

Meting van de beveiliging van domeinnamen in de EU

Onafhankelijke meting van beveiligingsmaatregelen van meer dan 18 miljoen URL's in de 27
lidstaten van de Europese Unie

PUBLIEK

Document informatie

Titel:	Meting van de beveiliging van domeinnamen in de EU
Versie:	0.1
Classificatie:	Publiek
Type:	Informatie
Auteur:	René van Etten
Eigenaar:	René van Etten
Publicatiedatum:	11 okt 2022
Herzieningsdatum:	14 oktober 2022
Gerelateerde documenten:	n.v.t.

Versie geschiedenis

Versie	Datum	Detail	Auteur
0.1	11 okt 2022	Concept	R. van Etten

ThreadStone Cyber Security B.V.
HSD Campus
Wilhelmina van Pruisenweg 104
2595 AN Den Haag
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:

De intellectuele eigendomsrechten van de diensten en rapportages van ThreadStone Cyber Security, waaronder begrepen de rechten op de daarin opgenomen gegevens en beeldmerken berusten bij ThreadStone Cyber Security. Zonder voorafgaande schriftelijke toestemming van ThreadStone Cyber Security is het niet toegestaan om deze uitgave, of enig onderdeel daarvan, aan te passen of te wijzigen, te verveelvoudigen, op te slaan in een geautomatiseerd gegevensbestand of op enige andere wijze ter beschikking te stellen aan derden, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of op een andere manier.

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.

© 2022 ThreadStone Cyber Security

Inhoudsopgave

Samenvatting	5
Voorwoord	6
Inleiding en aanleiding	7
Uitvoering	8
Resultaten	11
Overall score	11
De resultaten	11
Verspreidt de website geen malware?	13
De resultaten	13
Verspreidt de website geen spam?	14
De resultaten	14
Verspreidt de mailserver geen spam?	15
De resultaten	15
Kan de e-mail niet misbruikt worden?	16
De resultaten	16
Kan het verkeer met de website niet worden onderschept?	17
De resultaten	17
Zijn er geen ongebruikelijke aanvalspaden op de website mogelijk?	18
De resultaten	18
Worden bezoekers van de website voldoende beschermd?	19
De resultaten	19
Is informatie over de configuratie van de website afgeschermd?	20
De resultaten	20
Kan websiteverkeer naar de website niet worden gemanipuleerd?	21
De resultaten	21
Is de website gereed voor nieuwe standaarden?	22
De resultaten	22
Conclusie en discussie	23
Aanbevelingen en suggesties	25
Bijlagen	26
Verwijzingen naar andere bronnen	30

Samenvatting

Dit rapport geeft de resultaten weer van een meting op een aantal veel voorkomende kwetsbaarheden met betrekking tot digitale veiligheid van ruim 18 miljoen domeinen van organisaties in de 27 Europese lidstaten. 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 Europa, waarbij landen ten opzichte van elkaar worden bekeken.

Met een betrouwbaarheid van 99% (overall foutmarge van minder dan 1%) hebben we gemeten dat organisaties in België, Slowakije, Nederland, Tsjechië, Denemarken en Zweden hoger scoren dan het gemiddelde van de 27 lidstaten. Zij scoren overall het beste. Organisaties in de overige 21 lidstaten scoren onder het gemiddelde. De vijf landen die het slechtst scoren zijn Bulgarije, Italië, Frankrijk, Griekenland en Kroatië.

Toch vinden wij de resultaten van de meting in het geheel genomen teleurstellend. Een voorbeeld is de meting op de beveiliging van e-mail. Meer dan 85% van de organisaties heeft de e-mailprotocollen niet juist ingesteld, wat uiteindelijk tot vervalsing/misbruik (bijvoorbeeld zogenaamde spoofing) kan leiden.

Wij zijn van plan om jaarlijks een meting als deze uit te voeren, zodat er ook (kwalitatief) inzicht ontstaat in verbetering of verslechtering en wij wellicht bepaalde trends kunnen ontdekken op het gebied van digitale weerbaarheid en cybersecurity.

Voor onszelf is de doelstelling om met dit rapport het bewustzijn rondom digitale weerbaarheid te vergroten, en ook de urgentie daarvan aantoonbaar te maken. Uiteindelijk zien wij het liefst dat elke organisatie in de EU, van groot tot klein, een (niet-commercieel) rapport ontvangt waarmee de houder van het domein zelf aan de slag kan om zijn/haar weerbaarheid te verhogen. Hiervoor moeten we samenwerken met de juiste partijen, vooral met koepelorganisaties die op sectorniveau, landniveau of Europees niveau hun achterban kunnen bereiken en mobiliseren.

Voorwoord

Toen wij in 2015 een van de belangrijkste partners in de campagne Veilig Zakelijk Internetten werden, begonnen we aan een project waarbij we niet wisten hoe groot de kwetsbaarheid was bij het MKB op het gebied van informatiebeveiliging. Daarnaast wisten we niet hoe we deze doelgroep op een goede manier konden bereiken zodat we ze bij bepaalde risico's tot handelen konden brengen.

In de reis die we in de afgelopen jaren hebben afgelegd, hebben veel mensen ons (veelal onbewust) geholpen om onze denkwijze rond het verbeteren van (digitale) beveiliging steeds scherper te krijgen en de wijze om dit onder de aandacht te krijgen bij vooral organisaties zonder eigen security-afdeling. Uiteindelijk zijn we in onze reis gekomen tot de opzet van dit rapport, waarmee we willen helpen om inzicht te verschaffen in de huidige staat van het Europese internet.

Belangrijk daarbij zijn vooral de contacten met MKB-Nederland (vooral Ellen Jacobs en Coen van den Berg), de Haagse Hogeschool (vooral Rutger Leukfeldt, Lianne Slot en Raoul Notté), TNO (vooral Robin de Haas, Jeroen Laarakkers en Carlijn Broekman), Marcel Verbraak, Security Delta (vooral Joris den Bruinen) en het laatste duwtje om vooral naar metingen op Europees niveau te kijken dat gegeven werd door Bart Groothuis, lid van het Europees Parlement. Daarnaast had dit rapport niet tot stand gekomen zonder de MIT-subsidie die we hebben mogen ontvangen van de provincie Zuid-Holland. Daarnaast danken we uiteraard alle mensen die hebben geholpen om dit rapport tot stand te laten komen, met name Marjolein van Enk, Richard Klein en Kevin Ammerlaan.

Wij hopen dat dit rapport onze lezers op zijn minst boeit, maar vooral dat het aanzet tot verder nadenken over wat wij zelf en samen kunnen doen om het cybercriminelen in ieder geval niet makkelijker te maken om hun slag te slaan. Neem gerust contact met ons op als je vragen of opmerkingen hebt over dit rapport.

Inleiding en aanleiding

Na de succesvolle campagne Veilig Zakelijk Internetten versie 1, die we samen met MKB-Nederland uitvoerden en die uiteindelijk zelfs de European Crime Prevention Awardsⁱⁱ won, schaalden we op. 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. We schaalden niet alleen op in de uitvoerende kant, maar ook in de communicatie. MKB-Nederland mobiliseerde uiteindelijk zo'n 50 brancheverenigingen, waarmee we een communicatiebereik kregen van honderdduizenden ondernemers. Toch kregen we het met z'n allen niet voor elkaar om de 2.500 bedrijven te vinden die zich wilden inschrijven voor een kosteloze test.

Dit probleem heeft ons 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 MKBⁱⁱⁱ. 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.

Onze ervaring 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.

Wij hebben 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^{iv}).

We hebben onszelf de vraag gesteld:

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 hebben we besloten om te kijken of we een rapport kunnen samenstellen met risico's en kwetsbaarheden van een bepaalde onderneming op basis van uitvraag van allerlei openbare bronnen op het internet. Aangezien we geen goedkeuring van de ondernemer wilden hebben, leek de URL van een organisatie ons een logisch vertrekpunt. Daarmee kunnen we kwetsbaarheden in website, e-mail, gehackte accounts etc. blootleggen.

Uitvoering

In de uitvoering zijn we gestart met het controleren van enkele domeinen. Later is de computerkracht opgeschaald, zijn processen verder geautomatiseerd en inmiddels hebben we de mogelijkheid om zo'n 300.000 domeinen per dag te meten. Dit betekent dat we het volledige Nederlandse internet met ruim 6 miljoen URL's^v in ongeveer drie weken kunnen meten. Verdere opschaling hierin is overigens nog prima mogelijk: alle data is opgeslagen in een zogenaamde Elastic-omgeving, die bedoeld is voor het verwerken van (zeer) grote hoeveelheden data.

Toen onze tooling 'stond', hebben we besloten een meting uit te voeren over de beveiliging van alle domeinen in Europa, waarbij we beveiliging van organisaties in landen ten opzichte van elkaar meten. Er ligt geen echte onderzoeksvraag aan dit rapport ten grondslag, maar ThreadStone heeft dit rapport opgezet om een stap te zetten in het verwezenlijken van onze missie: *gezamenlijk het Nederlandse en Europese internet veiliger maken*. Wij denken dat de onafhankelijke, niet-commerciële meting, waarvan wij de resultaten feitelijk onderbouwd presenteren in dit rapport, inzicht geeft in de actuele verschillen in Europa.

Als we kijken naar het internet van de 27 leden van de Europese Unie, dan zijn de in tabel 1 genoemde aantallen domeinen geregistreerd volgens Domeinstats^{vi} d.d. 19 augustus 2022.

Domein	Land	Aantal domeinen volgens Domainnamestat
AT	Oostenrijk	1.840.950
BE	België	2.023.591
BG	Bulgarije	101.825
CY	Cyprus	7.596
CZ	Tsjechië	1.612.020
DE	Duitsland	23.151.760
DK	Denemarken	1.531.657
EE	Estland	175.405
ES	Spanje	2.230.449
FI	Finland	574.884
FR	Frankrijk	5.525.714
GR	Griekenland	439.075
HR	Kroatië	132.296
HU	Hongarije	969.667
IE	Ierland	388.156
IT	Italië	4.068.901
LT	Litouwen	244.402
LU	Luxemburg	119.065
LV	Letland	151.322
MT	Malta	14.317
NL	Nederland	6.696.486
PL	Polen	3.414.452
PT	Portugal	426.219
RO	Roemenië	860.596
SE	Zweden	2.623.779
SI	Slovenië	159.863
SK	Slowakije	626.976
	Totaal	60.111.423

We hebben gezocht naar gegevensbronnen met alle domeinen die zijn geregistreerd; hiervoor hebben we de Open Data-set van Rapid7 gebruikt^{vii}. Op het moment van uitvoeren van de meting was deze data nog openbaar. In totaal zijn er ruim 18 miljoen Europese URL's gemeten.

In tabel 2 zijn de aantallen domeinen per land weergegeven die we in ons databestand aantreffen. We hebben ons daarbij beperkt tot de 27 landen in de Europese Unie. In deze tabel is ook aangegeven dat we met deze aantallen een meting verrichtten die een maximale foutmarge van <1% en een 99% nauwkeurigheid heeft^{viii}. Alleen voor Cyprus en Malta geldt een iets hogere foutmarge vanwege het beperkte aantal domeinen dat daar geregistreerd is.

Domein	Land	Aantal domeinen volgens Domainnamestat	Aantal domeinen gecontroleerd	Foutmarge bij 99% betrouwbaarheid
AT	Oostenrijk	1.840.950	482.565	<1% foutmarge
BE	België	2.023.591	609.874	<1% foutmarge
BG	Bulgarije	101.825	37.072	<1% foutmarge
CY	Cyprus	7.596	1.400	3,11% foutmarge
CZ	Tsjechië	1.612.020	534.045	<1% foutmarge
DE	Duitsland	23.151.760	6.808.040	<1% foutmarge
DK	Denemarken	1.531.657	525.828	<1% foutmarge
EE	Estland	175.405	61.211	<1% foutmarge
ES	Spanje	2.230.449	534.404	<1% foutmarge
FI	Finland	574.884	218.843	<1% foutmarge
FR	Frankrijk	5.525.714	1.397.551	<1% foutmarge
GR	Griekenland	439.075	62.174	<1% foutmarge
HR	Kroatië	132.296	49.639	<1% foutmarge
HU	Hongarije	969.667	328.530	<1% foutmarge
IE	Ierland	388.156	109.644	<1% foutmarge
IT	Italië	4.068.901	1.218.426	<1% foutmarge
LT	Litouwen	244.402	81.791	<1% foutmarge
LU	Luxemburg	119.065	34.526	<1% foutmarge
LV	Letland	151.322	48.612	<1% foutmarge
MT	Malta	14.317	1.976	2,69% foutmarge
NL	Nederland	6.696.486	3.026.904	<1% foutmarge
PL	Polen	3.414.452	774.067	<1% foutmarge
PT	Portugal	426.219	135.697	<1% foutmarge
RO	Roemenië	860.596	238.676	<1% foutmarge
SE	Zweden	2.623.779	720.151	<1% foutmarge
SI	Slovenië	159.863	63.571	<1% foutmarge
SK	Slowakije	626.976	181.851	<1% foutmarge
	Totaal	60.111.423	18.287.068	

In het onderzoek hebben we geautomatiseerd elk van de ruim 18 miljoen 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?
- Is de website gereed voor nieuwe standaarden?

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.

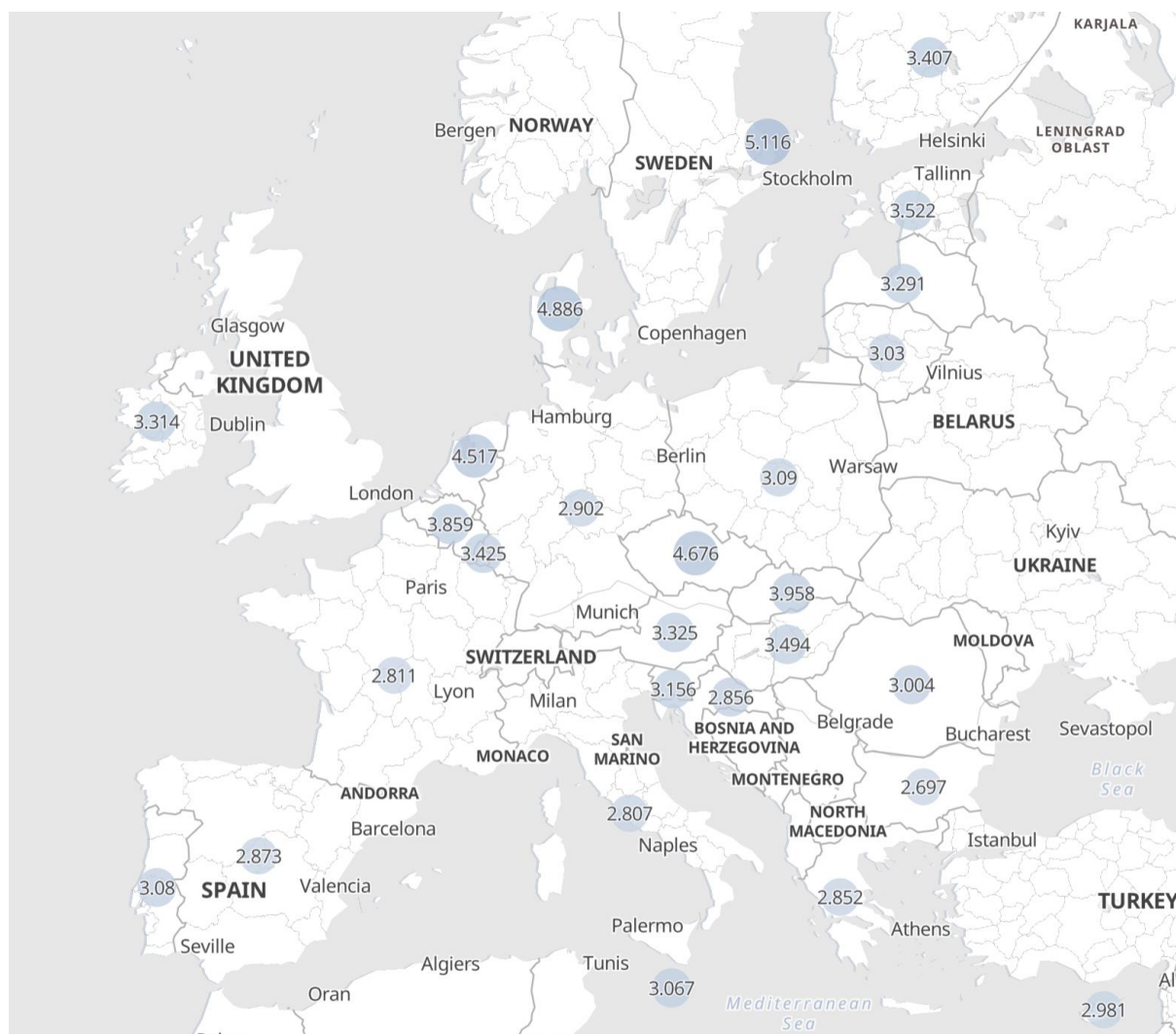
Resultaten

Overall score

Hieronder volgt eerst per land een overall score, van 1-10. Deze score is een gemiddelde van alle gemeten domeinen van het betreffende land. 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.

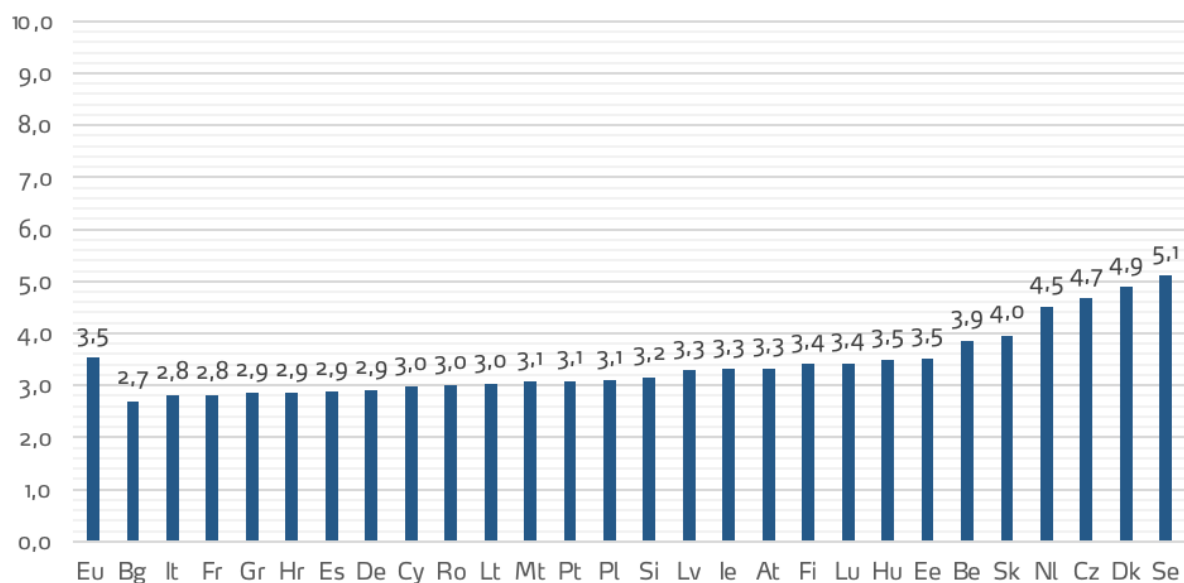
De resultaten

Uit de meting zijn de volgende scores per land gemeten (op de volgende pagina in tabelvorm):



In tabel (volgorde score van laag naar hoog):

Gemiddelde score van de 27 lidstaten



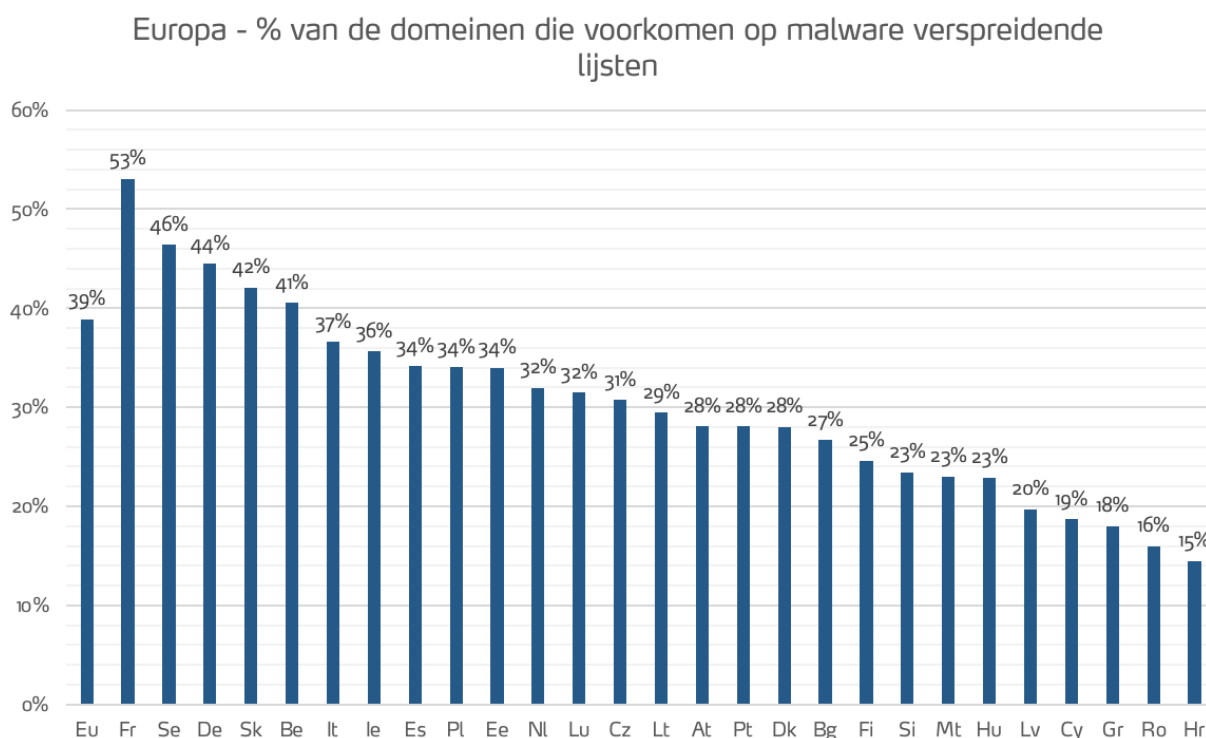
Hierna volgen de individuele metingen die zijn uitgevoerd.

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

De volgende resultaten zijn gemeten:

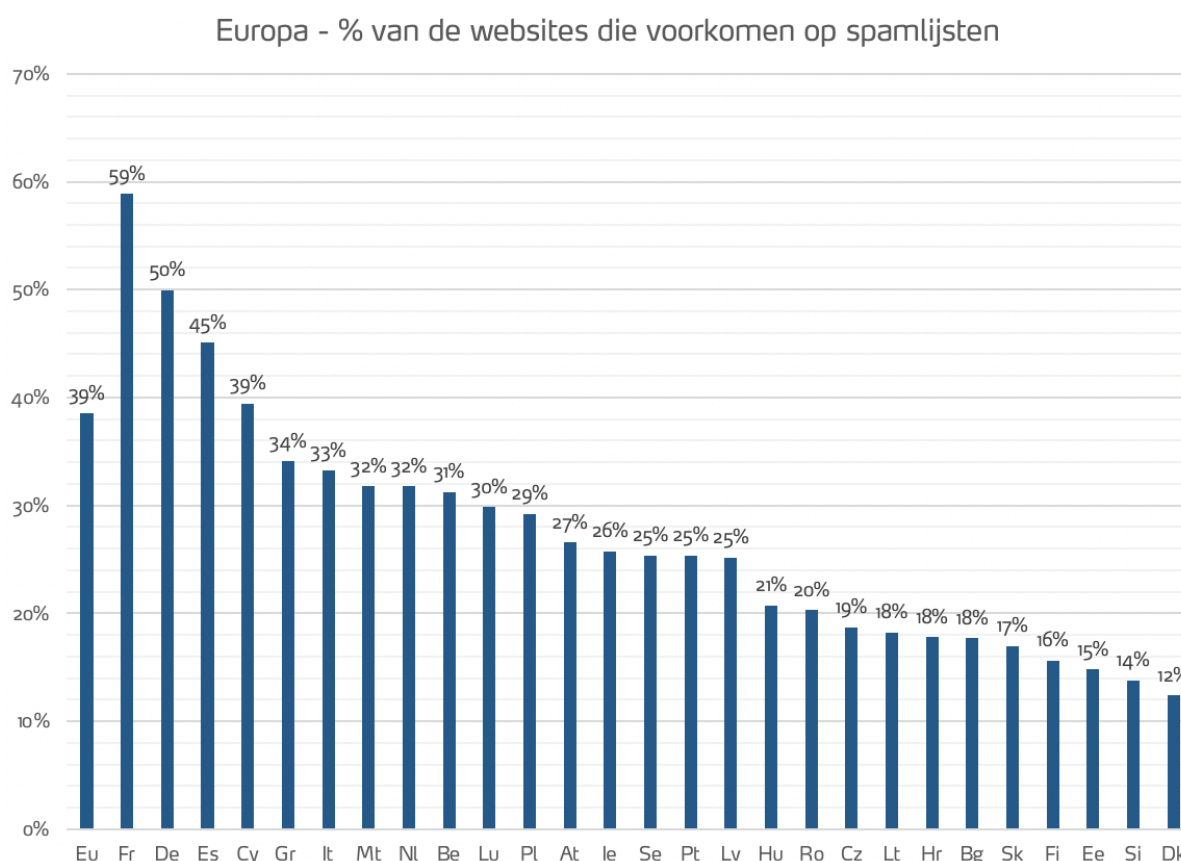


Verspreidt de website geen spam?

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

De volgende resultaten zijn gemeten:

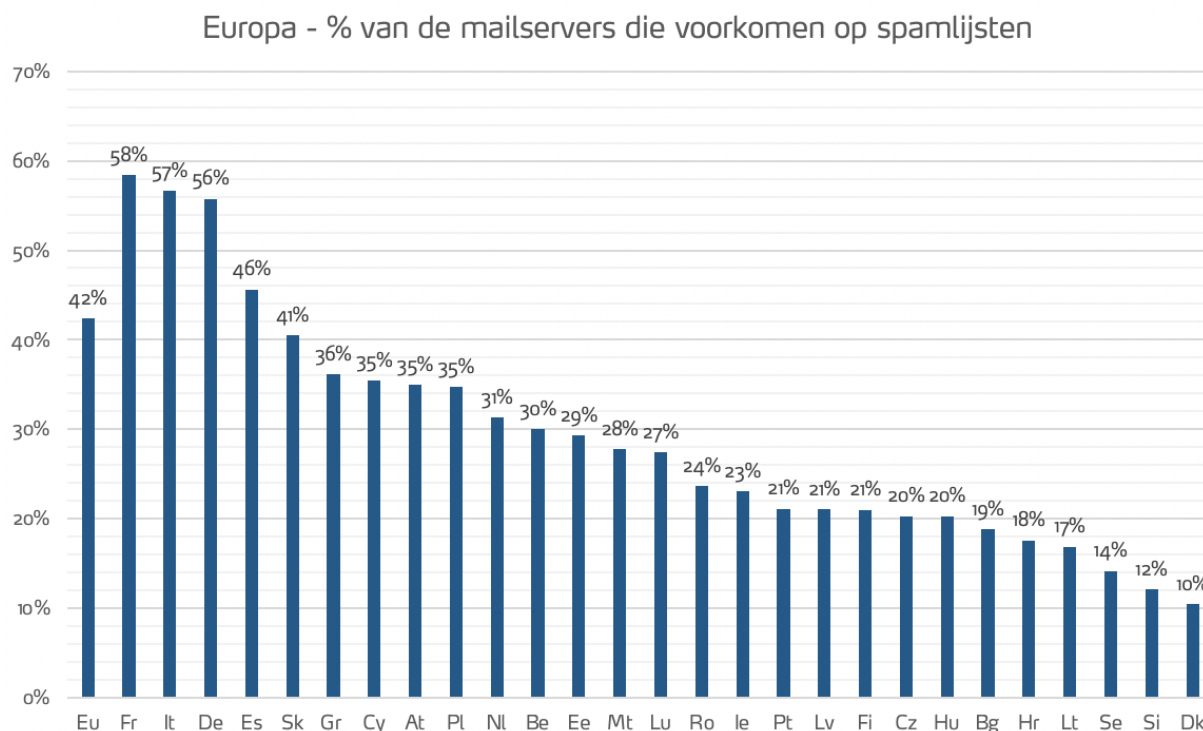


Verspreidt de mailserver geen spam?

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

De volgende resultaten zijn gemeten:

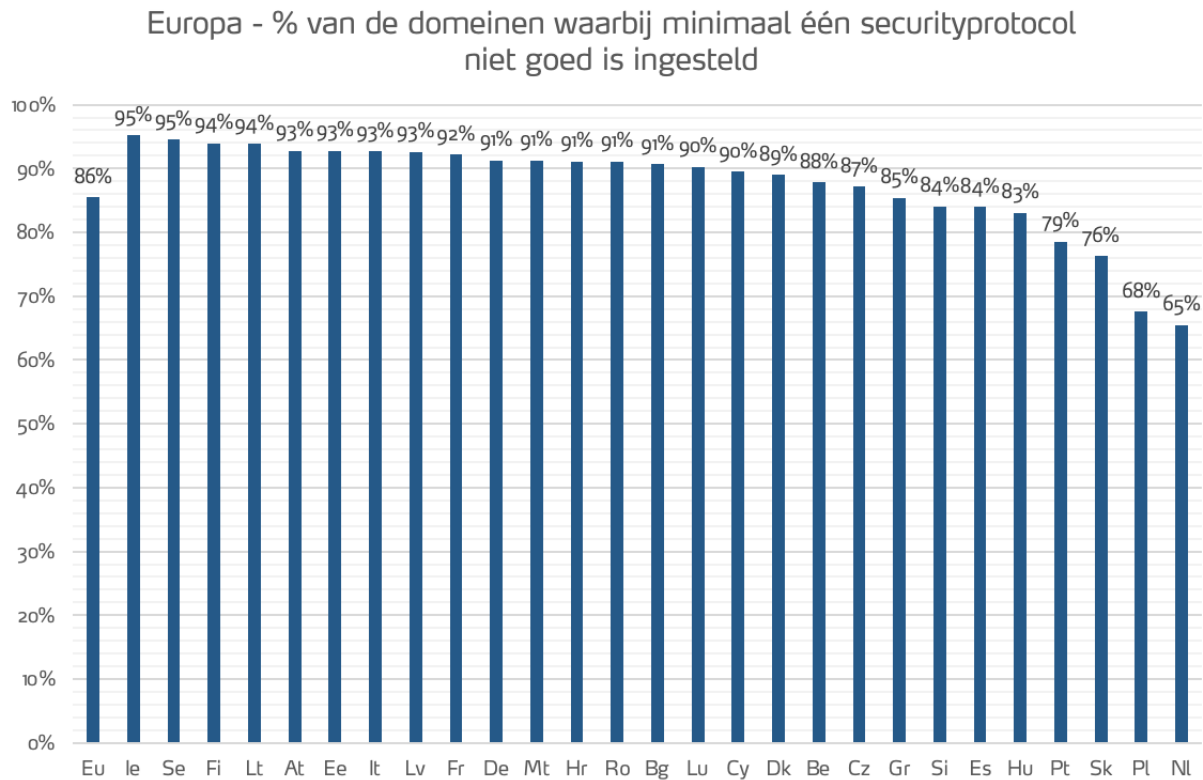


Kan de e-mail niet misbruikt worden?

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

De volgende resultaten zijn gemeten:

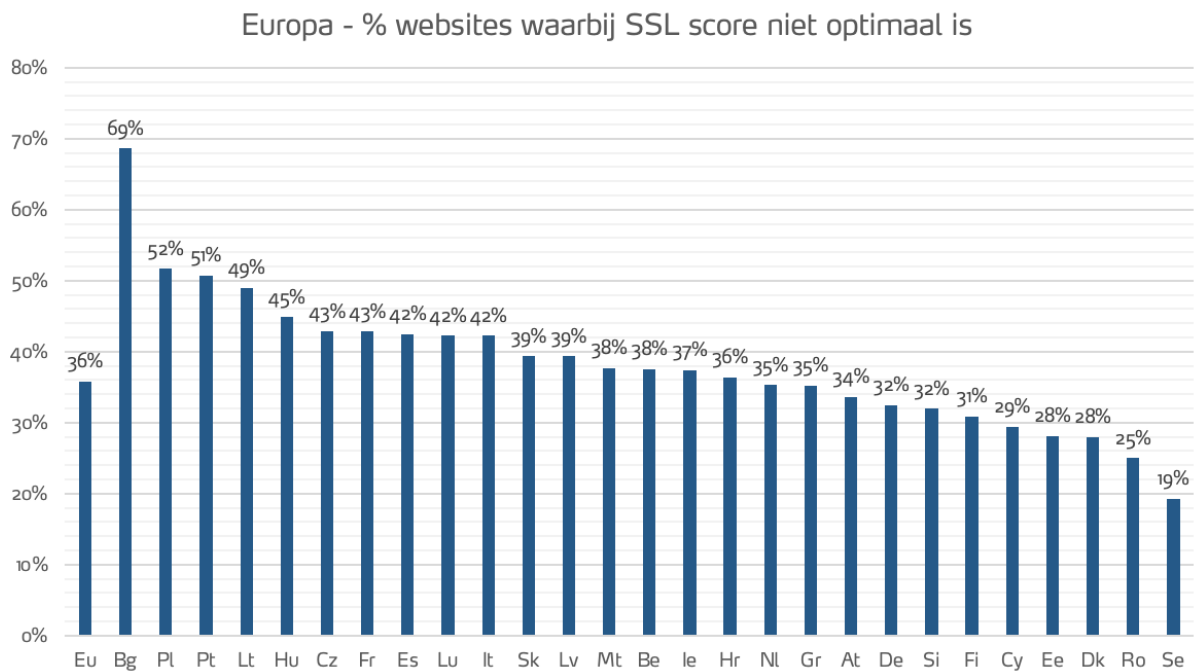


Kan het verkeer met de website niet worden onderschept?

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 (zogenoemd "https"). De resultaten in de grafiek geeft het percentage websites weer, waarbij de score lager is dan een zogenaamde 'A-grade'.

De resultaten

De volgende resultaten zijn gemeten:

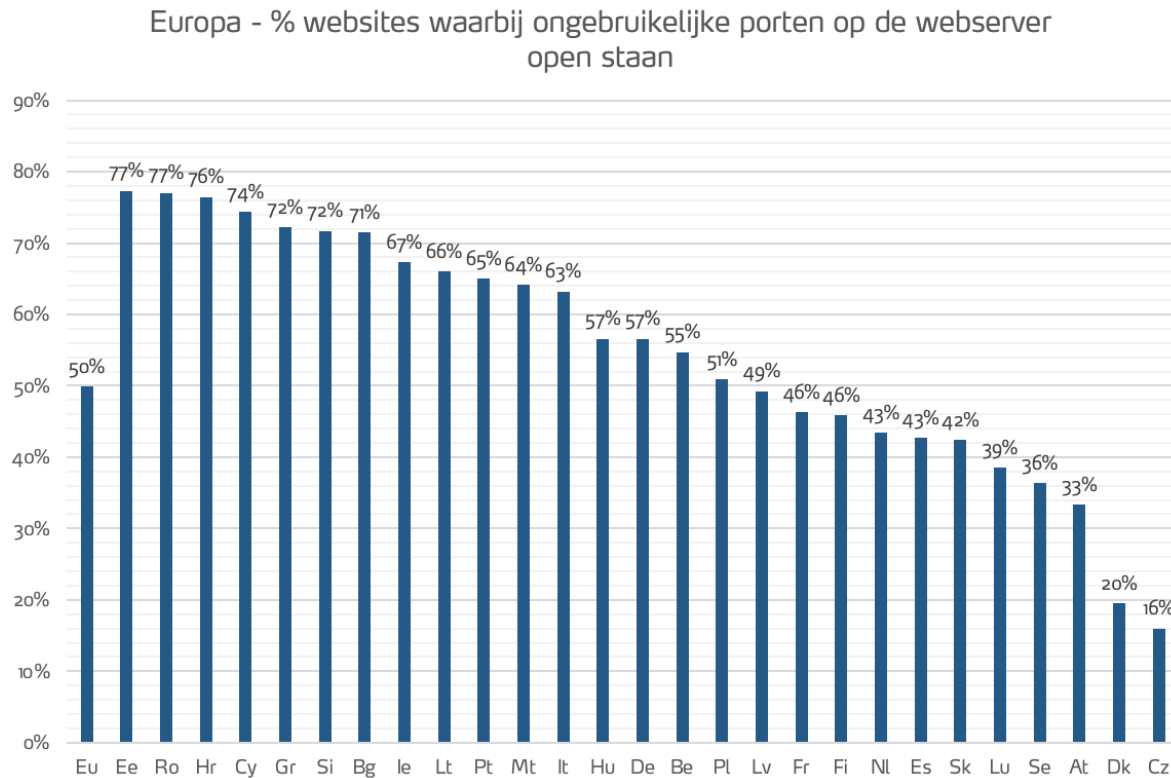


Zijn er geen ongebruikelijke aanvalspaden op de website mogelijk?

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

De volgende resultaten zijn gemeten:

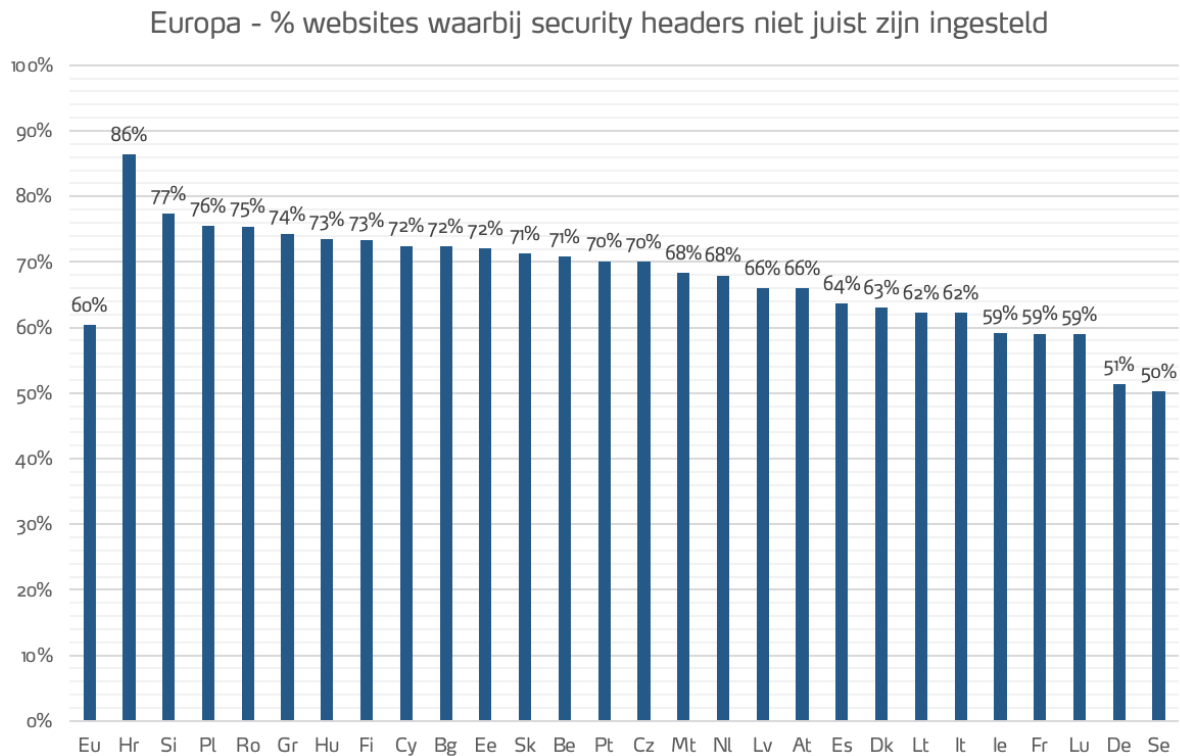


Worden bezoekers van de website voldoende beschermd?

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

De volgende resultaten zijn gemeten:

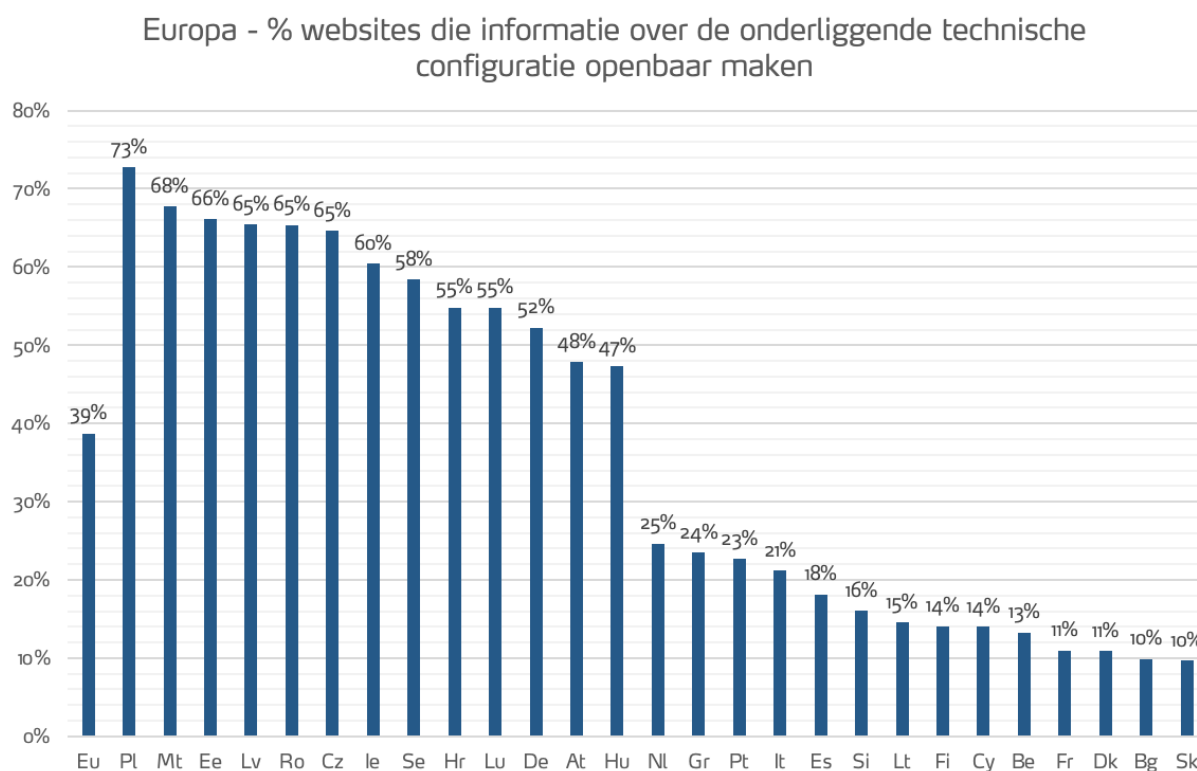


Is informatie over de configuratie van de website afgeschermd?

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

De volgende resultaten zijn gemeten:

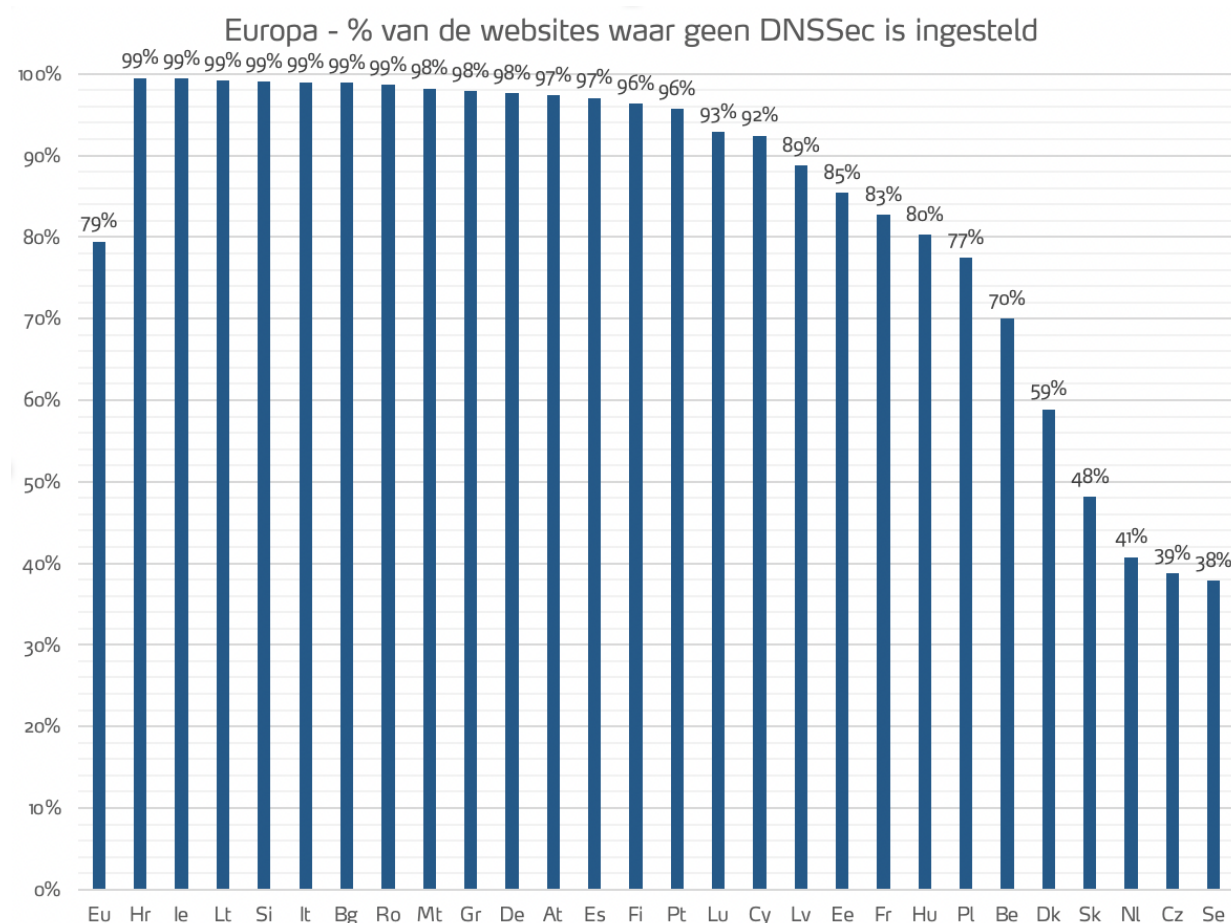


Kan websiteverkeer naar de website niet worden gemanipuleerd?

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

De volgende resultaten zijn gemeten:

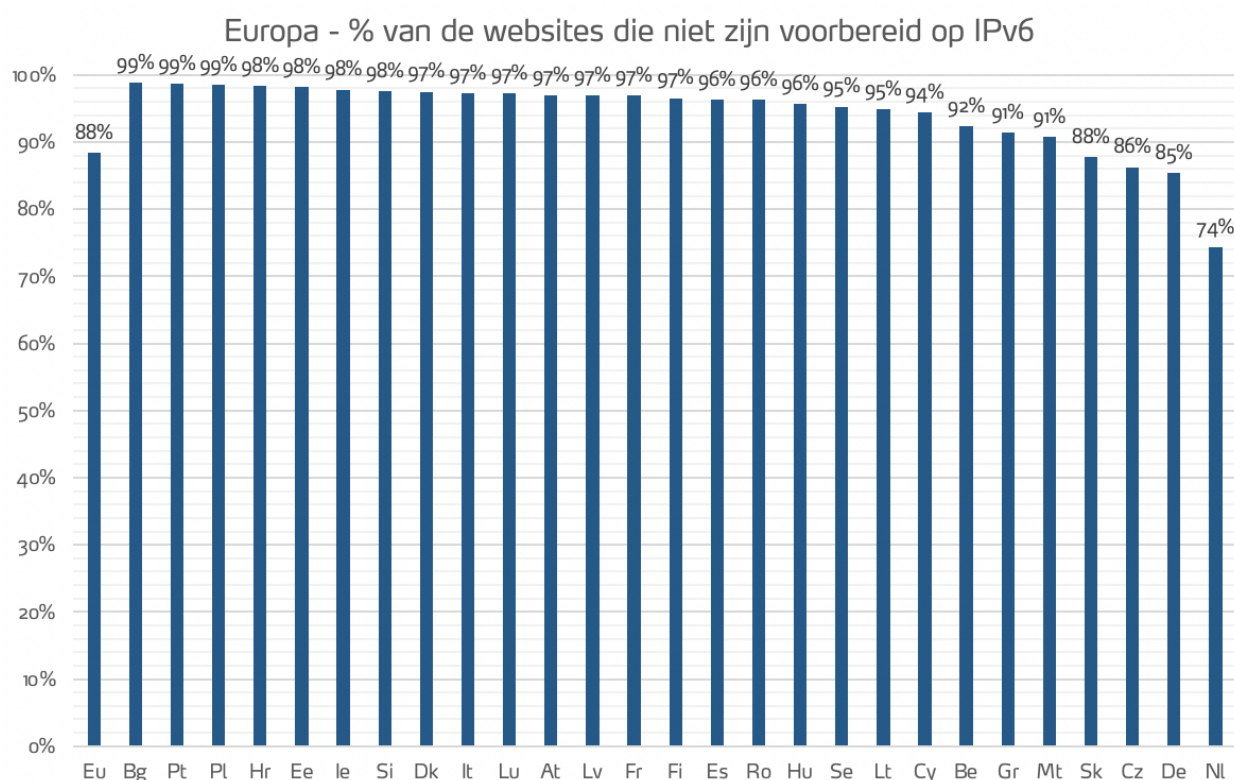


Is de website gereed voor nieuwe standaarden?

Wij controleren of de gemeten website, mailserver en zogenaamde nameserver de nieuwste internetprotocollen ondersteunen (IPv6). Deze controle geeft niet direct een security issue aan en is verder niet opgenomen in de overall scoreberekeningen.

De resultaten

De volgende resultaten zijn gemeten:



Conclusie en discussie

De algehele beveiliging van het Europese internet ligt op een laag niveau. Als we naar de gemiddelden over Europa kijken, dan komen we tot de volgende resultaten:

Gecontroleerde kwetsbaarheid	Resultaat EU	Technische meting	Mogelijk gevolg en impact
Verspreidt de website geen malware?	39% 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?	39% 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?	42% 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 86% 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 36% 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?	50% van de webserver 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?	60% 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 39% 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?	79% van de websites heeft geen DNSSec ingesteld	DNSSec is niet aanwezig	Kwaadwillenden kunnen wachtwoorden of andere vertrouwelijke informatie onderscheppen van bezoekers van de website.
Is de website gereed voor nieuwe standaarden?	88% van de webserver is niet gereed voor IPv6	Geen ondersteuning van IPv6 (geen security issue)	In de toekomst zal steeds meer en meer verkeer verlopen via de nieuwe IPv6-standaarden.

Als we kijken naar de gemiddelden, dan scoren alleen België, Slowakije, Nederland, Tsjechië, Denemarken en Zweden hoger dan het gemiddelde van de 27 lidstaten. De overige 21 lidstaten scoren onder het gemiddelde.

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 over Europa zeer slecht is geregeld (86% 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 webserver ongebruikelijke aanvalspaden open heeft staan, is een verantwoordelijkheid van deze bedrijven. Ditzelfde geldt voor het gereed maken van de webserver 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 in Europa. 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.

Wij zijn van mening dat elke organisatie in Europa een kosteloos rapport zou moeten ontvangen waarin de eigen kwetsbaarheden inzichtelijk worden gemaakt. Dit, tezamen met begrijpelijke communicatie door een betrouwbare, aansprekende bron en eventuele ondersteuning om gesignaleerde kwetsbaarheden werkelijk weg te nemen, kan ondernemers in beweging brengen.

ThreadStone werkt op dit moment samen met een aantal brancheorganisaties en Security Delta om rapportages per sector aan ondernemers aan te bieden (via de communicatiekanalen van de brancheorganisaties). Daarbij staat voorop dat de rapportages geen commerciële insteek hebben en alleen moeten dienen om de ondernemer bewust te maken en handelingsperspectief te bieden. Vanuit deze rapportages kan vervolgens verder worden gewerkt aan meer weerbare organisaties, ketens, sectoren tot aan complete landen en een meer cyberweerbare Europese Unie.

Met deze metingen wordt ook inzicht geboden in hoe organisaties ten opzichte van elkaar 'scoren'. Hoe doet een organisatie met 10 personen het ten opzichte van een organisatie met meer dan 250 medewerkers? Hoe doet een organisatie in de bouw het ten opzichte van een organisatie in de zakelijke dienstverlening? Hoe doet een organisatie in de provincie Friesland het ten opzichte van een organisatie op Sicilië? Door uitbreiding van onze databronnen kunnen we ook daar inzicht in gaan bieden, waardoor een kwalitatieve meting op cyberweerbaarheid mogelijk wordt die voortkomt uit kwantitatieve metingen.

Eenzijds meten en vergelijken we dus op 'macroniveau', anderzijds kunnen we rapportages aanleveren op 'microniveau', per ondernemer.

De komende tijd gaan wij door met het uitvoeren van deze metingen. In 2023 willen we een nieuw rapport opstellen, waarbij we ook de resultaten op landniveau verder zullen uitsplitsen. Daarnaast willen we een vergelijking maken met dit rapport om inzichtelijk te maken of we met z'n allen de juiste kant op bewegen. Ten slotte willen we ook graag meer duiding gaan geven aan de cijfers. Hiervoor komen we graag in gesprek met stakeholders om, mede op basis van dit rapport, vragen te beantwoorden zoals:

- Wat kunnen we leren van de landen die beter presteren dan de rest (wat is de achterliggende reden dat ze beter scoren)?
- Op welke wijze kunnen we helpen om de digitale weerbaarheid van de lidstaten van de Europese Unie omhoog te brengen?

Heb je hier ideeën over of heb je andere suggesties, aanbevelingen? Neem gerust contact met ons op: we gaan graag het gesprek aan!

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 uw 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.

Is uw website, mailserver en nameserver gereed voor nieuwe standaarden?

Aandachtspunt - Mogelijke impact

Uw server is niet voorbereid voor de nieuwe internetstandaarden.	In de toekomst zal steeds meer en meer verkeer verlopen via de nieuwe IPv6 standaarden. Het is daarom verstandig om hier ook voorbereid op te zijn.
--	---

Opbouw score

Deze controle maakt geen deel uit van de score. Een negatief resultaat op deze controle heeft dus geen impact op de score.

Verwijzingen naar andere bronnen

- ⁱ <https://nl.wikipedia.org/wiki/Spoofing>
- ⁱⁱ Verwijzing naar winnen Crime Prevention Awards
- ⁱⁱⁱ Verwijzing naar onderzoek HHS met Optimism Bias
- ^{iv} Verwijzing naar onderzoek waaruit blijkt dat merendeel van de ondernemers de IT uitbesteed
- ^v Verwijzing naar SIDN met 6M domeinen
- ^{vi} <https://domainnamestat.com/statistics/tldtype/country>
- ^{vii} <https://opendata.rapid7.com/>, op het moment van meten was deze data nog volledig openbaar
- ^{viii} <https://nl.checkmarket.com/steekproefcalculator>