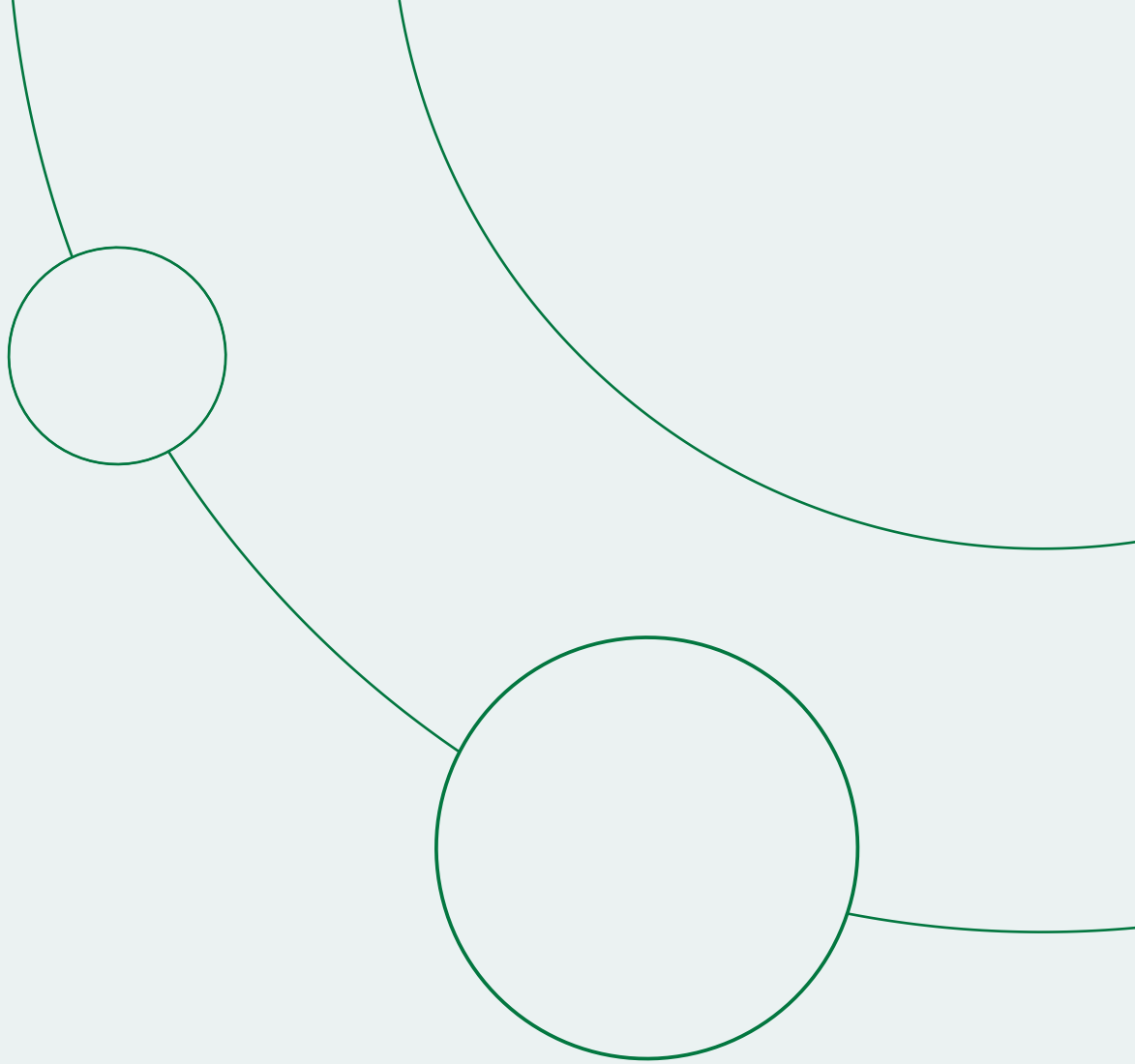
Handelingskader na een datalek

Rapportage van het onderzoek naar behoeften en verwachtingen van slachtoffers van een datalek

ROK: Research Community’s
Projectnummer Blauw: 34289
Mei 2026



blauw

Inleiding

Woord vooraf

Het viel op hoe sterk dit onderwerp leeft. Reacties kwamen niet alleen in grote aantallen, maar ook snel en betrokken binnen. Dit laat zien dat datalekken veel mensen raken en dat aandacht hiervoor belangrijk is.

Esra en Dori
Blauw Research
(welcome@blauw.com)

Methode

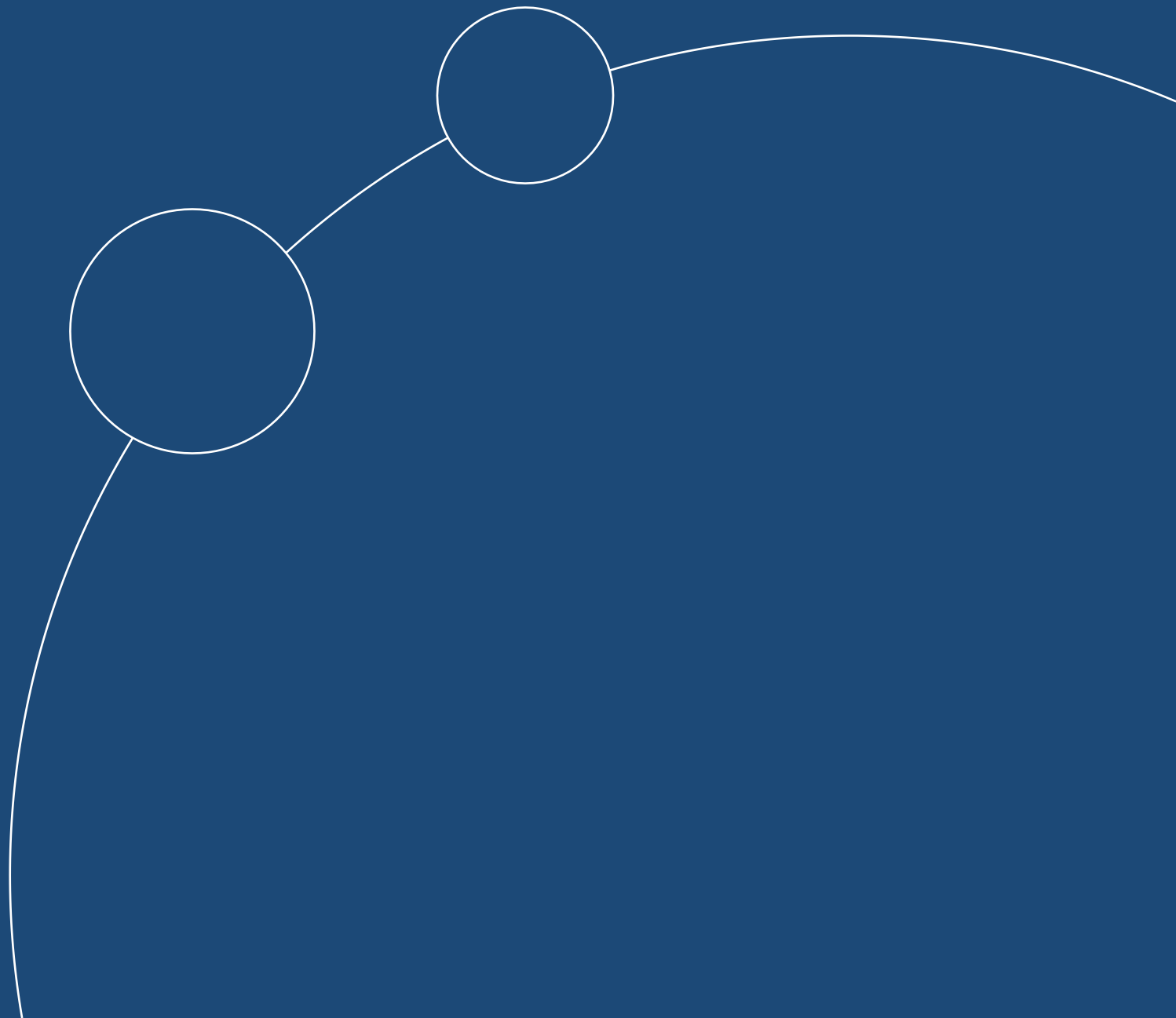
Het onderzoek is uitgevoerd in de online research community ‘Nederland Denkt Mee’.

Blauw Research beheert deze community in opdracht van het ministerie van Algemene Zaken, in het bijzonder voor Dienst Publiek en Communicatie (DPC).

Leeswijzer

Het onderzoek heeft een kwalitatieve basis.
Kwalitatief onderzoek biedt diepgaand inzicht in gedrag, motivaties en emoties. Het is een methodiek waarmee je het *waarom* achter onderzoeksresultaten kunt verklaren en heeft minder nadruk op statistiek (hoeveel).
De cijfermatige uitkomsten zijn indicatief en ze geven richting aan.

Management-samenvatting



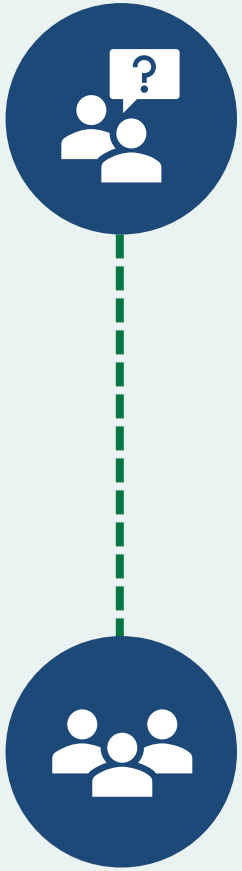
Achtergrond en doelstelling

Achtergrond

In de afgelopen periode hebben meerdere grootschalige datalekken en hacks van persoonsgegevens de maatschappelijke en politieke aandacht vergroot. In de Tweede Kamer is daarom de vraag opgeworpen om te onderzoeken of er behoefte is aan een duidelijk handelingskader voor slachtoffers van datalekken. Tegelijkertijd wordt onderzocht of aanvullende maatregelen, zoals een wettelijke nazorgplicht, nodig zijn om de positie van slachtoffers te versterken. Voor een effectieve uitwerking is het van belang inzicht te krijgen in hoe burgers datalekken ervaren, welke acties zij ondernemen en welke ondersteuning zij verwachten van betrokken partijen. De uitkomsten van dit onderzoek worden daarom gebruikt als inhoudelijke input voor het informeren van de Kamer over de ontwikkeling van een handelingskader dat aansluit bij de behoeften van burgers.

Onderzoeksdoel

Het doel van dit onderzoek is om de huidige houdingen, behoeften, gedragingen en kennis/inzicht van Nederlandse burgers te verkennen met betrekking tot hun handelingskader bij een datalek waarbij hun persoonsgegevens betrokken zijn.

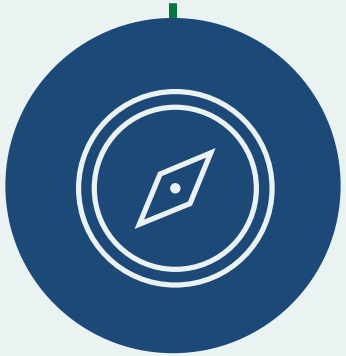


Onderzoeksvraag

Wat zijn de behoeften en verwachtingen van burgers die slachtoffer zijn van een datalek, en wat verwachten zij daarin van de getroffen organisatie en van andere (publieke) partijen?

Doelgroep

Dit onderzoek is uitgevoerd onder deelnemers van de community ‘Nederland Denkt Mee’, bestaande uit een brede afspiegeling van het Nederlandse publiek van 18 jaar en ouder. Binnen dit onderzoek is bovendien specifiek verdiepend gekeken naar de groep Nederlanders van 60 jaar en ouder.



Slachtoffers verwachten vooral dat getroffen organisatie hen concreet en proactief helpt

Burgers die slachtoffer zijn van een datalek hebben vooral behoefte aan duidelijkheid, zekerheid en concrete handelingsperspectieven. Zij verwachten daarbij primair dat de organisatie waar het datalek heeft plaatsgevonden de regie neemt in communicatie en ondersteuning. In de praktijk gebeurt dit vaak onvoldoende concreet, waardoor slachtoffers grotendeels zelf in actie komen en informatie zoeken.

De verwachtingen richting overheid en andere (publieke) partijen zijn beperkt en de verantwoordelijkheid wordt duidelijk bij de getroffen organisatie gelegd. Deze inzichten wijzen op het belang van een handelingskader dat met name organisaties helpt om slachtoffers snel, concreet en praktisch te ondersteunen.

Meer dan de helft is slachtoffer van datalek

Datalekken en hacks komen veel voor onder de onderzochte groep Nederlanders op de community. Meer dan de helft geeft aan hier ooit slachtoffer van te zijn geweest, waarbij het in sommige gevallen zelfs om meerdere incidenten gaat.

Het lekken betreft meestal naam- en contactgegevens, al is voor een aanzienlijk deel van de slachtoffers onduidelijk welke gegevens precies zijn buitgemaakt. De leden hebben het vaakst met een datalek van telecombedrijven* te maken. Ook zorginstellingen en online diensten worden vaak benoemd.

*Dit beeld is waarschijnlijk beïnvloed door de periode van het onderzoek. Kort na het datalek bij een grote telecomprovider.

Datalek raakt, maar impact verschilt en neemt door de tijd af

Slachtoffer zijn van een datalek gaat gepaard met uiteenlopende gevoelens, waarbij onveiligheid, onzekerheid en controleverlies het meest prominent naar voren komen. Veelgenoemde emoties zijn schrik, stress, boosheid en frustratie. *"Ik ben er erg van geschrokken. Je hebt een gevoel van controle verlies. Dat komt doordat iemand anders ineens toegang kan hebben tot iets dat voor mij heel persoonlijk is. Daarna ontstond onzekerheid: je weet niet wat er met je gegevens gebeurt en of er misbruik volgt."*

Deze gevoelens hangen sterk samen met het feit dat het datalek buiten de invloed van het individu plaatsvindt en dat vaak onduidelijk is wat er precies is gebeurd en wat de mogelijke gevolgen zijn. Tegelijkertijd geeft ongeveer de helft van de slachtoffers op de community aan dat een datalek hen minder raakt en dat zij het incident als (relatief) weinig impactvol ervaren.

De ervaren impact wordt in de praktijk regelmatig versterkt door concrete overlast, zoals het frequenter ontvangen van spam, *phishingmails* en verdachte telefoontjes. Tegelijkertijd neemt bij een deel van de slachtoffers de spanning na verloop van tijd af, met name wanneer zichtbare negatieve gevolgen uitblijven. Toch blijft er bij veel mensen een zekere waakzaamheid en een verminderd vertrouwen in organisaties bestaan. *"Ik maak me er niet heel erg druk om, maar ik hou alles wel een beetje extra in de gaten."*

Behoefte aan duidelijkheid en handelingsperspectieven

In de nasleep van een datalek willen slachtoffers begrijpen:
- wat er is gebeurd
- welke gegevens zijn gelekt
- wat de mogelijke gevolgen zijn, zowel op korte als langere termijn.

Daarnaast is er behoefte aan:
- concrete instructies of een stappenplan over wat zij zelf kunnen doen aan maatregelen om risico's te beperken.

Slachtoffers willen direct en persoonlijk geïnformeerd worden, in plaats van via algemene kanalen zoals het nieuws.

"Ik wil direct geïnformeerd worden; wat er gebeurd is en welke gegevens zijn gelekt. Ook wil ik weten wat het bedrijf gaat doen om dit in de toekomst te voorkomen."

Grootste verantwoordelijkheid bij getroffen organisatie

Er wordt verwacht dat getroffen organisaties:
- snel, transparant en proactief communiceren
- verantwoordelijkheid** nemen voor het incident
- ondersteunen bij vragen en problemen van slachtoffers
- in sommige gevallen compensatie bieden.

**verantwoordelijkheid nemen betekent: erkennen van de situatie, aanbieden van excuses en zichtbaar maatregelen nemen om schade te beperken en herhaling te voorkomen.

In de praktijk ervaren slachtoffers dat organisaties hier regelmatig tekortschieten. Communicatie is vaak te laat, onvoldoende concreet of onvoldoende afgestemd op de persoonlijke situatie. Adviezen blijven veelal algemeen van aard, waardoor ze als weinig behulpzaam worden ervaren.

Beperkte verwachtingen van de overheid na datalek

Spontaan worden overheid, toezichthouders of andere instanties nauwelijks genoemd, de focus ligt duidelijk op de organisatie zelf als primaire aanspreekpunt.

Wanneer expliciet wordt doorgevraagd naar de rol van overheid en andere instanties, ontstaat een aanvullend beeld.
- van toezichthouders zoals de Autoriteit Persoonsgegevens wordt met name verwacht dat zij toezicht houden, onderzoek doen naar de oorzaak van datalekken en indien nodig handhaven. Daarnaast zien slachtoffers een rol in het bieden van toegankelijke informatie en het bijdragen aan preventie.
- van hulporganisaties en de politie worden vooral ondersteuning en advies verwacht, bijvoorbeeld bij schade of aangifte, al is het vertrouwen in de effectiviteit hiervan beperkt.
- banken worden enkele keren genoemd als partij waarvan men actie verwacht. Sommigen verwachten dat banken verdachte transacties monitoren. Anderen zien banken als voorbeeld instantie waar de beveiliging op orde moet zijn.

Slachtoffers komen zelf in actie, maar missen richting

Na een datalek ondernemen de meeste slachtoffers zelf actie, vaak zonder of met beperkte ondersteuning vanuit de getroffen organisatie. Als gevolg daarvan voelen slachtoffers zich grotendeels op zichzelf aangewezen en gaan veel van hen zelf actief op zoek naar aanvullende informatie of nemen zij op eigen initiatief extra basismaatregelen. *"Ik heb zelf mijn wachtwoorden gewijzigd en tweestapsverificatie ingesteld."*

Deze maatregelen zijn vooral gericht op het beperken van risico's en het monitoren van mogelijke gevolgen. Denk aan:

- wijzigen van wachtwoorden
- instellen van tweestapsverificatie
- controleren van accounts
- alert zijn op *phishing*, spam en verdachte communicatie
- vaker controleren van hun bankrekening
- zelfstandig zoeken naar informatie of advies bij bekenden of experts.

Daarnaast is er ook een groep die weinig of niets onderneemt, bijvoorbeeld omdat de situatie niet als ernstig wordt ingeschat of omdat men niet goed weet wat er verwacht wordt. *"Ik heb niks gedaan, maar ik ben wel meer alert met het openen van e-mails."*

Een EHBO-kit spreekt aan, maar moet verder gaan dan algemeen advies

Tijdens het onderzoek is de volgende vraag over een EHBO-kit voorgelegd: *'Stel er komt een EHBO-kit voor hulp bij een datalek. Wat vinden jullie van dit idee?'.* De meeste leden zien dit idee als positief en kansrijk, omdat het inspeelt op hun behoefte aan duidelijkheid en houvast op een moment van onzekerheid. *"Ik vind het een leuk idee. In zo'n kit zouden stappenplannen moet zitten, welke stappen te nemen wanneer je slachtoffer bent van een datalek."*

Leden geven aan dat zo'n EHBO-kit vooral praktisch en direct toepasbaar moet zijn. Denk aan:

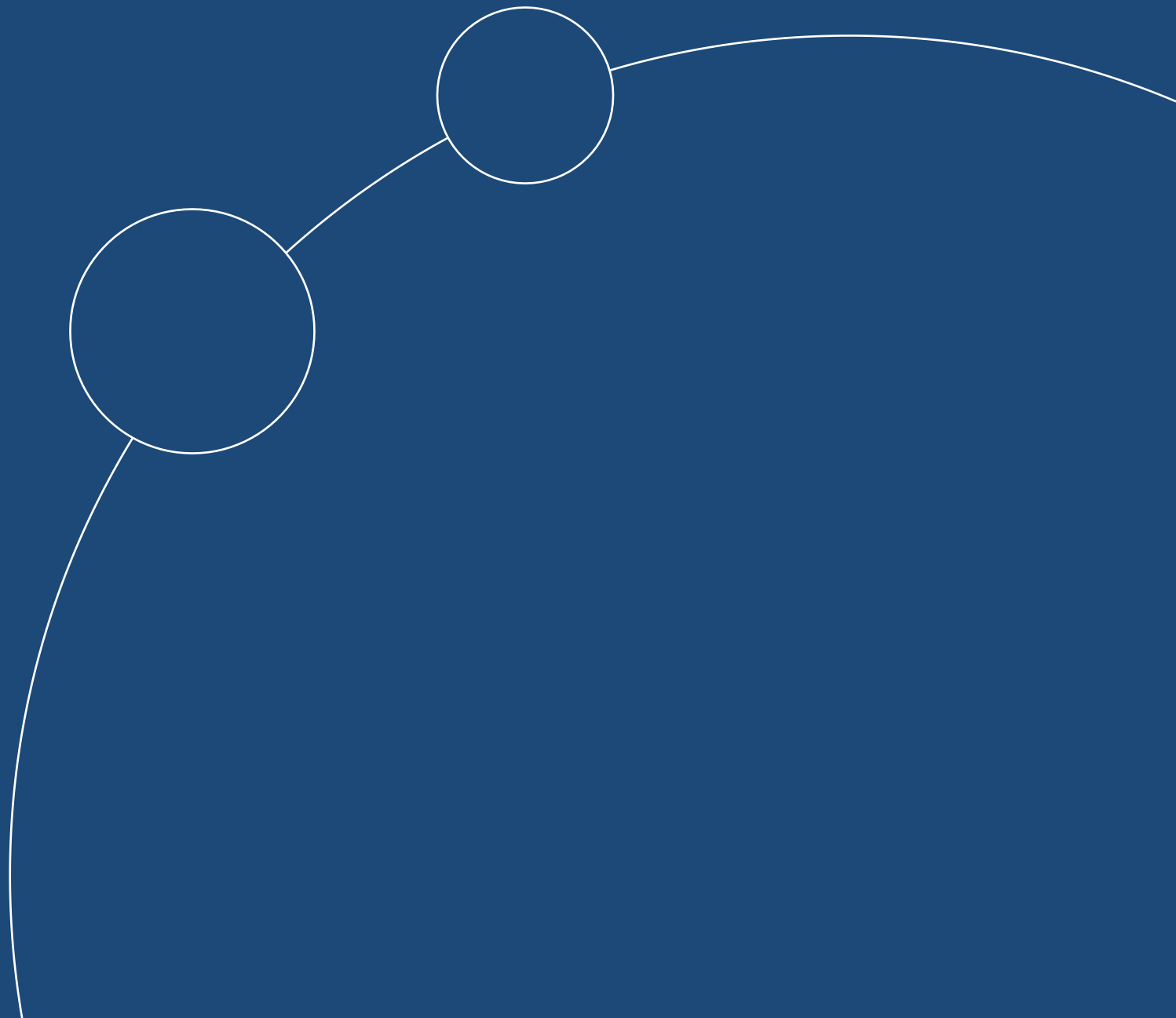
- stappenplan met concrete acties over wat je kan doen
- duidelijke uitleg van het datalek, wat er gebeurd is en wat dit betekent / mogelijke risico's en gevolgen voor slachtoffers
- concrete handvatten zoals een checklist of voorbeeldsituaties
- inzicht in impact en urgentie, waar mogelijk afgestemd op de persoonlijke situatie
- toegang tot hulp zodat duidelijk wordt waar men terecht kan.

Tegelijkertijd zijn er ook kritische geluiden. Sommige leden verwachten dat dergelijke informatie primair door de getroffen organisatie wordt aangeboden. Ook bestaat het risico dat de kit weinig toevoegt als de inhoud niet verder gaat dan algemene adviezen.

De term "EHBO-kit" wordt niet altijd passend gevonden. Enkele leden associëren dit met een medische EHBO-kit (zoals pleisters en verband). Voor anderen wekt de term de indruk dat een datalek snel en eenvoudig op te lossen is, terwijl het in werkelijkheid vaak complex is.

Bijlage

- Verdieping kwetsbare doelgroep
- Onderzoeksverantwoording
- Draaiboek



Verdieping kwetsbare doelgroep (ouderen, 60 plus)

Sterker de behoefte aan duidelijkheid en verantwoordelijkheid vanuit de organisatie

De inzichten voor de kwetsbare doelgroep ouderen (60 plus) zijn grotendeels in lijn met het totaalbeeld. Net als de totaalgroep hebben ouderen behoefte aan duidelijke informatie over wat er gebeurd is en welke gegevens zijn gelekt, maar ook aan concrete handelingsperspectieven. Ook ouderen vinden dat de primaire verantwoordelijkheid bij de getroffen organisatie ligt. Op enkele punten zien we duidelijke verschillen in de behoeften van ouderen:

Sterke behoefte aan duidelijkheid, maar ook gevoel van machteloosheid

- Ouderen geven vaker aan dat zij zelf weinig kunnen doen na een datalek. Ze doen wat ze kunnen, maar voelen zich hier vaak beperkt in, doordat zij zich afhankelijker voelen van de getroffen organisatie.
- De acties blijven ook vaak beperkt tot basismaatregelen (zoals een wachtwoord wijzigen of alert zijn).
- Een deel van de ouderen vraagt soms ook familie om hulp na een datalek en vraagt bijvoorbeeld hun zoon om te helpen met het wijzigen van gegevens.

Meer nadruk op verantwoordelijkheid en nazorg van getroffen organisatie

- Ouderen hechten meer waarde aan transparantie over wat er is gebeurd. Er is een sterkere behoefte aan fatsoenlijke en menselijke communicatie.
- Compensatie door de getroffen organisatie wordt vaker gezien als vanzelfsprekend. *"Ik verwacht korting op de abonnementskosten of een eenmalig bedrag."*

Grotere rol voor overheid, maar met beperkt vertrouwen

- Ouderen noemen vaker dat zij een rol weggelegd zien voor de overheid, toezichthouders en de politie.
- Tegelijkertijd is het vertrouwen in de effectiviteit van deze partijen ook beperkt (bijvoorbeeld dat deze partijen vaak te laat zijn met acties of dat de hulp te gebrekkig is). *"De overheid, die komt vaak als mosterd na de maaltijd."*

Behoefte aan een stappenplan, maar wel kritischer op de EHBO-kit

- Ouderen hebben nóg meer behoefte aan een praktisch en concreet stappenplan met wat zij moeten doen na een datalek. *"Het moet praktisch zijn en niet alleen uitleg. Wat moet ik doen?"*
- Het idee van een EHBO-kit spreekt een deel van de ouderen minder aan, omdat zij daarmee het idee krijgen dat de verantwoordelijkheid vooral bij het slachtoffer zelf ligt. Dit terwijl zij juist meer verantwoordelijkheid verwachten van de getroffen organisatie.

Verantwoording

Steekproef
Als steekproefkader zijn de deelnemers van community 'Nederland Denkt Mee' gebruikt. In totaal hebben we alle deelnemers uit de community uitgenodigd voor dit vraagstuk (213 leden), waarvan er 126 deelnemers hebben meegedaan aan minimaal één van de opdrachten (response rate: 59%). De verdeling van de respons per opdracht:

- Opdracht 1 (forumtopic): n=110
- Opdracht 2 (forumtopic): n=112
- Opdracht 3 (vragenlijst): n=118
- Opdracht 4 (forumtopic): n=106

NOTE: Net voor de onderzoeksperiode heeft een groot datalek bij een telecomprovider plaatsgevonden. Dit had impact op de reacties van respondenten en verklaard mogelijk het hoge aantal leden dat te maken heeft gehad met een datalek bij een telecomprovider.

Doelgroep

De doelgroep van dit onderzoek is Algemeen Nederlands Publiek (18+).

Opdrachten

Het onderzoek bestond uit 4 opdrachten:
1) Forumtopic
2) Forumtopic
3) Vragenlijst
4) Forumtopic

Veldwerkperiode

7 mei 2026 t/m 18 mei 2026

De opdrachten 1-3 gingen op 7 mei live. Opdracht 4 ging op 12 mei live. Alles ging op 18 mei offline.

Incentive

Deelnemers die het volledige vraagstuk invulden, ontvingen een vergoeding in de vorm van punten. Gespaarde punten kunnen worden ingewisseld voor een cadeaubon.

Draaiboek (1/3)

Forumtopics

1) Forumtopic: Een datalek: wat doet het met jou?

Live op 7 mei

De afgelopen tijd hoor je regelmatig over datalekken bij organisaties. Soms krijg je daar zelf een bericht over van de betreffende organisatie, soms lees je het in het nieuws. Dan hoor je dat jouw gegevens misschien zijn gelekt. We zijn benieuwd hoe jij dit ervaart. Beantwoord in dit forumtopic de volgende vragen:

- Ben je zelf wel eens slachtoffer geweest van een datalek of hack bij een organisatie?
- Hoe voelde dat voor jou? Waarom voelde je je zo?
- Is dat gevoel nog veranderd in de dagen/weken erna? Waardoor?

2) Forumtopic: Wat verwacht jij na een datalek?

Live op 7 mei

Stel: er is een datalek bij een organisatie waar jij klant bent (of was). Jouw persoonsgegevens zijn misschien in verkeerde handen gekomen. Je kan zelf actie ondernemen. En er zijn verschillende partijen die iets kunnen doen. Zoals de organisatie zelf, de overheid, toezichthouders of hulpinstanties. Wij horen graag wat jij in deze situatie verwacht en van wie. Beantwoord in dit forumtopic de volgende vragen:

- Wat heb je zelf gedaan?
- Van wie verwacht je verder ook actie na een datalek van jouw gegevens?
- Wat verwacht je concreet van die partij? Geef duidelijke voorbeelden.

4) Forumtopic: Wat vind je van een EHBO-kit?

Live op 12 mei

Stel er komt een EHBO-kit voor hulp bij een datalek. We zijn benieuwd wat jullie van dit idee vinden.

- Wat verwacht je van een EHBO-kit voor hulp bij een datalek?
- Welke informatie verwacht je hier te vinden?
- Welke acties moeten hierin benoemd staan?
- Had je het fijn gevonden als zoiets als een EHBO-kit bij een datalek bestaat?
- Was je er dan gaan kijken? Waarom wel/niet?

Draaiboek (2/3)
Vragenlijst

4) Vragenlijst: Gegevens gelekt, wat nu?
Live op 7 mei

1. Ben je wel eens slachtoffer geweest van een datalek of hack bij een organisatie? [single respons]
    - ja, 1 keer
    - ja, meerdere keren
    - nee (--> naar q16)
    - weet ik niet

2. Welke gegevens van jou zijn daarbij gelekt? (meerdere antwoorden mogelijk)
    - naam en contactgegevens (zoals adres en telefoonnummer)
    - inloggegevens (zoals email en wachtwoord)
    - financiële gegevens (zoals bankrekening)
    - identiteitsgegevens (zoals kopie paspoort of BSN)
    - medische gegevens (zoals welke ziekte, medicijngebruik en behandelingen)
    - weet ik niet
    - anders, namelijk… [open invoerveld]

3. Bij wat voor soort organisatie vond dit datalek plaats?
    - telecom
    - zorg
    - overheid
    - energie
    - webshop of online dienst
    - financiële instelling
    - anders, namelijk…[open invoerveld]

4. Hoe voelde dat voor jou? [single respons]
    - ik maakte mij veel zorgen
    - ik vond het vervelend, maar niet heel erg
    - het deed mij weinig
    - ik was boos
    - anders, namelijk…[open invoerveld]

5. Hoe hoorde jij dat er een datalek was? (meerdere antwoorden mogelijk)
    - via een bericht van de organisatie
    - via het nieuws
    - via iemand anders
    - weet ik niet meer
    - anders, namelijk…[open invoerveld]

6. Waar had je op het moment van het bekend worden van het datalek behoefte aan? [open vraag]

7. In welke categorie of categorieën past jouw antwoord op de vorige vraag het beste? (meerdere antwoorden mogelijk)
    - duidelijkheid van informatie
    - hulp bij wat ik moest doen
    - zekerheid over de situatie
    - dat iemand verantwoordelijkheid nam
    - anders, namelijk…[open invoerveld]

Vervolg op de volgende pagina.

Draaiboek (3/3)

Vragenlijst

8. Wat deed de organisatie na het datalek? (meerdere antwoorden mogelijk)
   - ze gaven uitleg over wat er was gebeurd
   - ze gaven advies over wat ik kon doen
   - ze boden hulp of ondersteuning
   - ze deden weinig of niets
   - weet ik niet meer
   - anders, namelijk: …[open invoerveld]

9. Was er iets dat de organisatie niet deed, maar wat jij wel had verwacht? [open invoerveld]

10. Welke adviezen kreeg jij van de organisatie? (bijvoorbeeld over veiligheid, fraude of vervolgstappen) [open vraag] En welk advies vond je waardevol?

11. Wat heb jij zelf gedaan nadat je hoorde over het datalek? [open vraag]

12. Waren er dingen die je graag wilde doen, maar wat niet kon of waarin je vastliep? Zo ja, waarom kon het niet of liep je vast?
    - ja, namelijk: …[open invoerveld]
    - nee

13. Welke informatie miste jij nog na het datalek? Zijn er dingen die je zelf wel hebt gedaan, maar waarover je niet geadviseerd bent? [open vraag]

14. Als je los denkt van wat er nu bestaat: wat zou er voor jou bij voorkeur moeten gebeuren na een datalek? [open vraag]

15. De Autoriteit Persoonsgegevens (AP) controleert of organisaties goed omgaan met persoonsgegevens en of zij zich aan de privacyregels houden. Na een datalek kan de AP bijvoorbeeld onderzoeken wat er is misgegaan of informatie geven aan burgers. Wat verwacht jij van de Autoriteit Persoonsgegevens na een datalek? [open vraag]

16. Naast de organisatie zelf en de toezichthouder zijn er ook organisaties die hulp bieden aan mensen die slachtoffer zijn van misbruik van hun gegevens, zoals de politie en een meldpunt voor identiteitsfraude. Wat verwacht jij van dit soort organisaties na een datalek? [open vraag]

Bedankt voor het invullen en het delen van jouw ervaringen.