VERTA

TRAJECT 2

De cyberveiligheid van je medewerkers bevorderen

Cyberveiligheid begint bij ons eigen handelen, van bestuur tot werkvloer.

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

VERTA

HERKEN JE DIT?

Techniek helpt, maar je medewerkers maken het verschil.

Je beveiliging is zo sterk als de mensen die er elke dag mee werken. Een nieuwe collega, een drukke dag, een mail die er echt uitziet: veel hangt af van de keuzes die medewerkers op dat moment maken.

Misschien herken je een of meer van deze situaties:

- Je medewerkers werken met gevoelige gegevens, maar niet iedereen weet precies wat er van hem of haar wordt verwacht.
- Een eenmalige training is lang geleden, of is er nog nooit geweest.
- De werkvloer, het kantoor en het bestuur hebben allemaal andere dingen nodig, maar krijgen dezelfde uitleg.
- Je hebt afspraken en beleid, maar je weet niet of ze in de praktijk worden gevolgd.
- Je wilt dat veilig werken gewoon is in je organisatie, in plaats van een los onderwerp.
- Een klant, auditor of verzekeraar vraagt om bewijs dat je medewerkers zijn getraind.
- Je wilt weten of een training echt iets verandert.

> Wat je zoekt is **een aanpak die past bij jouw mensen en jouw werk.**

VERTA

WAT IS TRAJECT 2?

Training die past bij elke afdeling, met zicht op wat het oplevert.

In Traject 2 kijk ik eerst hoe er binnen je organisatie wordt gewerkt en hoe er over veiligheid wordt gedacht. Daarna maak ik een plan en geef ik training die past bij elke afdeling. Van bestuur tot werkvloer krijgt iedereen uitleg die aansluit bij het eigen werk. Na afloop kijken we samen wat er is veranderd.

Geen standaardpresentatie voor iedereen, maar praktisch en herkenbaar. Je medewerkers leren wat ze in hun eigen dagelijks werk kunnen doen.

Voor wie?

Voor bedrijven en organisaties die willen dat veilig werken gewoon wordt. Bijvoorbeeld omdat je medewerkers met gevoelige gegevens werken, omdat klanten of toezichthouders ernaar vragen, of omdat je je voorbereidt op een audit of certificering. Ook als er al een training is geweest, kan dit traject helpen om het echt te laten landen.

6
stappen
van eerste scan tot evaluatie

1
training per afdeling
op maat van het werk

1
evaluatie
met zicht op resultaat

VERTA

WAT GEBEURT ER IN HET TRAJECT?

Zes stappen, van eerste indruk tot meetbaar resultaat.

01 Cultuurscan

Hoe wordt er in jouw organisatie over veiligheid gedacht en hoe ga je er in de praktijk mee om? Met een korte scan krijg ik een beeld van de uitgangssituatie.

02 Locatiebezoeken

Ik kom bij je langs en kijk hoe er in de praktijk wordt gewerkt: op kantoor, op de werkvloer, op de verschillende locaties.

03 Interviews en observaties

Ik praat met medewerkers van verschillende afdelingen en kijk mee. Zo hoor ik waar ze tegenaan lopen en wat ze nodig hebben.

04 Security awareness plan

Op basis van wat ik zie en hoor, en van de huidige dreigingen en trends in de cybersecurity, maak ik een plan: welke onderwerpen, voor wie, in welke volgorde en op welke manier.

05 Diverse trainingssessies

Elke afdeling krijgt een training die past bij haar werk, van bestuur tot werkvloer. Hands-on en interactief, gericht op het vergroten van inzicht, met voorbeelden uit je eigen organisatie en sector.

06 Evaluatie

Na afloop kijken we wat er is veranderd. Wat is blijven hangen, wat is er nog nodig en hoe houd je het levend?

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

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 Traject 2 weten je medewerkers wat ze moeten doen.

Je ontvangt

- Inzicht in hoe veiligheid in jouw organisatie leeft
- Een security awareness plan op maat
- Trainingssessies die aansluiten op elke afdeling
- Een evaluatie van wat er is veranderd en wat er nog nodig is
- Concrete tips om het gedrag vast te houden
- Een persoonlijk gesprek waarin ik alles toelicht

Wat het jou oplevert

Betrokken medewerkers. Ze weten waarom het ertoe doet en wat ze zelf kunnen doen.

Veilig werken als gewoonte. Het wordt een onderdeel van hoe jullie werken.

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

Voorbereid zijn. Op een audit of certificering, en op de dag dat er toch iets gebeurt.

Zicht op resultaat. Je ziet wat er verandert, niet alleen dat er training is geweest.

Een stevige basis om door te groeien, bijvoorbeeld richting een ISMS, ISO 27001 of NEN 7510.

VERTA

INVESTERING

Wat kost Traject 2?

Traject 2 werk ik uit op basis van een uurtarief van **€ 100,- (excl. btw)**. Hieronder zie je hoeveel tijd een gemiddeld traject kost, zodat je vooraf weet waar je aan toe bent. **De exacte prijs hangt sterk af van de grootte van je organisatie en het aantal afdelingen en trainingssessies.**

STAP		UREN (GEMIDDELD)	INVESTERING
01	Cultuurscan	4 - 6 uur	€ 400 - € 600
02	Locatiebezoeken	3 - 5 uur	€ 300 - € 500
03	Interviews en observaties	4 - 5 uur	€ 400 - € 500
04	Security awareness plan	6 - 8 uur	€ 600 - € 800
05	Diverse trainingssessies (± 4 trainingen)	5 - 10 uur	€ 500 - € 1.000
06	Evaluatie	2 - 3 uur	€ 200 - € 300
Totaal gemiddeld traject		**24 - 37 uur**	**€ 2.400 - € 3.700**

LOOPTIJD

Een traject duurt gemiddeld **2 tot 8 weken**, afhankelijk van de beschikbaarheid van de betrokkenen, de grootte van het bedrijf en het aantal trainingssessies dat nodig is.

> Dit zijn indicaties op basis van een gemiddeld traject. Het precieze aantal uren hangt af van de grootte en complexiteit van je organisatie, het aantal locaties en afdelingen en het aantal trainingssessies. Na een kort kennismakingsgesprek geef ik je een vaste, vooraf afgesproken prijs.

VERTA

HET GESPREK BEGINT HIER

Benieuwd hoe jouw medewerkers veilig werken?

Laten we kennismaken. In een vrijblijvend gesprek bekijken we waar je staat en wat Traject 2 voor jou kan betekenen.

NEEM CONTACT OP

info@vertasecurity.nl

www.vertasecurity.nl

WIL JE EERST JE BEDRIJF IN KAART BRENGEN?

Dan is er Traject 1: de cyberveiligheid van je bedrijf in kaart brengen.

Je krijgt een helder beeld van hoe veilig je bedrijf nu is, met concrete aanbevelingen.