Spam- en virusbescherming

Spambescherming

Spam is een groot probleem, 90-95% van alle mail is spam. Die willen we zo min mogelijk op onze server toelaten en nog minder in de mailboxen afleveren.

Op de CUmail.nl-server wordt inkomende mail op spam eerst gecontroleerd met de DMARC, DKIM en SPF protocollen:

- DMARC staat voor "Domain-based Message Authentication, Reporting and Conformance", een systeem voor validatie van e-mail dat is ontworpen om email spoofing te detecteren en te voorkomen. Bij e-mail spoofing wordt het afzenderadres vervalst.
- DKIM staat voor "DomainKeys Identified Mail", een techniek waarmee een organisatie verantwoordelijkheid neemt voor een bericht dat per e-mail wordt verzonden. Het biedt een basis voor authenticatie, waarmee reputatieservices opgezet kunnen worden. Deze reputatieservices kunnen op hun beurt door spamfilters worden gebruikt om mogelijke spam te detecteren.
- SPF staat voor "Sender Policy Framework", een protocol ter vermindering van spam door vast te stellen of de verzender van een e-mailbericht gerechtigd is te verzenden namens de vermelde afzender van het bericht.

> Tot 21 december 2018 werd ook nog het DNSBL protocol toegepast.
>
> - DNSBL staat voor "Domain Name System Blacklist", een zwarte lijst van lokaties op het internet die de reputatie hebben spam te versturen.
>
> We gebruikten de zwarte lijst van *zen.spamhaus.org*. Raadpleging van zo'n lijst bleek er echter toe te leiden dat de mailserver heel traag reageerde op pogingen om mail bij de server af te leveren. MXToolBox rapporteerde een transactietijd van langer dan 15 seconden, als gevolg waarvan een time-out optrad. Sinds de uitschakeling van DNSBL is de transactietijd een goede 3 seconden.

Vervolgens passen we SpamAssassin toe, een open-source programma voor mailservers waarmee spam kan worden herkend en onderschept. Dit wordt frequent voorzien van nieuwe gegevens om zo veel mogelijk spam tegen te houden. Standaard is ingesteld dat spam wordt geweigerd. Spamassassin kan worden getraind door spam, die niet als zodanig herkend in de inbox terecht is gekomen, naar de spambox te verplaatsen. Dit werkt met het IMAP protocol en met webmail. Als u het POP3 protocol gebruikt kan het alleen via webmail. Ook het e-mail programma Thunderbird op de eigen computer kan worden getraind, namelijk door de e-mail als spam aan te merken door te klikken op het vlamsymbooltje . Het wordt dan geel en de e-mail wordt verplaatst naar de spam map. Dat werkt zowel voor IMAP als voor POP3.

Daarnaast kunt u voor uw account zelf enkele instellingen van het spamfilter aanpassen. Log hiertoe in op mail.compusers.nl:8443 met het hoofd-e-mailadres (dus geen alias) als gebruikersnaam en het daarbij behorende wachtwoord. Kies dan bij @cumail-adressen voor *De mailaccountinstellingen wijzigen*, dan wel bij @[subdomein].cumail.nl adressen *een van de e-mailadressen*, bijvoorbeeld postmaster@mijnsubdomein.cumail.nl. Klik op het tabblad *Spamfilter*.

Daar kunt u de antispambescherming voor het e-mailadres inschakelen (standaard is dat het geval), en kunt u aangeven wat met als spam gemarkeerde berichten moet worden gedaan. Daarbij moet u bedenken dat het kan gebeuren dat goede mail ('ham') soms ook als spam wordt gemarkeerd. Er zijn drie mogelijkheden:

- **Spam markeren** door een op te geven tekst aan het onderwerp van de e-mails toe te voegen. Standaard is dat "***SPAM***". Dat is handig om het e-mailprogramma thuis de spam uit te laten filteren en naar de spam map te sturen. Daar kunt u dan snel even onderzoeken of er misschien ham tussen de spam terecht is gekomen.
- **Alle spamberichten verwijderen**. U zult de spam dan nooit zien, maar u loopt het risico dat een enkele keer ook goede mail wordt verwijderd.
- **Spam naar de spammap verplaatsen**. Ook dan kunt u de spam nakijken op per ongeluk als spam aangemerkte goede mail, maar in het e-mailprogramma thuis kan dat alleen als u het IMAP protocol gebruikt. U ziet dan wat er op de server in de spam map staat. Als u het POP3 protocol gebruikt zult u de spammap op de server alleen kunnen zien via webmail. Log daartoe in met uw hoofd-e-mailadres en wachtwoord op webmail.compusers.nl.

Onder *Geavanceerde bewerkingen tonen* vindt u nog wat interessante instellingen voor het spamfilter. Als u er op klikt ziet u als eerste de **gevoeligheid van het filter**. Om als spam te worden gemarkeerd moet een bericht tenminste zoveel spampunten hebben als u hier instelt. Het spamfilter voert een aantal verschillende tests uit van de inhoud en de onderwerpregel van elk bericht. Op basis hiervan wordt aan elk bericht een aantal punten toegekend. Hoe hoger het aantal punten, hoe waarschijnlijker het is dat een bericht spam is. Standaard is de gevoeligheid van het filter zo ingesteld dat alle berichten die 7 of meer punten krijgen, als spam worden gekenmerkt. Als u met die instelling te veel

spamberichten ontvangt, kunt u het filter gevoeliger instellen door een lagere waarde, bijvoorbeeld 6, 5 of zelfs 4, in te stellen. Let wel dat dit ook het risico hoger maakt dat goede berichten als spam worden gemarkeerd.

Tot slot kunt u zelf **witte en zwarte lijsten** samenstellen van domeinen waarvan berichten niet als spam resp. wel als spam moeten worden gemarkeerd. Helaas ontwijken veel spammers zwarte lijsten inmiddels door even gemakkelijk van domein te wisselen als van kleding. Het bijhouden van een zwarte lijst is dan dweilen met de kraan open.

Als u vindt dat u ondanks alle maatregelen teveel spamberichten ontvangt, laat het dan weten aan de postmaster van cumail. Misschien kunnen we er dan wat aan doen.

Virusbescherming

Alle mail op de server CUmail.nl wordt standaard gecontroleerd door de DrWeb virusscanner. Deze heeft een uitstekende reputatie, vooral voor mailservers. Elk half uur wordt de CUmail.nl-server voorzien van de nieuwste virus-'signatures'. Een tempo dat u thuis met uw virusscanner niet bij kunt houden.

Op de e-mailaccounts wordt standaard ingesteld dat alle inkomende en uitgaande mail door DrWeb wordt gecontroleerd. U kunt DrWeb zelf aan of uit zetten, zie 'Beheer mail-accounts'.