

Status implementatie informatieveiligheidsstandaarden in het mbo (IV-metingen)

Q4 2023

Datum	Versie	Auteur
25 januari 2024	1.0	Mick Deben

Met de zogenaamde IV-metingen controleert Surf ieder kwartaal de hoofddomeinen van de onderwijs- en onderzoeksector op de implementatie van verschillende informatieveiligheidsstandaarden. De metingen zijn gericht op zowel websites als e-mailbeveiliging van hoofddomeinen en hebben als doel instellingen te motiveren om ontbrekende standaarden te implementeren, en daarmee hun cyberweerbaarheid te verhogen. SURF gebruikt de API van [Internet.nl](https://internet.nl) voor de metingen en deelt de resultaten met de instellingen via haar besloten SCIPR- en SCIRT-communities.

Een nieuwe ontwikkeling is dat de Internet Cleanup Foundation vergelijkbare metingen voor de Nederlandse onderwijssector gaat verrichten. De organisatie publiceert de uitkomsten daarvan op [Basisbeveiliging.nl](https://basisbeveiliging.nl). Deze openbare publicatie is een extra reden voor instellingen om opvolging te geven aan de uitkomsten van de metingen.

In dit document zoomen we in op de resultaten van de IV-metingen bij mbo-instellingen in het vierde kwartaal van 2023 en geven we duiding aan de resultaten.

1 IV-metingen

1.1 De standaarden en geadresseerde risico's

Onderstaand schema geeft een overzicht van de standaarden die SURF met de IV-metingen controleert. Daarachter geven we aan welke risico's een instelling loopt als ze de standaard niet (juist) heeft geïmplementeerd.

Standaarden	Risico's
Web	
IPv6 Internet Protocol versie 6 (IPv6) is een modern protocol met veel meer adresruimte dan IPv4. Hierdoor kan ieder apparaat en iedere gebruiker zijn eigen IP-adres krijgen.	Wanneer een website of mailserver niet bereikbaar is vanaf IPv6-adressen, is een omweg via IPv4 noodzakelijk. Dit heeft negatieve impact op de bereikbaarheid en prestaties van het domein.
DNSSEC Domain Name System Security Extensions (DNSSEC) is een cryptografische beveiliging voor het DNS-protocol. Het vertaalt namen naar IP-adressen (bijvoorbeeld mbodigitaal.nl naar 46.19.218.100).	Zonder DNSSEC is de integriteit van DNS-informatie niet gewaarborgd. Concreet betekent het ontbreken van DNSSEC dat instellingen in mindere mate weerstand kunnen bieden tegen aanvallen als DNS hijacking, DNS cache poisoning, domain shadowing, Man-in-the-Middle (MitM) en DNS spoofing. ¹
HTTPS Hypertext Transfer Protocol Secure (HTTPS) zorgt ervoor dat HTTP-verkeer wordt versleuteld.	Het ontbreken van HTTPS betekent dat netwerkverkeer onversleuteld over het internet wordt getransporteerd. Hierdoor kan het eenvoudig worden onderschept, gelezen en gemanipuleerd.
Beveiligingsopties Beveiligingsopties refereren naar een aantal security headers die de beveiliging van een website verbeteren. ² Ook wordt gecontroleerd of een instelling een security.txt-bestand heeft gepubliceerd ten behoeve van het responsible disclosure proces.	Het ontbreken van de verschillende beveiligingsopties betekent dat websites in mindere mate weerstand kunnen bieden tegen MitM, clickjacking, code injecties en Cross Site Scripting (XSS).
RPKI Resource Public Key Infrastructure (RPKI) is een techniek die het mogelijk maakt voor eigenaren van blokken IP-adressen om te	Zonder RPKI kunnen andere netwerkbeheerders niet controleren of er een onbedoelde of kwaadwillige omleiding van internetverkeer plaatsvindt. RPKI voorkomt routelekken en -kapingen en is essentieel

¹ <https://nl.godaddy.com/help/wat-is-dnssec-6135#why>

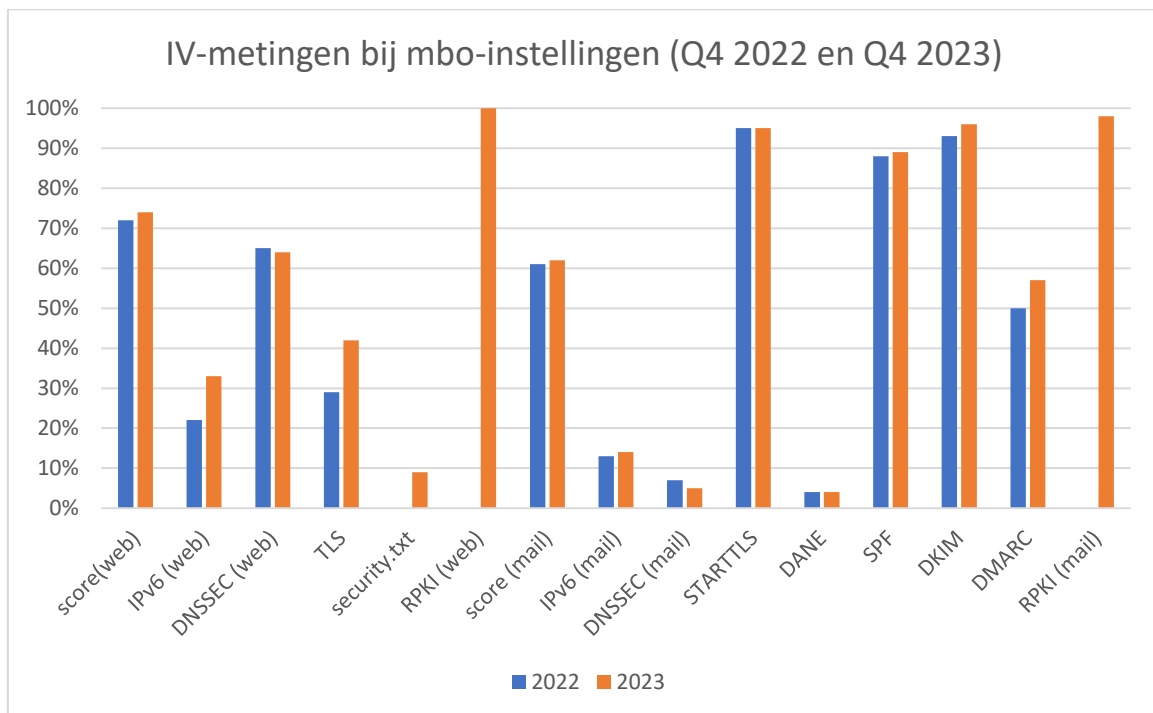
² <https://securityheaders.com/>

verklaren bij welk netwerk ze horen en hoe groot de blokken horen te zijn.	voor de beveiliging van websites en systemen.
Mail	
<p>SPF Sender Policy Framework (SPF) is een techniek die het mogelijk maakt om te verifiëren of een e-mailbericht is verzonden door een geautoriseerde afzender.</p>	Een ontbrekend of incorrect SPF-record kan anderen in staat stellen om e-mails te verzenden uit naam van de instelling ('spoofing'). Dit kan gebruikt worden in social-engineeringaanvallen zoals phishing om vertrouwen te wekken onder de ontvangers.
<p>DKIM Domain Keys Identified Mail (DKIM) maakt het mogelijk om de authenticiteit van een e-mailbericht te verifiëren.</p>	Het ontbreken van DKIM zorgt ervoor dat ontvangers de authenticiteit van een e-mail niet kunnen verifiëren. Daardoor kunnen ontvangers minder goed onderscheid maken tussen legitieme en frauduleuze (spoofing) e-mails.
<p>DMARC Domain-based Message Authentication, Reporting and Conformance (DMARC) is een techniek die het mogelijk maakt om de afleverbaarheid van e-mails te verbeteren.</p>	Het ontbreken van DMARC kan leiden tot hogere impact van phishingaanvallen, een verminderd inzicht in de afleverbaarheid van e-mails en een verhoogde kans op spammarkeringen.
<p>STARTTLS STARTTLS is een methode om beveiligde gegevensuitwisseling via TLS toe te voegen aan een bestaand netwerkprotocol, met behoud van terugwaartse compatibiliteit voor bijvoorbeeld Simple Mail Transfer Protocol (SMTP) en Lightweight Directory Access Protocol (LDAP).</p>	Door het ontbreken van STARTTLS blijven bestaande onveilige protocollen zoals SMTP onveilig, waardoor de integriteit en vertrouwelijkheid van verbindingen niet gegarandeerd kunnen worden.
<p>DANE DNS-based Authentication of Named Entities (DANE) is een generiek protocol voor het veilig publiceren van publieke sleutels en certificaten.</p>	Het ontbreken van DANE betekent dat het transport van mail- en webverkeer minder goed beveiligd is, bijvoorbeeld door verbindingen niet te versleutelen.

1.2 Status eind 2023

Onderstaande figuur vergelijkt de resultaten van de IV-metingen bij mbo-stellingen van het vierde kwartaal van 2022 met die van het vierde kwartaal van 2023.³ De resultaten laten zien dat er in een jaar beperkt vooruitgang is geboekt. In sommige gevallen is zelfs een verslechtering waargenomen. Het valt op dat mbo-instellingen laag scoren voor DNSSEC en DANE voor e-mail. Dit is te verklaren met het feit dat Microsoft geen of beperkt ondersteuning voor deze protocollen biedt.⁴

Ook valt op dat er weinig instellingen zijn met een coordinated vulnerability disclosure (CVD) / responsible disclosure beleid voor het melden van technische kwetsbaarheden en misconfiguraties (security.txt). Terwijl er speciaal voor mbo-instellingen wel een centraal meldpunt is op rd.mbodigitaal.nl. Wil je hier ook op aansluiten? Neem dan contact op met jeffeny.hoogervorst@surf.nl.



Noot: in 2022 werd nog niet gecontroleerd op security.txt en RPKI, waardoor deze scores in Q4 van 2022 op 0 zijn gezet.

³ <https://wiki.surfnet.nl/display/SCIPR/2023+Q4>

⁴ <https://techcommunity.microsoft.com/t5/exchange-team-blog/support-of-dane-and-dnssec-in-office-365-exchange-online/ba-p/1275494>

2 Programma Cyberveiligheid

Vanuit het programma Cyberveiligheid onderschrijven wij het belang van de standaarden en de IV-metingen van SURF. Deze dragen bij aan het verhogen van de technische weerbaarheid van instellingen. Daarom ondernemen we vanuit het programma Cyberveiligheid de volgende initiatieven om de adoptie van de standaarden onder de instellingen te verhogen:

- √ We ontwikkelen van een praktische handleiding voor de [implementatie van de e-mailbeveiligingsstandaarden](#) in Microsoft 365-omgevingen;
- √ We breiden de handleiding voor het [implementeren van de e-mailbeveiligingsstandaarden](#) uit met MTA-STS;
- √ We inventariseren alle (sub)domeinen van instellingen om de scope van de IV-metingen te kunnen uitbreiden met deze (sub)domeinen. Dit zorgt voor een completer beeld van de adoptie van de standaarden, en daarmee ook van het risicoprofiel van instellingen. (De geïnventariseerde (sub)domeinen worden nog niet meegenomen in de IV-metingen);
- √ We stellen een centraal CVD/RD-beleid beschikbaar op rd.mbodigitaal.nl;
- √ We ontwikkelen een praktische handleiding voor het [beveiligen van digitale communicatie](#) (TLS);
- √ We ontwikkelen een praktische handleiding voor het voorkomen van de [top 10 misconfiguraties in netwerken](#);
 - We stellen voor elke instelling een dashboard beschikbaar, waarmee zij de adoptie van de standaarden van alle domeinen kan monitoren en verbeteren (status: gestart);
 - We verbeteren de inhoud van het dashboard, zodat deze logischer, vollediger, leesbaarder wordt en naar handige formaten kan worden geëxporteerd (status: gestart).