Secura

VAN BIG NAAR BIO

Integrale benadering voor een succesvolle implementatie

SECURA

Vestdijk 59
5611 CA Eindhoven

Karspeldreef 8
1101 CJ Amsterdam

T +31 (0)88 888 31 00
E info@secura.com
W secura.com

Volg ons op:

Auteurs:
Heinrich W. Klöpping, MSc CISSP CCSP CIPP/E SCI, Principal Consultant, Secura
Ruud Kerssens, RE RA CISA CRISC, Principal Security Consultant & Auditor, Secura
Ing. Mario Sleegers, RE, CISSP, CISA, Principal Security Consultant/ EDP Auditor, Secura
Erwin Jansen, Manager Service Line Advisory, Audit and Security Certification, Secura

Oktober, 2019

Van BIG naar BIO

Integrale benadering voor een succesvolle implementatie

Gemeenten zijn nog bezig met de laatste punten voor de implementatie van de BIG en moeten alweer aan de slag met een nieuw normenkader: de BIO. De Baseline Informatiebeveiliging voor de Overheid (BIO) is het nieuwe normenkader dat de IBI, BIWA, BIR en BIG vervangt. In 2020 moet de gehele overheid werken conform de BIO.

Kortom, een uitdaging voor veel partijen, waaronder gemeenten. Dit white paper gaat specifiek in op de stap van de Baseline Informatiebeveiliging Gemeenten naar de BIO. We leggen uit wat, wanneer, waarom, hoe en door wie gedaan moet worden. Verder geven we aan wat we denken dat de grootste struikelblokken kunnen zijn in de migratie van BIG naar BIO.

Inhoud

Doelgroep

Dit white paper is met name bedoeld voor bestuurders (College, CISO) van middelgrote en kleine Gemeenten, de Gemeenteraad en organisaties waarmee de Gemeenten samenwerken.

Over Secura

Secura levert beveiligingsadviezen, doet audits, voert security testen en certificeringsdiensten uit en verzorgt trainingen. Secura bedient financiële instellingen, energiebedrijven, multinationals, rijksoverheid, lokale overheid en zorginstellingen.

Vragen over de BIO

Met name over de BIO kregen we in de afgelopen tijd veel vragen. Wat is de BIO, voor wie is de BIO relevant, wanneer moeten we er mee aan de slag, waarom is deze norm zo belangrijk en wat moet er in grote lijnen worden gedaan? In dit white paper geven we antwoord op deze vragen.

Wat is de BIO?

De Baseline Informatiebeveiliging voor de Overheid (BIO) is het nieuwe normenkader dat de IBI, BIWA, BIR en BIG vervangt. De BIO is gebaseerd op de recente versie van de internationaal geaccepteerde best practices in informatiebeveiliging, de ISO 27001 en ISO 27002 (ISO27K)[1]. De BIO is op 14 december 2018 aan de Ministerraad voorgelegd en goedgekeurd. De Overheid vindt deze baseline zo belangrijk dat verkend wordt of de systematiek van de BIO in een Algemene Maatregel van Bestuur (AMvB) vastgelegd kan worden[2]. De ISO27K normen waren eerder al door het Forum Standaardisatie op de 'pas-toe-of-leg-uit' lijst opgenomen. De BIO is dus een belangrijke standaard. Binnen de BIO zijn 14 onderdelen opgenomen:

1. Informatiebeveiligingsbeleid
2. Organisatie van informatiebeveiliging
3. Veilig Personeel
4. Beheer bedrijfsmiddelen
5. Toegangsbeveiliging
6. Cryptografie
7. Fysieke beveiliging
8. Beveiliging bedrijfsvoering
9. Communicatiebeveiliging
10. Acquisitie, ontwikkeling en onderhoud
11. Leveranciers
12. Incidentmanagement
13. Bedrijfscontinuïteit
14. Naleving

Voor wie is de BIO bedoeld?

De BIO vervangt de huidige normen voor rijk (BIR), gemeenten (BIG), provincies (IBI) en waterschappen (BIWA).

Wie is verantwoordelijk voor de uitvoering van de BIO?

De BIO stelt het expliciet: het lijnmanagement is verantwoordelijk voor de beveiliging van informatie(systemen). De BIO meldt ook dat de breed bekende Plan-Do-Check-Act managementcyclus het lijnmanagement verantwoordelijk maakt voor het treffen van maatregelen op basis van risicomanagement.

[1] Gemakshalve refereren we in de rest van dit stuk naar de verzameling gerelateerde standaarden als "de ISO27K standaarden".

[2] Staatssecretaris Knops (BZK) stuurde de Tweede Kamer de uitwerking van maatregelen die de informatieveiligheid bij de overheid moet verhogen, waarin dit voornemen staat omschreven; 16-10-2018, zie ook https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2018/10/16/kamerbrief-over-verhogen-informatieveiligheid-bij-de-overheid/kamerbrief-over-verhogen-informatieveiligheid-bij-de-overheid.pdf

[3] In dit geval de versie uit 2013, die vrijwel gelijk is aan die uit 2017 die de BIO grotendeels vormt

Lijnmanagers moeten dus in staat zijn om een risicoanalyse uit te (laten) voeren. In de BIO staat bij elke maatregel (control) vermeld wie verantwoordelijk is voor het treffen van deze maatregel. Voor gemeenten is het college eindverantwoordelijke voor deze beveiliging en voor de inrichting en werking van de beveiligingsorganisatie, maar de uitvoering ligt bij tal van rollen. Dit is geheel in overeenstemming met de al geldende praktijk rond ISO27K.

Wanneer moet de BIO zijn geïmplementeerd?

De implementatie van de BIO zou al in 2019 plaats moeten vinden. U bent er mogelijk dus al heel druk mee bezig. Zo niet dan moet u snel beginnen: in 2020 moet de hele overheid werken conform de BIO.

Waarom is de BIO zo belangrijk?

De standaard ís zo belangrijk omdat het gebruik van één normenkader voor de gehele overheid zal leiden tot eenduidigheid, minder complexe administratie, meer aansluiting bij internationale standaarden en best practices, lagere onderhoudskosten en minder grote problemen om hulp en ondersteuning te krijgen. De Rijksoverheid en auditors hoeven ook nog maar met één baseline te werken voor Gemeenten, Waterschappen en Provincies.

Ook voor de audits bij de gemeenten is de BIO. Bijvoorbeeld ENSIA, het gereedschap voor Gemeenten om in één keer slim verantwoording af te kunnen leggen over informatieveiligheid, veranderd qua grondslag van BIG naar BIO. De pilot loopt momenteel.

Kortom: één gezamenlijke taal voor alle overheidsorganisaties: helder en eenduidig gericht op verhogen informatieveiligheid.

Overeenkomsten en verschillen

Vanaf 2020 overal de BIO- dat lijkt ambitieus, maar de al in gebruik zijnde normenkaders IBI, BIWA, BIR, BIG én de nieuwe BIO hebben een grote gemeenschappelijkheid. Aan de basis liggen de meest recente versies[4] van de ISO27K standaarden. Over ISO27K is al kennis aanwezig in de markt en bij de overheid zelf.

Maar er zijn een aantal verschillen tussen de oude baselines, de BIO en de ISO normen die u goed in de gaten moet houden. Het accent ligt bij de BIO veel meer op risicoanalyse dan bij de BIG. Er zijn daarnaast drie basisbeveiligingsniveaus gedefinieerd en de maatregelen in de BIO zijn allemaal verplicht. Het zijn er dan wel weer minder dan in de BIG.

En vaak ontbreekt de bredere kijk op zaken. Het implementeren van de BIO kan de illusie geven dat er voldoende is gedaan, maar dat is niet altijd het geval.

[4] *Huidige versies (september 2019) zijn: ISO 27001:2017 en ISO27002:2017.*

Waarom de BIO alleen niet genoeg is

Als bestuurder van een Gemeente moet u zich jaarlijks verantwoorden over het niveau van uw informatieveiligheid. Wat doet u om informatie veilig te houden? Welke risico's accepteert u, welke niet? U moet dit zowel naar het Ministerie (verticale verantwoording) als naar het publiek (horizontale verantwoording, via de Gemeenteraad) uitleggen.

De BIO kent een aantal verplicht te implementeren maatregelen. Die moet u goed uitvoeren en dat moet u kunnen aantonen. Wat u verplicht bent te doen is vastgelegd in een normenkader. Dat is momenteel (2019) nog de BIG. In 2020 zal dit de BIO zijn.

Aan de basis van zowel BIO als BIG liggen de meest recente versies ISO27K standaarden. Of u het voldoende goed doet toetst u binnen het ENSIA project.

Per 1 juli 2017 is (vanuit de overheid) het project ENSIA (Eénduidige Normatiek Single Information Audit) voor gemeenten van start gegaan. De invoering van ENSIA betekent dat alle gemeenten vanaf 2017 werken met één effectief en efficiënt verantwoordingsstelsel voor informatieveiligheid. De verantwoording sluit aan op BIG en BIO.

De verantwoording richt zich zowel op het horizontale proces (naar de burgers toe) als het verticale proces (naar het Ministerie) op dezelfde beheersmaatregelen. Deze informatie verzamelt u door gebruik te maken van de gereedschappen binnen het ENSIA project. Het idee achter ENSIA is dat de horizontale verantwoording- die u deelt met het publiek en gelijkwaardige partners- het uitgangspunt is voor de verantwoording in de hiërarchie[5].

Een helder verhaal: het Ministerie schrijft normenkaders voor, die bent u verplicht te implementeren en u moet daar verantwoording over afleggen.

In de praktijk is de implementatie lastiger. Ten eerste is de basisnorm (ISO27K) niet zo maar begrepen, zeker niet de vertaling naar de werkzaamheden van de medewerkers. Er zijn zeker bij kleinere Gemeentes niet zo heel veel specialisten die dit normenkader (goed) begrijpen. De verbijzondering naar de BIG is daarbij weer anders dan de verbijzondering naar de BIO. De BIO legt bijvoorbeeld nadruk op het doen van risicoanalyses door lijnmanagers. Maar kunnen die dat wel? Welke methodologie gebruik je dan? Als je al ver was met de implementatie van de BIG, is dat dan voldoende? Zo niet, wat moet er dan nog gebeuren? Daarnaast is het werken met het ENSIA raamwerk ook iets dat kennis en ervaring vraagt.

Hoe pakt u het aan? U wilt snel stappen maken, maar daarbij wel een gedegen aanpak kiezen.

[5] *Simone Roos, voormalig Directeur-generaal Overheidsorganisatie, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)*

Secura heeft 20 jaar ervaring en beschikt over specialisten op alle aspecten van informatiebeveiliging en cyberveiligheid: Organisatie, Mensen, Processen en Techniek.

Secura helpt veel gemeenten op het gebied van informatiebeveiliging in advies- en auditdiensten, zoals een gap analyse om te bepalen wat u nog moet doen voor de BIO implementatie. Ook wordt Secura veel gevraagd voor het leiden en uitrollen van bewustwordingsprogramma's ten aanzien van informatiebeveiliging.

In deze diensten is Secura niet uniek. Het unieke van Secura is dat we vanuit een veel bredere visie proberen te helpen.

BIO en ENSIA zijn niet voldoende om echt "in control" te zijn. Compliance kan een doel zijn, maar het gaat er om of u organisatie echt haar informatieveiligheid op orde heeft. Dit vraagt om een integrale en methodische aanpak.
In onze aanpak combineert Secura bekende "best practices" en standaarden met onze ervaring en visie.

Zo zijn wij gekomen tot Secura's aanpak die waarborgt dat niet alleen wordt gekeken naar de implementatie van de BIO-maatregelen, maar ook naar de effectiviteit en de toegevoegde waarde van beheersmaatregelen gericht op detectie, respons en herstel. Secura's aanpak is conform BIO, verrijkt met de ISO 27 standaard en de NIST-cybersecurity standaard. Dit zijn:

1. Organisatie (beleid)
2. Risicoanalyse
3. Identificeer
4. Bescherm
5. Detecteer
6. Respons
7. Herstel

We vullen die aandachtsgebieden in door te kijken naar 4 aspecten.

1. Organisatie
2. Mensen
3. Processen
4. Techniek

Deze integrale aanpak wordt weergegeven in dit schema:

Deze integrale aanpakt dekt de volledig BIO norm, omdat alle BIO eisen binnen dit framework zijn opgenomen. Doordat Secura van deze geïntegreerde aanpak uitgaat, bent u beter in control dan wanneer u de BIO alleen als een checklist afkruist.

Als voorbeeld een scenario: het blijkt dat er een groot datalek is geweest binnen uw Gemeente. De BIO is keurig geïmplementeerd, de ENSIA bewees het. U dacht “in control” te zijn. De fout was door menselijk toedoen (onvoldoende kennis) en in de opvolging was het proces voor opvolging, analyse en maatregelen niet geborgd. Deze onderwerpen zouden met een geïntegreerde aanpak zeker benoemd zijn (onder aandachtsgebied “Respons” en onder het aspect “Mensen”). Dit is één van de aspecten die je makkelijk over het hoofd ziet, want het komt in de BIO nauwelijks aan de orde.

De grote lijn

Bij het implementeren van de BIO is de grote lijn als volgt:

1. Bepaal eerst de scope (het informatiesysteem),
2. dan het Basis BeveiligingsNiveau (BBN) van dat systeem,
3. dan de selectie voor dat systeem relevante beheersmaatregelen (controls) en
4. daarna volgt de implementatie van die controls.

Goed om te weten: interne audits en ENSIA helpen bij het controleren of alles juist is gedaan.

1. ***Informatiesysteem***

   De in de BIO geschetste aanpak is van toepassing voor elk informatiesysteem. Als u gaat migreren van BIG naar BIO is het vaststellen van de scope van het eerste systeem dat u gaat migreren van groot belang voor het vervolg. De definitie van informatiesysteem conform de BIO is: “een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie”. Het is dus zonder meer mogelijk om eerst een wat kleiner systeem te migreren en in het algemeen raden we dat aan. Houd rekening met het uitstralend effect van deze eerste migratie: als het een succes wordt is het draagvlak in de organisatie daarna veel groter dan na het falen van een aanpak met een te grote scope.

2. ***BBN***

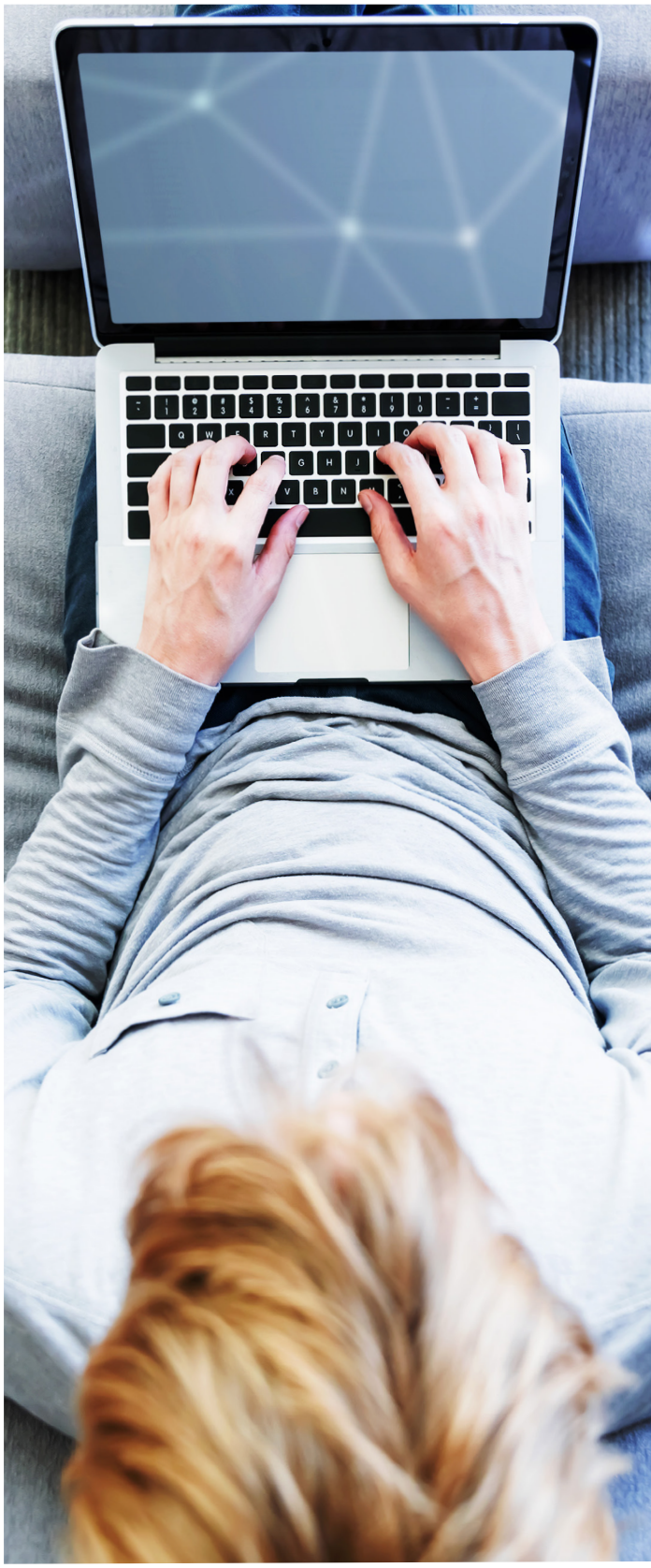
Per informatiesysteem bepaalt u eerst het basis beveiligingsniveau (BBN). Daarvoor is in de BIO een richtlijn opgenomen[6]. Het kiezen van het BBN doet u aan de hand van kwalitatieve criteria, vanuit de BIV-driehoek (Beschikbaarheid, Integriteit en Vertrouwelijkheid). Bijvoorbeeld door te bepalen hoe lang het systeem er uit mag liggen (B), hoe groot de gevolgen zijn van het verloren gaan of veranderen van gegevens (I) of wat de gevolgen zijn van kennisname van informatie door buitenstaanders. De granulariteit is beperkt: er zijn maar 3 van deze BBN's.

3. ***Controls***

In de BIG spreken we nog over beheersmaatregelen. In de BIO is de internationaal gangbare term "control" gebruikt. De controls zijn in tabellen opgenomen, gegroepeerd per aandachtsgebied / hoofdstuk. Er zijn 14 aandachtsgebieden / hoofdstukken (5 t/m 18) met in totaal 112 controls[7]. Per hoofdstuk zijn de relevante controls gelijst. De nummering loopt parallel met NEN-ISO 27002:2017. Per control staat vermeld welk minimum BBN een informatiesysteem moet hebben om de control verplicht te laten zijn (1 of 2 dus) en een omschrijving van de control, exact gelijk aan die van de 27K. Er is momenteel nog geen enkele control die BBN 3 als minimum aanmerkt.

4. ***Implementatierichtlijnen***

In de BIO staat weinig over de implementatie van de controls. De concrete eisen aan implementatie die wel in de BIO staan, zijn vaak afgeleid van wettelijke eisen. Als de BIO geen concreet advies geeft over de implementatie kunt u de implementatie van bestaande maatregelen uit de BIG gebruiken. Ook kunt u de maatregelen herijken met behulp van externe expertise, zoals die van Secura, of u gebruikt de producten van de IBD of ISO27K. In de ISO27002 standaard, die complementair is aan de BIO, zijn ook nuttige implementatierichtlijnen opgenomen. U kunt dit in de ISO-standaard nalezen, de Nederlandstalige versie hiervan, de NEN standaard, is voor medewerkers bij Gemeenten vrij in te zien. Maar implementatie van controls vereist praktische ervaring met deze controls. Dat hebben met name kleinere Gemeenten niet altijd, dan is het beter hulp te zoeken bij partijen die die ervaring wél hebben.



[6] *De BBN-toets, bijlage 2 van de BIO*

[7] *114 in de NEN/ISO 27002 norm, maar 6.1.4 ("contact with special interest groups") en 14.2.4 ("restrictions on chan-ges to software packages") zijn in de BIO vervallen.*

De voornaamste struikelblokken

De voornaamste struikelblokken bij migratie van BIG naar BIO zijn in onze ogen:

- het missen van een integrale benadering
- het niet goed kunnen bepalen wat er (nog) gedaan moet worden (gap analysis)
- de scope van het eerste migratieproject te ruim zetten
- het niet helder hebben van verantwoordelijkheid voor het informatiesysteem
- onvoldoende rekening houden met functiescheidingen
- onvoldoende ervaring met het maken van DPIA's. Hoewel strikt genomen geen onderdeel van de BIO, is het maken van data privacy impact analyses gezien het soort informatie dat bij Gemeenten wordt verwerkt meestal noodzakelijk
- het trainen van lijnmanagement op het doen van risicoanalyses
- het nog niet gereed zijn van ENSIA op basis van de BIO
- samenwerking met partijen zonder BIO controls
- Secura heeft specialisten op het gebied van ISO27K en BIO in huis, die kunnen helpen bij het adresseren en wegnemen van deze struikelblokken. Secura werkt vanuit de gepresenteerde 5x4 benadering en helpt u zo met breder kijken en beter in control zijn.

Stappen waarin wij u kunnen helpen:

- Initiële analyse (BIO nulmeting) - waar staat u?
- Gap analyse – wat moet er nog gedaan worden?
- Advies en aanpak voor eerste BIG/BIO migratie
- Trainen en begeleiden in het doen van risicoanalyses
- Trainen en begeleiden met ENSIA, zowel begrijpen als uitvoeren
- Hulp en begeleiding bij het analyseren van samenwerkingen met niet-BIO gebaseerde organisaties met bijvoorbeeld een 27K of andere certificering

Tot slot dragen wij graag bij in het invullen van de maatregelen, zoals het geven van awareness trainingen en het uitvoeren van tussentijdse beoordelingen en pentesten.

Als u een oriënterend gesprek aan wilt gaan kunt u contact opnemen met Secura.

De BIO inzien?
https://www.informatiebeveiligingsdienst.nl/ product/ baseline-informatiebeveiliging-overheid-bio/

Lijst van afkortingen

AMvB	Algemene Maatregel van Bestuur
BAG	Basisregistraties Adressen en Gebouwen
BBN	Basis Beveiligings Niveau
BGT	Basisregistraties Grootschalige Topografie
BIG	Baseline Informatiebeveiliging Gemeenten
BIO	Baseline Informatiebeveiliging Overheid
BIR	Baseline Informatiebeveiliging Rijksdienst
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid (zie CIA)
BIWA	Baseline Informatiebeveiliging Waterschappen
BRO	Basisregistratie Ondergrond
BRP	Basisregistratie Personen
BVR	Beveiligingsvoorschrift Rijksdienst
CIA	Confidentiality, Integrity and Availability (zie BIV)
DigiD	Digitale persoonsidentificatie
ENSIA	Eenduidige Normatiek Single Information Audit
IBD	Informatie Beveiligings Dienst
IBI	Interprovinciale Baseline Informatiebeveiliging
ISO	International Standardization Organisation
ISOR	Information Security Object Repository
MAPGOOD	Mens, Apparatuur, Programmatuur, Gegevens, Organisatie, Omgeving, Diensten
P&C cyclus	Planning & Control-cyclus
PUN	Paspoortuitvoeringsregeling
SUWInet	Structuur uitvoeringsorganisatie Werk en Inkomen (SUWInet)
VIR	Voorschrift Informatiebeveiliging Rijksdienst
VIR-BI	Voorschrift Informatiebeveiliging Rijksdienst- Bijzondere Informatie

Over Secura

Secura is een onafhankelijk, gespecialiseerd kennisbedrijf op het gebied van digitale beveiliging en levert beveiligingsadviezen, audits, testen, trainingen en certificeringsdiensten aan o.a. banken, overheden en zorginstellingen.

Het is onze missie organisaties te ondersteunen met de beste en up-to-date kennis om samen verder te werken aan een heldere en veilige toekomst.

Blijf up-to-date met nieuws, inzichten & advies, events & trainingen en meld u aan voor onze periodieke nieuwsbrief: https://www.secura.com/nl/subscribe

Volg ons via:

Neem contact op met info@secura.com of bezoek secura.com voor meer informatie.

AANMELDEN

VOOR NIEUWSBRIEF