

Richtsnoeren



Richtsnoeren 01/2021

over voorbeelden betreffende de melding van inbreuken in verband met persoonsgegevens

Vastgesteld op 14 december 2021

Versie 2.0

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Versiegeschiedenis

Versie 2.0	14 december 2021	Vaststelling van de richtsnoeren na openbare raadpleging
Versie 1.0	14 januari 2021	Vaststelling van de richtsnoeren voor openbare raadpleging

Inhoudsopgave

1	INLEIDING	5
2	RANSOMWARE	8
2.1	GEVAL nr. 1: Ransomware met een goede back-up en zonder exfiltratie	9
2.1.1	GEVAL nr. 1 — Voorafgaande maatregelen en risicobeoordeling	9
2.1.2	GEVAL nr. 1 — Risicobeperking en verplichtingen	10
2.2	GEVAL nr. 2: Ransomware zonder een goede back-up	11
2.2.1	GEVAL nr. 2 — Voorafgaande maatregelen en risicobeoordeling	11
2.2.2	GEVAL nr. 2 — Risicobeperking en verplichtingen	12
2.3	GEVAL nr. 3: Ransomware met back-up en zonder exfiltratie in een ziekenhuis	13
2.3.1	GEVAL nr. 3 — Voorafgaande maatregelen en risicobeoordeling	13
2.3.2	GEVAL nr. 3 — Risicobeperking en verplichtingen	14
2.4	GEVAL nr. 4: Ransomware zonder back-up en met exfiltratie	14
2.4.1	GEVAL nr. 4 — Voorafgaande maatregelen en risicobeoordeling	15
2.4.2	GEVAL nr. 4 — Risicobeperking en verplichtingen	15
2.5	Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van aanvallen met ransomware	16
3	AANVALLEN MET GEGEVENSEXFILTRATIE	17
3.1	GEVAL nr. 5: Exfiltratie van sollicitatiegegevens van een website	17
3.1.1	GEVAL nr. 5 — Voorafgaande maatregelen en risicobeoordeling	17
3.1.2	GEVAL nr. 5 — Risicobeperking en verplichtingen	18
3.2	GEVAL nr. 6: Exfiltratie van gehasht wachtwoord van een website	19
3.2.1	GEVAL nr. 6 — Voorafgaande maatregelen en risicobeoordeling	19
3.2.2	GEVAL nr. 6 — Risicobeperking en verplichtingen	19
3.3	GEVAL nr. 7: Credential stuffing-aanval op een bankwebsite	20
3.3.1	GEVAL nr. 7 — Voorafgaande maatregelen en risicobeoordeling	20
3.3.2	GEVAL nr. 7 — Risicobeperking en verplichtingen	21
3.4	Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van aanvallen door hackers	21
4	INTERNE BRON VAN MENSELIJK RISICO	22
4.1	GEVAL nr. 8: Exfiltratie van bedrijfsgegevens door een werknemer	22
4.1.1	GEVAL nr. 8 — Voorafgaande maatregelen en risicobeoordeling	23
4.1.2	GEVAL nr. 8 — Risicobeperking en verplichtingen	23
4.2	GEVAL nr. 9: Onbedoelde doorgifte van gegevens aan een betrouwbare derde	25
4.2.1	GEVAL nr. 9 — Voorafgaande maatregelen en risicobeoordeling	25
4.2.2	GEVAL nr. 9 — Risicobeperking en verplichtingen	25

4.3	Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van interne bronnen van menselijke risico's	26
5	VERLOREN OF GESTOLEN APPARATEN EN PAPIEREN DOCUMENTEN	27
5.1	GEVAL nr. 10: Gestolen materiaal met versleutelde persoonsgegevens	27
5.1.1	GEVAL nr. 10 — Voorafgaande maatregelen en risicobeoordeling	27
5.1.2	GEVAL nr. 10 — Risicobeperking en verplichtingen	28
5.2	GEVAL nr. 11: Gestolen materiaal met niet-versleutelde persoonsgegevens	28
5.2.1	GEVAL nr. 11 — Voorafgaande maatregelen en risicobeoordeling	28
5.2.2	GEVAL nr. 11 — Risicobeperking en verplichtingen	29
5.3	GEVAL nr. 12: Gestolen papieren dossiers met gevoelige gegevens	29
5.3.1	GEVAL nr. 12 — Voorafgaande maatregelen en risicobeoordeling	29
5.3.2	GEVAL nr. 12 — Risicobeperking en verplichtingen	29
5.4	Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van verlies of diefstal van apparaten	30
6	VERKEERDE ADRESSERING 31	
6.1	GEVAL nr. 13: Fout bij bezorging per post	31
6.1.1	GEVAL nr. 13 — Voorafgaande maatregelen en risicobeoordeling	31
6.1.2	GEVAL nr. 13 — Risicobeperking en verplichtingen	31
6.2	GEVAL nr. 14: Bij vergissing per e-mail verzonden zeer vertrouwelijke persoonsgegevens	31
6.2.1	GEVAL nr. 14 — Voorafgaande maatregelen en risicobeoordeling	31
6.2.2	GEVAL nr. 14 — Risicobeperking en verplichtingen	32
6.3	GEVAL nr. 15: Bij vergissing per e-mail verzonden persoonsgegevens	32
6.3.1	GEVAL nr. 15 — Voorafgaande maatregelen en risicobeoordeling	32
6.3.2	GEVAL nr. 15 — Risicobeperking en verplichtingen	33
6.4	GEVAL nr. 16: Fout bij bezorging per post	33
6.4.1	GEVAL nr. 16 — Voorafgaande maatregelen en risicobeoordeling	33
6.4.2	GEVAL nr. 16 — Risicobeperking en verplichtingen	33
6.5	Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van verkeerde adressering	34
7	Andere gevallen — Social engineering	35
7.1	GEVAL nr. 17: Identiteitsdiefstal	35
7.1.1	GEVAL nr. 17 — Risicobeoordeling, risicobeperking en verplichtingen	35
7.2	GEVAL nr. 18: Exfiltratie van e-mail	36
7.2.1	GEVAL nr. 18 — Risicobeoordeling, risicobeperking en verplichtingen	36

HET EUROPEES COMITÉ VOOR GEGEVENSBESCHERMING

Gezien artikel 70, lid 1, punt e), van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna “AVG” genoemd),

Gezien de EER-Overeenkomst, en met name bijlage XI en Protocol 37 bij die overeenkomst, als gewijzigd bij Besluit nr. 154/2018 van het Gemengd Comité van de EER van 6 juli 2018¹,

Gezien de artikelen 12 en 22 van zijn reglement van orde,

Gezien de mededeling van de Commissie aan het Europees Parlement en de Raad getiteld Gegevensbescherming als pijler van zeggenschap van de burger en de EU-aanpak van de digitale transformatie — twee jaar toepassing van de algemene verordening gegevensbescherming²,

HEEFT DE VOLGENDE RICHTSNOEREN VASTGESTELD

1 INLEIDING

1. Met de AVG wordt in bepaalde gevallen de verplichting ingevoerd om een inbreuk in verband met persoonsgegevens te melden aan de bevoegde nationale toezichhoudende autoriteit (hierna “TA” genoemd) en om de inbreuk mee te delen aan de personen op wier persoonsgegevens de inbreuk betrekking heeft (artikelen 33 en 34).
2. De Groep gegevensbescherming artikel 29 (WP29) heeft in oktober 2017 reeds *algemene* richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens opgesteld, waarin de desbetreffende onderdelen van de AVG worden geanalyseerd (Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679, WP 250) (hierna “Richtsnoeren WP 250” genoemd)³. Door de aard en het tijdstip ervan wordt in deze richtsnoeren echter niet aan alle praktische kwesties voldoende aandacht besteed. Daarom is er behoefte ontstaan aan *praktijkgerichte, op concrete zaken gebaseerde* richtsnoeren waarbij gebruik wordt gemaakt van de ervaringen die de TA’s hebben opgedaan sinds de AVG van toepassing is.
3. Dit document is bedoeld als aanvulling op de Richtsnoeren WP 250 en weerspiegelt de gemeenschappelijke ervaringen van de TA’s in de EER sinds de AVG van toepassing werd. Het doel ervan is verwerkingsverantwoordelijken te helpen om te bepalen hoe gegevensinbreuken moeten worden afgehandeld en welke factoren bij de risicobeoordeling in aanmerking moeten worden genomen.

¹ Verwijzingen naar “lidstaten” in dit document moeten worden gelezen als verwijzingen naar “lidstaten van de EER”.

² COM(2020) 264 final, 24 juni 2020.

³ G29 WP 250 rev.1, 6 februari 2018, Richtsnoeren voor de melding van inbreuken in verband met persoonsgegevens krachtens Verordening 2016/679 — bekrachtigd door de EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

4. Een verwerkingsverantwoordelijke en een verwerker kunnen pas een poging ondernemen om een inbreuk aan te pakken als zij in staat zijn er een te herkennen. In artikel 4, lid 12, AVG wordt een “inbreuk in verband met persoonsgegevens” gedefinieerd als “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgestuurde, opgeslagen of anderszins verwerkte gegevens”.
5. In zijn Advies 03/2014 betreffende de melding van inbreuken⁴ en in zijn Richtsnoeren WP 250 heeft de WP29 uitgelegd dat inbreuken kunnen worden ingedeeld volgens de volgende drie welbekende informatiebeveiligingsprincipes:
- ⌋ “vertrouwelijkheidsinbreuk” — als er sprake is van ongeoorloofde of onopzettelijke verstrekking van of toegang tot persoonsgegevens;
 - ⌋ “integriteitsinbreuk” — als er sprake is van een ongeoorloofde of onopzettelijke wijziging van persoonsgegevens;
 - ⌋ “beschikbaarheidsinbreuk” — als er sprake is van een onopzettelijk of ongeoorloofd verlies van toegang tot persoonsgegevens of een onopzettelijke of ongeoorloofde vernietiging van persoonsgegevens⁵.
6. Een inbreuk kan diverse aanzienlijke negatieve gevolgen voor personen hebben, wat kan leiden tot lichamelijke, materiële of immateriële schade. In de AVG wordt uitgelegd dat dit onder meer het volgende kan inhouden: verlies van controle over hun persoonsgegevens, de beperking van hun rechten, discriminatie, identiteitsdiefstal of -fraude, financiële verliezen, ongeoorloofde ongedaanmaking van pseudonimisering, reputatieschade, verlies van vertrouwelijkheid van door het beroepsgeheim beschermde persoonsgegevens, of enig ander aanzienlijk economisch of maatschappelijk nadeel voor de personen in kwestie. Een van de belangrijkste verplichtingen van de verwerkingsverantwoordelijke is om deze risico’s voor de rechten en vrijheden van betrokkenen te evalueren en om passende technische en organisatorische maatregelen te nemen om de risico’s aan te pakken.
7. De AVG bepaalt derhalve dat de verwerkingsverantwoordelijke:
- ⌋ alle inbreuken in verband met persoonsgegevens moet documenteren, met inbegrip van de feiten omtrent de inbreuk in verband met persoonsgegevens, de gevolgen daarvan en de genomen corrigerende maatregelen⁶;
 - ⌋ de inbreuk in verband met persoonsgegevens moet melden aan de toezichthoudende autoriteit, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen⁷;
 - ⌋ de inbreuk in verband met persoonsgegevens aan de betrokkene moet medelen wanneer de inbreuk in verband met persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen⁸.
8. Inbreuken op de gegevensbescherming vormen een probleem op zich, maar kunnen ook symptomen zijn van een kwetsbaar, mogelijk verouderd gegevensbeveiligingssysteem. Bovendien kunnen deze inbreuken duiden op zwakke plekken in het systeem, die moeten worden aangepakt. In het algemeen is het altijd

⁴ G29 WP 213, 25 maart 2014, Advies 03/2014 over kennisgeving bij inbreuken in verband met persoonsgegevens, blz. 5, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_nl.pdf

⁵ Zie Richtsnoeren WP 250, blz. 7. — Er moet rekening mee worden gehouden dat een gegevensinbreuk betrekking kan hebben op één categorie of op meerdere categorieën tegelijk of een combinatie daarvan.

⁶ Artikel 33, lid 5, AVG.

⁷ Artikel 33, lid 1, AVG.

⁸ Artikel 34, lid 1, AVG.

beter om gegevensinbreuken te voorkomen door erop voorbereid te zijn, aangezien verschillende gevolgen ervan naar hun aard onomkeerbaar zijn. Voordat een verwerkingsverantwoordelijke het risico in verband met een inbreuk als gevolg van een aanval *volledig* kan beoordelen, moet de onderliggende oorzaak van het probleem worden vastgesteld om te achterhalen of de zwakke plekken die tot het incident hebben geleid nog aanwezig zijn en daardoor nog kunnen worden uitgebuit. De verwerkingsverantwoordelijke kan in veel gevallen vaststellen dat het incident waarschijnlijk een risico inhoudt en daarom moet worden gemeld. In andere gevallen hoeft de melding niet te worden uitgesteld totdat het risico en het effect van de inbreuk volledig zijn beoordeeld, aangezien de volledige risicobeoordeling tegelijk met de melding kan plaatsvinden en de bij de beoordeling verkregen informatie zonder onredelijke vertraging in stappen aan de TA kan worden verstrekt⁹.

9. De inbreuk moet worden gemeld wanneer de verwerkingsverantwoordelijke van mening is dat deze waarschijnlijk een risico inhoudt voor de rechten en vrijheden van de betrokkene. Verwerkingsverantwoordelijken moeten deze beoordeling uitvoeren op het moment waarop zij kennis krijgen van de inbreuk. De verwerkingsverantwoordelijke mag niet wachten op een gedetailleerd forensisch onderzoek en (vroegtijdige) risicobeperkende maatregelen alvorens te beoordelen of de gegevensinbreuk waarschijnlijk een risico inhoudt en dus moet worden gemeld.
10. Indien een verwerkingsverantwoordelijke zelf vaststelt dat het risico onwaarschijnlijk is, maar het risico zich wel blijkt voor te doen, kan de bevoegde TA haar corrigerende bevoegdheden gebruiken en besluiten om sancties op te leggen.
11. Elke verwerkingsverantwoordelijke en elke verwerker moet beschikken over plannen en procedures voor de afhandeling van eventuele gegevensinbreuken. Organisaties moeten duidelijke rapportagelijnen hebben en moeten beschikken over personen die verantwoordelijk zijn voor bepaalde aspecten van het herstelproces.
12. Opleiding en bewustmaking van het personeel van de verwerkingsverantwoordelijke en de verwerker over kwesties op het gebied van gegevensbescherming met een focus op het beheer van inbreuken in verband met persoonsgegevens (vaststelling van een incident in verband met een inbreuk op persoonsgegevens en verdere te nemen maatregelen enz.) is ook van essentieel belang voor de verwerkingsverantwoordelijken en de verwerkers. Deze opleiding moet regelmatig worden herhaald, afhankelijk van het soort verwerkingsactiviteit en de omvang van de verwerkingsverantwoordelijke, en daarbij moet aandacht worden besteed aan de laatste trends en waarschuwingen in verband met cyberaanvallen of andere beveiligingsincidenten.
13. Het beginsel van verantwoordingsplicht en het begrip gegevensbescherming door ontwerp kunnen een analyse omvatten die wordt verwerkt in het eigen "Handboek voor de afhandeling van inbreuken in verband met persoonsgegevens" van een verwerkingsverantwoordelijke en een gegevensverwerker, dat tot doel heeft om in elke belangrijke stap van de verwerking voor elk aspect daarvan feiten vast te stellen. Een dergelijk handboek dat vooraf is opgesteld, zou voor verwerkingsverantwoordelijken en gegevensverwerkers een veel snellere informatiebron zijn om zonder onredelijke vertraging de risico's te beperken en aan de verplichtingen te voldoen. Dit zou ervoor zorgen dat in het geval van een inbreuk in verband met persoonsgegevens de mensen in de organisatie zouden weten wat ze moeten doen en dat het incident hoogstwaarschijnlijk sneller zou worden afgehandeld dan zonder risicobeperkende maatregelen of plan.

⁹ Artikel 33, lid 4, AVG.

14. Hoewel de hieronder vermelde gevallen fictief zijn, zijn ze gebaseerd op typische gevallen uit de collectieve ervaring van de TA met meldingen van inbreuken in verband met persoonsgegevens. De beschreven analyses hebben uitdrukkelijk betrekking op de onderzochte gevallen, maar met het doel om verwerkingsverantwoordelijken te helpen bij de beoordeling van hun eigen gegevensinbreuken. Elke wijziging in de omstandigheden van de hieronder beschreven gevallen kan leiden tot andere of grotere risico's, waardoor er dus andere of aanvullende maatregelen nodig zijn. In deze richtsnoeren worden de gevallen gestructureerd volgens bepaalde categorieën van inbreuken (bv. aanvallen met ransomware). Bij de afhandeling van een bepaalde categorie van inbreuken is er in elk van de gevallen behoefte aan bepaalde risicobeperkende maatregelen. Deze maatregelen worden niet noodzakelijkerwijs herhaald bij elke analyse van gevallen die tot dezelfde categorie van inbreuken behoren. Bij tot dezelfde categorie behorende gevallen worden alleen de verschillen aangegeven. Daarom moet de lezer alle gevallen lezen die relevant zijn voor de desbetreffende categorie van een inbreuk om alle te nemen correcte maatregelen te kunnen vaststellen en onderscheiden.
15. De interne documentatie van een inbreuk is een verplichting die losstaat van de risico's met betrekking tot de inbreuk en moet in elk van de gevallen worden uitgevoerd. Met de hieronder vermelde gevallen wordt getracht enig licht te werpen op de vraag of de inbreuk al dan niet aan de TA moet worden gemeld en aan de getroffen betrokkenen moet worden meegedeeld.

2 RANSOMWARE

16. Een veel voorkomende reden voor een melding van een inbreuk in verband met persoonsgegevens is een aanval met ransomware waarvan de verwerkingsverantwoordelijke het slachtoffer is geworden. In deze gevallen worden de persoonsgegevens met een kwaadaardige code versleuteld en vraagt de aanvaller de verwerkingsverantwoordelijke vervolgens om losgeld in ruil voor de decoderingscode. Dit soort aanvallen kan doorgaans worden geclassificeerd als een inbreuk op de beschikbaarheid, maar vaak kan het daarbij ook gaan om een inbreuk op de vertrouwelijkheid.

2.1 GEVAL nr. 1: Ransomware met een goede back-up en zonder exfiltratie

De computersystemen van een klein productiebedrijf werden blootgesteld aan een aanval met ransomware en de in die systemen opgeslagen gegevens werden versleuteld. De verwerkingsverantwoordelijke maakte gebruik van versleuteling in rust, waardoor alle gegevens waartoe de ransomware toegang had, waren opgeslagen in een met behulp van een geavanceerd versleutelingsalgoritme versleutelde vorm. De decoderings sleutel werd bij de aanval niet gekraakt, dat wil zeggen dat de aanvaller geen toegang tot de sleutel had en deze ook niet indirect kon gebruiken. De aanvaller had derhalve alleen toegang tot versleutelde persoonsgegevens. Met name werden noch het e-mailsysteem van het bedrijf, noch de cliëntsystemen voor toegang tot de e-mail getroffen. Het bedrijf maakt gebruik van de expertise van een extern cyberbeveiligingsbedrijf om het incident te onderzoeken. Er zijn logbestanden beschikbaar waarin alle gegevensstromen worden geregistreerd die het bedrijf verlaten (waaronder uitgaande e-mail). Nadat de logboeken en de door de detectiesystemen van het bedrijf verzamelde gegevens waren geanalyseerd, werd bij een door het externe cyberbeveiligingsbedrijf ondersteund intern onderzoek *met zekerheid* vastgesteld dat de dader alleen gegevens had versleuteld, zonder deze te exfiltreren. De logboeken laten geen uitgaande gegevensstroom tijdens de aanval zien. De door de inbreuk getroffen persoonsgegevens hebben betrekking op klanten en werknemers van het bedrijf, in totaal enkele tientallen personen. Er was direct een back-up beschikbaar en de gegevens waren een paar uur na de aanval hersteld. De inbreuk had geen gevolgen voor de dagelijkse activiteiten van de verwerkingsverantwoordelijke. Er was geen vertraging in de betalingen aan het personeel of de afhandeling van aanvragen van klanten.

17. In dit geval werden de volgende elementen van de definitie van een “inbreuk in verband met persoonsgegevens” gerealiseerd: een inbreuk op de beveiliging heeft geleid tot onrechtmatige wijziging van en ongeoorloofde toegang tot opgeslagen persoonsgegevens.

2.1.1 GEVAL nr. 1 — Voorafgaande maatregelen en risicobeoordeling

18. Net als bij alle risico's in verband met externe actoren kan de kans dat een aanval met ransomware slaagt, drastisch worden verminderd door de beveiliging van de omgeving voor gegevensbeheer aan te scherpen. Het merendeel van deze inbreuken kan worden voorkomen door ervoor te zorgen dat er passende organisatorische, fysieke en technologische beveiligingsmaatregelen zijn genomen. Voorbeelden van dergelijke maatregelen zijn een goed patchbeheer en het gebruik van een adequaat malware detectiesysteem. Een goede en aparte back-up zal de gevolgen van een eventuele geslaagde aanval helpen beperken. Bovendien zal een programma voor onderwijs, opleiding en bewustmaking van werknemers op het gebied van beveiliging (SETA) helpen om dit soort aanvallen te voorkomen en te herkennen. (Een lijst van aanbevolen maatregelen is te vinden in punt 2.5.) Een van de belangrijkste maatregelen is een goed patchbeheer dat ervoor zorgt dat de systemen up-to-date zijn en dat alle bekende kwetsbaarheden van de toegepaste systemen worden verholpen, aangezien de meeste aanvallen met ransomware op welbekende kwetsbaarheden zijn gericht.
19. Bij de beoordeling van de risico's moet de verwerkingsverantwoordelijke de inbreuk onderzoeken en het soort kwaadaardige code vaststellen om inzicht te krijgen in de mogelijke gevolgen van de aanval. Een van de risico's waarmee rekening moet worden gehouden, is het risico dat er gegevens zijn geëxfiltreerd zonder een spoor achter te laten in de logboeken van de systemen.
20. In dit voorbeeld had de aanvaller toegang tot persoonsgegevens en werd de vertrouwelijkheid van de cijfertekst met persoonsgegevens in versleutelde vorm gecompromitteerd. Gegevens die zijn geëxfiltreerd, kunnen door de dader echter niet worden gelezen of gebruikt, tenminste voorlopig niet. De door de verwerkingsverantwoordelijke gebruikte versleutelingsmethode is in overeenstemming met de stand van de techniek. De decoderings sleutel werd niet gekraakt en kon vermoedelijk ook niet met andere middelen

worden vastgesteld. Bijgevolg worden de vertrouwelijkheidsrisico's voor de rechten en vrijheden van natuurlijke personen tot een minimum beperkt, behoudens vooruitgang in cryptoanalyse waardoor de versleutelde gegevens in de toekomst leesbaar worden.

21. De verwerkingsverantwoordelijke moet rekening houden met het risico dat personen lopen als gevolg van de inbreuk¹⁰. In dit geval lijken de risico's voor de rechten en vrijheden van betrokkenen voort te vloeien uit het niet beschikbaar zijn van de persoonsgegevens en is de vertrouwelijkheid van de persoonsgegevens niet gecompromitteerd¹¹. In dit voorbeeld werden de negatieve gevolgen van de inbreuk vrij snel na de inbreuk beperkt. Met een goed back-upbeleid¹² zijn de gevolgen van de inbreuk minder ernstig en in dit geval kon de verwerkingsverantwoordelijke er effectief gebruik van maken.
 22. Wat betreft de ernst van de consequenties voor de betrokkenen konden er slechts geringe gevolgen worden vastgesteld, aangezien de getroffen gegevens binnen enkele uren werden hersteld, de inbreuk geen consequenties had voor de dagelijkse activiteiten van de verwerkingsverantwoordelijke en er geen significante gevolgen voor de betrokkenen uit voortvloeiden (bv. betalingen aan het personeel of de afhandeling van aanvragen van klanten).
- 2.1.2 GEVAL nr. 1 — Risicobeperking en verplichtingen
23. Zonder een back-up kan de verwerkingsverantwoordelijke weinig maatregelen nemen om het verlies van persoonsgegevens te herstellen en moeten de gegevens opnieuw worden verzameld. In dit specifieke geval kunnen de gevolgen van de aanval echter effectief worden beperkt door alle gecompromitteerde systemen te resetten naar een schone staat waarvan bekend is dat deze vrij is van kwaadaardige code, door de kwetsbaarheden te verhelpen en door de getroffen gegevens kort na de aanval te herstellen. Zonder back-up gaan er gegevens verloren en kan de ernst toenemen omdat de risico's of gevolgen voor personen ook kunnen toenemen.
 24. De tijdigheid van een effectief gegevensherstel vanaf de onmiddellijk beschikbare back-up is een belangrijke variabele bij het analyseren van de inbreuk. Het vaststellen van een passend tijdsbestek voor het herstel

¹⁰ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” de Richtsnoeren van de Groep gegevensbescherming artikel 29 voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking “waarschijnlijk een hoog risico inhoudt” in de zin van Verordening 2016/679, WP 248 rev.01, — bekrachtigd door de EDPB, <https://ec.europa.eu/newsroom/article29/items/611236>, blz. 9.

¹¹ Technisch gezien vereist de versleuteling van gegevens dat er “toegang” wordt verkregen tot de oorspronkelijke gegevens en in het geval van ransomware dat het origineel wordt verwijderd — de ransomwarecode moet toegang hebben tot de gegevens om deze te versleutelen en om de oorspronkelijke gegevens te verwijderen. Een aanvaller kan een kopie van het origineel maken alvorens dit te verwijderen, maar er worden niet altijd persoonsgegevens geëxtraheerd. Naarmate het onderzoek van een verwerkingsverantwoordelijke vordert, kan er nieuwe informatie aan het licht komen op grond waarvan deze beoordeling verandert. Toegang die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking van de persoonsgegevens of tot een beveiligingsrisico voor een betrokkene kan zelfs zonder interpretatie van de gegevens even ernstig zijn als toegang met interpretatie van de persoonsgegevens.

¹² Back-upprocedures moeten gestructureerd, samenhangend en herhaalbaar zijn. Voorbeelden van back-upprocedures zijn de 3-2-1- methode en de grootvader-vader-zoon-methode. Elke methode moet altijd op effectiviteit worden getest wat de dekking betreft en wanneer er gegevens moeten worden hersteld. De test moet ook regelmatig worden herhaald, met name in het geval van wijzigingen in de verwerking of in de omstandigheden van de verwerking, om de integriteit van het systeem te waarborgen.

van de gecompromitteerde gegevens is afhankelijk van de unieke omstandigheden van de inbreuk in kwestie. De AVG bepaalt dat een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging en, indien mogelijk, binnen 72 uur moet worden gemeld. Daarom kan worden vastgesteld dat overschrijding van de termijn van 72 uur in elk geval niet raadzaam is, maar als het gaat om gevallen met een hoog risiconiveau kan zelfs de naleving van deze termijn als onbevredigend worden beschouwd.

25. In dit geval stelde de verwerkingsverantwoordelijke na een gedetailleerde effectbeoordeling en incidentrespons vast dat het niet waarschijnlijk was dat de inbreuk een risico zou inhouden voor de rechten en vrijheden van natuurlijke personen, waardoor een mededeling aan de betrokkenen niet nodig is en de inbreuk evenmin aan de TA moet worden gemeld. Net als alle gegevensinbreuken moet de inbreuk echter worden gedocumenteerd overeenkomstig artikel 33, lid 5. De organisatie kan ook genoodzaakt zijn (of later door de TA worden verplicht) om haar organisatorische en technische maatregelen en procedures ter beveiliging van de persoonsgegevens en ter beperking van de risico's te actualiseren en te herstellen. In het kader van deze actualisering en herstelmaatregelen moet de organisatie de inbreuk grondig onderzoeken en de oorzaken en de door de dader gebruikte methoden vaststellen om soortgelijke gebeurtenissen in de toekomst te voorkomen.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	X	X

2.2 GEVAL nr. 2: Ransomware zonder een goede back-up

Een van de computers van een landbouwbedrijf werd blootgesteld aan een aanval met ransomware en daarbij werden de gegevens door de aanvalleur versleuteld. Het bedrijf maakt gebruik van de expertise van een extern cyberbeveiligingsbedrijf om zijn netwerk te bewaken. Er zijn logboeken beschikbaar waarin alle gegevensstromen worden geregistreerd die het bedrijf verlaten (waaronder uitgaande e-mail). Nadat de logboeken en de door de andere detectiesystemen verzamelde gegevens waren geanalyseerd, werd bij het interne onderzoek met ondersteuning van het cyberbeveiligingsbedrijf vastgesteld dat de dader de gegevens alleen had versleuteld, zonder deze te exfiltreren. De logboeken laten geen uitgaande gegevensstroom tijdens de aanval zien. De door de inbreuk getroffen persoonsgegevens hebben betrekking op de werknemers en klanten van het bedrijf, in totaal enkele tientallen personen. Er werden geen bijzondere categorieën van gegevens getroffen. Er was geen back-up in elektronische vorm beschikbaar. De meeste gegevens werden hersteld vanaf papieren back-ups. Het herstel van de gegevens nam vijf werkdagen in beslag en leidde tot geringe vertragingen in de levering van bestellingen aan klanten.

2.2.1 GEVAL nr. 2 — Voorafgaande maatregelen en risicobeoordeling

26. De verwerkingsverantwoordelijke had dezelfde voorafgaande maatregelen moeten nemen als genoemd in deel 2.1 en in punt 2.9. Het grootste verschil met het vorige geval is het ontbreken van een elektronische back-up en het ontbreken van versleuteling in rust. Dit leidt tot kritische verschillen in de volgende stappen.
27. Bij de beoordeling van de risico's moet de verwerkingsverantwoordelijke de infiltratiemethode onderzoeken en het soort kwaadaardige code vaststellen om inzicht te krijgen in de mogelijke gevolgen van de aanval. In dit voorbeeld werden de persoonsgegevens door de ransomware versleuteld zonder deze te exfiltreren. Daarom lijken de risico's voor de rechten en vrijheden van betrokkenen voort te vloeien uit het niet beschikbaar zijn van de persoonsgegevens en is de vertrouwelijkheid van de persoonsgegevens niet gecompromitteerd. Een grondig onderzoek van de firewall-logbestanden en de conclusies daarvan is essentieel om het risico vast te stellen. De verwerkingsverantwoordelijke moet op verzoek de feitelijke bevindingen van deze onderzoeken presenteren.

28. De gegevensverwerker mag niet uit het oog verliezen dat als de aanval meer geavanceerd is, de malware de functionaliteit heeft om logbestanden te bewerken en het spoor te verwijderen. Aangezien logbestanden niet naar een centrale logserver worden doorgezonden of gerepliceerd, kan de verwerkingsverantwoordelijke zelfs na een grondig onderzoek waarbij is vastgesteld dat de persoonsgegevens door de aanvaller niet zijn geëxfiltreerd dus niet verklaren dat de afwezigheid van een vermelding in de logbestanden bewijst dat er geen exfiltratie heeft plaatsgevonden. Daarom kan een inbreuk op de vertrouwelijkheid niet geheel worden uitgesloten.
29. Als de aanvaller toegang had tot de gegevens, moet de verwerkingsverantwoordelijke de risico's van deze inbreuk beoordelen¹³. Bij de risicobeoordeling moet de verwerkingsverantwoordelijke ook rekening houden met de aard, de gevoeligheid, het volume en de context van de persoonsgegevens waarop de inbreuk betrekking heeft. In dit geval zijn er geen bijzondere categorieën van persoonsgegevens getroffen en zijn de hoeveelheid gecompromitteerde gegevens en het aantal getroffen betrokkenen laag.
30. Het verzamelen van exacte informatie over de ongeoorloofde toegang is essentieel om het risiconiveau vast te stellen en een nieuwe of voortgezette aanval te voorkomen. Als de gegevens waren gekopieerd uit de databank, zou dat uiteraard een risicoverhogende factor zijn geweest. Bij twijfel over de bijzonderheden van de onrechtmatige toegang moet het ongunstigste scenario in aanmerking worden genomen en moet het risico dienovereenkomstig worden beoordeeld.
31. De afwezigheid van een back-updatabank kan worden beschouwd als een risicoverhogende factor, afhankelijk van de ernst van de gevolgen die voor de betrokkenen voortvloeien uit het niet beschikbaar zijn van de gegevens.

2.2.2 GEVAL nr. 2 — Risicobeperking en verplichtingen

32. Zonder een back-up kan de verwerkingsverantwoordelijke weinig maatregelen nemen om het verlies van persoonsgegevens te herstellen en moeten de gegevens opnieuw worden verzameld, tenzij er een andere bron beschikbaar is (bv. e-mails waarin bestellingen worden bevestigd). Zonder een back-up kunnen er gegevens verloren gaan en is de ernst afhankelijk van de gevolgen voor de personen.
33. Als de gegevens nog op papier beschikbaar zijn, zou het herstel van de gegevens geen al te grote problemen mogen opleveren¹⁴. Gezien het ontbreken van een elektronische back-updatabank wordt een melding aan de TA echter wel nodig geacht, omdat het herstel van de gegevens enige tijd in beslag nam en enige vertraging in de levering van de bestellingen aan klanten zou kunnen veroorzaken en omdat een aanzienlijke hoeveelheid metagegevens (bv. logboeken, tijdstempels) mogelijk niet terug te vinden is.
34. Het informeren van de betrokkenen over de inbreuk kan ook afhangen van de tijdsduur gedurende welke de persoonsgegevens niet beschikbaar zijn en van de problemen die daardoor kunnen ontstaan voor de activiteiten van de verwerkingsverantwoordelijke (bv. vertragingen in de overmaking van betalingen aan het personeel). Aangezien deze vertragingen in betalingen en leveringen kunnen leiden tot financiële verliezen voor de personen wier gegevens zijn gecompromitteerd, zou men ook kunnen stellen dat de inbreuk

¹³ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

¹⁴ Dit zal afhangen van de complexiteit en de structuur van de persoonsgegevens. In de meest complexe scenario's kan het herstellen van de gegevensintegriteit en de samenhang met de metagegevens, het zorgen voor correcte relaties binnen gegevensstructuren en het controleren van de nauwkeurigheid van de gegevens aanzienlijke middelen en inspanningen vergen.

waarschijnlijk een hoog risico inhoudt. Ook valt er mogelijk niet aan te ontkomen de betrokkenen te informeren als hun bijdrage nodig is om de versleutelde gegevens te herstellen.

35. Dit geval dient als voorbeeld voor een aanval met ransomware met een risico voor de rechten en vrijheden van de betrokkenen, maar waarbij geen sprake is van een hoog risico. Het geval moet worden gedocumenteerd overeenkomstig artikel 33, lid 5, en aan de TA worden gemeld overeenkomstig artikel 33, lid 1. De organisatie kan ook genoodzaakt zijn (of door de TA worden verplicht) om haar organisatorische en technische maatregelen en procedures ter beveiliging van de persoonsgegevens en ter beperking van de risico's te actualiseren en te herstellen.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✗

2.3 GEVAL nr. 3: Ransomware met back-up en zonder exfiltratie in een ziekenhuis

Het informatiesysteem van een ziekenhuis/gezondheidscentrum werd blootgesteld aan een aanval met ransomware en daarbij werd een aanzienlijk deel van de gegevens door de aanvaller versleuteld. Het bedrijf maakt gebruik van de expertise van een extern cyberbeveiligingsbedrijf om zijn netwerk te bewaken. Er zijn logboeken beschikbaar waarin alle gegevensstromen worden geregistreerd die het bedrijf verlaten (waaronder uitgaande e-mail). Nadat de logboeken en de door de andere detectiesystemen verzamelde gegevens waren geanalyseerd, werd bij het interne onderzoek met ondersteuning van het cyberbeveiligingsbedrijf vastgesteld dat de dader de gegevens alleen had versleuteld, zonder deze te exfiltreren. De logboeken laten geen uitgaande gegevensstroom tijdens de aanval zien. De door de inbreuk getroffen persoonsgegevens hebben betrekking op de werknemers en patiënten, in totaal duizenden personen. Er waren back-ups in elektronische vorm beschikbaar. De meeste gegevens werden hersteld, maar dat duurde twee werkdagen en leidde tot grote vertragingen in de behandeling van de patiënten, waardoor operaties moesten worden afgezegd/uitgesteld, en tot een lager dienstverleningsniveau als gevolg van het niet beschikbaar zijn van de systemen.

2.3.1 GEVAL nr. 3 — Voorafgaande maatregelen en risicobeoordeling

36. De verwerkingsverantwoordelijke had dezelfde voorafgaande maatregelen moeten nemen als genoemd in deel 2.1 en in punt 2.5. Het grootste verschil met het vorige geval is de grote ernst van de gevolgen voor een aanzienlijk deel van de betrokkenen¹⁵.
37. De hoeveelheid gecompromitteerde gegevens en het aantal getroffen betrokkenen zijn hoog, omdat ziekenhuizen gewoonlijk grote hoeveelheden gegevens verwerken. Het niet beschikbaar zijn van de gegevens heeft grote gevolgen voor een aanzienlijk deel van de betrokkenen. Bovendien blijft er een zeer ernstig restrisico bestaan voor de vertrouwelijkheid van de patiëntgegevens.
38. Het soort inbreuk en de aard, de gevoeligheid en het volume van de door de inbreuk getroffen persoonsgegevens zijn belangrijk. Hoewel er een back-up van de gegevens was gemaakt en de gegevens binnen enkele dagen konden worden hersteld, bestaat er nog steeds een hoog risico vanwege de ernst van de gevolgen die voor de betrokkenen voortvloeien uit het niet beschikbaar zijn van de gegevens op het moment van de aanval en de dagen daarna.

¹⁵ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

2.3.2 GEVAL nr. 3 — Risicobeperking en verplichtingen

39. Een melding aan de TA wordt noodzakelijk geacht, aangezien er bijzondere categorieën van persoonsgegevens bij de inbreuk betrokken zijn en het herstel van de gegevens veel tijd in beslag kan nemen, waardoor er grote vertragingen in de patiëntenzorg optreden. De betrokkenen moeten over de inbreuk worden geïnformeerd vanwege de gevolgen voor de patiënten, ook na het herstellen van de versleutelde gegevens. Hoewel er gegevens zijn versleuteld over alle patiënten die de afgelopen jaren in het ziekenhuis zijn behandeld, had de inbreuk alleen gevolgen voor de patiënten die in het ziekenhuis zouden worden behandeld gedurende de tijd dat het computersysteem niet beschikbaar was. De verwerkingsverantwoordelijke moet de gegevensinbreuk rechtstreeks aan die patiënten meedelen. Rechtstreekse mededeling aan de andere patiënten, van wie sommigen misschien al meer dan twintig jaar niet in het ziekenhuis zijn geweest, is mogelijk niet verplicht vanwege de uitzondering van artikel 34, lid 3, punt c). In een dergelijk geval komt er in de plaats daarvan een openbare mededeling¹⁶ of een vergelijkbare maatregel waarbij betrokkenen even doeltreffend worden geïnformeerd. In dit geval moet het ziekenhuis de aanval met ransomware en de gevolgen daarvan openbaar maken.
40. Dit geval dient als voorbeeld voor een aanval met ransomware met een hoog risico voor de rechten en vrijheden van de betrokkenen. Het geval moet worden gedocumenteerd overeenkomstig artikel 33, lid 5, aan de TA worden gemeld overeenkomstig artikel 33, lid 1, en aan de betrokkenen worden megedeeld overeenkomstig artikel 34, lid 1. De organisatie moet ook haar organisatorische en technische maatregelen en procedures ter beveiliging van de persoonsgegevens en ter beperking van de risico's actualiseren en herstellen.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓

2.4 GEVAL nr. 4: Ransomware zonder back-up en met exfiltratie

De server van een openbaarvervoerbedrijf werd blootgesteld aan een aanval met ransomware en daarbij werden de gegevens door de aanvaller versleuteld. Volgens de bevindingen van het interne onderzoek had de dader de gegevens niet alleen versleuteld, maar ook geëxfiltratie. Het soort gecompromitteerde gegevens betrof de persoonsgegevens van klanten en werknemers en van de enkele duizenden personen die gebruikmaken van de diensten van het bedrijf (bv. onlinekaartverkoop). Naast essentiële identiteitsgegevens zijn er ook identiteitskaartnummers en financiële gegevens zoals creditcardgegevens bij de inbreuk betrokken. Er was een back-up gemaakt, maar die werd door de aanvaller ook versleuteld.

¹⁶ In overweging 86 AVG wordt toegelicht dat “[d]ergelijke kennisgevingen aan betrokkenen zo snel als redelijkerwijs mogelijk [dienen] te worden gedaan, in nauwe samenwerking met de toezichthoudende autoriteit en met inachtneming van de door haarzelf of door andere relevante autoriteiten, zoals rechtshandavingsautoriteiten, aangereikte richtsnoeren. Zo zouden betrokkenen bijvoorbeeld onverwijld in kennis moeten worden gesteld wanneer een onmiddellijk risico op schade moet worden beperkt, terwijl een langere kennisgevingstermijn gerechtvaardigd kan zijn wanneer er passende maatregelen moeten worden genomen tegen aanhoudende of vergelijkbare inbreuken in verband met persoonsgegevens”.

2.4.1 GEVAL nr. 4 — Voorafgaande maatregelen en risicobeoordeling

41. De verwerkingsverantwoordelijke had dezelfde voorafgaande maatregelen moeten nemen als genoemd in deel 2.1 en in punt 2.5. Hoewel er een back-up was, werd die ook getroffen door de aanval. Alleen al deze regeling roept vragen op over de kwaliteit van de voorafgaande IT-beveiligingsmaatregelen van de verwerkingsverantwoordelijke en moet bij het onderzoek nader worden onderzocht, aangezien bij een goed back-upbeleid meerdere back-ups veilig moeten worden opgeslagen zonder toegang vanuit het hoofdsysteem om te voorkomen dat ze bij dezelfde aanval gecompromitteerd raken. Bovendien kunnen aanvallen met ransomware dagenlang onontdekt blijven, waardoor zelden gebruikte gegevens langzaam kunnen worden versleuteld. Hierdoor kunnen meerdere back-ups onbruikbaar worden en daarom moeten de back-ups regelmatig worden gemaakt en apart worden bewaard. Dit zou de kans op herstel vergroten, zij het met een groter verlies van gegevens.
42. Deze inbreuk betreft niet alleen de beschikbaarheid van de gegevens maar ook de vertrouwelijkheid, aangezien de aanvaller vanaf de server gegevens kan hebben gewijzigd en/of gekopieerd. Dit soort inbreuk houdt dan ook een hoog risico in¹⁷.
43. Door de aard, de gevoeligheid en het volume van de persoonsgegevens zijn de risico's nog groter, omdat het aantal getroffen personen hoog is, net als de totale hoeveelheid getroffen persoonsgegevens. Naast essentiële identiteitsgegevens zijn er ook identiteitsdocumenten en financiële gegevens zoals creditcardgegevens bij de inbreuk betrokken. Een gegevensinbreuk in verband met deze soorten gegevens vormt op zichzelf een hoog risico en bij gezamenlijke verwerking zouden de gegevens kunnen worden gebruikt voor onder meer identiteitsdiefstal of -fraude.
44. Als gevolg van ondeugdelijke serverlogica of organisatorische maatregelen werden de back-upbestanden getroffen door de ransomware, waardoor de gegevens niet konden worden hersteld en het risico toenam.
45. Deze gegevensinbreuk vormt een hoog risico voor de rechten en vrijheden van personen, omdat de inbreuk waarschijnlijk zou kunnen leiden tot zowel materiële schade (bv. financiële verliezen, aangezien er creditcardgegevens werden getroffen) als immateriële schade (bv. identiteitsdiefstal of -fraude, aangezien er identiteitskaartgegevens werden getroffen).

2.4.2 GEVAL nr. 4 — Risicobeperking en verplichtingen

46. Een mededeling aan de betrokkenen is essentieel zodat zij de noodzakelijke maatregelen kunnen nemen om materiële schade te voorkomen (bv. hun creditcards blokkeren).
47. Naast het documenteren van de inbreuk overeenkomstig artikel 33, lid 5, is in dit geval een melding aan de TA ook verplicht (artikel 33, lid 1) en is de verwerkingsverantwoordelijke ook gehouden om de inbreuk aan de betrokkenen mee te delen (artikel 34, lid 1). Dit laatste zou kunnen gebeuren door de betrokkenen persoonlijk op de hoogte te stellen. Bij personen van wie geen contactgegevens beschikbaar zijn, moet de verwerkingsverantwoordelijke echter een openbare mededeling doen, mits een dergelijke mededeling geen verdere negatieve gevolgen voor de betrokkenen zou hebben, bijvoorbeeld door middel van een kennisgeving op zijn website. In dit laatste geval is er een nauwkeurige en duidelijke mededeling vereist die goed zichtbaar is op de homepage van de verwerkingsverantwoordelijke, met exacte verwijzingen naar de desbetreffende bepalingen van de AVG. De organisatie kan ook genoodzaakt zijn haar organisatorische en technische maatregelen en procedures ter beveiliging van de persoonsgegevens en ter beperking van de risico's te actualiseren en te herstellen.

¹⁷ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓

2.5 Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van aanvallen met ransomware

48. Het feit dat een aanval met ransomware heeft kunnen plaatsvinden, wijst doorgaans op een of meer kwetsbare plekken in het systeem van de verwerkingsverantwoordelijke. Dit geldt ook voor aanvallen met ransomware waarbij de persoonsgegevens zijn versleuteld, maar niet zijn geëxfiltreerd. Ongeacht de uitkomst en de gevolgen van de aanval kan het belang van een alomvattende evaluatie van het gegevensbeveiligingssysteem — met bijzondere nadruk op IT-beveiliging — niet genoeg worden beklemtoond. De vastgestelde zwakke plekken en gaten in de beveiliging moeten worden gedocumenteerd en onmiddellijk worden aangepakt.

49. Aanbevolen maatregelen:

(De lijst van de volgende maatregelen is geenszins exclusief of volledig. Het doel is veeleer om ideeën voor preventie en mogelijke oplossingen aan te dragen. Elke verwerkingsactiviteit is anders en daarom moet de verwerkingsverantwoordelijke bepalen welke maatregelen het best bij de gegeven situatie passen.)

- J up-to-date houden van de firmware, het besturingssysteem en de applicatiesoftware op de servers, gebruikersmachines, actieve netwerkcomponenten en andere machines op hetzelfde LAN (waaronder wifi-apparatuur); ervoor zorgen dat er passende IT-beveiligingsmaatregelen worden getroffen en dat de maatregelen effectief zijn en regelmatig worden geactualiseerd wanneer de verwerking of de omstandigheden veranderen of evolueren. Dit omvat het bijhouden van gedetailleerde logboeken waarin wordt geregistreerd welke patches op welk tijdstempel zijn toegepast;
- J ontwerpen en organiseren van verwerkingssystemen en -infrastructuur voor het segmenteren of isoleren van gegevenssystemen en -netwerken, om verspreiding van malware binnen de organisatie en naar externe systemen te voorkomen;
- J toepassing van een moderne, veilige en beproefde back-upprocedure. Media voor back-ups voor de middellange en lange termijn moeten gescheiden van de operationele gegevensopslag worden bewaard, zodat zij buiten het bereik van derden zijn, ook in het geval van een geslaagde aanval (zoals dagelijkse incrementele back-up en wekelijkse volledige back-up);
- J gebruik van passende, geactualiseerde, effectieve en geïntegreerde antimalwaresoftware;
- J toepassing van een passend, geactualiseerd, effectief en geïntegreerd firewall- en indringersdetectie- en -preventiesysteem; het netwerkverkeer omleiden via de firewall/indringersdetectie, ook in het geval van thuiswerken of mobiel werken (bv. door voor de toegang tot het internet gebruik te maken van VPN-verbindingen met organisatorische beveiligingsmechanismen);
- J opleiden van werknemers over methoden voor het herkennen en voorkomen van IT-aanvallen. De verwerkingsverantwoordelijke moet middelen verschaffen om vast te stellen of via andere communicatiemiddelen ontvangen e-mails en berichten authentiek en betrouwbaar zijn. Werknemers moeten worden opgeleid om te herkennen wanneer een dergelijke aanval heeft plaatsgevonden, over de wijze waarop het eindpunt uit het netwerk moet worden verwijderd en over hun verplichting om de aanval onmiddellijk aan de beveiligingsfunctionaris te melden;
- J benadrukken van de noodzaak om het soort kwaadaardige code vast te stellen om na te gaan wat de gevolgen van de aanval zijn en om de juiste maatregelen te kunnen treffen om het risico te beperken. Wanneer een aanval met ransomware is geslaagd en er geen back-up beschikbaar is, kunnen beschikbare tools zoals die van het “no more ransom”-project (nomoreransom.org) mogelijk worden toegepast om

gegevens op te halen. Als er wel een veilige back-up beschikbaar is, wordt aangeraden de gegevens vanaf die back-up te herstellen;

- J doorsturen of repliceren van alle logboeken naar een centrale logserver (eventueel met aftekening of cryptografische tijdstempeling van logboekvermeldingen);
- J sterke versleuteling en meervoudige authenticatie, met name voor administratieve toegang tot IT-systemen, passend sleutel- en wachtwoordbeheer;
- J regelmatige kwetsbaarheids- en penetratietests;
- J oprichting van een Computer Security Incident Response Team (CSIRT) of een Computer Emergency Response Team (CERT) binnen de organisatie of aansluiting bij een collectief CSIRT/CERT; opstellen van een reactieplan voor inbreuken, een noodherstelplan en een bedrijfscontinuïteitsplan en ervoor zorgen dat deze plannen grondig zijn getest;
- J bij de beoordeling van tegenmaatregelen — risicoanalyse moet worden geëvalueerd, getest en geactualiseerd.

3 AANVALLEN MET GEGEVENSEXFILTRATIE

50. Aanvallen die zijn gericht op kwetsbaarheden in diensten die door de verwerkingsverantwoordelijke via het internet aan derden worden aangeboden en die bijvoorbeeld worden uitgevoerd door middel van injectieaanvallen (bv. SQL-injectie, path traversal), compromittering van websites en vergelijkbare methoden, kunnen lijken op aanvallen met ransomware in die zin dat het risico voortvloeit uit een handeling van een ongeautoriseerde derde. Die aanvallen zijn echter doorgaans gericht op het kopiëren, exfiltreren en misbruiken van persoonsgegevens met een kwaadwillige bedoeling en zijn dan ook voornamelijk inbreuken op de vertrouwelijkheid en mogelijk ook op de gegevensintegriteit. Tegelijkertijd heeft een verwerkingsverantwoordelijke die op de hoogte is van de kenmerken van dit soort inbreuken tal van maatregelen tot zijn beschikking die het risico van een geslaagde uitvoering van een aanval aanzienlijk kunnen beperken.

3.1 GEVAL nr. 5: Exfiltratie van sollicitatiegegevens van een website

Een uitzendbureau is het slachtoffer geworden van een cyberaanval waarbij een kwaadaardige code op zijn website werd geplaatst. Met deze kwaadaardige code werden via online-sollicitatieformulieren verstrekte en op de webserver opgeslagen persoonsgegevens toegankelijk gemaakt voor ongeautoriseerde personen. Mogelijk zijn er 213 van dergelijke formulieren getroffen. Na analyse van de getroffen gegevens werd vastgesteld dat er bij de inbreuk geen bijzondere categorieën van gegevens waren getroffen. De geïnstalleerde malwaretoolkit had functionaliteiten waarmee de aanvaller de exfiltratiegeschiedenis kon verwijderen en waarmee de verwerking op de server ook kon worden gevolgd en persoonsgegevens konden worden vergaard. De toolkit werd pas een maand na de installatie ervan ontdekt.

3.1.1 GEVAL nr. 5 — Voorafgaande maatregelen en risicobeoordeling

51. De beveiliging van de omgeving van de verwerkingsverantwoordelijke is uiterst belangrijk, aangezien het merendeel van deze inbreuken kan worden voorkomen door ervoor te zorgen dat alle systemen up-to-date worden gehouden, dat gevoelige gegevens worden versleuteld en dat de applicaties worden ontwikkeld volgens hoge beveiligingsnormen zoals sterke authenticatie, maatregelen tegen aanvallen met brute kracht,

“escaping” of “sanitising”¹⁸ van gebruikersinvoer enz. Er zijn ook periodieke IT-beveiligingsaudits, kwetsbaarheidsbeoordelingen en penetratietests nodig om dit soort kwetsbaarheden vooraf op te sporen en te verhelpen. In dit specifieke geval hadden tools voor de bewaking van de bestandsintegriteit in de productieomgeving mogelijk kunnen helpen om de code-injectie op te sporen. (Een lijst van aanbevolen maatregelen is te vinden in punt 3.7.)

52. Om te beoordelen welke maatregelen er moeten worden genomen, moet de verwerkingsverantwoordelijke altijd beginnen met het onderzoeken van de inbreuk door het soort aanval en de daarbij gebruikte methoden vast te stellen. De verwerkingsverantwoordelijke moet, om snel en efficiënt te kunnen handelen, beschikken over een reactieplan voor inbreuken waarin de snelle stappen worden beschreven die nodig zijn om het incident onder controle te krijgen. In dit specifieke geval was het soort inbreuk een risicoverhogende factor, aangezien niet alleen de vertrouwelijkheid van de gegevens werd ingeperkt, maar de infiltrant ook de middelen had om wijzigingen in het systeem aan te brengen, waardoor de gegevensintegriteit ook in twijfel moest worden getrokken.
53. De aard, de gevoeligheid en het volume van de persoonsgegevens waarop de inbreuk betrekking had, moeten worden beoordeeld om te bepalen in hoeverre de inbreuk gevolgen had voor de betrokkenen. Hoewel er geen bijzondere categorieën van persoonsgegevens werden getroffen, bevatten de gegevens waartoe toegang werd verkregen aanzienlijke informatie over de personen uit de onlineformulieren. Deze gegevens zouden op verschillende manieren kunnen worden misbruikt (benadering met ongevroegde marketing, identiteitsdiefstal enz.). Door de ernst van de gevolgen zal het risico voor de rechten en vrijheden van de betrokkenen dus toenemen¹⁹.

3.1.2 GEVAL nr. 5 — Risicobeperking en verplichtingen

54. Indien mogelijk moet de databank na oplossing van het probleem worden vergeleken met de op een beveiligde back-up opgeslagen databank. De bij de inbreuk opgedane ervaringen moeten worden benut bij het actualiseren van de IT-infrastructuur. De verwerkingsverantwoordelijke moet alle getroffen IT-systemen terugzetten naar een bekende schone staat, de kwetsbaarheid verhelpen en nieuwe beveiligingsmaatregelen uitvoeren om vergelijkbare gegevensinbreuken in de toekomst te voorkomen (bv. bestandsintegriteitscontroles en beveiligingsaudits). Als er niet alleen persoonsgegevens zijn geëxfiltreerd maar ook verwijderd, moet de verwerkingsverantwoordelijke systematische maatregelen nemen om de persoonsgegevens te herstellen in de staat waarin deze zich voorafgaand aan de inbreuk bevonden. Het kan noodzakelijk zijn om volledige back-ups en incrementele wijzigingen toe te passen en om vervolgens de verwerking sinds de laatste incrementele back-up eventueel opnieuw uit te voeren — waarvoor de verwerkingsverantwoordelijke de wijzigingen sinds de laatste back-up moet kunnen repliceren. Daarvoor kan het nodig zijn dat de verwerkingsverantwoordelijke het systeem zodanig heeft ontworpen dat de dagelijkse invoerbestanden worden bewaard voor het geval dat ze opnieuw moeten worden verwerkt, wat een robuuste opslagmethode en een geschikt bewaringsbeleid vereist.
55. Aangezien de inbreuk waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, moeten de betrokkenen er in het licht van het bovenstaande zeker over worden geïnformeerd (artikel 34, lid 1). Dit betekent uiteraard dat de desbetreffende TA('s) er ook bij moet(en) worden betrokken

¹⁸ “Escaping” of “sanitising” van gebruikersinvoer is een vorm van invoervalidatie die ervoor zorgt dat alleen goed geformatteerde gegevens in een informatiesysteem worden ingevoerd.

¹⁹ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

in de vorm van een melding van een inbreuk in verband met persoonsgegevens. Het documenteren van de inbreuk is verplicht krachtens artikel 33, lid 5, AVG en maakt de beoordeling van de situatie gemakkelijker.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓

3.2 GEVAL nr. 6: Exfiltratie van gehasht wachtwoord van een website

Een kwetsbaarheid voor SQL-injectie werd uitgebuit om toegang te krijgen tot een databank van de server van een kookwebsite. De gebruikers mochten alleen willekeurige pseudoniemen als gebruikersnaam kiezen. Het gebruik van e-mailadressen voor dit doel werd ontmoedigd. In de databank opgeslagen wachtwoorden waren gehasht met een sterk algoritme en de *salt* werd niet gecompromitteerd. Getroffen gegevens: gehashte wachtwoorden van 1 200 gebruikers. Voor de zekerheid heeft de verwerkingsverantwoordelijke de betrokkenen via e-mail over de inbreuk geïnformeerd en hen gevraagd hun wachtwoord te wijzigen, met name als hetzelfde wachtwoord voor andere diensten werd gebruikt.

3.2.1 GEVAL nr. 6 — Voorafgaande maatregelen en risicobeoordeling

56. In dit specifieke geval werd de vertrouwelijkheid van de gegevens gecompromitteerd, maar waren de wachtwoorden in de databank gehasht met een methode die aan de huidige eisen voldoet. Dit zou het risico met betrekking tot de aard, de gevoeligheid en het volume van de persoonsgegevens verminderen. Dit geval houdt geen risico's in voor de rechten en vrijheden van de betrokkenen.
57. Bovendien werden er geen contactgegevens (bv. e-mailadressen of telefoonnummers) van betrokkenen gecompromitteerd, wat betekent dat er geen significant risico bestaat dat de betrokkenen het doelwit worden van fraudepogingen (bv. door middel van "phishing"-e-mails of frauduleuze tekstberichten en telefoongesprekken). Er waren geen bijzondere categorieën van persoonsgegevens bij de inbreuk betrokken.
58. Sommige gebruikersnamen zouden als persoonsgegevens kunnen worden beschouwd, maar het onderwerp van de website laat geen negatieve associaties toe. Er moet echter worden opgemerkt dat de risicobeoordeling kan veranderen²⁰ als uit het soort website en de gegevens waartoe toegang is verkregen, zou kunnen blijken dat er sprake is van bijzondere categorieën van persoonsgegevens (bv. de website van een politieke partij of vakbond). Het gebruik van geavanceerde versleuteling zou de negatieve gevolgen van de inbreuk kunnen beperken. Door ervoor te zorgen dat slechts een beperkt aantal pogingen om in te loggen is toegestaan, wordt voorkomen dat brute force-inlogaanvallen slagen, waardoor de risico's van aanvallers die de gebruikersnamen al kennen sterk worden verminderd.

3.2.2 GEVAL nr. 6 — Risicobeperking en verplichtingen

59. De mededeling aan de betrokkenen zou in sommige gevallen als een risicobeperkende factor kunnen worden beschouwd, aangezien de betrokkenen ook de noodzakelijke stappen kunnen ondernemen om verdere schade als gevolg van de inbreuk te voorkomen, bijvoorbeeld door hun wachtwoord te wijzigen. Een kennisgeving was in dit geval niet verplicht, maar kan in veel gevallen als een goede praktijk worden beschouwd.

²⁰ Zie voor richtsnoeren over verwerkingen die "waarschijnlijk een hoog risico inhouden" voetnoot 10 hierboven.

60. De verwerkingsverantwoordelijke moet de kwetsbaarheid corrigeren en nieuwe beveiligingsmaatregelen uitvoeren om vergelijkbare gegevensinbreuken in de toekomst te voorkomen, zoals bijvoorbeeld systematische beveiligingsaudits van de website.
61. De inbreuk moet worden gedocumenteerd overeenkomstig artikel 33, lid 5, maar er is geen kennisgeving of mededeling nodig.
62. Ook wordt sterk aangeraden om een inbreuk in verband met wachtwoorden in elk geval aan de betrokkenen mee te delen, zelfs als de wachtwoorden zijn opgeslagen met behulp van een *salted hash* met een algoritme dat beantwoordt aan de stand van de techniek. Het verdient de voorkeur om gebruik te maken van authenticatiemethoden waarbij wachtwoorden niet op de server hoeven te worden verwerkt. De betrokkenen moet de keuze worden geboden om passende maatregelen te nemen met betrekking tot hun eigen wachtwoorden.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	X	X

3.3 GEVAL nr. 7: Credential stuffing-aanval op een bankwebsite

Een bank is het slachtoffer geworden van een cyberaanval op een van haar e-bankingwebsites. De aanval was erop gericht alle mogelijke gebruikersnamen te vinden met behulp van een vast triviaal wachtwoord. De wachtwoorden bestaan uit acht cijfers. Door een zwakke plek in de website is in sommige gevallen informatie over betrokkenen (naam, achternaam, geslacht, geboortedatum en -plaats, fiscale code, gebruikersidentificatiecodes) gelekt naar de aanvaller, zelfs als het gebruikte wachtwoord niet juist was of de bankrekening niet meer actief was. Ongeveer 100 000 betrokkenen werden hierdoor getroffen. De aanvaller slaagde erin in te loggen op ongeveer 2 000 rekeningen waarvoor het triviale wachtwoord werd gebruikt dat de aanvaller had geprobeerd. Na de aanval kon de verwerkingsverantwoordelijke alle onrechtmatige inlogpogingen vaststellen. De verwerkingsverantwoordelijke kon bevestigen dat er volgens de antifraudecontroles tijdens de aanval geen transacties op deze rekeningen waren verricht. De bank was op de hoogte van de gegevensinbreuk doordat haar centrum voor beveiligingsoperaties een groot aantal inlogverzoeken voor de website had waargenomen. Naar aanleiding daarvan heeft de verwerkingsverantwoordelijke de mogelijkheid om op de website in te loggen uitgeschakeld en een wachtwoordwijziging voor de gecompromitteerde rekeningen afgedwongen. De verwerkingsverantwoordelijke heeft de inbreuk alleen meegedeeld aan de gebruikers met een gecompromitteerde rekening, dat wil zeggen aan gebruikers wier wachtwoord was gecompromitteerd of wier gegevens waren onthuld.

3.3.1 GEVAL nr. 7 — Voorafgaande maatregelen en risicobeoordeling

63. Het is belangrijk te vermelden dat verwerkingsverantwoordelijken die gegevens van zeer persoonlijke aard verwerken²¹, een grotere verantwoordelijkheid hebben om voor een adequate gegevensbeveiliging te zorgen, bijvoorbeeld om een centrum voor beveiligingsoperaties op te zetten en andere maatregelen te nemen om incidenten te voorkomen en op te sporen en erop te reageren. Het niet voldoen aan deze hogere normen zal bij een onderzoek van een TA zeker tot zwaardere maatregelen leiden.

²¹ Zoals informatie over de betrokkenen met betrekking tot betalingsmethoden zoals creditcardnummers, bankrekeningen, onlinebetalingen, loonlijsten, bankafschriften, economische studies of andere gegevens die economische informatie over de betrokkenen kunnen onthullen.

64. Deze inbreuk heeft betrekking op financiële gegevens die verder gaan dan de identiteitsgegevens en gebruikersnamen, wat de inbreuk bijzonder ernstig maakt. Het aantal getroffen personen is hoog.
65. Het feit dat een inbreuk kon plaatsvinden in een dergelijke gevoelige omgeving wijst op aanzienlijke gaten in de beveiliging van het systeem van de verwerkingsverantwoordelijke en kan een aanwijzing zijn dat het moment is aangebroken dat een herziening en actualisering van de betrokken maatregelen “noodzakelijk” is overeenkomstig artikel 24, lid 1, artikel 25, lid 1, en artikel 32, lid 1, AVG. De gecompromitteerde gegevens maken een unieke identificatie van betrokkenen mogelijk en bevatten andere informatie over hen (waaronder geslacht, geboortedatum en -plaats) en kunnen bovendien door de aanvaller worden gebruikt om wachtwoorden van de klanten te raden of om een spear phishing-aanval uit te voeren die gericht is tegen de klanten van de bank.
66. Om deze redenen werd de gegevensinbreuk geacht waarschijnlijk een hoog risico in te houden voor de rechten en vrijheden van alle betrokkenen²². Het is daarom niet ondenkbaar dat de inbreuk leidt tot materiële schade (bv. financiële verliezen) en immateriële schade (bv. identiteitsdiefstal of -fraude).

3.3.2 GEVAL nr. 7 — Risicobeperking en verplichtingen

67. De in de beschrijving van het geval genoemde maatregelen van de verwerkingsverantwoordelijke zijn adequaat. Naar aanleiding van de inbreuk werd ook de kwetsbaarheid van de website gecorrigeerd en werden er andere maatregelen genomen om soortgelijke gegevensinbreuken in de toekomst te voorkomen, zoals het toevoegen van tweefactorauthenticatie aan de betrokken website en het versterken van de klantauthenticatie.
68. Het documenteren van de inbreuk overeenkomstig artikel 33, lid 5, AVG en het melden ervan aan de TA zijn in dit scenario niet facultatief. Bovendien moet de verwerkingsverantwoordelijke alle 100 000 betrokkenen (onder wie de betrokkenen wier rekening niet werd gecompromitteerd) informeren overeenkomstig artikel 34 AVG.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓

3.4 Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van aanvallen door hackers

69. Net als bij aanvallen met ransomware moeten de verwerkingsverantwoordelijken, ongeacht de uitkomst en de gevolgen van de aanval, in vergelijkbare gevallen de IT-beveiliging opnieuw evalueren.
70. Aanbevolen maatregelen²³:

(De onderstaande lijst van maatregelen is geenszins exclusief of volledig. Het doel is veeleer om ideeën voor preventie en mogelijke oplossingen aan te dragen. Elke verwerkingsactiviteit is anders en daarom moet de verwerkingsverantwoordelijke bepalen welke maatregelen het best bij de gegeven situatie passen.)

- J geavanceerde versleuteling en sleutelbeheer, met name wanneer wachtwoorden, gevoelige of financiële gegevens worden verwerkt. Cryptografisch hashen en salten van geheime informatie (wachtwoorden)

²² Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

²³ Zie voor de ontwikkeling van beveiligde webapplicaties ook: https://www.owasp.org/index.php/Main_Page

heeft altijd de voorkeur boven versleuteling van wachtwoorden. Het gebruik van authenticatiemethoden waarbij wachtwoorden niet op de server hoeven te worden verwerkt, verdient de voorkeur;

- J up-to-date houden van het systeem (software en firmware); ervoor zorgen dat alle IT-beveiligingsmaatregelen worden getroffen en dat deze maatregelen effectief zijn en regelmatig worden geactualiseerd wanneer de verwerking of de omstandigheden veranderen of evolueren. Om overeenkomstig artikel 5, lid 2, AVG te kunnen aantonen dat artikel 5, lid 1, punt f), is nageleefd, moet de verwerkingsverantwoordelijke een register bijhouden van alle updates die zijn uitgevoerd, met inbegrip van het tijdstip waarop de updates zijn toegepast;
- J gebruik van sterke authenticatiemethoden zoals tweefactorauthenticatie en authenticatieservers, aangevuld met een geactualiseerd wachtwoordbeleid;
- J veilige ontwikkelingsnormen omvatten de filtering van gebruikersinvoer (met gebruik van whitelisting voor zover praktisch uitvoerbaar), het ontwijken van gebruikersinvoer en maatregelen ter voorkoming van brute force-aanvallen (zoals beperking van het maximumaantal nieuwe pogingen). “Webapplicatie-firewalls” kunnen bijdragen tot een effectief gebruik van deze methode;
- J sterke gebruikersbevoegdheden en beleid voor toegangscontrolebeheer;
- J gebruik van passende, geactualiseerde, effectieve en geïntegreerde firewall-, indringersdetectie- en andere perimeterverdedigingssystemen;
- J systematische IT-beveiligingsaudits en kwetsbaarheidsbeoordelingen (penetratietests);
- J regelmatige evaluaties en tests om ervoor te zorgen dat de back-ups kunnen worden gebruikt om gegevens te herstellen waarvan de integriteit of de beschikbaarheid is aangetast;
- J geen sessie-ID in URL in platte tekst.

4 INTERNE BRON VAN MENSELIJK RISICO

71. De rol van menselijke fouten bij inbreuken in verband met persoonsgegevens moet worden benadrukt, omdat deze fouten vaak voorkomen. Aangezien dit soort inbreuken zowel opzettelijk als onopzettelijk kan worden gepleegd, is het voor de verwerkingsverantwoordelijken bijzonder moeilijk om de kwetsbaarheden vast te stellen en maatregelen te nemen om deze inbreuken te voorkomen. De internationale conferentie van commissarissen voor de bescherming van gegevens en de persoonlijke levenssfeer heeft het belang van de aanpak van dergelijke menselijke factoren erkend en in oktober 2019 een resolutie aangenomen waarin werd opgeroepen aandacht te besteden aan de rol van menselijke fouten bij inbreuken in verband met persoonsgegevens²⁴. Deze resolutie benadrukt dat er passende veiligheidsmaatregelen moeten worden genomen om menselijke fouten te voorkomen en voorziet in een niet-limitatieve lijst van dergelijke waarborgen en benaderingen.

4.1 GEVAL nr. 8: Exfiltratie van bedrijfsgegevens door een werknemer

Tijdens zijn opzegtermijn kopieert een werknemer van een bedrijf bedrijfsgegevens uit de databank van het bedrijf. De werknemer is geautoriseerd om alleen toegang tot de gegevens te krijgen om zijn functie uit te oefenen. Enkele maanden later, nadat hij zijn baan heeft opgezegd, gebruikt hij de gekopieerde gegevens (essentiële contactgegevens) voor een nieuwe gegevensverwerking waarvoor hij verwerkingsverantwoordelijke is om contact op te nemen met de klanten van het bedrijf om ze naar zijn nieuwe bedrijf te lokken.

²⁴ <http://globalprivacyassembly.org/wp-content/uploads/2019/10/AOIC-Resolution-FINAL-ADOPTED.pdf>

4.1.1 GEVAL nr. 8 — Voorafgaande maatregelen en risicobeoordeling

72. In dit specifieke geval zijn er geen voorafgaande maatregelen genomen om te voorkomen dat de werknemer de contactinformatie van de klanten van het bedrijf zou kopiëren, aangezien hij voor zijn functie rechtmatige toegang tot deze informatie nodig had en ook daadwerkelijk had. Aangezien voor de meeste functies met klantencontacten een bepaalde vorm van toegang van werknemers tot persoonsgegevens nodig is, zijn deze gegevensinbreuken misschien wel het moeilijkst te voorkomen. Beperkingen aan de reikwijdte van de toegang kunnen een belemmering vormen voor de werkzaamheden die de betrokken werknemer kan uitvoeren. Een goed doordacht toegangsbeleid en een voortdurende controle kunnen echter helpen dergelijke inbreuken te voorkomen.
73. Zoals gebruikelijk moet bij de risicobeoordeling rekening worden gehouden met het soort inbreuk en met de aard, de gevoeligheid en het volume van de getroffen persoonsgegevens. Bij deze soorten inbreuken gaat het doorgaans om inbreuken op de vertrouwelijkheid, aangezien de databank gewoonlijk intact blijft en de inhoud ervan “slechts” wordt gekopieerd voor verder gebruik. De hoeveelheid getroffen gegevens is gewoonlijk ook laag of gemiddeld. In dit specifieke geval werden er geen bijzondere categorieën van gegevens getroffen en had de werknemer de contactinformatie van de klanten alleen nodig om na uitdiensttreding contact met hen te kunnen opnemen. Daarom zijn de betrokken gegevens niet gevoelig.
74. Hoewel het enige doel van de ex-werknemer die met kwade bedoelingen de gegevens kopieerde beperkt kan zijn tot het verkrijgen van de contactinformatie van de klanten van het bedrijf voor zijn eigen commerciële doeleinden, kan de verwerkingsverantwoordelijke het risico voor de getroffen betrokkenen niet als laag beoordelen, aangezien de verwerkingsverantwoordelijke geen enkele zekerheid heeft over de bedoelingen van de werknemer. De gevolgen van de inbreuk mogen dan beperkt zijn tot blootstelling aan ongevraagde zelfmarketing van de ex-werknemer, verder en ernstiger misbruik van de gestolen gegevens is dus niet uitgesloten, afhankelijk van het doel van de door de ex-werknemer uitgevoerde verwerking²⁵.

4.1.2 GEVAL nr. 8 — Risicobeperking en verplichtingen

75. Het is niet eenvoudig om de negatieve gevolgen van de inbreuk in het bovengenoemde geval te beperken. Daarvoor kan het nodig zijn om onmiddellijk juridische stappen te ondernemen om te voorkomen dat de voormalige werknemer doorgaat met het misbruiken en verspreiden van de gegevens. Als volgende stap moet het doel zijn om vergelijkbare situaties in de toekomst te voorkomen. De verwerkingsverantwoordelijke kan proberen de ex-werknemer op te dragen te stoppen met het gebruiken van de gegevens, maar het succes van deze actie is in het gunstigste geval twijfelachtig. Passende technische maatregelen zoals het kopiëren of downloaden van gegevens naar verwijderbare apparaten onmogelijk maken, kunnen daarbij van nut zijn.
76. Er is geen pasklare oplossing voor dit soort gevallen, maar een systematische aanpak kan helpen ze te voorkomen. Zo kan het bedrijf overwegen om, waar mogelijk, bepaalde toegangsrechten in te trekken voor werknemers die hebben aangegeven ontslag te willen nemen, of om toegangslogs in te voeren, zodat ongewenste toegang kan worden geregistreerd en gesignaleerd. Het met de werknemers gesloten contract moet clausules bevatten die dergelijke acties verbieden.
77. Aangezien de betrokken inbreuk geen hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, zal al met al een melding aan de TA volstaan. Het informeren van de betrokkenen kan echter ook nuttig zijn voor de verwerkingsverantwoordelijke, omdat het wellicht beter is dat zij van het bedrijf horen dat er een gegevenslek heeft plaatsgevonden dan van de ex-werknemer die probeert contact met hen op te

²⁵ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

nemen. Het documenteren van de gegevensinbreuk overeenkomstig artikel 33, lid 5, is een wettelijke verplichting.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	X

4.2 GEVAL nr. 9: Onbedoelde doorgifte van gegevens aan een betrouwbare derde

Een verzekeringsagent heeft gemerkt dat hij — door verkeerde instellingen van een per e-mail ontvangen Excel-bestand — toegang had tot informatie over ongeveer twintig klanten die niet tot zijn klantenkring behoren. Hij is gebonden aan het beroepsgeheim en was de enige ontvanger van de e-mail. Op grond van de regeling tussen de verwerkingsverantwoordelijke en de verzekeringsagent is de agent verplicht een inbreuk in verband met persoonsgegevens zonder onredelijke vertraging aan de verwerkingsverantwoordelijke te melden. Daarom meldde de agent de fout onmiddellijk aan de verwerkingsverantwoordelijke, die het bestand corrigeerde en opnieuw verstuurde en de agent vroeg het eerste bericht te verwijderen. Volgens de bovenvermelde regeling moet de agent de verwijdering bevestigen in een schriftelijke verklaring, wat hij ook heeft gedaan. De verkregen informatie omvat geen bijzondere categorieën van persoonsgegevens, maar alleen contactgegevens en gegevens over de verzekering zelf (soort verzekering, bedrag). Na analyse van de door de inbreuk getroffen persoonsgegevens stelde de verwerkingsverantwoordelijke geen bijzondere kenmerken vast bij de personen of de verwerkingsverantwoordelijke die van invloed kunnen zijn op de omvang van de gevolgen van de inbreuk.

4.2.1 GEVAL nr. 9 — Voorafgaande maatregelen en risicobeoordeling

78. In dit geval vloeit de inbreuk niet voort uit een opzettelijke actie van een werknemer, maar uit een onopzettelijke menselijke fout als gevolg van onoplettendheid. Deze soorten inbreuken kunnen worden voorkomen of in frequentie worden verminderd door a) uitvoering van opleidings-, onderwijs- en bewustmakingsprogramma's waarbij werknemers een beter inzicht krijgen in het belang van de bescherming van persoonsgegevens, b) vermindering van bestandsuitwisseling via e-mail en in plaats daarvan gebruikmaking van bijvoorbeeld speciale systemen voor de verwerking van klantgegevens, c) dubbele controle van bestanden voordat deze worden verzonden, d) scheiding van de aanmaak en de verzending van bestanden.
79. Deze gegevensinbreuk betreft alleen de vertrouwelijkheid van de gegevens, en de integriteit en de toegankelijkheid ervan blijven intact. De gegevensinbreuk betrof slechts ongeveer twintig klanten en daarom kan de hoeveelheid getroffen gegevens als gering worden beschouwd. Verder bevatten de getroffen persoonsgegevens geen gevoelige gegevens. Het feit dat de gegevensverwerker onmiddellijk contact heeft opgenomen met de verwerkingsverantwoordelijke na kennis te hebben gekregen van de gegevensinbreuk, kan worden beschouwd als een risicobeperkende factor. (De mogelijkheid dat er gegevens naar andere verzekeringsagenten zijn verzonden, moet ook worden onderzocht en, indien bevestigd, moeten er passende maatregelen worden genomen.) Dankzij de nodige stappen die na de gegevensinbreuk zijn genomen, zal deze waarschijnlijk geen gevolgen hebben voor de rechten en vrijheden van de betrokkenen.
80. Door de combinatie van het lage aantal getroffen personen, de onmiddellijke ontdekking van de inbreuk en de maatregelen die zijn genomen om de gevolgen ervan tot een minimum te beperken, is er in dit specifieke geval geen sprake van een risico.

4.2.2 GEVAL nr. 9 — Risicobeperking en verplichtingen

81. Bovendien spelen ook andere risicobeperkende omstandigheden een rol: de agent is gebonden aan het beroepsgeheim, hij heeft het probleem zelf aan de verwerkingsverantwoordelijke gemeld en hij heeft het bestand op verzoek gewist. Bewustmaking en mogelijk opnemings van extra stappen in de controle van documenten met persoonsgegevens zullen waarschijnlijk helpen om vergelijkbare gevallen in de toekomst te voorkomen.

82. Naast het documenteren van de inbreuk overeenkomstig artikel 33, lid 5, zijn er geen andere maatregelen nodig.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	X	X

4.3 Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van interne bronnen van menselijke risico's

83. Een combinatie van de hieronder vermelde maatregelen — toegepast afhankelijk van de unieke kenmerken van het geval — moet de kans helpen verkleinen dat een vergelijkbare inbreuk zich opnieuw voordoet.

84. Aanbevolen maatregelen:

(De lijst van de volgende maatregelen is geenszins exclusief of volledig. Het doel is veeleer om ideeën voor preventie en mogelijke oplossingen aan te dragen. Elke verwerkingsactiviteit is anders en daarom moet de verwerkingsverantwoordelijke bepalen welke maatregelen het best bij de gegeven situatie passen.)

- J periodieke uitvoering van opleidings-, onderwijs- en bewustmakingsprogramma's voor werknemers over hun privacy- en beveiligingsverplichtingen en over de opsporing en melding van bedreigingen voor de beveiliging van persoonsgegevens²⁶. Ontwikkel een bewustmakingsprogramma om de werknemers te herinneren aan de meest voorkomende fouten die leiden tot inbreuken in verband met persoonsgegevens en hoe deze kunnen worden voorkomen;
- J invoering van robuuste en effectieve praktijken, procedures en systemen op het gebied van gegevensbescherming en privacy²⁷;
- J evaluatie van privacypraktijken, -procedures en -systemen om een blijvende effectiviteit te waarborgen²⁸;
- J opstellen van een adequaat beleid voor toegangscontrole en dwingen van gebruikers om de regels te volgen;
- J invoeren van methoden waarbij gebruikers moeten worden geauthenticeerd om toegang te krijgen tot gevoelige persoonsgegevens;
- J uitschakelen van het bedrijfsaccount van de gebruiker zodra de betreffende persoon het bedrijf verlaat;
- J controleren van ongebruikelijke gegevensstromen tussen de bestandserver en de werkstations van de werknemers;
- J installeren van I/O-interfacebeveiliging in de BIOS of met behulp van software die het gebruik van computerinterfaces controleert (vergrendelen of ontgrendelen, bv. USB-stick/cd/dvd enz.);
- J herzien van het toegangsbeleid voor werknemers (bv. inlogtoegang tot gevoelige gegevens en verplichten van de gebruiker om een zakelijke reden te vermelden, zodat deze beschikbaar is voor audits);
- J uitschakelen van open clouddiensten;
- J verbieden en voorkomen van toegang tot bekende open maildiensten;
- J uitschakelen van de schermafdruckfunctie in het besturingssysteem;

²⁶ Sectie 2, subsectie i), van de resolutie betreffende de rol van menselijke fouten bij inbreuken in verband met persoonsgegevens.

²⁷ Sectie 2, subsectie ii), van de resolutie betreffende de rol van menselijke fouten bij inbreuken in verband met persoonsgegevens.

²⁸ Sectie 2, subsectie iii), van de resolutie betreffende de rol van menselijke fouten bij inbreuken in verband met persoonsgegevens.

- J uitvoeren van een “clean desk”-beleid;
- J automatische vergrendeling van alle computers na een bepaalde tijd van inactiviteit;
- J gebruik van mechanismen (bv. (draadloze) token voor het inloggen op/openen van vergrendelde accounts) om snel van gebruiker te wisselen in gedeelde omgevingen;
- J gebruik van speciale systemen voor het beheren van persoonsgegevens waarbij passende mechanismen voor toegangscontrole worden toegepast en die menselijke fouten zoals het verzenden van mededelingen aan de verkeerde geadresseerde voorkomen. Het gebruik van spreadsheets en andere officedocumenten is geen passend middel om klantgegevens te beheren.

5 VERLOREN OF GESTOLEN APPARATEN EN PAPIEREN DOCUMENTEN

85. Een veel voorkomend geval is het verlies of de diefstal van draagbare apparaten. In deze gevallen moet de verwerkingsverantwoordelijke rekening houden met de omstandigheden van de verwerking, zoals het soort gegevens dat op het apparaat is opgeslagen, alsook met de onderliggende activa en de maatregelen die voorafgaand aan de inbreuk zijn genomen om een passend beveiligingsniveau te waarborgen. Al deze elementen zijn van invloed op de potentiële gevolgen van de gegevensinbreuk. De risicobeoordeling kan soms lastig zijn, omdat het apparaat niet langer beschikbaar is.
86. Deze soorten inbreuken kunnen altijd worden geclassificeerd als inbreuken op de vertrouwelijkheid. Als er echter geen back-up van de gestolen databank is gemaakt, kan het bij het soort inbreuk ook gaan om een inbreuk op de beschikbaarheid of een inbreuk op de integriteit.
87. Uit de onderstaande scenario's blijkt hoe de hierboven genoemde omstandigheden van invloed zijn op de waarschijnlijkheid en de ernst van de gegevensinbreuk.

5.1 GEVAL nr. 10: Gestolen materiaal met versleutelde persoonsgegevens

Tijdens een inbraak in een kinderdagverblijf werden twee tablets gestolen. De tablets bevatten een app met persoonsgegevens over de kinderen die het dagverblijf bezoeken. Daarbij ging het om de naam, de geboortedatum en de persoonsgegevens over het onderwijs van de kinderen. Zowel de versleutelde tablets, die op het moment van de inbraak uitgeschakeld waren, als de app waren beschermd met een sterk wachtwoord. De back-upgegevens waren daadwerkelijk en onmiddellijk beschikbaar voor de verwerkingsverantwoordelijke. Na kennisneming van de inbraak gaf het dagverblijf kort na de ontdekking van de inbraak op afstand opdracht om alle gegevens van de tablets te wissen.

5.1.1 GEVAL nr. 10 — Voorafgaande maatregelen en risicobeoordeling

88. In dit specifieke geval heeft de verwerkingsverantwoordelijke adequate maatregelen genomen om de gevolgen van een potentiële gegevensinbreuk te voorkomen en te beperken door apparaatversleuteling toe te passen, adequate wachtwoordbescherming in te voeren en een back-up te maken van de op de tablets opgeslagen gegevens. (Een lijst van aanbevolen maatregelen is te vinden in punt 5.7.)
89. Na kennisneming van een inbreuk moet de verwerkingsverantwoordelijke een beoordeling uitvoeren van de risicobron, de systemen die de gegevensverwerking ondersteunen, het soort persoonsgegevens dat bij de inbreuk betrokken is en de potentiële gevolgen van de gegevensinbreuk voor de betrokken personen. De hierboven beschreven gegevensinbreuk zou betrekking hebben gehad op de vertrouwelijkheid, beschikbaarheid en integriteit van de betrokken gegevens, maar dankzij de passende procedures van de verwerkingsverantwoordelijke voor en na de gegevensinbreuk heeft geen van deze inbreuken plaatsgevonden.

5.1.2 GEVAL nr. 10 — Risicobeperking en verplichtingen

90. De vertrouwelijkheid van de persoonsgegevens op de apparaten werd niet gecompromitteerd dankzij de sterke wachtwoordbescherming op zowel de tablets als de apps. De tablets waren zodanig geïnstalleerd dat bij het instellen van een wachtwoord ook de gegevens op het apparaat worden versleuteld. De bescherming werd nog versterkt door de poging van de verwerkingsverantwoordelijke om op afstand alles van de gestolen apparaten te wissen.
91. Dankzij de genomen maatregelen bleef de vertrouwelijkheid van de gegevens ook behouden. Bovendien zorgde de back-up ervoor dat de persoonsgegevens continu beschikbaar bleven en daarom konden er geen potentiële negatieve gevolgen optreden.
92. Het was dan ook niet waarschijnlijk dat de hierboven beschreven gegevensinbreuk een risico zou inhouden voor de rechten en vrijheden van de betrokkenen en daarom was er geen melding aan de TA of een mededeling aan de betrokkenen nodig. Deze gegevensinbreuk moet echter ook worden gedocumenteerd overeenkomstig artikel 33, lid 5.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	X	X

5.2 GEVAL nr. 11: Gestolen materiaal met niet-versleutelde persoonsgegevens

De elektronische notebook van een werknemer van een dienstverlenende onderneming werd gestolen. De gestolen notebook bevatte de voor- en achternamen, het geslacht, de adressen en de geboortedata van meer dan 100 000 klanten. Doordat het gestolen apparaat niet beschikbaar was, kon niet worden vastgesteld of er ook andere categorieën van persoonsgegevens waren getroffen. De toegang tot de harde schijf van de notebook was niet beschermd met een wachtwoord. De persoonsgegevens konden worden hersteld vanaf de beschikbare dagelijkse back-ups.

5.2.1 GEVAL nr. 11 — Voorafgaande maatregelen en risicobeoordeling

93. Er waren geen voorafgaande veiligheidsmaatregelen genomen door de verwerkingsverantwoordelijke, waardoor de op de gestolen notebook opgeslagen persoonsgegevens gemakkelijk toegankelijk waren voor de dief of anderen die het apparaat daarna in bezit kregen.
94. Deze gegevensinbreuk betreft de vertrouwelijkheid van de op het gestolen apparaat opgeslagen gegevens.
95. De notebook met de persoonsgegevens was in dit geval kwetsbaar omdat deze niet was beschermd met een wachtwoord en ook niet was versleuteld. Het gebrek aan essentiële beveiligingsmaatregelen verhoogt het risiconiveau voor de getroffen betrokkenen. Verder is het ook lastig om vast te stellen om welke betrokkenen het gaat, wat ook de ernst van de inbreuk vergroot. Het aanzienlijke aantal betrokken personen vergroot het risico, maar niettemin waren er geen bijzondere categorieën van persoonsgegevens bij de gegevensinbreuk betrokken.
96. Bij de risicobeoordeling²⁹ moet de verwerkingsverantwoordelijke rekening houden met de potentiële gevolgen en negatieve effecten van de inbreuk op de vertrouwelijkheid. Als gevolg van de inbreuk kunnen

²⁹ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

de betrokkenen het slachtoffer worden van identiteitsfraude op basis van de gegevens op het gestolen apparaat, waardoor het risico als hoog wordt beschouwd.

5.2.2 GEVAL nr. 11 — Risicobeperking en verplichtingen

97. De inschakeling van apparaatversleuteling en het gebruik van sterke wachtwoordbescherming van de opgeslagen databank hadden kunnen voorkomen dat de gegevensinbreuk een risico voor de rechten en vrijheden van de betrokkenen met zich mee zou brengen.
98. Als gevolg van deze omstandigheden moet niet alleen een melding aan de TA worden gedaan, maar ook een mededeling aan de betrokkenen.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓

5.3 GEVAL nr. 12: Gestolen papieren dossiers met gevoelige gegevens

Een papieren logboek werd gestolen uit een afkickkliniek voor drugsverslaafden. Het boek bevatte essentiële identiteits- en gezondheidsgegevens van de patiënten die in de kliniek waren opgenomen. De gegevens waren alleen op papier opgeslagen en er was geen back-up beschikbaar voor de artsen die de patiënten behandelen. Het boek was niet opgeborgen in een afgesloten lade of ruimte en de verwerkingsverantwoordelijke had geen regeling voor toegangscontrole en had ook geen andere veiligheidsmaatregelen voor de papieren documentatie.

5.3.1 GEVAL nr. 12 — Voorafgaande maatregelen en risicobeoordeling

99. Er waren geen voorafgaande veiligheidsmaatregelen genomen door de verwerkingsverantwoordelijke, waardoor de persoonsgegevens in dit boek gemakkelijk toegankelijk waren voor de persoon die het vond. Bovendien is het ontbreken van back-upgegevens door de aard van de persoonsgegevens in het boek een zeer ernstige risicofactor.
100. Dit geval dient als voorbeeld voor een gegevensinbreuk met een hoog risico. Doordat er geen passende veiligheidsmaatregelen waren genomen, zijn er gevoelige gezondheidsgegevens uit hoofde van artikel 9, lid 1, AVG verloren gegaan. Aangezien het in dit geval om een bijzondere categorie van persoonsgegevens ging, waren de potentiële risico's voor de betrokkenen groter. Hiermee moet ook rekening worden gehouden door de verwerkingsverantwoordelijke die het risico beoordeelt³⁰.
101. Deze inbreuk betreft de vertrouwelijkheid, beschikbaarheid en integriteit van de betrokken persoonsgegevens. Als gevolg van de inbreuk is het medisch beroepsgeheim doorbroken en kunnen niet-geautoriseerde derden toegang krijgen tot medische persoonsgegevens van de patiënten, wat ernstige gevolgen kan hebben voor het persoonlijke leven van de patiënt. De inbreuk op de beschikbaarheid kan ook de continuïteit van de behandeling van de patiënten verstoren. Aangezien niet kan worden uitgesloten dat er delen van de inhoud van het boek zijn veranderd/verwijderd, is de integriteit van de persoonsgegevens ook gecompromitteerd.

5.3.2 GEVAL nr. 12 — Risicobeperking en verplichtingen

102. Bij de beoordeling van de veiligheidsmaatregelen moet ook rekening worden gehouden met het soort onderliggende activa. Aangezien het patiëntenlogboek een fysiek document was, had de beveiliging ervan anders moeten worden georganiseerd dan die van een elektronisch apparaat. Pseudonimisering van de

³⁰ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

namen van de patiënten, bewaring van het boek in een beveiligd gebouw en in een afgesloten lade of ruimte en een adequate toegangscontrole met authenticatie bij het raadplegen ervan hadden de gegevensinbreuk kunnen voorkomen.

103. De hierboven beschreven gegevensinbreuk kan ernstige gevolgen hebben voor de betrokkenen; daarom zijn een melding aan de TA en een mededeling van de inbreuk aan de betrokkenen verplicht.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓

5.4 Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van verlies of diefstal van apparaten

104. Een combinatie van de hieronder vermelde maatregelen — toegepast afhankelijk van de unieke kenmerken van het geval — moet de kans helpen verkleinen dat een vergelijkbare inbreuk zich opnieuw voordoet.

105. Aanbevolen maatregelen:

(De lijst van de volgende maatregelen is geenszins exclusief of volledig. Het doel is veeleer om ideeën voor preventie en mogelijke oplossingen aan te dragen. Elke verwerkingsactiviteit is anders en daarom moet de verwerkingsverantwoordelijke bepalen welke maatregelen het best bij de gegeven situatie passen.)

- J schakel de versleutelingsfunctie van het apparaat in (zoals Bitlocker, Veracrypt of DM-Crypt);
- J gebruik een toegangscode/wachtwoord voor alle apparaten. Versleutel alle mobiele elektronische apparaten op zodanige wijze dat voor de ontsluiting een complex wachtwoord moet worden ingevoerd;
- J gebruik multifactorauthenticatie;
- J schakel de functie van zeer mobiele apparaten in waarmee deze bij verlies of zoekraken kunnen worden gelokaliseerd;
- J gebruik MDM (Mobile Device Management)-software/app en locatiebepaling. Gebruik antiverblindingsfilters. Sluit alle onbeheerde apparaten af;
- J sla indien mogelijk en passend bij de gegevensverwerking in kwestie de persoonsgegevens niet op een mobiel apparaat op, maar op een centrale backendserver;
- J is het werkstation aangesloten op de bedrijfs-LAN, maak dan een automatische back-up van de werkmappen, mits het onvermijdelijk is dat daarin persoonsgegevens worden opgeslagen;
- J gebruik een beveiligd VPN-netwerk (bv. een VPN waarbij een aparte tweefactorauthenticatiesleutel nodig is voor de totstandbrenging van een beveiligde verbinding) om mobiele apparaten op backendservers aan te sluiten;
- J verstrek fysieke sloten aan werknemers, zodat zij hun mobiele apparaten fysiek kunnen beveiligen wanneer deze zonder toezicht worden achtergelaten;
- J passende regeling voor apparaatgebruik buiten het bedrijf;
- J passende regeling voor apparaatgebruik binnen het bedrijf;
- J gebruik MDM (Mobile Device Management)-software/app en schakel de functie Wissen op afstand in;
- J gebruik gecentraliseerd apparaatbeheer met minimumrechten voor de eindgebruikers om software te installeren;
- J installeer fysieke toegangscontroles;
- J sla gevoelige informatie niet op mobiele apparaten of harde schijven op. Als het nodig is om toegang te krijgen tot het interne systeem van het bedrijf, moet gebruik worden gemaakt van de reeds vermelde beveiligde kanalen.

6 VERKEERDE ADRESSERING

106. De risicobron is ook in dit geval een interne menselijke fout. Hier is de inbreuk echter niet het gevolg van een kwaadwillige handeling, maar van onoplettendheid. Nadat de inbreuk heeft plaatsgevonden, kan de verwerkingsverantwoordelijke weinig uitrichten. Preventie is in deze gevallen dus nog belangrijker dan bij andere soorten inbreuken.

6.1 GEVAL nr. 13: Fout bij bezorging per post

Bij een detailhandelsbedrijf werden twee bestellingen voor schoenen ingepakt. Door een menselijke fout werden twee pakbonnen verwisseld, met als gevolg dat beide producten en de bijbehorende pakbonnen naar de verkeerde persoon werden gestuurd. Dit betekent dat de twee klanten elkaars bestellingen hebben ontvangen, met inbegrip van de pakbonnen met de persoonsgegevens. Na kennisneming van de inbreuk heeft de verwerkingsverantwoordelijke de bestellingen teruggeroepen en naar de juiste ontvangers gestuurd.

6.1.1 GEVAL nr. 13 — Voorafgaande maatregelen en risicobeoordeling

107. De bonnen bevatten de persoonsgegevens die nodig zijn voor een succesvolle levering (naam, adres, alsook het gekochte artikel en de prijs ervan). Het is belangrijk om vast te stellen hoe de menselijke fout überhaupt heeft kunnen gebeuren en of deze op enigerlei wijze had kunnen worden voorkomen. In het beschreven specifieke geval is het risico laag, aangezien het niet gaat om bijzondere categorieën van persoonsgegevens of om andere gegevens waarvan het misbruik aanzienlijke negatieve gevolgen zou kunnen hebben, de inbreuk niet het gevolg is van een systeemfout van de verwerkingsverantwoordelijke en er slechts twee personen bij betrokken zijn. Er konden geen negatieve gevolgen voor de personen worden vastgesteld.

6.1.2 GEVAL nr. 13 — Risicobeperking en verplichtingen

108. De verwerkingsverantwoordelijke moet zorgen voor gratis retournering van de artikelen en de bijbehorende bonnen en moet ook de verkeerde ontvangers vragen om alle eventuele kopieën van de bonnen met de persoonsgegevens van de andere persoon te vernietigen/verwijderen.
109. Ook al vormt de inbreuk zelf geen groot risico voor de rechten en vrijheden van de getroffen personen en is een mededeling aan de betrokkenen overeenkomstig artikel 34 AVG dus niet verplicht, een mededeling van de inbreuk aan hen is niet te voorkomen, aangezien hun medewerking nodig is om het risico te beperken.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	X	X

6.2 GEVAL nr. 14: Bij vergissing per e-mail verzonden zeer vertrouwelijke persoonsgegevens

De afdeling Werkgelegenheid van een bureau van een overheidsinstantie heeft een e-mailbericht — over toekomstige opleidingen — verstuurd aan de personen die als werkzoekend in haar systeem zijn geregistreerd. Een document met de persoonsgegevens van al deze werkzoekenden (naam, e-mailadres, postadres, socialezekerheidsnummer) werd per vergissing bij deze e-mail gevoegd. Het aantal getroffen personen bedraagt meer dan 60 000. Het bureau nam vervolgens contact op met alle ontvangers en vroeg hen het vorige bericht te verwijderen en de daarin opgenomen informatie niet te gebruiken.

6.2.1 GEVAL nr. 14 — Voorafgaande maatregelen en risicobeoordeling

110. Voor het versturen van dergelijke berichten hadden strengere regels moeten worden toegepast. Overwogen moet worden om aanvullende controlemechanismen in te voeren.

111. Doordat het aantal getroffen personen aanzienlijk is en het gaat om hun socialezekerheidsnummer, samen met andere, meer essentiële persoonsgegevens, neemt het risico, dat als hoog kan worden aangemerkt, nog verder toe³¹. De eventuele verspreiding van de gegevens door een of meer van de ontvangers kan door de verwerkingsverantwoordelijke niet worden beheerst.

6.2.2 GEVAL nr. 14 — Risicobeperking en verplichtingen

112. Zoals eerder vermeld, zijn de middelen om de risico's van een vergelijkbare inbreuk effectief te verminderen beperkt. Hoewel de verwerkingsverantwoordelijke om verwijdering van het bericht vroeg, kan hij de ontvangers niet dwingen om dat te doen en kan hij er dus ook niet zeker van zijn dat zij aan het verzoek voldoen.
113. De uitvoering van alle drie de hieronder beschreven maatregelen zou in een geval als dit vanzelfsprekend moeten zijn.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓

6.3 GEVAL nr. 15: Bij vergissing per e-mail verzonden persoonsgegevens

Een lijst van deelnemers aan een vijfdaagse cursus juridisch Engels in een hotel is bij vergissing verstuurd aan 15 voormalige deelnemers aan de cursus in plaats van aan het hotel. De lijst bevat namen, e-mailadressen en voedselvoorkeuren van de 15 deelnemers. Slechts twee deelnemers hebben hun voedselvoorkeur ingevuld en aangegeven dat zij lactose-intolerant zijn. Geen van de deelnemers heeft een beschermde identiteit. De verwerkingsverantwoordelijke ontdekt de fout onmiddellijk na het versturen van de lijst en informeert de ontvangers over de fout en vraagt hen de lijst te verwijderen.

6.3.1 GEVAL nr. 15 — Voorafgaande maatregelen en risicobeoordeling

114. Voor het versturen van berichten met persoonsgegevens hadden strenge regels moeten worden toegepast. Overwogen moet worden om aanvullende controlemechanismen in te voeren.
115. De risico's als gevolg van de aard, de gevoeligheid, het volume en de context van de persoonsgegevens zijn laag. De persoonsgegevens omvatten gevoelige gegevens over de voedselvoorkeur van twee van de deelnemers. Ook al gaat het bij de informatie dat iemand lactose-intolerant is om gezondheidsgegevens, het risico dat deze gegevens op een schadelijke manier worden gebruikt, moet als relatief laag worden beschouwd. Hoewel in het geval van gegevens over gezondheid doorgaans wordt aangenomen dat de inbreuk waarschijnlijk een hoog risico voor de betrokkene inhoudt³², kan er tegelijkertijd in dit specifieke geval geen risico worden vastgesteld dat de inbreuk tot lichamelijke, materiële of immateriële schade voor de betrokkene leidt als gevolg van de ongeoorloofde openbaarmaking van informatie over lactose-intolerantie. In tegenstelling tot enkele andere voedselvoorkeuren kan lactose-intolerantie gewoonlijk niet in verband worden gebracht met religieuze of levensbeschouwelijke overtuigingen. De hoeveelheid gecompromitteerde gegevens en het aantal getroffen betrokkenen zijn eveneens erg laag.

³¹ Zie voor richtsnoeren over verwerkingen die “waarschijnlijk een hoog risico inhouden” voetnoot 10 hierboven.

³² Zie Richtsnoeren WP 250, blz. 23.

6.3.2 GEVAL nr. 15 — Risicobeperking en verplichtingen

116. Samenvattend kan worden gesteld dat de inbreuk geen significante gevolgen had voor de betrokkenen. Het feit dat de verwerkingsverantwoordelijke onmiddellijk contact met de ontvangers heeft opgenomen nadat hij kennis had gekregen van de fout, kan als risicobeperkende factor worden beschouwd.
117. Als een e-mail aan een onjuiste/onrechtmatige ontvanger wordt verzonden, wordt aanbevolen dat de verwerkingsverantwoordelijke vervolgens een BCC-mail met een verontschuldiging aan de onbedoelde ontvangers stuurt waarin hij opdracht geeft de inbreukmakende e-mail te verwijderen en de ontvangers erop wijst dat zij niet het recht hebben de aan hen meegedeelde e-mailadressen verder te gebruiken.
118. Hierdoor was het niet waarschijnlijk dat deze gegevensinbreuk een risico zou inhouden voor de rechten en vrijheden van de betrokkenen en daarom was er geen melding aan de TA of een mededeling aan de betrokkenen nodig. Deze gegevensinbreuk moet echter ook worden gedocumenteerd overeenkomstig artikel 33, lid 5.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	X	X

6.4 GEVAL nr. 16: Fout bij bezorging per post

Een verzekeringsgroep biedt autoverzekeringen aan. Daartoe verstuurt de groep regelmatig aangepaste premiepolissen per post. Naast de naam en het adres van de polishouder bevat de brief het kentekennummer zonder onleesbaar gemaakte cijfers, de verzekeringspremies voor het lopende en het volgende verzekeringsjaar, de geschatte jaarlijks afgelegde afstand en de geboortedatum van de polishouder. Niet opgenomen zijn gezondheidsgegevens in de zin van artikel 9 AVG, betalingsgegevens (bankgegevens), economische en financiële gegevens.

De brieven worden verpakt door geautomatiseerde enveloppeermachines. Door een mechanische fout worden twee brieven voor verschillende polishouders in één envelop gedaan en per briefpost aan één polishouder verzonden. De polishouder opent de brief thuis en bekijkt zijn correct bezorgde brief evenals de verkeerd bezorgde brief voor een andere polishouder.

6.4.1 GEVAL nr. 16 — Voorafgaande maatregelen en risicobeoordeling

119. De verkeerd bezorgde brief bevat de naam, het adres, de geboortedatum, het niet onleesbaar gemaakte kentekennummer en de classificatie van de verzekeringspremie voor het lopende en het volgende jaar. De gevolgen voor de getroffen persoon moeten als middelgroot worden beschouwd, aangezien er niet openbaar beschikbare informatie, zoals de geboortedatum en niet onleesbaar gemaakte kentekennummers, en gegevens over de verhoging van de verzekeringspremies aan de onrechtmatige ontvanger zijn verstrekt. De waarschijnlijkheid van misbruik van deze gegevens wordt ingeschat als laag tot middelgroot. Hoewel veel ontvangers de ten onrechte ontvangen brief waarschijnlijk bij het afval doen, kan in individuele gevallen niet geheel worden uitgesloten dat de brief op sociale netwerken wordt verspreid of dat contact met de polishouder wordt opgenomen.

6.4.2 GEVAL nr. 16 — Risicobeperking en verplichtingen

120. De verwerkingsverantwoordelijke moet het originele document op zijn eigen kosten laten terugsturen. De verkeerde ontvanger moet er ook op worden gewezen dat hij/zij de gelezen informatie niet mag misbruiken.
121. Het zal waarschijnlijk nooit mogelijk zijn om bij een massamailing met behulp van volledig geautomatiseerde machines een fout bij de postbezorging geheel te voorkomen. Als de frequentie toeneemt, moet echter worden gecontroleerd of de enveloppeermachines correct zijn ingesteld en onderhouden dan wel of een ander structureel probleem tot een dergelijke inbreuk leidt.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	X

6.5 Organisatorische en technische maatregelen ter voorkoming/beperking van de gevolgen van verkeerde adressering

122. Een combinatie van de hieronder vermelde maatregelen — toegepast afhankelijk van de unieke kenmerken van het geval — moet de kans helpen verkleinen dat een vergelijkbare inbreuk zich opnieuw voordoet.

123. Aanbevolen maatregelen:

(De lijst van de volgende maatregelen is geenszins exclusief of volledig. Het doel is veeleer om ideeën voor preventie en mogelijke oplossingen aan te dragen. Elke verwerkingsactiviteit is anders en daarom moet de verwerkingsverantwoordelijke bepalen welke maatregelen het best bij de gegeven situatie passen.)

- J vaststellen van exacte normen — zonder ruimte voor interpretatie — voor het versturen van brieven/e-mails;
- J adequate opleiding voor het personeel over het versturen van brieven/e-mails;
- J bij het versturen van e-mails aan meerdere ontvangers worden deze standaard vermeld in het "BCC"-veld;
- J extra bevestiging is vereist bij het versturen van e-mails aan meerdere ontvangers die niet in het "BCC"-veld zijn vermeld;
- J toepassing van het vierogenprincipe;
- J automatische in plaats van handmatige adressering, waarbij de gegevens afkomstig zijn uit een beschikbare en geactualiseerde databank. Het geautomatiseerde adresseringssysteem moet regelmatig worden gecontroleerd op verborgen fouten en onjuiste instellingen;
- J toepassing van berichtvertraging (bv. het bericht kan worden verwijderd/bewerkt binnen een bepaalde tijd na het klikken op de drukknop);
- J uitschakelen van automatisch aanvullen bij het intypen van e-mailadressen;
- J bewustmakingssessies over de meest voorkomende fouten die leiden tot een inbreuk in verband met persoonsgegevens;
- J trainingssessies en handboeken over de afhandeling van incidenten die leiden tot een inbreuk in verband met persoonsgegevens en over de vraag wie moet worden geïnformeerd (de DPO moet erbij worden betrokken).

7 ANDERE GEVALLEN — SOCIAL ENGINEERING

7.1 GEVAL nr. 17: Identiteitsdiefstal

Het contactcentrum van een telecommunicatiebedrijf ontvangt een telefoontje van iemand die zich voordoet als een klant. De veronderstelde klant vraagt het bedrijf om het e-mailadres te wijzigen waarnaar de factureringsinformatie vanaf dat moment moet worden verstuurd. De werknemer van het contactcentrum valideert de identiteit van de klant door bepaalde persoonsgegevens te vragen, zoals vastgesteld in de procedures van het bedrijf. De beller geeft het juiste antwoord op de vraag naar het fiscaal nummer en het postadres van de klant (omdat hij toegang had tot deze gegevens). Na de validatie voert de telefonist de gevraagde wijziging uit en vanaf dat moment wordt de factureringsinformatie naar het nieuwe e-mailadres verstuurd. De procedure voorziet niet in een mededeling aan de vorige e-mailcontactpersoon. De maand daarna neemt de rechtmatige klant contact op met het bedrijf en vraagt hij waarom hij geen factuur op zijn e-mailadres ontvangt. Hij ontkent te hebben gebeld en om wijziging van het e-mailcontactadres te hebben gevraagd. Naderhand realiseert het bedrijf zich dat de informatie naar een onrechtmatige gebruiker is gestuurd en draait het de wijziging terug.

7.1.1 GEVAL nr. 17 — Risicobeoordeling, risicobeperking en verplichtingen

124. Dit geval dient als voorbeeld van het belang van voorafgaande maatregelen. Vanuit risico-oogpunt brengt de inbreuk een hoog risico met zich mee³³, aangezien factureringsgegevens informatie kunnen bevatten over het privéleven van de betrokkene (bv. gewoonten, contacten) en kunnen leiden tot materiële schade (bv. stalking, risico voor de fysieke integriteit). De tijdens deze aanval verkregen persoonsgegevens kunnen ook worden gebruikt om de overname van het account bij deze organisatie te vergemakkelijken of om gebruik te maken van verdere authenticatiemaatregelen bij andere organisaties. Gezien deze risico's moet de "juiste" authenticatiemaatregel voldoen aan hoge eisen, afhankelijk van de persoonsgegevens die als gevolg van authenticatie kunnen worden verwerkt.
125. De verwerkingsverantwoordelijke moet daarom zowel een melding aan de TA als een mededeling aan de betrokkene doen.
126. De bestaande validatieprocedure moet duidelijk worden verfijnd in het licht van dit geval. De voor de authenticatie toegepaste methoden waren niet toereikend. De kwaadwillende partij kon zich als de beoogde gebruiker voordoen door gebruik te maken van openbaar beschikbare informatie en informatie waartoe zij op andere wijze toegang had.
127. Het gebruik van dit soort statische kennisgebaseerde authenticatie (waarbij het antwoord niet verandert en waarbij de informatie niet "geheim" is, zoals wel het geval zou zijn bij een wachtwoord) wordt niet aanbevolen.
128. In plaats daarvan moet de organisatie een vorm van authenticatie gebruiken die zou leiden tot een hoge mate van vertrouwen dat de geauthenticeerde gebruiker de beoogde persoon is, en niet iemand anders. De invoering van een buiten de band vallende multifactorauthenticatiemethode zou het probleem oplossen, bijvoorbeeld verificatie van de wijzigingsaanvraag door een bevestigingsverzoek aan de vorige contactpersoon te sturen of door extra vragen toe te voegen en informatie te vragen die alleen zichtbaar is op de vorige facturen. Het is de verantwoordelijkheid van de verwerkingsverantwoordelijke om te bepalen

³³ Zie voor richtsnoeren over verwerkingen die "waarschijnlijk een hoog risico inhouden" voetnoot 10 hierboven.

welke maatregelen moeten worden ingevoerd, aangezien hij het best op de hoogte is van de bijzonderheden en vereisten van de interne bedrijfsvoering.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓

7.2 GEVAL nr. 18: Exfiltratie van e-mail

Een hypermarktketen ontdekte drie maanden na de configuratie dat enkele e-mailaccounts waren veranderd en dat er regels waren gemaakt zodat elke e-mail met bepaalde uitdrukkingen (bv. “factuur”, “betaling”, “bankoverschrijving”, “creditcardauthenticatie”, “bankgegevens”) naar een niet gebruikte map zou worden verplaatst en ook naar een extern e-mailadres zou worden doorgestuurd. Op dat moment was er ook al een social engineering-aanval uitgevoerd, dat wil zeggen dat de aanvaller, die zich voordeed als een leverancier, de bankgegevens van die leverancier in zijn eigen bankgegevens had laten veranderen. Ten slotte waren er op dat moment al diverse valse facturen met de nieuwe bankgegevens verstuurd. Het monitoringsysteem van het e-mailplatform gaf uiteindelijk een waarschuwing met betrekking tot de mappen. Het bedrijf kon om te beginnen al niet vaststellen hoe de aanvaller toegang tot de e-mailaccounts kon krijgen, maar veronderstelde dat een geïnfecteerde e-mail verantwoordelijk was voor het geven van toegang tot de gebruikersgroep die met de betalingen was belast.

Doordat het doorsturen van e-mails was gebaseerd op zoekwoorden, ontving de aanvaller informatie over 99 werknemers: naam en salaris over een bepaalde maand met betrekking tot 89 betrokkenen, en naam, burgerlijke staat, aantal kinderen, salaris, werkuren en overige informatie over de salarisafrekening van tien werknemers wier contract was beëindigd. De verwerkingsverantwoordelijke informeerde alleen de tien werknemers die tot de laatste groep behoren.

7.2.1 GEVAL nr. 18 — Risicobeoordeling, risicobeperking en verplichtingen

129. Ook al was de aanvaller vermoedelijk niet van plan om persoonsgegevens te verzamelen, de inbreuk in verband met persoonsgegevens houdt waarschijnlijk een hoog risico in voor de rechten en vrijheden van natuurlijke personen, aangezien de inbreuk zou kunnen leiden tot zowel materiële schade (bv. financiële verliezen) als immateriële schade (bv. identiteitsdiefstal of -fraude) of de gegevens zouden kunnen worden gebruikt om andere aanvallen (bv. phishing) te vergemakkelijken. Daarom moet de inbreuk worden meegedeeld aan alle 99 werknemers en niet alleen aan de 10 werknemers wier salarisgegevens werden gelekt.
130. Na kennisneming van de inbreuk heeft de verwerkingsverantwoordelijke een wachtwoordwijziging voor de gecompromitteerde accounts afgedwongen, het verzenden van e-mails naar het e-mailaccount van de aanvaller geblokkeerd, het door de aanvaller voor zijn of haar acties gebruikte e-mailadres doorgegeven aan de dienstverlener, de door de aanvaller ingestelde regels verwijderd en de waarschuwingen van het monitoringsysteem verfijnd om een waarschuwing te geven zodra een automatische regel wordt gemaakt. Een andere oplossing zou zijn dat de verwerkingsverantwoordelijke de gebruikers het recht ontnemt om doorstuurregels in te stellen en dit alleen op verzoek laat doen door het IT-serviceteam of dat de verwerkingsverantwoordelijke een beleid invoert waarbij de gebruikers de op hun account ingestelde regels in onderdelen waar financiële gegevens worden verwerkt eenmaal per week of vaker moeten controleren en rapporteren.

131. Het feit dat een inbreuk kon plaatsvinden en zo lang onontdekt bleef en het feit dat social engineering op langere termijn had kunnen worden gebruikt om meer gegevens te veranderen, hebben aanzienlijke problemen in het IT-beveiligingssysteem van de verwerkingsverantwoordelijke aan het licht gebracht. Deze problemen moeten onmiddellijk worden aangepakt, bijvoorbeeld door de nadruk te leggen op automatiseringsevaluaties en veranderingscontroles, incidentdetectie en responsmaatregelen. Verwerkingsverantwoordelijken die gevoelige gegevens, financiële informatie enz. verwerken, hebben een grotere verantwoordelijkheid om voor een adequate gegevensbeveiliging te zorgen.

Maatregelen die op grond van de vastgestelde risico's noodzakelijk zijn		
Interne documentatie	Melding aan de TA	Mededeling aan de betrokkenen
✓	✓	✓