegevens, klantgegevens, marketingstrategie, productplannen, etc. wil je niet in handen zien van de concurrentie en/of kwaadwillenden.

De verantwoordelijkheid voor het beschermen van al deze belangrijke bedrijfsinformatie ligt niet uitsluitend bij de IT-afdeling of de directie. Iedereen binnen het bedrijf draagt hiervoor zijn/haar steentje bij. Een bewuste medewerk(st)er weet wat hierin zijn/haar verantwoordelijkheden zijn.

Welke medewerk(st)ers lopen het grootste risico?
Medewerk(st)ers die door cybercriminelen het meest worden aangevallen zijn niet per definitie altijd onderdeel van het management. Het gaat met name om de mensen in de organisatie die van buitenaf makkelijk te vinden zijn. Bijvoorbeeld op de website van het bedrijf, op Social Media en/of in publicaties. Aanvallers weten precies welke phishing-berichten ze het beste aan die mensen kunnen sturen, op welke tijdstippen en met welk onderwerp. Met name in het geval van spearphishing ontvangen de slachtoffers een phishing e-mail over een onderwerp waarin ze echt persoonlijk geïnteresseerd zijn. Als die medewerk(st)er onbewust is, is de kans dat hij/zij erin trapt dan ook erg groot.

De mens kan de sterkste schakel worden!
Een veelgehoorde opmerking is dat de mens de "zwakke schakel" in de security is. En dat terwijl (zoals in de voorgaande tekst is uitgelegd) de mensen binnen de bedrijven juist worden aangevallen en dus de "first line of defense" zijn. Vergroting van het bewustzijn en de cyber-hygiëne is daarom belangrijk om van de mens de "sterkste schakel" te maken. Een "**Human Firewall**" dus!

Een bewuste medewerk(st)er:

- Kent het gevaar van phishing en klikt niet zomaar overal op wat hem/haar wordt voorgeschoteld.
- Weet hoe hij/zij veilig gebruik kan maken van (sterke) wachtwoorden
- Begrijpt het belang van het veilig omgaan met ICT-middelen als computers, laptops, smartphones, tablets, printers, etc.
- Weet waar hij/zij gegevens kan opslaan (lokaal? Cloud? USB-drives?)
- Deelt vertrouwelijke/gevoelige gegevens niet met ongeautoriseerde personen.
- Is bewust van het bestaan van de AVG en begrijpt waarom bedrijven zich hieraan moeten houden
- Weet waar hij/zij een security- of privacy-incident (datalek) intern moet melden.

Awareness: een continu proces

Het op peil brengen en houden van het bewustzijn op het gebied van security en privacy is een continu proces. Een campagne om het bewustzijn te vergroten bestaat uit onderdelen waarbij met regelmaat kleine “plukjes” informatie aan de medewerk(st)ers wordt aangeboden. Op die manier worden de medewerk(st)ers op een prettige manier getriggerd over dit belangrijke onderwerp.

De manier waarop de informatie wordt aangeboden en de “toon” die wordt aangeslagen bepalen de mate waarop de medewerk(st)ers getriggerd worden. Als de informatie bijvoorbeeld te technisch is zullen de medewerk(st)ers snel afhaken en niet verbeteren in hun “cyber-hygiëne”.

Betrokkenheid en medewerking van het management

Een belangrijk aspect voor het succes van een awareness campagne is de betrokkenheid en medewerking van het management. Een introductie van een awareness campagne vanuit de directie is daarom aan te raden. In deze introductie kan het belang van de informatiebescherming uitgelegd worden en het feit dat de verantwoordelijkheid hiervoor niet uitsluitend bij de IT-afdeling ligt. Als bijkomend voordeel kan worden aangegeven dat dit ook belangrijk is voor de privé situatie.

De introductie kan eventueel ook gedaan worden middels een videobericht. In een korte videoboodschap van circa 1 minuut geeft het directielid aan waarom informatiebeveiliging extra aandacht behoeft en noodzakelijk is voor het bedrijf. Dit creëert meer betrokkenheid bij het awareness traject. De vorm en inhoud van de video worden afgestemd met de wensen en behoeften van uw organisatie.

Het is van belang om de juiste cultuur te creëren op het gebied van informatiebescherming binnen een bedrijf.

Vergroting van de Awareness. Hoe dan?

Voor het vergroten van het bewustzijn (awareness) van mensen in een bedrijf op het gebied van security en privacy is een campagne nodig die past in de organisatie. De verschillende onderdelen en activiteiten van een campagne worden over een bepaalde tijdsperiode uitgestreken.

Het uitgangspunt is dat mensen pas gedragsverandering gaan vertonen als ze goed begrijpen waarom bepaalde dingen anders moeten en verandering nodig is. Daarom is het belangrijk dat de mensen de risico's waaraan ze blootstaan goed begrijpen. De informatie over het verlagen van risico's wordt dan beter opgenomen.

Verandering van gedrag

Om langdurige gedragsverandering te realiseren is het noodzakelijk om niet alleen te kijken naar het bewustzijn van de mensen maar ook naar de omstandigheden waarin de mensen werkzaam zijn (omgevingsfactoren). Bijvoorbeeld: Vaak weten mensen best wel dat ze veilige wachtwoorden moeten gebruiken maar doen ze het toch niet. Het bewustzijn is dan wel aanwezig, maar het ontbreekt bijvoorbeeld aan de motivatie en/of het beschikbaar zijn van een password-manager om de wachtwoorden te kunnen onthouden.

In grote lijnen zijn er een aantal stappen te doorlopen. In een management workshop kunnen onderstaande onderwerpen worden besproken.

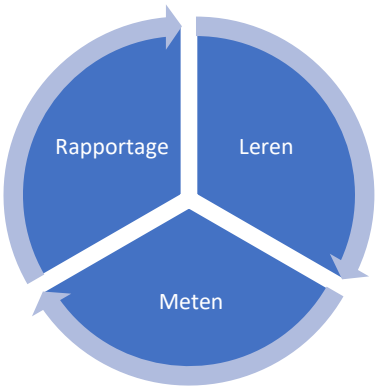
1. Breng de organisatie in kaart. (Verschillende bedrijfsonderdelen kunnen verschillende risicoprofielen hebben)
2. Definieer voor de onderdelen het gewenste veilige gedrag
3. Onderzoek waarom het gewenste veilige gedrag niet wordt nageleefd
    - Motivatie: Zijn de mensen gemotiveerd om het gewenste veilige gedrag te vertonen?
    - Capaciteit: Kunnen de mensen het gewenste veilige gedrag vertonen (Kennis)?
    - Gelegenheid: Krijgen mensen de kans om het gewenste veilige gedrag te vertonen (omgevingsfactoren)?
4. Bepaal de benodigde acties

Acties binnen een awareness campagne

Hieronder volgt een opsomming van een aantal mogelijke acties die binnen een awareness campagne uitgevoerd kunnen worden om het bewustzijn (de awareness) van de mensen in een organisatie te vergroten.

Nulmeting
Een awareness campagne start bij voorkeur met een “nulmeting”.
Na de nulmeting is inzichtelijk wat de huidige situatie is met betrekking tot de awareness.
De nulmeting bestaat standaard uit een online vragenlijst en een phishingtest via e-mail.
Het is mogelijk om de nulmeting uit te breiden met een of meerdere extra Social Engineering onderzoeken. Zie ook: https://www.kochconsultancy.nl/security-awareness/nulmetingen

Leren - Meten - Rapportage
De awareness campagne wordt vervolgens uitgevoerd door middel van een aantal activiteiten in een herhalende cyclus “Leren - Meten - Rapportage”.

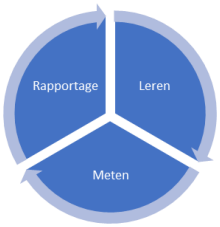


Leren:
Informatie-overdracht aan de medewerk(st)ers door middel van online- of klassikale awareness sessies en/of E-learning modules. Medewerk(st)ers worden ook getriggerd met security-hints en -tips via posters en Cartoons.

Meten:
Door middel van automatisch gesimuleerde phishing-aanvallen via E-mail, telefoon, SMS of USB-sticks blijven de medewerk(st)ers alert. Er zijn veel verschillende templates beschikbaar voor het uitvoeren van dergelijke phishingtesten.

Rapportage:
Uitgebreide rapportage met informatie van zowel training als phishing waarmee u inzicht krijgt in het effect van de awareness campagne. Geschikt voor het rapporteren aan het management en het bespreekbaar maken met medewerk(st)ers.

Leren



Het leren (trainen) van medewerk(st)ers kan op verschillende manieren gebeuren. Uiteraard is het heel goed mogelijk om binnen de awareness campagne een combinatie te maken van de verschillende leervormen.

Online security- en privacy-awareness presentaties

Het is mogelijk om diverse awareness sessies online te laten verzorgen. Hiervoor zijn een aantal presentatie-modules beschikbaar over de volgende onderwerpen:

- De gevaren van Internet
- Phishing en spearphishing, Social Engineering
- Veilig gebruik van passwords
- Diverse vormen van Internet Fraude (CEO-Fraude, leveranciersfraude, nepfacturen, Whatsapp-Fraude, Tikkie-fraude, QR-fraude, etc.)
- AVG voor medewerk(st)ers.
- AVG voor management

Deze (online) presentaties worden als webinar verzorgd en duren ongeveer 45 - 60 minuten. Het maximaal aantal kijkers is 50. Het voordeel hiervan is dat deze online sessies eenvoudig voor verschillende afdelingen of groepen medewerk(st)ers van een bedrijf kunnen worden ingepland.
Zie ook: https://www.kochconsultancy.nl/voorlichting-training/awareness-sessies-online

Klassikale awareness presentaties / training over security en privacy

Klassikale presentaties over security en/of privacy zijn zeer interactief en bevatten veel voorbeelden, filmpjes en er is voldoende gelegenheid voor het stellen van vragen. Voor deze sessies worden verschillende onderwerpen van de bovenstaande online presentatie-modules samengesteld tot één vloeiende presentatie van ongeveer 1,5 uur.

De meest gevraagde sessie is de 4-uurs Security Awareness training. Deze training bestaat uit 4 modules van 1 uur en wordt in de meeste gevallen verdeeld over twee dagen gegeven met 1 week tussenpauze. (Bijvoorbeeld 2 x een maandagochtend van 10-12 uur). Het voordeel hiervan is dat de deelnemers niet in één keer een grote “bulk” informatie krijgen en dat ze bij het begin van de tweede sessie hun vragen kunnen stellen en ervaringen gaan delen. Uiteraard kan deze training ook in 1 sessie van 4 uur verzorgd worden. Zie voor meer informatie:
https://www.kochconsultancy.nl/voorlichting-training/4-uur-security-awareness-training

De klassikale presentaties en de 4-uurs training worden bij de klant aan huis verzorgd en zijn inmiddels een eye-opener geweest voor velen. Door de vele interactiviteit is het maximaal aantal deelnemers aan de klassikale presentaties gesteld op 25. Voor de 4-uurs training is het maximale aantal deelnemers 15. Het voordeel van de klassikale presentaties en training is dat we in samenwerking met de klant de details over de te behandelen onderwerpen afstemmen en eventueel reeds bestaande procedures/richtlijnen die binnen het bedrijf al worden gebruikt meenemen in de presentatie(s) om ze nog eens onder de aandacht te brengen van de medewerk(st)ers.
Zie ook: https://www.kochconsultancy.nl/voorlichting-training/awareness-sessies-klassikaal

E-learning
Met een abonnement op het E-Learning platform kunt de medewerk(st)ers een leerprogramma aanbieden die ze kunnen uitvoeren wanneer het hen het beste uitkomt. De e-learning modules worden in de vorm van korte filmpjes op de computer afgespeeld. Het is ook mogelijk om bepaalde modules te bundelen in een "pakket" wat vervolgens aangeboden wordt aan de medewerk(st)ers. Het E-learning platform bevat tevens een aantal Posters en Cartoons die gebruikt kunnen worden om de aandacht voor security en privacy op een leuke, humoristische manier actueel te houden.

Met het E-learning platform is het ook mogelijk om zelf onbeperkt phishingtesten uit te voeren. De phishing e-mails en de landing pages kunnen worden gekozen uit een bibliotheek met diverse mogelijkheden. Zie ook: https://www.kochconsultancy.nl/voorlichting-training/e-learning-phishingtesten

Meten

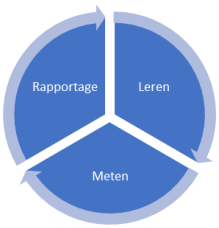
Phishing is momenteel een serieus gevaar voor iedereen op het Internet. De aanvallers "verleiden" hun slachtoffers om ergens op te klikken, een bijlage te openen of vertrouwelijke informatie te verstrekken. De verleiding wordt ingezet door middel van een "aantrekkelijke aanbieding", een "spectaculaire video", een "aanmaning voor een verkeersboete", een "storing in het netwerk", etc.
Bij een phishingtest wordt getest hoe gevoelig de mensen in de organisatie zijn voor dergelijke technieken die via verschillende media uitgevoerd kunnen worden (e-mail, telefoon, SMS, Whatsapp).

Phishingtesten (via e-mail)
Het uitvoeren van regelmatige phishingtesten is een belangrijk element in de awareness campagne. Met dergelijke phishingtesten kun je het effect meten van de awareness campagne. Er wordt een (ongevaarlijke) phishing-mail naar de medewerk(st)ers gestuurd en vervolgens wordt gekeken welk percentage van de medewerk(st)ers op een link klikt of een bijlage opent. Als een medewerker klikt krijgt hij/zij een "leermoment" met een uitleg op welke manier de phishing mail herkend had kunnen worden. In verloop van tijd zal het aantal mensen dat klikt op zo'n phishing e-mail sterk verminderen.
Zie ook: https://www.kochconsultancy.nl/security-awareness/phishing-testen

Het E-Learning platform maakt het mogelijk om onbeperkt zelf de phishingtesten te maken, plannen en uit te voeren.

Mystery Guest
De fysieke beveiliging van bedrijfsinformatie en ICT-middelen speelt natuurlijk ook een belangrijke rol bij het inschatten van de risico's. De Mystery Guest is een onderzoeker die zich voordoet als bijvoorbeeld een printermonteur. De Mystery Guest zal vervolgens onderzoeken in hoeverre het mogelijk is om ongeautoriseerd toegang te krijgen tot werkruimtes, bedrijfsinformatie, computers, kasten, klantendossiers, etc.
Zie ook: https://www.kochconsultancy.nl/security-awareness/mystery-guest

Rapportage

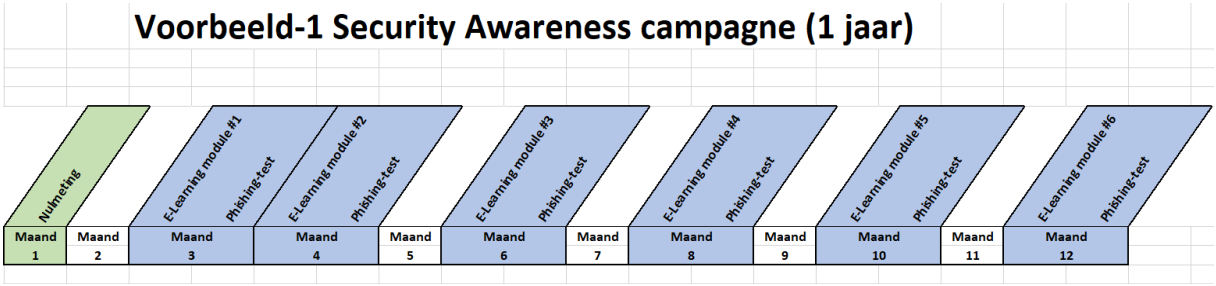


U krijgt de beschikking over professionele rapportages met de resultaten van de trainingen en phishingtesten. Hierbij wordt het effect van de awareness campagne inzichtelijk. Dergelijke rapportages zijn met name ook geschikt om op te nemen in de AVG privacy-administratie.

Voorbeelden van Awareness campagnes

Hieronder twee voorbeelden van hoe een awareness campagne ingericht zou kunnen worden over een periode van 1 jaar. Een campagne wordt altijd met de klant goed doorgesproken en daarbij worden de activiteiten en looptijd van de campagne gekozen die het beste bij de organisatie past.

Voorbeeld 1
In dit overzicht ziet u een basis awareness campagne met een looptijd van 1 jaar waarin uitsluitend phishingtesten en E-learning modules zijn opgenomen:



De campagne start in maand 1 met een nulmeting bestaande uit een online enquêteformulier en een phishingtest. Na deze nulmeting is er inzicht in de huidige situatie met betrekking tot het bewustzijn van de medewerk(st)ers in de organisatie op het gebied van security en privacy.

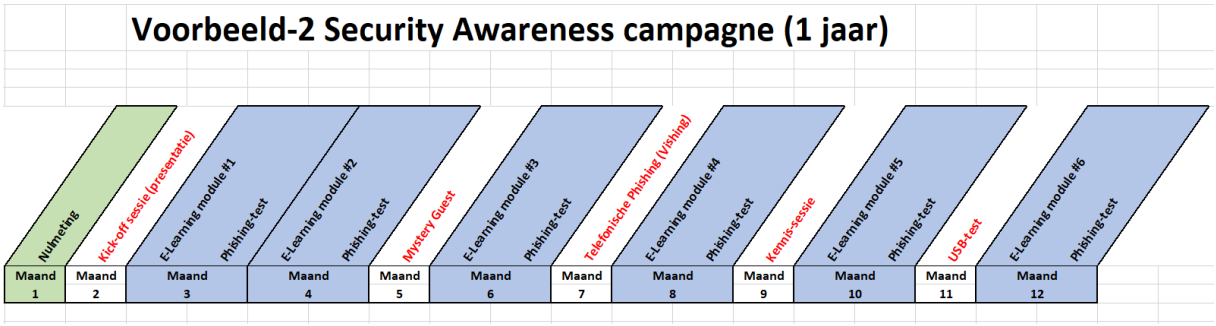
Vervolgens wordt er in maand 3 en in maand 4 een E-learning module aangeboden en een phishingtest uitgevoerd. De reden dat dit twee maanden achter elkaar gebeurt is om de organisatie een “boost” te geven over de onderwerpen security en privacy.

Daarna zal er 2-maandelijks een E-learning module worden aangeboden en een Phishingtest worden uitgevoerd. Dit zou bijvoorbeeld ook kunnen veranderen naar een maandelijkse e-learning module en een 2-maandelijkse phishingtest.

Het gehele programma kan ook uitgespreid worden over een langere looptijd.
Gedurende de gehele looptijd van de campagne kan gebruik gemaakt worden van Posters en Cartoons om medewerk(st)ers (én gasten) op een leuke manier te herinneren aan het belang van security en privacy.

Voorbeeld 2

In dit tweede overzicht ziet u een voorbeeld van een awareness campagne met een looptijd van 1 jaar waarin naast de E-learning modules en de phishingtesten ook een aantal additionele activiteiten zijn opgenomen:



De campagne start in maand 1 met een nulmeting bestaande uit een online enquêteformulier en een phishingtest. Na deze nulmeting is er inzicht in de huidige situatie met betrekking tot het bewustzijn van de medewerk(st)ers in de organisatie op het gebied van security en privacy.

In maand 2 wordt er een kick-off sessie georganiseerd voor de medewerkers waarin de awareness campagne wordt aangekondigd en het belang ervan wordt uitgelegd. Deze kick-off sessie kan klassikaal zijn maar het kan ook bestaan uit één of meerdere online presentaties (webinars) waarvoor de medewerkers zich kunnen aanmelden.

Vervolgens wordt er in maand 3 en in maand 4 een E-learning module aangeboden en een phishingtest uitgevoerd. De reden dat dit twee maanden achter elkaar gebeurt is om de organisatie een “boost” te geven over de onderwerpen security en privacy.

In maand 5 staat er in dit voorbeeld-schema een Mystery Guest bezoek gepland. Dit zou uiteraard ook een andere activiteit kunnen zijn.

Daarna zal er 2-maandelijks een E-learning module worden aangeboden en een Phishingtest worden uitgevoerd. Dit zou bijvoorbeeld ook kunnen veranderen naar een maandelijkse e-learning module en een 2-maandelijkse phishingtest.

In maand 7, 9 en 11 kunnen er ook additionele activiteiten gepland worden zoals een USB-test, een kennis-sessie (online of klassikaal) over een specifiek onderwerp naar keuze en een Vishingtest (Vishing = Phishing via de telefoon).

Het gehele programma kan ook uitgespreid worden over een langere looptijd.
Gedurende de gehele looptijd van de campagne kan gebruik gemaakt worden van Posters en Cartoons om medewerk(st)ers (én gasten) op een leuke manier te herinneren aan het belang van security en privacy.

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