Uniforme Beveiligingsvoorschriften

Veilig en betrouwbare e-mail

Datum	11-8-2020
Versie	0.1 Concept
Auteur	Edustandaard werkgroep Uniforme Beveiligingsvoorschriften

INHOUDSOPGAVE

Historie

Versie	Auteur	Toelichting	Datum
0.1	Jordy van den Elshout	Eerste concept	11 augustus 2020

1 Inleiding

1.1 Achtergrond

Bureau Edustandaard heeft een (advies)verzoek van het 'Ketenregieoverleg PO-VO' (hierna: KRO) gekregen voor de implementatie van de WDO-beveiligingsstandaarden in het onderwijs. Bureau Edustandaard heeft daarvoor de werkgroep Uniforme beveiligingsvoorschriften (UBV) de op opdracht gegeven om WDO-beveiligingsstandaarden in onderwijscontext te plaatsen en uit te werken in voorschriften.

De WDO-beveiligingsstandaarden zijn opgesteld voor overheidsorganisaties, zoals ministeries, uitvoeringsorganisatie en gemeentes. Dat zijn andere soorten organisaties, dan een schoolinstelling. Qua omvang en beschikbare middelen, zoals expertise. Dat betekent dat er ook extra aandacht besteed wordt aan effectiviteit van de WDO-beveiligingsstandaarden en de wijze van implementatie: stappenplan in combinatie met voorbeeld configuraties (best practices).

De WDO-Beveiligingsstandaarden verwijst naar de verplichte lijst van Forum Standaardisatie, met open standaarden. Deze lijst wordt als uitgangspunt genomen, maar niet uitputtend. Ook andere relevante standaarden en of configuraties daarvan die bedragen aan een veilig en betrouwbare e-mail worden meegenomen. Ambitie van de werkgroep UBV is om de relevante WDO beveiligingsstandaarden uit te werken tot maatregelen die goed implementeerbaar zijn en effectief zijn voor het onderwijs domein. In dit document worden afspraken voor veilig en betrouwbaar e-mail verkeer behandeld.

1.2 Doel

Het onderhouden van een eenduidige set van beveiligingsvoorschriften waarmee de veiligheid en betrouwbaarheid van e-mail in het onderwijs bevorderd wordt.

1.3 Doelgroep

Deze voorschriften zijn bedoeld voor organisaties die e-mail verzorgen en/of beheren in het onderwijs. Dat geldt voor de hele onderwijssector (PO, VO, MBO, HO en WO).

1.4 Samenhang met andere initiatieven

Deze voorschriften zijn onderdeel van de Uniforme beveiligingsvoorschriften (UBV) voor het onderwijs.

De meeste voorschriften komen voort uit de WDO-Beveiligingsstandaarden, de lijst met verplichte open standaarden van Forum Standaardisatie.

Sommige voorschriften gelden op basis van een BIV-classificatie. Hiervoor wordt gebruikt gemaakt van het 'Certificeringsschema informatiebeveiliging en privacy ROSA' van Edustandaard.

1.5 Taken en verantwoordelijkheden

Het eigenaarschap van deze voorschriften is belegd binnen Edustandaard, waar ook andere afspraken binnen het onderwijsdomein worden beheerd. Het beheer en de doorontwikkeling wordt uitgevoerd door de Edustandaard werkgroep Uniforme Beveiligingsvoorschriften (UBV).

1.6 Beheer en doorontwikkeling

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.

2 Algemeen

2.1 Welke standaarden

SPF, DKIM & DMARC worden vaak in één adem genoemd. En dat is logisch ook, aangezien ze gezamenlijk pas effectief zijn. Het vergroot de afleverbetrouwbaarheid van email en voorkomt misbruik (e-mail)domeinnaam door derden (phishing). De ontvangende partij moet hier wel op controleren, wat betekent dat naast het instellen voor uitgaande verkeer, de filtering op ingaande verkeer ook ingesteld moet worden.

Voor een veilige configuratie zijn bovengenoemde standaarden afhankelijk van DNSSEC. Deze vallen echter buiten dit thema en komen breder aanbod onder het thema Domeinbeveiliging.

STARTTLS & DANE zorgt dat communicatie tussen mailservers beveiligd is, zodat de integriteit en vertrouwelijkheid van e-mail beschermd wordt. DANE voorkomt een downgrade attack naar een versleutelde verbinding van SMTP.

Op de website internet.nl kan eenvoudig de toepassing van deze standaarden gecontroleerd.

2.2 Bron voor voorschriften

Voor de voorschriften wordt waar mogelijk gebruik gemaakt van 'hoger gelegen' afspraken. Bij voorkeur internationale afspraken (zoals van INAN), indien nodig nationale afspraken (zoals van Forum Standaardisatie en NCSC) en alleen als die niet voldoen aanvullende afspraken die in deze werkgroep worden gemaakt. Voor de volledigheid worden deze in basis overgenomen en voor details verwezen. Afwijken van bovenliggende afspraken wordt onderbouwd.

2.2.1 Forum Standaardisatie

De WDO-beveiligingstandaarden verwijzen naar de lijst met verplichte open standaarden van Forum Standaardisatie. Welke relevant zijn voor veilig en betrouwbare e-mail worden als uitgangspunt genomen, maar niet uitputtend.

2.2.1 NCSC Factsheet

Voor voorschriften wordt in basis van het advies uit de factsheets van NCSC gevolgd. Bij het maken van nadere invulling wordt gerefereerd aan deze factsheets. Dat betekent ook dat deze als basis geldt en gevolgd dient te worden.

MAIL-ALG-01
Volg de factsheets 'Bescherm domeinnaam tegen phishing' en 'Beveilig verbindingen van mailservers' van NCSC.

3 Bescherm domeinnamen tegen phishing

Een domeinnaam dient beschermd te worden, zodat ongeautoriseerden niet met dat domeinnaam e-mail kunnen verzenden en gebruiken voor een phishingaanval. Wanneer een domein beschermd is, draagt dit ook bij aan een hogere afleverbetrouwbaarheid van e-mail; de kans dat deze niet aankomt of in de SPAM-folder verdwijnt wordt daarmee verkleint.

"Het NCSC adviseert om elke domeinnaam van uw organisatie te voorzien van e-mailauthenticatie met behulp van SPF, DKIM en DMARC. Daarnaast adviseert het NCSC om alle uitgaande e-mail van uw organisatie met behulp van DKIM te ondertekenen"

Dit is een citaat uit de factsheet van NCSC Bescherm domeinnamen tegen phishing. Deze factsheet beschrijft tevens de aanleiding hiervan en geeft een beschrijving van SPF, DKIM en DMARC. Ook wat de voor- en nadelen hiervan zijn. Daarom wordt dit hier niet nader toegelicht. De nadruk ligt meer op de wijze van implementatie en effectiviteit daarvan in het onderwijsdomein.

3.0 Niet gebruikte domeinnamen parkeren

Wanneer een domeinnaam niet (voor e-mail) gebruikt wordt, zorg dan dat deze geparkeerd worden en niet gebruikt kunnen worden voor e-mail.

MAIL-DOMEIN-001 (Betrouwbaarheid)

Om misbruik van een niet gebruikte domein te voorkomen, plaats dan per domeinnaam:
- een zogenaamd “null MX” record in de DNS zone.
- een “SPF -all” record in de DNS zone.
- een “DMARC p=reject” record in de DNS Zone.
- geen DKIM record.

Implementatie: er is inzicht nodig welke domeinnamen in bezit zijn en welke daarvan niet gebruikt worden (voor e-mail). Op dat moment is de implementatie met weinig middelen te realiseren.

3.1 E-mailconfiguratie scheiden in (sub)domeinen

De toepassing van SPF, DKIM en DMARC kan het nodige werk met zich meebrengen. Ook kan het nodig zijn om verschillend beleid toe te passen voor verschillende soorten e-mail(stromen). Bijvoorbeeld automatische berichten uit een systeem versus e-mail van medewerkers of studenten. Mocht er een fout in de configuratie ontstaan of een domein op de blacklist komen, dan heeft dit niet direct impact op alle e-mailstromen.

MAIL-DOMEIN-001 (Betrouwbaarheid)

Advies is om per e-mailstroom één (sub)domein te hanteren.

3.2 Configuratie per (sub)domein

Elk (sub)domein dat gebruikt wordt voor e-mail, dient beveiligd te worden tegen phishing. Deze voorschriften mogen in de implementatiefase afwijken, om te voorkomen dat de e-mailstroom verstoord wordt. De implementatie kent namelijk zijn fases, zoals het beginnen met verkrijgen van inzicht om vervolgens de instellingen strenger in te stellen. Zie de bijlage voor de aanpak.

MAIL-DOMEIN-002 (Betrouwbaarheid)

Elk (sub)domein dat gebruikt wordt voor e-mail, dient beveiligd te worden tegen phishing.

Implementatie: er is inzicht nodig welke e-mailstromen er zijn. Op dat moment is de implementatie met weinig middelen te realiseren: elke e-mailstroom/systeem krijgt zijn eigen (sub)domein als afzendadres.

3.2.1 SPF-Policy

Met *Sender Policy Framework* (SPF) kan aangegeven worden vanaf welke mailservers (IP-adressen) de e-mail van een e-maildomein verstuurd mag worden. Dit wordt met een DNS-recordl op het domein kenbaar gemaakt. Deze informatie is daarmee publieke bekend en wordt door de ontvangende mailserver gebruikt om controleren of de e-mail van een legitieme mailserver afkomstig is.

Per domeinnaam dient (maar) één SPF-beleid aangemaakt te worden: een regel die bepaalt vanaf welke mailservers e-mail afkomstig mag zijn en hoe de ontvangende server moet acteren als dit niet klopt. De opties die geen bescherming bieden "+" (altijd accepteren) en "?" (geen policy; bericht doorlaten), mogen niet gebruikt worden. De overige juist wel.

MAIL-DOMEIN-001 (Betrouwbaarheid)
Het SPF beleid bestaat altijd uit de *optie* "~" (softfail) of "-" (fail) en alleen uit verwijzingen (ip-adres of dns-record) van servers die e-mail mogen verzenden.

Implementatie: er is inzicht nodig vanaf welke servers (IP-adressen, als dan niet via dns-record[1]) e-mail verstuurd wordt. Op dat moment is de implementatie met weinig middelen te realiseren. Inzicht kan middels een (handmatige) inventarisatie, of gebruik te maken van de DMARC-Rapportage functie. Zie hiervoor de aanpak in de bijlage.

3.2.2 DKIM

Domain Keys Identified Mail (DKIM) is het toepassen van een authenticatie op de e-mail. Hiermee kan de ontvangende partij controleren of de e-mail door een legitiem mailserver verstuurd is. Alle uitgaande e-mail moet daarvoor ondertekend worden met de DKIM-sleutel, die correspondeert met de sleutel in het DNS-record.

MAIL-DOMEIN-001 (Betrouwbaarheid)
Alle uitgaande e-mail wordt ondertekend met DKIM, die correspondeert met de DKIM-sleutel in het DNS record van het domeinnaam (van het afzendadres).

Implementatie: De toepassing van DKIM vergt meer middelen dan de toepassing van SPF. Om DKIM toe te passen moet er aanvullende software geïnstalleerd worden op de mailserver. Hierdoor afhankelijk van de gebruikte software van mailservers en/of providers.

Impact voor het onderwijs: voor e-mail van medewerkers wordt veelal een Office of Google omgeving gebruikt. Deze omgevingen ondersteunen DKIM. Voor een Leerling Administratie Systeem (LAS) waaruit gemaild wordt is ondersteuning hiervan niet bekend.

Impact voor leveranciers in het onderwijs: indien gebruikte software dit niet ondersteunt, dient dit aangeschaft te worden.

3.2.3 DMARC

Domain-based Message Authentication, Reporting & Conformance (DMARC) helpt ontvangende partijen hoe om te gaan met ontvangen e-mailberichten. Het geeft instructie aan de mailserver hoe de mail af te handelen als dit afwijkt van de SPF of DKIM informatie: Ontvangen, Quarantaine of Reject. Het beleid zou minimaal Quarantine en Reject moeten zijn, anders zou de mail altijd geaccepteerd worden.

MAIL-DOMEIN-xxx
Het DMARC beleid is minimaal 'Quarantine' of 'Reject'.

[1] Een verwijzing kan via IP-adres of DNS-records, zoals a, mx of cname -record.

Daarnaast kan de mate van alignment bepaald worden. De ontvangende mailserver controleert of het getoonde afzenderadres overeenkomt met het domein opgegeven onder SPF en DKIM. De waarde ‘strict’ zorgt voor een exacte vergelijking, terwijl de mailserver bij ‘relaxed’ controleert of het afzendadres binnen hetzelfde domein valt.

MAIL-DOMEIN-xxx
Het DMARC beleid voor ‘alignment’ is minimaal ‘relaxed’. Advies is ‘strict’.

Implementatie: vergt een gedegen aanpak, om te voorkomen dat de e-mailstroom niet verstoort wordt en uiteindelijk voldoende bescherm is; voldoet aan deze voorschriften.

Impact: <nog bepalen en aanvullen>

3.2.3.1 DMARC Rapportage

DMARC geeft inzicht aan domeineigenaren of een domein wordt misbruikt voor phishing. Het advies is om van deze functie gebruik te maken. Met name voor het inzicht wat het biedt voor implementatie, maar ook voor het onderhoud ervan: het geeft inzicht wanneer een domein misbruikt wordt of een legitieme server geblokkeerd wordt. Bijvoorbeeld door een wijziging in de ICT-omgeving of wanneer een reclamebureau die de opdracht gekregen heeft om een mailing te versturen.

3.3 Toepassing op inkomende e-mail

Voor een volledige bescherming (binnen de sector), dient zowel de versturende als ontvangende partij SPF, DKIM en DMARC op de juiste manier toe te passen.

MAIL-FILTER-001
Inkomende e-mail wordt gecontroleerd op SPF, DKIM en DMARC.

3 Beveilig verbinding van mailservers

E-mailberichten worden door verschillende mailservers over het internet verstuurd. De communicatie hiervan kan versleuteld worden met TLS. Daarmee wordt niet de versleuteling van het bericht bedoeld. Dat staat ook nader toegelicht in het het advies van NCSC; in de Factsheet Beveilig verbindingen van mailservers.

3.1 STARTTLS

Met STARTTLS wordt de communicatie tussen de mailservers beveiligd met TLS. Hiermee wordt de kans verkleint dat e-mail onderweg door ongeautoriseerde wordt aangepast of onderschept. Het biedt echter onvoldoende bescherming voor een veilige e-mailcommunicatie, gezien de afhankelijkheid van andere mailservers op het internet. Als deze geen STARTTLS ondersteunen, wordt de e-mail alsnog onbeveiligd over het internet verstuurd. Daarnaast kan een actieve aanvaller, die het verkeer verandert, STARTTLS eenvoudig ongedaan maken (*downgrade attack*).

Het advies van NCSC is: *"schakel in elk geval STARTTLS in voor al uw inkomende en uitgaande e-mailverkeer, ook als u het toepassen van DANE nog uitstelt. Tegen passieve aanvallers is STARTTLS op zichzelf een effectieve maatregel."*

Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies en configuraties(opties). Aangezien niet alle versies en opties voldoende bescherming bieden, dient de configuratie conform de UBV - TLS (verwijzing naar TLS Thema) voor M2M verkeer te geschieden.

MAIL-BEVEILIG-001
Configureer STARTTLS conform 'UBV - TLS voor M2M' op alle publieke mailservers (die bereikbaar zijn via het internet) voor inkomende en uitgaande e-mailverkeer. Daarnaast wordt geadviseerd om dit ook voor het interne e-mailverkeer toe te passen, de interne mailservers en systemen die e-mail versturen. Met name als deze systemen direct bereikbaar zijn voor gebruikers; geen scheiding in netwerken.

Implementatie: in de meeste gevallen zijn er enkele publiek verbonden mailservers en overige intern.

3.2 DANE

Met DANE, kort voor DNS-based Authentication of Named Entities, wordt richting andere mailservers duidelijk gemaakt dat de mailserver via een beveiligde verbinding bereikbaar is en dat een beveiligde verbinding de voorkeur heeft. Dit voorkomt dat STARTTLS niet gebruikt wordt en zorgt dus dat e-mail altijd over een beveiligde verbinding verstuurt wordt.

"Een actieve aanvaller, die het verkeer dus wel verandert, kan het gebruik van STARTTLS eenvoudig ongedaan maken. De aanvaller verandert het verkeer zó, dat de verzendende mailserver denkt dat de ontvangende mailserver geen STARTTLS ondersteunt. Andersom doet hij dat ook. Populair spreekt men dan van een STRIPTLS-aanval."

De implementatie is afhankelijk van de mogelijkheden in de enerzijds mailserver of -provider[2] en anderzijds de mogelijkheid van DNSSEC (van het domein van de e-mailprovider). DANE is een protocol dat alleen werkt als DNSSEC actief is. Indien configuratie niet mogelijk is of (nog)

[2] Office 365 gaat DANE ondersteunen:
https://techcommunity.microsoft.com/t5/exchange-team-blog/support-of-dane-and-dnssec-in-office-365-exchange-online/ba-p/1275494
G-Suite zou dit al ondersteunen, echter spreekt men niet sec over DANE
https://support.google.com/a/answer/2520500?hl=nl&ref_topic=2683828

onvoldoende effectief is, kunnen er ook andere maatregelen genomen worden. Zoals het beveiligen van het e-mailbericht zelf of andere kanalen te gebruiken om informatie waarvan de integriteit en vertrouwelijkheid noodzakelijk is.

MAIL-BEVEILIG-002
Configureer DANE als dit mogelijk is, neem anders aanvullende compenserende maatregelen zoals het beveiligen van het e-mailbericht zelf..

Implementatie: <nog bepalen en beschrijven>

Impact voor het onderwijs: <nog bepalen en beschrijven>

Impact voor de leveranciers: <nog bepalen en beschrijven>

BIJLAGE: AANPAK

<Hier dient een aanpak beschreven te worden, die ondersteunt in de implementatie van de voorschriften. Met name voor DMARC is bepaalde aanpak nodig om verstoringen van e-mailstromen te voorkomen. Bij implementatie en tijdens wijzigingen in het ict-landschap>

BIJLAGE: VOORBEELDCONFIGURATIES

<hier kunnen voorbeeldconfiguraties toegevoegd worden. Bijvoorbeeld van een SPF record zelf, maar ook opzet in (sub)domeinen>