Hoe houd je de persoonsgegevens van jouw klanten veilig?

Nienke Kolthof – Coördinator Datalekken

Zizi Bouwmans – Senior Inspecteur



AP | bescherming in een digitale wereld

Wat gaan we bespreken?

1. **Wat zien we?**
   - Steeds meer datalekken
   - Cyberaanvallen bij leveranciers
2. **Een goede voorbereiding**
   - Inzicht in jouw leveranciers
   - Welke rollen hebben jij en jouw leverancier?
   - De basisbeveiliging op orde
   - In gesprek over beveiliging
   - De omvang vooraf beperken
   - Taakverdeling bij een datalek
   - Sterke verwerkersovereenkomst
3. **Een datalek, wat nu?**
   - Overzicht op de situatie & onderzoek
   - Melden aan de AP en slachtoffers
   - Passende maatregelen nemen

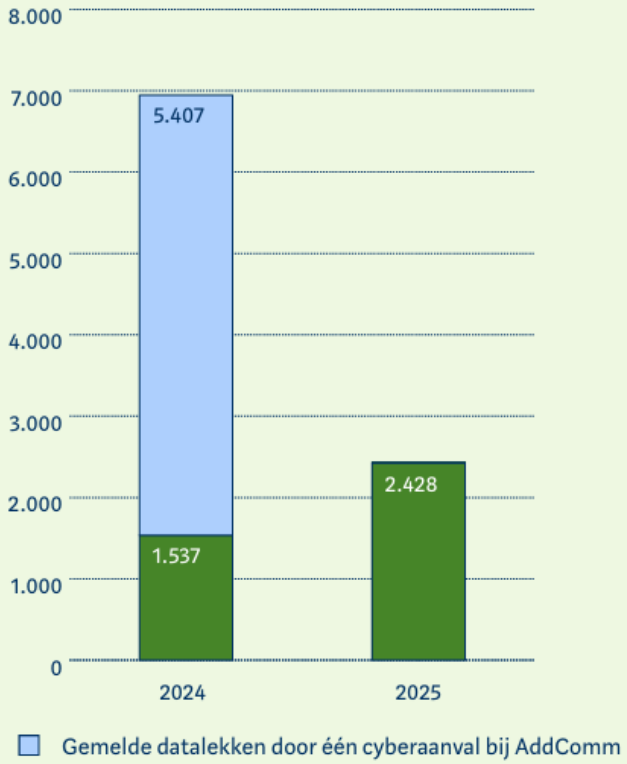

Wat zien we?

Steeds meer datalekken

- Stijgende lijn van datalekken en cyberaanvallen.
- Met de komst van AI zien we nieuwe datalekken en nieuwe risico’s.

- Een datalek is geen kwestie van ‘of’ maar ‘wanneer’.

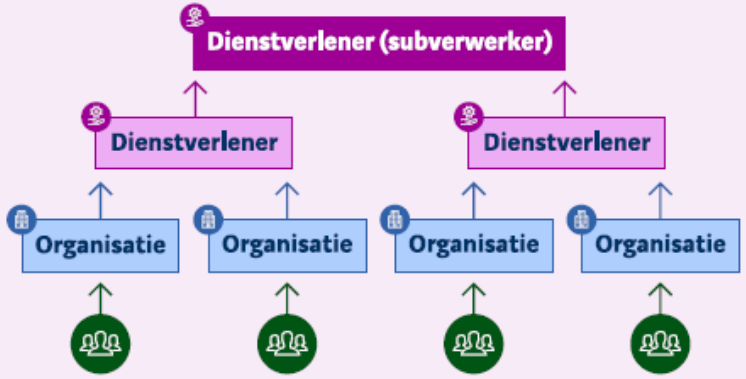
FIGUUR 4 | Datalekken door cyberaanvallen in 2024 en 2025



Cyberaanvallen bij leveranciers

- Leveranciers zijn een aantrekkelijk doelwit voor cybercriminelen: meerdere organisaties & veel persoonsgegevens.
- Een cyberaanval wordt dan al snel complex: wie moet wat wanneer doen?
- Informatie over de cyberaanval loopt stroef door de keten.

FIGUUR 2 | Overzicht leveranciersketen met subverwerker



Cyberaanvallen bij leveranciers

Gevolgen:

- Klanten van wie gegevens zijn gelekt worden niet, te laat of onvoldoende gewaarschuwd.
- Een organisatie kan zelf niet op tijd aanvullende beveiligingsmaatregelen nemen.
- Hoe kan je dit voor zijn?



NOS Nieuws • Dinsdag 5 april 2022, 19:24

Vertrouwelijke informatie gestolen bij aanval op woningcorporaties

Bij een digitale inbraak bij een ICT-dienstverlener van verschillende woningcorporaties is vertrouwelijke informatie gestolen. De aanval met ransomware (gijzelsoftware) kwam vorige week aan het licht en leidde tot veel overlast bij acht woningverhuurders. Zij kunnen nu niet in een deel van hun ICT-systemen en bij een deel van de gegevens.



Gegevens van NS-klanten op straat © ANP

Mogelijk miljoenen Nederlanders slachtoffer van datalek: 'Serverbedrijf hield informatie lang achter'



NOS Nieuws • Donderdag 25 maart 2021, 06:00

Datalek bij autobedrijven treft mogelijk miljoenen Nederlanders



Een goede voorbereiding

Inzicht in jouw leveranciers

Weet welke leveranciers jouw klantgegevens in handen hebben en wat ze daarmee doen:

- hoe
- hoelang
- waarvoor
- welke
- en van wie

worden persoonsgegevens verwerkt?

- Jouw leverancier kan ook leveranciers hebben ingeschakeld. Heb jij nog zicht op de gehele keten waar jouw klantgegevens doorheen gaan?

Welke rollen hebben jij en jouw leverancier?

- Spreek duidelijk af wie welke rol heeft en welke taken daaraan hangen:
  - **Verwerkingsverantwoordelijke**: bepaalt de doelen en middelen van de verwerking.
  - **Verwerker**: voert in opdracht van de verwerkingsverantwoordelijke de verwerking uit.

- Als verwerkingsverantwoordelijke blijf je verantwoordelijk voor de persoonsgegevens van jouw klanten, ook als je diensten uitbesteedt aan een leverancier of dienstverlener.

De basisbeveiliging op orde

Breng de risico's in kaart en stem beveiligingsmaatregelen hierop af. Belangrijke basismaatregelen zijn bijvoorbeeld:

- Meerfactorauthenticatie (MFA)
- Sterk wachtwoordbeleid
- Snel reageren op algemeen bekende kwetsbaarheden (CVEs)
- Netwerksegmentatie
- Goed monitoringssysteem om aanvallen en pogingen tot aanvallen te detecteren

In gesprek over beveiliging

Bespreek ook met jouw leveranciers welke maatregelen zij nemen en waarom. Denk in ieder geval aan:

- Back-ups: Hoe worden deze beheerd en getest?
- Updates: Hoe zorgt jouw leverancier voor tijdige updates?
- Wachtwoordbeleid: Welke richtlijnen gelden en is MFA ingesteld?
- Antivirus: Hoe voorkomt jouw leverancier dat computers besmet raken met virussen?

https://www.ncsc.nl/uitbesteden/bespreek-digitale-veiligheid-met-je-it-dienstverlener

De omvang vooraf beperken

Daarnaast kan je de omvang van een datalek vooraf al beperken:

- Dataminimalisatie: Welke gegevens heb je echt nodig om je werk te kunnen doen? En wat geldt voor jouw leverancier? Lever niet meer persoonsgegevens aan jouw leverancier dan dat de leverancier nodig heeft.
- Bewaartermijnen: Hoe lang heb je deze gegevens nodig? En maken de systemen het mogelijk om deze bewaartermijnen goed op te kunnen volgen? Kan jouw leverancier deze bewaartermijnen ook opvolgen? En controleer je dat als organisatie?

Taakverdeling bij een datalek

Maak concrete afspraken over de taakverdeling bij een datalek:

- Wie doet onderzoek naar het datalek?
- Bereikbaar contactpunt voor datalekken:
  - Een werknemer kan uit dienst gaan dus zorg het contactpunt up to date blijft.
  - Of gebruik een gezamenlijke mailbox die regelmatig wordt bekeken.
- Hoe snel informeert de leverancier je over een datalek en welke informatie heb je nodig?
  - Zo kort mogelijk, maar haalbaar.
  - Denk aan de informatie die je nodig hebt om te melden aan de AP en slachtoffers: aard van het datalek, de waarschijnlijke gevolgen, en de maatregelen om het datalek aan te pakken.
  - Spreek hierbij af dat de leverancier het ook moet melden als bepaalde informatie nog niet beschikbaar is.

Sterke verwerkersovereenkomst

- Deze afspraken leg je vast in de verwerkersovereenkomst die je met de leverancier afsluit.
- En het is belangrijk om die afspraken periodiek te herzien:
  - Heb je in de tussentijd meer diensten afgenomen van de leverancier?
  - Heeft de leverancier meer persoonsgegevens nodig dan initieel afgesproken?
  - Passen de afgesproken beveiligingsmaatregelen nog bij de huidige dreigingen?
  - Kloppen de vastgelegde contactpunten nog steeds?



Sterke verwerkersovereenkomst

- Verwerkersovereenkomsten krijgen vaak weinig prioriteit. Afspraken kunnen daardoor ontbreken, te vaag zijn of in de praktijk niet werken.
- Maar met goede afspraken kan je nu net verplichtingen binnen de leverancierskеten garanderen.

- Zorg ervoor dat medewerkers weten dat een verwerkersovereenkomst verplicht is, en welke afspraken belangrijk zijn voor jouw organisatie.
- En start niet met de verwerking voordat de verwerkersovereenkomst gesloten is. Hierdoor wordt nog onderhandelen over de afspraken lastiger.



Een datalek, wat nu?



Overzicht op de situatie & onderzoek

Zorg voor overzicht op de situatie & doe onderzoek

- Wat is er gebeurd? Wat is de oorzaak en is het datalek nog steeds gaande?
- Wat voor soort persoonsgegevens zijn mogelijk gelekt? En van wie? Probeer gelijk de maximale omvang van het datalek in te schatten. Welke gegevens en van hoeveel mensen waren terug te vinden in het getroffen systeem?
- Is er toegang geweest door iemand met kwade bedoelingen? Zijn er gegevens versleuteld, ingezien en/of gestolen?

Overzicht op de situatie & onderzoek

Factoren voor de risicobeoordeling:

- Het soort datalek
- Het soort persoonsgegevens: hoe gevoelig zijn de gegevens en om hoeveel gegevens gaat het?
- Het aantal slachtoffers
- Het gemak waarmee personen kunnen worden geïdentificeerd
- De ernst van de gevolgen voor slachtoffers
- Kenmerken van de ontvanger: is het bijv. iemand met kwaadwillende bedoelingen?
- Kenmerken van de persoon: gaat het bijv. om een kwetsbare groep?
- Kenmerken van uw organisatie

Melden aan de AP en slachtoffers

Het datalek melden aan de AP en slachtoffers

- Een datalek moet je binnen 72 uur melden bij de AP tenzij het **niet waarschijnlijk is dat het datalek een risico oplevert** voor mensen.
- Slachtoffers moeten snel geïnformeerd worden als het datalek **waarschijnlijk een hoog risico** voor hen oplevert.

Er zijn een paar uitzonderingen op het informeren van slachtoffers. Een daarvan geldt voor financiële ondernemingen die onder de Wet op het financieel toezicht (Wft) vallen.

https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/zo-meldt-u-een-datalek

https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/zo-informeert-u-slachtoffers-over-een-datalek

Passende maatregelen nemen

- Neem maatregelen om onmiddellijk het datalek te dichten en de schadelijke gevolgen te beperken
- En voorkom vergelijkbare incidenten
  - Is de basisbeveiliging nog steeds op orde? Zijn de maatregelen nog steeds afgestemd op de risico's?
  - Registreer het datalek in je datalekregister. Dit zorgt er ook voor dat je kan leren van eerdere datalekken en effectieve maatregelen kan nemen om de kans op nieuwe vergelijkbare datalekken te verminderen.

Conclusies



Datalekken komen veel voor. Ga ervan uit dat jij of jouw leverancier ooit geraakt zal worden door een groot datalek.



Krijg inzicht in jouw leveranciers en wat zij doen. Maak concrete afspraken over wie wat moet doen bij een datalek.



Zorg dat jij en jouw leverancier passende beveiligings-maatregelen nemen, afgestemd op de risico's die je ziet. Denk ook aan dataminimalisatie en bewaartermijnen.



Herzie de afspraken met jouw leverancier periodiek zodat ze blijven aansluiten op de praktijk.



Datalek bij jou of jouw leverancier? Doe onderzoek, neem passende maatregelen en beoordeel de risico's om te bepalen of het datalek gemeld moet worden aan de AP en slachtoffers.



AP | bescherming in een digitale wereld