Best Practice für die E-Mail-Authentifizierung - Optimale Möglichkeiten zur Bereitstellung von SPF, DKIM und DMARC

Inhalt

Einführung

In diesem Leitfaden werden drei derzeit verwendete Technologien zur E-Mail-Authentifizierung beschrieben: SPF, DKIM und DMARC und die verschiedenen Aspekte ihrer Implementierung. Es werden verschiedene Situationen der E-Mail-Architektur in der Praxis erörtert, und es werden Richtlinien für deren Implementierung im Cisco Email Security-Produktsatz erörtert. Da es sich um einen Leitfaden für praktische Best Practices handelt, werden einige der komplexeren Materialien weggelassen. Einige Konzepte können bei Bedarf vereinfacht oder zusammengefasst werden, um das Verständnis der vorgestellten Materie zu erleichtern.

Produktinformationen

Dieser Leitfaden ist ein Dokument der erweiterten Ebene. Um das vorgestellte Material durchzuarbeiten, sollte der Leser über Produktkenntnisse der Cisco Email Security Appliance verfügen, bis er über die Cisco Email Security Field Engineer-Zertifizierung verfügt. Darüber hinaus sollten die Leser über einen starken Befehl für DNS und SMTP und deren Betrieb verfügen. Die Übernahme der Grundlagen von SPF, DKIM und DMARC ist ein Plus.

E-Mail-Authentifizierung - Kurzübersicht

Sender Policy Framework (SPF)

Sender Policy Framework wurde erstmals 2006 als RFC4408 veröffentlicht. Die aktuelle Version ist in RFC 7208 festgelegt und in RFC 7372 aktualisiert. Im Wesentlichen bietet sie einem Domänenbesitzer eine einfache Möglichkeit, seine legitimen E-Mail-Quellen über DNS an die Empfänger anzugeben. Obwohl SPF in erster Linie die Adresse für den Rückgabepfad (MAIL FROM) authentifiziert, wird in der Spezifikation empfohlen (und ein Mechanismus bereitgestellt), auch das SMTP HELO/EHLO-Argument (FQDN des Sendergateways, wie bei SMTP-Konversation übertragen) zu authentifizieren.

SPF verwendet TXT-Typ DNS Resource Records (DNS-Ressourcendatensätze mit ziemlich einfacher Syntax):

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

Mit dem oben angegebenen Spirit Airlines-Datensatz können E-Mails von @spirituom.com-Adressen aus einem bestimmten /24-Subnetz stammen, zwei durch einen FQDN identifizierte Maschinen und die Office365-Umgebung von Microsoft. Der "~all"-Qualifizierer am Ende weist die Empfänger an, alle anderen Quellen als Soft Fail (Soft Fail) zu betrachten - einer von zwei Ausfallmodi von SPF. Beachten Sie, dass Absender nicht angeben, was Empfänger mit fehlerhaften Nachrichten tun sollen, nur in welchem Ausmaß sie scheitern.

Delta hingegen verwendet ein anderes SPF-Schema:

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

Um die Anzahl der erforderlichen DNS-Abfragen zu minimieren, erstellte Delta einen einzigen A-Datensatz, in dem alle SMTP-Gateways aufgelistet sind. Sie stellen außerdem einen separaten SPF-Datensatz für ihre Lieferanten in "_spf.vendor.delta.com" bereit. Sie enthalten auch Anweisungen für **Hard Fail** aller Nachrichten, die nicht durch den SPF authentifiziert wurden ("-all"-Qualifizierer). Darüber hinaus können wir den SPF-Datensatz der Anbieter nachschlagen:

```
_spf.vendor.delta.com text = "v=spf1 include:_spf-delta.vrli.com
include:_spf-ncr.delta.com a:delta-spf.niceondemand.com
include:_spf.airfrance.fr include:_spf.qemailserver.com
include:skytel.com include:epsl1 Alle"
```

E-Mails von Absendern @delta.com können also zu Recht von den E-Mail-Gateways von Air France stammen.

United dagegen verwendet ein viel einfacheres SPF-Schema:

```
united.com text = "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"
```

Neben ihren eigenen E-Mail-Gateways gehören dazu auch die E-Mail-Marketing-Anbieter ("usa.net" und "enviaremails.com.br"), die veralteten Continental Air Lines-Gateways sowie alle in ihren MX-Datensätzen aufgeführten Komponenten ("MX"-Mechanismus). Beachten Sie, dass MX (ein **eingehendes** Mail-Gateway für eine Domäne) möglicherweise nicht mit dem **ausgehenden** MX **identisch** ist. Während kleinere Unternehmen in der Regel die gleichen sind, verfügen größere Unternehmen über eine separate Infrastruktur für die Bearbeitung eingehender E-Mails und die separate Abwicklung ausgehender Sendungen.

Beachten Sie auch, dass alle oben genannten Beispiele umfassend von zusätzlichen DNS-Referrals ("Include"-Mechanismen) Gebrauch machen. Aus Leistungsgründen beschränkt die SPF-Spezifikation jedoch die Gesamtzahl der DNS-Lookups, die für das Abrufen eines endgültigen Datensatzes erforderlich sind, auf **zehn**. Alle SPF-Suchvorgänge mit mehr als 10 Stufen der DNS-Rekursion schlagen fehl.

Domain Keys Identified Mail (DKIM)

DKIM, spezifiziert in den RFC 5585, 6376 und 5863, ist eine Zusammenführung zweier historischer Vorschläge: DomainKeys von Yahoo und Identified Internet Mail von Cisco. Es bietet eine einfache Möglichkeit für Absender, ausgehende Nachrichten kryptografisch zu signieren und die Signaturen (zusammen mit anderen Überprüfungsmetadaten) in einen E-Mail-Header ("DKIM-Signature") einzufügen. Absender veröffentlichen ihren öffentlichen Schlüssel im DNS, sodass jeder Empfänger den Schlüssel abrufen und die Signaturen überprüfen kann. DKIM authentifiziert nicht die Quelle der physischen Nachrichten, sondern beruht auf der Tatsache, dass die Quelle, die im Besitz des privaten Schlüssels der Absenderorganisation ist, implizit berechtigt ist, in ihrem Namen eine E-Mail zu senden.

Um DKIM zu implementieren, würde eine sendende Organisation ein oder mehrere öffentliche Schlüsselpaare generieren und die öffentlichen Schlüssel im DNS als TXT-Datensätze veröffentlichen. Auf jedes Schlüsselpaar wird durch einen "Selektor" verwiesen, sodass DKIM-Prüfer zwischen Schlüsseln unterscheiden können. Ausgehende Nachrichten werden signiert und der DKIM-Signature-Header eingefügt:

```
DKIM-Signatur: v=1; a=rsa-sha1; c=entspannt/entspannt; s=vereint;
d=news.united.com;h=MIME-Version:Content-Type:Content-Transfer-
Encoding:Date:To:From:Reply-To:Subject:List-Unsubscribe:Message-ID;
i=MileagePlus@news.united.com; bh=IBSWR4yzI1PSRYtWLx4SRDSWII4=;

b=HrN5QINgnXwqkx+Zc/9VZys+yhikrP6wSZVu35KA0jfgYzhzSdfA2nA8D2JYIFTNLO8j4D
GmKh1MMTyYgwq
T01rEwL0V8MEY1MzxTrzijkLPGqt/sK1WZt9pBacEw1fMWRQLf3BxZ3jaYtLoJMRwxtgoWdf
HU35CsFG2CNYL=
```

Das Format der Signatur ist ziemlich einfach. "a"-Tag gibt Algorithmen für die Signierung an, "c" gibt das bzw. die verwendeten Kanonikalisierungsschemata an [1], "s" ist der Selektor oder die Schlüsselreferenz, "d" ist die Signaturdomäne. Der Rest dieses DKIM-Signature-Headers ist nachrichtenspezifisch: "h" listet signierte Header auf, "i" listet die Identität des signierenden

Benutzers auf, und schließlich endet der Header mit zwei separaten Hashes: "bh" ist ein Hash von signierten Headern, während "b" der Hashwert für den Text der Nachricht ist.

Beim Empfang einer DKIM-signierten Nachricht sucht der Empfänger den öffentlichen Schlüssel, indem er die folgende DNS-Abfrage erstellt:

```
<Selector>._domainkey.<Signaturdomäne>
```

wie im DKIM-Signature-Header angegeben. Im obigen Beispiel lautet unsere Abfrage "united._domainkey.news.united.com":

```
united.domainkey.news.united.com text = "g=*\"; k=rsa\; n=" "Kontakt"
"postmaster@responsys.com" "mit" "irgendwelchen" "Fragen" "bezüglich"
"dieses" "Signieren" "\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/Vh/xq+sSRLhL5CRU1drFTGMXX/Q2Kk
Wgl35hO4v6dTy5Qmxcuv5Awqx
Liz9d0jBaxtuvYALjlGkxmk5MemgAOcCr97GlW7Cr11eLn87qdTmyE5LevnTXxVDMjIfQJt6
OfZmw6Tp1t05t NPWh0PbyUohZYt4qpcbiz9Kc3UB2IBwIDAQAB\;"
```

Der zurückgegebene DNS-Datensatz enthält den Schlüssel sowie weitere optionale Parameter. [2]

Das Hauptproblem bei DKIM besteht darin, dass die ursprüngliche Spezifikation keine Werbung zulässt, die ein Absender DKIM verwendet. Wenn also eine Nachricht ohne Signatur eingeht, kann der Empfänger nicht leicht wissen, dass sie hätte signiert werden sollen und dass sie in diesem Fall höchstwahrscheinlich nicht authentisch ist. Da eine einzelne Organisation mehrere Selektoren verwenden kann (und wird), ist es nicht leicht, zu erraten, ob eine Domäne DKIM-fähig ist. Um dieses Problem zu lösen, wurde ein separater Standard entwickelt, Author Domain Signing Practices. Aufgrund der geringen Nutzung und anderer Probleme wurde 2013 jedoch ohne Nachfolger veraltet.

Domänenbasierte Authentifizierung, Reporting und Konformität von Nachrichten (DMARC)

DMARC ist die jüngste der drei abgedeckten E-Mail-Authentifizierungstechnologien und wurde speziell entwickelt, um die Mängel von SPF und DKIM zu beheben. Im Gegensatz zu den beiden anderen authentifiziert er den Header From einer Nachricht und stellt eine Verbindung zu den zuvor von den beiden anderen Nachrichten durchgeführten Prüfungen her. DMARC ist in RFC 7489 angegeben.

Der Mehrwert von DMARC über SPF und DKIM besteht aus:

- Achten Sie darauf, dass alle verfügbaren Identitäten (HELO, MAIL FROM und/oder DKIM-Signaturdomäne) mit dem Von-Header übereinstimmen (exakt übereinstimmend oder untergeordnet)
- Bereitstellung einer Möglichkeit für den Besitzer der Absenderdomäne, eine Richtlinie für Empfänger anzugeben, wie diese fehlerhafte Nachrichten **behandeln müssen**
- Bereitstellung einer Feedback-Möglichkeit für Absenderdomänenbesitzer, um über fehlerhafte Nachrichten informiert zu werden und so die Identifizierung von Phishing-Kampagnen oder Fehlern bei der Zuweisung von SPF-/DKIM-/DMARC-Richtlinien zu erleichtern

DMARC verwendet außerdem einen einfachen DNS-basierten Richtlinienverteilungsmechanismus:

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

Das einzige obligatorische Tag in der DMARC-Richtlinienspezifikation ist "p", das die Richtlinie angibt, die für ausfallende Nachrichten verwendet wird. Dabei kann es sich um eine der drei folgenden Kategorien handeln: Keine, Quarantäne, Ablehnen.

Die am häufigsten verwendeten optionalen Parameter haben mit der Berichterstellung zu tun: "rua" gibt eine URL an (entweder eine E-Mail an: oder eine http://-URL mithilfe der POST-Methode), um tägliche aggregierte Berichte über alle fehlgeschlagenen Nachrichten zu senden, die angeblich von einer bestimmten Domäne stammen. "ruf" gibt eine URL an, über die bei jedem Ausfall umgehend detaillierte Fehlerberichte gesendet werden können.

Gemäß Spezifikation **muss** ein Empfänger die angegebene Richtlinie einhalten. Andernfalls **müssen** sie den Besitzer der Absenderdomäne im Gesamtbericht benachrichtigen.

Das zentrale Konzept von DMARC ist die so genannte Identifikatorausrichtung. Durch die Identifikatorausrichtung wird festgelegt, wie eine Nachricht die DMARC-Überprüfung übergeben kann. SPF- und DKIM-IDs werden separat ausgerichtet, und eine Nachricht muss **eine** von ihnen übergeben, um den DMARC insgesamt zu übergeben. Es gibt jedoch eine DMARC-Richtlinienoption, bei der der Absender verlangen kann, dass ein Fehlerbericht generiert wird, auch wenn eine Ausrichtung erfolgreich ist, die andere jedoch fehlschlägt. Wir können dies im obigen Beispiel sehen, wenn das "fo"-Tag auf "1" gesetzt ist.

Es gibt zwei Möglichkeiten für Nachrichten, sich entweder an die DKIM- oder SPF-Identifikationsausrichtung zu halten: strikt und entspannt. Strikte Einhaltung bedeutet, dass der FQDN des Header From vollständig mit der Signing Domain ID ("d"-Tag) der DKIM-Signatur oder dem FQDN des SMTP-Befehls für SPF übereinstimmen muss. Relaxed hingegen ermöglicht Header From FQDN eine Unterdomäne der oben genannten zwei. Dies hat wichtige Auswirkungen, wenn Sie Ihren E-Mail-Datenverkehr an Dritte delegieren, was später in diesem Dokument besprochen wird.

Überlegungen zur SPF-Bereitstellung

SPF für Empfänger

Die SPF-Verifizierung ist auf den virtuellen Appliances der Cisco E-Mail Security Appliance oder Cloud E-Mail Security trivial. Im verbleibenden Teil dieses Dokuments wird jede Bezugnahme auf ESA auch CES enthalten.

Die SPF-Überprüfung wird in Mail Flow Policies (Mail-Flow-Richtlinien) konfiguriert. Die einfachste Methode, diese global auszuführen, ist, sie im Abschnitt Default Policy Parameters (Standardrichtlinienparameter) des/der entsprechenden Listener(s) zu aktivieren. Wenn Sie denselben Listener für die eingehende und ausgehende E-Mail-Erfassung verwenden, stellen Sie sicher, dass die SPF-Verifizierung für Ihre "RELAYED" Mail Flow Policy auf "Off" (Aus) eingestellt ist.

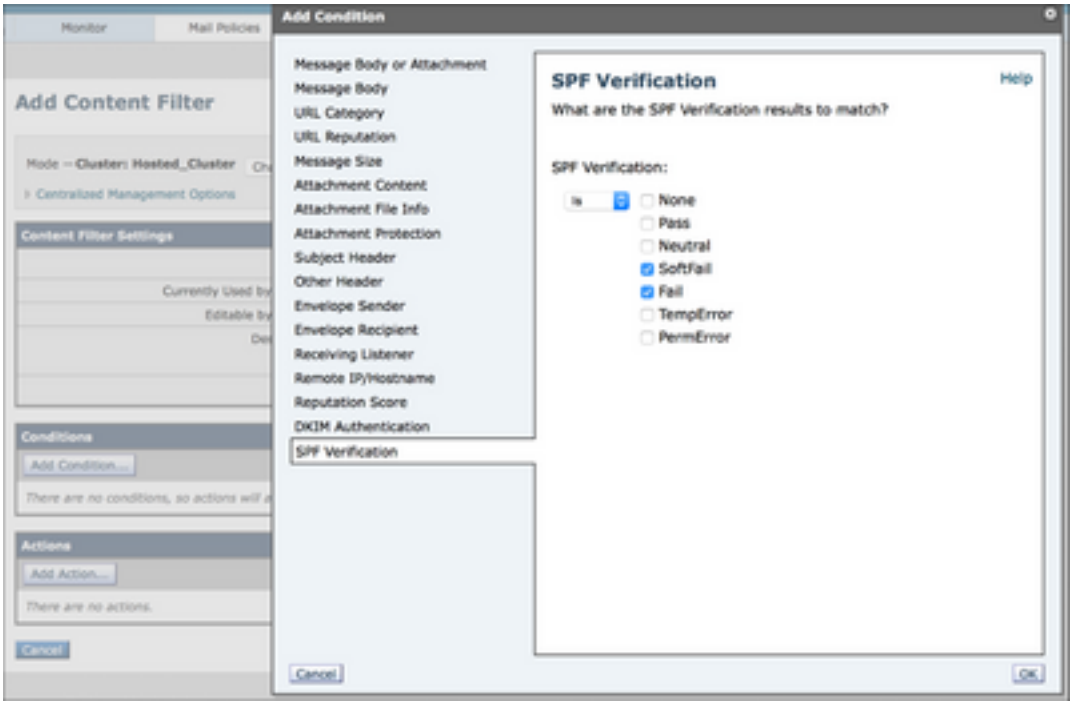
Da SPF keine Spezifikation der zu ergreifenden Richtlinienaktionen zulässt, wird bei der SPF-Überprüfung (sowie bei DKIM, wie weiter unten dargestellt) nur die Nachricht überprüft und für jede durchgeführte SPF-Prüfung ein Header eingefügt:

```
Received-SPF: Pass (mx1.hc4-93.c3s2.smtpi.com: Domäne
  united.5765@envfrm.rsys2.com gibt den 12.130.136.195 als
  permit sender) identity=mailfrom;
  client-ip=12.130.136.195; empfänger=mx1.hc4-93.c3s2.smtpi.com;
  velope-from="united.5765@envfrm.rsys2.com";
  xSender="united.5765@envfrm.rsys2.com";
  x-conformance=sidf_kompatible; x-record type="v=spf1"
Received-SPF: Keine (mx1.hc4-93.c3s2.smtpi.com: Kein Absender
  Authentifizierungsinformationen sind über die Domäne von
  postmaster@omp.news.united.com) identity=helo;
  client-ip=12.130.136.195; empfänger=mx1.hc4-93.c3s2.smtpi.com;
  velope-from="united.5765@envfrm.rsys2.com";
  xSender="postmaster@omp.news.united.com";
  x-conformance=sidf_kompatible
```

Beachten Sie, dass für diese Nachricht zwei "Identitäten" von SPF verifiziert wurden: "mailfrom", wie in der Spezifikation vorgeschrieben, und "helo", wie von der gleichen empfohlen. Die Nachricht wird offiziell SPF übergeben, da nur Erstere für die SPF-Compliance relevant sind, aber einige Empfänger können Absender sanktionieren, die für ihre HELO-Identitäten auch keine SPF-Datensätze enthalten. Daher empfiehlt es sich, die Hostnamen der ausgehenden Mail-Gateways in Ihre SPF-Datensätze aufzunehmen.

Sobald Mail Flow Policies eine Nachricht verifizieren, müssen lokale Administratoren festlegen, welche Aktion ausgeführt werden soll. Dies geschieht mithilfe der Nachrichtenfilterregel SPF-status() [3] oder durch Erstellen eines Content-Filters, der den gleichen Code verwendet und auf die entsprechenden Richtlinien für eingehende E-Mails angewendet wird.

Bild 1: Bedingung für SPF-Verifizierung Content-Filter



Empfohlene Filteraktionen sind das Verwerfen von Nachrichten, die fehlschlagen ("-all" im SPF-Datensatz), und das Verlassen von Nachrichten, die Softfail ("~all" im SPF-Datensatz) in einer Richtlinienquarantäne. Dies kann jedoch je nach Ihren Sicherheitsanforderungen variieren. Einige Empfänger kennzeichnen fehlerhafte Nachrichten einfach oder ergreifen keine sichtbaren Maßnahmen, sondern melden sie den Administratoren.

In letzter Zeit ist die Popularität von SPF deutlich gestiegen, aber viele Domänen veröffentlichen unvollständige oder falsche SPF-Datensätze. Um auf der sicheren Seite zu sein, sollten Sie möglicherweise alle Nachrichten, die bei SPF fehlschlagen, unter Quarantäne stellen und die Quarantäne für eine Weile überwachen, um sicherzustellen, dass keine "Fehlalarme" vorliegen.

Wenn Sie E-Mail-Services für andere Domänen oder Drittanbieter bereitstellen

Wenn Sie E-Mail-Zustellungs- oder Hosting-Services für Drittanbieter bereitstellen, müssen diese Hostnamen und IP-Adressen hinzufügen, die Sie verwenden, um ihre Nachrichten an ihre eigenen SPF-Datensätze zu übermitteln. Die einfachste Methode hierfür besteht darin, dass der Anbieter einen übergeordneten SPF-Datensatz erstellt und Kunden den "include"-Mechanismus in ihren SPF-Datensätzen verwenden.

```
suncountry.com text = "v=spf1 mx ip4:207.238.249.242 ip4:146.88.177.148
ip4:146.88.177.149 ip4:67.1 09.66.68 ip4:198.179.134.238
ip4:107.20.247.57 ip4:207.87.182.66 ip4:199.66.248.0/22 enthalten:cust
spf.extarget.com ~all"
```

Wie wir sehen können, hat Sun Country zwar einige seiner E-Mails unter eigener Kontrolle, aber die Marketing-E-Mails werden an Dritte ausgelagert. Durch die Erweiterung des angegebenen Datensatzes wird eine Liste der aktuellen IP-Adressen angezeigt, die von ihrem Marketing-Mailingdienstanbieter verwendet werden:

```
cust-spf.extarget.com text = " 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 ip4:209.43.22.0/28 ip4:198.245.80.0/20
```

```
ip4:136.147.128.0/20 ip4:136.147.176.0/20 ip4:13.111.0.0/18 -all"
```

Dank dieser Flexibilität können E-Mail-Service-Provider skalieren, ohne sich an jeden Kunden wenden zu müssen, um seine DNS-Datensätze zu ändern.

Wenn Sie E-Mail-Services von Drittanbietern verwenden

Ähnlich wie im vorherigen Absatz müssen Sie, wenn Sie E-Mail-Dienste von Drittanbietern verwenden und einen vollständig SPF-verifizierten E-Mail-Fluss einrichten möchten, eigene SPF-Datensätze in Ihren E-Mail-Verkehr einfügen.

```
jetblue.com beschreibender Text "v=spf1 include:_spf.qualtrics.com ?all"
```

JetBlue nutzt den Analyseservice Qualtrics, und das einzige, was sie tun müssen, ist einen korrekten SPF-Datensatz von Qualtrics zu erhalten. Ebenso stellen die meisten anderen ESPs SPF-Datensätze bereit, die in Kundendatensätze aufgenommen werden können.

Wenn Ihr ESP- oder E-Mail-Vermarkter keine SPF-Datensätze bereitstellt, müssen Sie die ausgehenden E-Mail-Gateways direkt in Ihrem angeben. Es liegt jedoch in Ihrer Verantwortung, diese Datensätze korrekt zu speichern. Wenn der Anbieter zusätzliche Gateways hinzufügt oder IP-Adressen oder Hostnamen ändert, kann Ihr Mail-Fluss gefährdet sein.

Weitere Risiken von Drittanbietern, die nicht SPF-fähig sind, ergeben sich aus der gemeinsamen Nutzung von Ressourcen: Wenn ein ESP dieselbe IP-Adresse verwendet, um E-Mails von mehreren Kunden zu senden, ist es technisch möglich, dass ein Kunde eine SPF-gültige Nachricht generiert, die so tut, als wäre er ein anderer Kunde, der diese Nachricht über dieselbe Schnittstelle bereitstellt. Aus diesem Grund sollten Sie vor der Einführung von SPF-Einschränkungen die Sicherheitsrichtlinien Ihres MSP und die Kenntnis der E-Mail-Authentifizierung untersuchen. Wenn der Kunde keine Antworten auf Ihre Fragen hat und die Tatsache, dass SPF einer der grundlegenden Vertrauensmechanismen im Internet ist, wird Ihnen dringend empfohlen, Ihre Wahl des MSP zu überdenken. Dabei geht es nicht nur um Sicherheit: Die Best Practices der MSPs SPF, DKIM, DMARC und anderer Absender [4] sind eine Garantie für die Lieferbarkeit. Wenn Ihr MSP ihnen nicht folgt oder sie falsch verfolgt, verringert dies ihre Vertrauenswürdigkeit bei großen Empfangssystemen und kann Ihre Nachrichten verzögern oder sogar blockieren.

(Sub)Domänen ohne E-Mail-Verkehr

Die meisten Unternehmen besitzen heute mehrere Domänen für Marketingzwecke, nutzen diese jedoch nur aktiv für den geschäftlichen E-Mail-Verkehr. Selbst wenn SPF korrekt in der Produktionsdomäne bereitgestellt wird, können Angreifer andere Domänen verwenden, die nicht aktiv für eine E-Mail verwendet werden, um die Identität eines Unternehmens zu verfälschen. SPF kann verhindern, dass dies durch einen speziellen "deny all" SPF-Datensatz geschieht - für alle Domänen (und Subdomänen!), die keinen E-Mail-Verkehr generieren, veröffentlichen Sie "v=spf1 -all" im DNS. Ein gutes Beispiel ist openspf.org - die Website des SPF Council.

Da die SPF-Delegierung nur für eine einzige Domäne gilt, ist es wichtig, auch alle SPF-Datensätze für alle Subdomänen zu veröffentlichen, die möglicherweise keine E-Mail generieren. Selbst wenn Ihre Produktionsdomäne einen "regulären" SPF-Datensatz hat, versuchen Sie, "alle" Datensätze Ihren Subdomänen ohne Datenverkehr zu verweigern. Auch hier gilt: Vergessen Sie nicht, dass Empfang nicht gleichbedeutend mit Senden ist: Eine Domäne empfängt zwar sehr wohl E-Mails, wird aber niemals eine Quelle sein. Dies gilt insbesondere für kurzfristige Marketing-

Domänen (z. B. Veranstaltungen, zeitlich begrenzte Werbeaktionen, Produkteinführungen usw.), in denen in diese Domänen eingehende E-Mails an Ihre Produktionsdomäne gesendet werden und alle Antworten auf diese E-Mails aus der Produktionsdomäne gesendet werden. Diese kurzfristigen Domänen verfügen über einen gültigen MX-Datensatz, sollten jedoch über einen SPF-Datensatz verfügen, der sie als keine **Quelle** von E-Mails identifiziert.

Überlegungen zur DKIM-Bereitstellung

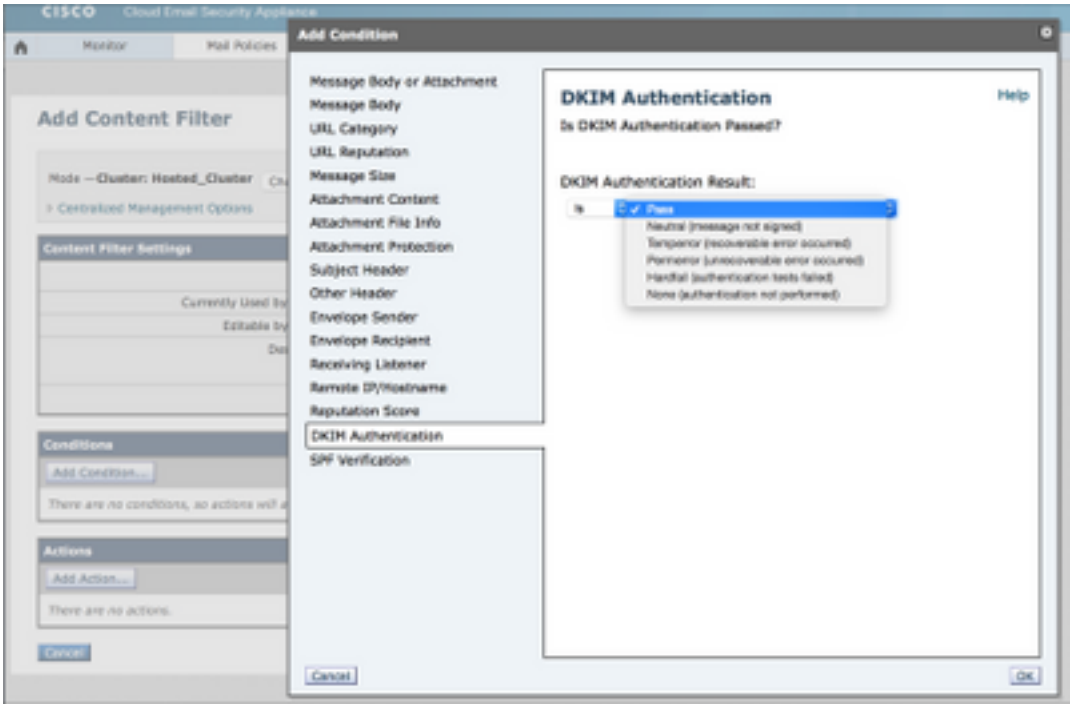
DKIM für Empfänger

Die Konfiguration der DKIM-Verifizierung auf der ESA ähnelt der SPF-Verifizierung. In den Standardrichtlinienparametern von Mail Flow Policies (Mail-Ablaufrichtlinien) wird die DKIM-Verifizierung einfach auf "Ein" gesetzt. Da DKIM keine Richtlinienspezifikation zulässt, wird hier lediglich die Signatur überprüft und ein Header "Authentication-Results" (Authentifizierungsergebnisse) eingefügt:

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

Alle Aktionen, die auf den DKIM-Verifizierungsergebnissen basieren, müssen mithilfe von Content-Filtern ausgeführt werden:

Bild 2: DKIM Verification Content Filter-Bedingung



Im Gegensatz zu SPF, das einfach ist, bearbeitet DKIM den eigentlichen Nachrichtentext, sodass einige Parameter eingeschränkt sein können. Optional können Sie DKIM-Verifizierungsprofile erstellen und verschiedenen Mail Flow-Policys verschiedene Verifizierungsprofile zuweisen. Sie ermöglichen es Ihnen, die Größe der zu akzeptierenden Signaturen zu begrenzen, Aktionen für den Abruf von Schlüsseln festzulegen und die Tiefe der DKIM-Verifizierung zu konfigurieren.

Wenn eine Nachricht mehrere Gateways passiert, kann sie mehrmals signiert werden und daher mehrere Signaturen enthalten. Damit eine Nachricht die DKIM-Verifizierung übergeben kann, müssen **alle** Signaturen überprüft werden. In der Standardeinstellung überprüft die ESA bis zu fünf

Signaturen.

Aufgrund der historischen Offenheit von SMTP und E-Mail und der Zurückhaltung des gesamten Internets, sich an (positive) Veränderungen anzupassen, gibt es immer noch mehrere Situationen, in denen DKIM-Signaturen legitim scheitern könnten, z. B. wenn Mailinglisten-Manager Nachrichten direkt weiterleiten, aber ändern oder wenn Nachrichten direkt und nicht als Anlagen zu neuen Nachrichten weitergeleitet werden. Aus diesem Grund besteht die Best Practice für Nachrichten, die nicht mit DKIM versendet werden, im Allgemeinen weiterhin darin, sie unter Quarantäne zu stellen oder zu kennzeichnen, anstatt sie zu verwerfen.

Vorbereitung auf die Unterzeichnung mit DKIM

Bevor Sie die DKIM-Signierung in Ihrer RELAYED Mail Flow Policy aktivieren können, müssen Sie die Schlüssel generieren/importieren, DKIM-Signaturprofile erstellen und die öffentlichen Schlüssel im DNS veröffentlichen.

Wenn Sie für eine einzelne Domäne signieren, ist der Prozess ganz einfach. Erstellen Sie das Schlüsselpaar, erstellen Sie Ihr einzelnes Signaturprofil im Abschnitt Domain Keys (Domänenschlüssel) der Mail-Policys, und klicken Sie auf die Option Generate (Erstellen) unter "DNS Text Record" (DNS-Textdatensatz), sobald Ihr Profil fertig ist. Veröffentlichen Sie den im DNS generierten Schlüssel. Schalten Sie schließlich die DKIM-Signierung in Ihrer Mail Flow Policy ein.

Wenn Sie mehrere Domänen signieren, wird es komplizierter. In diesem Fall haben Sie zwei Optionen:

1. Verwenden Sie ein einzelnes Signaturprofil, um für alle Domänen zu signieren. Sie speichern den (einzelnen) öffentlichen Schlüssel in der DNS-Zone der "primären" Domäne, und Ihre DKIM-Signaturen verweisen auf diesen Schlüssel. Diese Technik wurde in der Vergangenheit häufig von ESPs eingesetzt. Sie ermöglichte es ihnen, sich in großem Umfang anzumelden, ohne mit dem DNS-Raum einzelner Kunden interagieren zu müssen [5].
2. Erstellen Sie für jede Domäne, für die Sie sich anmelden, ein separates Signaturprofil. Dies macht eine komplexere Erstkonfiguration erforderlich, bietet aber viel mehr Flexibilität. Erstellen Sie ein Schlüsselpaar für jede Domäne, erstellen Sie ein Profil, das nur eine Domäne (und deren Subdomänen) im Abschnitt "Profilbenutzer" angibt, und veröffentlichen Sie den entsprechenden öffentlichen Schlüssel in der DNS-Zone dieser Domäne.

Option 1 ist zwar einfacher, aber dennoch wird DMARC letztendlich nicht mehr funktionieren. Da DMARC vorsieht, dass die Signing Domain-ID mit Header From ausgerichtet werden muss, schlägt die Abstimmung der ID mit DKIM fehl. Wenn Sie den SPF korrekt konfigurieren, können Sie ihn möglicherweise abbestellen und verlassen sich bei der DMARC-Verifizierung auf die SPF-Identifikationsausrichtung.

Wenn Sie Option 2 jedoch von Anfang an implementieren, müssen Sie sich keine Gedanken über DMARC machen. Es ist ziemlich einfach, den Signaturdienst für nur eine Domäne aufzuheben oder neu zu konfigurieren. Wenn Sie **einige** E-Mail-Dienste für eine Drittanbieterdomäne bereitstellen, müssen Sie höchstwahrscheinlich den Schlüssel für die Verwendung von diesen bereitstellen (und ihn in Ihre ESA importieren). Dieser Schlüssel ist domänenspezifisch, daher müssen Sie ein separates Profil erstellen.

Wenn Sie E-Mail-Services von Drittanbietern verwenden

Wenn Sie DKIM-Signierung verwenden und einen Teil Ihrer E-Mail-Verarbeitung (z. B. Marketing-E-Mails) an einen Drittanbieter auslagern, sollten Sie im Allgemeinen nicht möchten, dass dieser dieselben Schlüssel verwendet, die Sie in der Produktion verwenden. Dies ist einer der Hauptgründe für die Existenz von Auswahlern in DKIM. Stattdessen sollten Sie ein neues Schlüsselpaar generieren, den öffentlichen Teil in Ihrer DNS-Zone veröffentlichen und den geheimen Schlüssel an die andere Partei weitergeben. So können Sie diesen Schlüssel auch bei Problemen schnell aufheben und Ihre DKIM-Produktionsinfrastruktur unberührt lassen.

Obwohl es für DKIM nicht erforderlich ist (Nachrichten für dieselbe Domäne können mit mehreren verschiedenen Schlüsseln signiert werden), empfiehlt es sich, für jede E-Mail, die von einem Drittanbieter verarbeitet wird, eine separate Subdomäne bereitzustellen. Dies erleichtert die Nachverfolgung der Meldungen und ermöglicht später eine deutlich sauberere Implementierung von DMARC. Betrachten Sie beispielsweise die folgenden fünf DKIM-Signature-Header aus mehreren Nachrichten von Lufthansa:

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

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

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

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

DKIM-Signatur: v=1; a=rsa-sha1; c=entspannt/entspannt; s=lufthansa5;
d=fly-lh.lufthansa.com;
```

Wir sehen, dass Lufthansa fünf verschiedene Schlüssel (Selektoren) verwendet, die sich auf fünf separate Subdomänen zweier primärer Produktionsdomänen (lufthansa.com und milesandmore.com) aufteilen. Dies bedeutet, dass jede dieser Komponenten unabhängig gesteuert und an einen anderen Messaging-Service-Provider ausgelagert werden kann.

Überlegungen zur DMARC-Bereitstellung

DMARC für Empfänger

Die DMARC-Verifizierung auf der ESA ist profilbasiert. Im Gegensatz zu DKIM muss das Standardprofil jedoch bearbeitet werden, um die Vorgaben zu erfüllen. Das Standardverhalten der ESA besteht darin, keine Nachrichten zu verwerfen, es sei denn, der Kunde hat dies explizit angewiesen. Daher sind für das Standard-DMARC-Verifizierungsprofil alle Aktionen auf "No Action" (Keine Aktion) gesetzt. Darüber hinaus müssen Sie zur Aktivierung der richtigen Berichterstellung im DMARC-Abschnitt "Mail Policies" (Mail-Policys) "Global Settings" (Globale Einstellungen) bearbeiten.

Nachdem ein Profil eingerichtet wurde, wird die DMARC-Überprüfung wie die beiden anderen im Abschnitt Default Policy Settings (Standardrichtlinieneinstellungen) unter Mail Flow Policies (Mail-Ablaufrichtlinien) festgelegt. Aktivieren Sie das Kontrollkästchen, um aggregierte Feedback-Berichte zu senden. Dies ist wohl die wichtigste Funktion von DMARC für den Sender. Zum Zeitpunkt der Dokumenterstellung unterstützt die ESA keine Generierung von Fehlerberichten pro

Nachricht ("ruf"-Tag der DMARC-Richtlinie).

Da der Absender DMARC-Richtlinienaktionen empfiehlt, gibt es im Gegensatz zu SPF oder DKIM keine spezifischen Aktionen, die außerhalb der Profilkonfiguration konfiguriert werden können. Content-Filter müssen nicht erstellt werden.

Die DMARC-Überprüfung fügt dem Authentifizierungsergebnisheader zusätzliche Felder hinzu:

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

Im obigen Beispiel sehen wir, dass die DMARC anhand der DKIM-Identifikations-Alignment verifiziert wurde und dass die vom Sender angeforderte Richtlinie "none" lautet. Dies weist darauf hin, dass sich die DMARC-Bereitstellung derzeit in der "Monitor"-Phase befindet.

Wenn Sie E-Mail-Services für andere Domänen oder Drittanbieter bereitstellen

Die größte Sorge von ESPs hinsichtlich der DMARC-Konformität besteht in der richtigen Abstimmung der Kennungen. Stellen Sie bei der Planung für DMARC sicher, dass Ihr SPF korrekt eingerichtet ist, dass alle relevanten anderen Domänen Ihre ausgehenden Gateways in Ihren SPF-Datensätzen haben und dass keine Nachrichten gesendet werden, die nicht aufeinander abgestimmt werden können, in erster Linie durch Verwendung verschiedener Domänen für MAIL FROM und Header From Identity. Dieser Fehler wird in der Regel durch Anwendungen verursacht, die E-Mail-Benachrichtigungen oder Warnungen senden, da Anwendungsentwickler die Folgen der Inkonsistenz ihrer E-Mail-Identitäten meist nicht kennen.

Stellen Sie wie bereits beschrieben sicher, dass Sie für jede Domäne ein separates DKIM-Signaturprofil verwenden und dass Ihr Signaturprofil korrekt auf die Domäne verweist, für die Sie Signieren, wie in Header From verwendet wird. Wenn Sie Ihre eigenen Subdomänen verwenden, **können** Sie mit einem einzigen Schlüssel signieren, aber stellen Sie sicher, dass Sie DKIM in der DMARC-Richtlinie entspannt einhalten ("adkim="r").

Wenn Sie für eine größere Anzahl von Drittanbietern E-Mail-Services anbieten, die Sie nicht direkt kontrollieren, empfiehlt es sich im Allgemeinen, einen Leitfaden für die Übermittlung einer E-Mail zu verfassen, die am ehesten zugestellt wird. Da sich Benutzer-zu-Benutzer-E-Mails im Allgemeinen gut verhalten, dient dies in den oben genannten Beispielen meist als Richtliniendokument für Anwendungsentwickler.

Wenn Sie E-Mail-Services von Drittanbietern verwenden

Wenn Sie Drittanbieter verwenden, um einen Teil Ihres E-Mail-Datenverkehrs zu übertragen, ist die optimale Methode, eine separate Subdomäne (oder eine komplett andere Domäne) an den Drittanbieter zu delegieren. Auf diese Weise können sie die SPF-Datensätze nach Bedarf verwalten, über eine separate DKIM-Signaturinfrastruktur verfügen und nicht Ihren Produktionsdatenverkehr stören. Anschließend können die DMARC-Richtlinien für ausgelagerte E-Mails anders sein als für interne E-Mails. Stellen Sie, wie bereits erwähnt, bei der Berücksichtigung der von Drittanbietern bereitgestellten E-Mails immer sicher, dass Ihre Identifikatoren übereinstimmen, und Ihre Einhaltung von DKIM und SPF ist in Ihrer DMARC-Richtlinie entsprechend festgelegt.

(Sub)Domänen ohne E-Mail-Verkehr

Eine weitere Verbesserung von DMARC im Vergleich zu vorherigen E-Mail-Authentifizierungstechnologien ist der Umgang mit Subdomänen. Standardmäßig gilt die DMARC-Richtlinie einer bestimmten Domäne für alle Subdomänen. Wenn beim Abrufen von DMARC-Richtliniendatensätzen kein Datensatz auf der Kopfzeile von FQDN-Ebene gefunden werden kann, müssen Empfänger die Organisational Domain [6]des Absenders bestimmen und dort nach einem Richtliniendatensatz suchen.

Die DMARC-Richtlinie für eine Organisationsdomäne kann jedoch auch eine separate Subdomänenrichtlinie ("sp"-Tag eines DMARC-Datensatzes) festlegen, die für alle Subdomänen gilt, für die keine explizite DMARC-Richtlinie veröffentlicht wurde.

In dem zuvor im Kapitel "SPF" beschriebenen Szenario würden Sie:

1. Veröffentlichung eines expliziten DMARC-Datensatzes für alle Subdomänen, die legitime E-Mail-Quellen **sind**.
2. Veröffentlichen Sie eine Subdomain-Richtlinie mit dem Zusatz "Ablehnen" in Ihrem Organizational Domain Policy Record, um automatisch alle E-Mails abzulehnen, die nicht sendende Domänen imitieren

Diese Strukturierung Ihrer E-Mail-Authentifizierung gewährleistet den bestmöglichen Schutz Ihrer Infrastruktur und Marke.

DMARC-spezifische Probleme

Es gibt mehrere mögliche Probleme mit DMARC, die alle auf die Art und die Mängel anderer Authentifizierungstechnologien zurückzuführen sind, auf die sie sich stützt. Das Problem besteht darin, dass DMARC diese Probleme an die Oberfläche brachte, indem es aktiv eine Richtlinie zur Ablehnung der E-Mail weiterleitete und alle unterschiedlichen Absender-IDs in einer Nachricht korrelierte.

Die meisten Probleme treten bei der Verwaltung von Mailinglisten und Mailinglisten auf. Wenn eine E-Mail an eine Mailingliste gesendet wird, wird sie an alle Empfänger weitergeleitet. Die resultierende E-Mail mit einer Absenderadresse des ursprünglichen Absenders wird jedoch von der Hosting-Infrastruktur des Mailinglisten-Managers bereitgestellt, sodass die SPF-Prüfungen für Header From (die meisten Mailinglisten-Manager verwenden die Listenadresse als Envelope From (MAIL FROM) und die Adresse des ursprünglichen Absenders als Header From) fehlschlagen.

Da DMARC für SPF fehlschlagen wird, können wir uns auf DKIM verlassen, aber die meisten Mailinglisten-Manager fügen den Nachrichten auch Fußzeilen hinzu oder markieren Betreffzeilen mit dem Listennamen, wodurch die Verifizierung der DKIM-Signatur unterbunden wird.

Autoren von DKIM schlagen mehrere Lösungen für das Problem vor, die alle auf die Mailing-List-Manager hereinfallen, die die Adresse der Liste in allen From-Adressen verwenden müssen, und die ursprüngliche Absenderadresse auf andere Weise angeben.

Ähnliche Probleme ergeben sich aus Nachrichten, die durch das Kopieren der ursprünglichen Nachricht über SMTP an den neuen Empfänger weitergeleitet werden. Die meisten heute verwendeten Mail-Benutzer-Agenten erstellen jedoch eine neue Nachricht und fügen die weitergeleitete Nachricht entweder inline oder als Anhang zur neuen Nachricht hinzu. Auf diese Weise weitergeleitete Nachrichten werden DMARC weiterleiten, wenn der weiterleitende Benutzer den Test begibt (natürlich kann die Authentizität der ursprünglichen Nachricht nicht hergestellt werden).

Beispiel für einen Aktionsplan zur Implementierung der E-Mail-Authentifizierung

Die Technologien selbst sind zwar einfach, aber der Weg zur Implementierung einer kompletten E-Mail-Authentifizierungsinfrastruktur kann lang und beschwerlich sein. Für kleinere Unternehmen und Unternehmen mit kontrolliertem E-Mail-Verkehr ist dies relativ einfach, für größere Umgebungen jedoch möglicherweise eine außergewöhnliche Herausforderung. Es ist nicht unüblich, dass große Unternehmen Berater für das Management des Implementierungsprojekts einstellen.

Schritt 1: DKIM

DKIM ist relativ unauffällig, da Nachrichten ohne Vorzeichen nicht abgelehnt werden. Berücksichtigen Sie vor der tatsächlichen Umsetzung alle zuvor genannten Punkte. Wenden Sie sich an Dritte, an die Sie die Signierung delegieren könnten, stellen Sie sicher, dass Ihre Drittanbieter die DKIM-Signierung unterstützen, und überlegen Sie Ihre Strategie für das Auswahlmanagement. Einige Organisationen würden separate Schlüssel (Auswahlfelder) für verschiedene Organisationseinheiten behalten. Sie können die regelmäßige Umdrehung der Schlüssel für zusätzliche Sicherheit in Betracht ziehen. Löschen Sie jedoch Ihre alten Schlüssel nicht, bis alle Nachrichten bei der Zustellung zugestellt werden.

Besondere Beachtung sollte den Schlüsselgrößen geschenkt werden. Obwohl im Allgemeinen "mehr ist besser", müssen Sie berücksichtigen, dass das Erstellen von zwei digitalen Signaturen pro Nachricht (einschließlich Canonicalization, etc.) eine sehr CPU-teure Aufgabe ist und kann die Leistung von ausgehenden Mail-Gateways beeinflussen. Aufgrund des Computations-Overhead sind 2048 Bit die größte praktische Schlüsselgröße, die verwendet werden kann. Bei den meisten Bereitstellungen jedoch stellen 1024-Bit-Schlüssel einen guten Kompromiss zwischen Leistung und Sicherheit dar.

Für die erfolgreiche anschließende Implementierung von DMARC sollten Sie:

1. Identifizieren Sie alle Domänen, die Sie als senden, einschließlich Subdomänen.
2. Generieren von DKIM-Schlüsseln und Erstellen von Signierungsprofilen für jede Domäne
3. Bereitstellung relevanter privater Schlüssel für Dritte
4. Veröffentlichung aller öffentlichen Schlüssel in relevanten DNS-Zonen
5. Überprüfen, ob Dritte bereit sind, mit der Unterzeichnung zu beginnen
6. Aktivieren Sie die DKIM-Signierung in RELAYED Mail Flow Policy auf allen Ihren ESAs.
7. Drittanbieter zur Unterzeichnung benachrichtigen

Schritt 2: SPF

Die ordnungsgemäße Implementierung von SPF ist wahrscheinlich der zeitaufwendigste und umständlichste Teil einer E-Mail-Authentifizierungsinfrastruktur. Da die E-Mail sehr einfach zu verwenden und zu verwalten war und vollständig aus Sicherheits- und Zugriffsperspektive geöffnet war, wurden in der Vergangenheit keine strengen Richtlinien bezüglich der Benutzer und der Verwendung durchgesetzt. Daher haben die meisten Unternehmen heute nicht die vollständige Übersicht über alle verschiedenen E-Mail-Quellen, sowohl von innen als auch von außen. Das größte Problem bei der Implementierung von SPF besteht darin, herauszufinden, wer derzeit legitim E-Mails in Ihrem Namen versendet.

Suchkriterien:

1. offensichtliche Ziele - Exchange- oder andere Groupware-Server oder ausgehende Mail-Gateways
2. SvD-Lösungen oder andere E-Mail-Verarbeitungssysteme, die externe Benachrichtigungen generieren können.
3. CRM-Systeme Senden von Informationen für die Interaktion mit Kunden
4. verschiedene Anwendungen von Drittanbietern, die E-Mails senden können
5. Lab-, Test- oder andere Server, die E-Mails senden können
6. PCs und Geräte, die konfiguriert sind, eine externe E-Mail direkt zu senden

Die obige Liste ist nicht vollständig, da Organisationen unterschiedliche Umgebungen haben, sollte jedoch als allgemeine Richtlinie hinsichtlich der gesuchten Elemente angesehen werden. Wenn Sie (die meisten) Ihrer E-Mail-Quellen identifiziert haben, sollten Sie einen Schritt zurück gehen, um die Liste zu bereinigen, anstatt alle vorhandenen Quellen zu autorisieren. Im Idealfall sollten alle ausgehenden E-Mails über die ausgehenden E-Mail-Gateways zugestellt werden, mit einigen berechtigten Ausnahmen. Wenn Sie über eine eigene Marketing-E-Mail-Lösung verfügen oder eine Marketing-Lösung eines Drittanbieters verwenden, sollten Sie eine separate Infrastruktur als die E-Mail-Gateways für die Produktion verwenden. Wenn Ihr Mail-Zustellnetzwerk außergewöhnlich kompliziert ist, können Sie mit der Dokumentation des aktuellen Zustands in Ihrem SPF fortfahren, aber es dauert einige Zeit, um die Situation in der Zukunft zu bereinigen.

Wenn Sie mehrere Domänen über dieselbe Infrastruktur bedienen, können Sie einen universellen SPF-Datensatz erstellen und ihn mithilfe des "include"-Mechanismus in einzelnen Domänen referenzieren. Stellen Sie sicher, dass Ihre SPF-Datensätze nicht zu breit sind. Wenn z. B. nur fünf Computer in einem /24-Netzwerk SMTP senden, fügen Sie diese fünf individuellen IP-Adressen zum SPF hinzu, nicht zum gesamten Netzwerk. Ihre Datensätze sollten möglichst präzise sein, um die Wahrscheinlichkeit von schädlichen E-Mails zu minimieren, die Ihre Identität gefährden könnten.

Beginnen Sie mit einer Softwareausfalloption für nicht übereinstimmende Absender ("~all"). Ändern Sie es nur in "harte" (-alles), wenn Sie 100% sicher sind, dass Sie **alle** E-Mail-Quellen identifiziert haben, ansonsten riskieren Sie, Produktionsmail zu verlieren. Später, nach der Implementierung von DMARC und der vorübergehenden Ausführung im Überwachungsmodus, können Sie alle Systeme identifizieren, die Sie verpasst haben, und Ihre SPF-Datensätze aktualisieren, um vollständig zu sein. Erst dann ist es sicher, den SPF auf hardfail einzustellen.

Schritt 3: DMARC

Sobald Ihr DKIM und SPF so vollständig wie möglich eingerichtet sind, ist es an der Zeit, Ihre DMARC-Richtlinien zu erstellen. Berücksichtigen Sie alle in den vorherigen Kapiteln beschriebenen Situationen, und bereiten Sie die Bereitstellung von mehr als einem DMARC-Datensatz vor, wenn Sie über eine komplexe E-Mail-Infrastruktur verfügen.

Erstellen Sie E-Mail-Aliase, die Berichte empfangen, oder erstellen Sie eine Webanwendung, die Berichte aufnehmen kann. Dafür sind keine streng definierten E-Mail-Adressen erforderlich, aber es ist hilfreich, wenn sie beschreibend sind, z. B. rua@domain.com, dmarc.rua@domain.com, mailauth-rua@domain.com usw. Stellen Sie sicher, dass Sie über einen Prozess verfügen, mit dem ein Bediener diese Adressen überwachen und die SPF-, DKIM- und DMARC-Konfiguration entsprechend ändern kann, oder das Sicherheitsteam im Falle einer Spoofing-Kampagne benachrichtigen kann. Zunächst wird der Workload erheblich sein, wenn Sie die Datensätze so

anpassen, dass alle Fehler während der SPF- und DKIM-Konfiguration abgedeckt werden. Nach einiger Zeit werden Berichte wahrscheinlich nur Spoofing-Versuche anzeigen.

Legen Sie zunächst für Ihre DMARC-Richtlinie "none" und für die forensische Option zum Senden von Berichten für fehlgeschlagene Prüfungen ("fo=1") fest. Dadurch werden schnell Fehler in Ihrem SPF und DKIM erkannt, ohne den Datenverkehr zu beeinflussen. Wenn Sie mit dem Inhalt der eingereichten Berichte zufrieden sind, ändern Sie die Richtlinie in Abhängigkeit von Ihrer Sicherheitsrichtlinie und Ihrer Präferenz in "Quarantäne" oder "Ablehnen". Stellen Sie erneut sicher, dass die Betreiber Ihre empfangenen DMARC-Berichte kontinuierlich auf Fehlalarme analysieren.

Die vollständige und korrekte Implementierung von DMARC ist keine kleine oder kleine Aufgabe. Zwar können einige Ergebnisse (und die formelle "Implementierung" von DMARC) durch die Veröffentlichung unvollständiger Datensätze und einer Richtlinie "none" erzielt werden, doch liegt es sowohl im Interesse der Absenderorganisation als auch des Internets als Ganzes, dass alle diese Datensätze in vollem Umfang implementieren.

Was die Zeitpläne angeht, ist hier eine grobe Übersicht der einzelnen Schritte für ein typisches Projekt. Da jede Organisation anders ist, sind diese alles andere als zutreffend:

1. DKIM-Planung und -Vorbereitung	2-4 Wochen
2. DKIM-Testläufe	2 Wochen
3. SPF = Legacy Sender Identification	2-4 Wochen
4. Vorbereitung von DMARC-Richtlinien	2 Wochen
5. Testlauf für SPF- und DMARC-Datensätze	4-8 Wochen
6. SPF-Testlauf mit Hardwarefehlern	2 Wochen
7. DMARC-Testlauf mit Quarantäne/Ablehnung	4 Wochen
8. Überwachen von DMARC-Berichten und Anpassen von SPF/DKIM	ständig

In kleineren Unternehmen ist die Dauer der meisten Schritte, insbesondere in den Schritten 3 und 4, wahrscheinlich kürzer. Egal, wie einfach Ihre E-Mail-Infrastruktur Ihrer Meinung nach auch sein mag: Sie können während der Testläufe immer ausreichend Zeit zuweisen und Feedback-Berichte genau auf alles überwachen, was Sie verpasst haben.

Größere Unternehmen können eine noch längere Dauer derselben Schritte mit strengeren Testanforderungen erleben. Unternehmen mit komplexer E-Mail-Infrastruktur stellen nicht selten externe Hilfe ein, nicht nur für den technischen Aspekt der E-Mail-Authentifizierung, sondern auch für die Verwaltung des gesamten Projekts und die Koordination zwischen Teams und Abteilungen.

Weitere Referenzen

- Der Referenzstandort für SPF: http://www.openspf.org
- Der DKIM-Rat http://www.dkim.org
- DMARC-Hauptwebsite, ausgeführt von The Trusted Domain Project: http://www.dmarc.org
- dmarcian - eine Hilfe- und Ressourcen-Website, die von Tim Draegen, einem der Autoren von DMARC, betrieben wird. Besuchen Sie unbedingt den Bereich "Tools": http://www.dmarcian.com
- Das Record Validator Tool der Online Trust Alliance: https://otalliance.org/resources/spf-dmarc-record-validator
- DMARC Record Assistant - ein weiteres nützliches Tool zur Erstellung von DMARC-

Datensätzen: http://www.kitterman.com/dmarc/assistant.html
- SPF-Aufzeichnungstesttools: http://www.kitterman.com/spf/validate.html
- "Sei kein Phishing: Deep Dive Into Email Authentication Techniques", eine Präsentation der Cisco Live 2014 BRKSEC-3770: https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=76627

[1] Die Canonicalisierung geht über den Rahmen dieses Dokuments hinaus. Weitere Informationen zur DKIM-Canonicalisierung finden Sie im Abschnitt "Zusätzliche Referenzen".

[2] DKIM DNS-Datensatzparameter sind ebenfalls nicht im Umfang dieses Dokuments enthalten.

[3] Das Erstellen von Nachrichtenfiltern wird in diesem Dokument nicht behandelt. Weitere Informationen finden Sie in AsyncOS für E-Mail-Benutzerhandbücher.

[4] M3AAWG hat eine Reihe hervorragender Best Practices definiert, die von den meisten Branchen angewendet und anerkannt werden. Das Dokument "Best Practices für Absender" ist unter https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf verfügbar.

[5] Dieses Verhalten nutzt die Tatsache, dass ursprünglich DKIM die Nachrichtenquelle nicht überprüft, wie in MAIL FROM oder Header From angegeben. Es wird nur überprüft, ob die Signing Domain ID ("d"-Parameter der DKIM-Signatur und der Parameter "Domain Name" in Ihrem Signing-Profil) tatsächlich den öffentlichen Schlüssel des Paars hosten, das zum Signieren der Nachricht verwendet wurde. Die Authentizität des Absenders wird impliziert, indem der Header "From" (Von) signiert wird. Stellen Sie sicher, dass Sie alle Domänen (und Subdomänen) auflisten, für die Sie im Bereich "Profile Users" (Profilbenutzer) unterzeichnen.

[6] In der Regel liegt eine Domäne unter der TLD-Domäne oder dem entsprechenden ccTLD-Präfix (.ac.uk, .com.sg usw.).