Visie op hoogbeveiligde ICT-werkplekken binnen de (rijks-)overheid

Auteur: Drs. Daan Zegelaar
Versie: 1.0
Datum: 25-3-2022

Daan Zegelaar is IT consultant/architect bij Metis IT en heeft gedurende zijn IT loopbaan vrijwel voortdurend in het hoog beveiligde overheidsdomein gewerkt. Gedurende deze tijd heeft hij zowel de positieve- als negatieve kanten van een hoog beveiligde infrastructuur kunnen ervaren. Waar gegevenslekken, virusuitbraken en aanverwante problemen vrijwel non-existent zijn in een hoog beveiligde omgeving, is het daadwerkelijke gebruik van de hoogbeveiligde omgevingen voor zowel gebruiker, ontwikkelaar, als beheerder vaak omslachtig en tijdrovend. Daarnaast is het gedurende zijn loopbaan opgevallen, dat gebruikers vaak niet goed gefaciliteerd worden bij hun werkzaamheden, omdat het rubriceringsniveau is afgestemd op de hoogst gerubriceerde informatie en dit bepaalde werkzaamheden niet op een gemakkelijke manier toestaat. Dit leidt in sommige gevallen tot shadow-IT en daarmee verlies aan controle. Dit is een belangrijke reden voor het opstellen van dit rapport: het maximaal faciliteren van de gebruiker in zijn/haar (opsporings-) taken.

Dit visiedocument is opgesteld, om Rijks- en andere overheidsdiensten een handvat te geven hoe hoogbeveiligde werkplekken zijn te realiseren. Behandeld worden: welke regels gelden, hoe - rekening houdend met het vigerend beleid – ICT-technisch de werkplekken zijn te realiseren en wat dit voor gevolgen heeft voor de mogelijkheden die een werkplek biedt.

Balanceren
Uitgangspunt is om een goede balans te vinden tussen veiligheid en bruikbaarheid. Dit wordt bewerkstelligd door zoveel mogelijk gebruik te maken van de bestaande technische mogelijkheden en het maken van een goede risicoafweging. Dit als alternatief voor het eenvoudigweg uitsluiten van oplossingsmogelijkheden door het ontbreken van door het NBV[1] goedgekeurde ICT-componenten.

Rubricering[2]
Gebaseerd op diverse gesprekken met deskundigen uit het werkveld van binnen en buiten de (rijks)overheid, is de scope van dit document vastgesteld op de werkplekconcepten die geschikt zijn voor het verwerken, delen en opslaan van als Staatsgeheim Geheim (Stg.G), Staatsgeheim Confidentieel (Stg.C) en/of Departementaal Vertrouwelijk (Dep.V BBN2+ /BBN3)) gerubriceerde gegevens.

Bij het opstellen van de concepten is de volgende regelgeving in ogenschouw genomen:

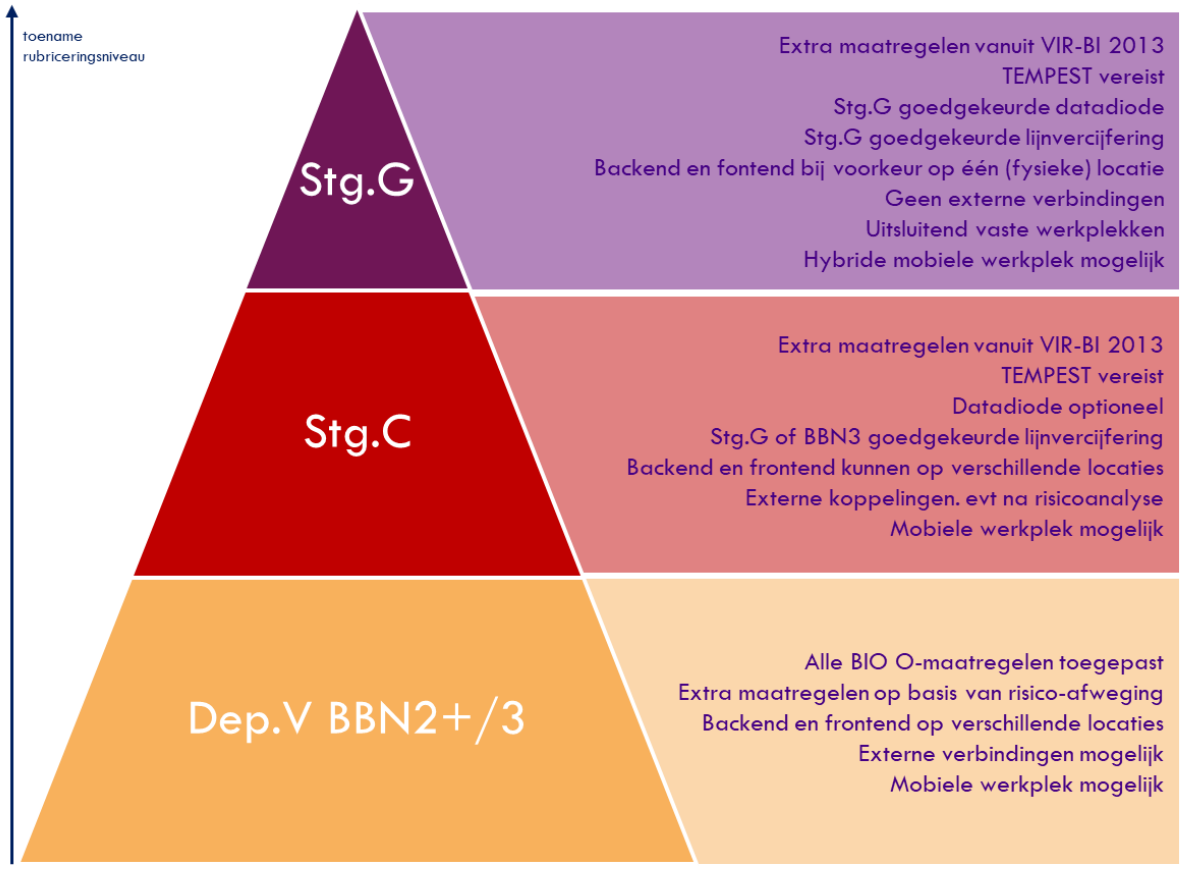
- BIO v1.04zv + BBN2+ voor gemeenten
- ISO/NEN 27001,27002
- VIR-BI 2013
- VBV32000(B)
- AIVD: NBV – Geëvalueerde producten
- GDPR/AVG
- WPG
- VIR 2007
- Evt. Wet op de bijzondere opsporingsdiensten
- NORA
- Pas-toe-of-leg-uit beleid
- CIS compliance baseline
- CC / EAL

Complicerende factoren
Op dit moment zijn er 2 complicerende factoren die de haalbaarheid van de werkplekconcepten, in bepaalde situaties, dwars kunnen zitten:

1. Er zijn momenteel geen door de NBV goedgekeurde ICT-componenten voor het niveau Stg.C beschikbaar.
2. De BBN3 norm is (nog) niet geformaliseerd. Daarom is bij het opstellen van dit visie document uitgegaan van de BBN2+ maatregelen voor gemeenten.

[1] NBV: Nationaal Bureau voor Verbindingsbeveiliging, Het NBV ondersteunt de Rijksoverheid bij de beveiliging van bijzondere informatie, zoals staatsgeheimen. Met kennis en expertise van voornamelijk de technische maatregelen in de informatiebeveiliging, helpt het NBV zijn klanten om bijzondere informatie zoals staatsgeheimen te beschermen
[2] Rubricering: het bepalen van het rubriceringsniveau en -duur van de bijzondere informatie op basis van de te verwachten nadelige gevolgen voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries als (een deel van) deze informatie bekend wordt bij niet geautoriseerde personen.

Overzicht en samenhang
In onderstaand figuur (figuur 1) is schematisch een overzicht en samenhang van de verschillende regels en maatregelen weergegeven die genomen moeten worden, al naar gelang het rubriceringsniveau toeneemt van laag naar hoog.



Figuur 1: schematische weergave regels en maatregelen. regels en maatregelen.

Zoals in figuur 1 is weergegeven worden, naar mate het rubriceringsniveau toeneemt, naast de noodzakelijke technische voorzieningen ook diverse procedures en andere regelgeving opgelegd.

Basisarchitectuur: variaties op een bekend thema
De best werkende oplossing voor elk rubriceringsniveau, met het oog op de praktische gebruiksmogelijkheden, is een uitgebalanceerde combinatie van beschikbare techniek, procedures en maatregelen. Vanuit deze visie is het zeer wel mogelijk een basisarchitectuur te hanteren per rubriceringsniveau, die op haar beurt op maat aangepast kan worden door specifieke functionele eisen van een bepaalde dienst. In feite is het hierdoor mogelijk efficiënter om te gaan met de middelen.

Van "openbaar" naar hoogbeveiligd
De werkzaamheden van gebruikers van hoogbeveiligde werkplekken bestaan in veel gevallen voor slechts een beperkt deel uit de verwerking van staatsgeheim gerubriceerde gegevens. In de meeste gevallen wordt met "openbare" informatie gewerkt. Echter het combineren van diverse informatie, die al dan niet uit openbare gegevensbronnen afkomstig is, met de dienst-specifieke kennis en inzichten, kan leiden tot een hoger rubriceringsniveau dan de oorspronkelijk verkregen inzichten en gegevens. Dit betekent dat de werkplek aan het hoogste rubriceringsniveau van de betreffend dienst moet voldoen.

In praktijk betekent dit dat voor een groot deel van de werkzaamheden van de gebruikers de extra beveiligingsmaatregelen van een hoog beveiligde werkplek als zeer beperkend of belemmerend worden ervaren. Te denken valt aan zaken als OSINT[3], inwinning of het bekijken van (live) camerabeelden. Kortom, dit geldt voor alle werkzaamheden waar het openbaar internet voor benodigd is.

Controleerbare mogelijkheden
Op basis van een risicoafweging, is het echter zeer wel mogelijk om specifieke werkplekken voor specifieke functies in te zetten, die niet volledig aan de staatsgeheime eisen voldoen, maar wel een basisbeveiliging geïmplementeerd hebben waardoor de veiligheid hoger is dan van een willekeurig systeem. Op deze manier wordt zogenaamde shadow-IT voorkomen en blijft de organisatie in control.

Voor de eerdergenoemde use-case OSINT kunnen al dan niet getempesteerde laptops worden aangeschaft, die worden voorzien van: encryptie, VPN-oplossingen en beperkte gebruikersrechten. Vervolgens kunnen de opgehaalde gegevens eventueel via een datadiode worden geüpload naar het hooggerubriceerde platform.

Gegevensuitwisseling
Daarnaast bestaat bij verschillende diensten de behoefte om regelmatig op een veilige, gecontroleerde wijze gegevensuitwisseling tussen verschillende gerubriceerde werkplek niveaus, omgevingen en domeinen mogelijk te maken. Zowel van "laag- naar hoog-", als van "hoog- naar laag-" gerubriceerde werkplekken.

Voor wat betreft gegevensuitwisseling tussen verschillend gerubriceerde omgevingen is het inzetten van een dubbele datadiode een controleerbare mogelijkheid, waarbij het versturen van gegevens van hoog gerubriceerd naar laag gerubriceerd wordt ingeperkt door een goedkeuringsportaal. Via dit portaal moet eerst, per uitwisseling, goedkeuring worden gegeven door een derde persoon (CISO/leidinggevende), voordat een gerubriceerd document in versleutelde vorm kan worden "verstuurd" naar het lager gerubriceerde platform. Door het nemen van extra maatregelen, zoals de hiervoor vermelde procedure, en het uitschakelen van o.a. de USB-toegang op de werkplekken, worden gegevenslekken vrijwel uitgesloten.

Bring Your Own Device (BYOD)
Wat betreft BYOD zijn er ook, al dan niet in beperkte mate, mogelijkheden om met gerubriceerde gegevens te kunnen werken. Door het inzetten van een versleutelde USB-opstartstick of portable disk wordt de eigen BYOD-laptop of -computer opgestart in een veilige virtuele omgeving, zonder de mogelijkheid tot gegevensuitwisseling tussen het eigen/persoonlijke systeem en de veilige virtuele omgeving. Op deze wijze worden de gegevens van de gebruiker zelf niet gebruikt en is het mogelijk een gecontroleerde omgeving op het eigen systeem te creëren. Vanuit de omgeving op de stick/disk kan dan vervolgens verbinding worden gemaakt met de gerubriceerde omgeving. Hierbij wordt bij voorkeur multifactor authenticatie toegepast.

[3] Open Source Intelligence (OSINT) is een techniek om online sporen die openbaar zijn, op een slimme manier te vinden en te verzamelen.

Toekomstperspectief

Cloudontwikkelingen

Onze verwachting voor de nabije toekomst (2022 - 2027) is dat de publieke cloud blijft groeien en de volledige on-premises mogelijkheden grotendeels gaat verdringen. Er zullen steeds minder en minder fabrikanten kiezen voor de mogelijkheid om software in eigen beheer te houden, waardoor het meer en meer noodzakelijk wordt om een "open" verbinding te hebben met partijen in de publieke cloud.

Vanuit het gezichtspunt van de meeste leveranciers van software geldt dat cloudproducten als "veiliger" kunnen worden beschouwd op het gebied van cybersecurity. In de basis klopt dit, aangezien updates en patches automatisch worden doorgevoerd, waardoor lekken veel sneller worden gedicht en er geen afhankelijkheid is van menselijk handelen in een "gesloten" eigen omgeving. Daarnaast zorgt de kracht van de publieke cloud ervoor, dat fabrikanten zeer flexibele producten kunnen leveren aan hun klanten, die over veel uitgebreidere mogelijkheden kunnen beschikken dan wanneer zij on-premises zouden worden uitgevoerd. Dit is voor de overgrote meerderheid van zowel klanten als leveranciers zeer aantrekkelijk. Een probleem voor gevoelige overheidsinformatie is dat de publieke cloud veelal onder Amerikaanse regelgeving valt en daardoor impliciet een aantal afhankelijkheden met zich meebrengt die in potentie niet wenselijk zijn. Hierdoor zal het lastig zijn voor de overheidsinstanties, die met gerubriceerde gegevens werken, om te profiteren van deze vooruitgangen. Alternatieven, zoals bijvoorbeeld het creëren van een eigen hoogbeveiligde Rijkscloud voor de verwerking en opslag van gerubriceerde gegevens lijken tot op heden niet van de grond te komen.

Wat zou wel kunnen voor Stg.G?

Voor een omgeving waar met name Stg.G gerubriceerde gegevens worden verwerkt en opgeslagen zijn er wat de publieke cloud betreft op korte termijn dus niet veel mogelijkheden te verwachten. Maar, wat wel zou kunnen is naar een "bundeling van de krachten" tussen de verschillende overheidsdiensten toe te werken. Door meer samenwerking, in de zin van het delen van (ICT-)resources en gemeenschappelijk gebruik van bepaalde voor Stg.G geschikte voorzieningen, zoals de behuizing van datacenters, is in potentie een grotere efficiëntie (kostendeling) te halen met een minimaal gelijkblijvende effectiviteit en verbeterde robuustheid van de systeemoplossing (kennis, resources en continuïteit). Hiervoor is echter wel de nodige politieke en ambtelijke wil vereist, om gezamenlijk met alle betrokken partijen tot heldere afspraken en verantwoordelijkheden te komen.

Mogelijk zorgt de groei en de toenemende mogelijkheden van de publieke cloud uiteindelijk tot een scenario waarbij een goede samenwerking tussen de diensten onontkoombaar wordt om de kosten te beperken en de mogelijkheden te vergroten.

Is een mobiele werkplek haalbaar?

Wel zien wij mogelijkheden om, met enige beperkingen, mobiel te werken. Door getempesteerde laptops te gebruiken in combinatie met een uploadfaciliteit, eventueel via een datadiode, zou er mogelijk een hybride situatie gebouwd kunnen worden gebaseerd op een officieel goedgekeurd Stg.G platform. Dit platform is dan op een veilige wijze te combineren met weliswaar goed beveiligde, maar niet officieel goedgekeurde, mobiele werkplekken. Op deze manier is er in ieder geval een oplossing voorhanden indien de situatie

hier om vraagt. Ook kan zo'n werkplek gebruik worden voor speciale gevallen als OSINT, veilige verslaglegging en/of op alternatieve locaties, etc.

Voor Stg.C kan meer
Wat betreft Stg.C en Dep.V BBN3 zien wij meer mogelijkheden. Hierbij valt te denken aan hybride cloudoplossingen, waarbij de gegevensstromen zodanig gescheiden worden dat de extra beveiligde informatie niet in de publieke cloud terecht komt, en mocht dit toch gebeuren, dat deze zodanig versleuteld is dat dit geen ernstig verhoogd risico op gegevenslekken oplevert. Er moet dan gedacht worden aan het werken met encryptiesleutels die alleen on-premises beschikbaar zijn, in combinatie met logische en/of fysieke scheidingen in het netwerk.

Mobiel werken
Hoewel ook voor de Stg.C werkplek op korte termijn geen officiële goedkeuring verwacht wordt, is het onzes inziens toch goed mogelijk een goed beveiligde, mobiele werkplek aan te bieden. Dit door aan de BBN3 mobiele werkplek enkele extra veiligheidsmaatregelen mee te geven (bijvoorbeeld geen gebruik van WiFi, eigen "geheime" APN voor 5G, evt. tempest of alleen toegang tot bepaalde afgeschermde delen van het netwerk vanaf een mobiele werkplek) is het beveiligingsniveau aanzienlijk te verbeteren. Uiteraard zal hier een uitgebreide risicoanalyse aan vooraf moeten gaan, of het geheel van maatregelen afdoende is voor de specifieke situatie.

Afsluitend, terugkomend op de eerdergenoemde complicerende factor
Zekerheid is van essentieel belang. En goedkeuringsstempel van het NBV geeft aan dat de componenten zeer secuur zijn onderzocht en voldoen aan de veiligheidseisen die het NBV daaraan stelt. De eerdergenoemde complicerende factor is: "er zijn momenteel geen door de NBV goedgekeurde ICT-componenten voor het niveau Stg.C beschikbaar".

Toch zijn, hoewel misschien niet ideaal, oplossingen te realiseren die aan de specifieke behoefte en in specifieke situaties kunnen voldoen. Voor een Stg.C omgeving zijn 2 mogelijkheden toepasbaar:

- Een combinatie van door het NBV goedgekeurde producten op Dep.V/BBN3 niveau en extra mitigerende maatregelen, of
- De oplossing baseren op componenten die goedgekeurd zijn voor Stg.(Z)G.

Maar voor alles geldt:
risicoafweging, doelmatigheid, controleerbaarheid, robuustheid en continuïteit van de oplossing en het gebruik daarvan, én natuurlijk gezond verstand.

Metis IT heeft ruime ervaring in het werkveld van hoog beveiligde omgevingen en met het bedenken, opstellen en inrichten van deze omgevingen binnen de rijksoverheid en private markt. Vanuit deze expertise kunnen de consultants van Metis IT hierin uitgebreid advies leveren en in nauwe samenwerking met de betreffende dienst een veilig totaalconcept creëren, passend bij de werkzaamheden van de gebruikers.