WHITEPAPER

Security Awareness:

Maak medewerkers tot een sterke schakel in de beveiliging van uw IT-omgeving

Medewerkers zijn in veel organisaties de zwakste schakel bij informatiebeveiliging. Onderzoek heeft namelijk uitgewezen dat ruim 70% van de beveiligingsincidenten wordt veroorzaakt door menselijke fouten. Is de techniek goed op orde, dan is dit zelfs meer dan 90%. Houd (cyber)criminelen buiten de deur en voorkom incidenten en datalekken door medewerkers te leren om gevaren te herkennen en te pareren. Maak uw medewerkers tot de sterkste schakel!

Maak medewerkers tot een sterke schakel in de beveiliging van uw organisatie

De mens is van nature behulpzaam. Een goede eigenschap, maar cybercriminelen misbruiken de goedgelovigheid van werknemers steeds vaker om de IT-omgeving binnen te dringen. Deze nieuwe benaderingswijze duidt erop dat cybercriminelen blijven zoeken naar zwakke plekken binnen organisaties.

Een belangrijke eerste stap is een optimale technische beveiliging van de IT-omgeving. Nu organisaties dit steeds beter op orde hebben, zoeken cybercriminelen steeds vaker naar andere ingangen. Uit onderzoek blijkt dat maar liefst 70% van de IT-beveiligingsincidenten wordt veroorzaakt door menselijke fouten. Daarom is het belangrijk om te werken aan het veiligheidsbewustzijn (Security Awareness) van uw medewerkers.

Waarom Security Awareness?

De beveiliging van een IT-omgeving wordt vaak vergeleken met een huis. Goede sloten op deuren en ramen (IT-Security) zijn een must, maar als de bewoner de deur opent voor een vreemde (hacker, phishingmail) dan is de schade niet te overzien. Daarom dienen IT-Security en Awareness hand in hand te gaan voor een optimale beveiliging. Medewerkers zijn zich onvoldoende bewust van hun eigen rol op het gebied van IT-veiligheid en de schade die daarmee kan worden aangericht.

> Beschikbaarheid van bedrijfsapplicaties en data is een must. Het is de ruggengraat van een organisatie en het moet absoluut voorkomen worden dat kwaadwillenden hier toegang toe krijgen. Het is daarom zaak om met mens én techniek een veilige omgeving te creëren.

Maarten de Rooij, IT Business Professional van ACA IT-Solutions

Meer dan een verdacht mailtje

Het eerste waar veel mensen aan denken bij cybercriminaliteit zijn phishing e-mails. Organisaties en hun werknemers moeten echter op veel meer zaken letten.

Voorbeelden van risico's:

- Ransomware
- Social engineering
- Onveilige data uitwisseling
- Onveilig wachtwoordbeheer
- Gevaarlijke URL's, apps en downloads
- Onveilige verbindingen andere werklocaties
- Onvoldoende fysieke bedrijfsbeveiliging

Leerdoelen werknemers:

- Phishing leren herkennen
- De waarde van informatie juist inschatten
- Individuele verantwoordelijkheden nemen
- Het verschil tussen 'beveiligd' en 'veilig' weten
- Het belang van 'clean desk' inzien
- Eigen werkwijze en processen heroverwegen
- Social engineering leren herkennen

Antwoord op social engineering

Social engineering is een techniek die wordt gebruikt door cybercriminelen om de zwakste schakel binnen de organisatie (de mens) te gebruiken om toegang te krijgen tot uw organisatie. Het doel is financieel gewin te behalen, malware te installeren of vertrouwelijke informatie te bemachtigen, zoals gebruikersnamen, wachtwoorden of bankgegevens.

Door werknemers bewust te maken van de gevaren en te leren hoe te acteren bij verdachte activiteiten, wordt de IT-omgeving veilig en worden risico's significant verlaagd. Security Awareness is dus het antwoord op criminelen die social engineering toepassen.

Security Awareness en GDPR-privacywetgeving

Van het bedrijfsleven en (overheids)instanties wordt verwacht dat zij alles in het werk stellen om op een veilige en respectvolle manier met data en persoonsgegevens om te gaan. Dat is kort samengevat de inhoud van de nieuwe GDPR-privacywet die vanaf 25 mei 2018 van kracht is. Security Awareness is dan ook nauw verbonden aan de GDPR-privacywetgeving. Sterker nog, het is een vereiste. Er wordt namelijk niet alleen verwacht dat alles op technisch vlak op orde is. Ook werknemers dienen te weten wat van hen wordt verwacht en hoe zij op een veilige en verantwoorde wijze omgaan met de IT-omgeving, applicaties die zij gebruiken en de data die ze verwerken.

Zes redenen om te starten met Security Awareness

Gegevens zijn goud waard
Stelt u zich eens voor dat u opeens alle data kwijt bent en geen toegang meer heeft tot uw bedrijfsapplicaties. Cybercriminelen vragen losgeld of verkopen uw (klant)data.

Reputatieschade is funest
De GDPR schrijft voor dat gedupeerden geïnformeerd moeten worden. Dit kan leiden tot enorme reputatieschade, zeker als dit ook in de media terecht komt.

Social engineering neemt toe
Steeds vaker richten cybercriminelen zich middels social engineering direct op uw medewerkers. Getracht wordt de medewerker te misleiden en zo toegang te krijgen tot uw bedrijf, IT-omgeving en bedrijfsgegevens.

Bewustzijn bespaart geld
Door medewerkers bewust te maken van hun individuele verantwoordelijkheden worden incidenten voorkomen en bespaart u flinke kosten voor uw organisatie en IT-afdeling.

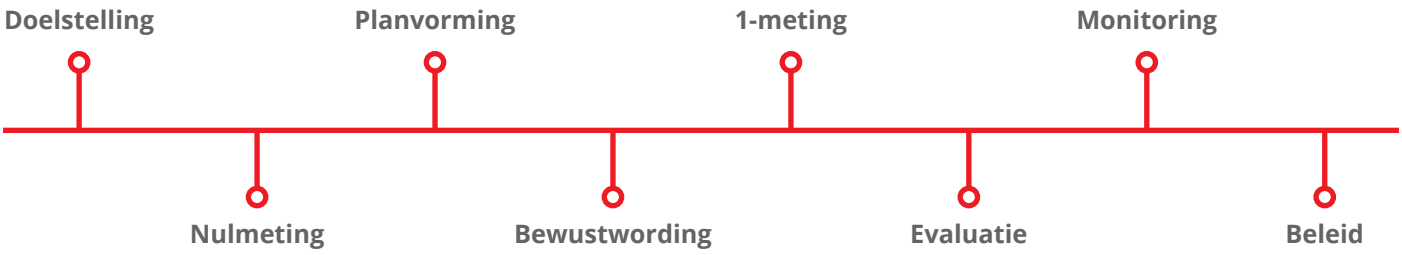
Verwachtingspatroon relaties
Klanten vertrouwen erop dat uw organisatie veilig en respectvol met hun privacygevoelige data omgaat. Een cyberaanval of onoplettendheid van een medewerker kan leiden tot vertrouwensbreuk en verlies van klanten.

Wetgeving vereist actie
De GDPR-privacywet dwingt organisaties om op veilige en verantwoorde manier met de IT-omgeving, applicaties en bedrijfsdata om te gaan.

Beemdstraat 38 5652 AB Eindhoven
T +31 (0)40 - 8 800 100 | info@aca-it.nl | www.aca-it.nl

·A·C·A· IT-SOLUTIONS

Stapsgewijs naar bewustzijn



Voor wie is Security Awareness?

Security Awareness wordt vaak gezien als iets voor het management en de IT-afdeling. Dat is een misvatting. Het is juist van belang dat elke medewerker op de hoogte is van de cybergevaren en weet hoe hij of zij moet handelen. Want elke medewerker kan een gevaarlijke e-mail ontvangen, een virus downloaden, vertrouwelijke gegevens verliezen of een onbevoegd persoon toegang verschaffen tot het bedrijfsnetwerk.

Het advies is om alle medewerkers te betrekken bij Security Awareness. Daarbij kan het wenselijk zijn om bepaalde groepen binnen het bedrijf anders of intensiever te trainen. Denk hierbij aan het management, de IT-afdeling en medewerkers die zich met bedrijfskritische processen bezig houden.

Onze diensten

- Phishing Tests
- Social Engineering
- Klassikale Trainingen
- E-learning
- Rapportages

Professionele leermethodes en ondersteuning

ACA IT-Solutions beschikt over een gespecialiseerd team dat u kan helpen met de opzet en uitrol van het Security Awareness programma. Het IT-Security Awareness programma stemmen wij, in samenspraak met u, af op uw organisatie, uw medewerkers en uw doelstellingen, zodat maximaal resultaat wordt behaald. Daarbij kunnen verschillende leermethodes worden ingezet, zoals klassikale trainingen, e-learning, social engineering en phishing-testen. Zo helpen we het bewustzijn in uw organisatie te optimaliseren.

Wilt u meer informatie of een afspraak maken?
Neemt u dan contact met ons op:

Adresgegevens
ACA IT-Solutions
Beemdstraat 38
5652 AB EINDHOVEN

Contactgegevens
T +31 (0)40 - 8 800 100
info@aca-it.nl
www.aca-it.nl

MINITEST: HOE 'AWARE' BENT U?

Security Awareness kent vele facetten. Om u een beeld te geven van ons Security Awareness Programma treft u hieronder een minitest op basis van onderwerpen die de revue zullen passeren. Beantwoordt u alle vragen juist?

1 **Welke soorten gegevens worden binnen de Europese Unie beschouwd als persoonsgegevens?**
(meerdere antwoorden mogelijk)

- ☐ Woonadres
- ☐ IP-adres
- ☐ Zakelijk e-mailadres
- ☐ Telefoonnummer

2 **Wat is de veiligste manier om gevoelige documenten met een collega te delen?**

- ☐ Gecodeerde e-mail
- ☐ Beveiligde file server
- ☐ USB-stick
- ☐ Dropbox

3 **Welk van de volgende wachtwoorden is het veiligst?**

- ☐ Voetbal1988
- ☐ dQ@R12X$
- ☐ Janvistgraag!
- ☐ Password123456789

4 **U ontvangt een e-mail van de volgende afzender, vanuit welk domein is de mail verstuurd?**
Afzender: afspraak@datumprikker.nl <afspraak@planning.datumpikker.nl>

- ☐ datumprikker.nl
- ☐ planning.nl
- ☐ afspraak.nl
- ☐ anders

5 **Welk van de volgende bijlagen is het veiligst om te openen?**

- ☐ Database.zip
- ☐ Resultaten.xlsm
- ☐ Training_v1.pptx
- ☐ Overzicht.jpg
- ☐ Administratie.exe
- ☐ CV_kiki_2018.msi

6 **Welke vorm van Social Engineering uit het onderstaande rijtje is het meest succesvol?**

- ☐ SMH (Social Media Hacking)
- ☐ Spear phishing
- ☐ Virusinfectie
- ☐ Key-Logger

7 **Welke van de onderstaande methoden is het best geschikt om uw accounts beter te beveiligen?**

- ☐ Data encryptie
- ☐ End-to-end encryptie
- ☐ Two-factor authentication
- ☐ WPA2 authentication

8 **Hoe kunt u geïnfecteerd raken met ransomware, ofwel gijzelsoftware?**
(meerdere antwoorden mogelijk)

- ☐ Door te klikken op een malafide weblink
- ☐ Via een Bitcoin transactie
- ☐ Door een besmette bijlage in een e-mailbericht
- ☐ Door te klikken op een advertentie

9 **Waaraan kunt u de meeste phishingmails herkennen?** (meerdere antwoorden mogelijk)

- ☐ Het e-mailadres van de afzender
- ☐ Een malafide link of bijlage
- ☐ Spelfouten
- ☐ Urgentie

10 **Wat is de veiligste vorm van draadloos internet?**

- ☐ Openbaar wifi-netwerk
- ☐ Wifi-netwerk beveiligd met WPA
- ☐ Wifi-netwerk beveiligd met wachtwoord
- ☐ 3G of 4G databundel

Heeft u alle vragen beantwoord en bent u benieuwd naar het resultaat?

Ga naar www.aca-it.nl/minitest voor de juiste antwoorden inclusief toelichting.

Hoe is het gesteld met het awareness-niveau in uw organisatie? Een nulmeting biedt uitkomst. Dit is een goede eerste stap om uw organisatie te beschermen tegen cybercriminelen. Neem geen risico en neem contact met ons op. Wij komen graag bij u langs voor een vrijblijvend adviesgesprek.

Beemdstraat 38 5652 AB Eindhoven
T +31 (0)40 - 8 800 100 | info@aca-it.nl | www.aca-it.nl

A·C·A IT-SOLUTIONS

Security Awareness: Maak medewerkers tot een sterke schakel in de beveiliging van uw IT-omgeving

ACA-IT.nl