Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Aanwijzing voor gebruikers versie 2012

ICT-Beveiligingsrichtlijnen voor Webapplicaties

U hebt een webapplicatie die voldoet aan de ICT-Beveiligingsrichtlijnen voor Webapplicaties van het NCSC. Op die manier weet u zich gerustgesteld met een veilige webapplicatie, maar weet u ook dat een veilige applicatie goed moet worden onderhouden om met zijn tijd mee te gaan.

Het NCSC publiceert in augustus 2015 een bijgewerkte versie van de ICT-Beveiligingsrichtlijnen voor Webapplicaties (hierna Richtlijnen genoemd). Deze begeleidende publicatie bevat aanwijzingen voor organisaties die al met de Richtlijnen uit 2012 werken, om te helpen met het besluiten tot bijwerken van bestaande webapplicaties naar de nieuwe Richtlijnen.

Richtlijnen en Verdieping
Versie 2012 van de ICT-Beveiligingsrichtlijnen voor Webapplicaties van het NCSC bestond uit twee genummerde delen. De nieuwe versie is op dezelfde manier uitgegeven, waarbij deel 1 nu de ondertitel "Richtlijnen" draagt en deel 2 de ondertitel "Verdieping".

Waarom zijn de Richtlijnen vernieuwd?

Het NCSC ontvangt geregeld feedback van gebruikers van de Richtlijnen. Op basis daarvan heeft het NCSC een aantal verbeterpunten opgemerkt en die doorgevoerd in de nieuwe versie. Daarnaast houdt het NCSC zicht op de ontwikkelingen in het dreigingslandschap om de Richtlijnen waar nodig aan te scherpen.

Wat zijn de belangrijkste wijzigingen?

De meest in het oog springende wijziging is een vernieuwde indeling. De hoofdstukindeling uit de versie van 2012 is vervangen door een indeling in domeinen en onderzoekslagen. Daarnaast is er een aantal richtlijnen toegevoegd, verwijderd of aangescherpt.

Hoe zijn de Richtlijnen georganiseerd?

De Richtlijnen zijn georganiseerd volgens het SIVA-raamwerk.[1] De Richtlijnen zijn ingedeeld in drie domeinen, waarvan één opgesplitst in vier onderzoekslagen:

- Beleidsdomein;
- Uitvoeringsdomein;
  - Toegangsvoorzieningslaag;
  - Webapplicatielaag;
  - Platform- en webserverlaag;
  - Netwerklaag.
- Beheersingsdomein (control).

Iedere richtlijn bevat een doelstelling op hoofdlijn, en is onderverdeeld in meerdere maatregelen.

Zijn er inhoudelijke wijzigingen aan de Richtlijnen?

Ja, er zijn ook inhoudelijke wijzigingen.

Welke richtlijnen zijn nieuw?

De nieuwe Richtlijnen hebben een onderverdeling van richtlijnen en bijbehorende maatregelen. Er zijn 6 geheel nieuwe richtlijnen en 62 toegevoegde maatregelen. In dit document zullen niet alle toevoegingen worden behandeld, in bijlage F van de Richtlijnen vindt u een tabel met de verschillen tussen versie 2012 en 2015.

Dit zijn een aantal opmerkelijke wijzigingen (NB: dit is geen uitputtende lijst):

- Beleidsdomein
  - Toevoeging van een responsible-disclosurebeleid.

[1] W. Tewarie, SIVA – Methodiek voor de ontwikkeling van auditreferentiekaders, 2014

- Toevoeging van diverse maatregelen voor het vastleggen van het ICT-landschap.

» Uitvoeringsdomein
- Toevoeging van een operationeel beleid voor de lagen webapplicaties, platformen en webservers, en netwerken.
- Toevoeging van maatregelen voor het vastleggen van de architectuur van de lagen webapplicaties, platformen en webservers, en netwerken.
- Toevoeging van enkele maatregelen voor de registratie van verleende toegang en gebruikte functionaliteit.
- Toevoeging van webapplicatiebeheer.
- Uitbreiding van een maatregel om TLS toe te passen op een geheel domein als een deel daarvan vertrouwelijke communicatie bevat.
- Toevoeging van een maatregel tegen session fixation.
- Toevoeging van een maatregel tegen clickjacking.
- Toevoeging van diverse maatregelen voor netwerkzonering en zone-scheidingen.

» Beheersingsdomein
- Toevoeging van een servicemanagementbeleid.
- Toevoeging van enkele maatregelen op het gebied van beschikbaarheidbeheer.

Welke richtlijnen zijn geschrapt?
Richtlijn B5-6 (zorg voor een extra set back-upcertificaten van een andere CA) is geschrapt.

Welke richtlijnen zijn aangescherpt?
Bijna alle richtlijnen en maatregelen zijn in formulering aangescherpt. Op die manier probeert het NCSC de ruimte voor interpretatie zo beperkt mogelijk te houden. Of deze verscherpte formulering ook betekent dat u de beveiliging van uw applicatie moet aanscherpen is afhankelijk van hoe de Richtlijnen uit 2012 ten tijde van toepassing zijn geïnterpreteerd.

Mijn applicatie voldoet aan de Richtlijnen uit 2012. Is mijn applicatie nu niet voldoende veilig meer?
Een applicatie die voldoet aan de Richtlijnen uit 2012 is veilig te noemen. Wel is het zo dat een veilige applicatie bij moet blijven met de trends, wat betekent dat u deze het beste kunt laten voldoen aan de nieuwe versie.

Is het dreigingsniveau veranderd?
Het dreigingsniveau is voor webapplicaties onverminderd hoog. Als u op de hoogte wilt blijven van actuele dreigingen, lees dan het jaarlijkse Cybersecuritybeeld Nederland van het NCSC, waarvan editie 2015 binnenkort verschijnt.

Wat moet ik nu doen met deze nieuwe versie?
Het NCSC adviseert om uw applicatie te laten voldoen aan de nieuwe versie van de Richtlijnen.

Zijn de Richtlijnen verplicht?
Het NCSC stelt de Richtlijnen aan niemand verplicht. De Richtlijnen (of een selectie daaruit) kunnen wel door opdrachtgevers verplicht gesteld worden.

Kost het veel werk om mijn applicatie aan de Richtlijnen te laten voldoen?
Hoe veel werk het kost hangt af van de omvang en exacte functionaliteit van uw webapplicatie en de beheerorganisatie daaromheen.

Moet ik onmiddellijk aan het werk met deze nieuwe versie?
Het NCSC adviseert om zo snel mogelijk de gevolgen voor uw applicatie te bepalen, en op basis daarvan een plan te maken hoe u deze kunt laten voldoen aan de nieuwe versie van de Richtlijnen. Het dreigingsniveau is echter niet zodanig dat dit onmiddellijk klaar moet zijn.

Zijn de Richtlijnen uit 2012 niet meer geldig?
Het NCSC adviseert de Richtlijnen uit 2012 niet meer toe te passen en een plan te maken om uw applicatie aan de nieuwe Richtlijnen te laten voldoen. Applicaties die aan de Richtlijnen uit 2012 voldoen zijn op dit moment nog wel veilig te noemen.

Wat betekent deze nieuwe versie voor de DigiD-aansluitnorm?
De aansluitnorm voor DigiD wordt bepaald door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Voor 2015 zal de aansluitnorm nog gebaseerd zijn op de NCSC-Richtlijnen uit 2012. Indien de aansluitnorm wordt aangepast zal dit worden aangekondigd door Logius.[2]

Wanneer komt de volgende nieuwe versie?
Wanneer er weer een nieuwe versie verschijnt, is nog niet vastgesteld. Het NCSC actualiseert de Richtlijnen wanneer de ontwikkelingen daartoe aanleiding geven. Bij acute ontwikkelingen is het ook mogelijk dat het NCSC een los addendum publiceert.

Is de nieuwe indeling definitief voor alle toekomstige versies?
Het NCSC heeft geprobeerd de Richtlijnen zo goed mogelijk in te delen en heeft dit met diverse partijen afgestemd om zo veel mogelijk aan de behoefte te voldoen. Afhankelijk van hoe de Richtlijnen in de praktijk gebruikt worden kan bepaald worden of de indeling nader moet worden aangepast. Feedback van gebruikers ontvangt het NCSC graag op richtlijnen@ncsc.nl.

[2] Meer informatie over de DigiD-aansluitnorm en ICT-beveiligingsassessments vindt u op de website van Logius: https://www.logius.nl/ondersteuning/digid/beveiligingsassessments/.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55
September 2015 | Aan deze informatie kunnen geen rechten worden ontleend.