mbo digitaal

Status implementatie informatieveiligheidsstandaarden in het mbo (IV-metingen)

Q4 2024

Datum	*Versie*	*Auteur*
13 januari 2025	1.0	Mick Deben

Surf voert ieder kwartaal IV-metingen uit om te controleren of de hoofddomeinen van de onderwijs- en onderzoeksector voldoen aan een lijst van aanbevolen informatieveiligheids-standaarden. De metingen zijn gericht op zowel websites als e-mailbeveiliging. Doel is om instellingen te motiveren eventuele ontbrekende standaarden te implementeren. Dit helpt hun cyberweerbaarheid te verhogen.

SURF gebruikt de API van 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. 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 2024. Ook 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. Daarnaast geven we aan welke risico's een instelling loopt als ze de standaard niet (juist) implementeert.

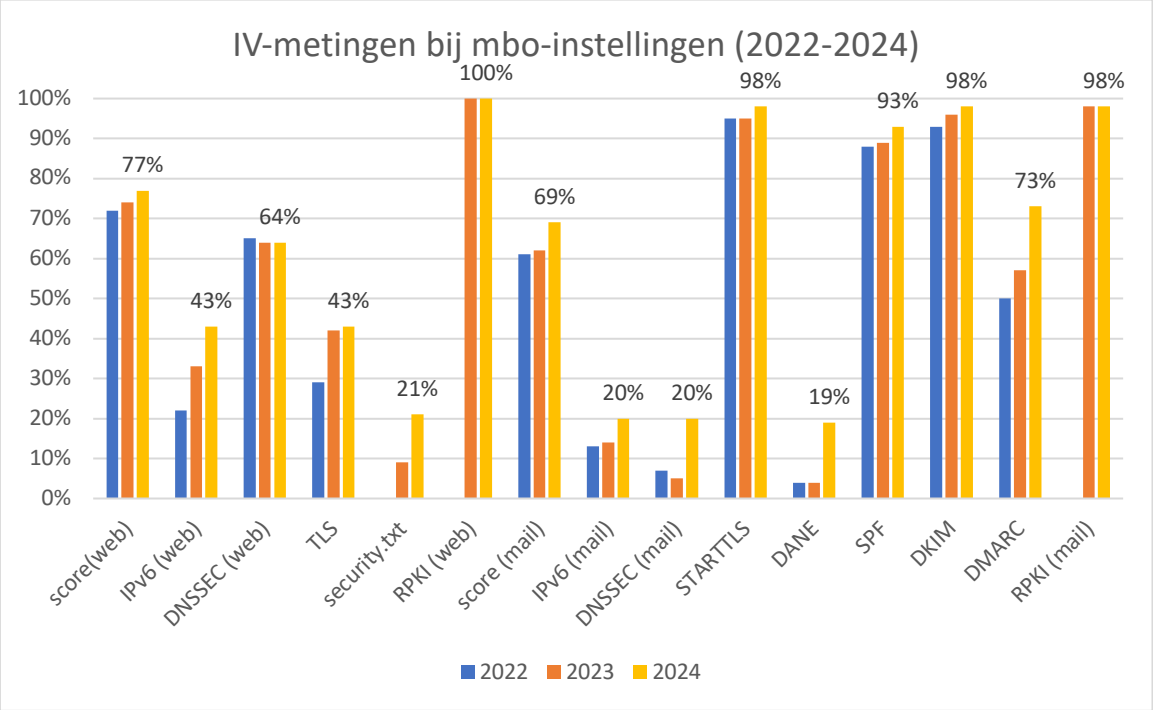
Standaarden	Risico's
Web	
IPv6 Internet Protocol versie 6 (IPv6) is een modern protocol met veel meer adresruimte dan IPv4. Hierdoor kan ieder apparaat en iedere gebruiker zijn eigen IP-adres krijgen.	Wanneer een website of mailserver niet bereikbaar is vanaf IPv6-adressen, is een omweg via IPv4 noodzakelijk. 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 minder weerstand kunnen bieden tegen aanvallen. Denk aan DNS hijacking, DNS cache poisoning, domain shadowing, Man-in-the-Middle (MitM) en DNS spoofing.[1]
HTTPS Hypertext Transfer Protocol Secure (HTTPS) versleutelt HTTP-verkeer.	Het ontbreken van HTTPS betekent dat netwerk- en internetverkeer onversleuteld plaatsvindt. Dat maakt onderscheppen makkelijk waardoor kwaadwillenden data kunnen lezen en manipuleren.
Beveiligingsopties Beveiligingsopties refereren naar security headers die de beveiliging van een website verbeteren.[2] Ook controleren deze of een instelling een security.txt-bestand heeft gepubliceerd voor het responsible disclosure proces.	Het ontbreken van de verschillende beveiligingsopties betekent dat websites minder weerstand kunnen bieden tegen MitM, clickjacking, code injecties en Cross Site Scripting (XSS).
RPKI Resource Public Key Infrastructure (RPKI) is een techniek die het voor eigenaren van blokken IP-adressen mogelijk maakt om te verklaren bij welk netwerk deze adressen horen en hoe groot de blokken horen te zijn.	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/

	voor de beveiliging van websites en systemen.
Mail	
SPF Sender Policy Framework (SPF) is een techniek die het mogelijk maakt om te verifiëren of een e-mailbericht komt van een geautoriseerde afzender.	Een ontbrekend of incorrect SPF-record betekent dat anderen e-mails kunnen verzenden uit naam van de instelling ('spoofing'). Dit kan gebeuren bij social-engineeringaanvallen zoals phishing om vertrouwen te wekken bij ontvangers.
DKIM Domain Keys Identified Mail (DKIM) helpt om de authenticiteit van een e-mailbericht te verifiëren.	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.
DMARC Domain-based Message Authentication, Reporting and Conformance (DMARC) is een techniek die het mogelijk maakt om de afleverbaarheid van e-mails te verbeteren.	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.
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).	Door het ontbreken van STARTTLS blijven bestaande onveilige protocollen zoals SMTP onveilig. De integriteit en vertrouwelijkheid van verbindingen valt dan niet te garanderen.
DANE DNS-based Authentication of Named Entities (DANE) is een generiek protocol voor het veilig publiceren van publieke sleutels en certificaten.	Het ontbreken van DANE betekent dat het transport van mail- en webverkeer minder goed beveiligd is, bijvoorbeeld doordat verbindingen niet versleuteld zijn.

1.2 Status eind 2024

Onderstaande figuur vergelijkt de resultaten van de IV-metingen bij mbo-stellingen vanaf het vierde kwartaal van 2022 met de vierde kwartalen van 2023 en 2024.[3] Alleen de scorepercentages van Q4 2024 zijn weergeven.



De resultaten laten zien dat er sinds Q4 2023 beperkt progressie is gemaakt. Het valt op dat mbo-instellingen eind 2024 voortgang geboekt hebben voor DNSSEC en DANE voor e-mail. Dit is te verklaren doordat Microsoft hier (eindelijk) ondersteuning voor biedt. Hoe je DNSSEC en DANE voor Microsoft 365 kunt implementeren hebben we onlangs toegevoegd aan de handreiking beveiligen e-mail.

De laagste drie scores hebben betrekking op de afwezigheid van (1) een coordinated vulnerability disclosure (CVD) of responsible disclosure (RD) beleid (inclusief een security.txt bestand) voor het melden van technische kwetsbaarheden en misconfiguraties; (2) DNSSEC en (3) DANE. Alle drie zijn snel en eenvoudig op te lossen door de stappen te volgen in de handreiking beveiliging e-mail (voor DNSSEC en DANE) en door aan te sluiten op het centrale CVD-beleid van de sector. Wij bevelen alle instellingen nogmaals aan om hierop aan te sluiten of om zelf een dergelijk beleid te publiceren.

Als je aansluit op het centrale beleid komen meldingen binnen bij SURFcert en worden ze van daaruit doorgezet naar de bij SURFcert bekende contactpersoon van de instelling. Aanvullend daarop krijg je ondersteuning van Ry en Mick voor de afhandeling van meldingen (indien gewenst). Een CVD-beleid biedt kansen om de beveiliging verder aan te schroeven en

[3] https://wiki.surfnet.nl/display/SCIPR/2024+Q4

introduceert geen extra dreiging. Wil je hier ook op aansluiten? Neem dan contact op met Mick Deben.

Verder zien we voor DMARC 73% naleving. Sommige instellingen hebben wel een DMARC-beleid geïmplementeerd, maar deze niet voldoende strikt ingesteld (p=quarantine of p=reject). Het doel is om naar 'reject' toe te werken. We bevelen instellingen aan om zo snel mogelijk. De stap naar 'quarantine' te zetten en actief DMARC-rapportages te monitoren.

Voor het activeren van IPv6 voor Microsoft Office 365 Exchange Online mail kunnen instellingen een Service Request indienen.[4]

Voor TLS (web) zien we 43% naleving. In de handreiking TLS bieden we concrete handvaten om verbeteringen hieraan door te voeren. Bij meer dan de helft van de instellingen is de website niet bereikbaar via IPv6. De hoofdwebsites van de instellingen worden veelal door externe partijen gehost. Dus om de punten die met TLS te maken hebben op te lossen zoeken we samenwerking met de leveranciers.

We hopen dat instellingen met de hierboven genoemde verwijzingen kunnen voldoen aan de resterende standaarden. Mocht je vragen hebben of ondersteuning wensen, neem dan contact op met Mick Deben.

[4] https://www.forumstandaardisatie.nl/stappenplan-activering-ipv6-op-microsoft-office-365-exchange-online-email

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 en onderhouden 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, om de adoptie van de standaarden van alle domeinen te kunnen monitoren en verbeteren (status: on hold);
- We verbeteren de inhoud van het dashboard, om deze logischer, volledige en leesbaarder te maken. Hierdoor kan de inhoud naar handige formaten worden geëxporteerd (status: on hold).