KOCHCONSULTANCY
Security- & Privacy Awareness

Awareness Vergroting

Security
Privacy

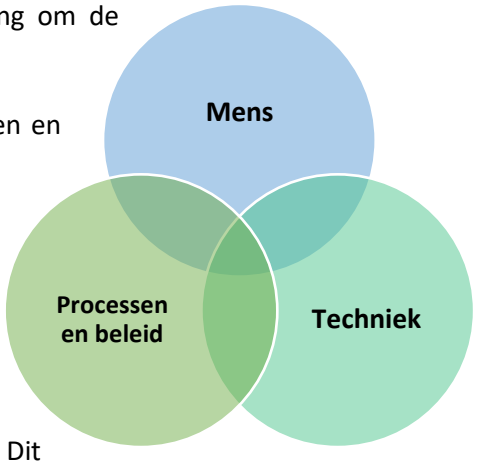
Maak uw medewerk(st)ers bewust.
Uw organisatie wordt dan weerbaar.

Oktober 2021

MENS, PROCES, TECHNIEK

Security is meer dan alleen techniek

Bij het verlagen van security- en privacy-risico's is het van belang om de volgende 3 belangrijke risico-aspecten in ogenschouw te nemen:



- Mens: Veilig gedrag van medewerk(st)ers met ICT-middelen en informatie
- Organisatie: Beleid, procedures
- Techniek: technische security maatregelen in het netwerk

In de praktijk wordt de focus door bedrijven gelegd op de laatste van de bovengenoemde drie. Er worden vaak verschillende technische security-maatregelen genomen in de vorm van monitoring systemen, Identity & Access management, DLP (Data Leakage Prevention) oplossingen, vulnerability management, etc. Dit zijn belangrijke en nuttige technische maatregelen die serieus bijdragen aan de bescherming van de bedrijfsinformatie.

Maar het is echter niet genoeg. De overige twee risico-aspecten uit het bovenstaande rijtje (mens en organisatie) zijn minstens zo belangrijk. Een goed beleid, juiste afspraken en duidelijke procedures zijn noodzakelijk. En "last but not least" natuurlijk het gedrag van de mensen in een organisatie.

Een veel gehoorde uitspraak is dat de mens "de zwakste schakel" is. Helaas wordt dit bevestigd door de cijfers uit de praktijk. Verreweg de meeste (>70%) cyber-incidenten en datalekken worden veroorzaakt door onveilig gedrag en menselijke fouten.

Awareness is alles

Als mensen niet bewust zijn van de gevaren en dreigingen waaraan ze bloot staan zijn ze een makkelijke prooi voor cybercriminelen. Cybercriminelen richten zich tegenwoordig op de medewerk(st)ers van bedrijven. Wist u bijvoorbeeld dat 91% van de cyber-aanvallen begint met het sturen van een phishing e-mail? Mensen worden hierbij verleid ergens op te klikken waarna ze besmet raken met virussen en/of malware. Grote operationele- en financiële schade is het gevolg. En dan hebben we het maar even niet over de reputatieschade.

Bewustwording (Awareness) is daarom belangrijk. Bewust personeel maakt een organisatie weerbaar. In dit document geven we een opsomming van een aantal diensten waarmee de awareness van de organisatie vergroot kan worden waardoor het aantal cyber-incidenten en datalekken sterk zal verminderen.

SECURITY AWARENESS NULMETING

Krijg inzicht in kennis & gedrag

Hoe informatiebewust zijn de medewerk(st)ers binnen uw organisatie? Kunnen zij gemanipuleerd worden om gevoelige informatie af te geven? Security Awareness metingen geven u hierin inzicht. Technische oplossingen worden regelmatig getest. Test daarom ook de belangrijkste factor in informatiebeveiliging: de mens

	Nulmeting	Uitbreiding*
Online vragenlijst	✓	-
Phishing simulatie	✓	-
Sms phishing	-	✓
Mystery guest	-	✓
Telefonische phishing	-	✓
USB-test	-	✓

* Selectie wordt met de opdrachtgever bepaald

De Security Awareness metingen geven inzicht in het veiligheidsniveau van uw organisatie en het gedrag van medewerk(st)ers. Beveiligingsrisico's komen aan het licht. Een nulmeting geeft u de basis voor meetbare gedragsverandering en actiepunten voor de toekomst.

De nulmeting bestaat uit:

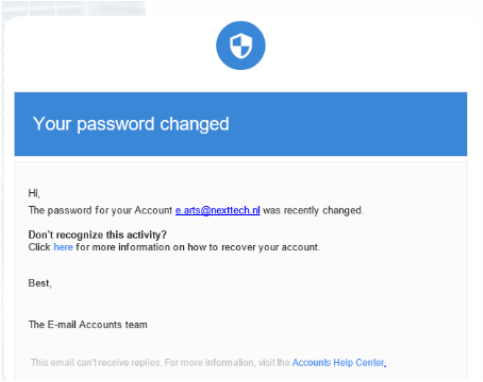
1. online vragenlijst
2. phishingtest.

Ad 1: Online vragenlijst

Er wordt een vragenlijst naar de medewerk(st)ers gestuurd bestaande uit een serie zorgvuldig samengestelde vragen over security gerelateerde onderwerpen, zoals alledaagse praktijksituaties die uw medewerk(st)ers op de werkvloer kunnen tegenkomen. Uit de resultaten van de vragenlijst blijkt in welke mate en op welke onderwerpen de medewerk(st)ers meer of minder veiligheidsbewust zijn en hier ook naar handelen.

Ad 2: Phishingtest

Bij de phishingtest ontvangen alle medewerk(st)ers een nep-phishingmail en wordt er gemeten hoeveel medewerk(st)ers die mail openen en/of doorklikken. Deze phishing test wordt gedaan met een generieke phishingmail. Een maatwerk phishingmail is ook mogelijk.
Het resultaat van deze test geeft aan hoe gevoelig de organisatie is voor phishing en of de medewerk(st)ers in staat zijn om een phishing e-mail te herkennen.



De nulmeting geeft inzicht in:

- Het actuele veiligheidsniveau, gedrag en mate van bewustzijn van medewerk(st)ers.
- De belangrijkste veiligheidsrisico's en focuspunten bij toekomstige security maatregelen.
- De effectiviteit van een trainingstraject

Rapportage

De uitgebreide rapportage geeft u inzicht in de resultaten per afdeling en onderwerp.
Experts zullen de onderzoeksresultaten voorzien van advies waarmee u gericht kan bepalen welke zaken rondom informatiebeveiliging, privacy en Security Awareness aandacht behoeven. Doordat de resultaten inzicht geven in de risico's en mogelijke gevolgen helpt dit bij het creëren van draagvlak bij het bestuur en de directie. We komen de resultaten graag bij u bespreken

Ook te gebruiken als evaluatiemeting

Meet de effectiviteit van een afgerond of nog lopend trainingstraject door de meting in te zetten als evaluatiemeting. Zo krijgt u ook inzicht in de resterende aandachtspunten

KLASSIKALE AWARENESS PRESENTATIES

Koch Consultancy verzorgt klassikale security- en privacy-awareness presentaties bij bedrijven aan huis. Dergelijke presentaties openen de ogen van mensen en zijn erop gericht de deelnemers bewust te maken en ze te stimuleren en motiveren naar veilig gedrag. Het voordeel van een klassikale sessie is dat de deelnemers direct hun vragen kunnen stellen en hun ervaringen kunnen delen met de andere deelnemers. Hierdoor ontstaan er vaak zeer leerzame gesprekken.

Awareness presentatie cybercriminaliteit – De gevaren van het Internet
Duur: 1,5 - 2 uur
Aantal deelnemers: max. 25
Deze presentatie is bedoeld voor iedereen in de organisatie die met ICT-middelen en bedrijfsinformatie werkt. Het is een (niet-technische!) interactieve presentatie waarin we de mensen meenemen naar de wereld van het Internet en de bijbehorende risico's en gevaren. We vertellen over het gebruik en de groei van het Internet en de manieren/methodes die door cybercriminelen worden gebruikt om achter bedrijfs- en persoonlijke informatie te komen.

Er wordt aandacht gegeven aan diverse onderwerpen, zoals:

- Social Engineering: Wat is het, hoe maken cybercriminelen hier gebruik van?
- Phishing (wat is het, welke soorten phishing bestaan er, hoe herken je het, wanneer worden ze gestuurd, wat te doen als je er een ontvangt)
- Veilig gebruik van wachtwoorden (Wat is een sterk wachtwoord, wachtwoord manager, delen van wachtwoorden, gebruik van dezelfde wachtwoorden voor meerdere accounts)
- Diverse vormen van internetfraude. (Nepfacturen, Tikkie-fraude, CEO-fraude, Whatsapp-Fraude)
- Maatregelen die je kunt nemen op je eigen werkplek.

Het is een informele presentatie, vol met voorbeelden, filmpjes en veel interactie. Deze presentatie is een eye-opener voor velen geweest. Het laat de mensen nadenken over de informatiebeveiliging, zowel op het werk als thuis in de privé omgeving. In verband met de interactiviteit kunnen aan deze presentatie maximaal 25 personen deelnemen.

Awareness presentatie privacy (AVG - Datalekken – Phishing)
Duur: 1,5 - 2 uur
Aantal deelnemers: max. 25
Deze presentatie is bedoeld voor iedereen in een bedrijf die gewend is te werken met persoonsgegevens (management, afdelingshoofden, medewerk(st)ers). Tijdens deze presentatie leggen we uit wat de AVG/GDPR en de meldplicht datalekken voor het bedrijf en alle medewerk(st)ers betekent. Een bedrijf komt in contact met de Autoriteit Persoonsgegevens als er een datalek ontstaat. We leggen daarom uit wat datalekken zijn, hoe ze ontstaan, hoe je de kans op datalekken kunt verlagen en wat je moet doen als je een datalek hebt veroorzaakt. Omdat phishing e-mails vaak verantwoordelijk zijn voor het veroorzaken van een datalek behandelen we dit onderwerp ook. We tonen veel voorbeelden van phishing e-mails en leggen we uit hoe phishing technieken (via e-mail, telefoon en Social Media) door cybercriminelen worden ingezet om via de medewerk(st)ers bij bedrijven binnen te dringen. In verband met de interactiviteit kunnen aan deze presentatie maximaal 25 personen deelnemen.

Awareness presentatie (Mix van de bovenstaande presentaties security – Privacy)
Duur: 2 - 2,5 uur
Aantal deelnemers: max. 25
Deze presentatie is een combinatie van de eerder genoemde security- en privacy-awareness presentaties. Deze presentatie duurt ongeveer 2 - 2,5 uur en behandelt naast de security-gerelateerde risico's ook de belangrijke aspecten met betrekking tot de AVG en datalekken. Deze presentatie geeft een compleet beeld en maakt duidelijk waarom security en privacy onlosmakelijk met elkaar verbonden zijn. Tegen geringe meerkosten is het mogelijk om specifieke onderwerpen in de presentatie in te voegen. Denk hierbij aan specifieke gedragsregels / procedures / richtlijnen die gebruikt worden. (Opslag beleid, clean desk policy, Code of Conduct, Thuisgebruik van apparatuur, BYOD, Gebruik van openbaar WIFI, etc.) In verband met de interactiviteit kunnen aan deze presentatie maximaal 25 personen deelnemen.

MANAGEMENT WORKSHOP AVG

Met deze workshop, speciaal gericht op het management van organisaties, vergroten we het bewustzijn en creëren we draagvlak op het gebied van de Europese Privacywetgeving. (AVG / GDPR).

Management workshop AVG/GDPR Privacywetgeving
Duur: 4 uur
Aantal deelnemers: max.12
Deze workshop van 4 uur is speciaal ontwikkeld voor directie, lijnmanagement en afdelingshoofden die verantwoordelijk en/of betrokken zijn bij de verwerking van persoonsgegevens. (Bijv. directie, compliance officers, financiële medewerk(st)ers, personeelszaken, juridische medewerk(st)ers, ICT-personeel). Deze personen dienen goed op de hoogte te zijn van de Europese regels omtrent het beschermen en waarborgen van de privacy van persoonsgegevens in verband met de verplichtingen en de gevolgen voor de aansprakelijkheid, de auditability en de compliance. Er is geen specifieke voorkennis benodigd.

Tijdens de workshop gaan we in op de AVG / GDPR privacywetgeving en de gevolgen van deze Europese wetgeving. Wat moet je doen om aan deze wet te voldoen en welke informatie moet je beschikbaar hebben in de privacy-administratie in het geval van een incident?
Er zal uitgelegd worden wat de verplichtingen zijn die de AVG / GDPR wetgeving oplegt en op welke manier een bedrijf zich kan voorbereiden om te voldoen aan deze wetgeving. Onderwerpen:

- De wet & regelgeving
- Wat zijn de eisen?
- Wat betekent dit voor u?
- Wat moet u minimaal doen?
- Hoe kunt u voldoen?
- Welke maatregelen moet u nemen?

ONLINE AWARENESS PRESENTATIES

Steeds meer medewerk(st)ers werken tegenwoordig vanuit huis. Het is daarom soms uit praktische redenen moeilijk om een klassikale awareness sessie te organiseren. Koch Consultancy verzorgt daarom ook diverse online awareness presentaties. Deze presentaties zijn eenvoudig te volgen, ook als je vanuit huis werkt. De online presentaties kunnen op verschillende manieren worden uitgevoerd:

- Live presentaties
- Automatische presentaties (= opname van een eerdere live presentatie)
- Presentaties die gedurende een bepaalde periode onbeperkt zijn te bekijken

Live presentaties

Live presentaties worden live verzorgd. Hiervoor wordt een datum/tijd afgesproken waarop de presentaties wordt gegeven. De medewerk(st)ers registreren zich voor de presentaties via een URL-link. Op de afgesproken datum/tijd kunnen ze dan via de link in de toegestuurde bevestiging de presentatie online bijwonen. Na de presentatie is er een "replay" beschikbaar waarmee de presentatie gedurende een dag nog is te bekijken.

Automatische presentaties

Een opname van een eerdere Live presentatie kan op verzoek meerdere keren worden "uitgezonden". Hiervoor worden dan meerdere data/tijden afgesproken voor het afspelen van de opname van de eerder verzorgde Live presentatie. Medewerk(st)ers kunnen dan zelf kiezen welke datum/tijd het beste uitkomt om de presentatie te bekijken.

On-Demand presentatie

Een "on-demand" presentatie wordt voor een bedrijf opgenomen en vervolgens gedurende een bepaalde periode beschikbaar gesteld voor alle medewerk(st)ers. Medewerk(st)ers ontvangen een URL-link waarmee ze gedurende die periode (24/7) de presentatie kunnen bekijken. Dit maakt het mogelijk voor de medewerk(st)ers om de presentatie 24/7, eventueel meerdere keren te bekijken. Dit is natuurlijk ideaal voor medewerkers die thuis aan het werk zijn.

Online presentatie: "Phishing - Social Engineering"

Voor wie geschikt: Iedereen die werkt met ICT-middelen als computers, laptops, e-mail, etc.
Duur: Ongeveer 30-40 minuten

In deze presentatie wordt een belangrijke methodiek besproken waar cybercriminelen erg succesvol mee zijn: Social Engineering. Eén van de meest gevaarlijkste vormen van Social Engineering is "Phishing". Er wordt uitgelegd wat phishing is en hoe je phishing kunt herkennen. De verschillende vormen van phishing (via e-mail, SMS, USB-stick, Telefoon) worden duidelijk uiteengezet. Ter illustratie worden veel voorbeelden getoond. Bewust personeel maakt een bedrijf weerbaar. Phishing activiteiten door cybercriminelen zijn verantwoordelijk voor grote schade in het bedrijfsleven. Verlaag dit risico daarom door het bewustzijn van medewerk(st)ers te vergroten zodat ze er niet "intrappen".

Online presentatie: "Passwords"

Voor wie geschikt: Iedereen die werkt met ICT-middelen als computers, laptops, e-mail, etc.
Duur: Ongeveer 30-40 minuten

Iedereen gebruikt (zakelijk en privé) passwords (wachtwoorden) om toegang te krijgen tot verschillende Internet-accounts. Helaas gaat er bij het gebruik van passwords veel fout met betrekking tot de security. In deze presentatie wordt uiteengezet op welke manier je het beste kunt omgaan met passwords. Wat is een sterk password? Hoe kun je ze onthouden? Wat zijn wachtzinnen (passphrases). Wat kan er gebeuren als je hetzelfde password gebruikt voor meerdere accounts? Waarom moet je passwords regelmatig veranderen? Wat is 2-factor authenticatie? Het gebruik van veilige passwords verlaagt het risico van uw bedrijf op het gebied van digitale inbraak en identiteitsfraude.

Online presentatie: "Fraude" (CEO-fraude, Nepfacturen, Whatsapp-fraude, Tikkie-fraude)

Voor wie geschikt: Iedereen die werkt met ICT-middelen als computers, laptops, e-mail, etc.
Duur: Ongeveer 30-40 minuten

Steeds meer bedrijven en privé-personen worden slachtoffer van een van de vele vormen van fraude. De schade kan daarbij oplopen tot zeer grote bedragen. Deze presentatie maakt medewerkers bewust van de verschillende vormen van fraude (CEO-fraude, nepfacturen, whatsapp-fraude, Tikkie-fraude) en op welke manier de criminelen te werk gaan. Bewuste medewerk(st)ers kennen deze vormen van fraude en trappen er niet in!

Online presentatie: "AVG voor Management"

Voor wie geschikt: Directie, lijnmanagement, afdelingshoofden van bedrijven en organisaties
Duur: Ongeveer 30-40 minuten
De AVG privacywetgeving is nog steeds bij veel bedrijven niet of niet volledig geïmplementeerd. Dit is niet nodig en het bedrijf loopt dan grote risico's op het moment van een privacy-incident. Tijdens deze presentatie wordt alles eens op een rijtje gezet over hoe een bedrijf compliant kan worden (en blijven!) aan de AVG. Onderwerpen die worden behandeld:

- Wat is de AVG?
- Persoonsgegevens - verwerkingen
- Welke verplichtingen zijn er?
- De AVG Privacy administratie
- Inzageverzoeken
- Privacy Statement
- Verwerkersovereenkomsten
- De FG (Functionaris Gegevensbescherming)
- Meldplicht datalekken
- De 5 stappen naar compliance - RI&E-Privacy

Online presentatie: "AVG - Datalekken voor medewerk(st)ers"

Voor wie geschikt: Alle medewerk(st)ers van bedrijven en organisaties
Duur: Ongeveer 30-40 minuten
Om datalekken en privacy-incidenten te voorkomen is het van belang dat alle medewerkers van een organisatie op de hoogte zijn van het belang van de AVG privacywetgeving en de mogelijke consequenties als een bedrijf niet goed omgaat met de bescherming van persoonsgegevens. In deze presentatie wordt voor de medewerkers in duidelijke taal uitgelegd wat de AVG is, wat persoonsgegevens zijn en waarom er voorzichtig mee omgegaan dient te worden. Daarna wordt ingegaan op wat een datalek is, waarom het voorkomen van datalekken belangrijk is, hoe ze ontstaan en hoe je datalekken kunt voorkomen. Bij het onderwerp "hoe ontstaan datalekken" zal in grote lijnen worden verteld over phishing technieken door hackers en het veilig gebruiken van wachtwoorden.

E-LEARNING

Om beveiligingsincidenten te minimaliseren is het van belang dat medewerk(st)ers bewust zijn van de mogelijke gevolgen van hun handelingen. Het creëren van bewustwording en gedragsverandering is geen eenmalige actie, maar een structureel proces. E-learning is hiervoor uitermate geschikt, omdat het de mogelijkheid biedt om leermodules periodiek uit te rollen. Medewerk(st)ers kunnen de leerstof volgen op het moment dat het hen het beste uitkomt op computer, tablet of smartphone.

Modulair opgebouwd

Bij het afsluiten van een abonnement krijgt u toegang tot alle beschikbare leermodules. De modules behandelen verschillende thema's op het gebied van informatiebeveiliging en privacy. U krijgt daarnaast automatisch toegang tot nieuw ontwikkelde modules. De volgorde, selectie en timing kan aangepast worden. Zo kunt u een leerprogramma samenstellen die perfect aansluit op de wensen van uw organisatie.

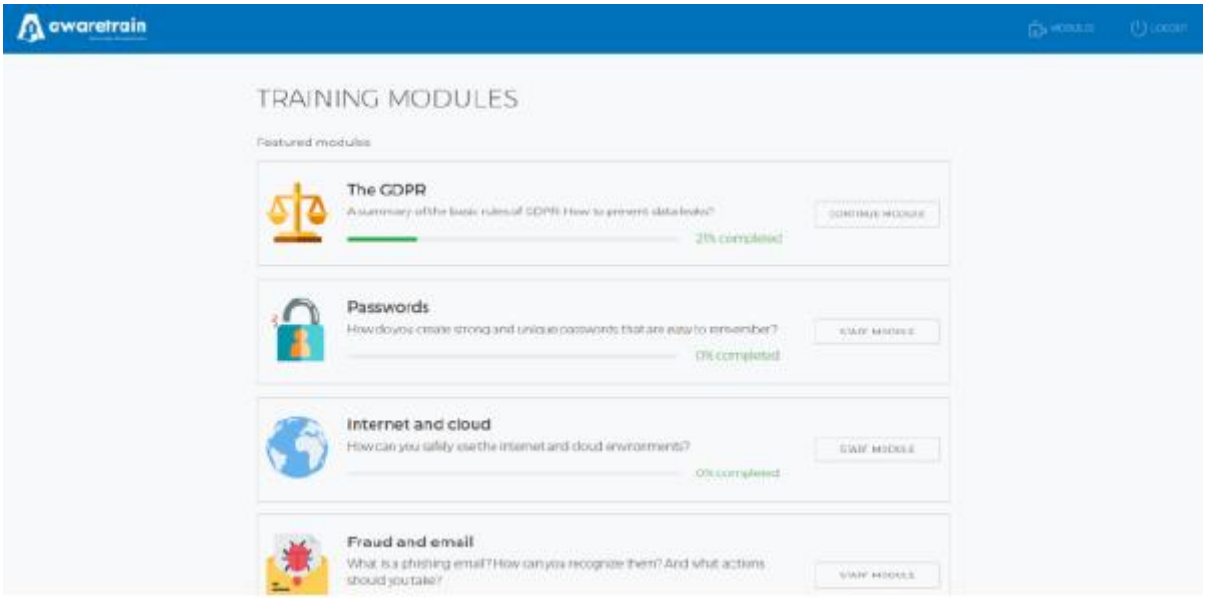
Onderwerpen van de E-learning modules:

Belang van security awareness
Sterke wachtwoorden
Veilig surfen op internet
Beveiligde verbinding
Informatie in de cloud
Gevaren van cybercrime
Phishing
De veilige computer
De veilige werkplek
Datavernietiging
Social engineering
Mobiele apparaten
Wifi
Apps downloaden
USB-opslag
Privacy
Digitale bedrijfsfraude
De AVG

In totaal zijn er meer dan 40 modules beschikbaar in 8 talen. Deze worden regelmatig aangevuld met nieuwe actuele modules over security- en privacy-gerelateerde onderwerpen.

Helder & toegankelijk

Geen overdaad aan regels, maar direct toepasbare tips om veiliger te werken, ook in privésituaties. De e-learning bestaat uit een serie van korte en toegankelijke modules van 5 - 15 minuten die bestaan uit geanimeerde video's afgewisseld met oefenvragen. Uw medewerk(st)ers leren wat hun rol is op het gebied van informatiebeveiliging, waardoor zij veilig(er) en bewust(er) gaan werken. Denk hierbij aan het herkennen van phishing e-mails en het versturen van (gevoelige) gegevens. Ook is er een afsluitende kennistest beschikbaar. Bij positief resultaat ontvangt men het Security Awareness certificaat.



Houd zelf de regie

U krijgt toegang tot het online leer-platform. Hiermee kunt u zelf leerprogramma's samenstellen, gebruikers en groepen beheren, en (per module) rapporten en certificaten genereren. Betrokken managers hebben realtime inzicht in de progressie en resultaten van de medewerk(st)ers. Dit alles in een gebruiksvriendelijke user interface. Zo heeft u altijd het juiste leermateriaal voor de juiste persoon op het juiste moment beschikbaar. Heeft u een eigen LMS? Het integreren van onze content in uw LMS is mogelijk.

Meertalig

De e-learning is beschikbaar in 8 talen: Nederlands, Engels, Duits, Frans, Spaans, Portugees, Pools en Tsjechisch. Op aanvraag kan elke gewenste taal ontwikkeld worden.

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 e-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 e-mail herkend had kunnen worden. In verloop van tijd zal het aantal mensen dat klikt op zo’n phishing e-mail sterk verminderen. Er zijn diverse voor gedefinieerde phishingmails beschikbaar die in te zetten zijn bij elke organisatie.

Tegen meerprijs is het mogelijk om inhoudelijke aanpassingen aan de e-mail en landingspagina te doen. De e-mails variëren van inhoud en niveau om zo het werkelijke gedrag van de medewerk(st)ers op regelmatige basis te kunnen testen.

SMS Phishing testen

Een groeiend aantal phishing-aanvallen wordt uitgevoerd via SMS, Facebook of WhatsApp. Veel mensen zijn hiervan niet op de hoogte en vertrouwen de inhoud van een SMS dan ook eerder dan de inhoud van een e-mail. Bij een SMS phishingtest wordt er een (ongevaarlijke) SMS gestuurd naar het mobiele telefoonnummer van mensen. Hierbij wordt een trucje (spoofing) uitgehaald waardoor de SMS van Voicemail (1233) afkomstig lijkt te komen. De SMS bevat een link naar een landingspagina die (net als de SMS) aan te passen is. Er wordt gemeten hoeveel mensen er klikken op de link in de SMS.

Telefonische Phishingtesten (Vishing)

Telefonische phishing, ook wel “Voice Phishing” of “Vishing” genoemd, is een succesvolle manier voor aanvallers om aan vertrouwelijke informatie te komen. Voor deze test worden medewerk(st)ers telefonisch benaderd door een onderzoeker die zich bijvoorbeeld voordoet als een helpdesk medewerker. Tijdens het telefoongesprek probeert de onderzoeker vertrouwelijke informatie te verkrijgen zoals bijvoorbeeld inlog-gegevens.

SECURITY AWARENESS AS A SERVICE

Met Security Awareness as a Service (SAaaS) combineren we de essentiële security awareness diensten om de medewerk(st)ers van uw organisatie veiligheidsbewust te maken in een abonnementsvorm.

Varianten & inhoud
Security Awareness as a Service is beschikbaar in twee abonnementsvormen:

- Essentials
- Premium.

Beide varianten geven toegang tot de volledige bibliotheek van online e-Learning modules. Nieuw ontwikkelde modules worden ook automatisch toegevoegd.

In de Premium variant zijn een nulmeting en phishing simulaties inbegrepen. Hierdoor kan gemeten worden of de training het beoogde effect heeft, want uiteindelijk gaat het om de vraag: gebruiken de medewerk(st)ers de opgedane kennis ook daadwerkelijk in de dagelijkse praktijk?

Premium	Essentials
Toegang tot alle modules ✓	Toegang tot alle modules ✓
Toegang tot privacy & AVG modules ✓	Toegang tot privacy & AVG modules ✓
Nieuwe modules ✓	Nieuwe modules ✓
Posters & cartoons ✓	Posters & cartoons ✓
Nulmeting (voorafgaand) ✓	Nulmeting (voorafgaand) ✗
Phishing simulatie (2-maandelijks) ✓	Phishing simulatie (2-maandelijks) ✗

Online training (E-Learning)
De e-learning zoals eerder in dit document beschreven is volledig beschikbaar in het “Essentials” en in het “Premium” abonnement. U heeft toegang tot alle modules.

Posters & Cartoons
Om de betrokkenheid te vergroten en het effect van het programma te versterken bieden we een ondersteunend contentpakket aan. Deze bestaat uit een serie van posters en cartoons die perfect aansluiten bij de verschillende thema’s die in de modules worden behandeld. Ideaal om te gebruiken in uw interne- en externe communicatie over security en privacy. De content is beschikbaar in 8 verschillende talen.

Nulmeting
De nulmeting is beschikbaar in het “Premium” abonnement.
Het is een goede manier om inzicht te krijgen in de huidige situatie met betrekking tot de security- en privacy-awareness. De nulmeting bestaat uit een online kennistest en een phishingtest.

- Online Kennistest
  De online kennistest bestaat uit een online vragenlijst over verschillende thema’s. Hiermee wordt gemeten in welke mate uw medewerk(st)ers veiligheidsbewust zijn en of zij daadwerkelijk veilig werken en handelen. De rapportage bevat een adviesplan over welke specifieke zaken op het gebied van informatiebeveiliging, privacy en security awareness extra aandacht vereisen.

- Phishing simulatie
  Bij de nulmeting wordt een phishingtest uitgevoerd. Alle medewerkers ontvangen een (ongevaarlijke) phishing e-mail en er wordt gemeten hoeveel mensen er op een link in deze phishing e-mail klikken. Dit geeft goed inzicht in de gevoeligheid van de organisatie op het gebied van phishing en hoe groot het risico is wat wordt gelopen.

OVERIGE DIENSTEN

Hieronder een overzicht van een aantal overige nuttige diensten die ingezet worden om de awareness in een organisatie te vergroten.

Mystery guest

Een onderzoeker komt als “mystery guest” bij u langs op locatie, bijvoorbeeld in de rol van printermonteur of service provider, om uw organisatie te infiltreren. We brengen in kaart in hoeverre er ongeautoriseerd toegang tot het pand en werkruimtes verkregen kan worden, werkstations vergrendeld zijn, inloggegevens achterhaald kunnen worden en toegang is tot vertrouwelijke informatie en dossiers van printers, papierbakken en bureaus. Dit onderzoek geeft u belangrijke informatie over de kwetsbaarheid van uw organisatie van binnenuit.

USB drop test

USB sticks en andere externe opslagmedia worden vaak gebruikt om gegevens uit te wisselen. Deze USB-opslag-media worden vaak verloren, vergeten of gestolen. Hackers verspreiden ook via USB-sticks hun virussen en malware. Een gevonden USB-stick kun je dus beter niet in je computer stoppen. Bij een USB-test worden in en rond een bedrijf een aantal USB-sticks neergelegd op “strategische” plekken zoals op het parkeerterrein, bij een koffiemachine of bij een printer. Vervolgens wordt gemeten hoeveel mensen in de verleiding zijn gekomen om de USB-stick in zijn/haar werkstation te stoppen.

Serious game spelshow

Duur: 1,5 uur

Aantal deelnemers: max. 60 (10 teams van 6 pers.)

Deze spelshow is een leuke en toegankelijke kennismaking met Security Awareness. Perfect om in te zetten in een bredere bewustwordingscampagne. Tijdens de spelshow strijden uw collega's in teamverband om de Awareness-bokaal. Ze worden door onze quizmaster uitgedaagd om in verschillende spelrondes na te denken over informatieveiligheid, cybercrime en privacy. Plezier, competitie en bewustwording staan centraal.

Phishing Quiz

Een uitdaging voor zelfs de meest oplettende medewerker. Deelnemers krijgen verschillende e-mailscenario's voorgelegd, deels legitiem, deels phishing. Vervolgens geeft de deelnemer aan hoe hij zou handelen in de specifieke situatie. Punten worden gescoord op basis van de gemaakte keuze. Na elk scenario volgt een uitgebreide uitleg over het beste antwoord. Door verschillende phishing technieken te gebruiken maken medewerk(st)ers kennis met de manieren waarop criminelen hen proberen te manipuleren.

Contact informatie

Koch Consultancy BV
Beetzlaan 5
3762 CA Soest

Tel: 06-53233269

Website: www.kochconsultancy.nl
E-mail: info@kochconsultancy.nl

KOCHCONSULTANCY
Security- & Privacy Awareness