



BSPA Security evaluatie

■ Voor wie is BSPA bestemd?

Nederlandse overheden die gebruik maken van IT-producten, ontwikkelaars van IT-producten (software of embedded)

■ Wat zijn de 'deliverables'?

Een Statement of Conformity (SoC), Deployment Advisory (DA) en Evaluation Technical Report (ETR)

■ Wat is het doel?

Vaststellen of de beveiligingskenmerken van een product effectief en afdoende zijn om deze in een BBN1- of BBN2-omgeving toe te passen.



Wat is BSPA?

Het Baseline Security Product Assessment is één van de instrumenten die het Nationaal Bureau voor Verbindingsbeveiliging (NBV) heeft ontwikkeld om in korte tijd en tegen beperkte kosten, noodzakelijke zekerheid te bieden daar waar beveiliging op basisniveau volstaat.

Het NBV maakt een deel uit van de Nederlandse inlichtingen- en veiligheidsdienst (AIVD). De AIVD is dan ook de uitvoerder van dit programma.

Het doel van deze regeling is een kader te bieden waarin producten getest kunnen worden aan de hand van een **Baseline Informatiebeveiliging Overheid** (afgekort BIO). Producten kunnen zowel hardware- als softwarecomponenten omvatten die worden gebruikt in het gevoelige, maar niet-gerubriceerde domein. Met een succesvol BSPA evaluatieresultaat kan een Nederlandse gebruikersorganisaties aantonen dat het product in kwestie voldoet aan de BIO BBN1-vereisten.

Het BSPA volgt een duidelijk gestructureerde en gefaseerde aanpak dat zich strikt houdt aan de BSPA-voorschriften. Een beoordeling van een beveiligingsproduct dat in het kader van de BSPA-schema uitgevoerd wordt heeft de volgende kernpunten:

- De beoordeling wordt uitgevoerd in een beperkt tijdsbestek en met beperkte middelen, met een aanbeveling om het binnen 25 mandagen te doen;
- Er wordt nagegaan of het product in overeenstemming is met de Security Evaluation Target (SET);
- De effectiviteit van de security kenmerken van het desbetreffend IT-product worden vastgesteld.

Het beoordelingsproces is ontworpen om uitgevoerd te worden als een onafhankelijke evaluatie met weinig betrokkenheid van de ontwikkelaar of vendor. De enige eisen zijn de geïnstalleerde producten zelf en de bijbehorende documentatie.

De BSPA-evaluatie kan een aantrekkelijke optie zijn voor fabrikanten die met de Nederlandse overheid willen samenwerken of gewoonweg een concurrentievoordeel willen behalen wanneer zij hun producten op de Nederlandse markt willen verkopen. Daarnaast kan zo een BSPA evaluatie ook worden gebruikt door overheidsinstanties om de security producten te testen die zij momenteel gebruiken of van plan zijn te gebruiken.

Bureau Veritas Cybersecurity is door de AIVD gelicenseerd om BSPA-diensten te verlenen en kan u helpen bij het gehele proces van de BSPA-evaluatie, vanaf een voorbereidingsfase tot en met het testen en uiteraard het volledige certificeringsproces ondersteunen. Afhankelijk van de gereedheid voor certificering kan Bureau Veritas Cybersecurity ook BSPA leveren als een pre-validatie ter voorbereiding op de officiële BSPA-certificering.

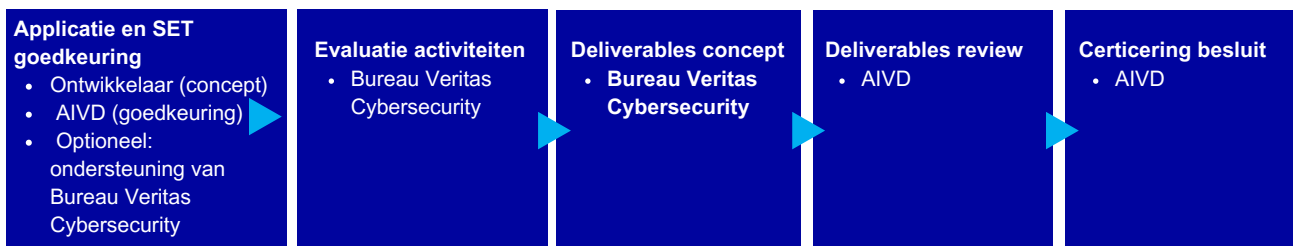
Scope van de beoordeling

Een BSPA-evaluatie kan gebruikt worden voor een grote verscheidenheid aan software- en hardwareproducten, zoals in de onderstaande tabel is weergegeven:

Product categorie	Voorbeelden
Netwerk beveiliging	VPN, link encryptie, Wi-Fi access point, etc.
Netwerkfiltering, detectie en respons	IDS, firewall, SSL proxy, etc.
Beveiligd berichtenverkeer	Beveiligde e-mail, beveiligde chat-app, beveiligde voice-call-app, etc.
Beveiliging van media en bestanden	Volledige schijfversleuteling, containerversleuteling, bestandsversleuteling, gegevenswissing, etc.
Identiteits- en toegangsbeheer	Wachtwoordmanager, sleutelbeheer en -distributie, tweefactorauthenticatie, toegangscontrole en federatie, etc.
Beveiligde OS-uitvoering omgeving	Secure-OS, secure-hypervisor, microkernel, scheidingskern, etc.
Hardware en embedded software	HW-gebaseerde encryptie, HW-gebaseerde secure-boot, USB-apparaat, toetsenbord (KVM-) schakelaar, smart-meter, sabotagebestendig apparaat, etc.
Smart cards en soortgelijke apparaten	Beveiligde IC's, JavaCards, transport-/toegangskarten, etc.

BSPA evaluatie & certificering van uw IT-producten

De belangrijkste stappen in het BSPA-evaluatie proces en wie de betrokken stakeholders zijn in elke fase, vindt u in het onderstaand overzicht.



Voordat de daadwerkelijke evaluatie van start gaat, wordt allereerst de SET gedefinieerd opgesteld om zo de verwachtingen tussen de opdrachtgever, het evaluatielaboratorium en de toezichhoudende instantie te managen en op elkaar af te stemmen. De SET omvat de te testen beveiligingskenmerken, en de omstandigheden waaronder de test wordt uitgevoerd.

Wanneer de SET is goedgekeurd, is het uitvoeren van het onderzoek de volgende stap binnen het proces. Er zijn drie belangrijke doelstellingen voor de evaluatie die door het evaluatielaboratorium zal worden uitgevoerd:

- Ten eerste moet er worden nagegaan of het product voldoet aan de beveiligingsspecificatie volgens de SET;
- Ten tweede moeten de veiligheidskenmerken van het product doeltreffend zijn, en bescherming bieden tegen aanvallers met een laag en gemiddeld aanvalspotentieel;
- Ten slotte is het belangrijk om het product te evalueren op eventuele negatieve gevolgen voor het host systeem en infrastructuur..

Bureau Veritas Cybersecurity zorgt voor het verzamelen van de benodigde documentatie en voert documentanalyse en penetratietesten uit op het product. Voorbeelden van vereiste testen op het product zijn bescherming van cryptografische

sleutels, impact van bekende kwetsbaarheden, authenticatie en autorisatie van gebruikers, toegang tot poorten en interfaces of onveilige configuraties.

Het evaluatiecertificeringsproces verloopt volgens de onderstaande 10 stappen plan:

1. Security Evaluation Target analyse
2. Product installatie
3. Compliance analyse
4. Compliance analyse volgens een source code review
5. Compliance analyse via een product test
6. Determination of the resistance against attacks
7. Kwetsbaarheidsanalyse
8. Bruikbaarheids analyse
9. Cryptografie evaluatie
10. Rapportage

Bureau Veritas Cybersecurity stelt het **Evaluation Technical Report (ETR)** op, met de resultaten en conclusies van de evaluatie. Samen met de ETR wordt er een concept geproduceerd van de **Deployment Advisory (DA)** voor de gebruikers, die de toezichhoudende instantie zal beoordelen. Op basis van deze documentatie ondersteunen wij het certificeringsproces bij de AIVD, dat uiteindelijk zal leiden tot het **Certificate of Conformity** voor uw product.





BUREAU
VERITAS

Uw Expert Partner in Cybersecurity

Bureau Veritas Cybersecurity is al twee decennia actief in informatiebeveiliging en privacy. Door gebruik te maken van onze ervaring en expertise zijn wij een sterke partner om uw informatiebeveiligingszaken efficiënt en grondig aan te pakken. Als gelicenseerd lab voor BSPA, is Bureau Veritas Cybersecurity uw partner gedurende het gehele evaluatie en certificatieproces.

Stap voor stap kunnen wij:

- U begeleiden bij het opstellen van de vereiste documentatie.
- Voer de vereiste documentcontrole en tests uit op het evaluatieproduct.
- Indien nodig, een prevalidatie leveren.
- Uitvoeren van het formele BSPA-certificeringsproces.

Door met Bureau Veritas in zee te gaan voor uw BSPA-evaluatie, heeft u de garantie dat u tijdens het hele proces voldoende ondersteuning krijgt van a tot z.

Een Statement of Conformity voor uw product is bewijs van uw security capaciteiten. Het verkrijgen van het BSPA certificaat kan leiden tot een aanzienlijk marktvoordeel voor de fabrikanten, met name wanneer zij zich richten op de Nederlandse markt. Voor Nederlandse overheidsinstanties is dit certificaat een bewijs dat het beoordeelde product veilig is en voldoet aan het BIO BBN1 niveau.

Bovendien kan deze evaluatie, gezien de aard van de BSPA-eisen en het BSPA-proces, worden gebruikt als opstapje voor andere, uitgebreidere certificeringen, op basis van internationaal erkende schema's zoals Common Criteria (CC).

Wilt u meer weten over het BSPA Security Schema?

Neem vandaag nog contact met ons op en leer over onze BSPA-evaluatie diensten in meer detail en ontdek welke dienst het beste bij uw (IT) product past.

Waarom Bureau Veritas Cybersecurity

Bureau Veritas Cybersecurity is uw specialist op het gebied van digitale veiligheid. Wij ondersteunen organisaties bij het in kaart brengen van risico's, het verbeteren van hun verdediging en het naleven van wet- en regelgeving. Onze dienstverlening omvat mens, proces en technologie: van awareness-trainingen en social engineering tot advies, compliance en technische security tests.

We werken in IT-, OT- en IoT-omgevingen en ondersteunen zowel digitale systemen als connected producten. Met ruim 300 cybersecurity-specialisten wereldwijd combineren we diepgaande technische kennis met internationaal bereik.

Bureau Veritas Cybersecurity is onderdeel van Bureau Veritas, wereldwijd actief in testen, inspectie en certificering.



BUREAU
VERITAS

Interesse?



cybersecurity@bureauveritas.com

Neem contact op:



cybersecurity.bureauveritas.com