VERTA

SECURITY AWARENESS SESSIE

Hands-on trainingssessie “Cyberveilig Werken”

Tijd voor actie! In 2 uur tijd leren cyberveilig werken!

Verta Security
Think. Act. Secure.
www.vertasecurity.nl

VERTA

HERKEN JE DIT?

Je medewerkers zijn je eerste verdedigingslinie.

Je beveiliging is zo sterk als de keuzes die medewerkers dagelijks maken. Daarom is het goed als iedereen weet waar de risico's zitten en wat hij of zij zelf kan doen.

Misschien herken je een of meer van deze situaties:

- Je medewerkers werken met gevoelige gegevens, maar niet iedereen weet waar de risico's op de eigen werkplek zitten.
- Phishing en andere trucs worden steeds overtuigender, en één klik kan genoeg zijn.
- Je wilt dat iedereen weet wat te doen als er toch iets gebeurt.
- Je zoekt een training waarbij mensen niet alleen luisteren, maar echt zelf aan de slag gaan.
- Een klant, auditor of verzekeraar vraagt of je medewerkers zijn getraind.

> **Een trainingssessie geheel toegespitst op de risico's en beveiliging van jouw bedrijf.**

VERTA

WAT IS DE SESSIE?

Een praktische workshop, toegespitst op jouw bedrijf.

In de sessie “Cyberveilig werken” leren je medewerkers niet alleen wat de risico's zijn, maar ook wat ze er zelf aan kunnen doen. Geen lange presentatie waarbij iedereen alleen toekijkt: na elk deel gaan de deelnemers in groepjes zelf aan de slag, met situaties uit hun eigen werk.

De sessie is opgebouwd volgens het ABC-model en bestaat uit drie onderdelen: Access, Behavior en Contingency.

Voor wie?

Voor teams, afdelingen of het hele bedrijf, van bestuur tot werkvloer. Het werkt het best als directe collega's samen in een groep zitten, zodat ze het over hun eigen werkplek kunnen hebben.

3
onderdelen
Access, Behavior, Contingency

± 2
uur
naar wens aan te passen

Iedereen
doet actief mee
in groepjes, op de eigen werkplek

VERTA

ONZE AANPAK

Het ABC-model: human risk management in drie lagen.

Het ABC-model richt zich op human risk management: de risico's die ontstaan door wat mensen doen, of juist laten. Elke laag verkleint de kans op een incident, en de gevolgen als het toch misgaat.

A Access TOEGANG

Hoe zorg je dat gegevens van klanten, medewerkers en gevoelige bedrijfsinformatie niet bij onbevoegden terechtkomen? Denk aan wachtwoorden, inloggen met een tweede stap (MFA) en beveiligde apparaten, maar ook aan fysieke beveiliging: deuren dicht en spullen opbergen. En aan social engineering, afluisteren en afkijken, en medewerkers met te veel rechten.

B Behavior GEDRAG

Phishing en datalekken herkennen, verdachte situaties signaleren en een cultuur opbouwen waarin veilig werken gewoon is. Hier komt de SCAR-methode om de hoek kijken: vier stappen die je leert integreren in je dagelijkse werkdag.

- **S** Signaleer — Scan
- **C** Controleer — Check
- **A** Activeer — Act
- **R** Rapporteer — Report

C Contingency NOODPLAN

Wat doe je als het toch misgaat? Wat doe je bij een datalek, of als je op een phishinglink hebt geklikt? Wat is de meldprocedure? Hoe blijf je veilig doorwerken, en heb je een back-up om op terug te vallen?

VERTA

HET PROGRAMMA

Hands-on Security Awareness sessie

Het programma bestaat uit **drie onderdelen**. Daarbij wordt het ABC-model gehanteerd: Access, Behavior en Contingency. Bij de eerste twee onderdelen ontvang je eerst kennis en ga je daarna zelf aan de slag.

1

Onderdeel 1: Access TOEGANG

Je ontvangt kennis over de A van het ABC-model: hoe voorkom je dat gegevens bij onbevoegden terechtkomen? Daarna worden de aanwezigen in groepen verdeeld, bij voorkeur directe collega's bij elkaar. Elke groep loopt de eigen werkplek na op mogelijke risico's en dreigingen rond Access.

Kennis · 20 minuten **Zelf aan de slag · 20 minuten**

2

Onderdeel 2: Behavior GEDRAG

Je ontvangt kennis over de B van het ABC-model: gedrag. Daarna gaan de groepen opnieuw uiteen. Ze bedenken welke herkenbare situaties voor hen gelden en hoe ze daarmee kunnen omgaan. Ze oefenen daarbij met de SCAR-methode: Signaleer, Controleer, Activeer, Rapporteer.

Kennis · 20 minuten **Zelf aan de slag · 20 minuten**

3

Onderdeel 3: Contingency NOODPLAN

Een korte presentatie over de C van het ABC-model: wat doe je als het toch misgaat? Je hoort hoe de meldprocedure van het bedrijf werkt en wat je moet doen bij een incident.

Kennis · ± 15 minuten

Aanbevolen: Er wordt aangeraden om de training op de werklocatie te laten plaatsvinden, zodat deelnemers daar zelf kunnen rondlopen om de Access- en Behavior-risico's te ontdekken.

VERTA

WAAR IK VOOR STA

Informatiebeveiliging die ook echt landt in je bedrijf.

Ik ben Kirsten, oprichter van Verta Security. Ik werk praktisch, begrijpelijk en zonder opgeheven vingertje.

WAT MIJ DRIJFT

- **Begrijpelijk.** Ik leg uit wat er speelt en waarom het ertoe doet, in gewone taal.
- **Praktisch.** Een plan dat in een la verdwijnt, helpt niemand. Je krijgt acties die je echt kunt uitvoeren.
- **Passend bij jouw bedrijf.** Ik maak het nooit groter of ingewikkelder dan nodig.
- **Onafhankelijk.** Ik kijk met je mee, zonder belang bij een product of leverancier.
- **Het begint bij mensen.** Techniek is belangrijk, maar veilig werken doe je met elkaar. Daarom kijk ik ook naar gedrag en afspraken.

Ik werk met twee vaste kaders, zodat informatiebeveiliging overzichtelijk blijft en je stap voor stap vooruit kunt:

ABC-model

Access · Behavior · Contingency

SCAR-methode

Scan · Check · Act · Report

VERTA

WAT LEVERT HET JE OP?

Na de sessie weet iedereen wat hij of zij moet doen.

Na de training

- Iedereen weet wat de eigen risico's op de werkplek zijn
- Ze herkennen risico's en dreigingen
- Ze weten hoe ze die voorkomen en ernaar handelen
- Ze weten wat ze moeten doen als er daadwerkelijk een incident plaatsvindt

Wat het jou oplevert

Betrokken medewerkers. Ze doen zelf mee, in plaats van alleen te luisteren.

Herkenbaar en praktisch. De voorbeelden komen uit hun eigen werk.

Een gedeelde taal. Iedereen gebruikt dezelfde stappen (SCAR) en weet wat te melden.

Naslagwerk. Wat er in de training is gedaan, kun je later nalezen.

Vertrouwen bij klanten. Je kunt laten zien dat je mensen zijn getraind.

Een eerste stap naar een veiliger werkcultuur, of een goede aanvulling op een traject.

INVESTERING

Wat kost de sessie?

Voor de security awareness sessie “Cyberveilig werken” werk ik met een vaste prijs, zodat je vooraf precies weet waar je aan toe bent.

VASTE PRIJS

€ 495,-

per sessie, exclusief btw

DE PRIJS IS INCLUSIEF

- Een voorbespreking om input voor de training op te halen
- De sessie zelf, ± 2 uur
- Naslagwerk over wat er in de training is gedaan

WANNEER EN HOE

Je kiest zelf: **op locatie of online**. De training wordt overdag gegeven; online kan ook ’s avonds. Reken op ± 2 uur. Dat kan naar wens worden ingekort of uitgebreid.

LOSSE BOEKING OF ONDERDEEL VAN TRAJECT 2

De training is los te boeken of als onderdeel van Traject 2.

> **Aanvullende wensen of meerdere sessies afnemen?** Vraag dan om een voorstel op maat.

HET GESPREK BEGINT HIER

Benieuwd wat deze sessie voor jouw team kan betekenen?

Laten we kennismaken. In een vrijblijvend gesprek bekijken we wat de sessie voor jouw bedrijf kan betekenen.

NEEM CONTACT OP

info@vertasecurity.nl

www.vertasecurity.nl

WIL JE MEER DAN EEN SESSIE?

Bekijk Traject 1 en Traject 2.

Traject 1: de cyberveiligheid van je bedrijf in kaart brengen. Traject 2: de cyberveiligheid van je medewerkers bevorderen.