GUARDIAN 360°

QUICKSCAN BENCHMARK

Benchmark-Bericht Web-Sicherheit

Niederlande · Belgien · Deutschland · Frankreich · weitere Länder

Ausgabe August 2026

Basierend auf 12.914 gescannten Domains

Inhaltsverzeichnis

1. Management-Zusammenfassung

Dieser Benchmark-Bericht erfasst das Sicherheitsniveau öffentlicher Websites auf Basis des Guardian360 Quickscan. Für diese Ausgabe wurden 12.914 Domains erfolgreich gescannt. Der Quickscan bewertet unter anderem das Vorhandensein wesentlicher Sicherheits-Header, häufige Fehlkonfigurationen, die Content Security Policy, die SPF-Einstellung im DNS und die Qualität der SSL/TLS-Konfiguration. Jede Domain erhält einen Wert von 0 bis 100.

Der Durchschnittswert über alle Domains liegt bei 68,6 Punkten, auf einer Skala mit maximal 100 Punkten. Das deutet auf ein solides Grundniveau hin, zugleich aber auf strukturelle Rückstände bei einigen wichtigen Sicherheitsmaßnahmen. Vor allem moderne, präventive Maßnahmen wie eine Content Security Policy und strenge SSL/TLS-Konfigurationen bleiben massiv zurück.

Zwischen den vier Kernmärkten von Guardian360 zeigen sich deutliche Unterschiede. **Belgien** schneidet mit einem Durchschnitt von 72,7 am besten ab und weist bei nahezu allen Themen die wenigsten Schwachstellen auf. **Die Niederlande** und **Deutschland** liegen mit 68,9 bzw. 68,4 nahe am Durchschnitt. **Frankreich** bleibt mit 64,3 zurück und weist bei den meisten Headern die höchsten Schwachstellenquoten auf.

Die wichtigsten Ergebnisse im Überblick:

- Fehlende Sicherheits-Header sind eher die Regel als die Ausnahme. Bei rund 60% aller Domains fehlt ein X-Frame-Options-Header und bei etwa der Hälfte eine korrekte HSTS-Einstellung.
- Eine Content Security Policy fehlt bei 73,2% der Domains. Das ist der häufigste Mangel über alle Länder hinweg.
- Drei Viertel der Domains (75,6%) weisen mindestens eine Schwachstelle in der SSL/TLS-Konfiguration auf, etwa veraltete Protokolle oder schwache Cipher.
- Basismaßnahmen sind hingegen breit in Ordnung. Schwerwiegende Fehlkonfigurationen wie eine offengelegte PHPinfo-Seite (1,6%) oder eine aktive HTTP-TRACE-Methode (0,9%) kommen selten vor.

Die Botschaft ist eindeutig. Die meisten Organisationen haben die Grundlagen im Griff, lassen aber leicht umsetzbare und hochwertige Sicherheitsgewinne bei Headern, CSP und TLS-Härtung liegen. Genau dort bietet der Quickscan einen konkreten und messbaren Ausgangspunkt für Verbesserungen.

2. Über diesen Benchmark

2.1 Ziel

Mit dem Quickscan führt Guardian360 einen automatisierten, nicht-intrusiven Sicherheitsscan der öffentlich zugänglichen Seite einer Website durch. Dieser Benchmark fasst die Ergebnisse einer großen Zahl von Scans zu einem Marktbild zusammen. Ziel ist es, Distributoren, Partnern und Kunden Einblick zu geben, wie das Sicherheitsniveau einer einzelnen Domain im Vergleich zum breiteren Markt und zu vergleichbaren Organisationen in anderen Ländern steht.

Möchten Sie wissen, wie Ihre eigene Domain abschneidet? Sie können kostenlos einen Quickscan durchführen unter **guardian360.de/quickscan**.

2.2 Datengrundlage

Der Benchmark basiert auf 12.914 Domains, die in diesem Messzeitraum erfolgreich gescannt wurden. Alle Domains fließen in den Gesamt-Benchmark ein. Für den Ländervergleich heben wir die vier Kernmärkte von Guardian360 hervor. Die Zuordnung zu einem Land erfolgt anhand der Länderkennung in der Top-Level-Domain.

Segment	Anzahl Domains	Ø-Wert	Median
Niederlande (.nl)	4.278	68,9	65
Belgien (.be)	609	72,7	75
Deutschland (.de)	2.887	68,4	65
Frankreich (.fr)	215	64,3	65
Sonstige Domain-Endungen	4.925	68,3	65
Alle Länder (gesamt)	**12.914**	**68,6**	**65**

Tabelle 1. Umfang und Durchschnittswert je Segment.

Die Zeile „Sonstige Domain-Endungen“ enthält die 4.925 Domains mit einer anderen oder generischen Endung wie .com, .eu, .ch und .net. Diese Domains fließen in den Gesamt-Benchmark ein, bilden aber kein eigenes hervorgehobenes Land, da die Endung kein verlässlicher Hinweis auf das Herkunftsland ist. Gemeinsam sorgen sie dafür, dass der Gesamt-Benchmark ein breites Marktbild abbildet.

2.3 Was der Quickscan misst

Der Quickscan bewertet mehrere Kategorien, die zusammen ein gutes Bild der Sicherheitshygiene einer Website ergeben:

- Sicherheits-Header: HTTP Strict Transport Security (HSTS), X-Content-Type-Options und X-Frame-Options.
- Content Security Policy (CSP): das Vorhandensein einer Richtlinie, die das Laden unerwünschter Inhalte verhindert.
- Fehlkonfigurationen: unter anderem das Fehlen einer HTTPS-Weiterleitung, das Preisgeben von Technik über die X-Powered-By- und Server-Header, eine offengelegte PHPinfo-Seite und eine aktive HTTP-TRACE-Methode.
- DNS: das Vorhandensein und die Korrektheit eines SPF-Records zur Verhinderung von E-Mail-Spoofing.
- SSL/TLS: die Verwendung veralteter Protokolle, schwacher Cipher und bekannter Schwachstellen in der verschlüsselten Verbindung.

3. Allgemeines Sicherheitsniveau

Der durchschnittliche Quickscan-Wert über alle 12.914 Domains beträgt 68,6 Punkte, bei einem Median von 65. Das bedeutet, dass eine typische Domain die wichtigsten Grundanforderungen erfüllt, aber an mehreren Stellen Verbesserungspotenzial lässt.

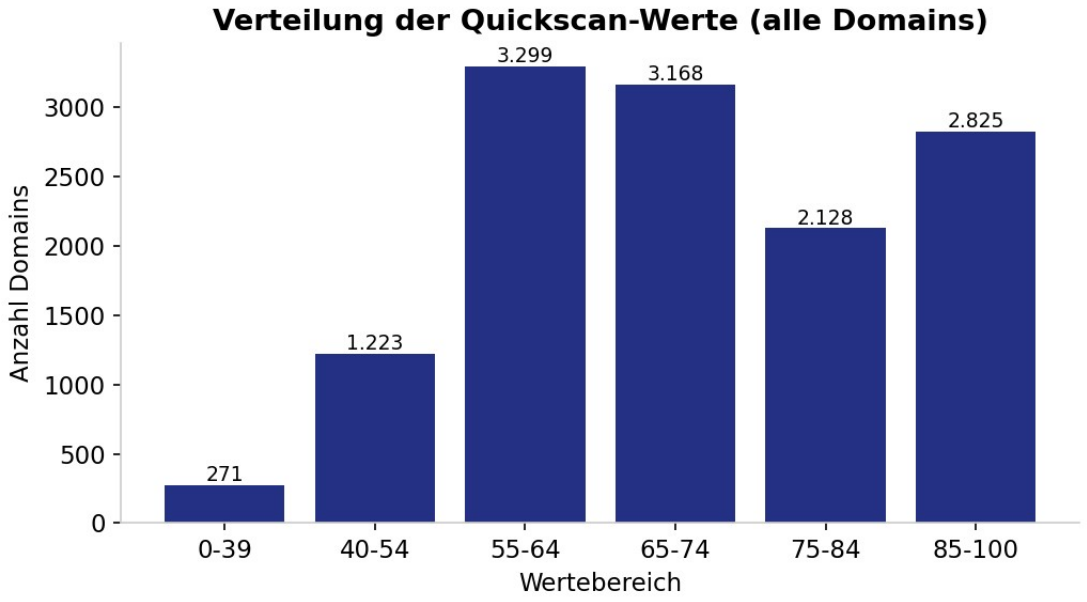

Abbildung 1. Verteilung der Quickscan-Werte über alle Domains.

Die Verteilung zeigt, dass der Schwerpunkt im mittleren Bereich liegt. Die größten Gruppen von Domains erreichen zwischen 55 und 74 Punkten. Am oberen Ende erreicht eine beträchtliche Gruppe von 2.825 Domains einen Wert von 85 oder höher, was zeigt, dass ein hohes Sicherheitsniveau gut erreichbar ist. Am unteren Ende erzielt eine kleinere, aber relevante Gruppe von 271 Domains weniger als 40 Punkte. Diese Domains weisen meist eine Häufung von Mängeln auf und sollten priorisiert werden.

4. Vergleich zwischen den Ländern

Obwohl die Länder im Durchschnittswert nahe beieinander liegen, gibt es bei einzelnen Aspekten deutliche Unterschiede. Die folgende Abbildung zeigt den Durchschnittswert je Land im Vergleich zum Gesamt-Benchmark.

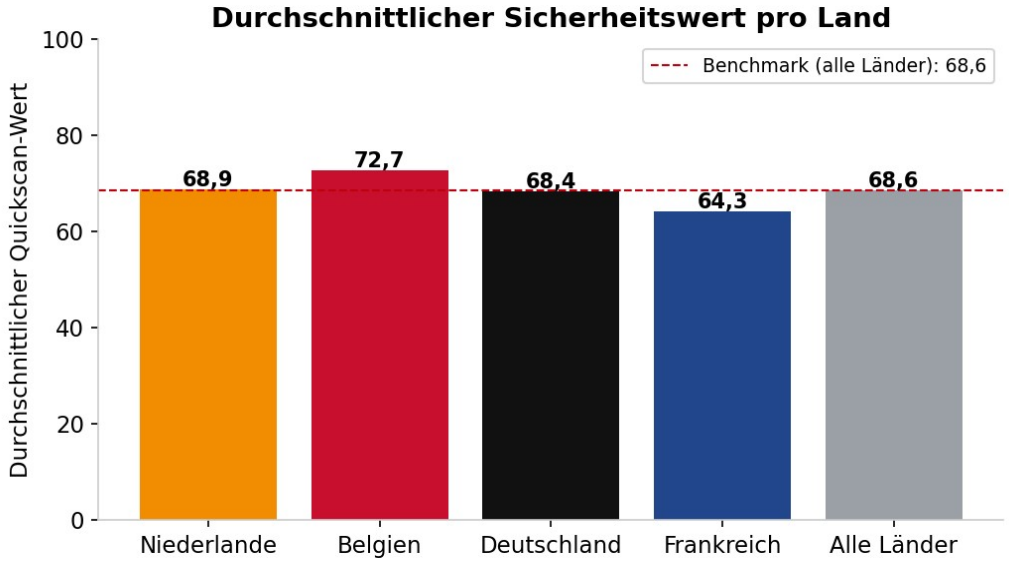

Abbildung 2. Durchschnittlicher Sicherheitswert je Land im Vergleich zum Benchmark.

Belgien sticht positiv hervor. Sowohl der Durchschnittswert von 72,7 als auch der Median von 75 liegen deutlich über dem Benchmark. Die Niederlande und Deutschland folgen dem Durchschnitt nahezu exakt. Frankreich liegt mit 64,3 am weitesten zurück, wobei die französische Stichprobe mit 215 Domains kleiner und damit anfälliger für Ausreißer ist.

Die nächste Abbildung veranschaulicht die Unterschiede je Thema. Dargestellt ist der Anteil der Domains je Land, bei denen die betreffende Schwachstelle gefunden wurde. Ein niedrigerer Wert ist besser.

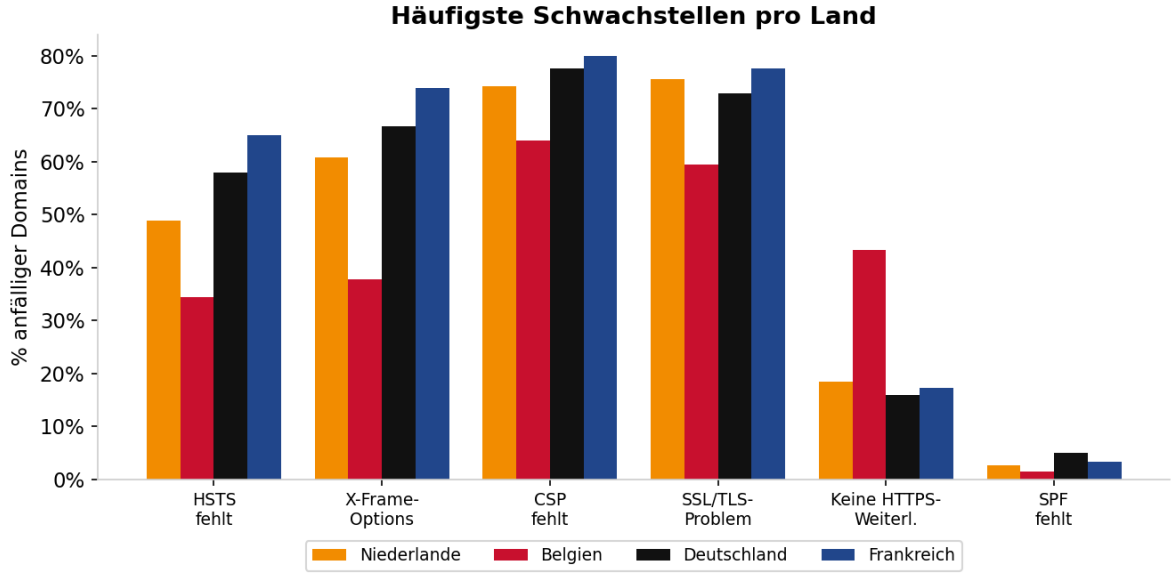

Abbildung 3. Anteil anfälliger Domains je Land für die wichtigsten Themen.

Das Bild bestätigt die starke Position Belgiens bei Sicherheits-Headern und bei SSL/TLS. Auffällig ist, dass Belgien bei der HTTPS-Weiterleitung schwächer abschneidet: 43,3% der belgischen Domains leiten Besucher nicht automatisch auf eine verschlüsselte Verbindung. Frankreich weist die höchsten Anteile fehlender Header auf, während Deutschland relativ häufig Technikinformationen über den Server-Header preisgibt und am häufigsten einen fehlenden oder schwachen SPF-Record hat.

5. Ergebnisse nach Thema

Die folgende Tabelle zeigt die vollständige Aufschlüsselung der Schwachstellenquoten je Thema und je Land. Alle Prozentwerte geben den Anteil der Domains an, bei denen der Mangel gefunden wurde. Für jedes Thema gilt: ein niedrigerer Wert ist besser.

Thema	NL	BE	DE	FR	Gesamt
HSTS fehlt oder schwach	48,9%	34,5%	57,9%	65,1%	49,9%
X-Content-Type-Options fehlt	54,1%	33,5%	57,6%	67,9%	53,7%
X-Frame-Options fehlt	60,9%	37,8%	66,7%	74,0%	60,4%
Content-Security-Policy fehlt	74,3%	64,0%	77,7%	80,0%	73,2%
Keine HTTPS-Weiterleitung	18,4%	43,3%	16,0%	17,2%	19,7%
X-Powered-By verrät Technik	31,9%	9,7%	23,5%	35,3%	25,5%
Server-Header verrät Version	3,2%	2,5%	9,4%	7,9%	5,4%
PHPinfo offengelegt	1,3%	0,2%	2,6%	1,4%	1,6%
HTTP TRACE aktiv	0,9%	0,5%	1,2%	1,9%	0,9%
SPF fehlt oder schwach	2,7%	1,5%	4,9%	3,3%	4,3%
SSL/TLS-Schwachstelle	75,7%	59,4%	72,9%	77,7%	75,6%

Tabelle 2. Anteil anfälliger Domains je Thema und je Land.

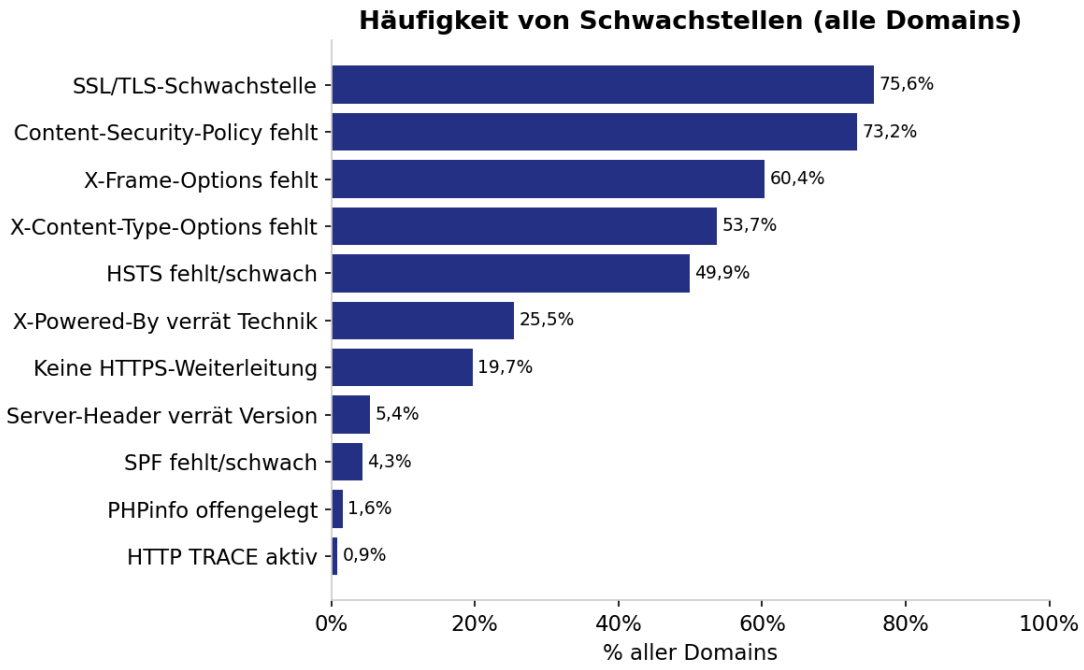

Abbildung 4. Häufigkeit von Schwachstellen über alle Domains, aufsteigend sortiert.

5.1 Sicherheits-Header

Sicherheits-Header sind eine günstige und wirksame Möglichkeit, einen großen Teil verbreiteter Angriffe abzuwehren. Dennoch fehlen sie vielfach. Bei 60,4% aller Domains fehlt ein X-Frame-Options-Header, wodurch die Website anfällig für Clickjacking ist. Bei etwa der Hälfte fehlt eine korrekte HSTS-Einstellung und bei 53,7% der X-Content-Type-Options-Header. Belgien schneidet bei allen drei Headern merklich besser ab, während Frankreich durchgehend die höchsten Anteile aufweist.

5.2 Content Security Policy

Die Content Security Policy ist der häufigste Mangel in diesem Benchmark. Bei 73,2% der Domains fehlt eine CSP vollständig. Eine gut eingerichtete CSP ist eine der stärksten Maßnahmen gegen Cross-Site-Scripting und das unerwünschte Einschleusen von Inhalten. Dass die Maßnahme so verbreitet fehlt, liegt daran, dass eine CSP sorgfältig auf die Website abgestimmt werden muss und daher oft aufgeschoben wird. Auch hier schneidet Belgien mit 64,0% am besten und Frankreich mit 80,0% am schlechtesten ab.

5.3 Fehlkonfigurationen

Die schwerwiegendsten Fehlkonfigurationen kommen glücklicherweise selten vor. Eine offengelegte PHPinfo-Seite wurde nur bei 1,6% der Domains gefunden und eine aktive HTTP-TRACE-Methode bei 0,9%. Das Preisgeben von Technikinformationen ist hartnäckiger. Bei 25,5% der Domains verrät der X-Powered-By-Header, welche Technologie verwendet wird, was Angreifern die gezielte Suche nach Schwachstellen erleichtert. Die HTTPS-Weiterleitung verdient in Belgien besondere Aufmerksamkeit, wo 43,3% der Domains diese Basismaßnahme vermissen lassen.

5.4 SPF und E-Mail-Sicherheit

Der SPF-Record verhindert, dass Angreifer einfach E-Mails im Namen einer Domain versenden. Über alle Domains fehlt ein korrekter SPF-Record bei 4,3%. Das ist relativ niedrig und zeigt, dass SPF inzwischen weit verbreitet ist. Deutschland schneidet hier mit 4,9% etwas schlechter ab.

5.5 SSL/TLS-Konfiguration

Die verschlüsselte Verbindung ist nahezu überall vorhanden, ihre Qualität lässt jedoch zu wünschen übrig. Bei 75,6% aller Domains wurde mindestens eine SSL/TLS-Schwachstelle gefunden, etwa die Unterstützung veralteter Protokolle wie TLS 1.0 oder das Anbieten schwacher Cipher. Zusammen mit der fehlenden CSP ist dies der häufigste Mangel. Belgien begrenzt den Schaden auf 59,4%, während Frankreich mit 77,7% den höchsten Anteil aufweist.

6. Fazit und Empfehlungen

Der Benchmark zeichnet einen Markt, in dem die Grundlagen weitgehend vorhanden sind, hochwertige präventive Sicherheitsmaßnahmen aber strukturell zurückbleiben. Vier Schlussfolgerungen stehen im Mittelpunkt.

1. Das Grundniveau ist solide, aber nicht mehr als das. Mit einem Durchschnittswert von 68,6 und einem Median von 65 liegt der Markt im Mittelfeld. Die große Gruppe von Domains zwischen 55 und 74 Punkten zeigt, dass sich mit begrenztem Aufwand viel gewinnen lässt.

2. Header, CSP und TLS sind die größten Chancen. Diese drei Themen weisen die höchsten Schwachstellenquoten auf und sind zugleich relativ einfach zu verbessern. Sie bilden damit den logischen Ausgangspunkt jedes Verbesserungsprozesses.

3. Es gibt deutliche Länderunterschiede. Belgien führt, Frankreich liegt zurück und die Niederlande und Deutschland folgen dem Benchmark. Diese Unterschiede bieten Ansatzpunkte für eine gezielte, länderspezifische Marktbearbeitung.

4. Der Quickscan macht es messbar. Da jede Domain einen eindeutigen Wert und eine konkrete Liste von Befunden erhält, lässt sich Verbesserung sofort sichtbar machen. Das macht den Quickscan zu einem starken Instrument sowohl für den ersten Kontakt als auch für die regelmäßige Fortschrittsmessung.

6.1 Empfehlungen für MSPs, Partner und Distributoren

- Positionieren Sie den Quickscan als kostenlose Erstmessung, mit der ein (potenzieller) Kunde sofort sieht, wie seine Domain im Vergleich zu diesem Benchmark abschneidet.
- Nutzen Sie die Länderunterschiede aus diesem Bericht für eine gezielte Marktbearbeitung, etwa indem Sie in Frankreich fehlende Sicherheits-Header in den Vordergrund stellen.
- Bieten Sie den Quickscan als wiederkehrenden Service an, damit Kunden ihren Fortschritt regelmäßig messen können und Verbesserungen sichtbar werden.

6.2 Empfehlungen für Organisationen

- Bestimmen Sie mit einem Quickscan Ihre eigene Ausgangsposition im Vergleich zu diesem Benchmark.
- Richten Sie die erste Verbesserungsrunde auf Sicherheits-Header und die HTTPS-Weiterleitung, da diese schnell und mit geringem Aufwand umsetzbar sind.
- Planen Sie eine zweite Runde rund um die Content Security Policy und die TLS-Härtung, wo der größte inhaltliche Gewinn liegt.
- Wiederholen Sie den Scan regelmäßig, damit der Fortschritt sichtbar bleibt und das Sicherheitsniveau erhalten bleibt.

Selbst einen Quickscan durchführen?

Neugierig, wie Ihre eigene Domain im Vergleich zu diesem Benchmark abschneidet? Führen Sie kostenlos einen Quickscan durch unter

guardian360.de/quickscan

Anhang. Methodische Hinweise

Die Zahlen in diesem Bericht sind aus den Rohdaten des Guardian360 Quickscan abgeleitet. Berücksichtigt wurden nur Scans mit dem Status „completed“. Fehlgeschlagene oder nicht vollständig abgeschlossene Scans wurden ausgeschlossen. Für diese Ausgabe betraf das 717 fehlgeschlagene Scans von insgesamt 13.631, womit 12.914 verwertbare Ergebnisse verbleiben.

Die Zuordnung zu einem Land erfolgt anhand der Länderkennung in der Top-Level-Domain. Eine Domain, die auf .nl endet, wird den Niederlanden zugeordnet, .be Belgien, .de Deutschland und .fr Frankreich. Diese Methode ist einfach und reproduzierbar, hat aber eine Einschränkung. Eine Organisation, die in einem bestimmten Land aktiv ist, aber eine generische Domain wie .com nutzt, wird diesem Land nicht zugeordnet. Diese Domains fließen in den Gesamt-Benchmark ein.

Eine Schwachstelle wird gezählt, wenn der Quickscan das betreffende Element als anfällig markiert. Bei SSL/TLS wird eine Domain als anfällig eingestuft, sobald mindestens ein Einzelbefund wie ein veraltetes Protokoll oder ein schwacher Cipher erkannt wird. Die angegebenen Prozentwerte beziehen sich stets auf den Anteil der Domains innerhalb des jeweiligen Segments.