1

Van: 5.1 (2e) - BD/NCSC/IVT
Verzonden: maandag 11 juli 2022 15:45
Aan: 5.1 (2e) ; 5.1 (2e) @belastingdienst.nl'
Onderwerp: concept memo/whitepaper 'open source security'
Bijlagen: Open Source Security.docx

Dag en 5.1 (2e

We zijn eerder ons vervolgtraject op het gebied van 'rijksbrede cybervraagstukken' gestart met de intentie om aan de slag te gaan met de security aspecten die samenhangen met open source. Dit is nu wat meer de kant van SBOM op gegaan, en dat is helemaal prima. Wel ligt er nog het vraagstuk van de security aspecten mbt Open Source. Dat is toch ook wel wear wat meer relevant geworden door de politiek discussie over het gebruik van open source binnen de overheid.

Daarmee heb ik de pen gepakt en een aantal zaken die te maken hebben met open security opgetikt. Zie bij deze de aanzet. Doel is om 1) inzichtelijk te maken dat er risico's en opletpunten zijn mbt Open Source en 2) hoe die opgepakt kunnen worden. Het is een eerste aanzet, hoewel hopelijk leesbaar. Een versie daarna, met jullie aanvullingen/opmerkingen verwerkt, kan dan naar de werkgroep.

Graag aan jullie de vraag wat jullie er van vinden, of er nog zaken missen, dan wel andere opmerkingen/reflecties. Doel is het uiteindelijk uit te brengen. Hoe en aan wie is nog even de vraag .

Hoor het graag en met groeten,
5.1(2e

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: maandag 11 juli 2022 15:56
Aan: 5.1(2e) - BD/NCSC/SK
Onderwerp: FW: concept memo/whitepaper 'open source security'
Bijlagen: Open Source Security.docx

Hy 5.1(2e), bij deze. Eerder heb ik met en 5.1(2e) het gehad over de wenselijkheid van een stuk als dit. Jan heeft ook aangegeven hier input voor te willen leveren. Mocht je al input/aanvullingen hebben, laat het vooral weten.

Met groeten, 5.1(2e

Van: 5.1(2e) < 5.1(2e) @uwv.nl>
Verzonden: woensdag 20 juli 2022 08:44
Aan: 5.1(2e) - BD/NCSC/IVT; 5.1(2e) @belastingdienst.nl'
Onderwerp: RE: concept memo/whitepaper 'open source security'
Bijlagen: Open Source Security.docx

5.1(2e

Prima nota! Wellicht is een samenvatting/kern aan het begin van de notitie goed – zie ook eerste aanzet in de notitie. Moeten we nog iets zeggen over de SBOM en op welke manier je dit beter/sneller kan beheersen? Is er naast de privacy by design, CI/CD ook aanvullend nog een aanbeveling voor monitoring / detectie en response als het om OSS gaat?

5.1(2e)

Van: 5.1(2e) @belastingdienst.nl
Verzonden: woensdag 20 juli 2022 09:04
Aan: 5.1(2e) - BD/NCSC/IVT
CC:
Onderwerp: Re: concept memo/whitepaper 'open source security'
Bijlagen: Open Source Security.docx

Hallo 5.1(2e)

Ik sluit me bij 5.1(2e) aan een prima notitie en wat mij betreft leidt het tot een formeel afwegingskader.

Daar sluiten de opmerkingen van 5.1(2e) naadloos op aan. Een stelling kan zijn dat zonder aanwezigheid van SBOM het onverantwoord is om OSS te gebruiken. Daarmee mitigatie aan de voorkant.

Vervolgens is het punt van geautomatiseerde monitoring noodzakelijk, wat mij betreft een verplichting.

Je kunt zelfs nadenken Wbni Combinatie tussen monitoring en geautomatiseerde policies in de pipeline

Met vriendelijke groet,

5.1(2e)
5.1(2e)
5.1(2e)
Belastingdienst
Laan van Westenenk 492 | 7334 DS | APELDOORN | 1e etage
Postbus 9050 | 7300 GM | APELDOORN
Secretaresse 5.1(2e)

M 5.1(2e)
E @belastingdienst.nl

http://www.belastingdienst.nl

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: woensdag 20 juli 2022 10:03
Aan: 5.1(2e) - BD/NCSC/IVT; 5.1(2e) - BD/NCSC/IVT; 5.1(2e) - BD/NCSC/SK; 5.1(2e) @ncsc.nl'
CC: 5.1(2e) - BD/NCSC/SK
Onderwerp: aanzet open source security advies
Bijlagen: Open Source Security.docx

Beste collega's,

Jullie kennen wellicht nog het interdepartementale traject rondom 'strategische cybersecurity vraagstukken Rijk'. Diverse NCSC collega's hebben daarvoor een bijdrage geleverd en het eindrapport is input geweest voor de nadere uitwerking van de I-Strategie Rijk.

De trekkers van dat traject, waaronder ikzelf, hebben daarna een beperkte doorstart gemaakt met een klein nieuw vervolgtraject waarbij de focus is uitgegaan naar de twee specifieke thema's: Open Source security en de toepassing van SBOM. Beiden eigenlijk als uitvloeisel van de Log4J kwetsbaarheid.
Vanuit het NCSC participeren 5.1(2e) en ik in dit traject. Naast dat we een aantal zaken (laten) uitwerken in het traject rondom SBOM heeft dus ook Open Source security specifiek de aandacht. Op dit moment ben ik bezig [redacted] JWV en [redacted] Belastingdienst om tot een adviesstuk te komen rondom de security afwegingen/vraagstukken/issues ten aanzien van de inzet van open source. Reden hiervoor is ook omdat het Rijksbrede beleid rondom de inzet van open source op dit moment de nodige aandacht heeft.

Een eerste aanzet voor een advies (old) ten aanzien van Open Source security, treffen jullie aan in de bijlage. Zouden jullie de komende paar weken hier een blik op kunnen werpen en eventuele aanvullingen, onjuistheden, omissies e.d. kunnen doorgeven? Dan kunnen we die verwerken in een volgende versie. Daarin zal ook een samenvatting komen en waarschijnlijk ook een aantal zaken ten aanzien van security governance (wie stelt kaders en ziet toe op naleving/borging daarvan?).

Een belangrijk ander aspect wat we er in willen brengen is een soort afwegingskader voor de inzet van Open Source, met elementen zoals:
- Voer altijd een risicoanalyse uit ten aanzien van de inzet van OSS en weeg daarin de robuustheid, professionaliteit van de betrokken OSS community mee. En definieer afspraken over de monitoring daarvan.
- Bepaal threshold waardes ten aanzien van:
  - Code kwaliteit, code ouderdom, commit frequentie, etc. en monitor dit..
- Voer altijd een technische due diligence analyse uit op de OSS code alvorens deze in te zetten in de eigen omgeving. Nieuwe releases worden ook altijd getest en gevalideerd in de eigen geautomatiseerde CI/CD omgeving.
- Overweeg OSS alleen toe op het moment dat de OSS integratie is gekoppeld aan een SBOM oplossing, al dan niet in een geautomatiseerde CI/CD straat.

- code signing.
- ..... etc etc

Mochten jullie hier ideeën bij hebben laat het vooral ook weten.

Mochten jullie hier opmerkingen, aanvullingen, correcties e.d. bij hebben laat het vooral weten voor medio augustus. Na mijn vakantie maak ik een volgende versie.

Met groeten,
5.1(2e

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: woensdag 20 juli 2022 10:31
Aan: 5.1(2e) @belastingdienst.nl'; 5.1(2e)
Onderwerp: RE: concept memo/whitepaper 'open source security'

Dag heren, dank voor jullie feedback en input. Allemaal goede punten. Ik zal ze verwerken in een volgende versie. Die zal wel pas komen na mijn vakantie in augustus vrees ik..:)

Ook de opmerkingen tav een richtlijn/richtsnoer lijken me een hele goede. Een aanzet daarvoor zal ik ook in de volgende versie meenemen. Inclusief het punt over de threshholds. Lijkt me goed om daar dan eens nader over door te praten. Wbni Wbni mede ook om OSS (libraries) kwetsbaarheden/afhankelijkheden in kaart te brengen en te registreren. Ben benieuwd of we daar ook met threshholds zouden kunnen werken.

Wordt vervolgd en op naar een volgende versie!

Grtn 5.1(2e)

Van: 5.1(2e) - BD/NCSC/SK
Verzonden: woensdag 17 augustus 2022 16:54
Aan: 5.1(2e) - BD/NCSC/IVT
Onderwerp: RE: concept memo/whitepaper 'open source security'

Hoi 5.1(2e)

Dank voor je mail en de inspanningen op het memo! Ik ben de afgelopen maand afwezig geweest, en ben daarnaast vanaf morgen ook 2,5 week afwezig. Ik wilde je laten weten dat ik daarna pas de mogelijkheid heb om inhoudelijk naar het memo te kijken. Ik denk dat het document ook intern goed als basis kan dienen, vooral richting het contact Wbni (dat raakt aan OSS) dat verder opgezet gaat worden.

Groeten,
5.1(2e)

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: maandag 11 juli 2022 15:56
Aan: 5.1(2e) - BD/NCSC/SK
Onderwerp: FW: concept memo/whitepaper 'open source security'

Hy 5.1(2e), bij deze. Eerder heb ik met 5.1(2e) het gehad over de wenselijkheid van een stuk als dit. [redacted] heeft ook aangegeven hier input voor te willen leveren. Mocht je al input/aanvullingen hebben, laat het vooral weten.

Met groeten, 5.1(2e

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: maandag 5 september 2022 09:48
Aan: 5.1(2e) '; 5.1(2e) @belastingdienst.nl'; 5.1(2e) - BD/DII/RPP; 5.1(2e) ; 5.1(2e) - BD/NCSC/SK; BD/DII/ICS; - BD/DII/ICS;
Onderwerp: open source security - RE: Samenwerking Cybersecurity- Opensource en Log4j.
Bijlagen: 20220722 concept Open Source Security [redacted] docx

Beste allen,

Vanmiddag hebben we weer overleg. Graag geef ik dan even een korte update over bijgevoegde concept memo inclusief handreiking over 'security rondom de inzet van open source'. Vanwege de vakantie heb ik helaas het stuk niet eerder kunnen versturen naar jullie. Een eerdere versie hebben [redacted] van commentaar voorzien. Dat is grotendeels verwerkt. Wat met name nog mist is de samenvatting.

Ik zou er op willen koersen om het stuk de komende weken zodanig af te ronden dat het naar de opmaak kan. Er is dus nog zeker tijd en ruimte voor opmerkingen, aanvullingen e.d.

Tot vanmiddag!
Grtn 5.1(2e

-----Oorspronkelijke afspraak-----
Van: 5.1(2e)
Verzonden: donderdag 23 juni 2022 09:22
Aan: 5.1(2e) ; 5.1(2e) @belastingdienst.nl'; BD/NCSC/IVT; 5.1(2e) - BD/DII/RPP; 5.1(2e) ; 5.1(2e); 5.1(2e) BD/NCSC/SK; BD/DII/ICS; - BD/DII/ICS; 5.1(2e)
Onderwerp: Samenwerking Cybersecurity- Opensource en Log4j.
Tijd: maandag 5 september 2022 16:15-17:00 (UTC+01:00) Amsterdam, Berlijn, Bern, Rome, Stockholm,
Wenen.
Locatie: MS-Teams

Beste allen,

Zoals al aangekondigd via de mail ontvangen jullie hierbij een uitnodiging voor de bespreking Samenwerking Cybersecurity – Opensource en Log4j op maandag 5 september a.s. van 16:15 uur tot 17:00 uur in MS-Teams.

Het is lastig om een datum te vinden die bij iedereen in de agenda's past, maar er moet wel een vervolgmeeting worden gepland.
Ik hoop dat dit tijdstip lukt.

Groeten,
5.1(2e)

5.1(2e)

UWV
Concern ICT/CIO OFFICE
La Guardiaweg 116-162 1043 DL Amsterdam
Locatie AMSG3 / D12
Postbus 58285 1040 HG Amsterdam
T 5.1(2e)
E

Van: 5.1(2e) BD/NCSC/IVT
Verzonden: maandag 26 september 2022 10:21
Aan: - BD/NCSC/SK; - BD/NCSC/OP; 5.1(2e) - BD/NCSC/IVT; 5.1(2e) - BD/NCSC/SK; BD/NCSC/SK; BD/NCSC/OP
Onderwerp: concept advies 'open source security' - graag eventueel commentaar.
Bijlagen: 20220919 concept Open Source Security.docx

Beste collega's,

Door de interdepartementale werkgroep 'Open Source security en SBOM' wordt gewerkt aan een aantal adviesproducten om de security aspecten/risico's van OS beter beheersbaar te maken. Ook het concept SBOM krijgt speciale aandacht. De werkgroep is een initiatief van een aantal CIO's en CTO's/directeuren van grote uitvoeringsorganisaties en het NCSC. Zelf zit ik hier in namens het NCSC. Tot recent zat ook 5.1(2e) hierin.

In werkgroep verband is gewerkt aan bijgevoegd advies over 'open source security'. Ik ben hier de penvoerder van, in nauwe afstemming met 5.1(2e)) en Belastingdienst (5.1(2e)). Het streven is om dit stuk op korte termijn als advies product formeel uit te brengen. Logischerwijs is dat denk ik dan een advies of whitepaper van het NCSC.

Zouden jullie dit stukken lezen en eventuele opmerkingen, aanvullingen, commentaar terug kunnen geven voor uiterlijk 9 oktober a.s.? Bij voorkeur in de vorm van concrete tekstsuggesties. Binnen de werkgroep zal parallel ook een laatste redactieronde plaats vinden.

Alvast hartelijk dank en met groeten,
5.1(2e

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: maandag 26 september 2022 10:33
Aan: 5.1(2e) @rws.nl)
Onderwerp: concept stuk over open source security
Bijlagen: 20220919 concept Open Source Security.docx

Hy 5.1(2e

Hoop dat alles goed gaat?

Door de interdepartementale werkgroep 'Open Source security en SBOM' wordt op dit moment gewerkt aan een aantal adviesproducten om de security aspecten/risico's van open source beter beheersbaar te maken. De werkgroep is een initiatief van een aantal CIO's en CTO's/directeuren van grote uitvoeringsorganisaties en bouwt voort op het traject waar we samen eerder ook aan hebben gewerkt:
'Strategische Cyber Security Vraagstukken Rijk'. Eén van de daarin toen benoemde onderwerpen was open source security. Dat heeft nu als vervolg een eigen traject gekregen. Zelf zit ik hier in namens het NCSC. Trekker is 5.1(2e). Daarnaast zitten er collega's in van Politie, UWV en MinJus.

In werkgroep verband is gewerkt aan bijgevoegd advies over 'open source security'. Ik ben hier de penvoerder van, in nauwe afstemming met 5.1(2e) en 5.1(2e). Het streven is om dit stuk op korte termijn als advies product formeel uit te brengen.

Zou je dit stuk kunnen tegenlezen? Ik hoop dat je de gelegenheid hebt om me eventuele opmerkingen, aanvullingen, commentaar terug te geven voor uiterlijk 9 oktober a.s.?

Alvast hartelijk dank en met groeten!
5.1(2e

Van: 5.1(2e) @rws.nl>
Verzonden: woensdag 28 september 2022 16:45
Aan: 5.1(2e) - BD/NCSC/IVT
Onderwerp: RE: concept stuk over open source security
Bijlagen: 20220919 concept Open Source Security - [redacted]docx

Hey 5.1(2e),
Goed bezig! Wel wat snel gereviewed, maar hier mijn review, succes!!

Met vriendelijke groet,

5.1(2e) MSc CISSP

Van: 5.1(2e) - BD/NCSC/SK
Verzonden: woensdag 5 oktober 2022 13:30
Aan: 5.1(2e) - BD/NCSC/IVT
CC: - BD/NCSC/SK
Onderwerp: Review concept advies 'open source security'
Bijlagen: 20220919 concept Open Source Security_Tegenlezen.docx

Beste 5.2(2e),

Mijn naam is 5.1(2e) en ik ben drie weken geleden als adviseur bij A&K gestart. 5.1(2e) heeft een aantal mensen in het team gevraagd om het advies over 'open source security' te lezen en van eventuele opmerkingen, aanvullingen of commentaar te voorzien. Ik heb dit gebundeld en in één document ondergebracht.

We vonden het een goed stuk en hebben niet zozeer suggesties voor de inhoud, maar met name voor de vorm. We hebben deze suggesties zo duidelijk mogelijk omschreven, maar ik kan me voorstellen dat er misschien nog vragen of onduidelijkheden bestaan. Mocht dit zo zijn, dan licht ik deze graag mondeling toe.

Met vriendelijke groet,

5.1(2e)

Ministerie van Justitie en Veiligheid | Ministry of Justice and Security
Nationaal Cyber Security Centrum (NCSC) | National Cyber Security Centre (NCSC)

M: 5.1(2e) E: 5.1(2e)@minjenv.nl
Werkdagen: ma/di/wo/do

Turfmarkt 147 | 2511 DP | Den Haag
Postbus 117 | P.O. Box 117 | 2501 CC | Den Haag | The Netherlands

---

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: dinsdag 8 november 2022 09:02
Aan: 5.1(2e) - BD/NCSC/SK; 5.1(2e) - BD/NCSC/SK; 5.1(2e) - BD/NCSC/OP; 5.1(2e) - BD/NCSC/IVT; 5.1(2e) - BD/NCSC/Staf; 5.1(2e) - BD/NCSC/IVT; Communicatie - NCSC
Onderwerp: 0.9 def concept van advies 'open source security'
Bijlagen: 20221107 Factsheet Open source security CONCEPT.dotx

Beste collega's,

Op basis van eerder commentaar een aanvullingen van een aantal van jullie stuur ik bij deze de 0.9 versie van het stuk toe. Ten opzicht van de vorige versie is met name de samenvatting/eerste deel veranderd op advies van 5.1(2e). Mochten jullie nog feitelijke onjuistheden of andere cruciale omissies zien, laat het vooral weten.

Ik zou er naar willen streven dan het stuk klaar is voor publicatie over een 2 tal weken. Ik hoop daarmee dat het lukt om voor de 16de november eventuele onjuistheden/omissies door te geven.

@Communicatie: worden factsheets extern/apart nog opgemaakt ? Of is deze opmaak in het sjabloon toerelkend?

Dank en met groeten,
5.1(2e

Van: 5.1(2e) - BD/NCSC/SK
Verzonden: donderdag 10 november 2022 16:27
Aan: 5.1(2e) - BD/NCSC/SK
CC: - BD/NCSC/IVT
Onderwerp: FW: 0.9 def concept van advies 'open source security'
Bijlagen: 20221107 Factsheet Open source security CONCEPT.dotx

Urgentie: Hoog

Ha 5.1(2

Zie onderstaande vraag van 5.1(2e. Ik weet niet precies welke afspraken we hierover hebben. Natuurlijk was jij vooral van de afspraken rond het Cyberadvies, maar ik denk dat we die wel als richtlijn kunnen aanhouden. (Ik weet in ieder geval dat 5.1(2e) mij altijd een sms-je stuurt ter aankondiging dat er iets aan komt, maar het daadwerkelijk doorsturen van documenten gebeurt door en aan anderen tussen NBV en NCSC.)
Kun jij 5.1(2e aangegeven wie we daarvoor dan als beste aanspreekpunt kunnen benaderen?

Dank,
5.1(2

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: donderdag 10 november 2022 16:07
Aan: 5.1(2e) - BD/NCSC/SK
Onderwerp: FW: 0.9 def concept van advies 'open source security'

Hy 5.1(2, de factsheet open source security nadert z'n voltooiing. Nu staat me bij dat we regelmatig het NBV/dienst ook vooraf op de hoogte stellen of hen informeren dat we iets uit gaan brengen. Weet jij welke afspraken daar over bestaan? Is dat altijd of alleen in bepaalde gevallen? Of weet je bij wie ik daarvoor moet zijn?

Met groeten en dank,
5.1(2e

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: vrijdag 11 november 2022 13:37
Aan: 5.1(2e) - BD/NCSC/SK; 5.1(2e) - BD/NCSC/SK
Onderwerp: RE: 0.9 def concept van advies 'open source security'

Hy 5.1(2e), dank voor de snelle reactie. @5.1(2, als ik je goed begrijp zou jij h'm naar je contact persoon kunnen mailen. Zou je dat willen doen? Ze kunnen er wel naar kijken en als ze fundamentele onjuistheden signaleren mogen ze die natuurlijk zeker nog even doorgeven. Een echte gedetailleerde review hoeft niet inderdaad. Een paar dagen later online brengen kan wel.

Als je dat zou willen doen, heel graag.

Grtn 5.1(2e

Van: 5.1(2e) - BD/NCSC/SK
Verzonden: vrijdag 11 november 2022 12:46
Aan: 5.1(2e) - BD/NCSC/SK
CC: - BD/NCSC/IVT
Onderwerp: RE: 0.9 def concept van advies 'open source security'

Hoi 5.1(en 5.1(2e,

Een factsheet zoals deze valt onder de langlopende producten, zoals we dat in de afstemming hebben genoemd. Ik maak zelf melding bij mijn contactpersoon welke langlopende publicaties er aan zitten te komen, daar zijn geen procedures voor in ons of hun operationele proces.

Als ik kijk naar het gewenste publicatietraject in de onderste mail ga ik ervan uit dat we hem niet meer ter review aan het NBV voor willen leggen.

Met vriendelijke groet,

5.1(2e)
Nationaal Cyber Security Centrum
5.1(2e)

Van: 5.1(2e) - BD/NCSC/SK <5.1(2e)@minjenv.nl>
Verzonden: donderdag 10 november 2022 16:27
Aan: 5.1(2e) - BD/NCSC/SK <5.1(2e)@minjenv.nl>
CC: - BD/NCSC/IVT <@minjenv.nl>
Onderwerp: FW: 0.9 def concept van advies 'open source security'
Urgentie: Hoog

Ha 5.1(2

Zie onderstaande vraag van 5.1(2e. Ik weet niet precies welke afspraken we hierover hebben.Natuurlijk was jij vooral van de afspraken rond het Cyberadvies, maar ik denk dat we die

wel als richtlijn kunnen aanhouden. (Ik weet in ieder geval dat 5.1(2e) mij altijd een sms-je stuurt ter aankondiging dat er iets aan komt, maar het daadwerkelijk doorsturen van documenten gebeurt door en aan anderen tussen NBV en NCSC.)
Kun jij 5.2(2e aangegeven wie we daarvoor dan als beste aanspreekpunt kunnen benaderen?

Dank,
5.1(e

Van: Communicatie - NCSC
Verzonden: donderdag 17 november 2022 12:50
Aan: 5.1(2e) - BD/NCSC/IVT
Onderwerp: RE: 0.9 def concept van advies 'open source security'

Dag 5.1(2e

Deze sjabloon is toereikend!

Groeten,

5.1(2

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: maandag 21 november 2022 10:40
Aan: 5.1(2e) - BD/NCSC/SK
Onderwerp: RE: 0.9 def concept van advies 'open source security'

Dank je.

Van: 5.1(2e) - BD/NCSC/SK
Verzonden: maandag 21 november 2022 10:29
Aan: 5.1(2e) - BD/NCSC/IVT
Onderwerp: RE: 0.9 def concept van advies 'open source security'

Hoi 5.1(2e)

Ik heb geen inhoudelijke reactie van het NBV gekregen.

Met vriendelijke groet,

5.1(2e)
Nationaal Cyber Security Centrum
5.1(2e)

Van: 5.1(2e) - BD/NCSC/IVT <5.1(2e)@minjenv.nl>
Verzonden: maandag 21 november 2022 10:17
Aan: 5.1(2e) - BD/NCSC/SK <5.1(2e)@minjenv.nl>

Onderwerp: FW: 0.9 def concept van advies 'open source security'

Hy 5.1(2, heb je wellicht nog opmerkingen vanuit het NBV ontvangen?

Met groeten,
5.1(2e)

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: vrijdag 11 november 2022 14:54
Aan: 5.1(2e) - BD/NCSC/SK <5.1(2e) @minjenv.nl>; 5.1(2e) - BD/NCSC/SK <5.1(2e) @minjenv.nl>
Onderwerp: RE: 0.9 def concept van advies 'open source security'

Top, Dank!

Van: 5.1(2e) - BD/NCSC/SK <5.1(2e) @minjenv.nl>
Verzonden: vrijdag 11 november 2022 14:45
Aan: 5.1(2e) - BD/NCSC/IVT <5.1(2e) @minjenv.nl>; 5.1(2e) - BD/NCSC/SK <5.1(2e) @minjenv.nl>
Onderwerp: RE: 0.9 def concept van advies 'open source security'

Hoi 5.1(2e),

Komt in orde. Ik laat het je weten als er inhoudelijke opmerkingen zijn.

Met vriendelijke groet,

5.1(2e)
Nationaal Cyber Security Centrum
5.1(2e)

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: vrijdag 9 december 2022 16:21
Aan: Communicatie - NCSC
Onderwerp: publiceren nieuwe factsheet Open Source Security
Bijlagen: FS Open source security 20221208.pdf

Beste collega's, van communicatie.

De definitieve versie van de factsheet 'Open Source Security' is inmiddels gereed gekomen. Zouden jullie deze kunnen publiceren op de website?

De volgende begeleidende tekst kan daarbij:

Open source software (OSS) heeft de afgelopen decennia wereldwijd een voorname stempel gedrukt op de ontwikkeling van digitale dienstverlening. Op dit moment bestaat het overgrote deel

van de digitale producten en diensten zelfs uit één of meerdere OSS-componenten. Open source is daarmee overal.

Het gebruik en de ontwikkeling van OSS kent diverse voordelen en (daardoor) een groeiende belangstelling. Naast voordelen kent de inzet van OSS echter ook specifieke risico's en uitdagingen. Het NCSC heeft hierover dit advies geschreven. Het gaat over de security risico's van OSS en over de daarbij behorende afwegingen en te nemen beheersmaatregelen.

Kunnen jullie het publiceren?

Dank alvast en met groeten,
5.1(2e)

Van: 5.1(2e) - BD/NCSC/IVT
Verzonden: dinsdag 3 januari 2023 09:15
Aan: 5.1(2e) - BD/NCSC/SK
CC: 5.1(2e) - BD/NCSC/SK; 5.1(2e) - BD/NCSC/SK; 5.1(2e) 5.1(2e) - BD/NCSC/SK; 5.1(2e) - BD/NCSC/SK
Onderwerp: RE: Factsheet Open Source Security

Beste 5.1(2e),

Dank nog voor je bericht. En nog de beste wensen.

Rond de Kerst hebben we het stuk van de website gehaald om zo voldoende ruimte en tijd te bieden aan 5.1(2e) en de mensen waarmee hij in contact staat om nog inhoudelijk op het stuk te reageren. Daarmee is er ook de gelegenheid voor jou en eventuele andere collega's om nog inhoudelijk op het stuk te reageren. Hierbij zou ik je willen vragen om bij voorkeur alle commentaar zoveel mogelijk te vervatten in concrete tekstvoorstellen. Ik hoop dat je begrijpt dat het anders lastig is om bijvoorbeeld je opmerkingen rondom zinsconstructies en langdradigheid scherp te krijgen en op een passende manier te verwerken. Mijn verwachting is dat 5.1(2e) komende week zijn gezamenlijke reactie doorstuurt. Ik zou in dat kader willen vragen om uiterlijk ook voor de 13de je tekstvoorstellen/review terug te sturen. Ik hoop dat dat lukt? Mocht het echt te krap tijd zijn, laat het even weten.

Met betrekking tot je laatste opmerking. Gedurende het schrijfproces zijn diverse S&K/A&K collega's betrokken; vanaf het prille begin tot aan het eind. Bij een flink aantal was dit traject dus bekend. Ik ga er vanuit dat zij, wanneer daar reden of noodzaak toe was gezien, dit stuk ook verder zouden hebben verspreid naar andere A&K collega's. Intern A&K is dat overigens ook gebeurd ihkv de inhoudelijke review.

Dank en met groeten,
5.1(2e)

Van: 5.1(2e) - BD/NCSC/SK
Verzonden: vrijdag 23 december 2022 13:35
Aan: 5.1(2e) - BD/NCSC/IVT
CC: 5.1(2e) - BD/NCSC/SK ; 5.1(2e) - BD/NCSC/SK ; 5.1(2e) BD/NCSC/SK ; 5.1(2e) - BD/NCSC/SK

Onderwerp: RE: Factsheet Open Source Security

Dag 5.1(2e),

Dank voor je uitgebreide reactie. Je geeft aan dat je openstaat voor correcties van onjuistheden, maar dat is niet het kernpunt van mijn kritiek. Het gaat mij om de algemene kwaliteit van het product.

Ik heb aangegeven dat ik het een langdradig stuk vindt, met ingewikkelde taalconstructies, gebruik maakt van niet objectieve bronnen en tendentieus is opgeschreven.

Langdradig
Elke factsheet tot nu toe heeft een zelfde opbouw die het idee van de Situation, Complication, Question volgt. Elk factsheet heeft een duidelijke kernboodschap die ondersteund wordt door de structuur van "Achtergrond", "Wat is er aan de hand", "Wat adviseert het NCSC". Dit factsheet heeft geen duidelijke kernboodschap en volgt niet die structuur. Daardoor heeft het niet de impact die het zou kunnen hebben.

Ingewikkelde taalconstructies
Dit stuk is niet toegankelijk voor een breed publiek. Het lijkt niet heel duidelijk gebruik te maken van een pyramidale schrijfstijl. De gemiddelde zin lengte in dit stuk is ontzettend hoog. Er wordt heel veel gebruik gemaakt van bijzinnen. Er wordt veel meer jargon gebruikt dan gebruikelijk in factsheets.

Niet objectieve bronnen
Een belangrijke bron voor dit stuk lijkt het OSSRA rapport te zijn van Synposys, waar maar liefst 4 keer naar verwezen wordt. De "wetenschappelijke" bronnen waar naar verwezen wordt zijn van dubieuze kwaliteit en voor zover ik kan zien niet ge-peer-reviewd.
In de wetenschappelijke literatuur is er op dit moment geen aanwijzing voor een verschil in risico of kwetsbaarheden in open vs closed source software. Analysis op dit gebied zijn veel genuanceerder en gaat met name over maturity van ontwikkelteams. Open of closed source is daarbij geen factor.
In het algemeen gebruikt dit stuk ook veel meer bronnen dan gebruikelijk in een factsheet, wat samenhangt met de eerder genoemde kritiek op de toegankelijkheid van het stuk.

Sowieso is het gebruikelijk om de partijen die hieraan bijdragen of reviewen te vernoemen.

Tendentieus
De insteek van het stuk is het veilig inzetten van open source software. Er wordt aangegeven dat OSS specifieke aandacht vereist. Maar alle aandachtspunten die benoemd worden gelden in een zelfde mate voor closed source software. Er wordt nergens in het stuk duidelijk genuanceerd dat er fundamenteel weinig verschil is tussen open en closed source.

De paragraaf die gaat over "Open source software'; veiliger dan closed source?" bevat niet echt een conclusie, maar wel veel tendentieuze beweringen. Er wordt verwezen naar oude bronnen en vooral aangegeven dat niet blijkt dat OSS veiliger is dan CSS.
Maar wat niet wordt gezegd, is dat er ook geen aanwijzingen CSS ook niet veiliger is dan OSS. In plaats daarvan worden er wel statistieken bij gehaald die een vergelijking maken tussen (gevonden!) kwetsbaarheden in open en closed source projecten. Terwijl die

statistieken niet zomaar te generaliseren zijn.

Ten slotte, qua QA. Ik blijf me verbazen dat het grootste deel van A&K niet afwist van het product en er niets over te zeggen hebben. Het uitbrengen van factsheets is de core business van A&K.

Groet,
5.1(2e)

From: 5.1(2e) - BD/NCSC/IVT <5.1(2e)@minjenv.nl>
Sent: 22 December 2022 16:36
To: 5.1(2e) - BD/NCSC/SK <@minjenv.nl>
Cc: - BD/NCSC/SK <5.1(2e)>; 5.1(2e) - BD/NCSC/SK <5.1(2e)@minjenv.nl - BD/NCSC/SK <5.1(2e)@minjenv.nl>; 5.1(2e) - BD/NCSC/SK <5.1(2e)@minjenv.nl>
Subject: RE: Factsheet Open Source Security

Dag 5.1(2e

Dank voor je bericht en goed dat je je beeld hierbij kenbaar maakt. Jammer dat het stuk niet aan je verwachtingen voldoet.

In reactie hierop het volgende:

Het stuk is opgesteld omdat hier extern veel behoefte aan bleek te bestaan. Tijdens het schrijven is ook afgestemd met een aantal externe partijen (binnen het Rijk) en ook intern is het stuk een aantal keren rondgestuurd voor feedback, review, aanvullingen, etc. Dat is ook gebeurd richting collega's van S&K. De review reactie die ik van de S&K collega's terug kreeg was o.a. dat zij het 'een goed stuk' vonden en 'weinig inhoudelijke punten' hadden. Meer in algemene zin kreeg ik van de tegenlezers/reviewers e.d. juist positieve reacties (ook over schrijfstijl). Ik vind het daarmee wat lastig om vast te stellen hoe zich dat precies verhoudt tot jouw reactie/oordeel.

Het uitgangspunt is natuurlijk dat ieder stuk dat we uitbrengen feitelijk juist is en geen fouten bevat. Vorige week heb ik al gesproken met 5.1(2e) die in contact staat met open source mensen die toen vergelijkbare bemerkingen hadden geuit als die jij hier doorgeeft, dat hij naar het stuk kijkt en daarbij aangeeft of/welke zaken nu precies echt onjuist zijn. Op het moment dat ik hem sprak had hij overigens geen specifieke onjuistheden paraat. Hij had het net als jij primair over schrijfstijl/vorm. Mocht je van oordeel zijn dat er zaken in het stuk staan die feitelijk onjuist zijn, laat het dan ook vooral weten. Als dat namelijk het geval is, dan kunnen we die onjuistheden aanpassen in een versie 1.1. Omdat ik tot op heden nog geen feitelijke onjuistheden heb gehoord, alle reviewcommentaar positief was en zo mogelijk is verwerkt, en er ook partijen zijn die er wel blij mee zijn :), ben ik terughoudend om het stuk al bij voorbaat terug te trekken.

De discussie rondom dit stuk raakt wel ook een breder vraagstuk. Dit is de eerste keer (naar mijn weten) dat er een WOO verzoek is ingediend vanwege een factsheet. Mijn verwachting is dat er in de toekomst alleen maar meer WOO verzoeken zullen komen waarin gevraagd

wordt om helderheid te verschaffen over ons handelen en onze afwegingen. Dat betekent dat we voor al onze producten de QA, herleidbaarheid, uitlegbaar e.d. goed op orde moeten hebben, ook daar waar het gaat om kennis/advies producten. Dit gaat zeker spelen op het moment dat we ons meer gaan uitspreken over zaken en er ook mensen zijn die het er niet mee eens zijn. De vraag is of we dat QA proces helemaal helder hebben, precies hebben uitgeschreven en adequaat ingericht hebben. Voor dit stuk heb ik de aanpak gevolgd zoals ik die ook bij andere interne trajecten heb gezien en gevolgd, waarbij de QA vooral in een brede review uitvraag zit. De vraag is, is de bestaande aanpak voldoende? Welke eisen hebben we in de toekomst aan de QA te stellen? Ik denk dat daar nog wel echt een verbeteropgave ligt.

Het lijkt met goed om hier in het nieuwe jaar, vanuit een breder perspectief, nog eens over door te praten. Wees tot die tijd vooral uitgenodigd om waar dat het geval is, feitelijke onjuistheden in het stuk terug te geven.

Met groeten,
5.1(2e)

Van: 5.1(2e) - BD/NCSC/SK <5.1(2e) @minjenv.nl>
Verzonden: donderdag 22 december 2022 13:16
Aan: 5.1(2e) - BD/NCSC/IVT < @minjenv.nl>
CC: - BD/NCSC/SK <5.1(2e) @minjenv.nl>; 5.1(2e) - BD/NCSC/SK <5.1(2e) @minjenv.nl>; - BD/NCSC/SK <5.1(2e) @minjenv.nl>
Onderwerp: Factsheet Open Source Security

Dag 5.1(2e),

Ik heb afgelopen dagen zitten dubben en wilde toch mijn zorgen kenbaar maken over de factsheet open source security. Ik wil vragen om te overwegen om de factsheet tijdelijk terug te trekken, te reviewen en later opnieuw te publiceren.
Ik heb hiervoor eerder vandaag 5.1(2e en 5.1(2 aangeschreven vanuit de veronderstelling dat het adviescluster, danwel de unit Kennisuitwisseling gaat over de publicatie van adviesproducten. Maar zij blijken hier niet over te gaan en niet het laatste woord te hebben over deze publicatie, beide tot mijn grote verbazing.

Ik vind eerlijk gezegd de inhoudelijke kwaliteit van de factsheet beneden de stand van het NCSC. Het is een langdradig stuk, gebruikt ingewikkelde taalconstructies, maakt niet gebruik van objectieve bronnen en is behoorlijk tendentieus geschreven.

Ik maak me zorgen om de publicatie van dit stuk, omdat het de (toekomstige) autoriteit van het NCSC als kennis en expertisecentrum aantast. De reacties vanuit de doelgroep en op social media zijn ook behoorlijk negatief en er is al direct een WOO verzoek ingediend over de totstandkoming van dit stuk.

En uit de indrukken die ik nu krijg, is dat WOO verzoek volledig terecht. Ik krijg sterk de indruk dat er voor dit factsheet niet de interne procedures zijn gevolgd die we normaalgesproken toepassen.

Dus, zouden we dan niet de eer aan onszelf houden en het stuk intrekken en er opnieuw naar kijken?

Ik realiseer me dat de timing lastig is, zeker nu 5.1 (2 e) op vakantie zijn. Maar toch lijkt me goed om hier snel op te handelen.

Groet,
5.1(2 e)