WebbMotell - ISPConfig

E-postautentisering och få ut värdet av en DMARC-policy

Inledning

För företag av alla storlekar är e-post en viktig del av infrastrukturen som stöder stora mängder kommunikation. För att förbättra säkerheten och pålitligheten för e-postkommunikation vänder sig många organisationer till e-postleverantörer (ESP) som webbmotell.se. Dessa ESP:er tillåter användare att skicka autentiserade e-postmeddelanden från sina domäner, genom att använda industristandardprotokoll som Sender Policy Framework (**SPF**) och DomainKeys Identified Mail (**DKIM**). Meddelanden som autentiserats med SPF eller DKIM kommer att klara din domäns policy för domänbaserad meddelandeautentisering, rapportering och överensstämmelse (**DMARC**).

Den här artikeln kommer att fokusera på DMARC:s policytillämpningsmekanism. Artikeln kommer att utforska några av anledningarna till att e-post kan misslyckas med DMARC-policyutvärderingen och föreslå lösningar för att åtgärda eventuella fel som du identifierar.

För en introduktion till DMARC och hur du noggrant väljer din e-postsändande domänidentitet. DMARC-efterlevnad är kritiskt för e-postleverans och är avgörande för organisationer som strävar efter att upprätthålla ett positivt avsändarrykte och säkerställa framgångsrik e-postleverans.

Det finns många fördelar när organisationer har denna korrekta inställning, dessa inkluderar:

- Förbättrad e-postleverans
- Minskad risk för att bli utsatt för e-postförfalskning och nätfiske
- Positivt avsändarrykte
- Minskad risk för att skickad e-post hamnar i mottagarens skräpkorg
- Ert "Brands" rykte.

Utifrån detta, låt oss utforska komplexiteten med DMARC och hur det kan gynna din organisations e-postkommunikation.

Vad är DMARC?

DMARC är en mekanism för domänägare att publisera SPF- och DKIM-skydd och berätta för mottagare hur de ska agera om dessa autentiseringsmetoder misslyckas.

Domänens DMARC-policy skyddar din domän från tredje part som försöker förfalska domänen i e-postheadern **"From:"** i e-postmeddelanden. Skadliga e-postmeddelanden som syftar till att skicka nätfiskeförsök med din domän kommer att bli föremål för en DMARC-policyutvärdering, vilket kan leda till att de sätts i

karantän eller avvisas av den e-postmottagande organisationen. Denna strikta policy säkerställer att e-postmeddelanden som tas emot av e-postmottagare verkligen kommer från den påstådda sändningsdomänen, vilket minimerar risken för att människor faller offer för e-postbaserade bedrägerier.

Domänägare publicerar DMARC-policyer som en TXT-post i domänens _dmarc.<domain> DNS-post. Till exempel, om domänen som används i **"From:"-**rubriken är exempel.se, så skulle domänens DMARC-policy finnas i en DNS TXT-post med namnet _dmarc.exempel.se. DMARC-policyn kan ha ett av tre policylägen:

- En typisk DMARC-distribution av en befintlig domän börjar med att publicera **"p=none".** En ingen-policy betyder att domänägaren befinner sig i en övervakningsfas; domänägaren övervakar meddelanden som inte är autentiserade med SPF och DKIM och försöker se till att all e-post är korrekt autentiserad

- När domänägaren är säker på att alla legitima användningsfall är korrekt autentiserade med SPF och/eller DKIM, kan de ändra DMARC-policy till **"p=quarantine"**. En karantänpolicy innebär att meddelanden som misslyckas med att skapa en domänjusterad autentiserad identifierare via SPF eller DKIM kommer att sättas i karantän av den e-postmottagande organisationen. Den e-postmottagande organisationen kan filtrera dessa meddelanden i skräppostmappar eller vidta en annan åtgärd som de anser bäst skyddar sina mottagare.

- Slutligen kan domänägare som är övertygade om att alla legitima meddelanden som använder deras domän är autentiserade med SPF eller DKIM ändra DMARC-policyn till **"p=reject"**. En avvisningspolicy innebär att meddelanden som misslyckas med att skapa en domänjusterad autentiserad identifierare via SPF eller DKIM kommer att avvisas av den e-postmottagande organisationen.

Följande är exempel på en TXT-post som innehåller en DMARC-policy, beroende på önskad policy (p-taggen):

	Name	Type
1	_dmarc.exempel.se	TXT
2	_dmarc.exempel.se	TXT
3	_dmarc.exempel.se	TXT

Tabell 1 – Exempel DMARC policy

Denna policy säger åt e-postleverantörer att tillämpa DMARC-policyn på

meddelanden som inte skapar en DKIM- eller SPF-autentiserad identifierare som är anpassad till domänen i "From"-huvudet. Justering innebär att en eller båda av följande inträffar:

- Meddelanden passerar SPF-policyn för MAIL FROM-domänen och MAIL FROM-domänen är densamma som domänen i "From"-huvudet, eller en underdomän av denna.
- Meddelanden har en DKIM-signatur signerad av en offentlig nyckel i DNS på en plats inom domänen för "From:"-huvudet.

DMARC-rapportering

Rua-taggen i domänens DMARC-policy anger platsen dit e-postmottagande organisationer ska skicka sammanställda rapporter om meddelanden som godkänner eller misslyckas med SPF- och DKIM-anpassning. I regel är detta en e-postadress, typ **rua=mailto:dmarcreports@exempel.se.**

Domänägare, dmarcreports@exempel.se i detta exempel, analyserar dessa rapporter för att upptäcka meddelanden som använder domänen i **"From:"** -huvudet men som inte är korrekt autentiserade med SPF eller DKIM. Domänägaren kommer att försöka säkerställa att alla legitima meddelanden autentiseras genom analys av DMARC:s samlade rapporter över tid.

E-postmottagande organisationer som stöder att skicka DMARC-rapporter skickar vanligtvis dessa sammanställda rapporter en gång om dagen, även om dessa metoder skiljer sig från leverantör till leverantör.

Vad skall man typiskt göra för implementera DMARC framgångsrikt?

I ett nötskal:

- Se till att alla e-postmeddelanden som använder domänen i "**From:"**-huvudet autentiseras med **DKIM**- och **SPF**-domänjusterade identifierare. Fokusera på **DKIM** som det primära sättet för autentisering.
- Publicera en **DMARC**-policy (none, quarantine, eller reject) för domänen som återspeglar hur domänägaren vill att e-postmottagande organisationer ska hantera oautentiserad e-post som påstår sig vara från deras domän.

Nya domäner och underdomäner

Det är enkelt att implementera DMARC för domäner och subdomäner som aldrig använts för e-post. Man har ingen ryggsäck här att ta hänsyn till.

Dessa domäner kan börja direkt med **"p=reject"** DMARC-tillämpningspolicy eftersom policyn inte kommer att påverka befintliga program för att skicka e-post. Denna strikta tillämpning är till för att säkerställa att det inte finns någon oautentiserad användning av domänen och dess underdomäner.

Befintliga domäner

Domäner, och subdomäner, som redan används för e-post, där är det lite trickigare. Problemet här är att få kolla på hur domänen används för att skicka e-post, vilka organisationer använder den, vilka hemsidor och program använder den, och när de använder den, vilka e-postservrar skickar de igenom, och så vidare.

För dessa är en DMARC-implemtentering en iterativ process. Det är viktigt att få en fullständig förståelse för hur domänen och dess underdomäner används för e-postsändning innan du publicear en restriktiv DMARC-policy (**p=quarantine** eller **p=reject**).

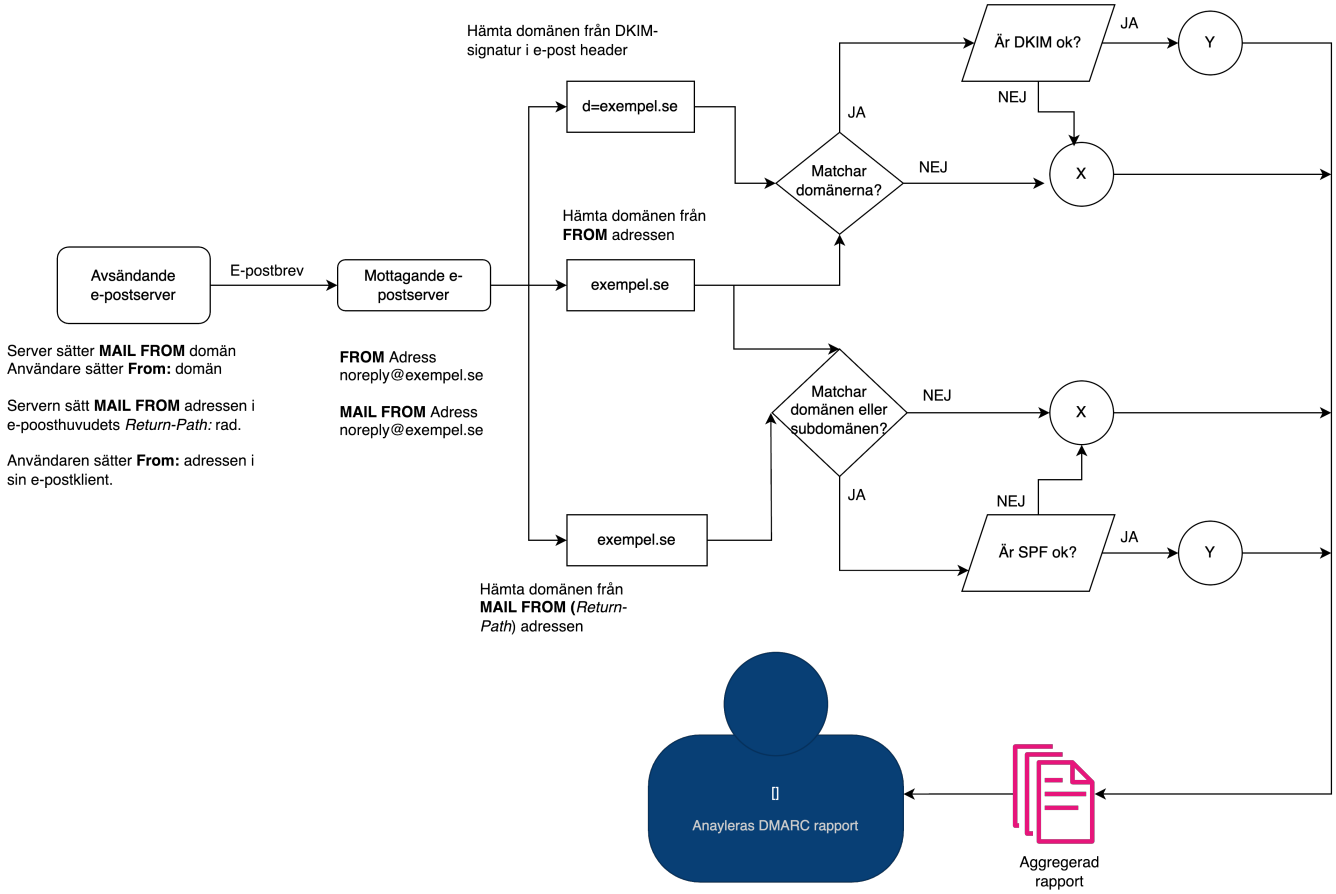
För att komma igång med DMARC-implementeringen är det här några åtgärder att vidta:

1. Publicera en **p=none** DMARC-policy (ibland kallad övervakningsläge) och ställ in rua-taggen till den mottagre där du vill ta emot samlade rapporter.
2. Analysera de samlade rapporterna. E-postmottagande organisationer skickar rapporter som innehåller information för att avgöra om domänen och dess underdomäner används för att skicka e-post och hur meddelandena autentiseras (eller inte) med en DKIM- eller SPF-domänjusterad identifierare. Ett lättanvänt analysverktyg är Dmarcian XML to Human Converter.
3. Undvik att publicera en **"p=quarantine"**- eller **"p=reject"**-policy i förtid. Om du gör det kan det leda till blockerad eller minskad leverans av legitima meddelanden från befintliga e-postprogram.

Ett alternativ att börja använda DMARC på en befintlig domän är att skapa en helt ny subdomän och använda denna för att skicka e-post. Denna är då "ren" och man kan vara säker på att den uppfyller en restriktiv DMARC och mail från denna kommer att komma fram. "Ryggsäcken" får man hantera med en ingen-policy under en period.

Överhuvudtaget är det en mycket bra ide att skapa separata subdomäner för massutskick av mail. Dessa riskerar i mycket större omfattning att bli "skitiga" och när de väl blir det, påverkar det inte den ordinarie domänen som organsiationen skickar vanlig mail med.

Bilden nedan illustrerar hur DMARC kommer att tillämpas på ett e-postmeddelande som tas emot av den e-postmottagande servern och åtgärder som vidtas baserat på tillämpningspolicyn:



För att DMARC skall uppfyllas hos den mottande e-postservern måste båda resultaten ovan vara **Y**.

Hur får SPF och DKIM DMARC att uppfyllas?

Hur SPF lever upp till DMARC

När du skickar ett e-postmeddelanden sätts automatiskt av e-post servern en **MAIL FROM** adress genom att sätta ett e-posthuvud **Return-Path**. Denna kan se ut så här:

```
Return-Path: <kalle@exempel.se>
```

När man skall skicka e-post måste man autentisera sig. Det gör man med sin e-postadress och lösenordet till denna (i regel). I detta exempel är det **kalle@exempel.se** som autentiserat sig. E-postservern vet då att det är just det här e-postkontot som skickar brevet. Denna rad är inte något som man som användare kan påverka, det är servern som sätter den. Till skillnad till **From:** raden i e-posthuvudet som användaren kan sätta till vad som helst i sin e-postklient. Så, **MAIL FROM** kan man lita på, men inte på **From:**.

När den mottagande e-postservern skall utvärdera SPF tittar den på den SPF policy som **MAIL FROM** domänen (exempel.se i detta exempel) har. Denna skall då

innehålla den avsändande e-postserver, dess IP-adress mer specifikt. Stämmer det, då får man "SPF=PASS".

Utöver "SPF=PASS" kräver **DMARC** att **MAIL FROM** domänen och **From:** domänen hör ihop, dvs att de antingen är desamma eller att **MAIL FROM** är en subdomän till **From:** domänen. Det sistnämnda fungerar endast om **DMARC** innehåller direktivet **aspf=r**, vilket är standardinställning om man inte anger den alls. **r** står här för relaxed.

Hur DKIM lever upp till DMARC

Två kriterier:

1. Att DKIM aktiverats för er domän. Detta är något ert webbhotell gör. Med ISPConfig kan användaren gör det själv, har man bara tillgång till den Enkla kontrollpanelen behöver man kontakta support.
2. Att man **alltid** skickar mail via sin **mailserver** hos webbhotellet. Detta är särskilt viktigt att tänka på när man skickar e-post från sin hemsida, t.ex. om man använder WordPress. Som standard skickar dessa e-post genom webbservern, och då kommer inte DKIM vara uppfyllt.

DMARC ställer dock ytterligare ett krav på **DKIM**, vilket också framgår av bilden ovan. **MAIL FROM** domänen måste vara samma som den är i **"d="** taggen i **DKIM**-signaturen som finns i själva e-postbrevet.

DKIM och SPF tillsammans

E-postmeddelanden är helt autentiserade när meddelandena passerar både DKIM och SPF, och både DKIM- och SPF-autentiserade identifierare är domänjusterade, dvs att de angivna domänerna stämmer överens enligt bilden ovan.

Om endast DKIM är domänjusterat, kommer meddelandena fortfarande att passera DMARC-policyn, även om SPF "pass" är ojusterat. E-postmottagare kommer att ta hänsyn till hela sammanhanget för SPF och DKIM när de avgör hur de kommer att hantera dispositionen av meddelandena du skickar, så det är bäst att fullständigt autentisera dina meddelanden när det är möjligt.

Google har satt som krav att antingen DKIM eller SPF skall vara uppfyllt för att brev överhuvudtaget skall tas emot. Här behöver de inte vara domänjusterade. Dock, om någon av dessa fallerar, då är det sannolikt att brevet tas emot, men hamnar i mottagarens skräpkorg.

Skickar man stora mängder mail till Google gmail adresser, då kräver Google att DMARC uppfylls fullt ut för att ta emot mailet.

Webbhotellet förenklar i regel denna process väsentligt, genom att kunna göra det genom några klick.

Varför misslyckas DMARC?

Det finns tillfällen då du kanske märker att meddelanden misslyckas med **DMARC**, oavsett om dina meddelanden är helt autentiserade eller delvis autentiserade. Följande är saker du bör hålla utkik efter:

Ändring av e-postinnehåll Ibland ändras e-postinnehåll under leveransen till mottagarnas e-postservrar.

Denna ändring kan vara ett resultat av en säkerhetsanordning eller anti-spam-agent längs leveransvägen (till exempel: meddelandet Ämne kan ändras med en "[EXTERN]"-varning till mottagarna). Det modifierade meddelandet ogiltigförklarar DKIM-signaturen vilket orsakar ett DKIM-fel. Kom ihåg att syftet med DKIM är att säkerställa att innehållet i ett e-postmeddelande inte har manipulerats under leveransprocessen. Om detta händer kommer DKIM-autentiseringen att misslyckas med ett autentiseringsfel som liknar "DKIM-signature body hash not verified".

Lösningar:

- Om du har full kontroll över hela vägen som e-postmeddelandet kommer att passera från avsändare till mottagare, se till att ingen e-postserver emellan ändrar e-postinnehållet under överföring.
- Sätt DMARC-policyn i övervakningsläge **(p=none)** tills dessa problem har identifierats/lösts.

Vidarebefordran av e-post

Vidarebefodran av e-post är ett stort problem att få att fungera med SPF/DKIM/DMARC. Med policies som Google har är det högst osäkert om vidarebefodrad e-post verkligen kommer fram till ens gmail-adress, och gör det väl det, då hamnar det i skräpposten.

Det är inte ovanligt att ett meddelande som vidarebefordras, resulterar i att både/antingen SPF och DKIM misslyckas med att skapa en domänjusterad autentiserad identifierare. För SPF betyder det att e-postservern för vidarebefordran inte är listad i MAIL FROM-domänens SPF-policy.

Det är möjligt för en e-postserver för vidarebefordran att undvika SPF-fel och ta ansvar för e-posthanteringen för de meddelanden den vidarebefordrar genom att skriva om MAIL FROM-adressen så att den ligger i den domän som kontrolleras av vidarebefordranservern. Vidarebefordran av servrar som inte skriver om MAIL FROM-adressen utgör en risk för identitetsattacker och nätfiske. **Å andra sidan, om e-postservern gör denna ändring i meddelandet, då kommer DKIM att fallera.** Det har utarbetats olika lösningar för att lösa detta, men ingen av dessa är tillräckligt robusta. Slutsatsen är helt enkelt att man inte skall använda sig av vidarebefodran. Gör man det ändå, då får man ta eget ansvar för det, e-postleverantören kan inte lösa det problemet.

Skickar e-post från sin webbsida

Detta är något som ofta glöms bort. Mail som skickas från en webbsida kan t.ex.

vara beställningsinformation, fakturor, supportärenden osv. Om man använder de standardfunktioner som ofta finns i olika program, då kommer man att skicka e-post som inte uppfyller DMARC. Man riskerar också att SPF och DKIM fallerar, och då kommer inte den e-post man skickar komma fram till t.ex. Google Gmail.

Här måste man se till att man konfigurerar sin hemsida att skicka e-post på rätt sätt. Läs mer om detta i denna artikel Hur kan jag använda mail med php?.

Referenser

- https://aws.amazon.com/blogs/messaging-and-targeting/email-authenctication-dmarc-policy/

Unikt lösnings-ID: #1042
Av: : Admin
Senast uppdaterad: 2024-01-27 07:38