KOCHCONSULTANCY
Security- & Privacy Awareness

Informatie + Prijzen

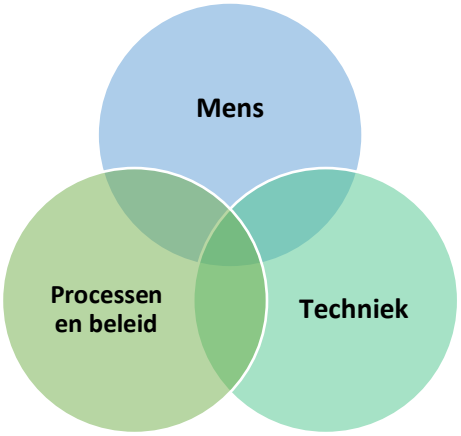
4-uur training
Security Awareness

Per Januari 2023

Awareness

Aanleiding

Vergroting van de security- en privacy-awareness van medewerkers is een belangrijke maatregel om de cyber-risico's van een organisatie te verlagen. Meer dan 70% van alle cyber-incidenten wordt veroorzaakt door menselijk gedrag. Er zijn drie aandachtsgebieden die geadresseerd moeten worden om risico's te verlagen: "Mens", "Proces" en "Techniek". Naast de technische en organisatorische securitymaatregelen is het dus van belang ervoor te zorgen dat de medewerk(st)ers van een bedrijf veilig en verantwoord omgaan met de beschikbaar gestelde ICT-middelen en bedrijfsinformatie.



Bewust personeel maakt de organisatie weerbaar. Dat verlaagt het aantal cyber-incidenten en datalekken. Een bewuste medewerk(st)er:

- Is bewust van de cyber-risico's waaraan hij/zij blootstaat
- 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
- Is bekend met de verschillende vormen van internet-fraude
- Begrijpt het belang van het veilig omgaan met ICT-middelen als computers, laptops, smartphones, tablets, printers, etc.
- Weet waar hij/zij gegevens kan/mag opslaan (lokaal? Cloud? USB-drives?)
- Deelt vertrouwelijke / gevoelige gegevens niet met ongeautoriseerde personen.
- Is bewust van het bestaan van de AVG privacywetgeving, ziet het belang ervan in en begrijpt waarom bedrijven zich hieraan moeten houden.
- Weet waar hij/zij een security- of privacy-incident (datalek) intern moet melden.

Security Awareness

"Security Awareness" is een breed begrip. Het omvat meerdere onderwerpen waarvan mensen tegenwoordig bewust moeten zijn. Dit geldt niet alleen op het werk, maar zéker ook in de privé sfeer. Bedrijven realiseren zich ook dat met de opkomst van thuiswerken en "hybride" (gedeeltelijk thuis) werken het veilige gedrag van mensen steeds belangrijker wordt om het risico te verlagen dat ze slachtoffer worden van cybercriminelen.

Thuis op de bank of aan de keukentafel staan mensen ook bloot aan cyber-risico's met hun laptop, tablet of smartphone. En wellicht zijn die risico's thuis zelfs groter dan op het werk, aangezien de mensen thuis wat minder alert zijn en de securitymaatregelen thuis over het algemeen minder professioneel zijn.

Security Awareness training

Er zijn veel activiteiten beschikbaar die erop zijn gericht het bewustzijn van mensen te vergroten. Eén daarvan is het verzorgen van Security Awareness training. Dit is een goede manier om de mensen bewust te maken over de diverse vormen van cybercriminaliteit en internet fraude. Het is daarbij van belang dat de presentaties geschikt zijn voor alle medewerk(st)ers. Dus géén technische verhalen maar een praktisch verhaal met Nederlandse voorbeelden en volop mogelijkheid voor interactie. Tijdens dergelijke presentaties ontstaan meestal heel interessante gesprekken met de groep waarin mensen openlijk hun ervaringen delen en hun vragen stellen.

Diverse modules vormen samen een compleet programma

Voor het vergroten van het bewustzijn op het gebied van security en privacy zijn een aantal modules beschikbaar die allemaal een specifiek onderwerp behandelen.

Het betreft de volgende modules t.b.v. Security Awareness voor medewerk(st)ers

- Inleiding – (De risico's van) Internet
- Social Engineering / Phishing
- Veilig omgaan met passwords
- Diverse vormen van Internet Fraude

Deze modules vormen tezamen een compleet programma van een dagdeel. (ongeveer 4 uur).
Het is ook mogelijk om deze modules "los" aan te bieden, dit gebeurt meestal door middel van online sessies maar deze modules (elk ongeveer een uur) kunnen natuurlijk ook bij de klant aan huis worden verzorgd.

4-uur klassikale Security Awareness training

Dit programma (duur: ongeveer 4 uur) wordt samengesteld uit de inhoud van de volgende modules:

- Inleiding – (De risico's van) Internet
- Social Engineering / Phishing
- Veilig omgaan met passwords
- Diverse vormen van Internet Fraude

Tijdens deze 4-uur training worden bovenstaande onderwerpen uitgebreid besproken en worden er veel voorbeelden gegeven.

Hieronder een overzicht van de onderwerpen die in de verschillende onderdelen worden behandeld.

Inleiding – (de risico's van) Internet

- Internet – gebruik
- Keerzijde van de medaille: Cybercriminaliteit
- En toch … we maken ons niet zo druk? (voorbeelden)
- Risicoverlaging: De mens is belangrijke factor
- Wat is hacken?
- Wat motiveert hackers?

Social Engineering /phishing

- Social Engineering – Wat is het?
- Misbruik van menselijke eigenschappen – voorbeelden
- Phishing
- Voorbeelden
- Ransomware
- Hoe herken je phishing?
    - "Technische" controle
    - "Content" controle
- Wat te doen als je een phishing e-mail ontvangt?
- Andere media die gebruikt worden voor Phishing

Veilig omgaan met passwords

- Passwords – Waarom belangrijk!
- Veel passwords leidt tot gebruik van makkelijke passwords (bijv. 123456)
- Hoe komen "ze" achter mijn password?
- Waarvoor worden gestolen passwords gebruikt?
- Wat is een veilig password?
- Passwords delen – 1 password voor meerdere accounts
- Passwords onthouden – Password Manager
- Multi Factor Authenticatie – Wachtwoord beleid

Diverse vormen van Internet Fraude

- CEO-Fraude
- Tikkie-Fraude
- Whatsapp Fraude
- Dating Fraude
- QR-Fraude
- Nepfacturen

De agenda van de 4-uur Security Awareness training kan in op verschillende manieren worden ingedeeld:

- Gehele training van 9.00 uur – 13.00 uur
- Gehele training van 13.00 uur – 17.00 uur
- Deel 1 in de ochtend (2 uur) en deel 2 in de middag (2 uur)
- De training kan ook in twee delen over verschillende dagen worden verzorgd. (bijvoorbeeld tweemaal een ochtend van 10.00 uur tot 12.00 uur)

4-uur Security Awareness Training	**Prijs per training** **1-2 Trainingen**	**Prijs per training bij meerdere trainingen:** **3-5 Trainingen**	**Prijs per training bij meerdere trainingen:** **>5 Trainingen**
Inleiding – (De risico's van) Internet Social Engineering – Phishing Veilig omgaan met passwords Diverse vormen van Internet Fraude	€ 1.295	€ 1.165 (10% korting)	€ 1.036 (20% korting)
	Max. 15 pers.	Max. 15 pers.	Max. 15 pers.

Condities:

- *Bij bedrijf aan huis*
- *Per training maximaal 15 deelnemers*
- *Voor bedrijven met meer deelnemers gelden kortingen voor de extra trainingen*
- *Reiskosten worden berekend @ 45 cent per gereden kilometer (van/naar Soest)*
- *Alle genoemde prijzen zijn excl. BTW*

Aanpassen aan uw bedrijfssituatie – Voorbereidend gesprek

Een security awareness training wordt altijd voorafgegaan door een MS-Teams gesprek over de bedrijfsspecifieke zaken die moeten worden meegenomen in de training. Dit gesprek is 1-2 weken voordat de training wordt verzorgd. Denk hierbij aan een reeds voorgekomen cyber-incident bij het bedrijf, een gedragscode, een opslagbeleid, password-beleid, clean-desk policy, toegangsbeleid, etc. Op deze manier maken we de training effectiever en goed toepasbaar voor de medewerk(st)ers.

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