Dia 1


W&bs Systems
Email “Netjes” versturen
Het gebruik van SPF, DKIM en DMARC voor het bezorgen van legitieme mail

Dia 2

Doel van vandaag

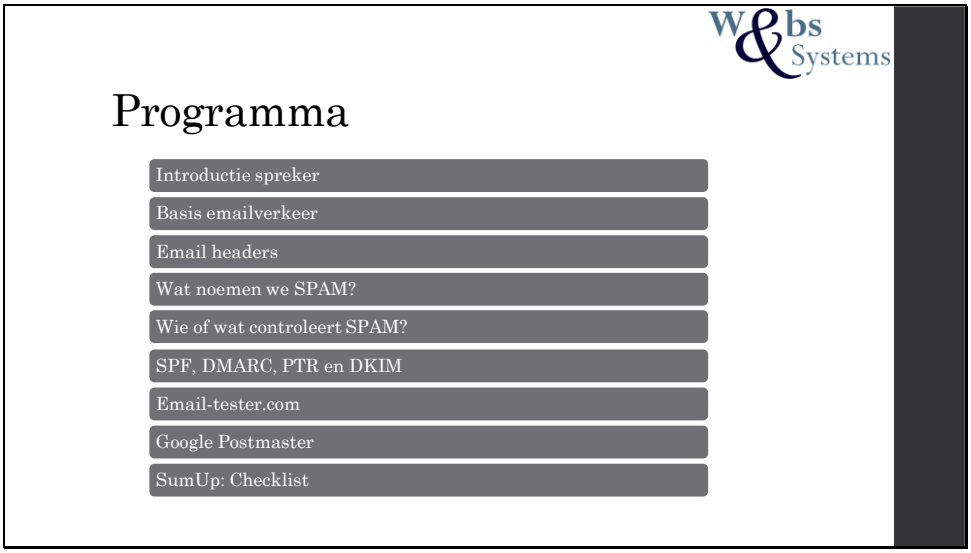
Wat zijn de ervaringen met SPAM?

Wat zijn jullie verwachtingen?

Na vandaag kan je:

- Analyseren waarom een bericht spam is
- Actie ondernemen om valse spam berichten te voorkomen

Dia 3


W&bs Systems
Programma
Introductie spreker
Basis emailverkeer
Email headers
Wat noemen we SPAM?
Wie of wat controleert SPAM?
SPF, DMARC, PTR en DKIM
Email-tester.com
Google Postmaster
SumUp: Checklist

Dia 4

Spreker: Jordi van Nistelrooij
Eigenaar van Webs en Systems.

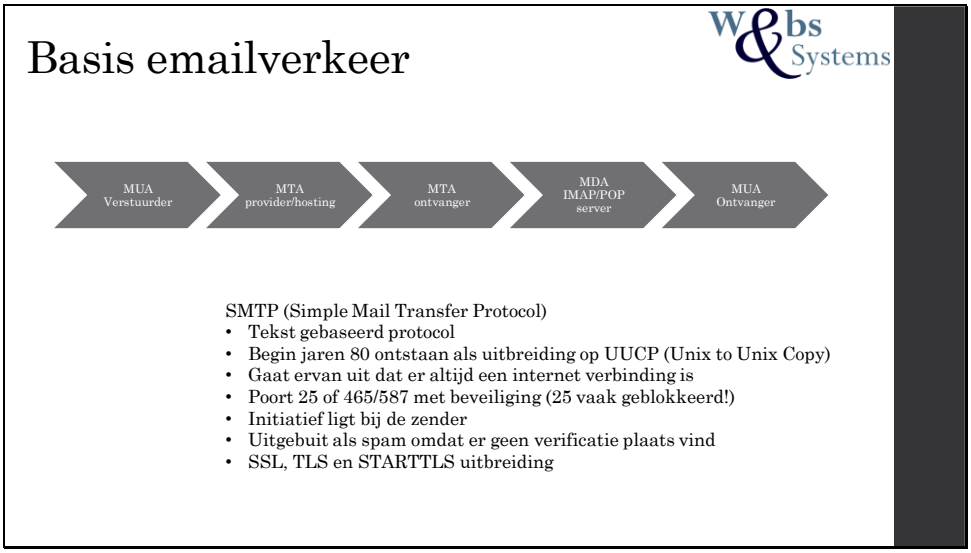
Webs en Systems focust op hosting van website voor de zzp en kleine onderneming. Door op maat gemaakte oplossing worden scherpe tarieven mogelijk gemaakt.
Ook verenigingen en non-porfit organisaties zijn welkom en genieten van een korting op de reeds lage prijzen.

Enkele activiteiten van WebsenSystems:
- Webhosting
- Domeinnamen
- Email delivery optimalisation
- Webdesign (Joomla! WP)
- Website editing
- SEO
- Custom programming
- Socialmedia promotion
- Training en Workshops
- Netwerk verbindingen
- Gasten netwerk
- Cloud opslag
- Netwerk opslag
- Server inrichting
- Storingsdienst lokaal
- Storingsdienst op afstand
- Onderhoud ICT systemen
- Wifi optimalisatie

https://websensystems.nl
info@websensystems.nl

Aan de rechterzijde zijn een aantal voorbeelden van websites uit het portofolio.
Van boven naar beneden:
https://wggt.nl (Wordpress)
https://volkstuinmalden.nl (Joomla!)
https://scoutinglangenboom.nl (Joomla!)
https://scoutingmalden.nl (Custom)
https://broodjesvanpauline.nl (Wordpress)

Dia 5



De basis taal waarmee emailberichten worden verstuurd is SMTP. Dit protocol is ook beschreven in de RFC definities.
(en) RFC 1869: Defines the capability for SMTP service extensions, creating Extended SMTP, or ESMTP
(en) RFC 1891: Delivery Status Notification (DSN) extension to SMTP
(en) RFC 5321: The Simple Mail Transfer Protocol; it consolidates, updates, and clarifies several previous documents
(en) RFC 2822: Internet (i.e. e-mail) Message Format, which obsoletes RFC 822
(en) RFC 4409: Message Submission for Mail

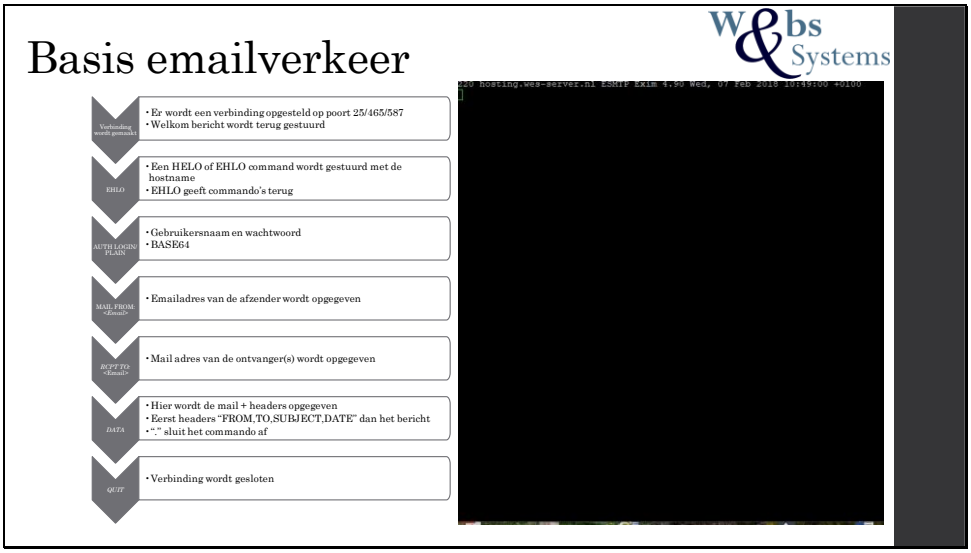
SMTP is een uitbreiding op de vroegere UUCP, en is in de basis nog weinig in gebruik. Door het gebrek aan authenticatie technieken is het basis protocol in de moderne wereld van SPAM ontoereikend geworden. Uitbreidingen op dit protocol worden nu gebruikt om uitbuiting tegen te gaan.

Een van de uitbreidingen is het versleutelen van de verbinding doormiddel van een TLS (of de vroegere SSL) certificaat. Om de beveiligde en onbeveiligde verbinding te scheiden wordt er gebruik gemaakt van 2 aparte poorten: 25 en 465. Omdat er van te voren niet bekend is of er een beveiligde verbinding met de server mogelijk is moet er eventueel van poort 25 naar 465 overgegaan worden en dus opnieuw een verbinding worden gestart. Hiervoor is STARTTLS in het leven geroepen. Dit commando zet de onbeveiligde verbinding naar het HELO of ELHO commando om naar een beveiligde verbinding. Om ook deze vorm van verbinding uit te filteren is poort 587 erbij gekomen. Doorgaans wordt tegenwoordig poort 25 door veel providers al geblokkeerd, dit omdat dit potentiele verbindingen zijn voor het versturen van SPAM.

Verzending van een email bericht verloopt over een aantal programma's. Deze zijn op de sheet weergegeven. De afkortingen worden hieronder verklaard.

MUA: Mail user Agent (Outlook, incredimail ed.) = POP/IMAP/SMTP Client
MTA: Mail Transfer Agent (EXIM, PostFix ed.) = SMTP Server
MDA: Mail Delivery Agent (Dovecot, Cyrus IMAP ed) = IMAP/POP Server

Dia 6



SMTP verbining is een text commando (en eventueel antwoord) gebaseerde verbinding.
In de onderstaande toelichting gebruik ik S voor de ontvangende server en C voor de versturende server/client.

Na het verbinding reageert S met een welkomsbericht.
C verstuurd hierop een HELO of EHLO commando met zijn eigen hostnaam.
HELO is een oudere versie welke alleen een bevestiging als reactie oproep. EHLO wordt beantwoord met een lijst van mogelijke COMMANDO's.

Hiernaar wordt tegenwoordig het STARTTLS commando door C gegeven. Hiermee wordt het protocol gestart (Indien door S ondersteund) om de verbinding te beveiligen.

Met de uitbreiding op het basis SMTP protocol verstuurd C nu het AUTH PLAIN/LOGIN naar S. Hiermee wordt het protocol gestart om in te loggen als een gebruiker van de server. Vroeger was dit niet nodig. Waardoor veel servers bloot lagen om SPAM te versturen. Tegenwoordig is dit bij bijna alle servers een verplichting.
Bij LOGIN reageert S met een in BASE64 gecodeerde vraag naar het gebruikersnaam. Deze wordt door C beantwoord met de in BASE64 encoded gebruikersnaam.
Hiernaar volgt op dezelfde wijze het wachtwoord.
Bij een AUTH PLAIN wordt er geen reactie gegeven door de server en worden gebruikersnaam en wachtwoord in BASE64 encoded op de zelfde regel meegestuurd.

Hiernaar volgen de commando's MAIL FROM: <..>, RPCT TO: <..> en DATA door C.
Deze geven de zender, ontvanger en inhoud van het bericht aan. DATA wordt afgesloten met een "." op een lege regel. In DATA worden datum, ontvanger, zender en onderwerp vermeld, gevolgd door een lege regel en dan de inhoud van het bericht.

De sessie wordt afgesloten met een QUIT.

Binnen een sessie kunnen meerdere berichten worden verstuurd of aan meerdere ontvangers een bericht. Moderne servers stellen hier echter wel limieten aan. Veel MUA sturen 1 bericht per sessie. Voor 50 mails wordt er dus 50 keer een verbinding opgesteld.

Het filmpje laat een live sessie zien. Hierin is ook de vertraging op te merken voor het antwoord van de server. Dit heeft te maken dat er met ieder commando scripts worden gedraaid die authenticatie en autorisatie controleren.

Dia 7

Email headers zijn een eerste bron om SPAM problemen te analyseren. Hierin kunnen we regels terug vinden die door de ontvangende server zijn toegevoegd naar dat deze het bericht heeft beoordeeld.
Bijna iedere MUA ondersteund de functie voor het opvragen hiervan.
Outlook: Open het bericht in een pop-up venster. Ga naar bestand > TAB info > eigenschappen. Onderin het verschijnende venster staan internetheaders.
GMAIL: na het openen van het bericht > rechtsboven het pijltje naar beneden > Origineel weergeven.

Analyseren van deze headers wordt ons makkelijker gemaakt door MXToolbox.com. Zijn hebben een test waarbij de headers worden geanalyseerd (https://mxtoolbox.com/EmailHeaders.aspx).

Het verkrijgen van headers vraagt wel enige hulp van de ontvangers. Zij moeten of het bericht als bijlage toevoegen of de headers opzoeken en kopiëren in het bericht. Een doorgestuurd bericht bevat niet de headers die wij nodig hebben.

Uit de headers is ook op te halen welke "route" het bericht heeft afgelegd. Ook is de zendende bron te achterhalen. Hiermee kunnen ook verdachten berichten worden onderzocht en specifieke ip adressen worden uitgefilterd.

In de mail headers vinden we ook de List en Precedent opties. Deze worden door onder meer google gewenst om bulk berichten doorgang te bieden naar de inboxen van haar gebruikers.

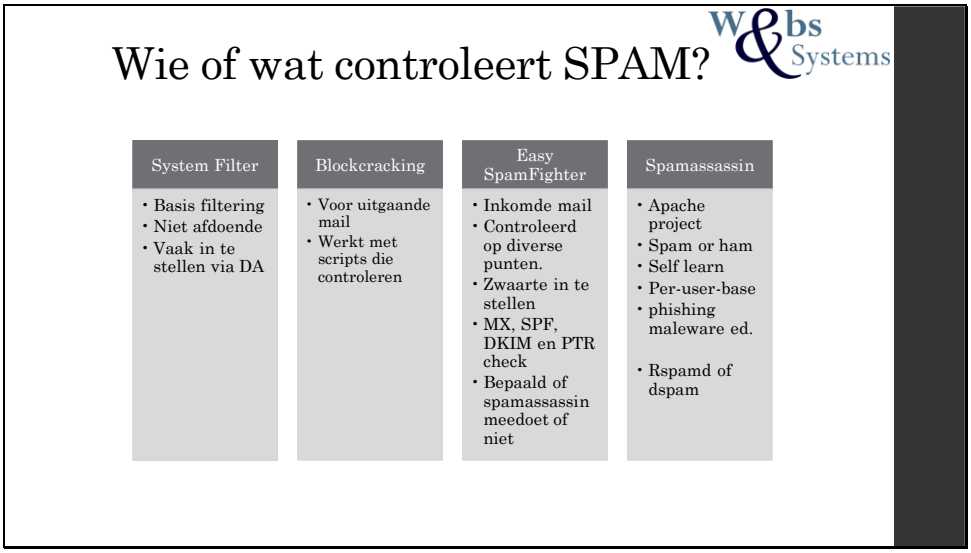
Dia 8

Wikipedia:
Oorspronkelijk was spam de merknaam van een bepaald soort ingeblikt vlees dat nog steeds bestaat en dat in Nederland bekendstaat onder de naam Smac. De Britse komieken van Monty Python gebruikten het in een sketch om het toen actuele verbod op 'unsolicited advertising' (sluikreclame) op televisie aan de kaak te stellen. In een lunchroom waar aan alle gerechten ongevraagd spam werd toegevoegd, en waarin een groepje Vikingen uit volle borst zingt: "*Spam spam spam spam. Lovely spam! Wonderful spam!*", werd normale conversatie door de spam-zangers vrijwel onmogelijk gemaakt, net als bij ongevraagde e-mail. Ook bij de aftiteling werd te pas en te onpas het woordje "spam" vermeld. Monty Python liet daarmee zien dat de wellicht wenselijke restricties aan reclame-uitingen op gespannen voet staan met het recht op vrije meningsuiting. In de latere e-mail-spamdebatten deden e-mailmarketeers ook vaak een beroep op het recht op vrije meningsuiting.
Wikipedia spamfilter
Als tegenhanger van de bekende term *spam* wordt sinds kort in kleine kring de term *ham* gebruikt.[bron?] Dit is de *goede kwaliteit* vlees als tegenhanger van de *slechte kwaliteit*van spam. *Ham* is alle e-mail die geen *spam* is. Het is niet noodzakelijkerwijs e-mail die de ontvanger wil ontvangen of waar de ontvanger om gevraagd heeft. Deze term wordt op dit moment in diverse spamfilterpakketten toegepast, veelal bij een techniek waarbij de ontvanger onderscheid kan maken tussen ham en spam om de filter zelflerend te maken.
SPAM is een geregistreerd handelsmerk van Hormel Foods Corporation, maar het woord *spam* is zo gebruikelijk geworden dat het niet langer door het merkenrecht beschermd wordt.

In de lijst zijn de veel voorkomende punten benoemd waarop berichten en verzenders worden beoordeeld om te bepalen of een bericht naar de inbox, spambox of ongelezen retour gaat.

Zijn de SPF, DMARC, DKIM en PTR records aanwezig?
Hoeveel berichten worden er verstuurd per tijdseenheid?
Is er gebruik gemaakt van TLS?
Hoeveel berichten zijn er in het verleden als SPAM aangemerkt van de verzender?
Hoeveel geadresseerde bestaan er niet?
Hoeveel linkjes werken er niet in de inhoud van het bericht?
Hoe is de balans tussen afbeeldingen en tekst? Natuurlijk of geforceerd?
Hoe is de reputatie van het Ip adres en van de domainnaam?
Zijn er opties opgenomen zoals vermeld op de vorige sheet?

Dia 9



SPAM wordt op de MTA op diverse lagen beoordeeld door verschillend programma's (eigenlijk scripts geschreven in C of Python).

Systeem filter komt ook voor bij de MUA. Deze zijn simpele instellingen die door een gebruiker kunnen worden gemaakt. Bijvoorbeeld: Een domeinnaam of email adres waarvan wel of niet de berichten binnen mogen komen. In DirectAdmin is dit in te stellen bij het email menu per domeinnaam.

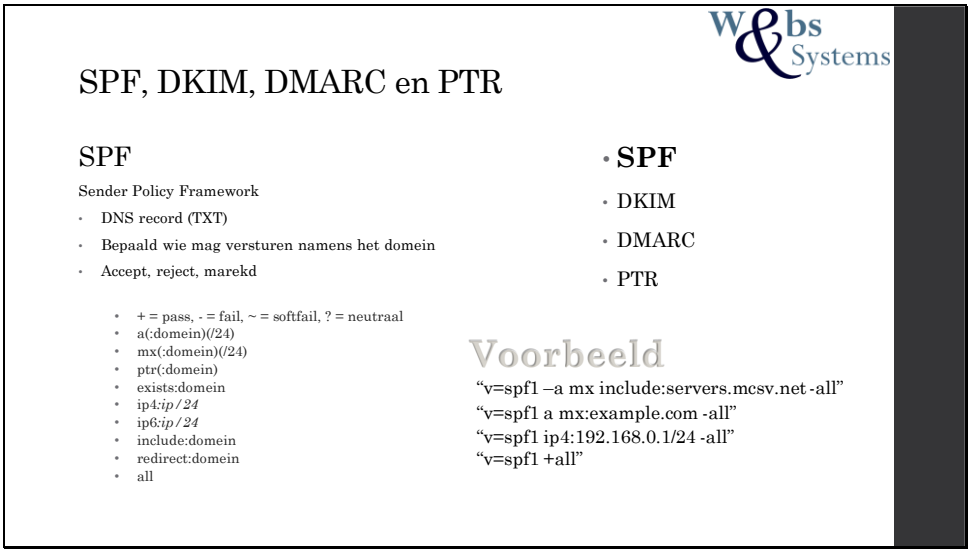
Blockcracker maakt gebruik van scripts om te beoordelen of bepaalde tekenreeksen voor komen. Deze worden per SPAM invasie geschreven om specifieke berichten tegen te kunnen houden.

ESF heeft een aantal regels waar wel of niet aan voldaan kan worden. Iedere regel kent een bepaalde weegfactor waarmee een totaal score wordt bepaald. Is deze boven het limiet wordt het bericht als SPAM gemerkt. Zit deze onder het limiet kan Spamassassin nog worden aangeroepen. Deze werkt doormiddel van een zelflerend algoritme waarmee het het bericht beoordeeld. Vind Spamassassin dat dit bericht SPAM is dan wordt er een extra aantal punten opgeteld bij ESF. Het daadwerkelijk verplaatsen van het bericht naar de SPAM box gebeurd door de MTA.

https://mirrors.thzhost.com/directadmin/services/custombuild/easy_spam_fighter/README.html

https://rspamd.com/comparison.html

Dia 10



SPF is een DNS record welke gebruikt wordt om aan te geven welke servers er mogen zenden namens het domein.
Doormiddel van opties (+,-,~ en ?) kan de actie worden bepaald.
Pass wil zeggen dat de zender wel mag zenden
Softfail wil zeggen dat het eigelijk niet mag maar het bericht naar de spambox zou mogen.
Fail wil zeggen dat het niet mag en het bericht geblokeerd moet worden.
Neutraal wil zeggen dat er geen oordeel wordt gegeven. Dit resulteerd meestal in het accepteren van het bericht.

Voor een diepe toelichting op de opties:
http://www.openspf.org/

Met een a en mx kan een domein worden opgegeven. Zonder domeinnaam wordt het domein in het zender adres gebruikt.
Van het domein wordt het ip adres opgehaald (indien mogelijk ip6) en vergeleken met de zender.

De include zorgt voor het invoegen van spf records van een ander domein.

Afsluitend wordt er altijd een all gedefineerd. Deze geeft aan wat er gedaan moeten worden als de voorgaande opties geen match zijn.

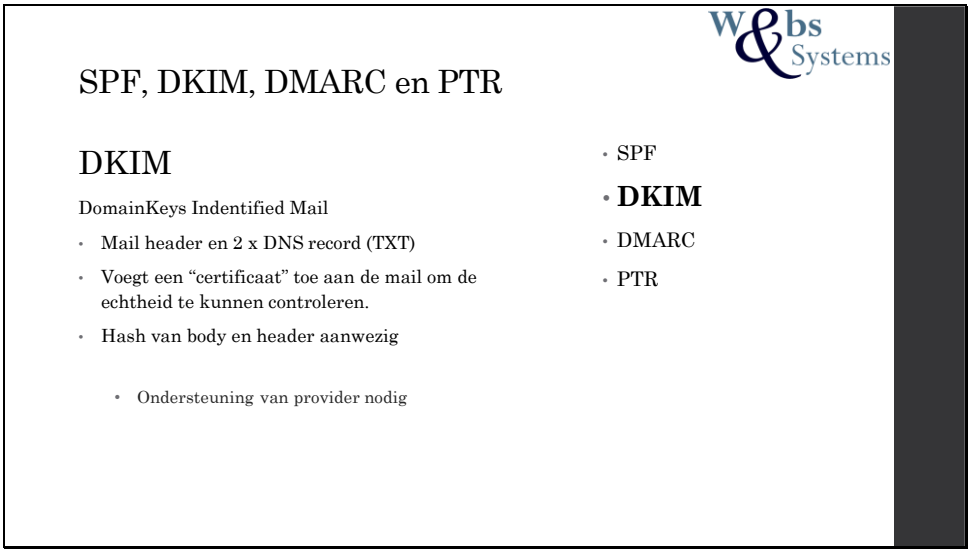
De voorbeelden:
Het eerste voorbeeld geeft aan dat het A record (meestal het ip van de webserver) geen berichten mag versturen. De MX daarin tegen wel. Ook worden de SPF records van MCSV.net (mailchimp) opgenomen, waarmee de toegestaande servers van MCSV ook door ons worden toegelaten. Als laatste mogen er geen andere servers versturen.

Het 2de voorbeeld laat toe dat er mail verstuurd wordt van het A record en van het MX record van example.com. Als laatste mogen er geen andere servers versturen.

Het 3de voorbeeld laat een intern netwerk zien waarbij de gehele iprange 192.168.0.0 – 192.168.0.255 toegestaan wordt mail te versturen. Dit kan het geval zijn bij een mailcluster. Ook hier worden andere servers niet toegestaan.

Het 4de voorbeeld is een bijzondere. Deze heeft het doel van SPF niet geheel begrepen en laat alle servers toe mail namens het domein te verzenden.

Dia 11



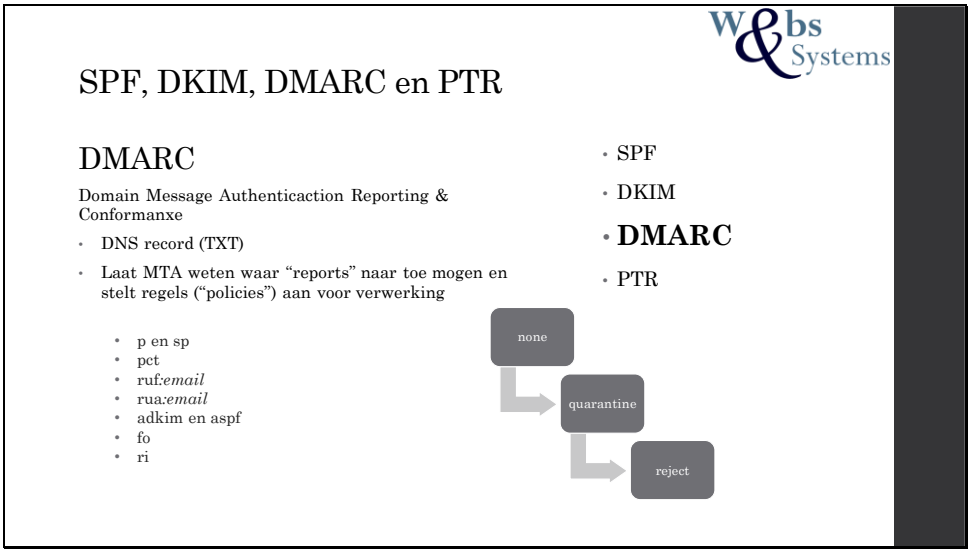
Met DKIM kunnen we de inhoud van het bericht "verzegelen". Als het ware kunnen we de middeleeuwse kaarsvet stempel gebruiken om te laten zien dat het bericht niet geopend is. Deze instelling maakt gebruik van een public en private key welke door de server moeten worden gegenereerd. Als je hosting dit dus niet ondersteund, moet je overstappen om dit toe te passen.

Wanneer het bericht verstuurd wordt, berekend de versturende server een hash bestaande uit elementen uit het header gedeelte van het bericht (Deze staan benoemd in de mailheader), en van de inhoud van het bericht. Deze elementen worden beschermt tegen het aanpassen onderweg.
Voor dat het bericht verzonden wordt worden de hashes versleuteld met de privatekey.

De ontvanger vraagt doormiddel van de selector en het domeinnaam vernoemd in de DKIM-signatuur in de mailheader de public key op (DNS record). Doormiddel van deze key ontcijferd hij de hashes.
Vervolgens maakt hij zelf ook hashes van het bericht en de geselecteerde headers. Deze vergelijkt hij met de hashes die ontcijfert zijn.

Als deze overeenkomen betekend dit dat het bericht origineel is en afkomstig is van de echter zender. Een kant tekening hierbij is het dns "kapen" waarbij een dns zone wordt nagebootst. Dit kan worden opgevangen met DNSSEC. Maar dat ligt buiten de scoop van deze cursus.

Dia 12



DMARC stelt regels voor ontvangende servers op, voor het omgaan met berichten afkomstig van het domein.
Bij het ontvangen van een bericht wordt doormiddel van een DNS request de dmarc record op gehaald.

De SPF en DKIM worden gevalideerd en de uitkomst hiervan wordt behandeld zoals opgegeven in de dmarc record.

Voorbeeld:
v=DMARC1; fo=1; ri=604800; p=reject; sp=reject; adkim=s; aspf=s; rua=mailto:spam-reports@domein.nl; ruf=mailto:spam-reports@domein.nl

fo=* => 0 = DKIM & SPF; 1 = DKIM of SPF; s = SPF; d = DKIM
ri=* => Raport interval in seconden
p=* => none, quarantine, reject
sp=* => zelfde als p alleen voor subdomains
adkim=* => s=strict r=relaxed; r toestaan verschil in subdomain
aspf=* => s=strict r=relaxed; r toestaan verschil in subdomain
rua=* => mailadres voor reject raports
ruf=* => mailadres voor forensics raports
pct=* => Percentage van de berichten welke volgens policys worden behandeld

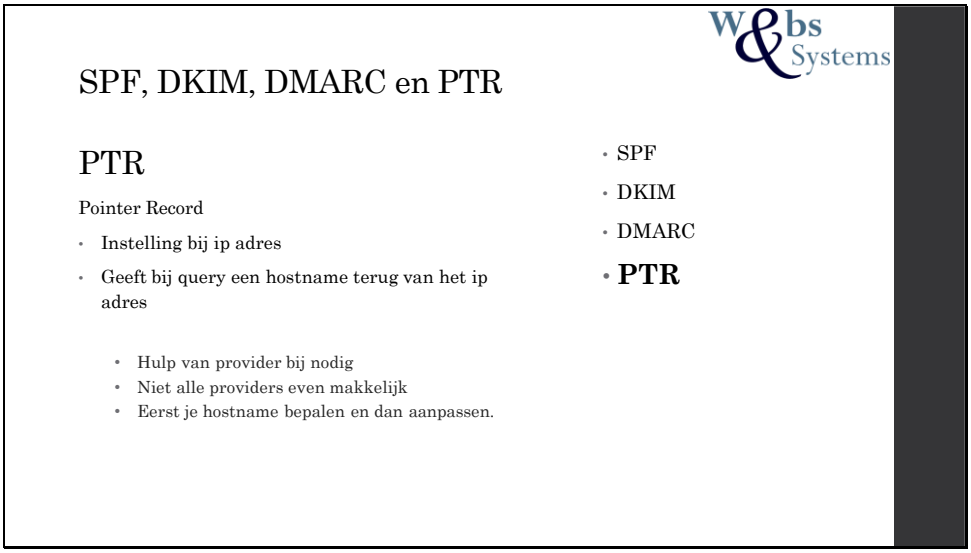
Een standaard werkwijze is om te beginnen met p=none, prt=100.
Hiermee wordt er alleen maar gemonitort. Je ontvangt berichten met de uitkomst van SPF en DKIM met de sendende ipadressen.

Hiernaar kan er overgegaan worden naar p=quarantine pct=10

Nu worden 10% van de berichten in de spam box gezet welke niet aan spf of dkim voldoen. Hierbij wordt het pct langzaam opgebouwd.

De laatste stap is p=reject pct=10.
Nu worden 10% van de berichten geweigert welke niet aan spf of dkim voldoen. Hierbij wordt het pct langzaam opgebouwd.

Dia 13



PTR is een speciale DNS Record.

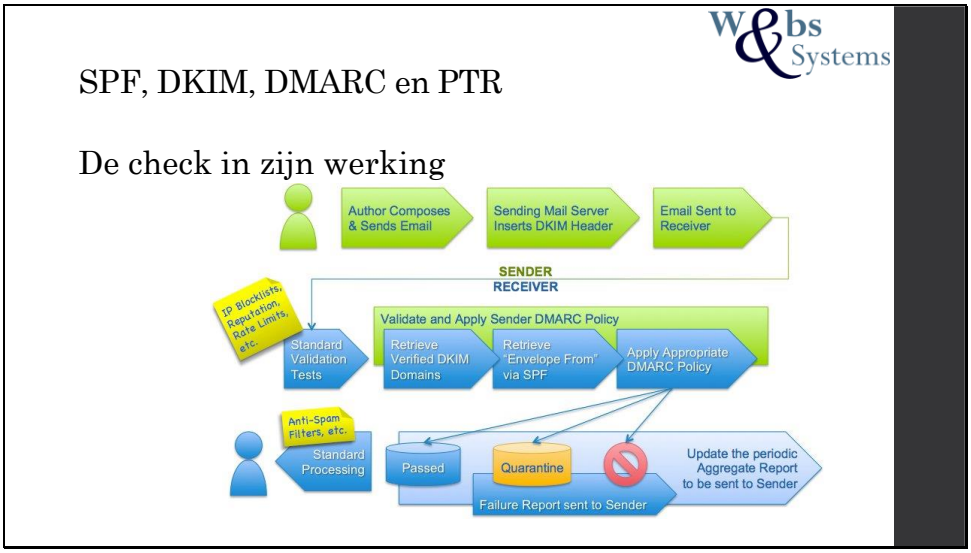
Normale wijs worden domeinnamen in een DNS server aan een ip adres gehangen. Bij een PTR werkt dit andersom. Hier worden ip adressen aan hostnamen gekoppeld.
Een PTR record is dan ook niet op de local DNS server aanwezig maar staat op hiervoor ingerichte root DNS servers.

Tijdens het SMTP commando wordt de hostname meegegeven in het EHLO commando. Op deze hostname wordt een DNS request uitgevoerd. Op het verkregen IP adres wordt een PTR request uitgevoerd. De verkregen hostname moet weer overeen komen.

Na het DATA commando wordt nogmaals een PTR check uitgevoerd. Echter nu op de hostname in het from veld.

PTR record is dus een server gerelateerde instelling. Dit moet jouw provider al hebben ingesteld.

Dia 14



Hier een schema wanneer welke controles worden uitgevoerd.

Hierbij is ook het traject van dmarc te herkennen.

Dia 15

Een van de tools om je instellingen mee te testen is Mxtoolbox.com. Zij bieden een grote hoeveelheid aan testen aan om je records mee te testen.
Ook is het mogelijk hierin email berichten te analyseren.

Dia 16

Mail-tester.com kan gebruikt worden om een inschatting te maken hoe het bericht wat je wilt versturen wordt beoordeeld.

Naar een door mail-tester.com gegenereerde mail adres stuur je het complete bericht toe. Naar enkele minuten krijg je een score te zien met daaronder de verbeter punten voor je mail.

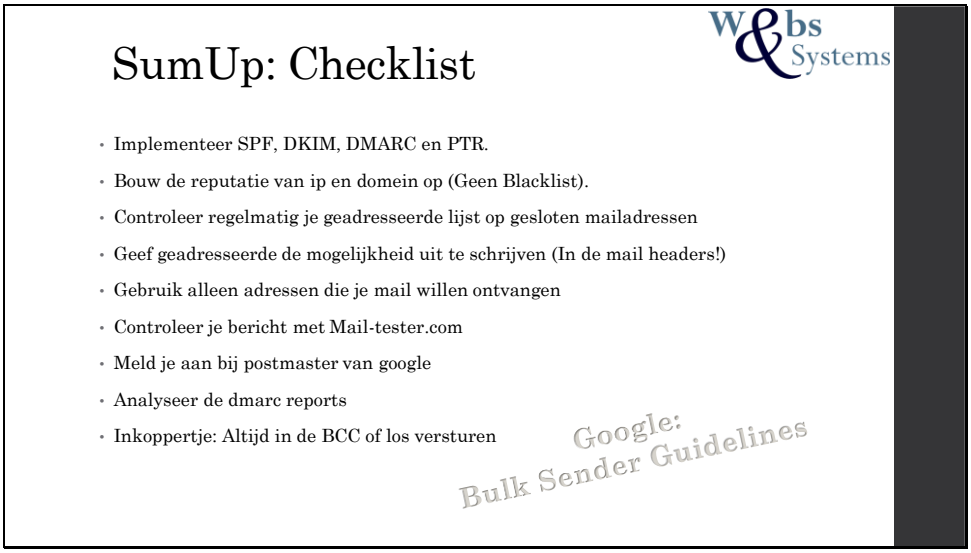
Ons advies om deze tool regelmatig te gebruik voor het versturen van bulkmail.

Dia 17

Google postmaster is een tool vanuit google.
Voor bulk senders (+1000 mails per maand) kunnen er gegevens worden gegenereerd hoe berichten zijn ontvangen.
Hieruit is bijvoorbeeld op te halen wat de IP en domein reputatie zijn, hoe vaak mail naar een spambox is gezet enz.

Aanmelden geschied met een google account. Domeinnamen moeten worden geverifieerd met een DNS record.

Dia 18



Google Bulk Sender Guidelines: https://support.google.com/mail/answer/81126?hl=nl

Hier een opsomming of checklist voor het netjes verzenden van mail. Hoeveel kan jij er afvinken?

De BSG van google geven heel netjes en overzichtelijk aan wat hun verwachten van een massa verstuurder. Deze is erg handig om een keer door te lezen.

Dia 19

Hulp nodig?

Https://websensystems.nl
info@websensystems.nl