Grondslag beveiligingsplan bevoegd aftappen

Datum: 22 november 2022
Versie: 2.1

NBIP nationale beheersorganisatie internet providers

Wie is NBIP

De Nationale Beheersorganisatie Internet Providers (NBIP) heeft de missie om telecomaanbieders en internet service providers (ISP's) te ontzorgen door hen diensten te bieden die efficiënt te exploiteren zijn. Deelnemers kunnen dure faciliteiten die ze niet vaak nodig hebben gezamenlijk via NBIP gebruiken. De kosten voor deelnemers houden we laag, door apparatuur/verbindingen in te zetten waar nodig. Ook helpt NBIP deelnemers te voldoen aan wettelijke verplichtingen, zoals aftapbaarheid, loket voor vorderingen, beveiligingsplannen en het opzetten van een CIOT levering. Hierdoor kunnen deelnemers van NBIP veilig hun diensten aan hun eindgebruikers aanbieden.

Door haar rol als onafhankelijke kennisorganisatie draagt NBIP bij aan de continuïteit en integriteit van de diensten die partijen via de digitale infrastructuur aanbieden. Kennis delen en vermeerderen zijn een van de speerpunten. Dit doen wij door:

- Deelname aan allerlei overlegorganen.
- Deelname aan en aansturing van projecten op DDoS-gebied.
- Deelnemers en belangstellenden te informeren over relevante ontwikkelingen.
- In toenemende mate een algemene rol op het gebied van veiligheid en integriteit tussen de overheid, internetgemeenschap en deelnemers op ons te neme

NBIP richt zich op groei in de diepte (iedereen) en breedte (diensten). Het not-for-profit karakter en onafhankelijke structuur van NBIP zorgen ervoor dat groei niet ten koste van alles gaat. Ook zijn we voortdurend op zoek naar vernieuwingen en zijn we diensten aan het ontwikkelen die passen bij de genoemde missie en voor zoveel mogelijk telecomaanbieders en internet service providers (ISP's) interessant zijn. Voor meer informatie, zie www.nbip.nl.

Waarom een beveiligingsplan?

Telecomaanbieders vallen onder de Telecomwet en zijn derhalve ook gehouden aan een groot aantal regels en wetten. De gehele telecomwet kunt u hier nalezen.

Wanneer u deze wet helemaal heeft uitgeplozen zult u tot de conclusie zijn gekomen dat er vele verplichtingen en regels op u van kracht zijn, ook weet u nu dat 2 verplichte beveiligingsplannen erg belangrijk zijn en zelf verplicht aanwezig en up to date moeten zijn binnen uw organisatie. Dit handboek gaat over 1 van die 2 beveiligingsplannen te weten het beveiligingsplan in het kader van het Besluit Beveiliging Telecom Gegevens (Bbgt).

Elke aanbieder* moet dus 2 plannen hebben, te weten:

- Beveiligingsplan hoofdstuk 13 Telecomwet. (Bbgt) (zie dit handboek)
- Beveiligingsplan hoofdstuk 11a Telecomwet (Het oude continuïteitsplan)

*Welke aanbieders moeten zich bij ACM registreren en bent u wel een aanbieder? Klik op deze link voor antwoorden op de meest gestelde vragen rond dit onderwerp.

Wie kan telecom-gegevens opvragen?

Voor we van start gaan met het maken van het beveiligingsplan, is het wel fijn te weten met wie u te maken kunt krijgen. De kans dat een politieagent bij u aan de deur komt met een vordering is klein, maar ook die mogelijkheid moet u meenemen in de uitwerking van uw beveiligingsplan.

Wie zit er aan de balie en mag die persoon de vorderingen zien en hoe gaat de vordering daarna verder in uw organisatie. Het oude postvak bij de balie is in dit kader dan ook geen werkbare optie en daarom moet u ook die route van een vordering goed in kaart brengen. De meeste vorderingen worden digitaal aan u opgelegd. Spoed-vorderingen kunnen ook per telefoon worden gedaan. Er zijn dus veel personen bevoegd tot het opleggen van een vordering.

De bevoegdheden van de opsporingsdiensten zijn voornamelijk ondergebracht in het Wetboek voor Strafvordering, Boek I, artikelen 126m tot en met 126nb. Net als de inlichtingendiensten mogen opsporingsdiensten, zoals de politie, verscheidene vormen van online dataverkeer aftappen en analyseren. Ook de politie werkt echter onder strikte voorwaarden. Zo mag de politie alleen aftappen als er verdenking is van een misdrijf dat een ernstige inbreuk op de rechtsorde vormt en waarop een gevangenisstraf van meer dan vier jaar staat. Voldoet het doelwit hieraan, dan moet de politie toestemming vragen van een rechter-commissaris. De daadwerkelijke tap-periode mag niet langer dan vier weken duren. Verlenging is mogelijk, maar alleen met toestemming van de officier van justitie. Anders dan de inlichtingendiensten mag de politie de ingewonnen gegevens tot dertig jaar bewaren.

Daarnaast maakt ook de politie gebruik van het CIOT om de actuele gebruikersgegevens te achterhalen.

Lastgevers:
Wie kan u dwingen gegevens te leveren?

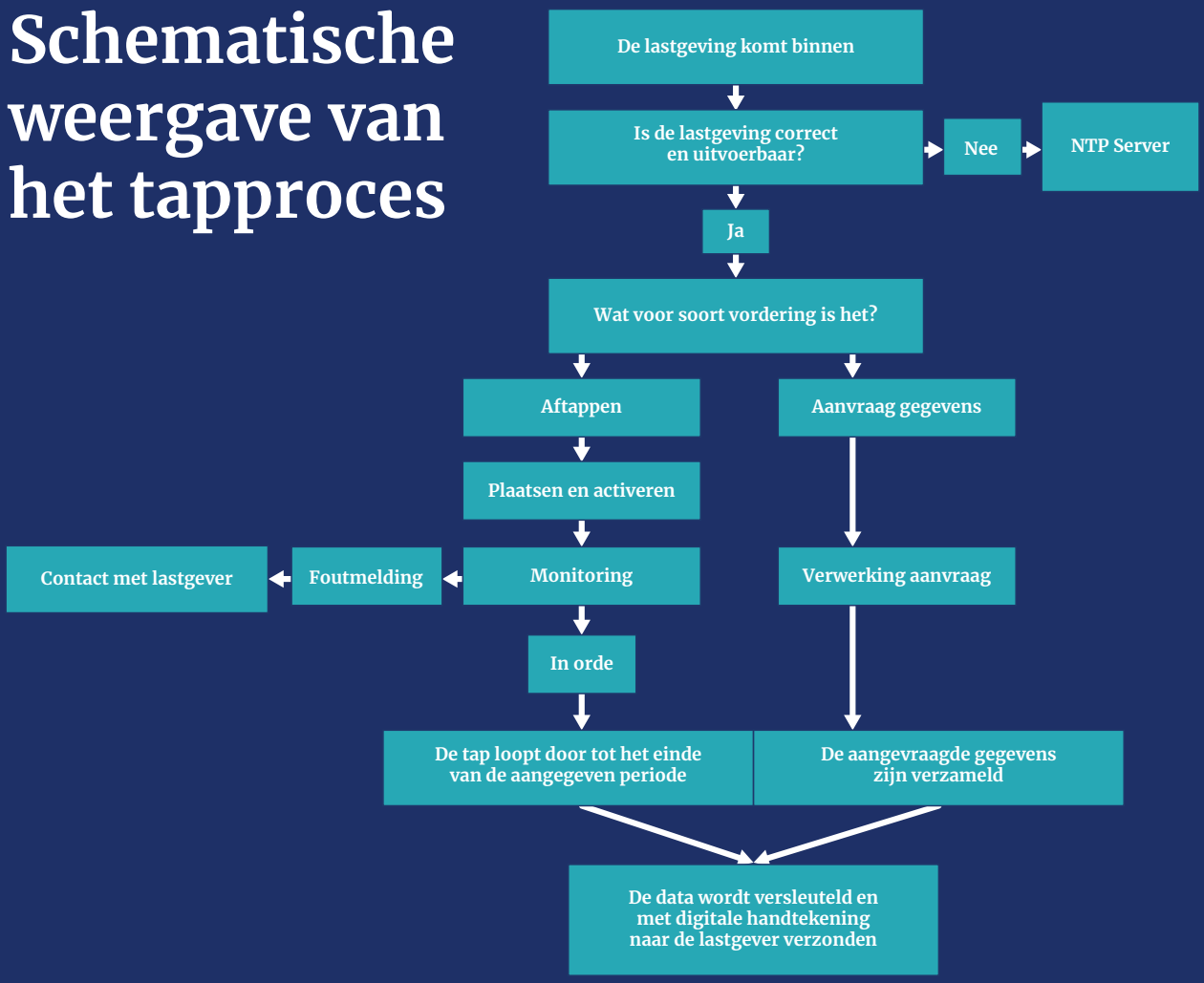
De officier van justitie of de korpschef voor zijn korps, dan wel door het hoofd van een andere opsporingsdienst voor zijn dienst aangewezen opsporingsambtenaar;

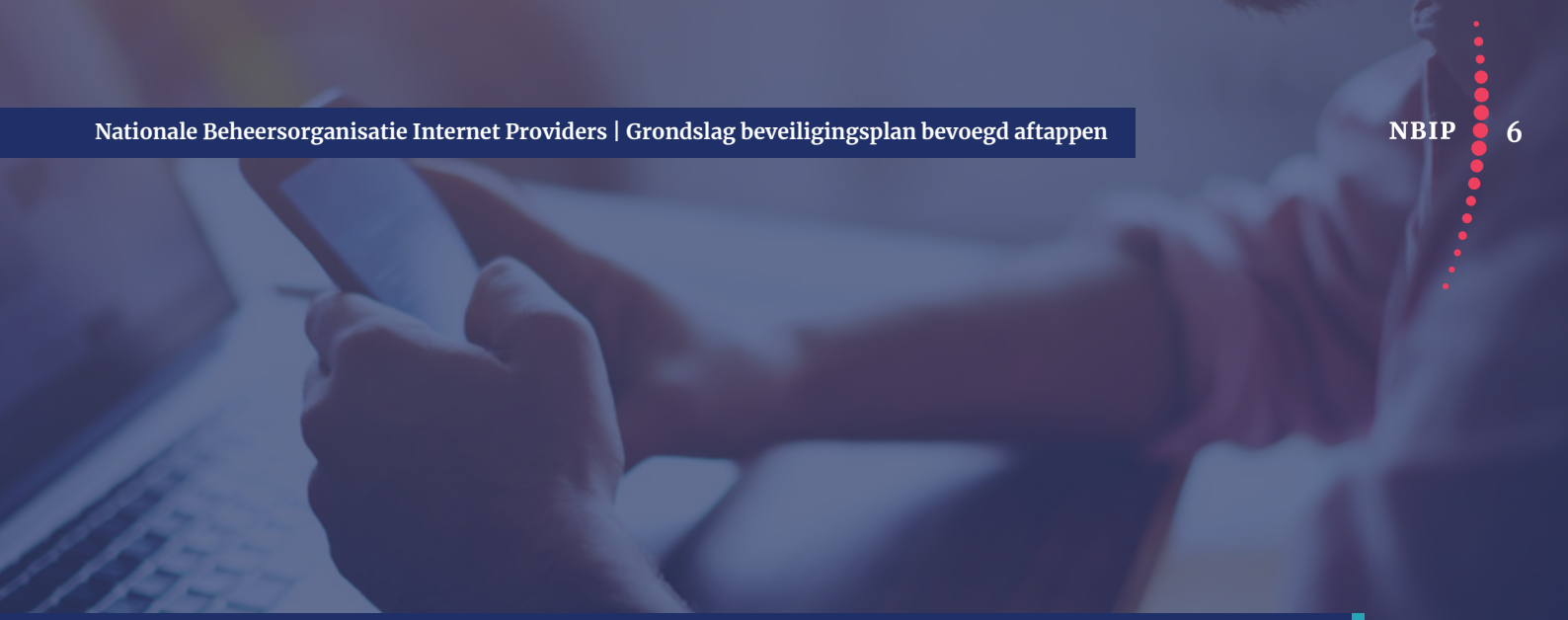
Het hoofd van de Algemene Inlichtingen- en Veiligheidsdienst, of de door hem aangewezen ambtenaar;

Het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst, of de door hem aangewezen ambtenaar (www.aivd.nl/onderwerpen/gegevens-van-communicatiediensten)

www.om.nl/onderwerpen/beleidsregels/aanwijzingen/opsporing---politie/aanwijzing-opsporingsbevoegdheden-2014a009

Schematische weergave van het tapproces





Samenvatting Bbgt

Beveiligingsplan Bbgt beschrijft dus hoe een aanbieder omgaat met de uitvoering en beveiliging van formele, vanuit de overheid opgelegde, tapverzoeken en bevelen. Voorheen noemde de overheid dit "beveiligingsplan hoofdstuk 13 Telecomwet" een beveiligingsplan. Tegenwoordig wordt ook vaak de afkorting Bbgt (Besluit beveiliging gegevens Telecommunicatie) gebruikt. (dit handboek).

In Jip en Janneke taal: Hoe gaat uw organisatie om met tapbevelen, Wie krijgt deze vorderingen in te zien. Wie kan zien wat er met die vorderingen en taps aan de hand is, is alles op basis van onderbuik en vertrouwen geregeld of neemt de organisatie de vorderingen en taps serieus en is alles ingericht en geborgd op veiligheid en extreme vertrouwelijkheid van deze gegevens? Dit is waar de Bbgt over gaat.

Meer specifiek en ten aanzien van bevoegd tappen zijn er zoals beschreven in de telecomwet eisen gesteld aan de beveiliging van gegevens. Deze zijn beschreven in het Besluit beveiliging telecom gegevens ook wel bekend als de Bbgt. (verder te noemen Bbgt plan)

www.wetten.overheid.nl/jci1.3:c:BWBR0015808&z=2018-05-01&g=2018-05-01

U heeft al een ISO 27001 certificaat?

NBIP adviseert los van een eventueel aanwezige ISO 27001 certificaat toch elke deelnemer om beveiligingsplan hoofdstuk 13 telecomwet (Bbgt) up-to-date te maken en door te voeren in de gehele organisatie. Deelnemers die een ISO 27001 certificering bezitten zijn niet uitgesloten van deze plannen maar hebben wel een voordeel ten opzichte van niet gecertificeerde deelnemers, omdat veel onderdelen van het ISO-plan gebruikt kunnen worden in uw Bbgt beveiligingsplan.

Mits zeer duidelijk beschreven, mag er naar onderdelen uit de ISO-plannen worden verwezen in het op te stellen beveiligingsplan. NBIP adviseert niet alleen te verwijzen maar ook een kopie op te nemen van de artikelen uit de ISO-plannen in het Bbgt beveiligingsplan. Beveiligingsplan hoofdstuk 13 Telecomwet (Bbgt) moet ook herkenbaar en up-to-date binnen de organisatie van de aanbieder te vinden zijn. Enkel verwijzingen naar andere plannen, zoals een ISO-certificering, zullen tijdens een inspectie van het AT niet volstaan.

Uw beveiligingsplan:

In dit hoofdstuk geeft NBIP u de basisopzet voor een Beveiligingsplan als beschreven in hoofdstuk 13 van de Telecomwet & het latere Bbgt. Telecomwet artikel 13.5 verplicht elke aanbieder al tot het handelen conform een beveiligingsplan en voor de helderheid heeft de wetgever dat artikel verduidelijkt met het Besluit beveiliging telecom gegevens. Artikel 13,5 blijft ook van kracht maar met het uitbrengen van het Bbgt is het hebben van een deugdelijk beveiligingsplan verduidelijkt.

Telecommunicatiewet geraadpleegd op 14-07-2022. Geldend van 01-05-2022 t/m heden

wetten.overheid.nl/jci1.3:c:BWBR0009950&hoofdstuk=13&z=2018-05-01&g=2018-05-01

Besluit Beveiliging Telecom Gegevens (Bbgt)
Het gehele Besluit beveiliging telecom gegevens bevat 10 hoofdstukken die elk relevante informatie bevatten maar niet elk op zich in het beveiligingsplan hoeven te worden opgenomen.

wetten.overheid.nl/jci1.3:c:BWBR0015808&z=2018-05-01&g=2018-05-01

De belangrijkste onderdelen die wel in uw plan moeten zijn opgenomen heeft NBIP in deze template genoteerd voor u.

Hoe moet uw plan er dan uitzien zult u zich afvragen, het antwoord daarop is lastig te geven maar er zijn wel enkele vuistregels die u kunt hanteren om tot een goed plan te komen.

Vuistregels voor opstellen het beveiligingsplan Bbgt :
Vuistregel 1: Neem de moeite het formele Bbgt besluit zelf even door te nemen en maak notities van de onderdelen die u opvallen als lastig/ moeilijk of onduidelijk.

www.wetten.overheid.nl/jci1.3:c:BWBR0015808&z=2018-05-01&g=2018-05-01

Vuistregel 2: Gebruik de onderstaande template om regel voor regel te snappen wat de wetgever u vraagt, maak ook hier aantekeningen die betrekking hebben op uw organisatie en ook als er regels onduidelijk zijn. Met een klein geluk zijn de NBIP tips en de door u uitgevoerde scan op de 10 hoofdstukken Bbgt samen een duidelijk antwoord op uw vraag.

Vuistregel 3: Begin gewoon met schrijven onder de verschillende regels in deze template over hoe een en ander bij u in de organisatie is ingeregeld.

Vuistregel 4: De opmaak komt als laatste aan bod, De inhoudelijke dekking en de en logische opbouw van uw eigen Bbgt plan zijn wanneer u de template volgt alvast in orde.

Vuistregel 5: Beschrijf niet hoe u het zou willen hebben binnen uw organisatie maar beschrijf hoe het nu is geregeld en maak aan de hand van uw eigen afwegingen een actielijst om in een latere fase die zaken organisatorisch in orde te maken en aan te passen in uw definitieve Bbgt plan.

Het is natuurlijk niet te bedoeling onze template als invuloefening te gebruiken maar wel als leidraad voor uw eigen plan kunt gebruiken. NBIP heeft de template ook in Word Formaat voor u beschikbaar, stuurt u hiervoor een mail naar bureau@connect.nbip.nl

Template Bbgt plan:

Hieronder heeft NBIP voor u onderdeel voor onderdeel de relevante onderwerpen voor uw eigen beveiligingsplan in een logische volgorde bij elkaar gezet. Lees wat de wetgever schrijft en bedenk wat de wetgever u vraagt. Schrijf dat op.

Artikel 1:

Dit artikel is een begripsdefinitie welke geen onderdeel hoeft te zijn van uw beveiligingsplan, een verklarende woordenlijst bij uw beveiligingsplan is wel aan te raden maar op zich geen verplichting.

Artikel 2:

Schrijf op hoe u de administratie rond personeel en aanraking met gevoelige gegevens heeft ingeregeld.

2.1 Beveiligingseis algemeen

Er is een functionaris, belast met het toezicht op de uitvoering en naleving van de beveiligingsmaatregelen. De functionaris voert daartoe regelmatig controles uit en legt de resultaten daarvan vast.

NBIP-tip: Neem een rooster met naam en rugnummers op van het bevoegde personeel. U kunt ook verwijzen naar een bestaand rooster maar dan moet dat rooster wel als onderdeel van dit plan worden toegevoegd. Ook toegang tot dat (externe) rooster moet in dit plan beschreven worden.

2.2 Beveiligingseisen ten aanzien van personeel

A. In de functiebeschrijving van personeel dat belast is met de verwerking van de informatie en gegevens wordt de verantwoordelijkheid voor de beveiliging daarvan beschreven.

B. Personeel dat in aanraking komt met de informatie en gegevens tekent een geheimhoudingsverklaring.

C. Uitsluitend personeel dat overeenkomstig de functiebeschrijving belast is met de verwerking van de informatie en gegevens heeft toegang tot de informatie en de gegevens.

NBIP-tip: De functiebeschrijvingen van het telecomaanbieder moeten zijn voorzien van een herkenbaar hoofdstuk of taak. Zijn die functiebeschrijvingen nog niet beschikbaar, dan neemt u ook hier een rooster op met naam en rugnummers van het bevoegde personeel en beschrijf de aanvulling op de bestaande functiebeschrijvingen. U kunt hier verwijzen naar bestaande functiebeschrijvingen maar dan moet ook de toegang tot de functiebeschrijvingen (extern) in dit plan staan beschreven.

2.3 Fysieke beveiliging en beveiliging van de omgeving

A. De informatie en de gegevens worden zoveel mogelijk binnen één ruimte geconcentreerd.

B. De ruimte waarbinnen de informatie en de gegevens aanwezig zijn is deugdelijk fysiek beveiligd.

C. De fysieke beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.

D. Toegang tot de ruimte waar de gegevens of de informatie zich bevindt is uitsluitend toegestaan aan daartoe geautoriseerde personen voor zover dit voor hun functie noodzakelijk is.

E. Het binnentreden en verlaten van de ruimte moet zodanig zijn geregeld dat er sprake is van gecontroleerd en achteraf herleidbare toegang tot op individueel niveau.

F. Documenten waarin, dan wel verwisselbare gegevensdragers waarop, de informatie en de gegevens zijn vastgelegd worden in deugdelijk beveiligde opbergmiddelen bewaard.

G. Personen belast met onderhouds- en reparatiewerkzaamheden in de ruimte waarin de informatie en de gegevens zich bevinden worden door eigen geautoriseerd personeel begeleid.

NBIP-tip: Beschrijf hier de fysieke en organisatorische zaken van en over de ruimte waar de tapgegevens zich behoren te bevinden. Denk aan cameratoezicht, opslag van videobeelden, registratie van toegangspassen, pincode gebruik, toegang tot patchkasten door wie en wanneer, waarom enzovoort.

Artikel 3:

Dit artikel beschrijft dat u dit plan moet hebben, en dat de bevoegde instantie dit plan op kan vragen. Artikel 3 is dan op zich ook geen hoofdstuk in uw beveiligingsplan.

3.1 De aanbieder draagt zorg voor een beveiligingsplan, waarin hij aangeeft op welke wijze door hem uitvoering is gegeven aan zijn beveiligingsplicht. In het beveiligingsplan wordt ten minste aangegeven op welke wijze uitvoering is gegeven aan de maatregelen bedoeld in de bijlage.

3.2 Op een daartoe strekkend verzoek van de bevoegde autoriteit wordt door de aanbieder inzage verleend in het beveiligingsplan.

NBIP-tip: Wanneer u een onderdeel van het onderstaande plan als niet relevant beoordeelt, laat het onderwerp dan wel staan in uw plan maar geef een verklaring waarom u het onderwerp als niet relevant beoordeeld heeft.

Artikel 4:

Minimaal VOG voor al het personeel in de keten.

NBIP-tip: Dit artikel heeft u al in artikel 2 beschreven.

Artikel 5:

Bewaartermijn LI en LD gegevens

wetten.overheid.nl/jci1.3:c:BWBR0010975&z=2017-01-01&g=2017-01-01

NBIP-tip: Dit artikel beschrijft hoe lang u de data moet bewaren maar is op zich geen onderdeel van uw plan, wel van uw verplichtingen.

Artikel 6:

Meldplicht beveiligingsincidenten

NBIP-tip: Hier beschrijft u hoe en wie bij uw organisatie van lekken of de constatering daarvan verantwoordelijk is, wie de melding doet,wie welke actie kan en zal ondernemen en hoe preventief op lekken te controleren is en welke frequentie u daarvoor heeft vastgelegd.

Aanvullende informatie: Verplichte melding bij lekken data (vanuit binneninn en buitenuit) of toegang tot de LI installatieonderdelen door onbevoegden moet gemeld worden.

NBIP advies: De overheid bedoeld hiermee dat als de data die gelekt is zou kunnen leiden tot het mislukken van een komend of lopend justitieel onderzoek bijvoorbeeld omdat de persoon/ instelling onder tap kan vernemen van een aanwezige tap/onderzoek op hem/haar dan is het echt mis en spreekt men over een serieus lek.

Met andere woorden: Is er, ondanks de getroffen (voorzorgsmaatregelen, toch een beveiligingsincident in (een deel van) uw

netwerk en/of dienst? Dan bent u in het kader van de zorgplicht verplicht om dit direct te melden. De overheid heeft hier speciale instructies en formulieren voor die u hier kunt vinden.

Datalekken, gegevens op straat geraakt, USB drive met data weg, elektronische of fysieke inbraak in de systemen en/of serverruimtes gehad en onbekend wat er is ingezien, gekopieerd en zo voort. Dat had u moeten voorkomen, maar als u onverhoopt toch gedoe krijgt dient u dit tot in detail te melden aan het Agentschap Telecom. De uiterlijke termijn is 4 weken maar NBIP adviseert die termijn zo kort mogelijk te houden.

Let op! Niet melden is geen keuze, ook als u denkt dat de gevolgen beperkt zullen zijn.

Boerenverstand:

Bij constatering van datalekken stopt u natuurlijk als eerste het lekken, daarna doet u direct de melding bij het Agentschap Telecom.

Het Agentschap Telecom maakt na uw verplichte melding de afweging wat de grootte van het issue is, en wat de volgende stap zal zijn.

Zijn de gevolgen onbekend maar het lijkt erop toch wel een hele hoop gedoe te gaan worden, kunt u het lekken niet direct stoppen of staat u spreekwoordelijk met de rug tegen de muur? Dan kunt u bij het Agentschap Telecom ook telefonisch een melding maken. U kunt 24 uur per dag telefonisch een melding doen. Dat kan via het speciale meldnummer **0900 70 70 701**. Dit informatienummer kost 5 cent per minuut, plus de gebruikelijke belkosten.

Artikel 7:

NBIP-tip: Dit artikel heeft u al in artikel 2 beschreven.

Verplichte geheimhouding voor alle medewerkers die te maken krijgen met LI en LD kunnen te krijgen met de Wet op de inlichtingen- en veiligheidsdiensten 2017 en de Telecommunicatiewet. Dit hoeft specifiek geen onderdeel van uw beveiligingsplan te zijn.

Artikel 8:

U heeft delen van uw LI keten uitbesteed aan derden.

1: Indien de aanbieder de uitvoering van werkzaamheden uitbesteedt aan een derde en in dat kader de derde kennis neemt of kan nemen van gegevens en informatie als bedoeld in artikel 2, eerste lid, draagt de aanbieder er zorg voor dat de derde zich verplicht:

A. De desbetreffende gegevens en informatie te beveiligen tegen kennisneming door onbevoegden;

B. Met betrekking tot de desbetreffende gegevens en informatie geheimhouding te betrachten;

C. De ingevolge dit besluit gestelde maatregelen na te leven;

D. Alle informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichting noodzakelijk is.

2: De verplichtingen van de derde als bedoeld in het eerste lid worden geregeld in een schriftelijke overeenkomst tussen aanbieder en derde. Op een daartoe strekkend verzoek van de bevoegde autoriteit wordt inzage verleend in de overeenkomst.

NBIP verlangt van haar deelnemers hier een actieve rol in. (Deelname aan deelnemersvergadering, beoordelen van voorstellen en bestudering voorgenomen bestuursbesluiten en dergelijke).

3: De aanbieder is verantwoordelijk voor de naleving door de derde van de verplichtingen, bedoeld in het eerste lid.

NBIP-tip: Artikel 8 van het Bbgt beschrijft wat u heeft gedaan om de uitbesteding van de LI aan derden veilig en conform de eisen de wetgever hieraan heeft gesteld te borgen. In uw geval bent u naar alle waarschijnlijkheid deelnemer van NBIP tapdiensten u kunt daarom in dit hoofdstuk daar

melding van maken. Door Stichting NBIP genomen maatregelen worden hier niet gevraagd te vermelden maar een bewustwording van uw eigen verantwoording aangaande Bbgt voorschriften moet wel uit uw plan blijken.

Tekstsuggestie:
Wij hebben als aanbieder van openbare diensten de in dit Bbgt plan geïmplementeerd en handelen daar ook naar maar het daadwerkelijke afhandelen van LD en LI zaken is in het geheel uitbesteed aan stichting NBIP. Aanbieder heeft de momenteel geldende deelnemersovereenkomst met stichting NBIP bijgevoegd bij dit beveiligingsplan.

De LI vorderingen die eventueel nog via onze eigen ingangen binnen zouden komen worden conform onze beschreven procedures beveiligd tegen onbevoegden en voor verdere afhandeling zo snel als mogelijk gerouteerd naar Stichting NBIP. Naast de beschreven technische maatregelen die binnen ons eigen netwerk zijn geïmplementeerd en is het eventueel aanwezige tapsysteem van NBIP binnen ons netwerk gezien als actieve TAP. Verder heeft NBIP heeft een raad van deelnemers met daarin afgevaardigden van de deelnemers die via de voorzitter van de raad van deelnemers samen met het bestuur de gevraagde onderdelen en naleving van artikel 8 Bbgt scherp in de gaten houden.

NBIP-tip: Omdat u als deelnemer van NBIP de door NBIP anoniem gemaakte tap bevelen en of taps niet zelf zet zal er bij uw in het netwerk en of systeem geen data achterblijven waar de wetgever hier aan refereert. Wel kan er een bij u achter zijn gebleven een elektronisch of papier spoor wat u op moet kunnen ruimen.

IV. Beheer van communicatie- en bedieningsprocessen

A. De status/rubricering van de informatie en de gegevens (staatsgeheim of vertrouwelijk) dient te allen tijde als zodanig herkenbaar te zijn.

B. Reproductie van de informatie of de gegevens is alleen toegestaan door daartoe geautoriseerde personen uitsluitend voor zover dat nodig is voor de goede uitvoering van de bijzondere last dan wel een opdracht op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2017 als bedoeld in artikel 13.2, eerste en tweede lid, van de wet dan wel een verzoek op grond van artikel 13.4 van de wet.

C. De informatie of de gegevens worden niet buiten de normale ruimte gebracht, tenzij dat voor de goede voortgang van de werkzaamheden noodzakelijk is. In dat geval wordt de verblijfplaats van de informatie of de gegevens geregistreerd.

D. De verwijdering en vernietiging van de informatie en gegevens geschiedt op een onomkeerbare wijze. Van de verwijdering en vernietiging wordt een rapport opgemaakt, dat in afschrift wordt gezonden aan de bevoegde autoriteit wie het aangaat dan wel een door deze aangewezen instantie.

V. Toegangsbeveiliging van geautomatiseerde informatiesystemen

A. De toegang tot geautomatiseerde informatiesystemen waarin de informatie en de gegevens worden verwerkt is op deugdelijke wijze beveiligd, onder meer door middel van persoonsgebonden authenticatie.

B. De logische beveiliging is zodanig ingericht dat ongeautoriseerde toegang en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt.

C. Het aantal foutieve inlogpogingen is beperkt tot drie. Overschrijding van het aantal foutieve inlogpogingen leidt tot definitieve blokkering, welke uitsluitend door de functionaris, bedoeld in onderdeel I van deze bijlage, kan worden opgeheven. Het voorgaande is niet van

toepassing op de systeembeheerder, met dien verstande dat bij drie foutieve inlogpogingen een hernieuwde inlogpoging slechts kan plaatsvinden via een voor noodsituaties ingericht account en persoonsgebonden authenticatie voor het gebruik waarvan door de functionaris, bedoeld in onderdeel I van deze bijlage toestemming moet worden verleend.

D. Het geautomatiseerde systeem, waarin de gegevens en de informatie worden verwerkt, wordt niet eerder verlaten dan nadat een (handmatig of automatisch) toegangsbeveiliging mechanisme in werking is gesteld.

E. Alle handelingen met betrekking tot de verwerking van de informatie en de gegevens in het geautomatiseerde informatiesysteem worden persoonsgebonden vastgelegd teneinde onderzoek mogelijk te maken.

F. Toegang tot het geautomatiseerde informatiesysteem is uitsluitend voorbehouden aan daartoe geautoriseerd personeel.

G. De toegangsrechten van de gebruikers worden periodiek geëvalueerd.

H. De autorisaties van alle gebruikers worden vastgelegd.

NBIP-tip: Beschrijf in dit (bovenstaande) deel van het plan alles dat is geregeld rondom elektronische toegang tot systemen en gegevens. Ook de mogelijk mislukte toegangspogingen moeten geregistreerd worden en daarop moet worden geacteerd.

VI. Ontwikkeling, onderhoud en reparatie van geautomatiseerde informatiesystemen

A. Alle wijzigingen in apparatuur, software of procedures die de beveiliging van de gegevens en informatie kunnen beïnvloeden zijn controleerbaar, dat wil zeggen bekend en beoordeeld door of namens de aanbieder als zijnde aanvaardbaar.

B. Het onderhouden van geautomatiseerde informatiesystemen, voor zover deze nog toegang verschaffen tot gegevens en informatie, vindt op locatie plaats.

C. In afwijking van onderdeel b, is het op afstand onderhouden van geautomatiseerde informatiesystemen slechts toegestaan, indien dit wordt uitgevoerd door daartoe geautoriseerde personen als bedoeld in onderdeel lII van deze bijlage, en slechts op tijdstippen waarvoor door de functionaris, bedoeld in onderdeel I, onder a, van deze bijlage, toestemming is verleend en er aantoonbaar voldoende waarborgen bestaan voor het handhaven van het beveiligingsniveau van de gegevens en informatie.

D. Reparatie aan het geautomatiseerde informatiesysteem waarin de informatie en de gegevens worden verwerkt vindt op locatie plaats. Van de eerste volzin kan worden afgeweken indien de informatie en gegevens zijn verwijderd en niet te achterhalen zijn.

Artikel 9
Is de ingangsdatum van het Bbgt en geen onderdeel van het beveiligingsplan

Artikel 10
Is het origineel slotformulier en ondertekening van het besluit door de minister en geen onderdeel van het beveiligingsplan

Einde van uw plan

Begrippenverklaring

NBIP-tip: Hier beschrijft u elk lastig woord/ afkorting die u gebruikt in uw plan.

Bedenk dat uw plan door specialisten maar ook "nieuwe" niet zo technische mensen kan worden gelezen en het moet helder zijn voor elke lezer.

Aanbieder: Aanbieder van een telecommunicatienetwerk en/of -dienst, zoals vastgelegd in de Telecommunicatiewet, artikel 13

Definities in de Telecommunicatiewet:
openbaar telecommunicatienetwerk: elektronisch communicatienetwerk dat geheel of gedeeltelijk wordt gebruikt om openbare telecommunicatiediensten aan te bieden, voor zover het netwerk niet gebruikt wordt voor het verspreiden van programma's;

openbare telecommunicatiedienst: voor het publiek beschikbare dienst die geheel of gedeeltelijk bestaat in het overbrengen van signalen via een elektronisch communicatienetwerk, voor zover deze dienst niet bestaat uit het verspreiden van programma's;

AT: Agentschap Telecom, toezichthouder op wettelijke verplichtingen rond aftappen, zie http://www.agentschap-telecom.nl/

Bbgt en BBGAT
Bbgt: Besluit beveiliging gegevens telecommunicatie

Opvolger van het BBGAT, Besluit Beveiliging Gegevens Aftappen Telecommunicatie Zie: wetten.overheid.nl/BWBR0015808

BBGAT: Besluit Beveiliging Gegevens Aftappen Telecommunicatie Voorloper van het Bbgt

Zie: wetten.overheid.nl/BWBR0015808

Gegevens
Gegevens die door de eindgebruiker zijn gegenereerd, zoals tapdata, en doorgestuurd naar een bevoegde instantie. Ook gegevens die gerelateerd zijn aan het gebruik van de eindgebruiker van een dienst van de aanbieder, zoals gespreksgegevens. Dit zijn dataretentie gegevens.

Informatie
Informatie betreft de informatie over een vordering van een daartoe bevoegde instantie. Dit betreft de vordering zelf en de informatie die vervolgens door de aanbieder wordt verstrekt.

De informatie gaat dus over de informatie over het aftappen (en dataretentie) die door de bevoegde instantie is verstrekt aan de aanbieder en de informatie die vervolgens door de aanbieder wordt aangeleverd.

De onderliggende definities in het Bbgt is als volgt: Artikel 2, lid 1

A. De gegevens welke in het kader van het verlenen van medewerking aan de uitvoering van een bevoegd gegeven bijzondere last dan wel een toestemming op grond van de Wet op de inlichtingen- en veiligheidsdiensten 2002 tot het aftappen of opnemen van telecommunicatie door een bevoegde autoriteit aan de aanbieder zijn verstrekt;

B. De informatie welke door de aanbieder aan een bevoegde autoriteit is verstrekt op grond van de artikelen 13.2b en 13.4 van de wet alsmede de gegevens welke zijn vervat in het aan deze verstrekking ten grondslag liggende verzoek of in de aan deze verstrekking ten grondslag liggende vordering om informatie van de desbetreffende bevoegde autoriteit;

C. De gegevens die door de aanbieder worden geraadpleegd en verder worden verwerkt met het oog op het voldoen aan een verzoek of vordering op grond van de artikelen 13.2b en 13.4 van de wet.

NBIP
Stichting Nationale Beheersorganisatie Internet Providers, www.nbip.nl/

(Natuurlijk vallen telecom providers ook onder deze afkorting)

Preambule
Een preambule is een (vaak ongenummerde) inleidende tekst op de bepalingen van een contract, wet of verdrag. In de preambule wordt het doel geschetst, een onderliggende filosofie en/of de omstandigheden die hebben geleid tot de wet of het verdrag.

ULI:
Unit Landelijke Interceptie, de tapkamers van de overheid

VOG:
Verklaring Omtrent Gedrag; zie voor informatie: www.rijksoverheid.nl/onderwerpen/verklaring-omtrent-het-gedrag

NBIP nationale beheersorganisatie internet providers

Voor meer informatie:
www.nbip.nl