이메일 인증을 위한 모범 사례 - SPF, DKIM 및 DMARC를 구축하는 최적의 방법

목차

소개

이 설명서에서는 현재 사용 중인 세 가지 주요 이메일 인증 기술, 즉 SPF, DKIM, DMARC에 대해 설명하고, 구현의 다양한 측면에 대해 설명합니다.Cisco Email Security 제품 세트에 몇 가지 실제 이메일 아키텍처 상황과 이를 구현하기 위한 지침이 설명되어 있습니다.이 가이드는 실무 모범 사례 가이드이므로 보다 복잡한 자료 중 일부는 생략됩니다.필요한 경우, 제시된 사항에 대한 이해를 쉽게 하기 위해 특정 개념을 단순화하거나 요약할 수 있다.

제품 지식 요구 사항

이 설명서는 고급 문서입니다.제시된 자료를 계속 살펴보려면 Cisco Email Security Appliance에 대한 제품 지식을 Cisco Email Security Field Engineer 인증 수준으로 유지해야 합니다.또한 독자는

DNS 및 SMTP 및 해당 작업을 강력하게 명령해야 합니다.SPF, DKIM 및 DMARC의 기본 사항을 아는 것은 플러스입니다.

이메일 인증 - 간단한 개요

SPF(Sender Policy Framework)

발신자 정책 프레임워크는 RFC4408로 2006년에 처음 게시되었습니다. 현재 버전은 RFC7208에 지정되어 RFC7372에서 업데이트됩니다. 기본적으로 도메인 소유자는 DNS를 사용하여 수신자에게 합법적인 전자 메일 소스를 광고할 수 있는 간단한 방법을 제공합니다.SPF가 주로 반환 경로(MAIL FROM) 주소를 인증하지만, 사양은 SMTP HELO/EHLO 인수(SMTP 대화 중에 전송된 발신자 게이트웨이의 FQDN)를 인증하도록 권장(및 제공) 합니다.

SPF는 TXT 유형 DNS 리소스 레코드를 매우 간단한 구문으로 사용합니다.

```
spirit.com        = "v=spf1 mx a ip4:38.103.84.0/24 a:mx3.spirit.com
a:mx4.spirit.com include:spf.protection.outlook.com ~all"
```

위의 Spirit Airlines 기록을 통해 @spirit.com 주소의 이메일은 특정 /24 서브넷, FQDN으로 식별되는 시스템 2개 및 Microsoft의 Office365 환경에서 가져올 수 있습니다.끝에 있는 "~all" 한정자는 수신자에게 SPF의 두 가지 실패 모드 중 하나인 소프트 페일로 다른 소스를 고려하도록 지시합니다.발신자는 수신자가 실패한 메시지에 대해 수행할 작업을 지정하지 않으며, 수신자가 실패할 정도까지 지정합니다.

반면 Delta는 다른 SPF 체계를 사용합니다.

```
delta.com  = "v=spf1 a:smtp.hosts.delta.com
include:_spf.vendor.delta.com -all"
```

필요한 DNS 쿼리 수를 최소화하기 위해 Delta는 모든 SMTP 게이트웨이를 나열하는 단일 "A" 레코드를 만들었습니다.또한 "_spf.vendor.delta.com"에서 벤더에 대해 별도의 SPF 레코드를 제공합니다.또한 SPF에서 인증하지 않은 메시지**를 하드** 실패(Hard Fail)하는 지침("-all" qualifier)도 포함합니다. 공급업체의 SPF 레코드를 더 자세히 살펴볼 수 있습니다.

```
spf.vendor.delta.com  = "v=spf1 include:_spf-delta.vrli.com
include:_spf-ncr.delta.com a:delta-spf.nicondemand.com
include:_spf.airfrance.fr include:_spf.qemailserver.com
include:skytel.com include:epsl1.com ?all"
```

따라서 발신자 @delta.com에서 보내는 이메일은 Air France의 이메일 게이트웨이와 같이 합법적으로 발송될 수 있습니다.

반면 United는 훨씬 단순한 SPF 체계를 사용합니다.

```
united.com  = "v=spf1 include:spf.enviaremails.com.br
include:spf.usa.net include:coair.com ip4:161.215.0.0/16
ip4:209.87.112.0/20 ip4:74.112.71.93 ip4:74.209.251.0/24 mx ~all"
```

자체 회사 메일 게이트웨이 외에도 이메일 마케팅 공급자("usa.net" 및 "enviaremails.com.br"), 레거시 Continental Air Lines 게이트웨이, MX 레코드("MX" 메커니즘)에 나열된 모든 것이 포함됩니다. MX(도메인의 **수신** 메일 게이트웨이)는 **발신**과 같지 않을 수 있습니다.소규모 기업의 경우 대개 동일하지만, 대규모 조직은 수신 메일을 처리하는 별도의 인프라를 갖추고 발신 처리를 별도로 담당

하게 됩니다.

또한 위의 모든 예에서는 추가 DNS 조회("include" 메커니즘)를 광범위하게 사용합니다. 그러나 성능상의 이유로 SPF 사양은 최종 레코드를 검색하는 데 필요한 총 DNS 조회 수를 **10**으로 제한합니다.10개 이상의 DNS 재귀가 포함된 모든 SPF 조회는 실패합니다.

DKIM(Domain Keys Identified Mail)

RFC 5585, 6376 및 5863에 지정된 DKIM은 두 가지 역사적인 제안의 병합입니다.Yahoo의 DomainKeys 및 Cisco의 확인된 인터넷 메일입니다.발신자가 발신 메시지에 암호로 서명하고 다른 확인 메타데이터와 함께 이메일 헤더("DKIM-Signature")에 서명을 포함할 수 있는 간단한 방법을 제공합니다. 발신자는 DNS에 공개 키를 게시하므로 수신자가 키를 쉽게 검색하고 서명을 확인할 수 있습니다.DKIM은 물리적 메시지의 소스를 인증하지 않지만 발신자가 조직의 개인 키를 소유하고 있는 경우 해당 사용자를 대신하여 이메일을 전송할 수 있는 암시적 권한이 있다는 사실에 의존합니다.

DKIM을 구현하기 위해 전송 조직은 하나 이상의 공개 키 쌍을 생성하고 DNS에 공개 키를 TXT 레코드로 게시합니다.각 키 쌍은 "selector"에서 참조되므로 DKIM 확인자가 키를 구분할 수 있습니다.발신 메시지가 서명되고 DKIM-Signature 헤더가 삽입됩니다.

```
DKIM :v=1;a=rsa sha1;c=/s=;d=news.united.com;h=MIME-Version:Content-
Type:Content-Transfer-Encoding:Date:To:Reply-To:Subject:List-
Unsubscribe:Message-
ID;i=MileagePlus@news.united.com;bh=IBSWR4yzI1PSRYtWLx4SRDSWI4=;

b=HrN5QINgnXwqx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdf2nA8D2JYFTNLO8J4MMT1
HYgwYYq1TTT01YSYYYSSSYSSYYSYYSRSSYSYYYYSSSSYSYYSSYYYYYEwL0V8MEY1MzxTrzi
kLPGqt/sK1WZt9pBacEw1fMWRQLf3BxZ3jaYtLoJmrWxtgoWdfHU35CsCNYLo=
```

서명의 형식은 상당히 간단합니다."a" 태그는 서명에 사용되는 알고리즘을 지정하고, "c"는 [1]에서 사용되는 정규화 체계를 지정하고, "s"는 선택기 또는 키 참조이고, "d"는 서명 도메인입니다.이 DKIM-Signature 헤더의 나머지는 메시지별로 다릅니다."h"는 서명된 헤더를 나열하고, "i"는 서명 사용자의 ID를 나열하며, 헤더는 두 개의 개별 해시로 끝납니다."bh"는 서명된 헤더의 해시이고 "b"는 메시지 본문의 해시 값입니다.

DKIM 서명 메시지를 수신하면 수신자는 다음 DNS 쿼리를 구성하여 공개 키를 조회합니다.

```
<selector>._domainkey< >
```

DKIM-Signature 헤더에 지정되어 있습니다.위의 예에서 쿼리는 "united._domainkey.news.united.com"입니다.

```
united_domainkey.news.united.com  = "g=*\;k=rsa\;n=" ""
"postmaster@responsys.com" "with" "any" "questions" "" "this" "signing"
"\;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLh5CRU1drFTGMXX/Q2
KWgl35v6dQawx5Mxcuv5QuQuQuC
9d0jBaxtuvYALgkxmk5MemgAOcCr97GlW7Cr11eLn87qdTmyE5LevnTXxVDMjIfQJt6OFzmw
1t05NPWhZYt4qpcbiz9Kc3UB2IBwIDAQAB\;"
```

반환된 DNS 레코드에는 키 및 기타 선택적 매개 변수가 포함되어 있습니다.[2]

DKIM의 주요 문제는 발신자가 DKIM을 사용하는 광고에 대해 초기 사양을 허용하지 않았다는 것입

니다.따라서, 어떤 메시지가 서명 없이 오는 경우, 수신자가 그것이 서명되었어야 하고 그러한 경우, 그것은 대부분 진정되지 않을 것이라는 것을 아는 쉬운 방법이 없습니다.단일 조직에서 여러 개의 선택기를 사용할 수 있으므로 도메인이 DKIM이 활성화되었는지 여부를 "추측"하는 것은 간단하지 않습니다.별도의 표준인 Author Domain Signing Practices가 이를 지원하도록 개발되었지만, 사용량이 적고 기타 문제가 발생하여 2013년에 후속 작업 없이 폐기되었습니다.

DMARC(Domain-based Message Authentication, Reporting and Conformance)

DMARC는 SPF와 DKIM의 단점을 해결하기 위해 특별히 개발된 세 가지 이메일 인증 기술 중 막내입니다.다른 2와 달리, 메시지의 Header From을 인증하고 다른 두 사람이 이전에 수행한 검사에 연결합니다.DMARC는 RFC7489에 지정되어 있습니다.

DMARC over SPF 및 DKIM의 부가 가치:

- 사용 가능한 모든 ID(HELO, MAIL FROM 및/또는 DKIM 서명 도메인)가 From 헤더와 정렬(정확히 일치 또는 하위)되는지 확인합니다.
- 발신자 도메인 소유자가 실패한 메시지를 처리하는 방법에 대한 수신자에 대한 정책을 지정할 수 있는 방법 제공
- 발신자 도메인 소유자에게 장애가 발생한 메시지에 대해 통지할 피드백 기능을 제공하여 피싱 캠페인 또는 SPF/DKIM/DMARC 정책 할당에서 오류를 쉽게 식별할 수 있도록 합니다.

DMARC는 또한 간단한 DNS 기반 정책 배포 메커니즘을 사용합니다.

```
_dmarc.aa.com  = "v=DMARC1\;p=
\;fo=1\;ri=3600\;rua=mailto:american@rua.agari.com,mailto:dmarc@aa.com\;
ruf=mailto:american@ruf.agari.com,mailto:dmarc@aa.com"
```

DMARC 정책 사양의 유일한 필수 태그는 "p"이며, 실패한 메시지에 사용할 정책을 지정합니다.세 가지 중 하나일 수 있습니다.없음, 격리, 거부

자주 사용되는 선택적 매개 변수는 보고와 관련이 있습니다."rua"는 URL을 지정합니다(mailto:또는 http:// URL(POST 메서드 사용))을 사용하여 특정 도메인에서 오는 것으로 보이는 모든 실패 메시지에 대한 일별 집계 보고서를 보냅니다."ruf"는 실패한 모든 메시지에 대한 즉각적인 세부 실패 보고서를 제출할 URL을 지정합니다.

사양에 따라 수신자는 광고된 정책을 준수해야 **합니다**.그렇지 않으면 집계 보고서의 발신자 도메인 소유자에게 알려야 **합니다**.

DMARC의 중심 개념은 소위 식별자 정렬입니다.식별자 맞춤은 메시지가 DMARC 확인을 전달하는 방법을 정의합니다.SPF와 DKIM 식별자는 별도로 정렬되며, DMARC를 전체적으로 전달하려면 **모든** 메시지를 전달해야 합니다.그러나 발신자가 한 정렬이 통과하더라도 실패 보고서가 생성되도록 요청할 수 있지만 다른 정렬은 실패해도 이를 요청하는 DMARC 정책 옵션이 있습니다.위의 예에서 "fo" 태그가 "1"로 설정되어 있는 것을 확인할 수 있습니다.

메시지에는 DKIM 또는 SPF 식별자 맞춤을 준수하는 두 가지 방법이 있으며, 엄격하고 느립니다 .Strict Conlistant는 Header From의 FQDN이 DKIM 서명의 Signing Domain ID("d" 태그) 또는 SPF용 MAIL FROM SMTP 명령의 FQDN과 완전히 일치해야 함을 의미합니다.반면, Relaxed(느림)는 FQDN의 헤더가 앞서 언급한 두 개의 하위 도메인이 될 수 있도록 합니다. 이는 이메일 트래픽을 서드파티에 위임할 때 중요한 영향을 미칩니다. 이 문제는 문서의 뒷부분에서 설명합니다.

SPF 구축 고려 사항

수신자용 SPF

SPF 확인은 Cisco Email Security Appliance 또는 Cloud Email Security 가상 어플라이언스에서 구성할 수 없습니다.이 문서의 나머지 부분에서는 ESA에 대한 모든 참조 항목에도 CES가 포함됩니다.

SPF 확인은 Mail Flow Policies(메일 플로우 정책)에서 구성됩니다. 이를 전역적으로 실행하는 가장 쉬운 방법은 해당 리스너의 Default Policy Parameters(기본 정책 매개변수) 섹션에서 활성화하는 것입니다. 수신 및 발신 메일 수집에 동일한 리스너를 사용하는 경우 "RELAYED" 메일 플로우 정책에 SPF 검증이 "Off"로 설정되어 있는지 확인하십시오.

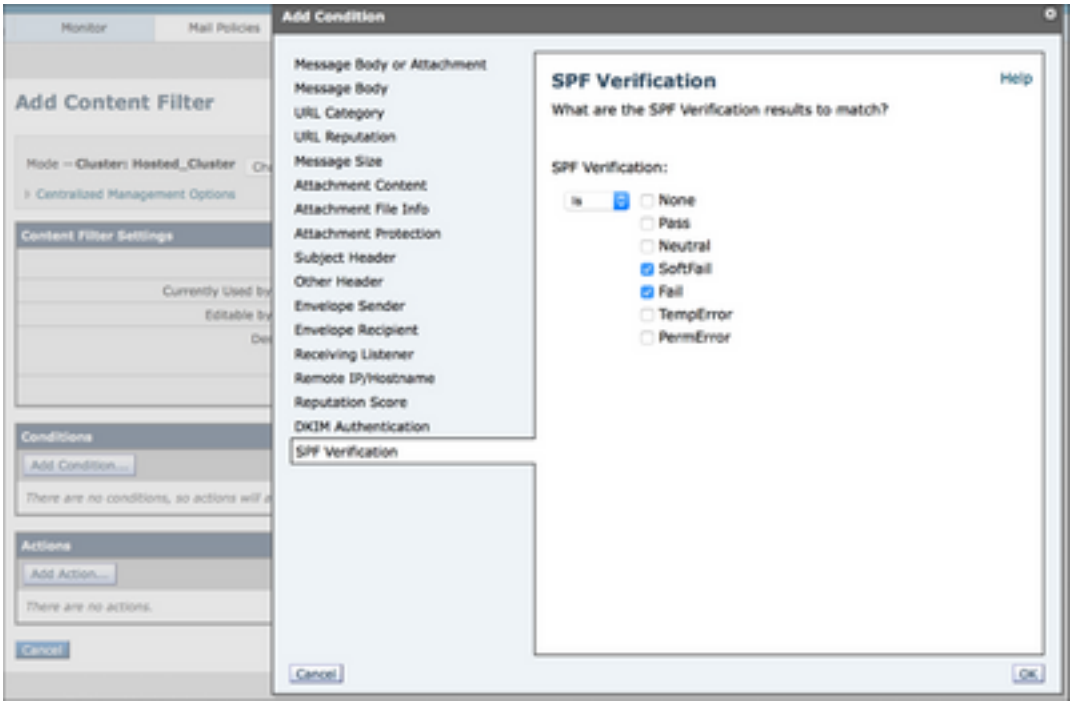
SPF에서는 정책 작업의 사양을 적용할 수 없으므로 SPF 확인(DKIM 및 DKIM)은(는) 메시지만 확인하고 수행되는 각 SPF 검사에 대한 헤더 집합을 삽입합니다.

```
Received-SPF:(mx1.hc4-93.c3s2.smtpi.com:

  united.5765@envfrm.rsys2.com 12.130.136.195 .

   ) identity=mailfrom

  client-ip=12.130.136.195receiver=mx1.hc4-93.c3s2.smtpi.com;

  envelope-from="united.5765@envfrm.rsys2.com";

  x-sender="united.5765@envfrm.rsys2.com";

  x-conformance=sidf_compatible;x-record-type="v=spf1"

Received-SPF:(mx1.hc4-93.c3s2.smtpi.com:



  postmaster@omp.news.united.com) identity=helo

  client-ip=12.130.136.195receiver=mx1.hc4-93.c3s2.smtpi.com;

  envelope-from="united.5765@envfrm.rsys2.com";

  x-sender="postmaster@omp.news.united.com";

  x-conformance=sidf_compatible
```

이 메시지에 대해 SPF에서 2개의 "ID"를 검증했습니다."mailfrom"은 사양에서 지시하며, "helo"는 동일한 조건에서 권장됩니다.메시지는 SPF 규정 준수와 관련이 있으므로 SPF를 공식적으로 통과하지만 일부 수신자는 HELO ID에 대한 SPF 레코드를 포함하지 않는 발신자를 허용할 수 있습니다.따라서 SPF 레코드에 발신 메일 게이트웨이의 호스트 이름을 포함하는 것이 좋습니다.

Mail Flow Policies(메일 플로우 정책)에서 메시지를 검증하면 로컬 관리자가 수행할 작업을 구성할 수 있습니다.이 작업은 메시지 필터 규칙 SPF-status() [3]를 사용하거나, 동일한 를 사용하여 수신 콘텐츠 필터를 생성하고 적절한 수신 메일 정책에 적용하여 수행됩니다.

그림 1:SPF 확인 콘텐츠 필터 조건



권장되는 필터 작업은 Policy Quarantine에서 Fail("-all", SPF 레코드의 경우 "~all")인 메시지를 삭제하고, Softfail("~all")인 메시지를 격리하는 것이지만 보안 요구 사항에 따라 다를 수 있습니다.일부 수신자는 실패한 메시지에 태그를 지정하거나, 가시적인 조치를 취하지 않고 관리자에게 보고합니다.

최근 SPF의 인기가 크게 증가했지만, 많은 도메인이 불완전하거나 잘못된 SPF 레코드를 게시합니다.안전한 쪽에 있으려면 모든 SPF 실패 메시지를 격리하고 격리를 한동안 모니터링하여 "오탐"이 없는지 확인해야 합니다.

다른 도메인 또는 타사에 이메일 서비스를 제공하는 경우

서드파티용 이메일 전달 또는 호스팅 서비스를 제공할 경우, 해당 메시지를 자체 SPF 레코드로 전달하는 데 사용하는 호스트 이름과 IP 주소를 추가해야 합니다.이를 수행하는 가장 쉬운 방법은 공급자가 "umbrella" SPF 레코드를 생성하고 고객이 SPF 레코드에 "include" 메커니즘을 사용하도록 하는 것입니다.

```
suncountry.com  = "v=spf1 mx ip4:207.238.249.242 ip4:146.88.177.148
ip4:146.88.177.149 ip4:67.109.66.68 ip4:198.179.134.238
ip4:107.20.247.57 ip4:207.87.182.66 ip4:199.66.248.0/22 include:cust-
spf.exacttarget.com ~all"
```

보시다시피 Sun Country는 이메일 중 일부를 자체 제어하고 있지만 마케팅 이메일은 외부 업체에 아웃소싱됩니다.참조된 레코드를 확장하면 마케팅 메일 서비스 공급자가 사용하는 현재 IP 주소 목록이 표시됩니다.

```
cust-spf.exacttarget.com  = " v=spf1 ip4:64.132.92.0/24
ip4:64.132.88.0/23 ip4:66.231.80.0/20 ip4:68.232.192.0/20
ip4:199.122.120.0/21 ip4:207.67.38.0/24 ip4:207.67.98.192/27
ip4:207.250.68.0/24 ip4:207.245.80.0/20 147.128.0/20 147.176.0/20
111.0.0/18 ip4:19.43.22.0/28 ip4:133030004:6. ip4:13.-all"
```

이러한 유연성을 통해 이메일 서비스 공급자는 각 고객에게 연락하여 DNS 레코드를 수정할 필요 없이 확장할 수 있습니다.

서드파티 이메일 서비스를 사용하는 경우

이전 단어와 마찬가지로, 타사의 이메일 서비스를 사용 중이고 완전히 SPF 확인 메일 흐름을 설정하려면 자신의 SPF 레코드를 포함해야 합니다.

```
jetblue.com   "v=spf1 include:_spf.qualtrics.com - all"
```

JetBlue는 Qualtrics 분석 서비스를 사용하며 Qualtrics의 올바른 SPF 레코드를 포함하기만 하면 됩니다.마찬가지로, 대부분의 다른 ESP는 고객의 레코드에 포함할 SPF 레코드를 제공합니다.

ESP 또는 이메일 마케터가 SPF 레코드를 제공하지 않는 경우 발신 메일 게이트웨이를 직접 목록에 추가해야 합니다.그러나 이러한 레코드를 정확하게 유지하는 것은 사용자의 책임입니다. 공급자가 추가 게이트웨이를 추가하거나 IP 주소 또는 호스트 이름을 변경하는 경우 메일 흐름이 위험에 노출될 수 있습니다.

SPF를 의식하지 않는 타사의 추가적인 위험은 리소스 공유에서 발생합니다.ESP가 동일한 IP 주소를 사용하여 여러 고객의 이메일을 전달하는 경우, 한 고객이 동일한 인터페이스를 통해 서비스를 제공하는 다른 고객으로 가장하여 SPF 유효 메시지를 생성할 수 있습니다.따라서 SPF 제한을 적용하기 전에 MSP의 보안 정책 및 이메일 인증 인식을 조사해야 합니다.SPF가 인터넷상의 기본적인 신뢰 메커니즘 중 하나인 점을 고려하면 MSP를 선택하는 것을 재고하는 것이 좋습니다. SPF, DKIM, DMARC 및 기타 발신자 모범 사례 [4]를 MSP에서 사용하는 보안에 대한 것은 아닙니다 .MSP가 이를 따르지 않거나 잘못 따라가면 대용량 수신 시스템과의 신뢰도가 낮아지고 메시지가 지연되거나 차단될 수 있습니다.

(하위)이메일 트래픽이 없는 도메인

오늘날 대부분의 조직에서는 마케팅을 위해 여러 도메인을 소유하고 있지만 기업 이메일 트래픽에는 하나의 도메인만 사용합니다.SPF가 프로덕션 도메인에 올바르게 구축되었더라도 악의적인 사용자는 이메일에 적극적으로 사용되지 않는 다른 도메인을 사용하여 조직의 ID를 스푸핑할 수 있습니다.SPF는 이메일 트래픽을 생성하지 않는 모든 도메인(및 하위 도메인!)에 대해 특수 "deny all" SPF 레코드를 통해 이러한 현상이 발생하는 것을 방지할 수 있습니다. DNS에 "v=spf1 -all"을 게시합니다.대표적인 예가 openspf.org입니다. SPF Council의 웹 사이트입니다.

SPF 위임은 단일 도메인에만 유효하므로, 이메일을 생성하지 않을 수 있는 사용 중인 모든 하위 도메인에 대해 "deny all" SPF 레코드도 게시하는 것이 중요합니다.프로덕션 도메인에 "regular" SPF 레코드가 있더라도, 트래픽 없이 하위 도메인에 "deny all" 레코드를 추가하도록 합니다.또한 수신은 전송과 동일하지 않다는 점을 잊지 마십시오.도메인은 이메일을 매우 잘 받을 수 있지만 소스는 되지 않습니다.이는 단기 마케팅 도메인(예: 이벤트, 제한된 시간 프로모션, 제품 출시...)에서 해당 도메인으로 수신되는 이메일을 프로덕션 도메인으로 전달하며 해당 이메일에 대한 모든 응답이 프로덕션 도메인에서 전달되는 경우 매우 사실입니다.이러한 단기 도메인은 유효한 MX 레코드를 가지지만 SPF 레코드가 있어야 하며, 이 레코드는 이메일 **소스**가 없음을 나타냅니다.

DKIM 구축 고려 사항

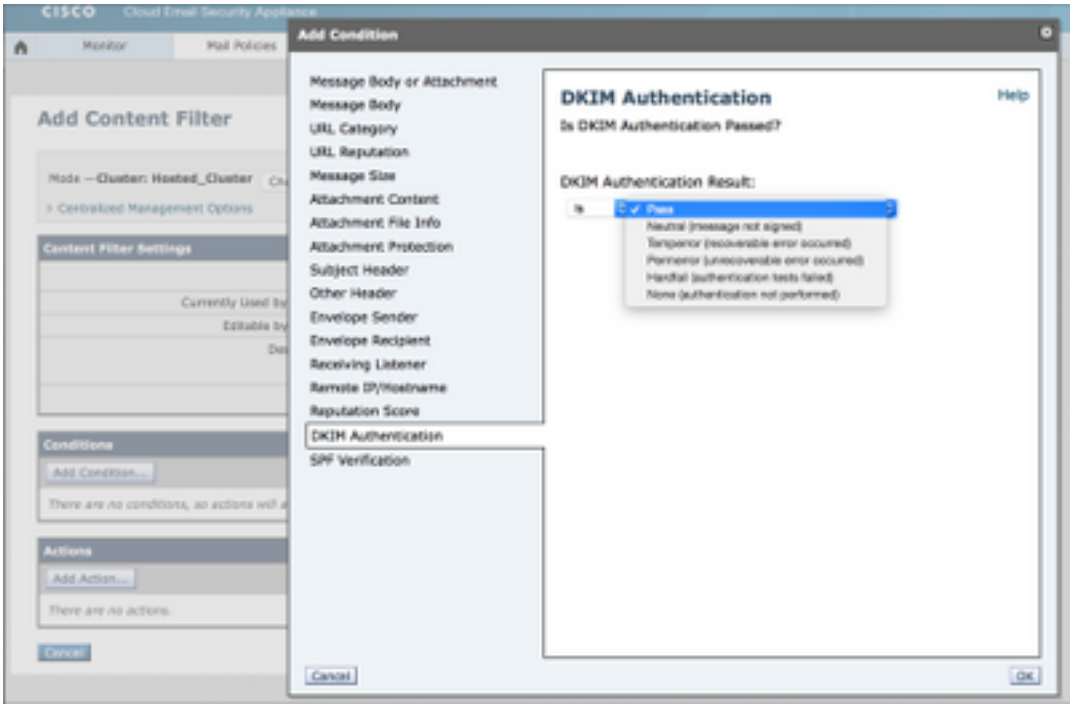
수신자용 DKIM

ESA에서 DKIM 확인을 구성하는 것은 SPF 확인과 유사합니다.Default Policy Parameters of Mail Flow Policies(메일 플로우 정책의 기본 정책 매개변수)에서 DKIM Verification(DKIM 확인)을 "On(켜기)"으로 설정하면 됩니다.DKIM은 정책 사양을 허용하지 않으므로 서명을 확인하고 "Authentication-Results" 헤더를 삽입합니다.

```
 :mx1.hc4-93.c3s2.smtpi.com;dkim=pass( )
header.i=MileagePlus@news.united.com
```

DKIM 확인 결과를 기반으로 한 모든 작업은 콘텐츠 필터에 의해 수행되어야 합니다.

그림 2:DKIM 확인 콘텐츠 필터 조건



간단한 SPF와 달리 DKIM은 실제 메시지 텍스트를 조작하므로 일부 매개변수가 제한될 수 있습니다.선택적으로, DKIM 확인 프로필을 생성하고 다른 메일 플로우 정책에 다른 확인 프로필을 할당할 수 있습니다.이를 통해 수락할 시그니처의 키 크기를 제한하고, 키 검색 실패 작업을 설정하고, DKIM 확인 깊이를 구성할 수 있습니다.

메시지가 여러 게이트웨이를 통과하므로 여러 번 서명될 수 있으므로 여러 개의 서명을 전달할 수 있습니다.메시지가 DKIM 확인을 통과하려면 **모든** 서명을 확인해야 합니다.기본적으로 ESA는 최대 5개의 서명을 확인합니다.

SMTP 및 이메일의 과거 개방성과 (긍정적) 변경에 적응하는 전체 인터넷의 거부로 인해 메일 목록 관리자가 메시지를 직접 릴레이하고 수정하는 경우나 새 메시지에 대한 첨부 파일이 아닌 직접 메시지를 전달하는 경우와 같이 DKIM 서명이 합법적으로 실패할 수 있는 경우가 여전히 있습니다.따라서 일반적으로 DKIM에 실패한 메시지에 대해서는 삭제 대신 격리 또는 태그를 지정하는 것이 좋습니다.

DKIM으로 서명 준비 중

RELAYED Mail Flow Policy에서 DKIM 서명을 켜려면 키를 생성/가져오고 DKIM 서명 프로필을 만들고 DNS에 공개 키를 게시해야 합니다.

단일 도메인에 서명하는 경우 프로세스가 간단합니다.키 쌍을 생성하고 Mail Policies(메일 정책)의 Domain Keys(도메인 키) 섹션에서 단일 서명 프로필을 생성한 다음 프로파일이 준비되면 "DNS Text Record(DNS 텍스트 레코드)" 아래의 "Generate(생성)" 옵션을 클릭합니다.DNS에서 생성된 대로 키를 게시합니다.마지막으로 메일 플로우 정책에서 DKIM 서명을 켜십시오.

여러 개의 다른 도메인에 서명하면 더 복잡해집니다.이 경우 두 가지 옵션이 있습니다.

1. 단일 서명 프로필을 사용하여 모든 도메인에 서명합니다."기본" 도메인의 DNS 영역에 (단일) 공개 키를 저장하면 DKIM 서명이 해당 키를 참조합니다.이 기술은 과거에 ESP에서 사용하던 방식이었습니다. 개별 고객의 DNS 공간 [5]과 상호 작용하지 않고도 대규모 서명을 할 수 있었습니다.
2. 서명하는 각 도메인에 대해 별도의 서명 프로필을 생성합니다.따라서 초기 컨피그레이션이 더욱 복잡해지지만 앞으로 훨씬 더 유연하게 진행할 수 있습니다.각 도메인에 대한 키 쌍을 만들고, "Profile Users(프로필 사용자)" 섹션에서 하나의 도메인(및 하위 도메인)만 지정하는 프로필을 만들고, 해당 특정 도메인의 DNS 영역에 관련 공개 키를 게시합니다.

옵션 #1는 시작하는 것이 더 쉽지만, 궁극적으로 DMARC가 깨진다는 점을 기억하십시오 .DMARC에서 서명 도메인 ID를 Header From과 정렬해야 하므로 DKIM과 식별자 맞춤이 실패합니다.SPF를 올바르게 구성하고 DMARC 확인을 통과하기 위해 SPF 식별자 맞춤을 사용하면 문제를 해결할 수 있습니다.

그러나 처음부터 옵션 #2을 구현하면 DMARC에 대해 걱정할 필요가 없으며 단일 도메인에 대해 서명 서비스를 취소하거나 재구성하는 것이 매우 쉽습니다. 또한 서드파티 도메인에 **일부** 이메일 서비스를 제공하는 경우, 대부분의 경우 해당 도메인에서 사용할 키를 받아야 합니다(그리고 ESA로 가져오기). 해당 키는 도메인별로 다르므로 별도의 프로필을 생성해야 합니다.

서드파티 이메일 서비스를 사용하는 경우

일반적으로 DKIM 서명을 사용하고 이메일 처리(예: 마케팅 이메일)의 일부를 서드파티에 오프로드하는 경우 프로덕션에서 사용하는 것과 동일한 키를 사용해서는 안 됩니다.이것이 DKIM에 선택기가 존재하는 주된 이유 중 하나입니다.대신 새 키 쌍을 생성하고 DNS 영역에 공개 부분을 게시하고 다른 사람에게 비밀 키를 전달해야 합니다.또한 운영 DKIM 인프라를 그대로 유지하면서 문제가 발생할 경우 해당 특정 키를 신속하게 취소할 수 있습니다.

DKIM에는 필요하지 않지만(동일한 도메인에 대한 메시지는 여러 개의 다른 키로 서명할 수 있음) 서드파티에서 처리하는 모든 이메일에 대해 별도의 하위 도메인을 제공하는 것이 좋습니다.따라서 메시지 추적이 쉬워지고 나중에 DMARC를 훨씬 더 효율적으로 구현할 수 있습니다.예를 들어, 루프트한자(Lufthansa)의 여러 메시지에서 다음 5개의 DKIM-Signature 헤더를 고려해 보십시오.

```
DKIM :v=1;a=rsa sha1;c=/s=d=newsletter.milesandmore.com

DKIM :v=1;a=rsa sha1;c=/s=lufthansa2;d=newsletter.lufthansa.com

DKIM :v=1;a=rsa sha1;c=/s=lufthansa3.d=lh.lufthansa.com;

DKIM :v=1;a=rsa sha1;c=/s=lufthansa4;d=e.milesandmore.com

DKIM :v=1;a=rsa sha1;c=/s=5d=fly-lh.lufthansa.com;
```

루프트한자가 두 기본 프로덕션 도메인(lufthansa.com 및 milesandmore.com)의 5개의 개별 하위 도메인으로 분할된 5개의 서로 다른 키(선택기)를 사용하고 있음을 알 수 있습니다. 즉, 각 서버를 독립적으로 제어할 수 있으며 각 서비스를 다른 메시징 서비스 공급자에게 아웃소싱할 수 있습니다 .

DMARC 구축 고려 사항

수신자용 DMARC

ESA에 대한 DMARC 확인은 프로필 기반이지만, DKIM과 달리 기본 프로파일은 사양을 준수하도록 편집해야 합니다.ESA의 기본 동작은 고객이 명시적으로 지시하지 않는 한 어떤 메시지도 삭제하지 않는 것입니다. 따라서 기본 DMARC 확인 프로필은 모든 작업을 "No Action(작업 없음)"으로 설정합니다.또한 올바른 보고서 생성을 사용하려면 "메일 정책"의 DMARC 섹션에서 "전역 설정"을 편집해야 합니다.

프로파일이 설정되면 다른 두 가지 경우와 마찬가지로 메일 플로우 정책의 기본 정책 설정 섹션에서 DMARC 확인이 설정됩니다.집계 피드백 보고서를 전송하려면 확인란을 선택해야 합니다. 이는 발신자에게 DMARC의 가장 중요한 기능입니다.작성 시 ESA는 메시지별 오류 보고서 생성(DMARC 정책의 "ruf" 태그)을 지원하지 않습니다.

SPF 또는 DKIM과 달리 DMARC 정책 작업은 발신자가 권고하므로 프로파일 컨피그레이션 외부에서 구성할 수 있는 특정 작업은 없습니다.콘텐츠 필터를 만들 필요는 없습니다.

DMARC 확인은 Authentication-Results 헤더에 추가 필드를 추가합니다.

```
 :mx1.hc4-93.c3s2.smtpi.com;dkim=pass( )
header.i=MileagePlus@news.united.com;dmarc=(p=none dis=none)
d=news.united.com
```

위의 예에서는 DKIM 식별자 정렬을 기반으로 DMARC가 확인되었고 발신자가 "none"으로 요청한 정책이 확인되었음을 알 수 있습니다.이는 현재 DMARC 구축의 "모니터" 단계에 있음을 나타냅니다.

다른 도메인 또는 타사에 이메일 서비스를 제공하는 경우

DMARC 규정 준수에 대한 ESP의 가장 큰 문제는 적절한 식별자 정렬을 달성하는 것입니다 .DMARC를 계획할 때 SPF가 올바르게 설정되었는지, 다른 모든 관련 도메인에 SPF 레코드에 발신 게이트웨이가 있는지, 정렬에 실패할 메시지를 전송하지 않는지, 주로 MAIL FROM 및 Header From ID에 다른 도메인을 사용하여 확인합니다.이 오류는 주로 응용 프로그램 작성자가 전자 메일 ID가 불일치할 경우 발생하는 결과를 대부분 인식하지 못하기 때문에 전자 메일 알림 또는 경고를 보내는 응용 프로그램에서 발생합니다.

앞서 설명한 대로 각 도메인에 대해 별도의 DKIM 서명 프로필을 사용하고 서명 프로필이 Header From에서 사용한 대로 서명하려는 도메인을 올바르게 참조하는지 확인하십시오.자체 하위 도메인을 사용하는 경우 단일 키로 서명할 **수** 있지만 DMARC 정책("adkim="r")에서 DKIM 준수를 완화하도록 설정해야 합니다.

일반적으로 직접 제어할 수 없는 다수의 서드파티에 대해 이메일 서비스를 제공하는 경우, 전달할 가능성이 가장 높은 이메일을 제출하는 방법에 대한 지침 문서를 작성하는 것이 좋습니다.사용자 간 이메일은 일반적으로 잘 작동하므로, 위의 예에서 볼 수 있듯이, 이는 대부분 애플리케이션 개발자를 위한 정책 문서로 사용됩니다.

서드파티 이메일 서비스를 사용하는 경우

서드파티를 사용하여 이메일 트래픽 중 일부를 전달하는 경우, 가장 좋은 방법은 별도의 하위 도메인(또는 완전히 다른 도메인)을 서드파티 제공자에게 위임하는 것입니다.이렇게 하면 SPF 레코드를 필요에 따라 관리하고, 별도의 DKIM 서명 인프라를 가지며, 프로덕션 트래픽에 지장을 주지 않습니다.그러면 아웃소싱 이메일에 대한 DMARC 정책은 사내 정책과 다를 수 있습니다.앞서 언급한 대로, 서드파티 제공 이메일을 고려할 때 항상 식별자가 일치하는지, DKIM 및 SPF에 대한 충실도 DMARC 정책에서 적절하게 설정되었는지 확인하십시오.

(하위)이메일 트래픽이 없는 도메인

이전 이메일 인증 기술보다 향상된 DMARC는 하위 도메인을 처리하는 방식입니다.기본적으로 특정 도메인의 DMARC 정책은 모든 하위 도메인에 적용됩니다.DMARC 정책 레코드를 검색할 때 FQDN의 헤더 레벨에서 레코드를 찾을 수 없는 경우 수신자는 보낸 사람의 조직 도메인[6]을 결정하고 그곳에서 정책 레코드를 조회해야 합니다.

그러나 조직 도메인에 대한 DMARC 정책은 명시적 DMARC 정책이 게시되지 않은 하위 도메인에 적용되는 별도의 하위 도메인 정책("DMARC 레코드의 sp" 태그)을 지정할 수도 있습니다.

앞서 SPF 장에서 설명한 시나리오에서 다음을 수행합니다.

1. 합법적인 이메일 소스인 하위 도메인에 대해 명시적 DMARC 레코드를 게시합니다.
2. 조직 도메인 정책 레코드에 "reject"의 하위 도메인 정책을 게시하여 보내지 않는 도메인을 스푸핑하는 모든 이메일을 자동으로 거부합니다.

이러한 종류의 이메일 인증 구조를 통해 인프라와 브랜드를 최대한 보호할 수 있습니다.

DMARC 관련 문제

DMARC에는 몇 가지 잠재적인 문제가 있으며, 이 모든 문제는 DMARC가 의존하는 다른 인증 기술의 특성과 단점에서 기인합니다.문제는 DMARC가 이메일을 거부할 정책을 적극적으로 추진하고 메시지의 모든 다른 발신자 식별자를 상호 연관시켜 이러한 문제를 표면화했다는 점입니다.

대부분의 문제는 메일 목록 및 메일 목록 관리 소프트웨어에서 발생합니다.메일을 메일 목록으로 보내면 모든 수신자에게 다시 배포됩니다.그러나 원래 발신자의 발신자 주소가 있는 결과 이메일은 메일 목록 관리자의 호스팅 인프라에서 전달되므로, SPF에서 헤더 From을 확인하지 못합니다(대부분의 메일 목록 관리자는 목록 주소를 Envelope From(MAIL FROM)으로 사용하고 원래 발신자의 주소는 Header From으로 사용).

DMARC는 SPF에 대해 실패하므로 DKIM을 사용할 수 있지만 대부분의 메일 목록 관리자는 메시지에 바닥글을 추가하거나 목록 이름으로 피체에 태그를 지정하여 DKIM 서명 확인을 끊을 수 있습니다.

DKIM의 작성자는 이 문제에 대한 몇 가지 해결 방법을 제안합니다. 이 모든 해결 방법은 모든 보낸 사람 주소의 목록 주소를 사용하고 원래 보낸 사람 주소를 다른 방법으로 표시해야 하는 메일링 목록 관리자에게 요약됩니다.

SMTP를 통해 원본 메시지를 새 수신자에게 복사하기만 하면 전달된 메시지에서도 비슷한 문제가 발생합니다.그러나 현재 사용 중인 대부분의 메일 사용자 에이전트는 새 메시지를 올바르게 구성하고 전달된 메시지를 인라인 또는 새 메시지에 대한 첨부 파일로 포함합니다.이러한 방식으로 전달된 메시지는 전달 사용자가 전달하면 DMARC를 전달합니다(물론 원래 메시지의 신뢰성을 설정할 수 없음).

이메일 인증 구현을 위한 샘플 작업 계획

기술 자체는 간단하지만 완전한 이메일 인증 인프라를 구현하는 방법은 길고 복잡할 수 있습니다.소규모 조직과 통제된 메일 흐름을 가진 기업은 상당히 간단할 뿐 아니라, 규모가 큰 환경에서는 매우 어려울 수 있습니다.대기업이 구현 프로젝트를 관리하기 위해 컨설팅 도움을 고용하는 것은 흔한 일입니다.

1단계:DKIM

서명되지 않은 메시지는 거부되지 않으므로 DKIM은 상대적으로 비침해적입니다.실제 구현 전에 앞서 언급한 모든 사항을 고려하십시오.서드파티에 서명을 위임할 수 있는 타사에 문의하고, 타사에서 DKIM 서명을 지원하는지 확인하고, 선택 관리 전략을 고려하십시오.일부 조직에서는 조직 구성 단위별로 별도의 키(선택기)를 유지합니다.추가 보안을 위해 키를 정기적으로 순환하는 것을 고려할 수 있지만 전송 중인 모든 메시지가 전달될 때까지 이전 키를 삭제하지 않도록 해야 합니다.

주요 사이즈를 고려해야 합니다.일반적으로 "많을수록 좋음"은 하지만 메시지당 두 개의 디지털 서명(정규화 등)을 생성하는 작업은 CPU 비용이 많이 드는 작업이며 발신 메일 게이트웨이의 성능에 영향을 미칠 수 있다는 점을 고려해야 합니다.계산 오버헤드로 인해 2048비트는 사용할 수 있는 가장 큰 실제 키 크기인 반면, 대부분의 구축에서 1024비트 키는 성능과 보안 사이에서 좋은 절충이 됩니다.

DMARC를 성공적으로 구현하려면 다음을 수행해야 합니다.

1. 하위 도메인을 포함하여 다른 이름으로 보내는 모든 도메인 식별
2. DKIM 키를 생성하고 각 도메인에 대한 서명 프로필 생성
3. 타사에 관련 개인 키 제공
4. 관련 DNS 영역에 모든 공개 키 게시
5. 서드파티 서명 준비 완료
6. 모든 ESA에서 릴레이된 메일 플로우 정책에서 DKIM 서명 켜기
7. 서드파티에 서명을 시작하도록 알림

2단계:SPF

SPF를 올바르게 구현하면 이메일 인증 인프라 구현에서 가장 많은 시간과 번거로운 부분이 될 것입니다.이메일은 사용 및 관리가 매우 간단했고 보안 및 액세스 관점에서 완전히 개방되었기 때문에, 지금까지 조직은 이메일의 사용 방법과 사용 방법에 대해 엄격한 정책을 시행하지 않았습니다.이로 인해 오늘날 대부분의 조직에서는 내부 및 외부에서 모든 다양한 이메일 소스를 완벽하게 파악하지 못하고 있습니다.SPF 구현의 가장 큰 문제는 현재 누가 귀하를 대신하여 이메일을 합법적으로 보내고 있는지 확인하는 것입니다.

원하는 사항:

1. 명확한 대상 - Exchange 또는 기타 그룹웨어 서버 또는 발신 메일 게이트웨이
2. 외부 알림을 생성할 수 있는 DLP 솔루션 또는 기타 이메일 처리 시스템
3. 고객과 상호 작용하는 정보를 보내는 CRM 시스템
4. 이메일을 전송할 수 있는 다양한 서드파티 애플리케이션
5. Lab, 테스트 또는 이메일을 보낼 수 있는 기타 서버
6. 외부 이메일을 직접 보내도록 구성된 개인 컴퓨터 및 장치

조직의 환경이 다르기 때문에 위의 목록은 완전하지 않지만, 무엇을 찾아야 하는지에 대한 일반적인 지침으로 간주해야 합니다.이메일 소스가 확인되면(대부분의 경우) 한 단계 뒤로 물러서서 모든 기존 소스를 인증하는 대신 목록을 정리합니다.가장 좋은 방법은 모든 발신 이메일을 발신 메일 게이트웨이를 통해 전달해야 하며 몇 가지 분명한 예외가 있습니다.자체 마케팅 메일 솔루션을 보유하고 있거나 타사 마케팅 메일 솔루션을 사용하는 경우 프로덕션 이메일 게이트웨이와 별도의 인프라를 사용해야 합니다.메일 전달 네트워크가 매우 복잡할 경우 SPF에서 현재 상태를 문서화하는 작업을 계속 진행할 수 있지만, 나중에 상황을 정리하는 데 시간이 걸립니다.

동일한 인프라에서 여러 도메인을 제공하는 경우 단일 범용 SPF 레코드를 생성하고 "include" 메커

니즘을 사용하여 개별 도메인에서 참조할 수 있습니다.SPF 레코드가 너무 크지 않은지 확인합니다.예: /24 네트워크의 시스템 5개만 SMTP를 보낼 경우, 전체 네트워크가 아닌 5개의 개별 IP 주소를 SPF에 추가합니다.가능한 한 구체적으로 레코드를 지정하여 악의적인 이메일이 사용자의 신원을 손상시킬 가능성을 최소화합니다.

일치하지 않는 발신자("~all")에 대한 소프트페일 옵션으로 시작합니다. 100% 이메일 소스를 **모두** 확인했다면(-all)으로 변경하기만 하면 프로덕션 이메일이 손실될 위험이 있습니다.나중에 DMARC를 구현하고 잠시 모니터 모드에서 실행한 후 누락된 시스템을 식별하여 SPF 레코드를 업데이트할 수 있습니다.그래야 SPF를 hardfail로 설정할 수 있습니다.

3단계:DMARC

DKIM과 SPF가 최대한 완전하게 설정되면 이제 DMARC 정책을 생성할 때입니다.이전 장에 언급된 모든 상황을 고려하고 복잡한 이메일 인프라가 있는 경우 둘 이상의 DMARC 레코드를 구축할 준비를 합니다.

보고서를 수신할 이메일 별칭을 만들거나 보고서를 수집할 수 있는 웹 애플리케이션을 만듭니다.이에 사용할 엄격하게 정의된 이메일 주소는 없지만 rua@domain.com, dmarc.rua@domain.com, mailauth-rua@domain.com 등과 같이 설명이 필요한 경우 유용합니다.운영자가 이러한 주소를 모니터링하고 SPF, DKIM 및 DMARC 컨피그레이션을 적절하게 수정하거나 스푸핑 캠페인의 경우 보안 팀에 알림을 보낼 수 있는 프로세스가 있는지 확인합니다.처음에는 SPF 및 DKIM 컨피그레이션 중에 놓친 사항을 기록하도록 레코드를 조정하면 워크로드가 상당할 것입니다.잠시 후 보고서는 스푸핑 시도만 나타낼 수 있습니다.

처음에는 DMARC 정책을 "none"으로 설정하고 포렌식 옵션을 설정하여 **모든** 오류 검사("fo=1")에 대한 보고서를 전송합니다. 그러면 트래픽에 영향을 미치지 않으면서 SPF 및 DKIM의 모든 오류를 신속하게 검색할 수 있습니다.제출된 보고서의 내용에 만족하면 보안 정책 및 환경 설정에 따라 정책을 "격리" 또는 "거부"로 변경합니다.다시 한 번, 운영자가 수신한 DMARC 보고서에서 오탐을 지속적으로 분석하도록 합니다.

DMARC를 완전하고 올바르게 구현하는 것은 작은 작업이나 짧은 작업이 아닙니다.일부 결과(및 DMARC의 공식적인 "구현")는 불완전한 레코드 집합과 "없음" 정책을 게시함으로써 얻을 수 있지만, 모든 사람이 기능의 전범위에서 이를 구현하는 것은 발신자 조직과 인터넷 모두에게 가장 큰 이익이 됩니다.

타임라인과 관련하여, 다음은 일반적인 프로젝트의 개별 단계에 대한 대략적인 개요입니다.각 조직이 다르기 때문에 정확성이 떨어집니다.

1. 기획준비	2-4주
2. DKIM 시험성적	2주
3. SPF - 합법적인 발신자 식별	2-4주
4. DMARC 정책준비	2주
5. SPF 및 DMARC 레코드 테스트 실행	4-8주
6. SPF 테스트 실행(hardfail 포함)	2주
7. DMARC 시험(검역/거부 포함)	4주
8. DMARC 보고서 모니터링 및 그에 따른 SPF/DKIM 조정	지속적인

규모가 작은 조직에서는 대부분의 단계, 특히 3단계와 4단계를 더 짧게 처리할 수 있습니다. 이메일 인프라가 아무리 간단하다고 생각하더라도 항상 테스트 실행 중에 충분한 시간을 할당하고, 놓친 사항에 대해 피드백 보고서를 면밀하게 모니터링합니다.

규모가 큰 조직에서는 더 엄격한 테스트 요건으로 동일한 단계를 더 오래 진행할 수 있습니다.복잡한 이메일 인프라를 보유한 기업이 외부 지원을 고용하는 것은 일반적이지 않으며, 이메일 인증 구

현의 기술적 측면뿐만 아니라 전체 프로젝트를 관리하고 팀 및 부서 간에 조정합니다.

추가 참조

- SPF의 참조 사이트:http://www.openspf.org
- DKIM 위원회:http://www.dkim.org
- DMARC 주 웹 사이트, Trusted Domain Project에서 실행:http://www.dmarc.org
- dmarhian - DMARC의 저자 중 한 명인 Tim Draegen이 운영하는 도움말 및 리소스 사이트입니다."툴" 섹션을 참조하십시오.http://www.dmarcian.com
- Online Trust Alliance의 레코드 유효성 검사기 도구:https://otalliance.org/resources/spf-dmarc-record-validator
- DMARC Record Assistant - DMARC 레코드를 생성하는 데 유용한 툴입니다 .http://www.kitterman.com/dmarc/assistant.html
- SPF 레코드 테스트 도구:http://www.kitterman.com/spf/validate.html
- "피싱하지 마세요.Deep Dive Into Email Authentication Skills", Cisco Live 2014 프레젠테이션 BRKSEC-3770:https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1]정규화는 이 문서의 범위를 벗어납니다.DKIM 정규화에 대한 자세한 내용은 "추가 참조" 섹션의 자료를 참조하십시오.

[2] DKIM DNS 레코드 매개 변수도 이 문서의 범위를 벗어납니다.

[3] 메시지 필터 만들기는 이 문서의 범위를 벗어납니다.도움이 필요하면 AsyncOS for Email 사용 설명서를 참조하십시오.

[4] M3AWG는 대부분의 업계에서 적용 및 인정받는 우수한 모범 사례를 정의했습니다.Sender Best Common Practices 문서는 https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf에서 확인할 수 있습니다.

[5] 이 동작은 원래 DKIM이 MAIL FROM 또는 Header From에 명시된 메시지 소스를 전혀 확인하지 않는다는 사실을 활용합니다.DKIM 서명의 서명 도메인 ID("d" 매개변수, 서명 프로파일의 "도메인 이름" 매개변수)가 실제로 메시지에 서명하는 데 사용된 쌍의 공개 키를 호스팅하는지 확인만 합니다.발신자 신뢰성은 "From" 헤더가 서명되어 있음을 의미합니다."Profile Users(프로필 사용자)" 섹션에서 로그인한 모든 도메인 및 하위 도메인을 나열하기만 하면 됩니다.

[6] 일반적으로 도메인은 TLD 또는 관련 TLD 접두사(.ac.uk, .com.sg 등)보다 한 단계 낮은 도메인입니다.