Leidraad Cybersecurity voor goede doelen 2026

Lancering & toelichting op de actualisatie

Webinar Goede Doelen Nederland | 10 juni 2026

Patrick Jordens | The Trusted Third Party (TT3P)

The Trusted Third Party

Goede Doelen Nederland
Brancheverenging

Programma

11:00	Opening
11:02	Floris Jan de Koning (Responders.NOW) - Wat er echt gebeurt bij een cyberincident
11:15	Poll: "Ik heb wel eens een incident van dichtbij meegemaakt"
11:20	Patrick Jordens (TT3P) - De visie en het systeem achter de leidraad
11:30	Poll: "Wij voeren risicoanalyses uit op kritieke systemen en leveranciers"
11:35	Patrick Jordens - De delta: wat is nieuw in deze leidraad en waarom?
11:55	Poll & afsluiting

Goede Doelen Nederland
Brancheverenging

The Trusted Third Party

Wat gebeurt er echt als een organisatie wordt gehackt?

Floris Jan de Koning | Responders.NOW

- Ransomware als businessmodel: professioneel, grootschalig, winstgevend
- De impact: financieel, reputationeel, juridisch en psychologisch
- Het dilemma: betalen of niet?
- Waarom voorbereiding het verschil maakt

Mediaoptredens: RTL Tonight, NPO Radio 1, EenVandaag (Odido-hack, 2026)

Goede Doelen Nederland
Brancheverenging

The Trusted Third Party

"Ik heb wel eens een cyberincident van dichtbij meegemaakt."

- Ja, in mijn eigen organisatie
- Ja, bij een andere organisatie
- Nee, maar ik maak me er wel zorgen over
- Nee, en wij zijn echt niet interessant genoeg

De visie achter de leidraad

Er is in praktijk bij goede doelen te vaak geen plan en te weinig verankering.

**Veel goede doelen pakken puzzelstukken,
maar weten niet welke puzzel ze precies leggen.**

Geen beleid	Geen eigenaarschap	Geen toetsing
Maatregelen genomen, maar niet vastgelegd wie waarvoor verantwoordelijk is	IT regelt het wel, dus het bestuur hoeft er niet over na te denken	Beleid bestaat op papier, maar niemand controleert of het werkt

Goede Doelen Nederland
Brancheverenging

The Trusted Third Party

De visie achter de leidraad

Begin bij het begin: van risico naar beleid naar maatregel

1. Risicoanalyse	2. Beleid & keuzes	3. Implementatie	4. PDCA-borging
Wat beschermen we? Waarom? Voor wie? Welke risico's accepteren we?	Bestuurlijke afwegingen. Welke maatregelen? Wie is verantwoordelijk?	Maatregelen inrichten. Medewerkers trainen. Leveranciers aanspreken.	Toetsen en evalueren. Bijsturen waar nodig. Aantoonbaar in control.

De leidraad begint niet bij de firewall. Hij begint bij de vraag: wat is voor onze organisatie echt van belang?

Goede Doelen Nederland
Brancheverenging

The Trusted Third Party

Het kan wel

Cybersecurity is te organiseren, ook voor goede doelen

Je hoeft niet alles tegelijk. Je moet wel bewust kiezen.

Begin klein

Risicoanalyse op een pagina, eigenaarschap benoemen, drie prioriteiten vaststellen.

Bouw stap voor stap

Geen big bang. Elke verbetering telt. PDCA werkt ook op kleine schaal.

Maak het bestuurlijk

Neem cybersecurity op in bestuursvergaderingen. Stel jaarlijks een basisnorm vast.

Gebruik de leidraad

Praktisch, proportioneel, geschreven voor goede doelen. Niet voor IT-specialisten.

POLL

"Wij voeren risicoanalyses uit op kritieke systemen en leveranciers en die vormen de basis van ons beleid."

- Ja, structureel en gedocumenteerd
- Deels, we doen het maar niet systematisch
- Nee, maar we zijn er mee bezig
- Nee, dit hebben we nog niet opgepakt

Wat is er nieuw in de leidraad 2026?

1. Bestuurlijke verankering en aantoonbaarheid
2. BIV voor goede doelen: risico's vertaald naar de praktijk
3. Shadow IT en shadow AI
4. Ketenbeveiliging als bestuurlijke verantwoordelijkheid
5. Security management als doorlopend proces

Goede Doelen Nederland
Brancheverenging

The Trusted Third Party

1. Bestuurlijke verankering en aantoonbaarheid

De kern

- Bestuurders dragen verantwoordelijkheid voor cyberrisico
- Aantoonbaarheid: opzet, bestaan en werking
- Niet alleen beleid op papier, maar werking in de praktijk
- Het CBF, toezichthouders, accountants en verzekeraars vragen hier actief naar

De kernvraag

"Zijn wij aantoonbaar in control?"

Cybersecurity is geen IT-project.
Het is een vraagstuk van continuiteit, verantwoordelijkheid en bestuurlijke regie.

Verdieping: Bestuurderstraining cybersecurity

Voor bestuurders, directieleden en interne toezichthouders van goede doelen die meer willen dan bewustwording. Die echt grip willen op cybersecurity als governance- en continuïteitsvraagstuk.

Datum: Donderdag 10 september 2026

Tijd: 09:30 - 13:00 uur (inloop 09:15), inclusief lunch

Locatie: Kantoor Goede Doelen Nederland, Amsterdam

Kosten: 280,- per deelnemer | max. 10 deelnemers

Inclusief interactieve ransomware-simulatie
Aanmelden via Goede Doelen Nederland

Goede Doelen Nederland
Brancheverenging

The Trusted Third Party

2. BIV voor goede doelen

Beschikbaarheid, Integriteit en Vertrouwelijkheid. Vertaald naar de praktijk

B Beschikbaarheid

- Fondsenwervingssystemen offline
- CRM onbereikbaar voor medewerkers
- Donatiepagina's down tijdens campagne

I Integriteit

- Rekeningnummer aangepast in factuur
- E-mail verstuurd uit naam van bestuurder
- Donateursgegevens ongemerkt gewijzigd

V Vertrouwelijkheid

- Donateursbestand uitgelekt
- Persoonsgegevens begunstigden gestolen
- Interne correspondentie openbaar

3. Shadow IT en Shadow AI

De blinde vlek die aanvallers actief misbruiken

Medewerkers en vrijwilligers die zonder medeweten van IT eigen tools, AI-applicaties of no-code-platforms inzetten voor werk. Functioneel waardevol, maar beveiligingstechnisch een groeiend risico.

Onbeveiligde AI-tools	Donateursdata ingevoerd in ChatGPT of andere externe AI zonder dataverwerkingsafspraak
No-code apps	Zelfgebouwde analyse-tools zonder authenticatie, logging of encryptie
Ketenrisico	Koppelingen tussen CRM, e-mail en betaalplatforms die buiten IT om zijn opgezet
Governance-gat	Als niemand weet welke tools worden gebruikt, beoordeelt dus niemand de risico's

Verdieping: de Odido-casus

Wat elke goede doelen-organisatie hiervan kan leren

Geen geavanceerde hack. Een aaneenschakeling van bestuurlijke keuzes die jarenlang niet zijn heroverwogen.

In de handout

- Reconstructie van de aanvalsketen
- De ketenrisico's: eigen medewerkers of externe partner?
- De blast radius: wat kan één account aanrichten?
- Drie artikelen uit de Cyberbeveiligingswet
- Drie bestuurlijke lessen en drie vragen voor uw directie

Koppeling naar dit webinar

- Ketenbeveiliging begint bij inzicht in wie toegang heeft tot welke donateursdata
- Odido laat zien wat er mis gaat als ketenrisico niet bestuurlijk wordt geagendeerd
- De lessen uit de casus kunnen de basis vormen van uw eerste prioriteiten

► **De handout 'De Odido-hack: wat elke organisatie hiervan kan leren' ligt voor u klaar**

4. Ketenbeveiliging als bestuurlijke verantwoordelijkheid

Ketenrisico is organisatierisico

1

Inzicht in ketenrisico's

Inventariseer alle leveranciers en hun toegang

2

Beveiligingseisen vooraf

Leg minimumeisen vast bij selectie en contractering

3

Toegang en minimale rechten

Beperk wat leveranciers mogen zien en doen

4

Monitoring en signalering

Detecteer afwijkingen tijdig

5

Gezamenlijke incidentrespons

Stem meldafspraken en escalatielijnen af

6

Bestuurlijke verankering

Ketenrisico op de bestuurstafel, niet bij IT

Goede Doelen Nederland
Brancheverenging

The Trusted Third Party

5. Security management als doorlopend proces

Cybersecurity is geen project. Het is een continue verantwoordelijkheid.

P Plan	Risicoanalyse Beleid Doelstellingen
D Do	Maatregelen Training Implementatie
C Check	Toetsen Audit Evaluatie
A Act	Bijsturen Verbeteren Aantonen

"Ik ga na dit webinar iets concreets opnemen op de agenda van mijn organisatie."

- Ja, ik ga een risicoanalyse oppakken
- Ja, ik ga cybersecurity op de bestuurstafel zetten
- Ik wil meer informatie via TT3P
- Ik ga de leidraad downloaden en doorlezen

patrick.jordens@tt3p.nl | www.tt3p.nl | Bestuurderstraining 10 september 2026