Training: Cyberweerbaarheid voor goede doelen

Samen met The Trusted Third Party (TT3P) organiseren we de training: **Cyberweerbaarheid voor goede doelen**.

Cybercriminaliteit heeft een ontwrichtende werking op de maatschappij en de ontwikkelingen op dit gebied gaan snel. Het is voor iedere goededoelenorganisatie, groot of klein, van belang om actief over dit onderwerp na te denken, beleid te formuleren én effectieve beheersmaatregelen te treffen.

In deze training staat het in de organisatie verankeren van informatiebeveiliging en cybersecurity centraal. Het opbouwen van informatiebeveiliging vanaf de basis zorgt ervoor dat jouw organisatie zelf de regie heeft over dit onderwerp en zelfstandig afgewogen en breed gedragen (investerings)beslissingen kan maken over informatiebeveiliging.

De training bestaat uit twee modules:

- Module 1 (fysiek): **Hoe wordt mijn goede doel cyberweerbaar?**
- Module 2 (online): **Wees voorbereid, denk als een hacker!**

De twee modules vullen elkaar aan en worden alleen als pakket aangeboden.
Tijdens de training is er gelegenheid voor het stellen van vragen en het (kort) bespreken van praktijkvoorbeelden.

Kosten
De kosten voor deze training van één dagdeel (fysiek) en één dagdeel (online) zijn (totaal voor beide modules samen) EUR 175,- (btw vrij) per deelnemer. Dit is inclusief lunch tijdens de fysieke training. Het minimum aantal deelnemers is 8, het maximale aantal deelnemers is 12.

MODULE 1 - Hoe wordt mijn goede doel cyberweerbaar?

Cybersecurity governance biedt een strategisch beeld van hoe een organisatie haar beveiliging organiseert en beheert, inclusief het bepalen van de risicobereidheid, het bouwen van verantwoordingskaders en het vaststellen van wie verantwoordelijk is voor het nemen van beslissingen.

Programma
- Waar gaat informatiebeveiliging over?
- Praktijk casus: wat gebeurt er als een organisatie gehackt wordt?
- Wat zijn risico-inventarisatie en risico-evaluatie?
- Hoe bepaal je de risicobereidheid en het volwassenheidsniveau voor informatiebeveiliging van jouw organisatie?
- Hoe bepaal je passende technische en organisatorische maatregelen?
- Hoe beperk je risico's in de leveranciersketen? (supply chain risico's)
- Hoe creëer je bewustzijn en draagvlak voor het volgen van procedures bij medewerkers?

- Wie zijn de stakeholders bij informatiebeveiligingsincidenten? Hoe bereid je preventief de communicatie voor die nodig is bij een eventueel beveiligingsincident?

MODULE 2 - Wees voorbereid, denk als een hacker!

In deze module nemen een hacker en een cyber-attack recovery specialist je mee in hun dagelijkse praktijk. Zij delen hun lessen voor jouw organisatie en de quick-wins voor het voorkomen van en het voorbereiden op cyber-aanvallen. Je leert hoe een hacker naar jouw organisatie kijkt. En je leert dat recovery na een cyber-aanval altijd lukt, maar veel sneller en soepeler verloopt als je organisatie goed voorbereid is.

Programma

- Wat zijn de veel voorkomende cyber-dreigingen? (o.a. phishing, ransomware, malware, social engineering, CEO-fraude).
- Hoe kun je de technische beveiliging testen? (o.a.: review, kwetsbaarhedenscan, pentest, red teaming of audit).
- Wat is incident response?
- Hoe wordt een IT-omgeving na een aanval geschoond en weer opgebouwd?
- Hoe zorgt een recovery specialist dat je organisatie na een cyberaanval snel weer kan vertrouwen op het netwerk, de applicaties en de data?
- Hoe kun je zorgen dat jouw organisatie zo goed mogelijk voorbereid is op mogelijke cyber-aanvallen?
- Wat zijn de do's en dont's voor een effectieve back-up strategie?

Voor wie is deze training?

Medewerkers die (direct of indirect) verantwoordelijk zijn voor risicomanagement, bedrijfsvoering of ICT. Bijvoorbeeld hoofden bedrijfsvoering, privacy functionarissen, ICT-managers en coördinatoren en bestuursleden. Geschikt voor zowel grote als kleinere organisaties; met of zonder eigen ICT afdeling.
Vaak is cybersecurity afhankelijk van een externe IT partner. Het is verstandig om zelf ook de basiskennis te beheersen, zodat je regie en controle kunt houden op de maatregelen die zij voorstellen en uitvoeren.

Over de trainers

<u>Patrick Jordens (module 1)</u>
Patrick is oprichter van onder andere The Trusted Third Party (TT3P - cyberveiligheid risicomanagement, consultancy & awareness). Patrick heeft jarenlange ervaring op het gebied van risicomanagement bij privacy en informatiebeveiliging, ook specifiek in de goededoelensector. Hij heeft corporates, MKB bedrijven, grote en kleine goede doelen bijgestaan bij het vormen, implementeren, controleren en het beheren van beleid voor privacy en informatiebeveiliging en in praktijk veel organisaties bijgestaan in het geval van beveiligingsincidenten. Verder is hij is gastddocent aan de Hogeschool van Rotterdam en de Haagse Hogeschool.

<u>Erik Rutkens (module 2)</u>
Erik is deeltijd practor Digitaal Veilige Apparatuur bij Noorderpoort College en oprichter en eigenaar van Dayzero. Dayzero ondersteunt innovatieve, schaalbare en maatschappelijk relevante cybersecurity

ondernemers actief met kennis, netwerk, talent en/of kapitaal. Een voorbeeld is Hacksclusive, waar Erik tevens mede-oprichter en directeur van is. Erik is ook mede-oprichter van Zerocopter. Daarnaast is Erik een van de initiatiefnemers Cybersecurity Noord, dat door publiek-private samenwerking de weerbaarheid van het mkb in Noord-Nederland wil vergroten.

Patrick Louwe (module 2)
Patrick is cyber-attack recovery specialist en oprichter van It2grow. Zijn consultants werken dagelijks bij organisaties die recent aan een hack zijn onderworpen en die hun bedrijfsvoering zo snel mogelijk moeten herstellen. Patrick heeft een duidelijke visie op de manier waarop organisaties zich technisch en organisatorisch moeten voorbereiden op een aanval van cyber criminelen. Die visie gaat niet alleen over beveiliging en bescherming, maar ook over de manier waarop je als organisatie het beste kunt handelen in het geval je te maken hebt met een hack of andere vorm van cyber crime.

Resultaat
Na het volgen van deze training ben je bekend met de basisbeginselen van governance op het gebied van informatiebeveiliging voor goededoelenorganisaties. Je weet dat een goed gedocumenteerd, bij de organisatie passend, beleid de basis vormt voor een cyberweerbare organisatie en je hebt geleerd welke onderdelen daarin niet mogen ontbreken.

Je hebt geleerd hoe hackers kijken naar jouw organisatie. Je weet wat er gebeurt na een cyber-aanval en welke voorbereidingen hierop noodzakelijk zijn.

Na afloop ontvang je een certificaat van deelname en kun je voor een onbeperkte termijn na de training bij de Patrick Jordens terecht met vragen.

Tijden, datum & locatie
Deze training bestaat uit twee keer een ochtend of middag. Module 1 vindt plaats op kantoor bij Goede Doelen Nederland. Adres: 100 Watt gebouw, James Wattstraat 100, 5e etage, 1097 DM Amsterdam. Module 2 vindt online plaats via Zoom.

Op de website van Goede Doelen Nederland vind je de data en tijdstippen van deze training.

Annuleringsvoorwaarden
Let op: bij annulering vanaf twee weken vóór de training ben je 50% van de kosten verschuldigd en bij annulering vanaf één week vóór de training ben je 100% van de kosten verschuldigd. Je kunt je wel laten vervangen door een collega. Bij aanmelding ga je automatisch akkoord met deze annuleringsvoorwaarden. Goede Doelen Nederland behoudt zich het recht voor de training te annuleren bij onvoldoende aanmeldingen.

Contactgegevens trainer:
Patrick Jordens patrick.jordens@tt3p.nl

Contactgegevens Goede Doelen Nederland
Jojanneke Brinkman, inkoop, brinkman@goededoelennederland.nl