mbo digitaal

Status implementatie informatieveiligheidsstandaarden in het mbo (IV-metingen)

Q4 2022

Datum 11 oktober 2023 *Versie* 1.0 *Auteur* Mick Deben

Ieder kwartaal controleert SURF alle hoofddomeinen van de onderwijs- en onderzoeksector op de implementatie van verschillende informatieveiligheidsstandaarden met behulp van de zogenaamde IV-metingen. Deze metingen vinden plaats via de API van internet.nl en de resultaten worden via de SCIPR- en SCIRT-communities van SURF gedeeld met de instellingen. De IV-metingen zijn gericht op zowel websites als e-mailbeveiliging van hoofddomeinen. Het doel van de metingen is om instellingen te motiveren de ontbrekende standaarden te implementeren, en daarmee de cyberweerbaarheid te verhogen. In dit document zoomen we in op de status in Q4 2022 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.

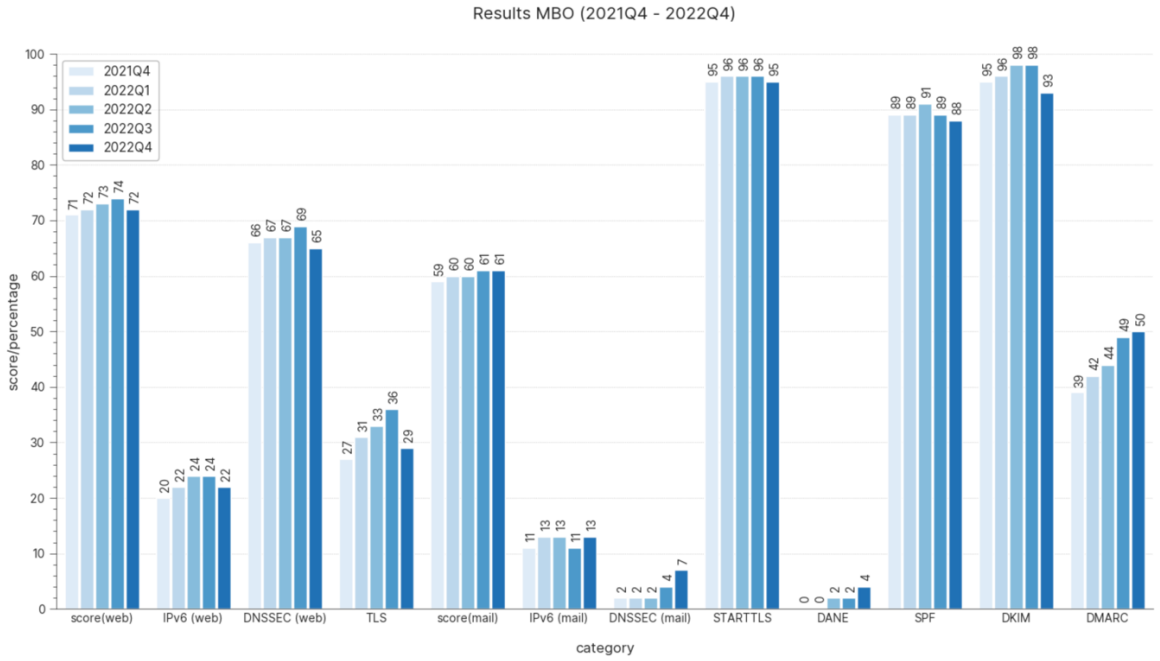
Standaarden	Risico's
Web	
IPv6 Internet Protocol versie 6 (IPv6) is een modern protocol met veel meer adresruimte dan IPv4. Hierdoor kan ieder apparaat en iedere gebruiker zijn eigen IP-adres krijgen.	Wanneer een website of mailserver niet bereikbaar is vanaf IPv6-adressen is een omweg via IPv4 noodzakelijk. 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 DNS hijacking, DNS cache poisoning, domain shadowing, Man-in-the-Middle (MitM) en DNS spoofing aanvallen.[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 controleren ze 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) aanvallen.
RPKI Resource Public Key Infrastructure (RPKI) is een techniek die het mogelijk maakt voor eigenaren van blokken IP-adressen om te verklaren bij welk netwerk ze 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 route-lekken 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 is verzonden door een geautoriseerde afzender.	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.
DKIM Domain Keys Identified Mail (DKIM) maakt het mogelijk 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, waardoor de integriteit en vertrouwelijkheid van verbindingen niet gegarandeerd kunnen worden.
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 door verbindingen niet te versleutelen.

1.2 Status eind 2022

De resultaten van alle IV-metingen in 2022 zijn weergeven in onderstaande figuur.[3] De resultaten laten zien dat er beperkte vooruitgang is geboekt. In sommige gevallen is zelfs een verslechtering ten opzichte van eerdere metingen waargenomen. Het valt op dat instellingen laag scoren voor DNSSEC en DANE voor e-mail. Dit is te verklaren met het feit dat Microsoft nog geen ondersteuning voor deze protocollen biedt.[4]



[3] https://wiki.surfnet.nl/display/SCIPR/2022+Q4#id-2022Q4-MBO
[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. Zij 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:

- Het ontwikkelen van een praktische handleiding voor de implementatie van de e-mailbeveiligingsstandaarden in Microsoft 365-omgevingen.
- Het inventariseren van alle (sub)domeinen van instellingen om de scope van de IV-metingen te kunnen uitbreiden met die (sub)domeinen. Dit leidt tot een completer beeld van de adoptie van de standaarden, en daarmee ook van het risicoprofiel van instellingen.
- Het beschikbaar stellen van een dashboard voor elke instelling, waarmee zij de adoptie van de standaarden van alle domeinen kan monitoren en verbeteren.
- Het verbeteren van de inhoud van het dashboard, zodat deze logischer, volledi ger, leesbaarder wordt en naar handige formaten kan worden geëxporteerd.