The Trusted Third Party

Rapport cybersecurity bij Nederlandse goede doelen

Oktober 2024

Inhoudsopgave

Inleiding

Digitale transformatie is niet alleen een keuze maar een noodzaak geworden. Daarom staan ook goede doelen voor de uitdaging om hun activiteiten en diensten online te brengen. Deze digitale verschuiving biedt talloze voordelen, zoals het vergroten van het bereik en het efficiënter inzamelen van donaties. Echter, met deze kansen komen ook risico's, met name op het gebied van cybersecurity.

Het belang van cybersecurity kan niet worden onderschat, vooral niet voor organisaties die, net als goede doelen, afhankelijk zijn van het vertrouwen van het publiek. Een enkel beveiligingsincident kan niet alleen financiële verliezen veroorzaken, maar ook, en misschien nog wel belangrijker, onherstelbare schade toebrengen aan de reputatie van een organisatie. In het Verenigd Koninkrijk heeft recent onderzoek uitgewezen dat goede doelen net zo kwetsbaar zijn voor cyberaanvallen als elk ander type organisatie, bijvoorbeeld commercieel of overheid. Dit roept de vraag op: hoe staat het met de cyberveiligheid van Nederlandse goede doelen?

Op die vraag gaan we in dit rapport in. En alhoewel er echt aansprekende voorbeelden zijn van hoe het wél moet, geeft de stand van cybersecurity bij goede doelen anno 2024 reden tot zorg.

Dit rapport is samengesteld om te dienen als bewustwordingsinstrument voor Nederlandse goede doelen om het belang van cybersecurity te leren begrijpen en te erkennen. Gebaseerd op het rapport uit het Verenigd Koninkrijk, leggen we de kwetsbaarheden bloot die goede doelen hebben ten aanzien van cyberaanvallen, illustreren we de mogelijke gevolgen van dergelijke aanvallen, en doen we aanbevelingen voor effectieve beschermingsmaatregelen. Door het adaptief maken van de inzichten uit het Britse rapport voor de Nederlandse context, streven we ernaar om met dit rapport Nederlandse goede doelen te wapenen tegen de groeiende dreiging van cybercriminaliteit.

Hopelijk leidt dit rapport ertoe dat alle goede doelen in Nederland hun cybersecurity-maatregelen evalueren en versterken. Goede doelen moeten goed samenwerken om hun organisaties, en degenen die ze dienen, te beschermen tegen de steeds verder ontwikkelende digitale bedreigingen.

Waarom zijn goede doelen kwetsbaar?

De digitalisering van diensten biedt goede doelen ongekende kansen om hun missie uit te voeren en hun doelgroepen te bereiken. Tegelijkertijd opent het de deur voor cybercriminelen om kwetsbaarheden te exploiteren. Maar wat maakt goede doelen in het bijzonder kwetsbaar voor deze bedreigingen?

Beperkte middelen
Veel goede doelen opereren met beperkte budgetten, waarbij de nadruk ligt op het maximaliseren van de impact op hun specifieke doelstelling en doelgroepen. Dit kan betekenen dat er minder budget beschikbaar wordt gemaakt voor cyberbeveiliging. De essentiële basisbescher-mingsmaatregelen worden daardoor soms over het hoofd gezien.

Afhankelijkheid van vrijwilligers
Goede doelen vertrouwen sterk op de inzet van vrijwilligers die mogelijk niet altijd voldoende zijn getraind op het gebied van cybersecurity. Daarnaast is de bereidheid om te werken met beperkingen als gevolg van cybersecurity, zoals multi-factor authenticatie (MFA) laag. Gebrek aan training kan leiden tot veiligheidsrisico's, zoals het klikken op phishing-links of het onbedoeld delen van gevoelige informatie. Gebrek aan bereidheid bij vrijwilligers om te werken onder een strenger cybersecurity regime stelt goede doelen voor grote dilemma's. Vrijwilligers zijn cruciaal voor goede doelen organisaties, maar als ze dreigen af te haken omdat ze met, in hun ogen, allerlei lastige beperkingen moeten werken, wordt er in praktijk toch vaak voor gekozen om de beperkingen weer op te heffen.

Groeiende online diensten
Met de toename van online donaties en digitale dienstverlening groeit ook het aanvalsoppervlak voor cybercriminelen. Goede doelen die hun activiteiten uitbreiden naar het digitale domein zonder adequate beveiligingsmaatregelen en zonder effectief beleid hieromtrent, lopen een groter risico op datalekken en cyberaanvallen.

Gevoelige gegevens
Goede doelen verzamelen en bewaren vaak gevoelige informatie over hun begunstigden en donateurs. Deze gegevens kunnen aantrekkelijke doelwitten zijn voor cybercriminelen die uit zijn op identiteitsdiefstal of financieel gewin.

Het unieke risicoprofiel
Naast de bovengenoemde factoren, is er een uniek risicoprofiel verbonden aan de sector. Goede doelen zijn vaak gericht op het verlenen van hulp tijdens crises of in conflictgebieden, wat ze tot potentiële doelwitten maakt voor statelijke actoren of hacktivistische aanvallen. Dergelijke aanvallen kunnen gericht zijn op het onderbreken van de hulpverlening of het stelen van gevoelige informatie over kwetsbare groepen.

De combinatie van bovenstaande factoren maakt duidelijk waarom cybersecurity een cruciale overweging moet zijn voor elke organisatie binnen de goede doelensector. Het is essentieel dat goede doelen hun cybersecuritystrategieën proactief beheren om hun organisaties, donateurs en de mensen die ze dienen, te beschermen.

Potentiële cyberdreigingen voor goede doelen

Cyberaanvallen kunnen vele vormen aannemen, elk met unieke risico's en uitdagingen. Voor goede doelen zijn de voornaamste bedreigingen:

Phishing en social engineering
Phishingaanvallen, waarbij aanvallers zich voordoen als betrouwbare entiteiten om gevoelige informatie te ontlokken, vormen een significante bedreiging. Goede doelen, met hun brede netwerk van donateurs en vrijwilligers, zijn vaak het doelwit van dergelijke tactieken.

Malware en ransomware
Malware, inclusief ransomware, kan verwoestende gevolgen hebben, van het stelen van gevoelige gegevens tot het volledig verlammen van de operationele capaciteit van een organisatie. De afhankelijkheid van goede doelen van digitale systemen maakt hen kwetsbaar voor dergelijke aanvallen.

DDoS-aanvallen
Distributed Denial of Service (DDoS)-aanvallen, bedoeld om websites en online diensten ontoegankelijk te maken, kunnen kritieke fondsenwervingscampagnes en bewustwordingsinspanningen onderbreken.

Datalekken
Datalekken, hetzij door cyberaanvallen of door menselijke fouten, kunnen leiden tot het verlies van vertrouwelijke informatie over donateurs en begunstigden, wat het vertrouwen in een organisatie ernstig kan schaden.

Wie zou de goede doelen sector kunnen targeten?

Het is cruciaal om te begrijpen wie interesse zou kunnen hebben in het targeten van goede doelen en waarom.

Cybercriminelen
Aangetrokken door winstbejag, kunnen cybercriminelen proberen direct toegang te krijgen tot systemen en deze met ransomware proberen plat te leggen of gevoelige (persoons)gegevens stelen. In beide gevallen kan een cybercrimineel losgeld eisen.

Hacktivisten
Groepen die gemotiveerd zijn door politieke of sociale kwesties kunnen goede doelen targeten, die zij zien als tegenstrijdig met hun overtuigingen of doelen.

Statelijke actoren
In sommige gevallen kunnen goede doelen die werken in of rond conflictgebieden of die betrokken zijn bij gevoelige kwesties, het doelwit worden van statelijke actoren die geïnteresseerd zijn in spionage of in het ondermijnen van humanitaire inspanningen.

Voorbeelden van hacks in de sector

De hack op het Internationale Comité van het Rode Kruis

In januari 2022 werd het Internationale Comité van het Rode Kruis (ICRC) het doelwit van een geavanceerde cyberaanval, waarbij de persoonlijke gegevens en vertrouwelijke informatie van meer dan 515.000 kwetsbare individuen werden gecompromitteerd. Deze individuen omvatten mensen gescheiden van hun families door conflicten, migratie en rampen, vermiste personen en hun families, en personen in detentie. De aard van de gestolen gegevens onderstreept de ernstige risico's van cyberaanvallen op goede doelen, vooral die betrokken zijn bij gevoelige humanitaire acties.

De aanvallers maakten gebruik van hackingtools die typisch worden geassocieerd met geavanceerde aanhoudende dreigingsgroepen (APT's), een indicatie dat de daders niet alleen over aanzienlijke middelen beschikten, maar ook over de intentie om significante schade toe te brengen. Deze tools zijn specifiek ontworpen voor offensieve cyberoperaties en zijn niet publiekelijk beschikbaar, wat de ernst en gecoördineerde aard van de aanval verder benadrukt.

De impact van deze cyberinbreuk op het ICRC was veelzijdig, met niet alleen operationele verstoringen, maar ook potentiële risico's voor de veiligheid en het welzijn van de getroffen individuen. In reactie op de inbreuk ondernam het ICRC onmiddellijk acties om de schade te beperken en getroffen personen te beschermen. Dit omvatte het versterken van hun cybersecurity-infrastructuur en -protocollen, evenals het samenwerken met internationale cybersecurity-experts en wetshandhavingsinstanties om de aanval te onderzoeken.

Het exacte kostenplaatje van de ICRC-hack in termen van financiële schade, reputatieschade, en herstelinspanningen is niet publiekelijk gespecificeerd in de beschikbare samenvattingen en rapporten over de cyberaanval. Dit komt mede doordat organisaties zoals het ICRC, die betrokken zijn bij gevoelige humanitaire werkzaamheden, vaak terughoudend zijn met het delen van specifieke financiële details van cybersecurity-incidenten. De kosten kunnen breed variëren, afhankelijk van directe financiële verliezen, tot investeringen in verbeterde beveiligings-maatregelen, eventuele boetes of juridische kosten, en bovendien de impact op het vermogen van de organisatie om fondsen te werven en hun missie uit te voeren.

Wat wel duidelijk is, is dat de impact van dergelijke aanvallen verder gaat dan alleen de onmiddellijke financiële kosten. De hack heeft waarschijnlijk geleid tot significante investeringen in cybersecurityverbeteringen, externe consultancy en kosten gerelateerd aan het informeren en beschermen van de getroffen individuen. Daarnaast zijn de reputatieschade en het verlies van vertrouwen bij donateurs, partners en de mensen die de organisatie dient, moeilijk in geld uit te drukken, maar kunnen ze een langdurige impact hebben op de effectiviteit en financiering van de organisatie.

De Blackbaud hack

De Blackbaud hack, die medio 2020 aan het licht kwam, is een voorbeeld van een aanzienlijk datalek dat een breed scala aan organisaties trof, waaronder universiteiten, goede doelen en non-profitorganisaties wereldwijd. Een voorbeeld van zo'n getroffen organisatie is de Belgische vestiging van Plan International. Blackbaud, een toonaangevende leverancier van cloudsoftware voor fondsenwerving en het beheer van donateurrelaties, werd het slachtoffer van een ransomware-aanval waarbij gevoelige data van klanten werden gecompromitteerd.

De aanvallers slaagden erin om een aanmerkelijk deel van de data te stelen voordat ze werden ontdekt. De bestanden bevatten persoonlijke informatie van donateurs, zoals namen, adressen, telefoonnummers, en in sommige gevallen zelfs financiële gegevens. Na de ontdekking van de inbreuk heeft Blackbaud naar verluidt losgeld betaald aan de aanvallers, in ruil voor de belofte dat de gestolen data zouden worden verwijderd.

De hack had een directe impact op een groot aantal goede doelen, die plotseling geconfronteerd werden met de uitdaging om hun donateurs en andere betrokkenen te informeren over het datalek. Voor veel van deze organisaties veroorzaakte de inbreuk niet alleen zorgen over de privacy en veiligheid van gevoelige informatie, maar ook over het potentiële verlies van vertrouwen bij hun donateurs en de bredere gemeenschap.

In reactie op het incident namen getroffen organisaties stappen om hun systemen te beveiligen, getroffen individuen te informeren en hun cyberweerbaarheid te vergroten. Blackbaud zelf verklaarde dat het maatregelen had genomen om het beveiligingslek te dichten en beloofde zijn beveiligingsprotocollen te versterken om toekomstige aanvallen te voorkomen. Het bedrijf kwam echter ook onder vuur te liggen vanwege de manier waarop het de inbreuk had afgehandeld, inclusief kritiek op het betalen van losgeld en de slechte communicatie naar getroffen klanten.

De Blackbaud-hack laat zien dat cybersecurity een continue inspanning vereist en dat de bescherming van gevoelige gegevens een gedeelde verantwoordelijkheid is, niet alleen van de organisatie zelf, maar ook van haar leveranciers.

13.000 getroffen klanten	Schikking van bijna **50M**	**> 20M** getroffen individuen

Hoe staan Nederlandse goede doelen ervoor?

The Trusted Third Party (TT3P) heeft zich als doel gesteld om de cybersecurity binnen de goede doelen sector te helpen versterken. Dankzij gerichte risico-inventarisaties en -evaluaties voor een breed scala aan opdrachtgevers, heeft TT3P een diepgaand inzicht verworven in de cybersecuritypositie van Nederlandse goede doelen. Dit inzicht wordt versterkt door een zorgvuldig onderhouden benchmark, die organisaties in staat stelt hun cybersecurity-prestaties direct te vergelijken met die van hun gelijken binnen de sector. Het interessante van deze benchmark is, dat deze gebaseerd is op het erkende ISO 27001 framework, wat organisaties helpt om een gestandaardiseerd niveau van informatiebeveiliging te hanteren, zelfs als ze niet ISO-gecertificeerd (hoeven te) zijn.

Het ontbreekt veel goede doelen aan beleid en boardroom awareness

Vooropgesteld dat er natuurlijk ook goede doelen zijn die cybersecurity hoge prioriteit hebben gegeven, schetsen de resultaten die TT3P veelvuldig tegenkomt bij goede doelen een duidelijk beeld: veel goede doelen kampen met vergelijkbare uitdagingen op het gebied van cybersecurity. Ze hebben geen actueel en goed gedocumenteerd informatiebeveiligingsbeleid en werken dus onvoldoende planmatig aan cybersecurity. En dat terwijl cybercriminaliteit een van de grootste organisatierisico's van vandaag vormt. Er zijn vaak wel een aantal technische beheersmaatregelen getroffen. Maar het is niet voor niets dat bij standaarden als bijvoorbeeld ISO 27001 en ook voor het voldoen aan wetgeving op het gebied van cybersecurity, er wordt vereist dat er actueel beleid kan worden aangetoond en dat de beheersmaatregelen voorkomend uit dat beleid geïmplementeerd moeten zijn en gecontroleerd en beheerd moeten worden.

Een organisatie moet aantoonbaar in control zijn. Met alle techniek van de wereld kan een hacker niet buiten worden gehouden als de organisatorische maatregelen niet op orde zijn. Een virusscanner, firewall en een backup zorgen er simpelweg niet voor dat systemen 100% veilig zijn. Het ontbreken van beleid is direct gevolg van het gemis aan betrokkenheid bij het onderwerp van besturen en management teams. Cybersecurity is bij goede doelen te vaak helemaal niet belegd of alleen bij de ICT-afdeling.

Geen plan voor hacksituaties en geen inzicht in cyberrisico's bij leveranciers

Wanneer met ICT-leveranciers wordt gewerkt is er bij goede doelen nauwelijks inzicht in en controle op cybersecurity risico's bij deze leveranciers. Dat geldt overigens ook voor andere kritische leveranciers. Fondsenwerving bijvoorbeeld wordt vaak uitbesteed en daarbij worden grote hoeveelheden data verstrekt aan leveranciers of leveranciers hebben zelf direct toegang tot de systemen met de data. Er wordt onterecht aangenomen dat een leverancier 'toch wel goed beveiligd zal zijn'. De Blackbaud case uit dit rapport, maar bijvoorbeeld ook de hack op NEBU, die wordt behandeld in het datalekkenrapport over 2023 van de Autoriteit Persoonsgegevens, tonen aan dat de werkelijkheid weerbarstiger is.

Wanneer er dan sprake is van een hack blijkt de voorbereiding daarop onvoldoende. Goede doelen missen vaak een effectief incidentresponsplan. Zo'n plan stel je op als voorbereiding op een beveiligingsincident, zoals een hack. En in het plan is opgenomen wat het scenario is bij een hack. Wie wordt er bijvoorbeeld als eerste gebeld om de hack op te lossen? Hoe zijn we weer zo snel mogelijk operationeel? Hoe en wat communiceren we met medewerkers en betrokkenen? En wat als er een journalist belt?

Meer mogelijkheden voor de optimalisatie van cybersecurity
Daarnaast is er onvoldoende inzicht in de gebruikte hardware en software, en wordt de cruciale functie van security officer vaak belegd bij iemand zonder de vereiste tijd en expertise. Bovendien worden cyberrisico-inventarisaties & -evaluaties zelden adequaat uitgevoerd. Opvallend is ook het gebrek aan continue awareness activiteiten onder medewerkers, een ontoereikend beleid rond het gebruik van privé apparatuur en de onderwaardering van cybersecurity op bestuurs- en managementniveau.

Cybersecurity benchmark
Deelname aan de TT3P benchmark biedt goede doelen inzicht in hoe zij presteren ten opzichte van vergelijkbare organisaties en stelt hen ook in staat om gerichte verbeteringen door te voeren op basis van concrete en meetbare KPI's. Door deel te nemen, kunnen goede doelen leren van de best practices binnen de sector, hun eigen cybersecuritybeleid versterken, en zo bijdragen aan een veiligere omgeving voor zowel eigen medewerkers als degenen die zij ondersteunen.

TT3P nodigt u uit om deel te nemen aan deze benchmark; het is een kans om uw organisatie te beschermen tegen de steeds veranderende dreigingen in het digitale landschap en om uw toewijding aan informatiebeveiliging te tonen. Samen kunnen we een verschil maken in de cybersecurity van de goede doelensector. Ontdek hoe uw organisatie zich verhoudt en neem de stappen naar een digitaal veiligere toekomst.

Boardroom awareness bij goede doelen

Het is essentieel dat bestuurders van goede doelen zich realiseren dat cybersecurity niet slechts een ICT-probleem is, maar een kern-verantwoordelijkheid van het bestuur. Te vaak wordt deze cruciale kwestie overgelaten aan de ICT-afdeling of de externe ICT-leverancier, terwijl de strategische en operationele implicaties veel verder reiken. Cyberdreigingen evolueren voortdurend en raken elke laag van de organisatie, van de financiële stabiliteit tot de reputatie. Bestuurders moeten begrijpen dat hun betrokkenheid van vitaal belang is om deze risico's effectief te beheersen.

De verantwoordelijkheid ligt bij het bestuur om een cultuur van bewustzijn en paraatheid te bevorderen, regelmatige risico-inventarisaties te integreren in haar governancepraktijken en ervoor te zorgen dat de organisatie voldoet aan relevante wet- en regelgeving. De betrokkenheid van het bestuur kan het verschil maken tussen een organisatie die voorbereid is op cyberdreigingen en een organisatie die wordt verrast en verlamd door een aanval. Het is van cruciaal belang dat bestuurders cybersecurity tot een prioriteit maken in hun bestuurskamer.

Aanwijzingen voor verbetering van cybersecurity binnen goede doelen

Het is van wezenlijk belang dat goede doelen proactieve stappen ondernemen om hun cyberweerbaarheid te versterken. Dit omvat o.m.:

Uitvoeren van cybersecurity risico-inventarisaties en -evaluaties
Het is cruciaal voor goede doelen om regelmatig, doch zeker eenmaal per jaar, hun cybersecurity-risico's te identificeren en te (laten) beoordelen. Dit helpt organisaties om te begrijpen waar hun kwetsbaarheden liggen en welke bedreigingen het meest relevant zijn voor hun specifieke omstandigheden. Door dit inzicht kunnen goede doelen gerichte acties ondernemen om de risico's te mitigeren en zich te beschermen tegen potentiële aanvallen. Een risico-inventarisatie is ook een uitstekend instrument om te (laten) toetsen of beheersmaatregelen die zijn genomen in het verleden nog steeds goed functioneren.

Vormen en uitrollen van informatiebeveiligings-beleid
Een gestructureerd informatiebeveiligingsbeleid is de ruggengraat van elke cybersecuritystrategie. Het ontwikkelen van een dergelijk beleid vereist een zorgvuldige planning en betrokkenheid van het hele team. Het beleid moet duidelijk de technische en organisatorische beheers-maatregelen, verantwoordelijkheden, en gedrags-regels omtrent informatiebeveiliging binnen de organisatie uiteenzetten. Beleid is geen papieren werkelijkheid. Informatiebeveiligingsbeleid is altijd actueel gedocumenteerd, geïmplementeerd, wordt beheerd en op de juiste werking in de praktijk gecontroleerd.

Waarom zijn deze eerste stappen belangrijk?
Risico-inventarisaties en evaluaties stellen goede doelen in staat om proactief potentiële kwetsbaarheden in hun systemen en processen te identificeren, voordat deze door kwaadwillenden kunnen worden uitgebuit.

Het helpt organisaties om hun middelen effectief in te zetten door prioriteit te geven aan de meest kritieke verbeterpunten.

Het hebben van een goed gedefinieerd beleid is essentieel voor het creëren van een cultuur van cybersecurity binnen de organisatie. Het biedt een raamwerk voor het nemen van beslissingen en het implementeren van beveiligingsmaatregelen en dus ook voor goed onderbouwde investeringen. Bovendien versterkt het de verantwoordelijkheid en het bewustzijn onder werknemers en vrijwilligers, en zorgt het ervoor dat iedereen weet hoe te handelen in het geval van een beveiligings-incident.

Technische beveiligingsmaatregelen
Implementatie van basisbeveiligingsmaatregelen zoals firewalls, antivirussoftware, back-ups en regelmatige updates en patches voor alle systemen.

Bewustwording en training
Het vergroten van de bewustwording en het trainen van personeel en vrijwilligers om phishing pogingen te herkennen en veilig online te werken.

Incidentresponsplannen
Het ontwikkelen en oefenen van een incident responsplan om effectief te kunnen reageren op en herstellen van cyberaanvallen.

Door de bovenstaande stappen te implementeren, kunnen goede doelen niet alleen hun cyber-weerbaarheid versterken maar ook het vertrouwen van hun donateurs, begunstigden, en de bredere gemeenschap behouden. Het is een cruciale investering in de duurzaamheid en effectiviteit van hun missie in het digitale tijdperk.

Implementatie van cybersecurity-maatregelen en responsstrategie voor incidenten

In het licht van de toenemende cyberdreigingen is het essentieel dat goede doelen niet alleen preventieve technische en organisatorische maatregelen nemen om cyberaanvallen te voorkomen, maar ook voorbereid zijn op mogelijke beveiligingsincidenten. Dit onderdeel behandelt het belang van een geïntegreerde aanpak voor cybersecurity en de ontwikkeling van een effectieve responsstrategie voor incidenten.

Integratie van cybersecurity in de organisatie-cultuur

Cybersecurity moet gezien worden als een integraal onderdeel van de organisatiecultuur. Dit vereist betrokkenheid op alle niveaus, van het bestuur tot de medewerkers en eventuele vrijwilligers. Het regelmatig organiseren van trainingen en bewustwordingscampagnes is van belang om te zorgen dat iedereen binnen de organisatie de basisprincipes van digitale veiligheid begrijpt en toepast. Dit omvat ook het promoten van een cultuur waarin het melden van een potentieel foute handeling of van verdachte activiteiten wordt aangemoedigd, zonder angst voor repercussies.

Ontwikkeling van een responsstrategie voor incidenten

Een gedegen responsstrategie voor cyber-securityincidenten is belangrijk voor het minimaliseren van de schade als gevolg van een aanval. Deze strategie moet duidelijke richtlijnen bevatten over hoe te reageren op verschillende soorten incidenten, wie verantwoordelijk is voor wat, en hoe en wanneer externe partijen, zoals de autoriteiten, leveranciers of cyberbeveiligings-bedrijven, betrokken moeten worden. Belangrijke elementen van een responsstrategie zijn:

- Onmiddellijke detectie en beoordeling: Snelle identificatie van een incident en beoordeling van de omvang en de impact.
- Communicatieplan: Duidelijke procedures voor interne en externe communicatie tijdens en na een incident.
- Herstelprocessen: Stappen voor het herstellen van getroffen systemen en diensten om de bedrijfscontinuïteit te waarborgen.
- Evaluatie en verbetering: Post-incident analyse om te leren van het voorval en toekomstige beveiligingsmaatregelen te versterken.

Samenwerking met externe partijen

Geen enkele organisatie is een eiland, vooral niet als het gaat om cybersecurity. Goede doelen moeten streven naar samenwerking met externe partijen, zoals cybersecuritybedrijven, branche-organisaties, en andere goede doelen, om kennis en middelen te delen. Deze samenwerking kan helpen bij het versterken van de algemene cyberweerbaarheid door toegang te bieden tot gespecialiseerde expertise en inzichten in de nieuwste bedreigingen en verdedigings-mechanismen.

Handreiking Cybersecurity Goede Doelen Nederland

Samenwerken met andere goede doelen en relevante autoriteiten helpt om informatie over dreigingen te delen en beste praktijken uit te wisselen. Brancheorganisatie Goede Doelen Nederland organiseert met regelmaat trainingen over cyberweerbaarheid voor verantwoordelijke functionarissen bij haar leden. In aanvulling daarop is in 2024 de Handreiking Cybersecurity voor leden van Goede Doelen Nederland gepubliceerd.

In niet al te technisch taalgebruik wordt daarin aan de lezer de basisprincipes en het belang van cybersecurity uitgelegd, hoe risico's kunnen worden geïnventariseerd en hoe er passende beveiligingsmaatregelen genomen kunnen worden. Hierdoor zullen ook managers zonder ICT-achtergrond het belang van cyberweerbaarheid van hun organisatie begrijpen en inzien welke eventueel noodzakelijke investeringen gedaan moeten worden om systemen en gegevens veilig te houden.

Inkoopsamenwerking Goede Doelen Nederland voor cybersecuritydiensten

Brancheverenigingen Goede Doelen Nederland heeft een inkoopsamenwerking met The Trusted Third Party (TT3P), specialist in cybersecurity diensten. TT3P helpt organisaties met het optimaal inrichten van informatiebeveiliging op het vlak van techniek, beleid, organisatie en mens.

Zo kan het risico op gijzeling van bedrijfssystemen, bedrijfsgegevens en het onrechtmatig toegang verkrijgen tot data door onbevoegde derden aanmerkelijk worden verkleind. De diensten omvatten onder meer technische security audits, risico-inventarisaties, flexibele security officer diensten, security awareness trainingen en phishing simulaties. De diensten zijn beschikbaar voor en passend bij zowel grote als kleine organisaties.

Responsible disclosure en samenwerking met ethische hackers

Een effectieve manier waarop goede doelen hun cyberbeveiliging continu kunnen verbeteren, is het implementeren van een responsible disclosure-beleid en door samen te werken met ethische hackers. Responsible disclosure moedigt individuen aan om beveiligingslekken te melden bij een organisatie en biedt een veilig en gestructureerd kader voor goede doelen om deze informatie te ontvangen en te verwerken.

Responsible disclosure
Responsible disclosure is een beleid waarbij individuen die kwetsbaarheden in ICT-systemen ontdekken, deze op een verantwoorde manier kunnen melden aan de organisatie, zodat het probleem veilig kan worden opgelost voordat het openbaar wordt gemaakt. Dit beleid dient de volgende elementen te omvatten:

- Een duidelijk communicatiekanaal (zoals een specifiek e-mailadres) voor het melden van kwetsbaarheden.
- Richtlijnen over hoe informatie over de kwetsbaarheid gedeeld moet worden, met de nadruk op vertrouwelijkheid.
- Een belofte van de organisatie om de melding serieus te nemen en binnen een redelijke termijn te onderzoeken.
- Eventueel een beloningssysteem of erkenning voor degenen die waardevolle meldingen doen.

Samenwerking met ethische hackers
Ethische hackers, ook wel bekend als penetration testers of white hat hackers, gebruiken hun vaardigheden om proactief beveiligingslekken in systemen en netwerken te identificeren, met als doel de organisatie te helpen deze op te lossen voordat kwaadwillenden ze kunnen uitbuiten. Goede doelen kunnen overwegen om:

- Externe ethische hackers in te huren voor geplande penetratietests.
- Deel te nemen aan bug bounty-programma's. Hierin worden ethische hackers beloond voor het ontdekken en het melden van alle kwetsbaarheden.
- Workshops en trainingssessies te organiseren met ethische hackers om personeel en vrijwilligers te leren over de nieuwste cyber-dreigingen en -verdedigingsmechanismen.

Samen sterker: Het pad vooruit in cybersecurity

Digitalisering biedt goede doelen nieuwe mogelijkheden om hun missies te ondersteunen en uit te breiden. Echter, zoals geïllustreerd door de incidenten bij het Internationale Comité van het Rode Kruis en Blackbaud, brengt digitalisering ook significante risico's met zich mee. Cyberaanvallen kunnen niet alleen de operationele capaciteit van een organisatie verstoren, maar ook de privacy van gevoelige gegevens compromitteren, wat leidt tot verlies van vertrouwen onder donateurs en begunstigden.

De aard en omvang van cyberdreigingen evolueren continu, waardoor het voor organisaties noodzakelijk is om hun cyberbeveiligings-maatregelen doorlopend te evalueren en te versterken. Dit vereist een proactieve benadering, met een focus op zowel preventie als paraatheid bij incidenten.

Oproep tot samenwerking

Deelnemen aan netwerken voor het delen van informatie en beste praktijken met andere goede doelen en relevante organisaties kan de collectieve weerbaarheid tegen cyberdreigingen vergroten.

TT3P, partner van Goede Doelen Nederland, hanteert een benchmark voor cybersecurity van goede doelen. De benchmark bevat data van risico-inventarisaties van tientallen goede doelen-organisaties. Wilt u meer weten over de benchmark en erachter komen waar uw goede doelen organisatie staat ten opzichte van andere organisaties in de sector? Neem dan contact met ons op via info@tt3p.nl.

Laten we samenwerken om een veiligere digitale toekomst te creëren voor goede doelen en de gemeenschappen die zij dienen.

Disclaimer

De informatie die in dit rapport wordt verstrekt, is bedoeld voor algemene informatiedoeleinden en mag niet worden opgevat als professioneel advies. Hoewel de grootste zorg is besteed aan het waarborgen van de nauwkeurigheid en actualiteit van de inhoud, aanvaardt The Trusted Third Party (TT3P) B.V. geen aansprakelijkheid voor eventuele fouten, weglatingen of onnauwkeurigheden, noch voor enige actie of beslissing genomen op basis van de informatie vervat in dit document. Wij raden aan om altijd professioneel advies in te winnen voordat u handelt op basis van de inhoud van dit rapport.

De situaties en voorbeelden die in dit rapport worden besproken, zijn illustratief en kunnen niet direct van toepassing zijn op alle organisaties of situaties. The Trusted Third Party (TT3P) B.V. is niet verantwoordelijk voor de resultaten van acties ondernomen op basis van de informatie verstrekt in dit document. Gebruikers van dit rapport doen dit op eigen risico.