Cyberkracht meting Bouwend Nederland

Onafhankelijke meting van beveiligingsmaatregelen leden Bouwend Nederland

PUBLIEK

Document informatie

Titel:	Cyberkracht meting Bouwend Nederland
Versie:	1.0
Classificatie:	Publiek
Type:	Informatie
Auteur:	René van Etten
Eigenaar:	René van Etten
Publicatiedatum:	27 dec 2023
Herzieningsdatum:	7 februari 2024
Gerelateerde documenten:	n.v.t.

Versie geschiedenis

Versie	Datum	Detail	Auteur
0.1	27 dec 2023	Concept	R. van Etten
1.0	7 feb 2024	Definitief	R. van Etten

ThreadStone Cyber Security B.V.
Westblaak 100
3012 KM Rotterdam
www.threadstone.eu

T: +31 (0)85 060 7000
M: info@threadstone.eu

Kvk : 614 262 02
BTW nummer: NL 85 43 36 631 B01
IBAN: NL34 RABO 0192 0442 14

LET OP:

ThreadStone Cyber Security kan op geen enkele manier aansprakelijkheid aanvaarden voor de gevolgen van onvolledigheid of onjuistheid van informatie die in dit rapport of de diensten van ThreadStone Cyber Security ter beschikking worden gesteld. Ook kan deze rapportage niet worden gezien als (bindend) advies. Het is niet mogelijk om garanties te bieden in het kader van compliant zijn met de Algemene Verordening Gegevensbescherming of andere wetgeving die betrekking heeft op de diensten en rapportages van ThreadStone Cyber Security.

Met de diensten van ThreadStone Cyber Security wordt u mogelijk verwezen naar andere websites, rapporten en technische oplossingen die niet onder controle staan van ThreadStone Cyber Security. Wij hebben geen controle over de aard, inhoud en de beschikbaarheid van deze bronnen. Daarnaast zijn deze bronnen aan tussentijdse verandering onderhevig, waardoor bepaalde informatie mogelijk niet meer actueel of incompleet kan zijn. De opname van welke informatie dan ook is niet noodzakelijkerwijs een aanbeveling of onderschrijving van standpunten die door (andere) bronnen of wetgever worden geuit en hebben slechts een informatieve strekking.

Inhoudsopgave

Samenvatting

Dit rapport geeft de resultaten weer van een meting op een aantal veel voorkomende kwetsbaarheden met betrekking tot digitale veiligheid van 4107 domeinen van organisaties die lid zijn van Bouwend Nederland. De meting is uitgevoerd om via internet 'van buitenaf' de kwetsbaarheden op te sporen. In openbare bronnen op internet is gezocht naar kwetsbaarheden in relatie tot de domeinnamen van de betreffende organisaties. Bij die aanpak is vooraf geen expliciete toestemming van het bedrijf nodig: het gaat immers om openbare informatie.

De doelstelling van dit rapport is om tot een kwalitatief beeld te komen van de cyberveiligheid van de leden van Bouwend Nederland.

Inleiding en aanleiding Cyberkracht metingen

Na de succesvolle campagne Veilig Zakelijk Internetten versie 1, die ThreadStone samen met MKB-Nederland heeft uitgevoerd (en die uiteindelijk zelfs de European Crime Prevention Awards[i] won) is de capaciteit opgeschaald. Het project kreeg een budget om in totaal 2.500 organisatie te bereiken met de controle van hun website en het publieke IP-adres van de organisatie op technische kwetsbaarheden. Er werd niet alleen opgeschaald op de uitvoerende kant, maar ook in de communicatie. MKB-Nederland mobiliseerde uiteindelijk zo'n 50 brancheverenigingen, waarmee er een communicatiebereik van honderdduizenden ondernemers werd bewerkstelligd. Toch werd de doelstelling om met z'n allen 2.500 bedrijven te vinden die zich wilden inschrijven voor een kosteloze test niet behaald.

Dit probleem heeft ThreadStone Cyber Security jarenlang beziggehouden. Vele gesprekken met ondernemers zijn gevoerd, en over het algemeen bleek dat MKB'ers zich geen potentieel slachtoffer voelen, denken dat hun IT'er verantwoordelijk is, niet overzien dat het om meer dan techniek gaat, denken dat beveiliging duur en ingewikkeld is en uiteindelijk geen urgentie zien in aandacht besteden aan digitale beveiliging. Er geldt een zogenaamde 'optimism bias' voor het grootste deel van het MKB[ii]. Tot het henzelf – of een organisatie in de nabijheid - overkomt… Zelfs bij het aanmelden bij een kosteloze campagne worden nut en noodzaak veelal niet ingezien, ondanks alle communicatiepower die in de jaren is ingezet.

De ervaring van ThreadStone is dat MKB'ers gaan acteren als ze zelf slachtoffer worden of als ze met de neus op feiten worden gedrukt doordat een bedrijf met dezelfde omvang of in dezelfde branche te maken krijgt met bijvoorbeeld ransomware, phishing of CEO-fraude. Pas dan steekt de vraag '*Zou ons dit ook kunnen overkomen?*' de kop op en wordt er gehandeld.

ThreadStone heeft de afgelopen jaren allerlei acties uitgevoerd om te kijken op welke wijze we toch het bewustzijn bij de MKB'ers omhoog kunnen brengen. Daarbij ligt de nadruk op het geautomatiseerd voorzien van informatie waarmee de ondernemer zelf aan de slag kan of eenvoudig maatregelen en acties met zijn of haar IT'er kan afstemmen (het merendeel van de MKB'ers met 5 tot 100 medewerkers besteedt zijn/haar IT uit[iii]).

De belangrijkste vraag die is gesteld is:

Hoe kunnen we de MKB-ondernemer bereiken met kwalitatief goede en op de onderneming gerichte informatie, zónder dat we inschrijving of goedkeuring – en daarmee actie vanuit de klantorganisatie - nodig hebben, om met deze informatie de ondernemer vervolgens bewuster te maken?

Hierop is besloten om te kijken of er een rapport kan worden samengesteld met risico's en kwetsbaarheden van een bepaalde onderneming op basis van uitvraag van allerlei openbare bronnen op het internet. Aangezien de doelstelling is dat er geen expliciete goedkeuring van de ondernemer nodig is, is de URL van een organisatie als vertrekpunt gekozen. Daarmee kunnen kwetsbaarheden in website, e-mail, gehackte accounts etc. worden blootgelegd.

Uitvoering

In de uitvoering zijn ruim 4100 domeinen (URL's) van organisaties aangeleverd die bij Bouwend Nederland zijn aangesloten. Deze domeinen zijn gemeten op basis van een onafhankelijke, niet-commerciële cyber kracht meting, waarvan de resultaten feitelijk onderbouwd worden gepresenteerd in dit rapport.

In dit onderzoek zijn, geautomatiseerd, elk van de ruim 4100 domeinen op onderstaande risico's gecontroleerd:

- Verspreidt de website geen malware?
- Verspreidt de website geen spam?
- Verspreidt de mailserver geen spam?
- Kan de e-mail niet misbruikt worden?
- Kan het verkeer met de website niet worden onderschept?
- Zijn er geen ongebruikelijke aanvalspaden op de website mogelijk?
- Worden bezoekers van de website voldoende beschermd?
- Is informatie over de configuratie van de website afgeschermd?
- Kan websiteverkeer naar de website niet gemanipuleerd worden?

Voor een onderbouwing van de wijze waarop de controles zijn uitgevoerd verwijzen we naar bijlage 1. Hierin is ook opgenomen hoe we per domein tot een scoreberekening zijn gekomen.

Resultaten

Overall score

Allereerst hebben we een overall score berekend op basis van een gemiddelde van alle gemeten domeinen. Voor de onderbouwing van de scoreberekening verwijzen we naar bijlage 1. De scoretabel loopt van 1 tot 10, waarbij een 10 een uitstekende score en een 1 een zeer slechte score is.

De resultaten

De gemiddelde score bedraag 4,8.

Hierna volgen de individuele metingen die zijn uitgevoerd.

Verspreidt de website geen malware?

Wij controleren of de gemeten website voorkomt op zogenaamde 'blacklists'. Op deze blacklists worden websites bijgehouden waarvan bekend is dat ze malware (malafide software, virussen etc.) verspreiden. De gemeten URL's komen dus voor op deze lijsten, wat niet hoeft te betekenen dat de websites zelf ook malware verspreiden.

De resultaten

621 van de 4107 websites (15,1%) staat geregistreerd als malware verspreidend.

Verspreidt de website geen spam?

Wij controleren of de gemeten website voorkomt op zogenaamde 'blacklists'. Op deze blacklists worden de onderliggende IP-adressen van websites bijgehouden waarvan bekend is dat zij spam (ongewenste e-mail) versturen. De gemeten URL's komen dus voor op deze lijsten, wat niet hoeft te betekenen dat de websites zelf ook spam versturen.

De resultaten

911 van de 4107 websites staat geregistreerd als spam verspreidend. Op 29 websites hebben we de controle niet kunnen uitvoeren. Dit betekent dat 22,3% van de gecontroleerde websites bekend staat als spam verspreidend.

Verspreidt de mailserver geen spam?

Wij controleren of de gemeten mailserver voorkomt op zogenaamde 'blacklists'. Op deze blacklists worden mailservers bijgehouden waarvan bekend is dat zij spam (ongewenste e-mail) versturen. De IP-adressen van de mailservers komen dus voor op deze lijsten, wat niet hoeft te betekenen dat de mailservers zelf ook spam verspreiden.

De resultaten

1364 van de 4107 mailservers staat geregistreerd als spam verspreidend. Op 124 mailservers hebben we de controle niet kunnen uitvoeren. Dit betekent dat 34,2% van de gecontroleerde mailservers bekend staat als spam verspreidend.

Kan de e-mail niet misbruikt worden?

Wij controleren de instellingen van de mailserver. Als de mailserver niet correct is ingesteld, kan dit betekenen dat kwaadwillenden uit naam van de betreffende organisatie mails kunnen versturen, met alle gevolgen van dien.

De resultaten

1852 van de 4107 mailservers hebben de protocollen niet (volledig) goed ingesteld. Dit betekent dat 45,1% van de gecontroleerde mailservers niet goed staat ingesteld.

Kan het verkeer met de website niet worden onderschept?

Wij controleren of het verkeer tussen de gemeten website en bezoekers versleuteld is. Een bezoeker ziet dit aan een groen slotje links in de browser (zogenaamd "https"). De resultaten in de grafiek geeft het percentage websites weer, waarbij de score lager is dan een zogenaamde 'A-grade'.

De resultaten

871 van de 4107 SSL certificaten hebben geen 'A-grade'. Van 181 domeinen hebben we de controle niet kunnen uitvoeren. Dit betekent dat 22,2% van de gecontroleerde domeinen haar SSL certificaten niet goed heeft ingesteld.

Zijn er geen ongebruikelijke aanvalspaden op de website mogelijk?

Wij controleren welke poorten er op de server van de gemeten website "open" staan. Hoe meer poorten er open staan, hoe meer aanvalspaden een kwaadwillende heeft om op de desbetreffende website in te breken.

De resultaten

Bij 2543 websites staan meer porten open dan de gebruikelijke port 80 en 443. Dit betekent dat 61,9% van de websites meer porten open heeft staan dan benodigd.

Worden bezoekers van de website voldoende beschermd?

Wij controleren of communicatie op de browser van de bezoeker van de website niet kan worden gemanipuleerd. Dit doen we door na te gaan of zogenaamde securityprotocollen op de juiste wijze worden afgedwongen op de browser van bezoekers van de desbetreffende website.

De resultaten

Bij 3457 websites worden bezoekers onvoldoende beschermd doordat security headers niet juist zijn ingesteld. Bij 308 websites hebben we deze controle niet kunnen uitvoeren. Dit betekent dat bij 91,0% van de websites de security headers niet juist zijn ingesteld.

Is informatie over de configuratie van de website afgeschermd?

Wij controleren of we kunnen herleiden welke software(versies) door de gemeten website wordt gebruikt. Een kwaadwillende kan met deze kennis gerichte aanvallen uitvoeren. Dit meten we door na te gaan of zogenaamde security headers op de juiste wijze zijn ingesteld.

De resultaten

Bij 3173 websites worden bezoekers onvoldoende beschermd doordat security headers niet juist zijn ingesteld. Bij 194 websites hebben we deze controle niet kunnen uitvoeren. Dit betekent dat bij 81,1% van de websites informatie wordt gegeven over de onderliggende technische configuratie.

Kan websiteverkeer naar de website niet worden gemanipuleerd?

Wij controleren of bezoekers die naar de gemeten domeinnaam gaan ook altijd op de betreffende website terechtkomen (en niet worden omgeleid naar een website van kwaadwillenden). Dit meten we door te kijken of DNSSec is ingesteld.

De resultaten

1567 van de 4107 websites hebben de DNSSec niet goed ingesteld. Dit betekent dat DNSSec bij 38,2% van de gecontroleerde websites niet goed staat ingesteld.

Conclusie en discussie

De algehele beveiliging ligt nog op een laag niveau. Als we naar de gemiddelden kijken, dan komen we tot de volgende resultaten:

Gecontroleerde kwetsbaarheid	Resultaat Bouwend Nederland	Technische meting	Mogelijk gevolg en impact
Verspreidt de website geen malware?	15,1% van de websites of hun webserver komen voor op spamlijsten	De website of het IP- adres van de webserver komt voor op minimaal 1 malware-lijst	Bezoekers van de website ontvangen mogelijk malware (malafide software) op hun systemen. Deze malafide software kan bij deze bezoekers zorgen voor (veel) overlast, zoals inbraak of platleggen van hun systemen. Ook kan het voorkomen dat bezoekers de website niet meer kunnen benaderen.
Verspreidt de website geen spam?	22,3% van de websites of hun webserver komen voor op spamlijsten	De website komt op minimaal 1 spam-lijst voor	De eigenaar van de website kan worden aangesproken op het verspreiden van spam waardoor de website kan worden afgesloten. Daarnaast kunnen e-mails niet aankomen bij de geadresseerden.
Verspreidt de mailserver geen spam?	34,2% van de mailservers komen voor op spamlijsten	De mailserver komt op minimaal 1 spam-lijst voor	De eigenaar van de website kan worden aangesproken op het verspreiden van spam waardoor de mailserver kan worden afgesloten. Daarnaast kunnen e-mails niet aankomen bij de geadresseerden.
Kan de e-mail niet misbruikt worden?	Bij 45,1% van de domeinen blijken de e-mail security-protocollen niet goed ingesteld te zijn	Minimaal 1 van de waardes SPF, DKIM en DMARC zijn niet of niet juist ingesteld	Onbevoegden kunnen eenvoudig namens (medewerkers van) de betreffende organisatie e-mails versturen, of e-mails komen niet aan.
Kan het verkeer met de website niet worden onderschept?	Bij 22,2% van de websites blijkt SSL niet optimaal te zijn ingesteld	SSL-score B, C, D of hoger	Onbevoegden kunnen communicatie van bezoekers van de betreffende website onderscheppen. De website kan lager in de zoekresultaten van Google presteren dan mogelijk is.
Zijn er geen ongebruikelijke aanvalspaden op de website mogelijk?	61,9% van de webservers heeft ongebruikelijke aanvalspaden open staan	Andere poorten dan de als veilig beschouwde poorten ['80','443', '22', '2222', '993', '995', '465'] staan open	Kwaadwillenden kunnen aanvalspaden vinden in de webserver, waardoor deze kan worden gehackt (stelen of manipuleren van data en/of verstoren van de werking).
Worden bezoekers van de website voldoende beschermd?	91,0% van de websites heeft security-headers niet voldoende ingesteld	Minimaal 1 ontbrekende security header	Onbevoegden kunnen communicatie met de website (met mogelijk gevoelige gegevens van bezoekers) onderscheppen en mogelijk manipuleren.
Is informatie over de configuratie van de website afgeschermd?	Bij 81,1% van de websites wordt informatie afgegeven over de onderliggende technische configuratie	Minimaal 1 configuratie-header kan worden uitgelezen	Doordat eenvoudig achterhaald kan worden welke software de website gebruikt, is het makkelijker voor een kwaadwillende om te controleren of de website kwetsbaar is. Hierdoor kunnen eenvoudiger openingen in

			de website worden gevonden waardoor deze kan worden gehackt (stelen of manipuleren van data of verstoren van de werking).
Kan websiteverkeer naar de website niet worden gemanipuleerd?	38,2% van de websites heeft geen DNSSec ingesteld	DNSSec is niet aanwezig	Kwaadwillenden kunnen wachtwoorden of andere vertrouwelijke informatie onderscheppen van bezoekers van de website.

De reden dat er slecht wordt gescoord is in de optiek van ThreadStone te wijten aan:

1. Onvoldoende perceptie van het risico of het risico wordt (te) laag ingeschat.
   Zeker als er een informatieve website ("digitale brochure") is, dan is de gedachte bij veel organisaties dat het niet zoveel uitmaakt als deze gehackt wordt of slecht beveiligd is. Toch zien we bijvoorbeeld ook bij de instelling van de e-mailprotocollen dat dit zeer slecht is geregeld (meer dan 57% van de gemeten domeinen heeft de e-mailbeveiliging niet op orde). Dit gaat dus verder dan alleen de beveiliging van de website en daarom is het in onze optiek voor vrijwel iedere organisatie van belang;

2. Onduidelijkheid over verantwoordelijkheden.
   Websites worden ontwikkeld door websitebouwers. Vervolgens worden deze geplaatst bij bedrijven die de hosting verzorgen. Deze laatste groep rekent vaak een bedrag per maand voor het leveren van de hosting. Wij zien veel eindgebruikers die er – onterecht – vanuit gaan dat zij daarmee ook een contract hebben afgesloten voor de beveiliging en het up-to-date houden van hun website. Hierover zijn in beginsel echter al slechte/geen afspraken gemaakt met de websitebouwer (die hier eigenlijk verantwoordelijk voor is);

3. Onvoldoende kennis en aandacht bij hostingpartijen.
   Wij zien veel hostingpartijen die te weinig aandacht geven aan informatiebeveiliging. Dat bijvoorbeeld 50% van de webservers ongebruikelijke aanvalspaden open heeft staan, is een verantwoordelijkheid van deze bedrijven. Ditzelfde geldt voor het gereed maken van de webservers voor de nieuwe internetstandaard IPv6. Veelal wordt het doorvoeren van dit soort wijzigingen en verbeteringen gezien als kostenpost in plaats van een verbetering voor het totale internet;

4. Onvoldoende kennis en aandacht bij websitebouwers.
   Wij zien veel websitebouwers die te weinig aandacht geven aan informatiebeveiliging. Dat bijvoorbeeld 60% van de websites de security-headers niet op orde heeft, dat 39% van de websites informatie afgeeft over de onderliggende infrastructuur, dat 79% van de websites geen DNSSec heeft en dat ten slotte bij 36% van de websites de SSL-certificaten niet juist zijn ingesteld, geeft aan dat hier onvoldoende aandacht voor is. Veelal is er een gebrek aan kennis om dit soort wijzigingen en verbeteringen door te voeren.

Aanbevelingen en suggesties

Wij zien voldoende aanleiding om bezorgd te zijn over de digitale weerbaarheid van organisaties binnen de branche. Sinds de campagne Veilig Zakelijk Internetten in 2018 stopte, is er steeds meer aandacht voor het onderwerp cyberveiligheid gekomen, maar in onze optiek spreekt dit helaas nog steeds vooral de grotere organisaties aan – met een eigen securityafdeling. ZZP'ers en MKB'ers hebben meestal niet de kennis en kunde om online risico's goed in te schatten en daarop te anticiperen. Zij gaan er veelal onterecht vanuit dat dit soort dingen gewoon geregeld is.

Daarnaast worden ze hoogst zelden persoonlijk aangesproken op dergelijke risico's die samenhangen met hun eigen situatie, waardoor het veelal ongrijpbaar en ontastbaar blijft. Er zijn voldoende campagnes die aangeven dat organisaties aandacht moeten besteden aan hun cyberweerbaarheid, maar de meeste worden niet bereikt. Ook doordat ze denken dat ze het goed geregeld hebben of hebben uitbesteed. Degenen die de boodschap wel oppikken, weten vaak niet waar ze moeten starten omdat cyberweerbaarheid zo veelomvattend is: het grijpt in op beleid, processen, (medewerkers)bewustzijn én techniek.

Bijlage 1: Onderbouwing van de uitgevoerde controles en scoreberekening

Per controle wordt in dit document aangegeven wat het aandachtspunt is bij een negatieve controle en welke impact dit kan hebben.

Als alle uitgevoerde controles positief zijn, dan scoort de betreffende domeinnaam een 10. Per controle kan er (gewogen) aftrek zijn op basis van de ernst van de geconstateerde kwetsbaarheid.

Hieronder volgen alle uitgevoerde controles met de score-aftrek bij een negatief resultaat. Een domein dat bijvoorbeeld bekend staat als malware verspreidend krijgt hiervoor dus 3 punten aftrek en kan nooit meer hoger scoren dan eindcijfer 7. Uiteraard is de hoogste score een 10 en de laagste score een 1.

Verspreidt uw website geen malware?

Aandachtspunt - Mogelijke impact

Uw website komt op blacklist(s) voor en lijkt malware te verspreiden.	Bezoekers van uw website ontvangen mogelijk malware (malafide software) op hun systemen. Deze malafide software kan bij deze bezoekers zorgen voor (veel) overlast, zoals inbraak of platleggen van hun systemen. Ook kan het voorkomen dat bezoekers uw website niet meer kunnen benaderen.

Opbouw score

Score	Onderbouwing
0	De website komt niet voor op malware verspreidende lijsten
1	Het IP van de website komt voor op malware lijsten.
3	De website komt voor op malware lijsten
Invalid	De test kon niet worden uitgevoerd.

Verspreidt uw website geen spam?

Aandachtspunt - Mogelijke impact

Uw website komt op blacklist(s) voor en lijkt spam te verspreiden.	U kunt worden aangesproken op het verspreiden van spam waardoor uw website kan worden afgesloten. Daarnaast komen uw e-mails waarschijnlijk niet aan bij de geadresseerden.

Opbouw score

Score	Onderbouwing
0	De website komt niet voor op spamlijsten
1	De website komt voor op <= 2 spam lijsten
2	De website komt voor op <= 5 spam lijsten
3	De website komt voor op <= 200 spam lijsten

Verspreidt uw mailserver geen spam?

Aandachtspunt - Mogelijke impact

Uw mailserver komt op blacklist(s) voor en lijkt spam te verspreiden.	U kunt worden aangesproken op het verspreiden van spam waardoor uw mailserver kan worden afgesloten. Daarnaast komen uw e-mails waarschijnlijk niet aan bij de geadresseerden.

Opbouw score

Score	Onderbouwing
0	De mailserver komt niet voor op spamlijsten
1	De mailserver komt voor op <=2 spam lijsten
2	De website komt voor op <= 5 spam lijsten
3	De website komt voor op <= 200 spam lijsten
Invalid	De server heeft geen mx record

Kan uw e-mail niet misbruikt worden?

Aandachtspunt - Mogelijke impact

E-mailprotocollen zijn niet juist ingesteld.	Onbevoegden kunnen eenvoudig namens (medewerkers van) uw organisatie e-mails versturen, of uw e-mails komen niet aan.

Opbouw score

Score	Onderbouwing
0	SPF, DMARC en DKIM zijn allemaal goed ingesteld
1	Een van de waardes is niet goed ingesteld
2	Twee van de waardes zijn niet goed ingesteld
Invalid	De test kon niet worden uitgevoerd.

Kan het verkeer met uw website niet worden onderschept?

Aandachtspunt - Mogelijke impact

Communicatie met uw website is niet (juist) versleuteld, waardoor verkeer mogelijk kan worden onderschept.	Onbevoegden kunnen communicatie van bezoekers van uw website onderscheppen. Uw website kan lager in de zoekresultaten van Google presteren dan mogelijk is.

Opbouw score

Score	Onderbouwing
0	SSL correct ingericht, score A of A+
1	SSL Score B
2	SSL Score C
3	SSL Score D of hoger
Invalid	De test kon niet worden uitgevoerd.

Zijn er geen ongebruikelijke aanvalspaden op uw website mogelijk?

Aandachtspunt - Mogelijke impact

Er staan ongebruikelijke digitale deuren open. Hier kunnen kwaadwillenden mogelijk een opening vinden die ze kunnen gebruiken om in te breken.	Kwaadwillenden kunnen aanvalspaden vinden in uw website waardoor deze kan worden gehackt (stelen of manipuleren van data en/of verstoren van de werking).

Opbouw score

Score	Onderbouwing
0	Alleen de veilige poorten staan open ['80','443', '22', '2222', '993', '995', '465']
0,25	Een extra poort buiten de veilige poorten is open
0,5	Twee extra poorten buiten de veilige poorten is open
0,75	Drie extra poorten buiten de veilige poorten is open
1	Vier of meer extra poorten buiten de veilige poorten is open
Invalid	De test kon niet worden uitgevoerd.

Worden bezoekers van uw website voldoende beschermd?

Aandachtspunt - Mogelijke impact

Securityprotocollen worden niet juist afgedwongen op de browser van de bezoeker.	Onbevoegden kunnen communicatie met uw website (met mogelijk gevoelige gegevens van bezoekers) onderscheppen en mogelijk manipuleren.

Opbouw score

Score	Onderbouwing
0	Alle security headers zijn goed geïmplementeerd op de website voor zowel http als https
0,5	1 ontbrekende header
1	2 ontbrekende headers
1,5	3 ontbrekende headers
2	4 of meer ontbrekende headers
Invalid	Het was niet mogelijk om de headers van de website te lezen.

Is informatie over de configuratie van uw website afgeschermd?

Aandachtspunt - Mogelijke impact

Uw website verstrekt configuratie informatie. Hiermee wordt aan kwaadwillenden informatie en kennis verstrekt die ze kunnen gebruiken om nieuwe aanvalspaden te vinden.	Doordat eenvoudig achterhaald kan worden welke software uw website gebruikt, is het makkelijker voor een kwaadwillende om te controleren of uw website kwetsbaar is. Hierdoor kunnen eenvoudiger openingen in uw website worden gevonden waardoor deze kan worden gehackt (stelen of manipuleren van data of verstoren van de werking).

Opbouw score

Score	Onderbouwing
0	Er wordt geen informatie vrijgegeven over welke achterliggende software wordt gebruikt op de website (zowel op http als op https)
0,50	1 configuratie header (de header ontbreekt op https en niet op http bijvoorbeeld)
1	4 configuratie headers
Invalid	Het was niet mogelijk om de headers van de website te lezen.

Kan websiteverkeer naar uw website niet worden gemanipuleerd?

Aandachtspunt - Mogelijke impact

Het is mogelijk om websiteverkeer naar uw website te manipuleren, waardoor u niet kunt garanderen dat uw bezoekers úw website bezoeken maar zij dat wel denken (en dus worden doorgesluisd naar een malafide website).	Kwaadwillenden kunnen wachtwoorden of andere vertrouwelijke informatie onderscheppen van bezoekers van uw website.

Opbouw score

Score	Onderbouwing
0	DNSSec aanwezig
2	Geen DNSSec aanwezig
Invalid	De test kon niet worden uitgevoerd.

Verwijzingen naar andere bronnen

[i] Verwijzing naar winnen Crime Prevention Awards
[ii] Verwijzing naar onderzoek HHS met Optimism Bias
[iii] Verwijzing naar onderzoek waaruit blijkt dat merendeel van de ondernemers de IT uitbesteed