SEGMENT

Datalek dichten en voorkomen

21 april 2017

Datalekken bij gemeenten; 'het is een beetje een zooitje'

Datalekken

Bijna tweederde van de gemeenten meldde vorig jaar een datalek van persoonlijke gegevens van burgers.

Liza van Lonkhuyzen 27 januari 2017

SEGMENT

Wat zijn datalekken?

SEGMENT

Wettelijke definitie

Wet Bescherming Persoonsgegevens:
“een inbreuk op de beveiliging,
als bedoeld in artikel 13 Wbp”
moet worden gemeld.

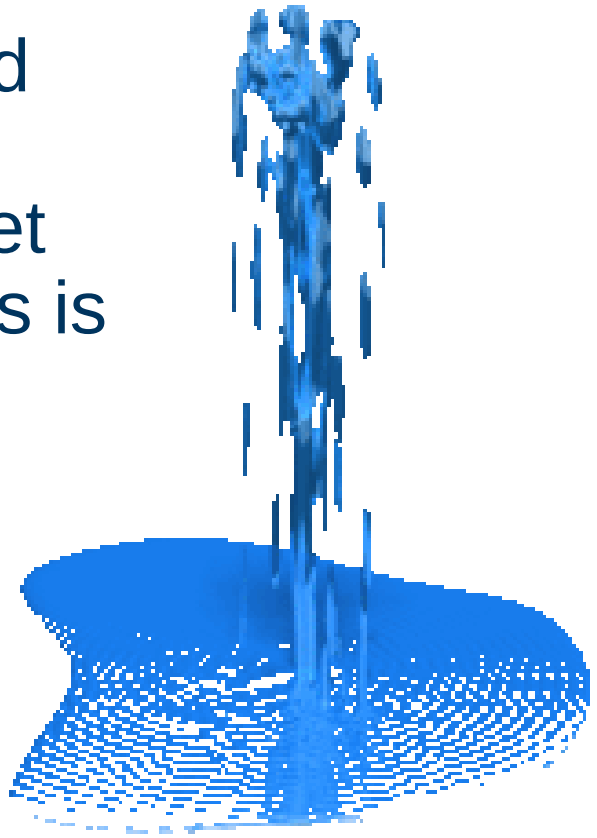
Artikel 13: persoonsgegevens moeten worden beveiligd tegen verlies of tegen enige vorm van onrechtmatige verwerking.

‘Datalek’ komt als term niet voor in de WBP.

SEGMENT

Inbreuk

Iedere situatie waarin persoonsgegevens zijn blootgesteld aan verlies of onrechtmatige verwerking, is een datalek, tenzij het hoogst onwaarschijnlijk is dat er iets is misgegaan.



SEGMENT

Soorten datalekken

Opzettelijk: bewust veroorzaakt

Voorbeelden:

- ✓Uitbuiten van kwetsbaarheden in systemen, webservers
- ✓Ontfutselen van vertrouwelijke gegevens
- ✓Diefstal van gegevensdragers
- ✓Enz…

SEGMENT

Soorten datalekken

Onopzettelijk: niet doelbewust veroorzaakt

Voorbeelden:

- ✓Verlies van niet-beveiligde informatiedragers
- ✓Verzenden van gegevens via onbeveiligde e-mail
- ✓Domme pech, bijv. crash van een harddisk
- ✓Enz…

SEGMENT

Oorzaken datalekken

- Menselijk falen: 25 %
- Technisch falen: 29 %
- **Moedwillig: 46 %**

Bron: Ponemon Institute 2015

SEGMENT

Ervaringen AP met meldingen

- Verkeerd verzonden e-mails
- Ransomware
- Onbeveiligde formulieren
- Onvoldoende vertrouwelijkheid binnen samenwerkingsverbanden

SEGMENT

Voorkomen van datalekken

Type strategieën:

- ✓ Vermijden (van gebruik persoonsgegevens in het proces)
- ✓ Beperken van nadelig effect (uitvoeren proces met minimum aan gegevens)
- ✓ Voorkomen (gegevens afschermen door goede authenticatie en autorisatie)
- ✓ Verhinderen (defense-in-depth, samenspel van maatregelen)
- ✓ Privacy by design (al bij het ontwikkelen van werkwijzen/systemen rekening houden met privacy)
- ✓ Gebruik van ISMS (borging beveiliging in processen)

SEGMENT

Transparante cultuur

- ✓Management heeft voorbeeldfunctie
- ✓iBewustzijn bij de medewerkers stimuleren
- ✓Glasheldere (communicatie over) procedures
- ✓Laat medewerkers weten wat van hen wordt verwacht in de relatie tot bescherming van persoonsgegevens
- ✓Bewustwording, opleiden, trainen en oefenen

SEGMENT

Beveiliging

- ✓Beperk de toegang tot persoonsgegevens (‘need to know’)
- ✓Houdt autorisaties actueel en voorkom te ruime toegangsrechten (‘least privilege’)
- ✓Beveiliging van werkplek en gegevensdragers
- ✓BYOD-beleid met passende maatregelen
- ✓Versleuteling van gegevens en beveiligde gegevensuitwisseling

SEGMENT

Organisatie en beleid

Beleid: het onderwerp datalekken moet verankerd worden in de beleidscyclus van de organisatie

Wie is er verantwoordelijk?
Zorg voor een bestuurlijke sponsor, bijv. een portefeuillehouder privacy & informatiebeveiliging

Wie coördineert?
De Functionaris Gegevensbescherming (FG)

Wie voert uit?
Het lijnmanagement is integraal verantwoordelijk voor de uitvoering van het eigen proces, dus ook voor de gegevensbescherming binnen dat proces

SEGMENT

Kernrollen

Bij ieder datalek zijn betrokken:

- ✓De **proceseigenaren** waar het datalek invloed op heeft;
- ✓De **Functionaris Gegevensberscherming**, advies en toezicht op omgang met meldplicht
- ✓De **CISO**, met onderzoeks- en adviesrol
- ✓Het **ICT-management**, voor onderzoek beveiligingsincident en herstel van de ICT

Overige rollen

- ✓- Juridische zaken (aansprakelijkheidsbepaling);
- ✓- Financiën (welke verzekering is gewenst);
- ✓- Communicatie (voorkomen reputatieschade);
- ✓- KCC (vroegtijdige transparantie);
- ✓- Bewerker;
- ✓- Afhankelijk van situatie mogelijk anderen betrekken

SEGMENT

Help, een datalek

Beoordeel het signaal: wat is er aan de hand, welke acties zijn nodig?

- Bestrijden ICT-incident
- Is er sprake van een datalek? Meld- en herstelproces opstarten
- Proceseigenaar informeren

FG, CISO en proceseigenaar vormen het datalekteam

SEGMENT

Eerste beeldvorming

Waar heeft het datalek plaatsgevonden?

Binnen/buiten de organisatie, welke systemen zijn betrokken, is sprake van verlies/diefstal van fysieke gegevensdragers?

Om wat voor data gaat het?

Persoonsgegevens, welke, hoeveel, gevoeligheid

Wat is de oorzaak?

Verkeerde verstrekking, verlies, misbruik van autorisatie

Lekt het nog?

Is er nog steeds sprake van een datalek?

Registreer het incident

Lessons learned voor toekomstige situaties

SEGMENT

Geen paniek

SEGMENT

Beperken van het incident

Insluitende en schade beperkende maatregelen

- Beheerst uitschakelen van het systeem
- Loskoppelen van het computernetwerk
- Aanpassen firewall
- Blokkeren bepaalde gebruikersaccounts
- Wijzigen wachtwoorden
- Bewijsmateriaal veiligstellen
- Overleg met ICT hoe het datalek te stoppen

SEGMENT

Bepalen van de impact

Beveiligingsincident ≠ datalek,

datalek = beveiligingsincident.

Welke gegevens zijn gelekt?

Minimaal gegevens verzamelen die benodigd zijn om melding aan AP te doen (zie Richtsnoeren AP)

Wat is de impact van het lek op de betrokken personen?

Lekken van gevoelige gegevens moet ook gemeld worden aan de persoon zelf

Wat is de impact op de organisatie?

Werkwijze aanpassen, inschatten van de kosten

SEGMENT

Bepalen meldaanpak en herstelaanpak

Meldaanpak:

Moet er gemeld worden? Zo ja, aan wie? Welke gegevens zijn daarvoor nodig? Hoe worden betrokkenen geïnformeerd, langs welke kanalen?

Herstelaanpak:

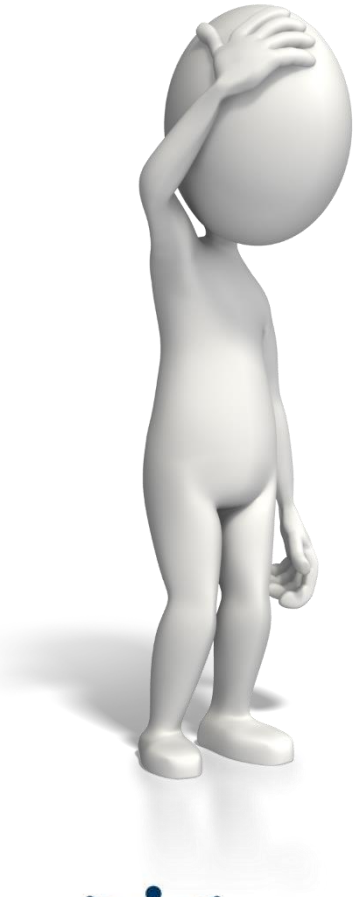
Gericht verbeteren informatiebeveiliging

Nazorg aan betrokkenen

Borging van het organisatiebelang (herstel verloren gegevens, voorkomen reputatieschade)

SEGMENT

Moet je het datalek melden?



Melden van een datalek hoeft alleen als er een *aanzienlijke kans* is dat het datalek *ernstige* nadelige gevolgen heeft voor de bescherming van persoonsgegevens:

- ✓ Zijn er gevoelige persoonsgegevens gelekt (bijv. BSN)?
- ✓ Heeft het datalek (waarschijnlijk) nadelige gevolgen voor de betrokkenen?

In beide gevallen melden bij de AP.

SEGMENT

Herstel

Doel van de herstelfase:

- Verbeteren van de beveiliging van persoonsgegevens (voorkomen herhaling van het datalek);
- Leveren van nazorg aan de betrokkenen
- Opkomen voor het organisatiebelang

SEGMENT

Verbeteren van de beveiliging

Onderzoek de beveiliging

Voldoet de beveiliging aan de normen (wettelijk, organisatie, eigen acceptatie)?

Kunnen er verbetermaatregelen worden doorgevoerd?

SEGMENT

Nazorg aan betrokkenen

Doel is schade bij betrokkenen te beperken of te herstellen

Laat weten waar ze terecht kunnen voor nadere informatie of ondersteuning (Contactpunt voor nazorg).

Welke maatregelen kunnen betrokkenen zelf nemen om nadelige gevolgen van het datalek te beperken? Bijvoorbeeld het wijzigen van inloggegevens.

SEGMENT

Opkomen voor het organisatiebelang

Doel is het beperken van de impact van het datalek op de eigen organisatie

Risicomanagement op orde?

Voorbereiden op schadeclaims en boetes

Verhalen van schade bij bewerker

Disciplinaire maatregelen bij datalek door eigen medewerker

Afhandeling van verzekeraar

Bedrijfscontinuiteitsplan in werking stellen

Herstel van vertrouwen

SEGMENT

Registreer, evalueer en verbeter

- Startpunt is goede incidentenregistratie
- Vastleggen hoe de behandeling van het datalek is uitgevoerd
- Evalueer het datalek, individueel of in teamverband
- Verbeter de maatregelen om datalekrisico’s beter te beheersen
- Controleer de aanpak op actualiteit

SEGMENT

Vragen?

SEGMENT