FS-20140617.04B

Dhr. Michiel Oosterwijk en dhr. Koen Sandbrink
Nationaal Cyber Security Centrum
Den Haag

**Forum Standaardisatie**

Bezoekadres:
Wilhelmina v Pruisenweg 52
2595 AN Den Haag
96810
2509 JE Den Haag
www.logius.nl

**Inlichtingen bij**
B.S.J. Knubben
*Senior Adviseur*
bart.knubben@logius.nl

**Datum**
28 mei 2014

notitie

Review "Beveiligingsrichtlijnen voor Webapplicaties, Deel 2" van NCSC (editie 2014, 1e review, d.d. 25-2-2014)

FORUM STANDAARDISATIE

## 1. Achtergrond

Het Nationaal Cyber Security Centrum (NCSC) heeft aan het Bureau Forum Standaardisatie (BFS) gevraagd om een review uit te voeren van de nieuwe concept-versie van de "Beveiligingsrichtlijnen voor Webapplicaties" (hierna: "NCSC-richtlijnen"). Deze notitie bevat het resultaat van de review.

## 2. Aanpak en opzet

De scope van de reactie omvat het werkdomein van Forum Standaardisatie, namelijk standaarden en interoperabiliteit. Aan deze notitie hebben Marco Davids (SIDN), Lancelot Schellevis en Bart Knubben (BFS) bijgedragen. De notitie zal nog ter informatie aan het Forum Standaardisatie worden voorgelegd.

In de eerstvolgende paragraaf staan een paar opmerkingen over de NCSC-richtlijnen als geheel. De paragraaf daarna bevat een inventarisatie van de relevante standaarden van de lijsten van het Forum Standaardisatie. In paragrafen daarna volgen relevante inhoudelijke opmerkingen, eerst die binnen de scope zijn en daarna ook een aantal overige opmerkingen.

## 3. Algemene opmerkingen

- Ondanks de omvang leest het prettig, is het duidelijk opgezet en een nuttige handleiding voor het inrichten van het beveiligingsbeleid. Het is wel zeer omvangrijk en daardoor waarschijnlijk niet gemakkelijk te 'handlen' voor de doelgroep. Je zou haast willen dat er een tool was, een applicatie of zo, die je door het geheel zou kunnen leiden.
- De informatie uit het document kan eenvoudiger worden hergebruikt door het niet als beveiligde PDF1.7, maar als PDF/A en/of als HTML te publiceren.
- Het is meer een handleiding voor het goed inrichten van het beveiligingsbeleid m.b.t. webapplicaties, dan een standaard. Het lijkt daarmee niet direct geschikt om als standaard te plaatsen op de 'pas toe of leg uit'-lijst. Toch willen we graag met NCSC verder in gesprek over of het zinvol is en, zo ja, hoe Forum/College eventueel op een andere wijze status zouden kunnen verlenen aan de NCSC-richtlijnen.

## 4. Relevante standaarden

Een webapplicatie kan verschillende koppelvlakken hebben die beveiligd moeten worden. Het primaire gebruikerskoppelvlak is eigenlijk altijd HTTP(S). Dat geldt ook voor de redacteur. Daarnaast is er veelal een e-mailkoppelvlak (wachtwoordherstel, nieuwsbrief, doorsturen gegevens ingevuld formulier etc.). Ook heeft de technisch beheerder vaak koppelvlakken ter beschikking, zoals SSH en FTP.

Hieronder staan de relevante standaarden voor deze koppelvlakken die zijn opgenomen op de 'pas toe of leg uit'-lijst[1] of op de lijst met gangbare standaarden[2] van het Forum Standaardisatie. In het onderstaande is per standaard aangegeven of deze vermeld is in het document van NCSC.

| Standaard | Lijst | Korte beschrijving | In NCSC-richtlijnen? |
|---|---|---|---|
| IPv6 en IPv4 | Pas toe of leg uit | Internetnummers | Nee |
| NEN-ISO27001 en 27002 | Pas toe of leg uit | Informatiebeveiliging | Ja |
| DNSSEC | Pas toe of leg uit | Beveiliging van domeinnamen | Ja |
| SAML2.0 | Pas toe of leg uit | Authenticatie | Ja |
| HTML | Gangbaar | Web opmaak taal | Ja |
| XML | Gangbaar | Taal voor gestructureerde content | Ja |
| HTTP | Gangbaar | Uitwisseling webgegevens | Ja |
| HTTPS | Gangbaar | Beveiligde uitwisseling webgegevens | Ja |
| TLS1.2 (in behandeling) | Pas toe of leg uit? | Protocol voor 'SSL-verbindingen' | Ja |
| AES | Gangbaar | Encryptie-algoritme | Nee |
| SHA-2 | Gangbaar | Hash-algoritme | Nee |
| X.509 | Gangbaar | Certificaten | Ja |
| UTF-8 | Gangbaar | Karakterset | Ja |
| SNMP | Gangbaar | Netwerken, managen apparatuur | Ja |
| FTP (SFTP / FTPS) | Gangbaar | Overdracht van bestanden | Ja |
| SSH | Gangbaar | Beveiligd protocol voor shell-instructies | Ja |
| DKIM | Gangbaar | E-mail authenticatie | Nee |
| SMTP | Gangbaar | E-mail versturen | Ja (niet STARTTLS voor SMTP) |
| POP3 | Gangbaar | E-mail ontvangen | Ja (niet STARTTLS voor |

[1] 'Pas toe of leg uit'-lijst met open standaarden: http://forumstandaardisatie.nl/ptolu
[2] Lijst met gangbare open standaarden: http://forumstandaardisatie.nl/gangbaar

| Standaard | Lijst | Korte beschrijving | In NCSC-richtlijnen? |
|---|---|---|---|
| | | | POP) |
| IMAP | Gangbaar | E-mail ontvangen | Nee |



## 5. Opmerkingen m.b.t. standaarden en interoperabiliteit

| # | Onderwerp, paragraaf en/of pagina | Opmerking |
|---|---|---|
| 1 | Algemeen | De in de vorige paragraaf genoemde standaarden hebben een status binnen de (semi-)publieke sector. In het NCSC-richtlijnen wordt (nog) niet gerefereerd aan deze status. |
| 2 | Algemeen | Een aantal relevante standaarden (IPv6, AES, SHA-2, DKIM, en POP3, IMAP, SMTP incl. STARTTLS) wordt niet vermeld in de NCSC-richtlijnen. |
| 3 | E-mail | E-mail-beveiliging (o.a. STARTTLS voor SMTP) en e-mailauthenticatie (DKIM en aanverwante standaarden DMARC en SPF) lijkt relevant maar komt niet aan bod. Het document bevat wel de volgende citaten: "Voor CSRF kan dit via links op malafide website en in e-mails." (p.83) en "Spoofing is jezelf voordoen als een ander. Iemand kan het e-mailadres van een ander gebruiken als zogenaamd afzendadres, zodat de geadresseerde in verwarring raakt. Deze methode kan handig zijn voor de verspreiding van virussen, omdat de ontvanger zou kunnen denken dat de afzender betrouwbaar is." (p.172). |
| 4 | IPv6 | IPv6 wordt niet genoemd. Bij zaken als "IP-whitelisting" moet hier ook rekening mee worden gehouden. Daarnaast lijkt op zijn minst een verwijzing naar de volgende documenten op zijn plaats: NCSC-whitepaper over IPv6 (https://www.ncsc.nl/binaries/nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ip-versie-6-ipv6/1/Whitepaper%2BIP%2Bversie%2B6.pdf) en recente TNO-rapport over security testing van IPv6 (https://www.tno.nl/downloads/testing_the_security_of_IPv6_implementations.pdf). |
| 5 | 1.2 Webapplicaties (p. 1) en op alle andere plaatsen in het document waar aan RFC's wordt gerefereerd. | Goed om gericht te verwijzen naar relevante RFC's en bijbehorende URL's. Wel handiger om per RFC consequent naar de overzichtspagina in de IETF-datatracker te verwijzen ipv naar txt-versie. Dat vergroot het inzicht in samenhang. Voorbeeld is https://datatracker.ietf.org/doc/rfc2616/ |
| 6 | 1.12 Relatie met andere documenten (p.8) | Op verschillende plekken wordt ISO27001/27002 versie 2013 genoemd. Bedacht moet worden dat 2005-versies nu nog zeer courant en zijn op dit moment zijn opgenomen op de 'pas toe of leg uit'-lijst. Ook zijn de verschillende overheidsbaselines informatiebeveiliging (BIR, BIG etc.) gebaseerd op de 2005-versies. |
| 7 | Relatie met andere normen en | De relatie met ISO27001/27002 komt aan bod. De relatie met de overheidsbaselines informatiebeveiliging (BIR, BIG |

| # | Onderwerp, paragraaf en/of pagina | Opmerking |
|---|---|---|
| | standaarden (verschillende pagina's) | etc.) ontbreekt echter. |
| 8 | B.06 Public-Key Infrastructure (PKI)-beleid, p. 22 e.v. | Het lijkt logisch om hier ook te refereren aan PKIoverheid (http://www.logius.nl/producten/toegang/pkioverheid/). Daarnaast zou je hier referenties verwachten naar wet- en regelgeving (WEH) en normen (zoals ETSI TS 102 042 en TTP.NL Scheme). |
| 9 | B.06 Public-Key Infrastructure (PKI)-beleid, p. 22 e.v. | Hier zou je ook een referentie naar SHA-2 goed zijn en afraden van MD5 en SHA-1. SHA-2 staat op de lijst met gangbare standaarden van het Forum Standaardisatie ( https://lijsten.forumstandaardisatie.nl/open-standaard/sha-2). Ook lijkt nader advies over algoritmes hier op zijn plek (zie bijvoorbeeld rapport "Algorithms, Key Sizes and Parameters" van ENISA , http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-sizes-and-parameters-report). |
| 10 | B.07 Transactiebeleid, p.28 | In de tekst staat "beveiligde verbinding (zoals HTTPS)". Dat doet vermoeden dat er alternatieven zijn. De enige beveiligde verbinding van een webaplicatie voor de gebruiker is echter HTTPS; er zijn geen alternatieven. Als de webapplicatie ook nog mail verstuurd dan is STARTTLS voor SMTP wellicht relevant. Ook kunnen er andere koppelvlakken zijn waarvoor beveiligde verbinding van belang is, zoals voor de beheerder (FTPS, SFTP, SSH). Het lijkt goed om een overzicht te geven van versleutelde en onversleutelde protocollen en hun functie. |
| 11 | B.08 contractmanagement | Bij onderdeel B.08 contractmanagement is het goed als aangegeven wordt dat de juiste beveiligingsstandaarden zouden moeten worden uitgevraagd bij aanschaf van nieuwe applicaties. |
| 12 | B10 hardeningsproces | Bij B10 hardeningsproces missen we een verwijzing dat het aanbevelingswaardig is dat ICT componenten ondersteund dienen te worden door de meest actuele beveiligingsstandaarden. Zou goed zijn als dit bij het onderdeel /01 procesmatig en procedureel terugkomt. (pag 34) |
| 13 | B11 ICT Landschap | Bij B11 ICT Landschap, komt niks terug over het gebruik van standaarden. Het lijkt ons relevant om aan te geven dat (beveiligings)standaarden ook een ICT component zijn binnen het ICT landschap waarmee rekening gehouden dient te worden bij het vaststellen van dit landschap |
| 14 | 3.1 Toegangsvoorziening | Hier ontbreekt "Attribute-based access control". Een standard als XACML is dan relevant. Zie bijv. https://www.pvib.nl/download/?id=17683535&download=1 |
| 15 | 3.1 Toegangsvoorziening | Hier kan behalve aan DigiD ook gerefereerd worden aan eHerkenning. Beide werken o.b.v. de open standaard SAML2.0. |

| # | Onderwerp, paragraaf en/of pagina | Opmerking |
|---|---|---|
| 16 | p. 70 | Op pagina 70 gaat het over het gebruik van digitale handtekeningen. Hier lijkt een verwijzing is naar B06 (PKI) op zijn plaats. |
| 17 | p.71 | Vermelden dat TLS 1.2 de voorkeur geniet. Wel slim om vanwege interoperabiliteit fall-back te hebben op TLS1.0 en 1.1. SSL, ook versie 3.0, kan worden uitgezet. Zie ook best practice van SSLlabs: https://www.ssllabs.com/downloads/SSL_TLS_Deployment_Best_Practices_1.3.pdf |
| 18 | p. 71 | Een referentie naar HSTS (RFC 6797) lijkt hier op zijn plaats. |
| 19 | p. 44, 68, 81 | Op verschillende plekken wordt er gesproken over "hashing" maar er wordt niet gerefereerd aan relevante standaarden (SHA-2) en aan standaarden die worden afgeraden (MD5). Zie ook opmerking 9. |
| 20 | p.86 | Bij de flags voor cookies zou ook wat opgenomen kunnen worden over HSTS (RFC 6797). |
| 21 | U/NW.06 Hardening van Netwerken (p. 114) | 'hostname.bind' moet 'version.bind' zijn. |
| 22 | U/NW.06 Hardening van Netwerken (p. 107 en p. 114) | Op p. 114 staat "Overweeg een onderscheid te maken tussen 'authoritative name servers' (waar de domeinnamen / zonefiles op draaien) en 'recursive resolvers' (waar client-systemen hun DNS vragen aan stellen)". Op p. 107 staat "Zorg ervoor dat authoratieve DNS-servers en recursive/caching DNS-servers logisch gescheiden zijn, door ze in aparte netwerken te plaatsen." De laatste forumlering is sterker en verdient de voorkeur. |
| 23 | U/NW.06 Hardening van Netwerken (p. 107 en p. 114) | Melding maken van ".nl Control". Zie: https://www.sidn.nl/over-nl/domeinnaam-beschermen/ |
| 24 | Afkortingen (p. 164) | De afkorting DNS staat voor 'Domain Name System'. |
| 25 | Authenticatiemechanismen (p. 43) | Forum Standaardisatie heeft een handreiking betrouwbaarheidsniveaus ontwikkeld waarmee een organisatie kan bepalen welk niveau van authenticatie past bij het risico van de door hem aangeboden elektronische dient. Zie: http://www.forumstandaardisatie.nl/themas/authenticatie-en-autorisatie/ |
| 26 | Paragraaf 1.11 | Paragraaf 1.11 gaat in op het onderhoudt van de richtlijnen. Dit is echter erg beperkt. Er is alleen een verwijzing dat opmerking aangedragen kunnen worden naar een algemeen email adres. Hierbij een suggestie om het beheer van de richtlijnen te verbeteren:<br>• Inrichten klankbord groep waarin verschillende experts uit de verschillende type overheidsorganisaties in vertegenwoordigd zijn. Deze klankbord groep zou idealiter op regelmatige basis bij elkaar komen om zodoende zorg te dragen voor de actualiteit en het beheer van het document. Bij eventuele wijziging kunnen deze personen ook hun achterban consulteren.<br>• Het inrichten van een beheerorganisatie die verantwoordelijk is voor het versiebeheer. Een |

| # | Onderwerp, paragraaf en/of pagina | Opmerking |
|---|---|---|
| | | verantwoordelijke aanwijzen binnen het NCSC die er zorg voor draagt dat het document wordt beheert en vindbaar is. Hierbij kan worden verwezen naar BOMOS.<br>• Het inrichten van een omgeving waar relevante documentatie over de richtlijnen gevonden kan worden en aangeven dat deze vrij toegankelijk en gebruikt mag worden.<br>• Aangeven dat bij wijzigingen volgt er een openbare consultatie waarbij iedereen input kan leveren op de doorontwikkelingen van de richtlijnen. Daarbij ook kenbaar maken waar de openbare consultatie wordt gepubliceerd.<br>• Aangegeven dat iedereen opmerkingen en input kan aanleveren en wat de reactietijd hierop is.<br>• Bovenstaande kan als zondanig worden aangegeven in de beveiligingsrichtlijnen, het is daarbij natuurlijk wel zaak om deze beheerorganisatie daadwerkelijk in te richten en beleggen. |
| **Additionele punten toegevoegd aan eerste review d.d. 3 april 2014** | | |
| 27 | TOTP (o.a. p.43, p.44, p.51, p.80) | 2-factor authenticatie wordt op meerdere plekken in het document genoemd (o.a. p.43, p.44, p.51, p.80). Goed om daar te verwijzen naar TOTP (RFC6238, https://datatracker.ietf.org/doc/rfc6238/). Deze standaard wordt meer en meer gebruikt. Zie: http://en.wikipedia.org/wiki/Time-based_One-time_Password_Algorithm |
| 28 | Conformiteitstooling | Voor verschillende zaken bestaat tooling om te controleren of een bepaalde maatregel/standaard goed geïmplementeerd is, bijv. voor certificaten (https://www.ssllabs.com/ssltest/) en voor DNSSEC (http://dnssec-debugger.verisignlabs.com/). Natuurlijk bestaan er hiervoor ook besturingssysteem-tools zoals openssl en dig. Goed om i.i.g. onder "audit-invalshoek" explicieter hierover relevante zaken op te nemen. |
| 29 | TLS (p.71) | Forward secrecy: De nadruk hierop kan wel wat groter. Het wordt nu slechts in de marge genoemd. |
| 30 | TLS (p.71) | Het zou goed zijn als NCSC nog concreter advies zou geven voor een veilige TLS-configuratie. Dat kan kan uiteraard obv gangbare internationale best practices van Qualys/SSLlabs, OWASP en NIST. Zie ook de volgende tips voor veilige TLS-serverconfiguratie: https://blog.surfnet.nl/?p=3290 |

## 6. Overige opmerkingen

| # | Paragraaf en/of pagina | Opmerking |
|---|---|---|
| 1 | Algemeen | Ondanks dat in de inleiding wordt genoemd dat er rekening gehouden moet worden met de cloudomgeving, komt dit specifieke onderwerp niet tot nauwelijks terug. De focus ligt meer op de situatie dat het beveiligingsbeleid in control is bij de desbetreffende organisatie zelf. Terwijl in de praktijk veel webapplicaties in de cloud staan. Hoe hiermee om te gaan mag mij betreft wel in een aparte paragraaf terugkomen. |
| 2 | Afkortingen, p. 164 | In de afkortingenlijst staat 2x keer DDOS |
| 3 | U/NW.03 | Er wordt drie keer gesproken over Webijvoorbeelderkeer. Wat |

| | | |
|---|---|---|
| | Netwerkzonering, p. 100 en 105 | is dit, of is dit een schrijffout? |
| 4 | U/TV.01 Toegangsvoorzienings beleid, p.44<br>U/TV.02 Toegangsvoorzienings architectuur, p.52 | Ergens vermelden dat Single Sign On ook een risico kan zijn en hoe je dat kan mitigeren bijv. met maatregelen als two-factor authentication en step-up authentication. |
| 5 | p.86 | Bij de flags voor cookies zou ook wat opgenomen kunnen worden over HSTS (RFC 6797). |
| 6 | p.71 | "Cookies zijn versleuteld." Dat biedt geen toegevoegde waarde. Hashing eventueel wel. Een cookie mag geen persoonsgegevens bevatten. Zie: https://www.owasp.org/index.php/OWASP_Application_Security_FAQ#How_about_encrypting_the_session_id_cookies_instead_of_using_SSL.3F |
| 7 | p. 71 | Bepaalde maatregelen worden niet genoemd, zoals het voorkomen van browser caching. Zie: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet en https://www.owasp.org/index.php/Session_Management_Cheat_Sheet |