De internetstandaarden (3)

Joep Bär

Hoe voorkom je misbruik van je mailadres?
Vervolg op mijn artikelen in de Softwarebus, nummers 2022-5 en 2022-6.

Ontvangen reacties

Op 'Is de e-mail in je eigen mailprogramma goed beveiligd?' heb ik diverse vragen ontvangen. Twee soorten daarvan zal ik behandelen.

1. Tegelijk gebruik van POP en IMAP
Meerdere personen gebruiken POP op de pc en IMAP op andere apparaten, en ervaren er problemen mee. Om deze op te lossen is van belang het volgende essentiële verschil tussen POP en IMAP te onthouden:

- POP haalt alleen de mail op van de server uit postvak-in. De mail op de server wordt na de ingestelde periode (meestal 14 dagen) verwijderd van de server. Het verzenden van de mail gaat via het eigen apparaat.

- IMAP gebruikt voor alles alleen de server, 100% identiek aan webmail. Alle mappen op de server zijn toegankelijk. De e-mail in de inbox kan worden verwijderd via een POP-account na de daarin ingestelde bewaartermijn.

Alternatieven
Waar mogelijk heeft alternatief 1 de voorkeur. Alternatief 2 is de tweede keuze. Alternatief 3 wordt alleen aangeraden bij uitgebreide wensen.

1. Is de opslagruimte op de server voldoende groot, gebruik dan alleen IMAP. Het omschakelen van POP naar IMAP is eenvoudig: maak ook een IMAP-account aan en verplaats alle historie van het POP-account naar IMAP en verwijder het POP-account.
2. Is de ruimte op de server onvoldoende dan is de beste oplossing om op één apparaat POP te gebruiken (meestal een pc of laptop) en alle andere IMAP of webmail. Gebruik de IMAP-apparaten om mail te lezen en alleen mail te verzenden die niet gearchiveerd hoeft te worden.
   Het opschonen van de gebruikte ruimte op de server kan vanaf ieder IMAP-apparaat.
3. Ja, je moet alle apparaten kunnen gebruiken om in ieder geval de mail te lezen en verzenden, liefst ook het recente archief. Het archiveren is nu een groot probleem. Dat vergt goed mailbeheer! En synchronisatie van het adresboek werkt niet op het POP-account.

   Oplossing: zet op alle apparaten een IMAP-account. Installeer tevens op één apparaat een tweede account van hetzelfde mailadres maar dan met POP. Stel synchronisatie van de adresboeken in.

   Werk vervolgens overal alleen in het IMAP-account. Schoon regelmatig de IMAP-omgeving op om te voorkomen dat de ruimte op de server vol loopt en je geen mail meer kunt ontvangen. Dit kan door het volledig verwijderen van alle overbodige mails (inclusief prullenbak) en het verplaatsen van alle mail die al gearchiveerd kan worden naar je POP-account vanaf het IMAP-account.

2. Inkomende en uitgaande mail via dezelfde provider
Aan het eind zal ik aangeven waarom dit van belang is. En waarom het verzenden via een andere provider plotseling niet meer werkt of nooit heeft gewerkt.

Digitale fraude/phishing

Iedereen kent wel enkele manieren waarop misbruik gemaakt kan worden van e-mailadressen. Het bekendste is het gebruik door spammers van willekeurige mailadressen om hun boodschap te verspreiden. Of het nu een aanbieding van porno is, de verkoop van credit cards om porno te betalen, malware of een nepfactuur: naar schatting is 90% van de dagelijks verzonden mail spam of phishing-mails.
Voor de zo verzonden mails worden altijd e-mailadressen van anderen gebruikt. Er is een levendige handel in verzamelde mailadressen. En dat van jou kan hier tussen staan.
En het is erg vervelend als hiervoor jouw mailadres wordt gebruikt en jij erop wordt aangesproken of dat door jou verzonden e-mail wordt geweigerd omdat jouw adres of dat van de geadresseerde op een zwarte lijst staat omdat jij een spammer zou zijn.

Maatregelen tegen misbruik van een mailadres

Er worden al jarenlang extra manieren bedacht om e-mailadressen te beveiligen. En iedere manier wordt steeds dwingender ingevoerd. Eerst als optie, dan als gewenst en ten slotte verplicht. De huidige set heeft de volgende cryptische benamingen: DNSSEC, DMARC, DKIM, SPF en DANE.

Wat houden deze in en hoe weet je welke voor jouw mailadres(sen) al in gebruik zijn. drijvende kracht achter de invoering van maatregelen zijn de grote mail-verwerkers Facebook, Google en Microsoft, die veel last hebben van phishing. Zij dwingen alle anderen steeds meer om deze maatregelen ook in te voeren. Zo niet, dan groeit ieder jaar de kans dat jouw mail in een spambox terecht komt. (link 5)

Hoe veilig zijn jouw mailadressen?

Net als in mijn eerste artikel: ‘Voldoet jouw website aan de internetstandaarden?’ roepen we de hulp in van de gratis website **https://internet.nl** . We gebruiken nu de optie om een e-mailadres te testen.
Na een klik op ‘Start test’ is het resultaat binnen enkele minuten te zien. Ieder testonderdeel kan aangeklikt worden om uitleg te krijgen van wat ermee wordt bedoeld en vaak hoe eventuele verbeteringen mogelijk zijn.

Achtergrondinformatie DNS (link 3)

Diverse van de hieronder genoemde aanpassingen moeten in het Domain Name System (DNS) worden doorgevoerd. Het DNS is de wereldwijde database waarin alle internetdiensten van iedere internet-aansluiting zijn vastgelegd. Niet alleen welke computer (server) handelt de dienst af, maar ook welke beveiligingen zijn ingeschakeld. En hoe is die computer/-server te bereiken? Voorbeelden van diensten zijn:

- Op welke server staat welke website resp. e-mail;
- Omzetten van de naam van een website naar het IP-adres van de server waar de website op staat (link 4);
- welke beveiligingen en andere instellingen zijn aanwezig.

Het DNS is niet één centrale database, maar bestaat uit zeer vele databases, waarvan vele bij providers worden onderhouden. Wijzigingen worden continu naar alle aangesloten DNS-databases doorgegeven.

Modern adres (IPv6)

Goed gedaan! Je mailserver is bereikbaar voor verzenders met moderne adressen (IPv6). Daardoor is je mailserver volledig onderdeel van het moderne Internet.

Toon details

Nameservers van domein
- IPv6-adressen voor nameservers
- IPv6-bereikbaarheid van nameservers

Mailserver(s)
- IPv6-adressen voor mailserver(s)
- IPv6-bereikbaarheid van mailserver(s)

Resultaat: modern adres (IPv6)
Een apparaat (computer/server/camera/gadget/…) dat op internet aangesloten is, moet bereikt kunnen worden via een IP-adres (een soort huisnummer) dat wereldwijd uniek moet zijn. Er is begonnen met IPv4, de oude standaard. Het aantal adressen (computers) dat hiermee bereikt kan worden is al jaren kleiner dan het aantal apparaten dat via internet is aangesloten. Via IPv6 kan ieder apparaat wereldwijd een uniek adres krijgen.

Ondertekende domeinnamen (DNSSEC)

Goed gedaan! Je e-mailadresdomein en je mailserverdomein(en) zijn ondertekend met een geldige handtekening (DNSSEC). Verzenders die domeinhandtekeningen controleren, kunnen daardoor betrouwbaar het IP-adres van je ontvangende mailserver(s) opvragen.

Toon details

E-mailadresdomein
- DNSSEC aanwezigheid
- DNSSEC geldigheid

Mailserverdomein(en)
- DNSSEC aanwezigheid
- DNSSEC geldigheid

Deze test geeft aan of IPv6-adressen worden gebruikt. In het DNS zijn de nameservers opgenomen waarin het IPv4 en/of het IPv6 staat. Van beide worden de instellingen onderhouden door de DNS- resp. server-providers. Als je zelf het DNS van een een server beheert, moet het IPv6-adres zelf worden ingesteld, net als het IPv4-adres. (link 4)

Resultaat: ondertekende domeinnaam (DNSSEC)
DNSSEC wordt nagenoeg altijd ingesteld door je (domein-)-provider. Ook als je zelf DNS-instellingen kunt aanpassen.

Echtheidswaarmerken tegen phishing (DMARC, DKIM en SPF)

Goed gedaan! Je domein bevat alle echtheidswaarmerken tegen e-mailvervalsing (DMARC, DKIM en SPF). Ontvangers kunnen daardoor betrouwbaar phishing- of spammails die jouw domeinnaam in hun afzenderadres misbruiken, scheiden van jouw echte e-mails.

Toon details

DMARC
- DMARC aanwezigheid
- DMARC policy

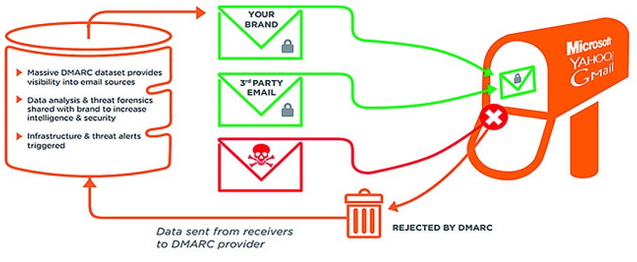
DKIM
- DKIM aanwezigheid

SPF
- SPF aanwezigheid
- SPF policy

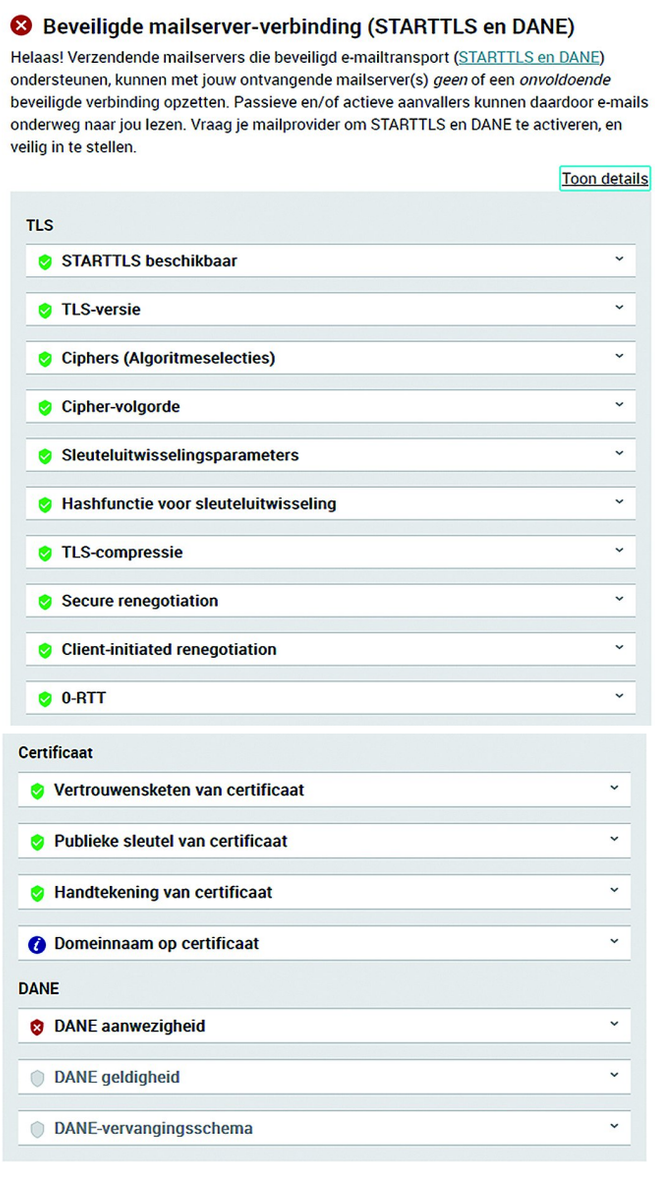
Resultaat: echtheidswaarmerken tegen phishing (DMARC, DKIM en SPF)
DMARC biedt een manier om e-mail voor jouw domein te verifiëren, rapporten op te vragen en zich te conformeren aan een gepubliceerd beleid. Het is een aanvulling op de onderstaande twee beveiligingsstandaarden.

De mailserver voorziet met de DKIM-instelling de body en de header van elk uitgaand bericht van een digitale handtekening. De publieke sleutel wordt via DNS gepubliceerd, zodat een ontvangende mailserver de digitale handtekening kan verifiëren. Zo wordt voorkomen dat kwaadwillenden een bericht namens een ander kunnen verzenden (mail spoofing) of de inhoud van een bericht onderweg kunnen veranderen. SPF voorkomt dat ontvangende mailservers mail-berichten accepteren van ongeautoriseerde servers. Daartoe wordt een lijst van geldige adressen via DNS gepubliceerd. Dat zijn typisch de SMTP-servers die eindgebruikers instellen voor hun uitgaande berichten, maar bijvoorbeeld ook de adressen van een externe dienstverlener die namens jou of een organisatie mail verstuurt. Ontvangende systemen kunnen deze lijst van servers gebruiken om de verzender te controleren voor zij een bericht aannemen.

Hoewel deze drie standaarden meestal gezamenlijk worden ingezet, hoeft dat niet per se. Je kunt ook alleen SPF of DKIM inzetten, of DMARC weglaten. Ondertekening met DNSSEC is voor deze beveiligingsprotocollen niet strikt noodzakelijk – dat wil zeggen verplicht volgens de standaarden – maar wel een belangrijke toevoeging. Maar uiteraard: als je toch bezig bent, stel ze alle drie in.



Het drietal DKIM, SPF en DMARC maakt het mogelijk om de verwerking van mail veel efficiënter te maken. E-mailservers kunnen de binnenkomende berichten uitsplitsen in twee grote bakken: berichten van ongeauthentiseerde domeinen of van wel-geauthentiseerde domeinen die nog niet eerder gezien zijn enerzijds, en bewezen gewenste mail-domeinen anderzijds.
Voor die laatste categorie is de verwerking simpel: die berichten kunnen gelijk afgeleverd worden. Berichten van onbeveiligde en nog onbekende domeinen moeten uitvoerig gecontroleerd worden. Daarvoor worden dan meer resources ingezet. Bovendien loont het om even te wachten met de beslissing: een nieuw spam-mailadres staat pas na enige tijd op zwarte lijsten. De gegevens van DMARC, DKIM en SPF moeten via het DNS worden gepubliceerd.



Resultaat: beveiligde mailserver-verbinding (STARTTLS en DANE)
Onderdeel STARTTLS en DANE zijn de verantwoordelijkheid van de provider/degene die de server inricht.
Onderdeel certificaat: om de e-mail met een beveiligde verbinding op te halen en te verzenden moet een SSL-certificaat aan de domeinnaam worden gekoppeld. Voor eenvoudige websites is een gratis certificaat van Lets Encrypt voldoende. Maar is er meer garantie nodig dat de website van de organisatie is zoals die zich voordoet, dan zal een betaald certificaat nodig zijn. Bijvoorbeeld voor een webwinkel of een multinational.
Soms wordt dit certificaat verzorgd door de provider. Anders kan (meestal) het certificaat via het controlpanel worden ingesteld.
Het is verstandig om het soort certificaat te vermelden in het DNS met een CAA tekstrecord. Lees hieronder hoe.

Resultaat: route-autorisatie (RPKI)
Dit is de verantwoordelijkheid van de provider/degene die de server inricht.

Inhoud van DMARC-, DKIM-, SPF- en CAA-records in het DNS

Er is niet zoiets als HET … record. Iedereen heeft andere belangen. Ik geef verwijzingen naar websites waar de mogelijkheden per recordsoort worden uitgelegd, soms met een programmaatje om zo'n record aan te maken. Zoek eventueel zelf met de recordnaam, zoals: 'dmarc instellen'. Ik geef steeds een voorbeeld van de door mij meest gebruikte gegevens voor het fictieve domein voorbeeld.nl.

Een DNS-record bestaat uit vijf delen, waarvan de eerste drie worden beschreven: naam, type en inhoud. De (levens)duur zal veelal 1 dag = 86400 seconden zijn en de prioriteit is voor geen van de records van belang.
In de naam staat steeds voorbeeld.nl. Dat staat meestal al ingevuld in het DNS, waarbij de rest ervoor wordt gezet.

DMARC (link 6 en 7)

naam: _dmarc.voorbeeld.nl (dus alleen _dmarc invullen!
type: TXT
inhoud: "v=DMARC1;p=quarantine;aspf=r;adkim=r;"

Begin nooit met p=reject. Als je een fout hebt gemaakt met je instellingen, dan wordt meteen geen enkele mail afgeleverd. Als je instelling geen fouten veroorzaakt, maakt dan de policy strikter.

DKIM (link 8)

De publieke sleutel (die in het DNS moet worden vermeld) wordt meestal in het controlpanel vermeld, onder de DNS-instellingen. Het is een zeer lange reeks van tekens.

naam: x._domainkey.voorbeeld.nl
type: TXT
inhoud: "v=DKIM1; k=rsa; p=…"

Ik heb hier alleen de starttekens vermeld. De reeks tekens -na p=- is voor ieder domein anders.

SPF (link 9)

naam: voorbeeld.nl
type: TXT
inhoud: "v=spf1 a mx -all"

Hierin staat dat de mail alleen door de server, genoemd in het MX record van dit domein, mag worden verzonden. Zo niet, dan verdwijnt het bij de ontvangende mailserver in de spambox of prullenbak.
In plaats van resp. in aanvulling op het MX record, kunnen respectievelijk een of meer IPv4- en IPv6- adressen worden opgegeven, maar ook andere domeinen via de includ- optie.

Voorbeeld: include:mail.test.nl. Er is een belangrijke restrictie in dit record: het aantal mailadressen is beperkt. En dat is lastig als je de mail ook via XS4all, Ziggo, Microsoft, etc. wil versturen. Deze hebben zo enorm veel mailservers, die ken je niet allemaal en ze passen niet allemaal. Daarom is er een 'verzameladres' voor veel grote mailverzenders. Een aantal zijn bij mij bekend:

- include:smtp.spf.ziggo.nl
- include:xs4all.nl
- include:freedom.nl
- include:spf.protection.outlook.com

Essentieel is het teken vóór het woordje all aan het eind. Het maakt een groot verschil of je ~, -, + of ? gebruikt. Maak het zo restrictief mogelijk.
Voorbeeld: CompUsers heeft twee maildomeinen: compusers.nl en cumail.nl. Voor cumail.nl zou het record er als volgt uit kunnen zien om mail via beide mailservers te kunnen verzenden:
inhoud: "v=spf1 a mx include:mail.compusers.nl -all"

CAA (link 10)

naam: voorbeeld.nl
type: TXT
inhoud: 0 issue "letsencrypt.org"

Waarom inkomende en uitgaande mail via dezelfde provider? Je loopt geen risico dat je mail plotseling niet meer kan worden verzonden. De mailinstellingen op de server en het DNS staan afgestemd op jouw mailgebruik. Gebruik je een andere provider om je mail te verzenden, dan loop je de kans dat deze zijn instellingen, zonder aankondiging, aanpast. Of ze al zo strikt heeft gemaakt dat verzenden niet mogelijk is. En dan wil je mail niet meer de deur uit. En dat met een vaak onbegrijpelijke melding, en dus paniek.

Links

1. **vragen: joep@bar.cumail.nl**
2. **https://internet.nl**
3. **https://nl.wikipedia.org/wiki/Domain_Name_System**
4. **https://nl.wikipedia.org/wiki/IP-adres**
5. **https://www.sidn.nl/moderne-internetstandaarden/e-mailbeveiliging**
6. **https://www.dmarcanalyzer.com/nl/dmarc-2/**
7. **https://www.dmarcanalyzer.com/nl/dmarc-2/hoe-maak-ik-een-dmarc-record/**
8. **https://www.sparkpost.com/resources/tools/dkim-wizard/**
9. **https://www.antagonist.nl/blog/spf-record/**
10. **https://www.sslcertificaten.nl/support/Terminologie/CAA_DNS_Records**