Position paper – Digitale Dolle Mina's

Rondetafelgesprek Cyberveiligheid en informatiebeveiliging
20 mei 2026 – Blok 1: Experts

Cyberveiligheid is niet neutraal: wie al kwetsbaar is, loopt het grootste risico

Cyberveiligheid wordt vaak gepresenteerd als een technisch vraagstuk. Maar dat is maar een deel van het verhaal. In de praktijk gaat het ook over macht, bescherming en ongelijkheid.

Datalekken en gebrekkige informatiebeveiliging raken namelijk niet iedereen op dezelfde manier. Voor sommige mensen betekent een datalek vooral overlast, onzekerheid of administratieve schade. Voor anderen kan het leiden tot stalking, intimidatie, outing, nepprofielen, doxing of zelfs fysiek gevaar.

Vanuit de Digitale Dolle Mina's vragen wij daarom aandacht voor een blinde vlek in het debat over cyberveiligheid: de impact op vrouwen, lhbti+-personen en andere groepen voor wie persoonsgegevens geen neutrale administratieve gegevens zijn, maar informatie die direct tegen hen gebruikt kan worden.

Een adres is voor iemand in een onveilige thuissituatie geen simpel databestand, maar een reëel gevaar. Een telefoonnummer is voor iemand die wordt gestalkt geen contactgegeven, maar een directe lijn voor intimidatie en controle. Medische gegevens zijn voor veel vrouwen niet alleen privacygevoelig, maar raken aan lichamelijke integriteit, autonomie en veiligheid.

1. Een datalek is nooit neutraal

De recente casussen laten zien dat organisaties nog te vaak handelen alsof alle gegevens en alle betrokkenen hetzelfde risico kennen. Dat is niet zo.

Wanneer persoonsgegevens uitlekken van mensen met een afgeschermd adres, van slachtoffers van huiselijk geweld of stalking, van medewerkers in risicovolle functies, ministers, staatssecretarissen, kamerleden, medewerkers van veiligheidsdiensten, beveiligde personen of van mensen van wie medische of identiteitsgevoelige gegevens op straat belanden, is er meer aan de hand dan een standaard privacy-incident.

Dan gaat het om een voorzienbaar veiligheidsrisico.

Juist daarom moet in beleid, toezicht en crisisrespons veel explicieter worden meegenomen dat de gevolgen van een datalek ongelijk verdeeld zijn. Cyberveiligheid zonder oog voor kwetsbaarheid is geen neutrale cyberveiligheid, maar een vorm van schijnveiligheid.

2. Preventie begint bij dataminimalisatie en risicobewust ontwerp

Veel organisaties nemen technische maatregelen, laten audits uitvoeren en voldoen op papier aan normen. Toch blijven ernstige incidenten zich voordoen. Dat komt niet alleen door technische tekortkomingen, maar ook door de manier waarop systemen en processen zijn ingericht.

Te vaak geldt nog steeds:

- er wordt meer data opgeslagen dan nodig is;
- gevoelige gegevens worden centraal samengebracht;
- vrije notitievelden bevatten informatie die daar uit veiligheidsoogpunt niet thuishoort;
- de impact op specifieke risicogroepen wordt niet vooraf meegewogen.

Dat is een fundamenteel probleem.

Organisaties moeten er bij de inrichting van systemen en gegevensverwerking vanuit gaan dat zich onder hun klanten of gebruikers personen bevinden die extra risico lopen. Dat geldt temeer wanneer de organisatie hiervan expliciet kennis heeft, bijvoorbeeld doordat hierover notities zijn opgenomen in klantdossiers.

Dat betekent wat ons betreft:

- **dataminimalisatie als harde norm** en niet als papieren beginsel;
- **segmentatie van gegevens** zodat één incident niet meteen alles blootlegt;
- **geen onnodige opslag van contextinformatie** over stalking, bedreiging, geweld of andere zeer gevoelige omstandigheden in herleidbare systemen;
- waar signalering nodig is: werken met **beperkte categorieën, codes of afgeschermde risicomarkeringen** in plaats van uitgebreide vrije tekstvelden;
- verplichte risicobeoordelingen waarin expliciet wordt gekeken naar de gevolgen voor kwetsbare groepen.

De kernvraag moet niet alleen zijn: *kan iemand binnenkomen?*
Maar ook: *wat gebeurt er als data eenmaal buiten ligt, en wie lopen dan het meeste gevaar?*

3. Crisisbeheersing is nu te veel gericht op organisaties, te weinig op slachtoffers

Zodra een datalek of cyberincident aan het licht komt, zien we in de praktijk vaak hetzelfde patroon: juridische afwegingen, reputatiemanagement en algemene communicatie. Wat ontbreekt, is een aanpak die uitgaat van de mensen die door het incident daadwerkelijk in gevaar kunnen komen.

Voor slachtoffers van stalking, huiselijk geweld, bedreiging of doxing is een algemene melding onvoldoende. Zij hebben behoefte aan concrete, eerlijke en bruikbare informatie over wat het lek voor hén betekent.

Niet:
“Uw persoonsgegevens kunnen mogelijk betrokken zijn.”

Maar bijvoorbeeld:
“Uw adresgegevens zijn gelekt. Dit kan leiden tot ongewenst bezoek aan huis.”
“Uw telefoonnummer is openbaar geworden. Dit kan leiden tot ongewenst contact of intimidatie.”
“Neem deze stappen als u zich onveilig voelt.”

Heldere communicatie is in zulke gevallen geen extra service, maar onderdeel van de veiligheidsrespons.

Wij zien daarom behoefte aan:

- **snellere en duidelijkere communicatie** met handelingsperspectief richting betrokkenen;
- **communicatie die aansluit op concrete risico’s**, niet alleen op juridische meldplichten;
- **specifieke escalatie- en hulpstructuren** voor mensen in risicovolle situaties;
- **betere samenwerking** tussen getroffen organisaties, toezichthouders en instanties die expertise hebben op stalking, geweld en slachtofferbescherming.

4. Nazorg moet ook fysieke en sociale veiligheid omvatten

In het huidige systeem krijgen slachtoffers na een datalek vaak generieke adviezen: wijzig uw wachtwoord, wees alert op phishing, controleer uw accounts. Dat is nuttig, maar lang niet altijd voldoende.

De impact van een datalek is namelijk niet alleen digitaal. Voor bepaalde groepen is die ook sociaal, psychisch en fysiek.

Daarom moet nazorg veel serieuzer worden ingericht, met in elk geval:

- **gerichte ondersteuning** voor mensen met verhoogd veiligheidsrisico;

- **aandacht** voor afscherming, monitoring en praktische veiligheidsmaatregelen;
- **protocollen** voor situaties waarin gelekte gegevens kunnen leiden tot hernieuwd geweld, intimidatie of controle;
- **verkenning** van een laagdrempelige publieke voorziening of loket voor slachtoffers van ernstige datalekken.

5. Digitale veiligheid is een publieke waarde

Wij vinden dat de overheid scherper moet erkennen dat cyberveiligheid niet uitsluitend een verantwoordelijkheid is van individuele organisaties of burgers. Zeker waar het gaat om grootschalige verwerking van persoonsgegevens moet de bescherming van mensen centraal staan, niet alleen de continuïteit van systemen.

Daar hoort bij:

- stevigere **handhaving** op dataminimalisatie, bewaartermijnen en beveiliging;
- expliciete **aandacht** voor de gevolgen van datalekken voor vrouwen, lhbti+-personen en andere kwetsbare groepen;
- meer **normstelling** op veilige inrichting van gegevensverwerking;
- het uitgangspunt dat informatiebeveiliging ook een kwestie is van gelijke bescherming.

Want een systeem dat formeel voor iedereen hetzelfde werkt, maar in de praktijk de zwaarste gevolgen afwentelt op wie al kwetsbaar is, is geen rechtvaardig systeem.

Slot

De centrale vraag zou wat ons betreft niet alleen moeten zijn hoe we organisaties beter beschermen tegen cyberincidenten, maar ook:

wie betalen de prijs als die bescherming faalt?

Zolang organisaties datalekken vooral benaderen als technische of bestuurlijke incidenten, blijven de gevolgen voor de zwaarst getroffen groepen onderbelicht.

Digitale veiligheid is pas echte veiligheid als zij ook werkt voor mensen voor wie een datalek niet alleen vervelend is, maar ook gevaarlijk.

Een systeem is pas veilig als het ook veilig is voor mensen die het meeste risico lopen.

Digitale Dolle Mina's
Baas over eigen data