TRANSPORT LAYER SECURITY HEALTHCHECK

Januari, 2015

LEAKFREE – IT Security made simple

Inhoudsopgave

INTRODUCTIE

Introductie

Dit document is een overzicht van een in januari 2015 door LeakFree uitgevoerd onderzoek naar de staat van Transport Layer Security (TLS) beveiliging bij een groot aantal prominente publieke Nederlandse webservers.

TLS faciliteert cryptografisch beveiligde verbindingen tussen twee computersystemen en wordt voor een brede waaier aan verschillende toepassingen gebruikt: van web (HTTPS) en e-mail (STARTTLS voor IMAP, POP3 en SMTP) tot Voice-over-IP (VoIP) en Virtual Private Network (VPN) verkeer. TLS vormt de ruggengraat van veilige communicatie over internet en het gebruik van versleutelde verbindingen is in sommige gevallen dan ook verplicht binnen sommige organisaties en bedrijfssectoren. Een goed geconfigureerde en veilige TLS opstelling is dan ookvan groot belang. In de praktijk wil het nogal eens lastig blijken om dit goed op orde te krijgen, met alle gevolgen van dien. In de afgelopen jaren zijn er verschillende kwetsbaarheden in zowel bepaalde versies van het TLS protocol als specifieke implementaties daarvan ontdekt [1,2,3] en hebben we gezien hoe serieus de gevolgen van aanvallen op zowel de onderliggende infrastructuur [4,5] als TLS-servers zelf [6,7] kunnen zijn. Om deze redenen heeft LeakFree besloten een korte test van de veiligheid van TLS configuraties binnen de Nederlandse context uit te voeren en de resultaten in dit onderzoeksraport te publiceren.

Dit onderzoek is uiteraard niet uitputtend en dient vooral als indicatie van, en waarschuwingssignaal over, de huidige staat van TLS beveiliging. Om beheerders van TLS configuraties enkele handvaten ter verbetering te bieden heeft LeakFree een gratis te downloaden whitepaper met *best practices* gepubliceerd [8].

TESTOVERZICHT

Methodologie

Om een beeld te krijgen van de veiligheidstoestand van TLS configuraties in Nederland zijn er door LeakFree een aantal lijsten gemaakt met interessante subjecten (zie volgende sectie) als representatieve doorsnede voor de meest prominente webservers binnen hun veld. Uiteraard zijn deze niet representatief voor webservers in het algemeen aangezien onderhoud en securityawareness veel hoger zal liggen bij deze prominente webservers dan gemiddeld het geval is. Daarmee dienen ze echter wel als goede maatstaf voor een korte *healthcheck*. Immers, als de configuraties van dergelijke prominente webservers mankementen vertonen is het zeer waarschijnlijk dat minder *'high profile´* webservers dat ook doen.

Er zijn twee losse tests met een onderling verschillende aanpak uitgevoerd op dezelfde subjecten, waarvan het eindresultaat het gemiddelde van beide tests is. Dit om een evenwichtig overzicht te krijgen en de impact van onvolledigheden, gebrekkigheden en verschillende test-criteria in tools en methodologie alsmede vertekende resultaten als gevolg van connectie-problemen te minimaliseren. Iedere test bestond uit een combinatie van publiek beschikbare [9,10] tools en enkele door LeakFree ontwikkelde tools. De tests poogden om een uitvoerig maar niet uitputtend overzicht te bieden en tegelijkertijd zo *non-intrusive* mogelijk te zijn. De nadruk ligt dan ook op een algemeen overzicht van de meest prominente en ergste veiligheidsrisico's. In het testoverzicht werd uiteindelijk niet gekeken naar de mankementen bij individuele subjecten maar naar hun verspreiding over de gehele testset.

TESTOVERZICHT

Tijdens de tests is er gekeken naar de volgende zaken en hun verspreiding binnen de testsets (voor een toelichting van deze elementen en de daaraan verbonden risico's verwijzen we naar de Transport Layer Security Whitepaper van LeakFree [8]:

- Is er ondersteuning voor TLS?
- Certificaatgerelateerde zaken:
    - Is het certificaat geldig?
    - Wordt de hostname gedekt?
    - Gebruikt het certificaat een zwakke sleutellengte of zwak hashing algoritme?
    - Gebruikt het certificaat een zwak gegenereerde sleutel?
    - Bevindt er zich een zwak certificaat in de certificate chain?

- Protocolgerelateerde zaken:
    - Welke TLS versies worden er ondersteunt?
    - Welke TLS versie wordt er maximaal ondersteunt?

- Versleutelingsgerelateerde zaken:
    - Worden zwakke versleutelingsmethoden (RC2, RC4, DES) ondersteunt?
    - Wordt er slechts zwakke versleutling ondersteunt (zwakke methoden of sleutellengtes)?
    - Wat is de kleinst ondersteunde sleutellengte?

- Configuratiegerelateerde zaken:
    - Is er ondersteuning voor HTTP Strict Transport Security?
    - Is er ondersteuning voor secure renegotiation?
    - Is er ondersteuning voor secure cookies?
    - Is er ondersteuning voor TLS_FALLBACK_SCSV?
    - Is er ondersteuning voor Forward Secrecy?

- Kwetsbaarheidsgerelateerde zaken:
    - Is de configuratie kwetsbaar voor een van de volgende zaken: BEAST, CRIME, BREACH, POODLE, HEARTBLEED, TRIPLE HANDSHAKE of CVE-2014-0224

TESTOVERZICHT

Bepaalde testelementen zijn niet onmiddelijk een indicatie voor een uitbuitbare kwetsbaarheid aangezien in veel gevallen er tegenwoordig ook client-side mitigaties zijn (zoals in het geval van BEAST). In één enkel geval, namelijk CVE-2014-0224, is er expliciet getest op uitbuitbare kwetsbaarheid en zijn de corresponderende statistieken een directe indicatie van het aantal kwetsbare servers.

Hoewel bepaalde misconfiguraties uiteraard niet direct tot een kwetsbaarheid hoeven te leiden is hun aanwezigheid wel een reden tot zorg aangezien gebruikers met oudere browsers (zoals Internet Explorer 6 op Windows XP) in het geval van een slecht geconfigureerde server wel kwetsbaar zijn. Tevens zijn ze een indicatie van de mate waarin *best practices* worden nageleeft en daarmee een indicatie voor de kans dat deze configuraties waarschijnlijk (langer dan nodig) kwetsbaar zullen zijn voor nieuwe kwetsbaarheden.

Test-sets

Gekozen is voor de volgende testsets als representatief voor hun specifieke segment:

- De top 200 meest populaire websites binnen het .nl TLD
- De websites van de top 50 grootste Nederlandse gemeenten
- 55 prominente overheidswebsites
- 55 websites van Nederlandse mulitnationals en andere prominente bedrijven

Deze testsets bieden een kijk op de staat van TLS-gebruik voor webservers zowel binnen de publieke als de private sector in Nederland.

TESTOVERZICHT

Resultaten

De geaggregeerde resultaten van de uitgevoerde tests zijn in dit raport opgenomen in de appendix. Hieronder volgt een samenvatting van de meest noemenswaardige mankementen gedeeld door de meeste of alle sectoren:

Van de geteste servers bood steeds een kleine minderheid geen enkele ondersteuning voor TLS en was daarmee bij voorbaat als onveilig te classificeren.

Certificaten

Met betrekking tot de gebruikte certificaten sprongen de volgende zaken in het oog:

- *Ongeldig certificaat of hostname mismatch*: Een onacceptabel percentage van de geteste certificaten was als onveilig te classificeren (hetzij vamwege ongeldigheid doordat ze verlopen of self-signed waren, hetzij door onvoldoende hostname dekking). Ongeacht verdere configuratie is hiermee de gehele TLS opstelling onveilig.

- *Zwak signature algoritme*: Een te groot percentage van de certificaten in sommige sectoren gebruikte een zwak hashing algoritme. Dit betrof altijd het het nog steeds veelgebruikte SHA-1. Vanwege compatibiliteitsredenen is dit begrijpelijk maar stappen dienen ondernomen te worden om dit in de nabije toekomst uit te faseren.

- *Zwak in-chain certificaat*: Het overgrote deel van de certificaten had een *in-chain* certificaat wat als 'zwak' te classificeren viel (vanwege een zwak signature algoritme of een zwakke sleutellengte), waarmee de hele *certificate chain* in gevaar komt. Een goede *Public Key Infrastructure (PKI)* dient dit zoveel mogelijk te voorkomen.

TESTOVERZICHT

Protocolversies

Met betrekking tot de ondersteunde protocolversies sprongen de volgende zaken in het oog:

- *Ondersteuning voor kwetsbare protocolversies*: Ondanks het relatief geringe aantal servers dat ondersteuning voor kwetsbare protocolversies (zoals SSL 2.0 en 3.0) bood dient ondersteuning hiervoor uitgeschakeld te zijn. In het geval van SSL 2.0 zelfs ongeacht mogelijke compatibiliteitskwesties.

- *Geen ondersteuning voor nieuwe protocolversies:* Te weinig servers ondersteunden de nieuwste (en veiligere) protocolversies, waarmee gebruikers van nieuwere browsers gedwongen worden om op oudere en onveiligere protocolversies terug te vallen.

Versleutelingsmethoden

Met betrekking tot de ondersteunde versleutelingsmethoden sprongen de volgende zaken in het oog:

- *Ondersteuning voor kwetsbare bulkversleutelingsalgoritmen*: Hoewel een relatief klein percentage kwetsbare en verouderde algoritmen (zoals RC2 en DES) ondersteunde kan compatibiliteit hier geen excuus zijn. In het geval van RC4 dient ondersteuning ook langzaam uitgefaseerd te worden.

- *Ondersteuning voor zwakke sleutellengtes*: De kleinste geobserveerde sleutellengte voor bulkversleuteling betrof 40-bits, wat volstrekt onveilig is gegeven moderne standaarden.

TESTOVERZICHT

Configuratie

Met betrekking tot de configuratieinstellingen sprongen de volgende zaken in het oog:

- *Afwezigheid ondersteuning voor HTTP Strict Transport Security (HSTS)*: Het overgrote merendeel van de servers bood geen ondersteuning voor HSTS en stelt daarmee clients onnodig blood aan de daarmee geassocieerde risico's (zoals een *SSL-Stripping* aanval).

- *Afwezigheid ondersteuning Forward Secrecy*: Het overgrote deel van de servers bood geen ondersteuning voor Forward Secrecy, wat in het geval van een toekomstige diefstal van de certificaat *private keys* met terugwerkende kracht alle eerder onderschepte verkeer ook in gevaar brengt.

- *Afwezigheid ondersteuning secure cookies*: Het overgrote deel van de servers bood geen ondersteuning voor secure cookies waardoor een aanvaller, ondanks een beveiligde verbinding, hier alsnog informatie uit kan extraheren.

- *Afwezigheid ondersteuning TLS_FALLBACK_SCSV*: Het merendeel van de servers bood geen ondersteuning voor TLS_FALLBACK_SCSV waardoor een aanvaller in staat is om een zogenaamde *downgrade* aanval uit te voeren.

Hoewel de bovenstaande configuratie-opties strict genomen niet noodzakelijk voor een veilige TLS-configuratie zijn verdient ondersteuning de voorkeur. Ondersteuning van bovenstaande opties vergroot de veiligheid zonder dat dit ten koste gaat van compatibiliteit.

TESTOVERZICHT

Kwetsbaarheden

Met betrekking tot de kwetsbaarheden in TLS sprongen de volgende zaken in het oog:

- *BEAST:* Het overgrote deel van de servers was kwetsbaar voor BEAST. Hoewel de meest moderne browsers client-side mitigatie hiertegen bevatten geldt dit niet voor verouderde browsers.

- *CRIME:* Hoewel slechts een klein deel van de servers in sommige sectoren kwetsbaar was voor CRIME en hoewel successvolle exploitatie hiervan afhankelijk is van het ontwerp van de webapplicaties op de server, is dit een onnodig risico aangezien CRIME-mitigatie geen compatibiliteitsproblemen met zich meebrengt.

Het verhelpen van sommige kwetsbaarheden (zoals BEAST) brengt zorgvuldige en gecompliceerde afwegingen met zich mee. Om BEAST veilig te verhelpen gaat dit of ten koste van de compatibiliteit of introduceert men een andere zwakte in de configuratie.

- *BREACH*: Hoewel de meeste servers mogelijk kwetsbaar voor BREACH zijn is dit niet met zekerheid te zeggen aangezien successvolle exploitatie afhangt van het ontwerp van de webapplicaties op de server. Tevens kan de meest voor de handliggende BREACH-mitigatie (het uitschakelen van ondersteuning voor HTTP-compressie) grote (negatieve) gevolgen voor de performance hebben.

- *POODLE:* Een klein deel van de servers was kwetsbaar voor de SSL-variant van POODLE en een ongeveer evengroot deel voor de TLS versie. In beide gevallen betreft het hier een onnodig risico.

- *CVE-2014-0224:* Een klein deel van de servers was kwetsbaar (zowel theoretisch als praktisch uitbuitbaar) voor CVE-2014-0224, tevens een onnodig risico gegeven het feit dat mitigatie geen compatibiliteitsproblemen met zich meebrengt.

Conclusie

Over het algemeen is te zien dat de veiligheid van TLS configuraties in de Nederlandse context op veel vlakken nog te kort schiet.

De grootste problemen lijken te liggen bij het percentage van servers dat geen enkele of volledig onveilige (in de vorm van ongeldige of self-signed certificaten) ondersteuning voor TLS biedt. Ten tweede springt ofwel nodeloze backwards compatibility, ofwel gebrekkig regelmatig onderhoud (in de vorm van ondersteuning voor verouderde en kwetsbare protocolversies en versleutelingsalgoritmen) in het oog. Het gevolg hiervan is een te groot percentage servers dat kwetsbaar is voor verschillende (vaak al geruime tijd bekende) kwetsbaarheden. Met name BEAST, POODLE (in SSL en TLS variant) en CVE-2014-0224 kwamen in alle sectoren terug. Als laatste wordt vrijwel nergens ondersteuning geboden voor extra veiligheidsmaatregelen zoals HSTS, secure cookies, forward secrecy of downgrade prevention.

Het lijkt er echter wel op dat ernstige kwetsbaarheden met veel media aandacht uiteindelijk verholpen worden, zoals blijkt uit het feit dat geen enkele van de geteste servers kwetsbaar was voor HEARTBLEED.

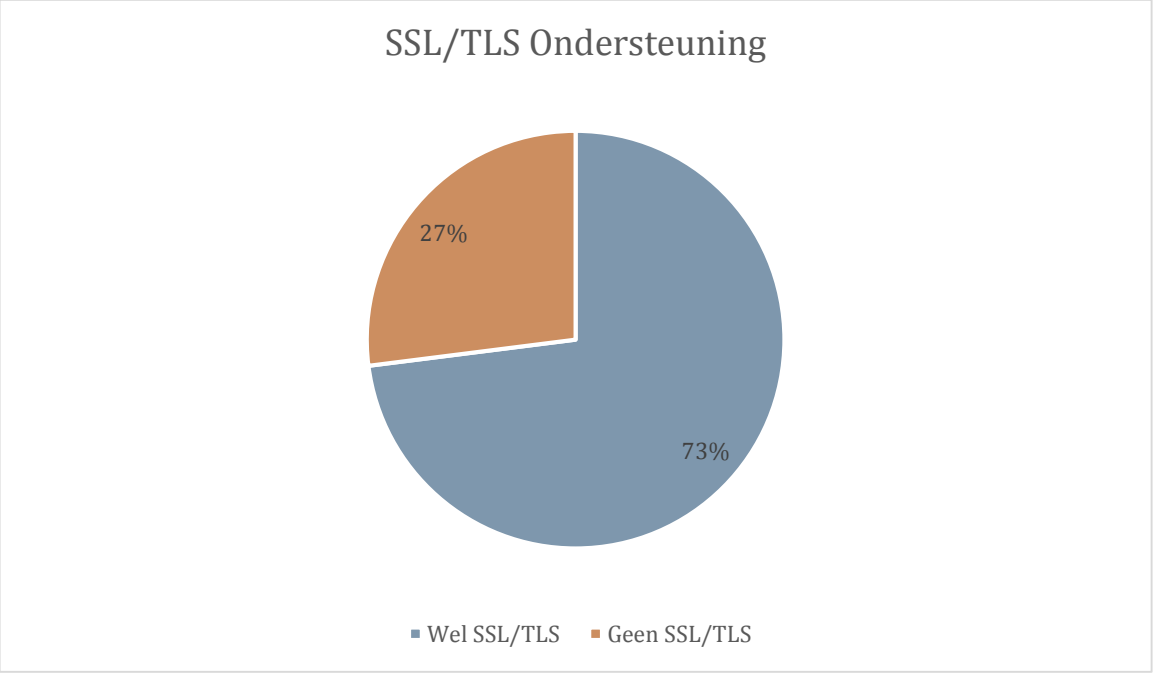
Om systeembeheerders, beveiligings- en andere IT professionals tegemoet te komen heeft LeakFree een gratis te downloaden *'TLS best practices'* whitepaper ter beschikking gesteld [8]. Het goed, efficient en veilig opzetten van TLS configuraties vereist specialistische kennis en is vaak maatwerk. Contact met een security professional wordt dan ook aangeraden om de veiligheid van uw communicatie en computersystemen te waarborgen.

APPENDIX: TOP 200 MEEST POPULAIRE .NL WEBSITES

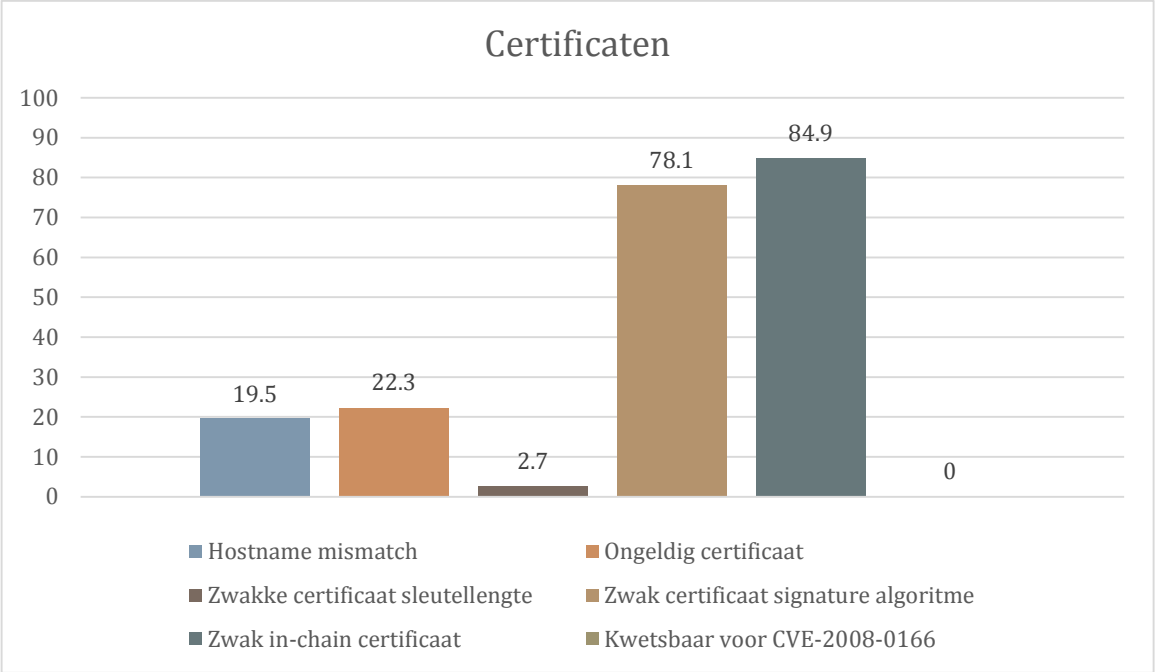
Statistieken voor TLS test over de "*top 200 meest populaire .nl TLD websites*" test-set. Alle statistieken zijn afgerond op een decimaal. De in staafdiagram weergegeven statistieken hebben betrekking op het deel van de geteste servers dat TLS ondersteuning bood en zijn uitgedrukt in procenten.

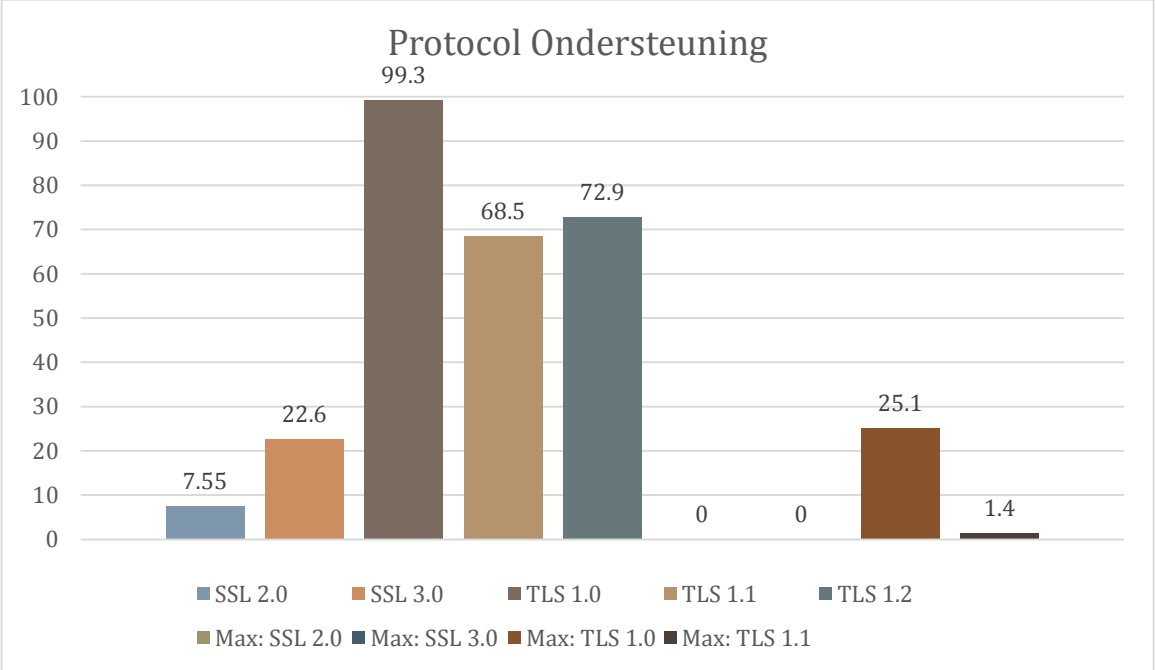
Gegevens:

- Meest voorkomende certificaat signature algoritme: sha1WithRSAEncryption
- Meest voorkomende certificaat sleutellengte: 2048-bits
- Meest gedeelde *in-chain* certificaat common name: RapidSSL CA (gedeeld door 6.16%)
- Kleinste geobserveerde sleutellengte voor bulkversleuteling: 40-bits
- Grootste geobserveerde sleutellengte voor bulkversleuteling: 256-bits
- Kleinste geobserveerde maximum sleutellengte voor bulkversleuteling: 128-bits

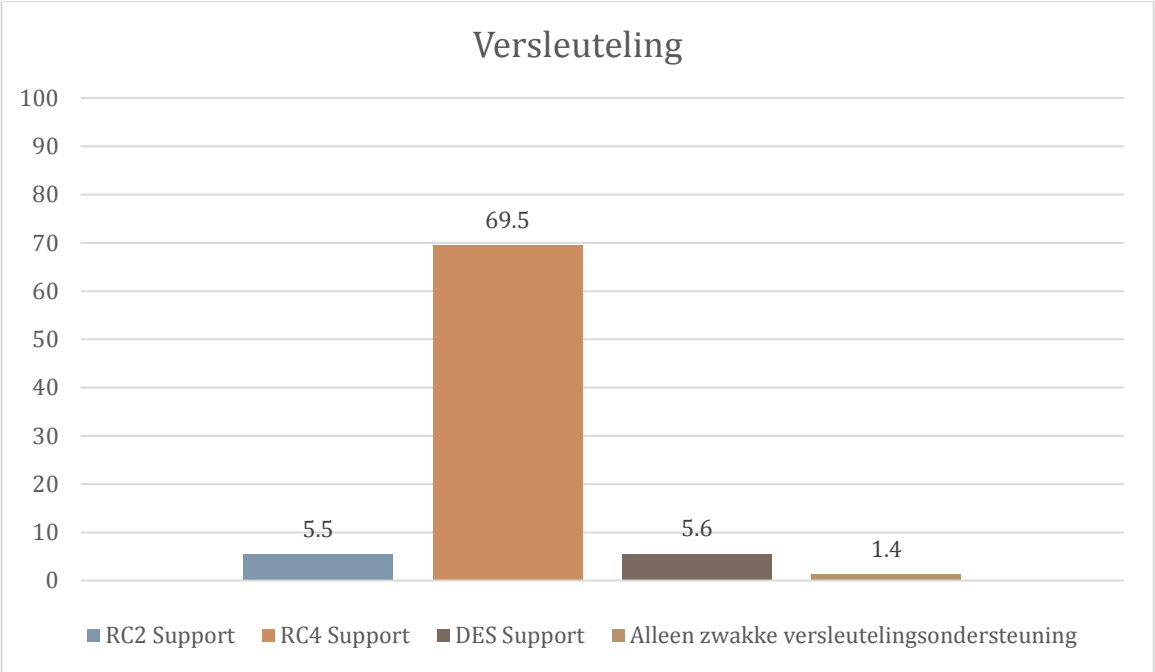


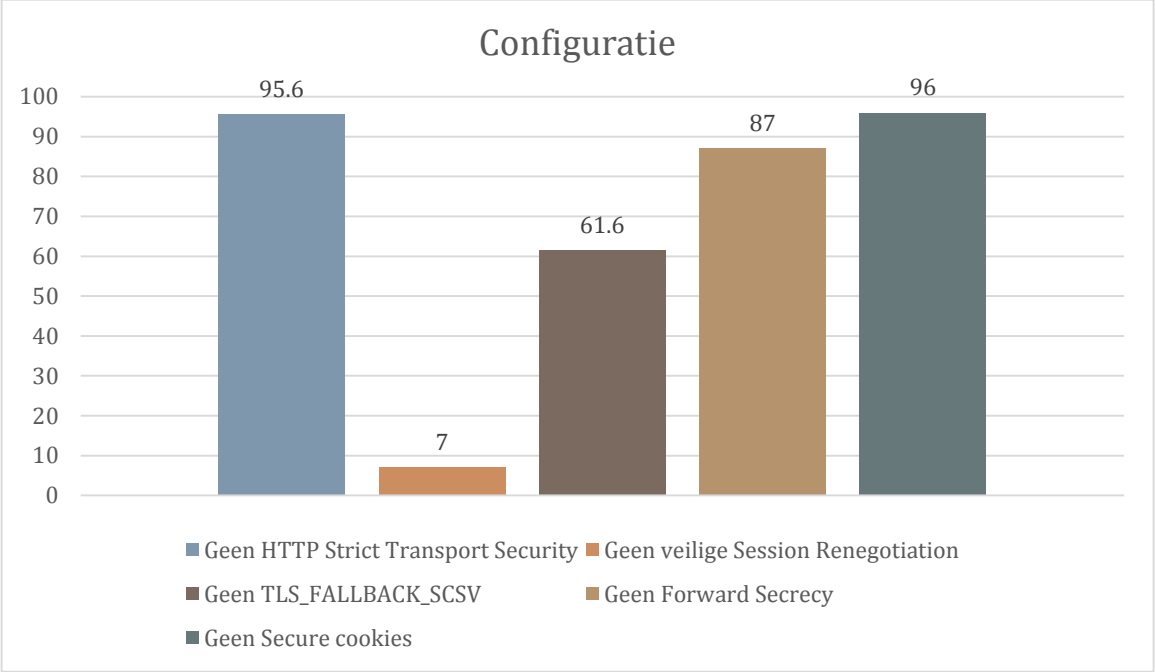
APPENDIX: TOP 200 MEEST POPULAIRE .NL WEBSITES



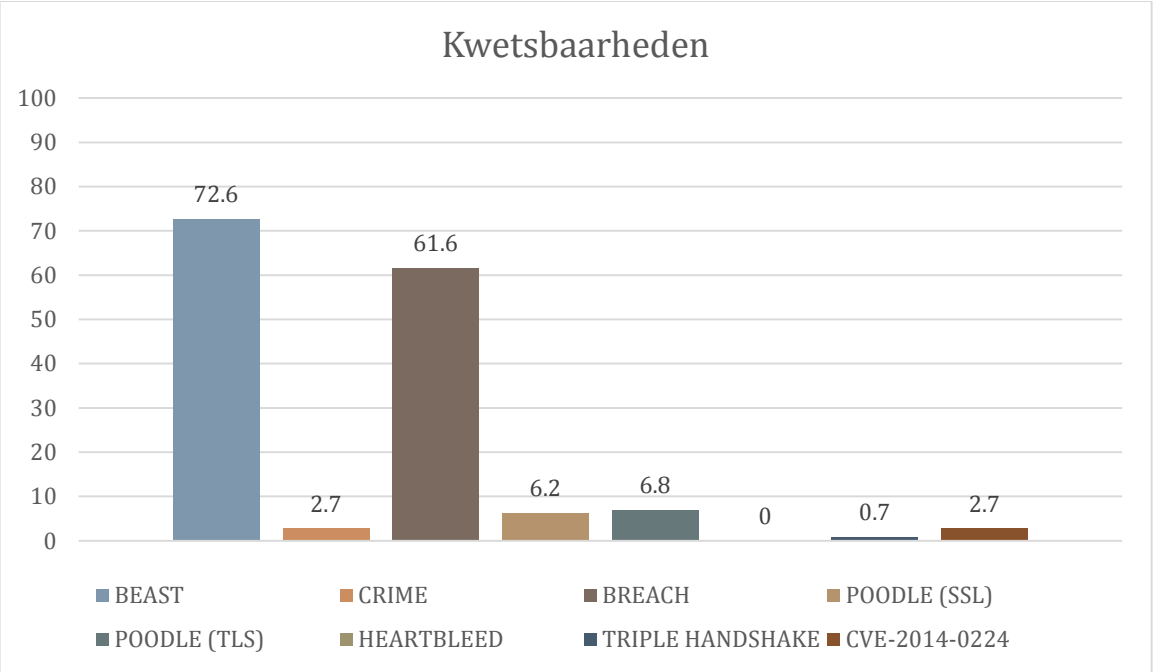


APPENDIX: TOP 200 MEEST POPULAIRE .NL WEBSITES





APPENDIX: TOP 200 MEEST POPULAIRE .NL WEBSITES

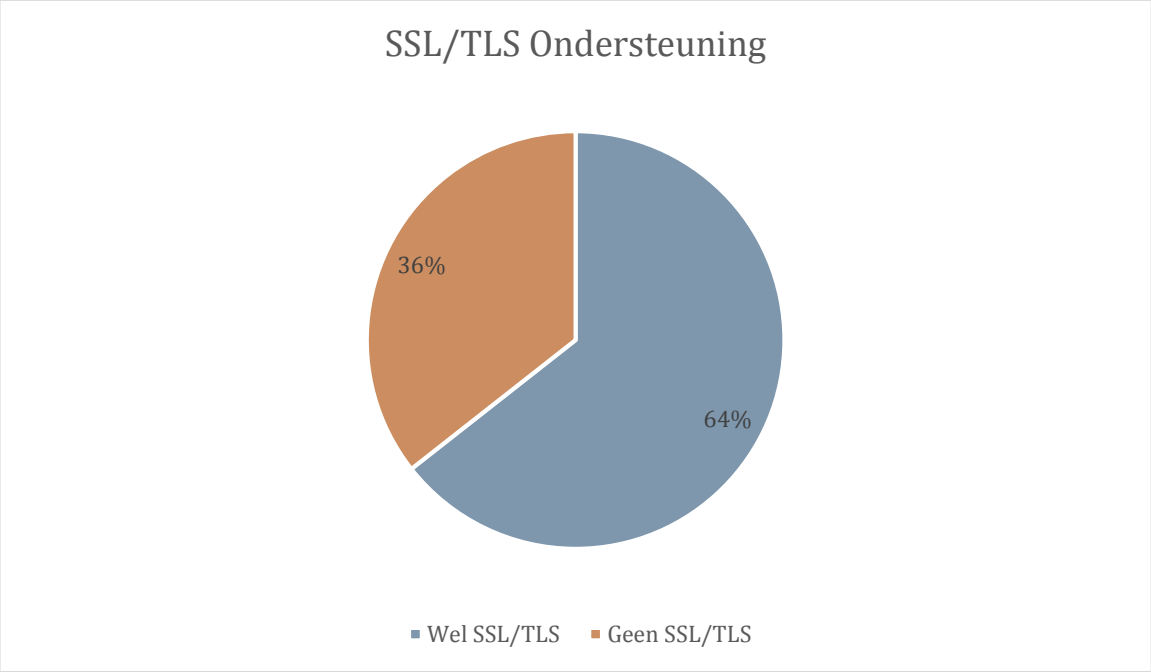


APPENDIX: 55 PROMINENTE OVERHEIDSWEBSITES

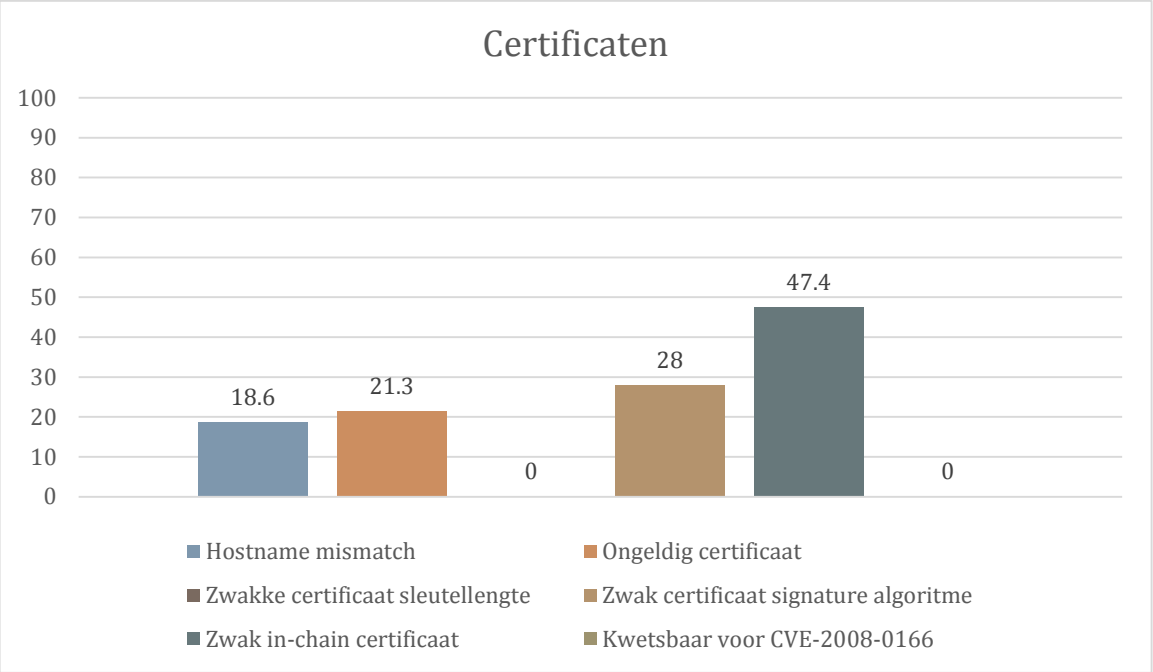
Statistieken voor TLS test over de *"55 prominente overheidswebsites"* test-set. Alle statistieken zijn afgerond op een decimaal. De in staafdiagram weergegeven statistieken hebben betrekking op het deel van de geteste servers dat TLS ondersteuning bood en zijn uitgedrukt in procenten.

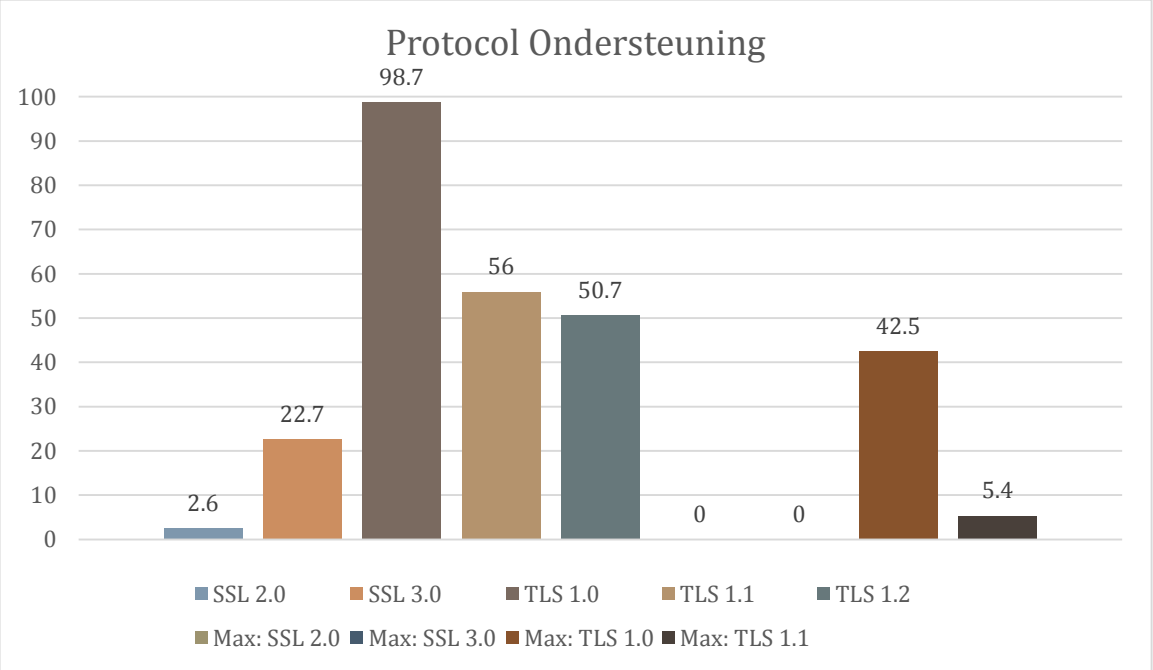
Gegevens:

- Meest voorkomende certificaat signature algoritme: sha256WithRSAEncryption
- Meest voorkomende certificaat sleutellengte: 2048-bits
- Meest gedeelde *in-chain* certificaat common name: Staat der Nederlanden Organisatie CA - G2 (gedeeld door 15.78%)
- Kleinste geobserveerde sleutellengte voor bulkversleuteling: 40-bits
- Grootste geobserveerde sleutellengte voor bulkversleuteling: 256-bits
- Kleinste geobserveerde maximum sleutellengte voor bulkversleuteling: 128-bits

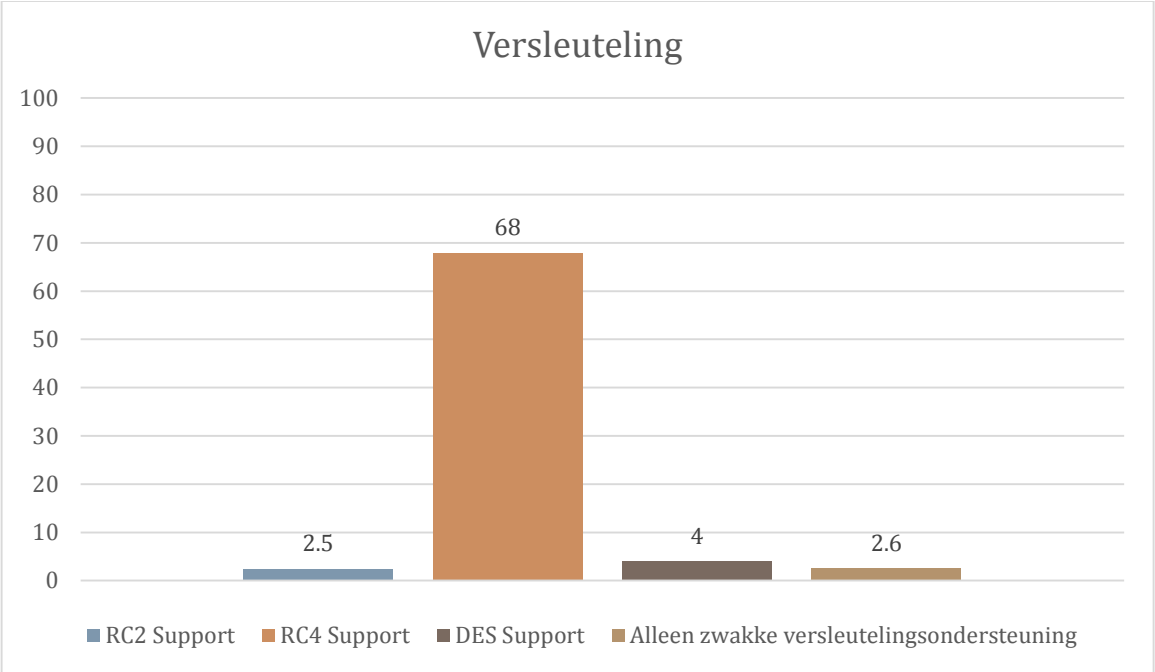


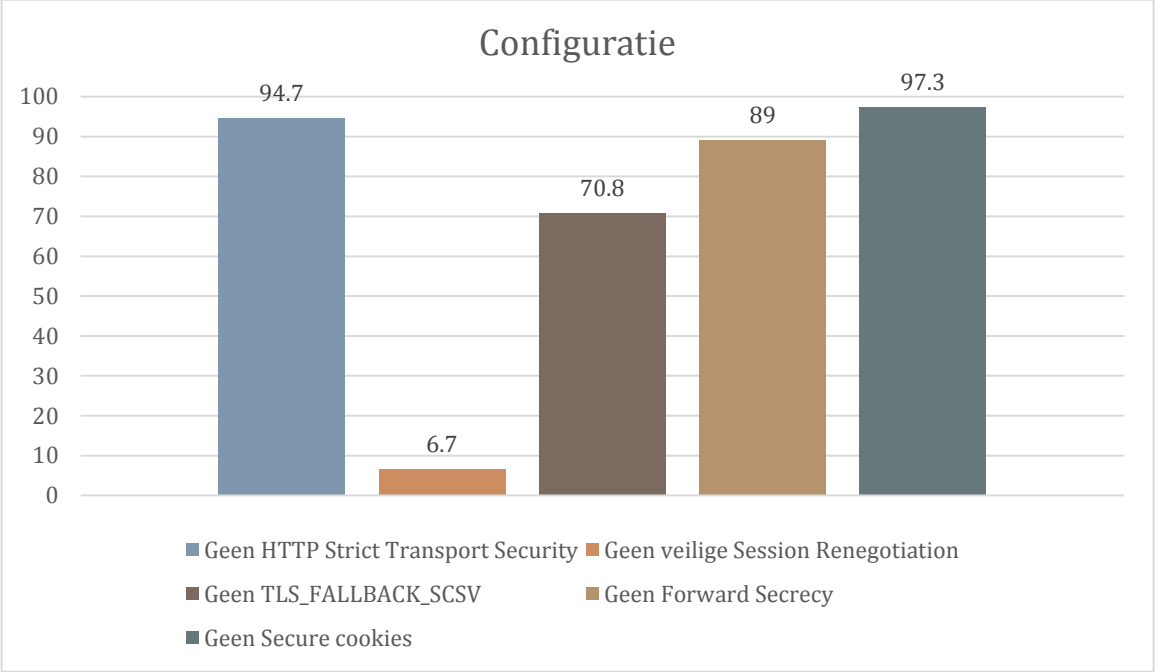
APPENDIX: 55 PROMINENTE OVERHEIDSWEBSITES



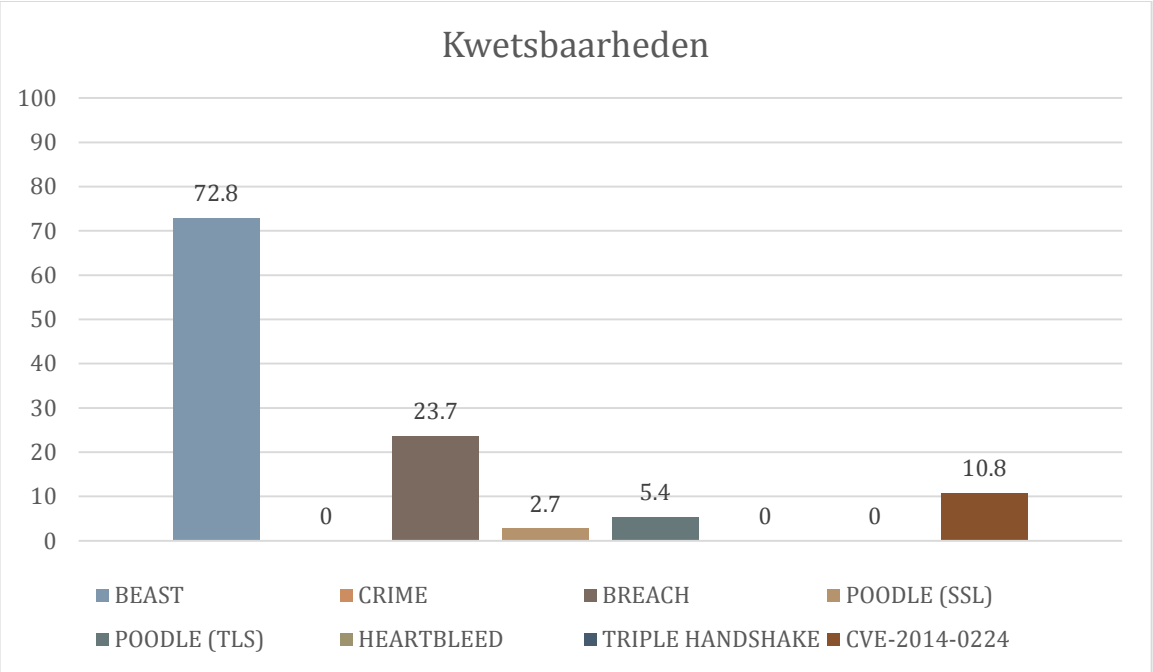


APPENDIX: 55 PROMINENTE OVERHEIDSWEBSITES





APPENDIX: 55 PROMINENTE OVERHEIDSWEBSITES

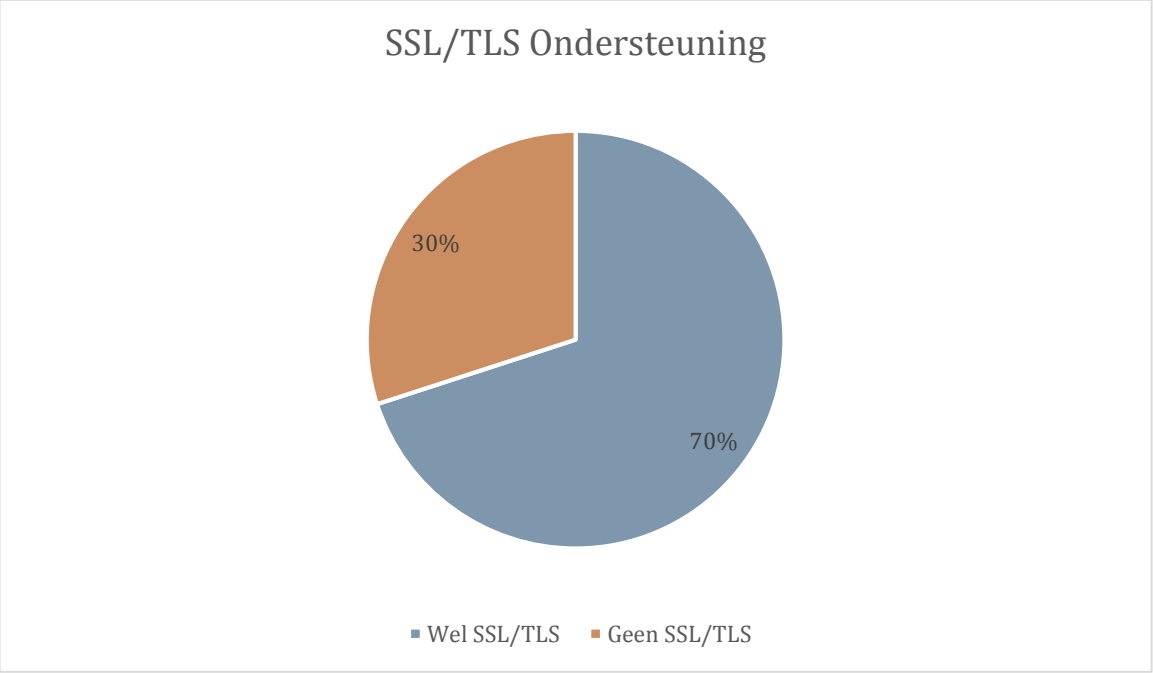


APPENDIX: TOP 50 GROOTSTE GEMEENTEN

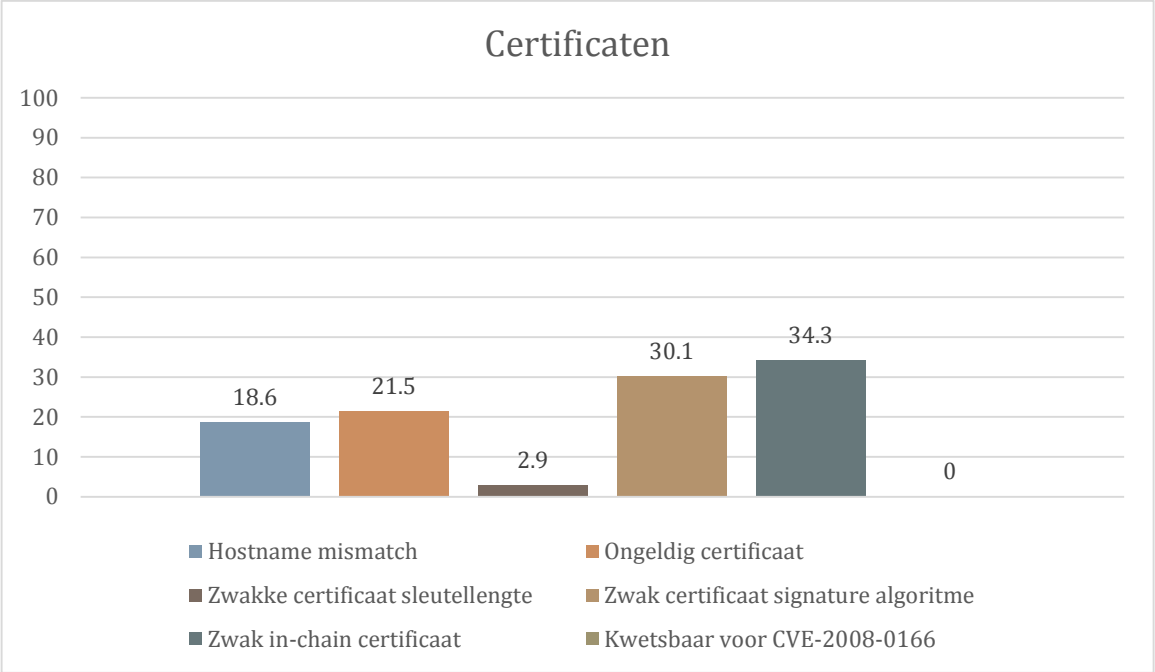
Statistieken voor TLS test over de "*top 50 grootste Nederlandse gemeenten*" test-set. Alle statistieken zijn afgerond op een decimaal. De in staafdiagram weergegeven statistieken hebben betrekking op het deel van de geteste servers dat TLS ondersteuning bood en zijn uitgedrukt in procenten.

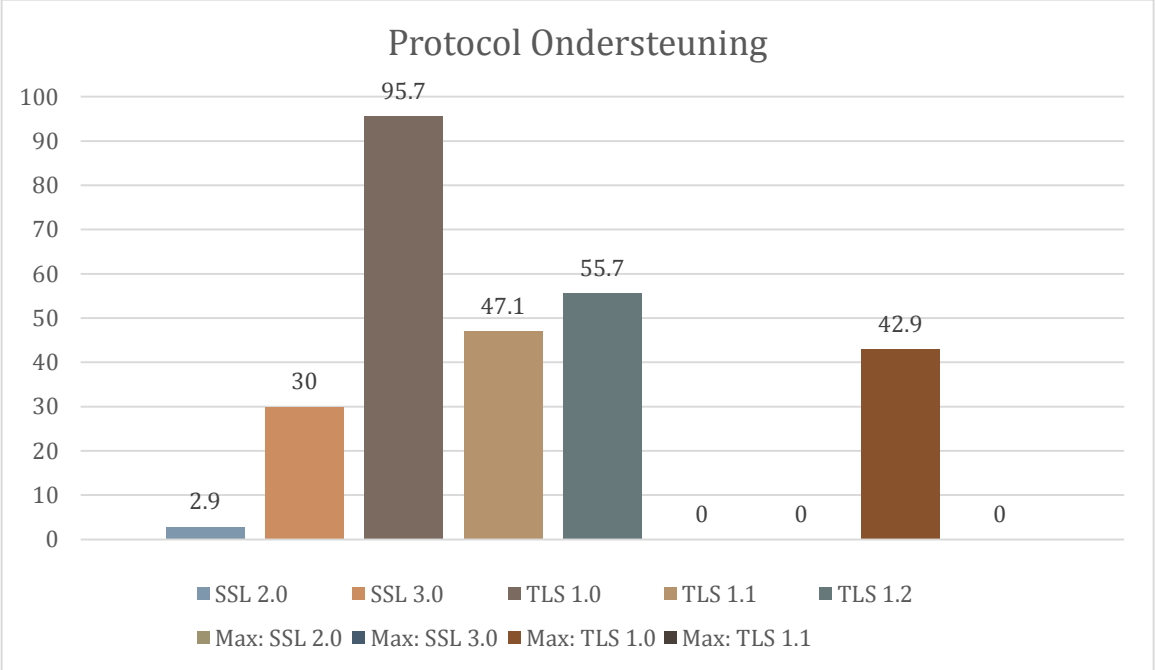
Gegevens:

- Meest voorkomende certificaat signature algoritme: sha256WithRSAEncryption
- Meest voorkomende certificaat sleutellengte: 2048-bits
- Meest gedeelde *in-chain* certificaat common name: KPN Corporate Market CSP Organisatie CA - G2 (gedeeld door 37.14%)
- Kleinste geobserveerde sleutellengte voor bulkversleuteling: 40-bits
- Grootste geobserveerde sleutellengte voor bulkversleuteling: 256-bits
- Kleinste geobserveerde maximum sleutellengte voor bulkversleuteling: 128-bits

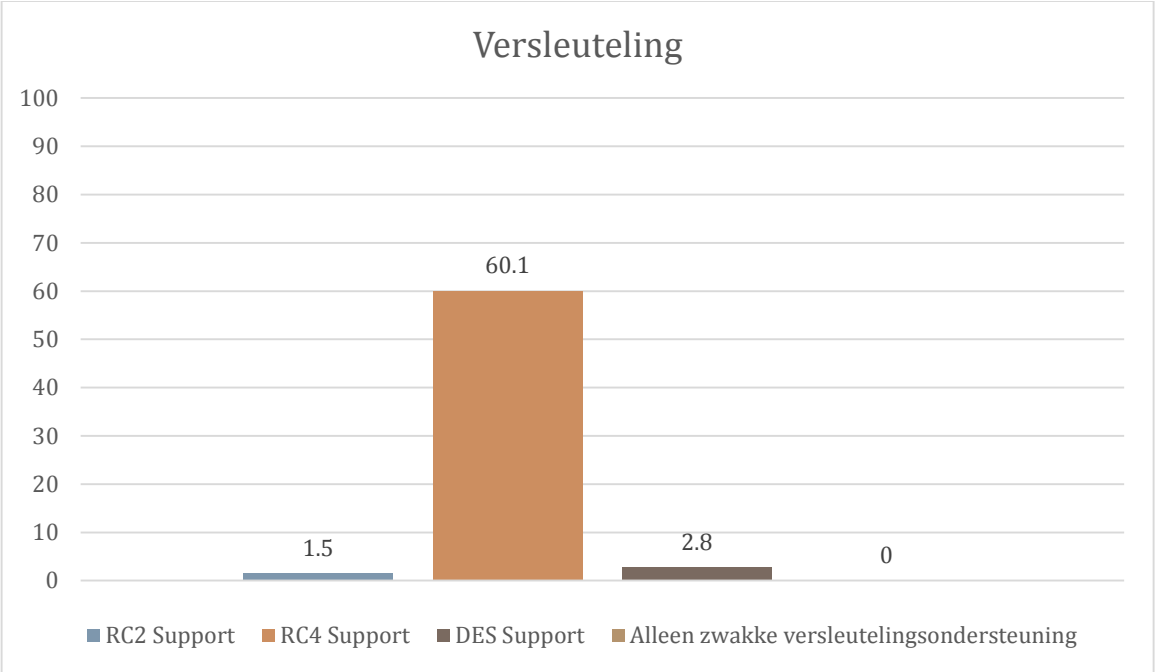


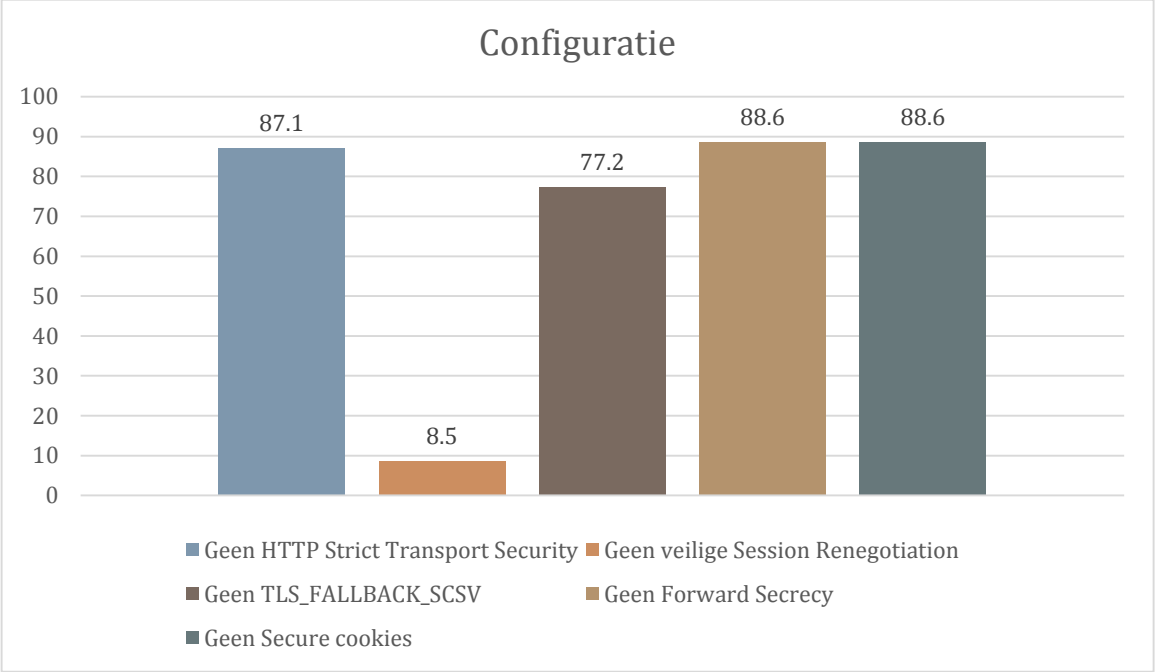
APPENDIX: TOP 50 GROOTSTE GEMEENTEN



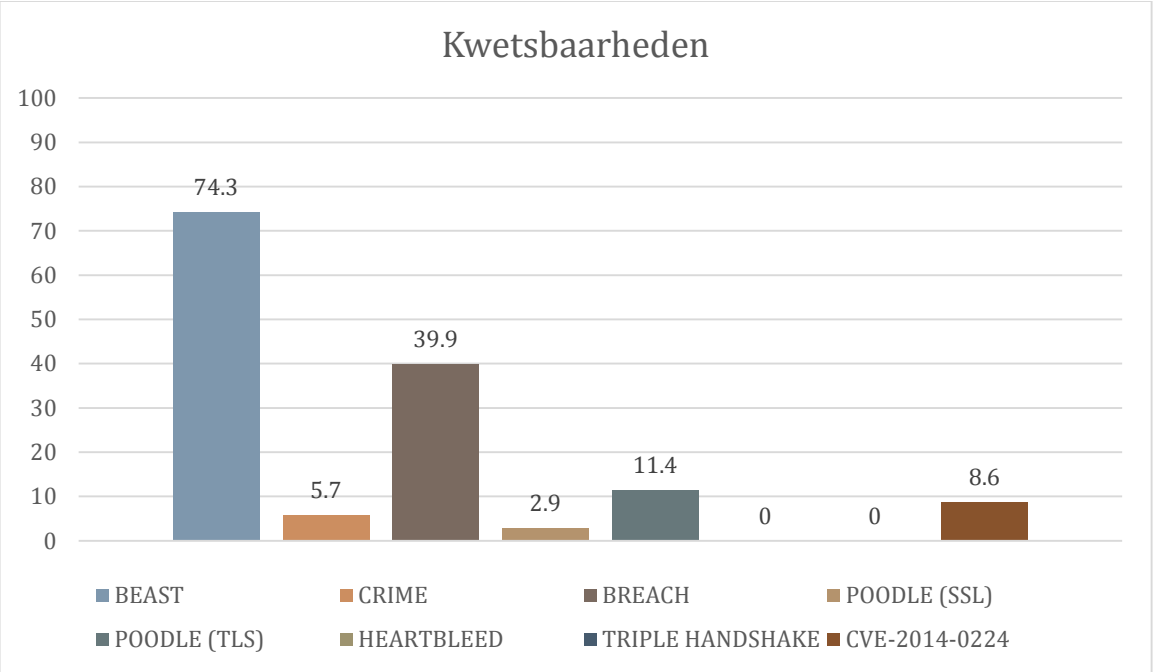


APPENDIX: TOP 50 GROOTSTE GEMEENTEN





APPENDIX: TOP 50 GROOTSTE GEMEENTEN

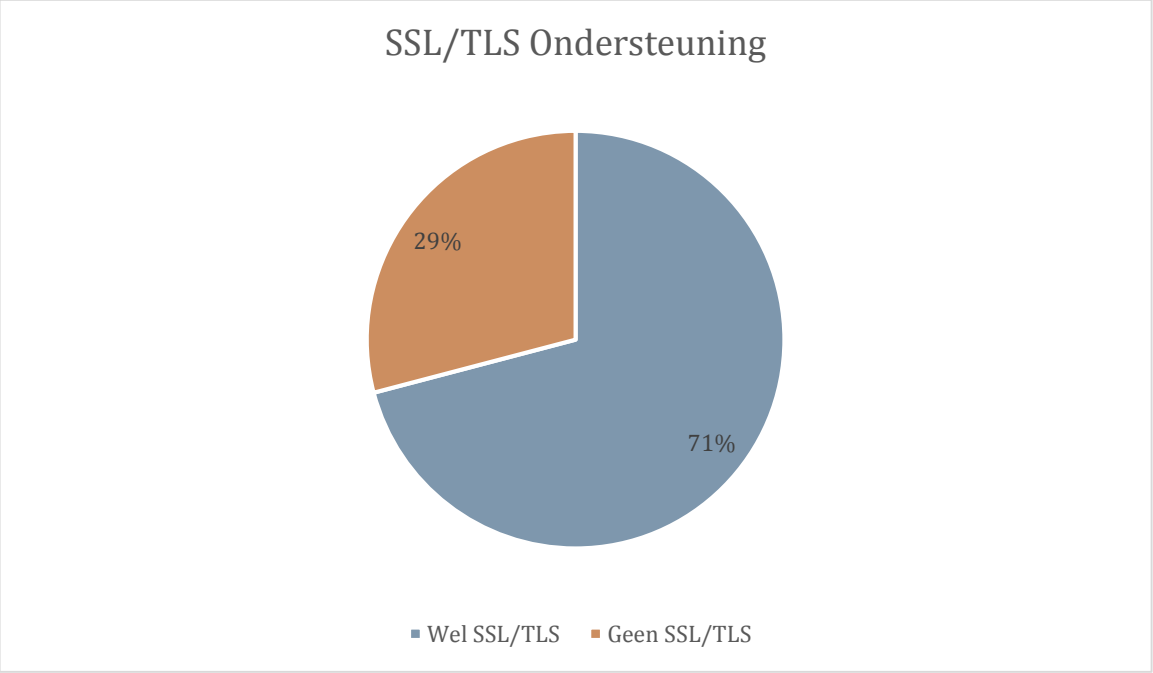


APPENDIX: 55 PROMINENTE NEDERLANDSE BEDRIJVEN

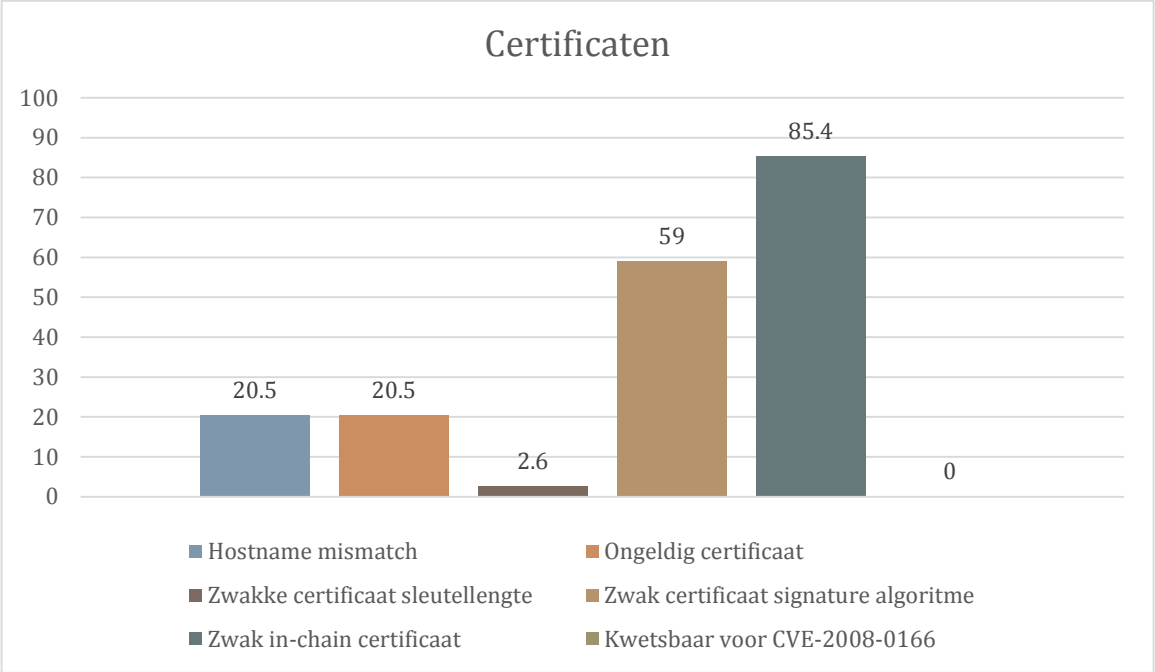
Statistieken voor TLS test over de "*websites van 55 Nederlandse multinationals en andere prominente bedrijven*" test-set. Alle statistieken zijn afgerond op een decimaal. De in staafdiagram weergegeven statistieken hebben betrekking op het deel van de geteste servers dat TLS ondersteuning bood en zijn uitgedrukt in procenten.

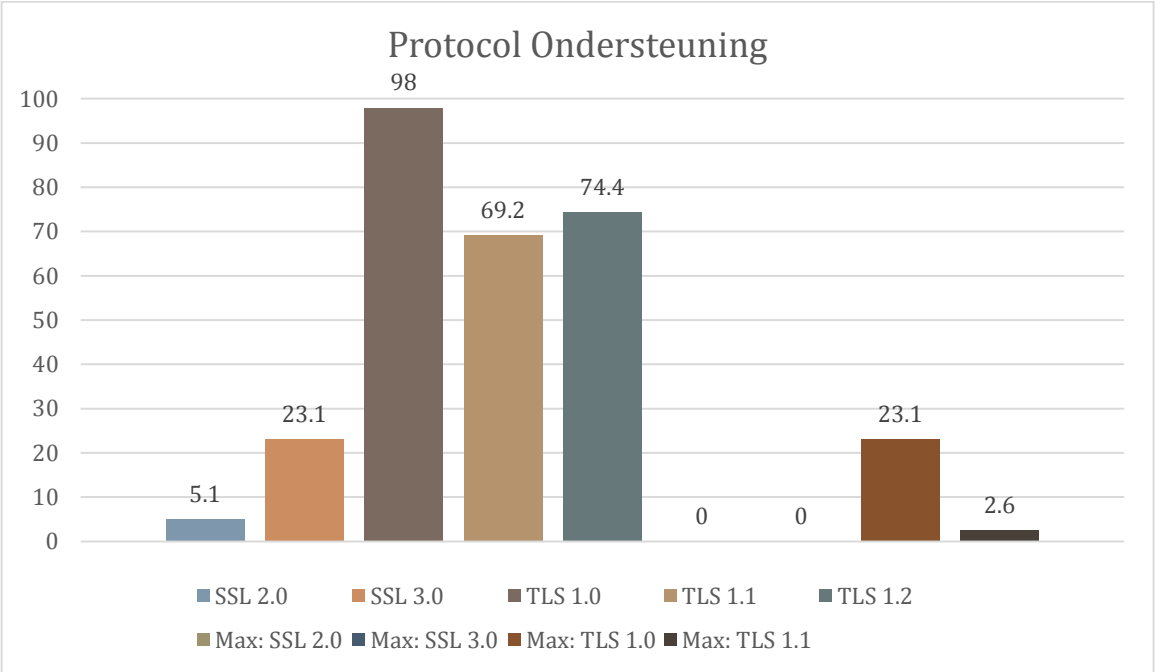
Gegevens:

- Meest voorkomende certificaat signature algoritme: sha1WithRSAEncryption
- Meest voorkomende certificaat sleutellengte: 2048-bits
- Meest gedeelde *in-chain* certificaat common name: Symantec Class 3 EV SSL CA - G3 (gedeeld door 9.75%)
- Kleinste geobserveerde sleutellengte voor bulkversleuteling: 40-bits
- Grootste geobserveerde sleutellengte voor bulkversleuteling: 256-bits
- Kleinste geobserveerde maximum sleutellengte voor bulkversleuteling: 128-bits

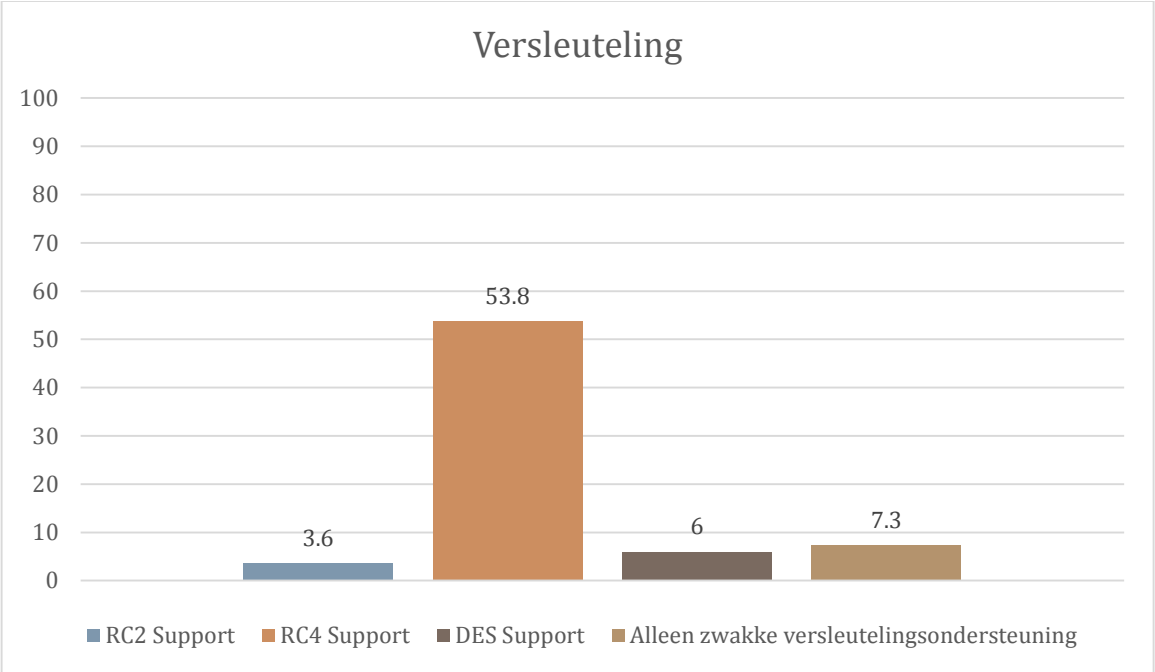


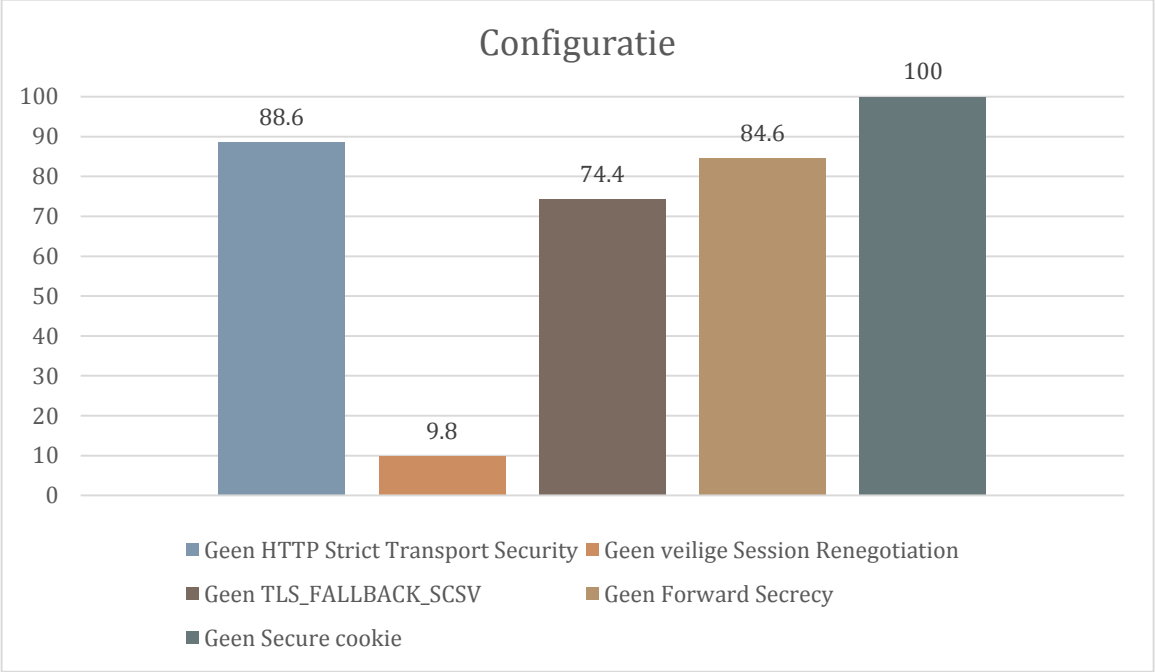
APPENDIX: 55 PROMINENTE NEDERLANDSE BEDRIJVEN



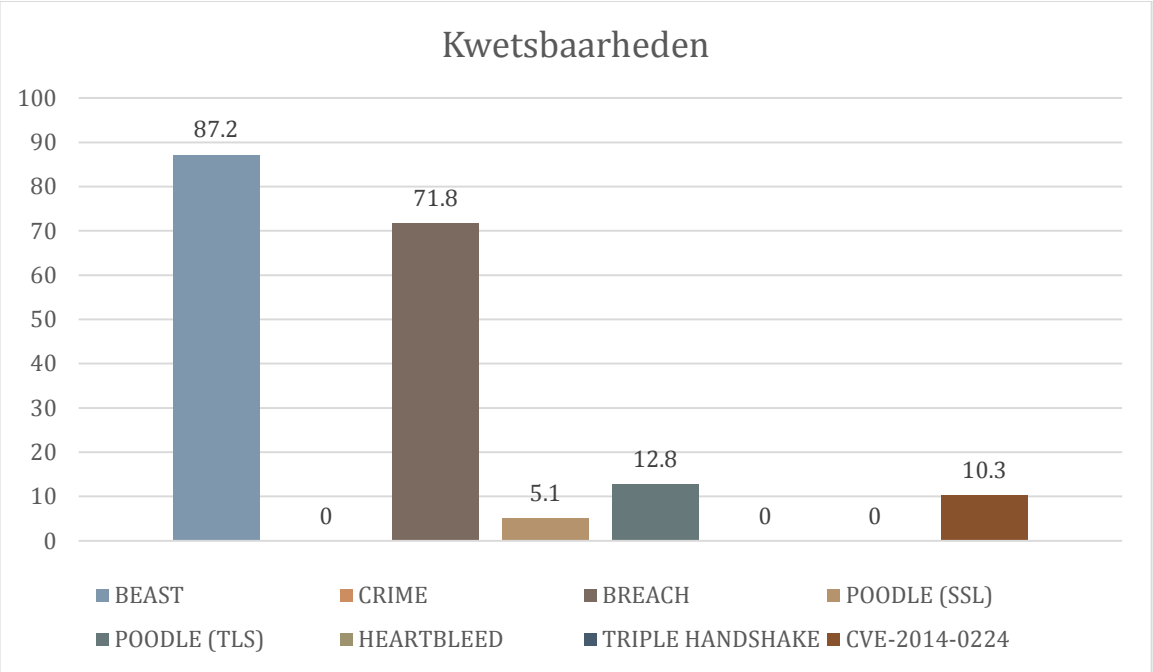


APPENDIX: 55 PROMINENTE NEDERLANDSE BEDRIJVEN





APPENDIX: 55 PROMINENTE NEDERLANDSE BEDRIJVEN



APPENDIX: REFERENTIES

Referenties

1. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
2. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
3. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0224
4. http://nl.wikipedia.org/wiki/Hack_bij_DigiNotar
5. http://hackmageddon.com/2011/12/10/another-certification-authority-breached-the-12th/
6. http://www.cbc.ca/news/business/heartbleed-bug-rcmp-asked-revenue-canada-to-delay-news-of-sin-thefts-1.2609192
7. http://www.reuters.com/article/2014/08/20/us-community-health-cybersecurity-idUSKBN0GK0H420140820
8. https://www.leakfree.nl/files/leakfree_ssl_tls_whitepaper.pdf
9. https://github.com/nabla-c0d3/sslyze
10. https://www.ssllabs.com/ssltest/

APPENDIX: DOCUMENTSGESCHIEDENIS

VERSIE 1.0

Wijziging	Datum	Auteur
Publicatie 1e versie	29-01-2015	Jos Wetzels

Over LEAKFREE

LeakFree is een jong IT-security consultancy bedrijf. Wij verzorgen onder andere beveiligingstesten en brengen whitepapers en beveiligingsadviezen uit. Hiermee helpen wij onze opdrachtgevers risico's en potentiële bedreigingen voor hun digitale infrastructuur en gevoelige informatie te identificeren, zodat pro-actieve maatregelen genomen kunnen worden om toekomstige schade te voorkomen.

Onze medewerkers hebben jaren ervaring in de IT-security en verzorgden beveiligingstesten in diverse sectoren, van hostingbedrijven tot grote Nederlandse banken. Door haar kleinschalige en flexibele organisatie is LeakFree in staat kwalitatief goed en scherp geprijsd maatwerk te leveren in nauw overleg met haar opdrachtgevers.

CONTACT

E-mail contact@leakfree.nl
http://www.leakfree.nl