edustandaard

Memo

Voor:	Standaardisatieraad, Edustandaard
Van:	Bureau Edustandaard
Datum:	13 oktober 2021
Betreft:	Memo bij het advies en aanmeldformulier m.b.t. **UBV Veilig en Betrouwbaar e-mailverkeer v0.9**

1. Samenvatting

De afspraak UBV – Veilig en Betrouwbaar e-mailverkeer is namens de Edustandaard werkgroep Uniforme Beveiligingsvoorschriften (UBV) ingediend door Jordy van den Elshout (indiener) op 17 juni 2021 middels het Aanmeldformulier afspraak bij Edustandaard - UBV Veilig en Betrouwbaar e-mailverkeer.

Dit aanmeldformulier is namens Bureau Edustandaard verwerkt en beoordeeld door Jeroen Hamers (standaardisatie expert) en heeft geresulteerd in het volgende advies van Bureau Edustandaard voor inbeheername van UBV Veilig en Betrouwbaar e-mailverkeer v0.9:

✓ Voldoende, met aandachtspunten.

Dit advies is voor wederhoor voorgelegd aan de indiener. Ontvangen reacties zijn in het advies verwerkt.

Voorafgaand aan de beoordeling door Bureau Edustandaard:

Na positief advies voor inbeheername door de werkgroep Uniforme Beveiligingsvoorschriften (UBV) is versie 0.5 gedurende de periode van 18 februari tot 29 maart 2021 voorgelegd voor consultatie. Voorliggende versie (0.9) is bijgewerkt op basis van deze consultatie en de laatste opmerkingen die door de werkgroep zijn gemaakt.

Van de ingediende afspraak is geen ROSA-scan gemaakt. De ingediende afspraak is wel gepresenteerd bij de Architectuurraad tijdens de architectuurraadbijeenkomst op 1 juli 2021.

2. Doel en Doelgroep

De afspraak ‘UBV – Veilig en Betrouwbaar e-mailverkeer’ beoogt een aantal standaarden voor e-mailverkeer in samenhang te beschrijven zodat ze goed implementeerbaar zijn in het onderwijsdomein. Deze dragen bij aan de afleverbetrouwbaarheid van e-mail en bescherming van domeinnamen tegen misbruik, zoals bijvoorbeeld phishing. De beveiligingsstandaarden die hiervoor van belang zijn (SPF, DKIM en DMARC) en de juiste toepassing ervan, worden toegelicht. Dat geldt ook voor de toepassing van STARTTLS en DANE, die de communicatie tussen mailservers beveiligt. Beveiligingsstandaarden voor beveiliging van het e-mailbericht zelf, zoals versleuteling of ondertekening, vallen buiten scope en worden niet behandeld. Dat geldt ook voor de verdere afhandeling binnen de e-mailtoepassing zelf.

De Wet Digitale Overheid (WDO) stelt genoemde beveiligingsstandaarden verplicht voor (semi-)publieke organisaties. Genoemde beveiligingsstandaarden zijn onderdeel van de lijst open standaarden van Forum Standaardisatie. Deze lijst is als uitgangspunt genomen, maar ook andere relevante standaarden en of configuraties die bijdragen aan een veilig en betrouwbaar e-mailverkeer worden behandeld. De voorschriften in ‘UBV – Veilig en Betrouwbaar e-mailverkeer’ faciliteren een effectieve implementatie van deze standaarden in het onderwijsdomein.

3. Advies van bureau Edustandaard

Hieronder een samenvatting van de gedetailleerde uitwerking van het advies van Bureau Edustandaard.

Het bureau geeft het volgende advies: ✓ Voldoende, met aandachtspunten om de volgende redenen:

1.1 Neem expliciete links op naar onderliggende standaarden genoemd bij 1.1

1.4 *DNSSEC/DANE is nog niet overal beschikbaar.*

.a. Neem dit onderwerp expliciet op bij de periodieke bespreking van de opzet en de werking van de voorschriften (zoals in paragraaf 1.6 van de afspraak staat beschreven).

.b. Verschaf (bijvoorbeeld via de website Edustandaard) meer inzicht in waar (bijv. welke systemen) voorschrift: MAIL-BEVEILIG-002 al standaard wordt toegepast of kan worden toegepast.

2.1 *Hoofdstuk 5 bevat voor een deel van de afspraak een aanpak voor implementatie. Voor andere delen zijn er minder concreet uitgewerkte voorbeelden in de afspraak opgenomen.*
Indien mogelijk zou het de implementeerbaarheid vergroten als er implementatie voorbeelden in de afspraak (of in een bijlage) beschikbaar komen.

Overig Corrigeer genoemde typo’s en verkeerde verwijzingen.

4. Advies Werkgroep Uniforme Beveiligingsvoorschriften (UBV)

De werkgroep geeft een positief advies over de in beheer name van de standaard om de volgende redenen:

- De afspraak: “UBV-Veilig en Betrouwbaar email**verkeer**”, heeft een ruime publieke consultatie gekend.
- De resultaten zijn verwerkt en de werkgroep is van mening dat deze voldoende is uitgewerkt om in beheer te worden genomen.
- Implementatie vergt logischerwijs een gefaseerde invoer om verstoringen in e-mailcommunicatie te voorkomen.
  ⇒ *Dit is in hoofdstuk 5 van de afspraak uitgewerkt.*

5. Advies Architectuurraad

De Architectuurraad adviseert positief over de in beheer name van UBV-Veilig en Betrouwbaar e-mailverkeer. Zie agendapunt 7 van verslag architectuurraadbijeenkomst 1 juli 2021.
Voor deze afspraak is geen ROSA-scan uitgevoerd.

6. Roadmap

Het beheer van de afspraak is als volgt vormgegeven:

“Binnen Edustandaard wordt periodiek (minimaal eenmaal per jaar) de opzet en de werking van de voorschriften besproken met alle relevante stakeholders die vertegenwoordigd zijn in de Standaardisatieraad. Hiertoe wordt input verzameld vanuit de Edustandaard werkgroep Uniforme beveiligingsvoorschriften en vanuit Edu-K.”

Er is geen specifieke roadmap voor de afspraak beschikbaar, maar naast voorschriften voor Veilig en Betrouwbaar e-mailverkeer, die door de werkgroep besproken worden, zijn er ook andere aanpalende uniforme beveiligingsvoorschriften, zoals ‘UBV Security Headers’ en ‘UBV Domeinnaambeveiliging’.

7. Gevraagd besluit

De leden van de Standaardisatieraad wordt gevraagd om, gelet op bovenstaande overwegingen, in te stemmen met de in beheer name van de afspraak “UBV Veilig en Betrouwbaar e-mailverkeer”, v0.9, welke bij inbeheername zal worden omgedoopt tot versie 1.0.

Tevens adviseert Bureau Edustandaard de Standaardisatieraad om bij het bespreken van het in beheer nemen van deze afspraak stil te staan (en eventueel vervolgstappen te formuleren) bij de beantwoording van vraag 6.2 van het aanmeldformulier. Daarin doet de werkgroep het volgende voorstel:

> *“Het gebruik maken van het dashboard van internet.nl, die de mogelijkheid geeft om een batch van domeinnamen te scannen op de meeste eisen uit de voorschriften. Dit dashboard kan ook ingezet worden voor alle gebruikte domeinnamen in het PO/VO. Op basis hiervan - indien gewenst - gestuurd worden.*
>
> *Voor het MBO en HO wordt dit reeds door Surf gedaan. Zij scannen eens per kwartaal de domeinnamen en publiceren de resultaten hiervan op een afgeschermde pagina.”*

Naast de vraag of een dergelijk overzicht wenselijk en uitvoerbaar is zal moeten worden besproken wat er eventueel verder nog bestuurlijk geregeld moet worden om de implementatie van de afspraak zo goed mogelijk te verwezenlijken.

Tot slot nog twee aanvullende adviezen die de standaardisatieraad kan meegeven aan de werkgroep UBV:

- Het onderwerp van deze afspraak krijgt ook buiten het onderwijs veel aandacht. Bureau Edustandaard adviseert (wellicht ten overvloede) om vanuit de werkgroep ook minstens één persoon af te vaardigen om deel te nemen in bredere overleg verbanden over dit onderwerp.
- In de afspraak en op het aanmeldformulier staat: *“Binnen Edustandaard wordt periodiek (minimaal eenmaal per jaar) de opzet en de werking van de voorschriften besproken met alle relevante stakeholders die vertegenwoordigd zijn in de Standaardisatieraad. Hiertoe wordt input verzameld vanuit de Edustandaard werkgroep Uniforme beveiligingsvoorschriften en vanuit Edu-K.”*
  Het lijkt Bureau Edustandaard verstandig om hier **één primair verantwoordelijke** voor te benoemen, die bewaakt dat dit minimaal eenmaal per jaar wordt uitgevoerd.