Sender Policy Framework

Die Fälschung von E-Mail-Absenderadressen nimmt Überhand. Das einfache Absender-Authentifizierungsverfahren SPF sorgt für etwas mehr Sicherheit. Und es dient im Kampf gegen Spam als Grundlage für domainbasierte Reputationssysteme. Julian Mehnle

Lange Jahre hatte es gedauert, in denen Internetnutzer dem anschwellenden Phänomen gefälschter E-Mail-Absenderadressen hilflos gegenüber standen, bis 2003 die ersten Verfahren zur Authentifizierung von Absenderadressen aufkamen. In den darauffolgenden Jahren sprossen zahlreiche neue Verfahren wie Pilze aus dem Boden, doch nur einige wenige haben überdauert. Sender Policy Framework (SPF) (1) ist eines davon, und derzeit dasjenige, mit dem mit Abstand höchsten Verbreitungsgrad.

Das Grundkonzept von SPF

Als sogenanntes pfadbasiertes Authentifizierungsverfahren setzt SPF dort an, wo das Konzept des MX-DNS-Records zur Spezifikation der Mailempfangsserver einer Domain endet. Bereits Vorgängerverfahren von SPF wie zum Beispiel Reverse MX (RMX) entwarfen ein direktes Gegenstück zum MX-Record: einen neuen Recordtyp, mit dem eine Domain ihre Versandserver gegenüber Mailempfängern spezifizieren konnte. SPF ging Ende 2003 einen Schritt weiter und ermöglicht es, in einem DNS-Record mit einfachen und doch mächtigen Ausdrücken sehr komplexe Mailversandinfrastrukturen von Domains zu beschreiben, anhand derer Mailempfänger überprüfen können, ob eine eingehende Mail tatsächlich von einem autorisierten Server stammt.

Das Sender Policy Framework, das die IETF mittlerweile als RFC 4408 veröffentlicht hat (2), unterstützt die Authentifizierung sowohl des Servernamens als auch der Umschlag-Absenderadresse (Envelope Sender, Return Path), die das HELO- beziehungsweise MAIL FROM-Kommando des SMTP-Protokolls überträgt. Der Servername, im Folgenden HELO-Domain genannt, dient lediglich Informationszwecken und schlägt sich üblicherweise in den »Received:«-Kopfzeilen nieder, die jeder Übertragungsabschnitt hinzufügt. Die Umschlag-Absenderadresse, im Folgenden MAIL-FROM-Domain genannt, dient sowohl als informative Angabe der Absenderadresse als auch als Rückadresse für Benachrichtigungen bei Zustellungsproblemen – zwei Zwecke, die häufig nicht klar getrennt sind.

Für jede vor Fälschung zu schützende HELO- oder MAIL-FROM-Domain richtet der Domainverwalter einen DNS-Record vom Typ »TXT« oder (neuerdings) »SPF« als sogenanntes Sendeschema (Sender Policy) ein.

Die Konfiguration in **Listing 1** bedeutet beispielsweise, dass ausschließlich die Mailserver mit den IP-Adressen 192.168.0.1 und 192.168.0.2 den Domainname example.com als HELO- oder MAIL-FROM-Domain verwenden dürfen. Anderen Mailserver ist die Nutzung verboten. Entsprechend ist die Verwendung des Domainnames mailout.example.com in »HELO« oder »MAIL FROM« nur von den IP-Adressen 192.168.0.2 und fef0::1 gestattet

Die Anatomie eines SPF-Records

Grundsätzlich besteht ein SPF-Record aus einer Versionsmarkierung (»v=spf1«), auf die eine Reihe von mit Leerzeichen getrennten Direktiven folgt. Eine Direktive kann entweder ein so genannter Mechanismus sein, der letztlich eine Menge von IP-Adressen beschreibt, die zur Verwendung der betreffenden Domain beim Mailversand autorisiert sind, oder ein Modifikator, der die Verarbeitung des SPF-Records beeinflusst. Die verschiedenen unterstützten Mechanismen (**Tabelle 1**) ermöglichen die einfache Abbildung von Mailversandservern.

Wie die Tabelle zeigt, darf man bei den Mechanismen »a« und »mx« den Domainname weglassen, an dessen Stelle tritt dann implizit der zu authentifizierende Domainname – bei der Authentifizierung von example.com ist ein einfaches »a« also eine Abkürzung für »a:example.com«. Die Mechanismen »ip4« und »ip6« ermöglichen, durch einen Schrägstrich abgetrennt, die Angabe einer Netzblock-Größe, jeweils von 0 bis 32 und von 0 bis 128. Auch die Mechanismen »a« und »mx« unterstützen dies, und zwar für IPv4-Netzblöcke (»a/24«), IPv6-Netzblöcke (»a//48«), oder auch beides zugleich (»a/24//48«). In diesen Fällen leitet SPF von den durch DNS-Auflösung erhaltenen IP-Adressen Netzblöcke der entsprechenden Größe ab. In der obigen Beispielkonfiguration entspricht »a:mailout.example.com/24« also dem Netz-

Listing 1: SPF-Konfiguration einer Beispieldomain

```
01 example.com           IN      A       192.168.0.1
02 mailout.example.com   IN      A       192.168.0.2
03 mailout.example.com   IN      AAAA    fef0::1
04 example.com           IN      MX      1 mailout.example.com.
05
06 example.com           IN      TXT     "v=spf1 a mx -all"
07 mailout.example.com   IN      TXT     "v=spf1 a -all"
```

block 129.168.0.0/24 sowie der einzelnen IPv6-Adresse »fef0::1«, während »a:mailout.example.com/24//48« zusätzlich den gesamten Netzblock »fef0::1/48« erfasst.

Mit dem »include«-Mechanismus lassen sich Sendeschemas anderer Domains in das eigene Sendeschema einbeziehen. Dies ist hilfreich, wenn man neben der eigenen Versandinfrastruktur manchmal eine fremde benutzt (zum Beispiel beim Mailversand über ein Mobiltelefon), oder wenn man die eigene Domain gänzlich auf fremder Infrastruktur hostet. Google bietet dafür beispielsweise unter dem Domainnamen aspmx.googlemail.com gezielt einen eigenen SPF-Record an, auf den Nutzer dann per »include:aspmx.googlemail.com« verweisen können.

Die Parametrisierung von Domainnamen über Makros, wie in der Tabelle für den »exists«-Mechanismus angedeutet, stellt eine fortgeschrittene Möglichkeit dar, komplexere oder gar dynamische Infrastrukturen zu definieren. Die verschiedenen unterstützten Makros, wie auch der »exists«-Mechanismus und die Modifikatoren, sind in der SPF-Spezifikation (2) beschrieben.

Tabelle 1: SPF-Mechanismen zur Beschreibung autorisierter IP-Adressen

Mechanismus	Bedeutung	Beispiel
ip4	IPv4-Adresse oder -Netzblock	ip4:192.168.0.1
		ip4:192.168.0.0/24
ip6	IPv6-Adresse oder -Netzblock	ip6:fef0::1
		ip6:fef0::1/48
a	Auflösung eines A-Records zu einer oder mehreren IP-Adresse(n)	a
		a:mailout.example.com
mx	Auflösung eines MX-Records zu einer oder mehreren IP-Adresse(n)	mx
		mx:example.net
exists	Abfrage eines A-Records ähnlich einer DNS-Blacklist	exists:%{ir}._spf.%{d}
include	Einbeziehung des Sendeschemas einer anderen Domain	include:example.net
all	Alle möglichen IP-Adressen	all

Auswertung des Sendeschemas

Es ist möglich, jedem Mechanismus einen so genannten Qualifikator voranzustellen, der die Logik des Mechanismus verändert. So lässt sich über ein vorangestelltes »-« (Minus) die Autorisierung einer Menge von IP-Adressen in ein ausdrückliches Verbot verkehren, wie zum Beispiel in »-all«, was alle IP-Adressen verbietet, die nicht zuvor ausdrücklich autorisiert wurden. Ein »~« (Tilde) ist ein abgeschwächtes Verbot, das Empfängern rät, Mails von derart gekennzeichneten IP-Adressen nicht geradewegs abzuweisen, sondern vielleicht nur als verdächtig zu markieren. Ein »?« bezeichnet Unschlüssigkeit – häufig in einem abschließenden »?all« verwendet. In diesem Fall sind die Adressen so zu behandeln, als ob es keinerlei SPF-Record gäbe. Das optionale »+« ist die Standardlogik.

Der Empfänger einer E-Mail, der die HELO- oder MAIL-FROM-Domain authentifizieren möchte, sucht nun im DNS unter der entsprechenden Domain nach einem SPF-Record. Findet er einen, so betrachtet er die darin enthaltenen Mechanismen der Reihe nach und sucht nach Übereinstimmungen mit der IP-Adresse des einliefernden Mailservers. Führt einer der Mechanismen zu einem Treffer, so bestimmt sein Qualifikator das Ergebnis der Authentifizierung.

Fehlerbehandlung

DNS-Timeouts und einige andere DNS-Fehler betrachtet der Empfänger dabei als vorrübergehende Fehler in der SMTP-Transaktion und beantwortet sie üblicherweise mit einem temporären Fehlercode (4xx). Syntax-Fehler oder die Überschreitung von gewissen Sicherheitsschranken sind dauerhafte Fehler, die der Verwalter des SPF-Records beheben muss. Eine Übersicht der möglichen Ergebnis-Codes und deren Bedeutung findet sich in **Tabelle 2**.

Ist die IP-Adresse des einliefernden Mailservers zur Verwendung der Domain in »HELO« oder »MAIL FROM« autorisiert, dann ist die Authentifizierung der Domain erfolgreich. Andernfalls liegt eine Fälschung vor. Die Reaktion des Empfängers auf den einen oder anderen Fall

spezifiziert SPF jedoch mit wenigen Ausnahmen nicht, da der Empfänger in der Regel ohnehin die aus seiner Sicht nützlichste Reaktion wählt und eine mögliche Vorschrift meist ignorieren würde. SPF fordert lediglich, dass das Ergebnis »Neutral« exakt wie »None« zu behandeln ist, und gibt einige Empfehlungen zur Behandlung von Fehlerfällen.

Paradigmenwechsel bei MAIL-FROM-Adressen

SPF setzt auf einen kleinen Paradigmenwechsel in Bezug auf die zwiespältige Interpretation der MAIL-FROM-Adresse. Die SMTP-Spezifikation definiert diese einerseits als Absenderadresse, andererseits aber als Rückadresse für DSNs. Diese beiden Definitionen geraten miteinander in Konflikt, sobald jemand eine E-Mail von einem anderen Postfach als jenem verschickt, das als Rückadresse für DSNs gewünscht ist – zum Beispiel weil der Benutzer gerade den E-Mail-Dienst des Mobilfunkanbieters verwendet. Soll er nun die E-Mail-Adresse seines Mobilfunkpostfachs angeben, oder die seines Hauptpostfachs? SPF vereinheitlicht die Definitionen zugunsten der tatsächlichen Absenderadresse und erzwingt damit implizit, dass DSNs immer auch an den ursprünglichen Versender zurück gelangen. In der Tat war auch die Flutwelle an DSNs, die aufgrund von Absenderadressfälschungen unschuldige Domains überschwemmte, eine der Initialzündungen für die Entwicklung von SPF. (Ein weiterer Beitrag dieser Ausgabe geht auf dieses Backscatter-Problem ausführlich ein.)

Eine konzeptionelle Konsequenz dieser vereinheitlichten Definition ist, dass es zwischen der Netzwerkinfrastruktur einer SPF-geschützten Absenderdomain und der einer SPF-bewussten Empfängerdomain keine grauen Bereiche mehr geben kann, die eine E-Mail auf ihrem Übertragungsweg „irgendwie“ durchquert. Das äußert sich insbesondere im häufig beschworenen »Forwarding-Problem«, das kommerzielle Weiterleitungsdienste, aber auch klassische Alias- beziehungsweise ».forward«-Weiterleitungen betrifft.

Empfängt ein sogenannter Forwarder eine E-Mail von einer SPF-geschützten Domain, so leitet er sie an eine neue Empfängeradresse weiter, in aller Regel jedoch unter Beibehaltung der

ursprünglichen MAIL-FROM-Adresse. Führt der endgültige Empfänger nun eine SPF-Authentifizierung durch, so schlägt diese fehl, da der Forwarder nicht Teil des Sendeschemas der ursprünglichen MAIL-FROM-Domain ist. Der Forwarder ist von einem Adressfälscher schlicht nicht zu unterscheiden.

Allerdings unterliegen praktisch alle derartigen Weiterleitungen der Kontrolle des Empfängers, so dass es ihm möglich ist, jene Mails von der SPF-Authentifizierung auszunehmen, die ihn über die von ihm konfigurierten Weiterleitungen erreichen. Konsequenterweise sollte die SPF-Authentifizierung dann natürlich auf den Systemen stattfinden, die die Weiterleitungen durchführen.

Kurz: die SPF-Authentifizierung sollten immer die Mailempfangsservern an der Außengrenze einer Domain duchführen. In der Praxis gibt es nur relativ wenige Berichte über weiterleitungsbedingte Probleme mit SPF, zumal die Verbreitung problematischer Weiterleitungen erheblich geringer ist, als auf den ersten Blick vielleicht zu vermuten wäre. Im Fall des Falles ist SPF-bedingten DSNs die Zieladresse einer Weiterleitung zu entnehmen, so dass der Absender sein Adressbuch ergänzen und die nicht zugestellte Mail erneut und direkt an die Zieladresse senden kann. Mailinglisten sind übrigens grundsätzlich nicht betroffen, da sie regelmäßig vor der Verteilung einer Mail deren MAIL-FROM-Adresse auf ihre eigene Domain umschreiben.

Tabelle 2: SPF-Ergebnis-Codes und deren Bedeutung

Qualifikator	Ergebnis-Code	Bedeutung
+ Die Verwendung der Domain ist autorisiert	Pass	
-	Fail	Die Verwendung der Domain ist nicht autorisiert
~	SoftFail	Die Verwendung der Domain ist nicht autorisiert, jedoch Vorsicht!
?	Neutral	Über die Verwendung der Domain wird keine Aussage getroffen
	TempError	Ein vorrübergehender Fehler ist aufgetreten, zum Beispiel ein DNS-Timeout
	PermError	Ein dauerhafter Fehler ist aufgetreten, zum Beispiel ein Syntax-Fehler im SPF-Record
	None	Es wurde kein SPF-Record für die Domain gefunden

Ausbringen und Testen

Wie alle E-Mail-Absenderauthentifikationssysteme hat die Umsetzung von SPF zwei Seiten: die Absenderseite und die Empfängerseite. Wer den vollen Nutzen einfahren möchte, muss beides berücksichtigen. Auf der Absenderseite gilt es, ein vollständiges Sendeschema für die Mailversandinfrastruktur seiner Domain zu entwickeln, das alle tatsächlich für den Versand verwendeten Mailserver umfasst. Dies geht am besten in Absprache mit allen für die Infrastruktur Verantwortlichen.

Weiter sind SPF-Records – wie MX-Records – bei späteren Änderungen der Infrastruktur anzupassen. Bei der Erstellung eines Sendeschemas ist zu beachten, dass SPF-Records zur Authentifizierung nicht nur der MAIL-FROM-Domain, sondern auch der HELO-Domain dienen. Technisch betrachtet ist die Einrichtung von Sendeschemata sehr einfach, da lediglich DNS-Records des Typs »TXT« in der betroffenen DNS-Zone angzulegen sind. BIND ab Version 9.4 und aktuelle Versionen einiger anderer DNS-Server-Produkte unterstützen auch den speziell für SPF reservierten Record-Typ »SPF« mit dem Typ-Code 99. Im Zweifelsfall empfiehlt sich die gleichzeitige Konfiguration von identischen Records beider Typen. Es gibt bereits eine Reihe von Werkzeugen, die bei der Erstellung von SPF-Records helfen beziehungsweise mit denen sich deren Korrektheit einfach prüfen lässt **(3)**.

Verbreitung

Auf Empfängerseite beschränkt sich der Aufwand auf den Einsatz eines SPF fähigen Mailservers. Die meisten Open-Source-Server unterstützen SPF inzwischen entweder von Haus aus oder es gibt entsprechende Erweiterungsmodule mit SPF-Unterstützung **(4)**, nicht zuletzt Spamassassin. Auch viele kommerzielle Server haben SPF bereits implementiert.

Untersuchungen zur SPF-Verbreitung

Zur absenderseitigen Verbreitung von SPF gibt es mittlerweile einige Untersuchungen (5). Trotz des inhärenten Henne/Ei-Problems solch zweiseitiger Verfahren, bei denen der Nutzen des Absenders von der Verbreitung auf Empfängerseite und der Nutzen des Empfängers von der Verbreitung auf Absenderseite abhängt, hat sich der Einsatz von SPF nach 2004 schnell ausgebreitet. Laut der Measuring Factory (6) hatten im August 2006 fünf Prozent aller .com- und .net-Second-Level-Domains einen SPF-Record veröffentlicht. Im Oktober 2007 waren es 12,6 Prozent. Das WIDE-Projekt (7) beobachtet laufend den Verbreitungsgrad unter .jp-Third-Level-Domains, der von 3,5 Prozent im August 2006 über 7,5 Prozent im Oktober 2007 auf zuletzt beachtliche 17,3 Prozent im Januar diesen Jahres anstieg.

Offensichtlich variiert das Volumen an versandten Mails von Domain zu Domain und während einige, wenige Domains einen Großteil aller versandten Mails verantworten, gehen von anderen Domains nur wenige oder gar keine Mails aus. Daher ist auch der Verbreitungsgrad relativ zum E-Mail-Volumen einer Domain von Interesse. Im Jahr 2006 berichtete Google auf der Conference on Email and Anti-Spam (CEAS) (8), zum damaligen Zeitpunkt seien rund 20 Prozent des von Google Mail empfangenen Spams sowie rund 40 Prozent des Nicht-Spams mit SPF authentifiziert gewesen. Microsoft berichtete Ende 2007 auf dem Spam Summit (9) der US Federal Trade Commission von aus seiner Sicht etwa 45 Prozent des Nicht-Spams, die mit dem auf SPF aufsetzenden Verfahren »SenderID« (siehe unten), also im Wesentlichen mit SPF, authentifiziert geweseb seien und schätzte die weltweite Anzahl der für E-Mail-Versand verwendeten Domains mit SPF-Records auf knapp 12 Millionen.

Die empfängerseitige Verbreitung ist naturgemäß schwer zu messen, wenn man von Messwerkzeugen wie einem klassischen Spam-Run einmal absieht. Allerdings haben sich in den letzten Jahren eine Menge größerer und kleinerer E-Mail-Diensteanbieter dazu bekannt, eingehende Mails einer SPF-Authentifizierung zu unterziehen, darunter Anbieter mit

so bekannten Namen wie beispielsweise AOL, Google, oder Microsoft.

Microsoft's Konkurrenz: die SenderID

Da die Umschlagadressen einer E-Mail, also »HELO« und »MAIL FROM«, sich nach dem Empfang per SMTP zwar in diversen Kopfzeilen niederschlagen, aber kein Mail-Clients sie angezeigt, bietet SPF keinen Schutz gegen die Fälschung der für den Benutzer sichtbaren Absenderadressen, wie er zur Bekämpfung des Phishing-Phänomens vonnöten wäre. Daher entwarf Microsoft 2004 in einem klassischen Fall von Embrace & Extend eine Erweiterung zu SPF namens SenderID (10), die es sich zum Ziel setzte, zusätzlich die üblicherweise angezeigten Kopfzeilenadressen zu authentifizieren.

Zu diesem Zweck definiert SenderID eine neue, virtuelle Absenderadresse mit der Bezeichnung Purported Responsible Address (PRA), die sich aus vier verschiedenen echten Kopfzeilen ableitet: »Resent-Sender:«, »Resent-From:«, »Sender:«, »From:«. »Resent-*:«-Kopfzeilen entstehen bei einer manuellen Weiterleitung einer E-Mail. Existiert nun keine der »Resent-*:«-Kopfzeilen, dann entspricht die PRA der »Sender:«-Adresse, beziehungsweise der »From:«-Adresse falls auch erstere nicht existiert. Ansonsten betrachtet man einzelne zusammenhängende Blöcke von »Resent-*:«-Kopfzeilen und die PRA entspricht dann der »Resent-Sender:«- beziehungsweise »Resent-From:«-Adresse im obersten, das heißt jüngsten Block.

Sender-ID-Records beginnen mit einer geänderten Versionsmarkierung (»spf2.0«, ohne »v=«), an die sich der Geltungsbereich (scope) des Records anschließt, also die mit dem beschriebenen Sendeschema authentifizierbaren Adresstypen. Mögliche Geltungsbereiche sind: »mfrom«, »pra«, und »mfrom,pra«, insgesamt also zum Beispiel: »spf2.0/mfrom,pra«. Ansonsten ist SenderID weitgehend identisch mit SPF – in der Tat referenziert die relativ kurze Sender-ID-Spezifikation im Wesentlichen die SPF-Spezifikation.

Mehrwert zweifelhaft

Allerdings bietet SenderID bei genauer Betrachtung keinen praktischen Mehrwert gegenüber SPF, denn effektiv schützt es lediglich die »Resent-Sender:«-Adresse vor Fälschung. Da die aber die allermeisten Mail-Clients ebenso wenig anzeigen wie die Umschlagadressen, reicht es aus Sicht eines Fälschers völlig aus, diese Adresse ungefälscht zu belassen oder eine ungeschützte Domain zu verwenden, um den Schutz der anderen, für den Benutzer sichtbaren Kopfzeilenadressen zu unterlaufen.

Marketinggetrieben

Neben einem den eigentlich trivialen PRA-Algorithmus umfassenden Microsoft-Patent bietet die Sender-ID-Spezifikation aus einem weiteren Grund Anlass zu einer Kontroverse: Sie definiert SPF-Records mit der klassischen »v=spf1«-Versionsmarkierung rückwirkend als mögliche Grundlage für die PRA-Authentifizierung. Verschiedene Äußerungen Microsofts sowie die damals wie heute verschwindend geringe Verbreitung von »spf2.0«-Records legen die Vermutung nahe, dass diese technisch fragwürdige Entscheidung vor allem dem Wunsch geschuldet ist, den beträchtlichen Stamm bestehender SPF-Records als Werbeargument unter dem Mantel von SenderID zu verwenden. Diese Kontroverse war, neben dem PRA-Patent, auch der Grund für die Lähmung und den anschließenden Auseinanderbruch der MARID-Arbeitsgruppe der IETF im Jahr 2004, die angetreten war, um aus den zahlreichen damals konkurrierenden Verfahren einen gemeinsamen IETF-Standard zu schmieden. Der Bruch führte dann dazu, dass die IETF sowohl SPF als auch SenderID lediglich als RFCs mit »experimental«-Status veröffentlichte.

Reputationssysteme

Bislang fanden sich im Werkzeugkasten der Spambekämpfung neben inhalts- und verhaltensbasierten Filtern hauptsächlich DNS-Blacklists, die anhand verschiedener Kriterien als spamverdächtig ausgewählte IP-Adressen führen. Betrachtet man die zunehmende Bedeutung von Botnetzen, die aus kompromittierten Endbenutzerrechnern bestehen, für die Spamverteilung, so ergibt sich schnell, dass der Ansatz IP-Adressen-basierter Reputationssysteme nur zu beschränktem Erfolg führen kann. Aus einem Grund: neue, unverbrauchte IP-Adressen können Spammer zu einfach und zu kostengünstig erlangen.

Über den von SPF geleisteten Fälschungsschutz hinaus ergibt sich mit authentifizierten Absenderdomains nun ein wichtiges und zukunftsträchtiges Sprungbrett: domainbasierte Reputationssysteme. Die einfachste Variante sind

Right-Hand-Side Blacklists (RHSBLs, »rechte Seite des @«), das domainbasierte Äquivalent zu klassischen DNS-Blacklists. Wie letztere ergeben RHSBLs binäre Urteile – sie klassifizieren gutartige oder bösartige Absender – allerdings hier eben bezogen auf Domains. Komplexere Systeme, die auch graduelle Urteile fällen und die teilweise sogar dezentral organisiert sind, werden derzeit erforscht.

Schon weil Domains für Spammer deutlich schwieriger oder teurer zu beschaffen sind als fremde IP-Adressen, bietet dieser Ansatz einen Vorteil. Darüberhinaus lässt sich eine außerordentlich schlechte oder gute Reputation einer Domain durch die inhärent hierarchische Struktur des DNS auch wesentlich einfacher und effizienter skalieren als die einer IP-Adresse. Zwar gibt es öffentlich zugängliche Datenbanken wie das WHOIS oder RouteViews.org, die Auskunft über die Netzblockzugehörigkeit von IP-Adressen geben können, jedoch sind diese Dienste entweder für Massenabfragen zu ineffizient oder auf die Kooperation von Netzwerkinhabern angewiesen.

Fazit: Wo steht das Sender Policy Framework?

Insgesamt dürfte SPF die kritische Masse überschritten und damit den Durchbruch als pfadbasiertes Absenderauthentifizierungsverfahren erreicht haben. Allerdings ist derzeit unter E-Mail-Empfängern keine Tendenz absehbar, SPF-lose Domains schlechter zu behandeln als solche Domains, die ein SPF-Sendeschema veröffentlicht haben. Dagegen ahnden die Empfänger allerdings Authentifizierungsfehlschläge durchaus drastisch. Auch wenn sich vor allem große Diensteanbieter konservativ verhalten und noch vor einer strikten Abweisung von E-Mails mit laut SPF gefälschten Absenderadressen zurückschrecken, so schlägt zum Beispiel ein SPF-»Fail« bei Spamassassin (11) mit heftigen 2,6 Spampunkten zu Buche.

Pfadbasierte Authentifizierungsverfahren wie SPF und kryptografische Verfahren wie DomainKeys/DKIM ergänzen sich, da beide Klassen von Verfahren unterschiedliche Problemfelder abdecken.

Während SPF vor Fälschungen der für den E-Mail-Transport wichtigen Umschlagadressen schützt, verschaffen DomainKeys und womöglich DKIM der Fälschung der für den Benutzer sichtbaren Adressen Abhilfe. Die Verfahren unterliegen auch jeweils klassenspezifischen inhärenten Schwächen – SPF bei Alias-Weiterleitungen, DK/DKIM bei Nachrichtenmodifikation durch Forwarder und Mailinglisten –, so dass eine Kombination der verschiedenen Verfahren nahe liegt und in der Praxis zu erwarten sein dürfte.

Gemeinsam mit den benachbarten Verfahren stellt SPF eine Lösung für das lang beklagte Problem der E-Mail-Absenderadressfälschung dar. Und obwohl Spammer 2004 unter den Ersten waren, die SPF-Records veröffentlichten, werden dank SPF und Co. domainbasierte Reputationssysteme zukünftig eine schlagkräftige Waffe auch im Kampf gegen Spam sein. *(jcb)* ■■■

Infos

(1) SPF-Projekt: (http://www.openspf.org)

(2) SPF-Spezifikation: (http://www.openspf.org/RFC_4408)

(3) Werkzeuge für Erstellung und Test von SPF-Records: (http://www.openspf.org/Tools)

(4) Mailserver und Module mit SPF-Unterstützung: (http://www.openspf.org/Implementations#mtas)

(5) Statistiken zur Verbreitung: (http://www.openspf.org/Statistics)

(6) Measurement Factory: (http://www.measurement-factory.com/)

(7) WIDE Project (Widely Distributed Integrated Environment: (http://www.wide.ad.jp)

(8) Conference on Email and Anti-Spam (CEAS): (http://www.ceas.cc)

(9) Spam Summit der Federal Trade Commission (FTC): (http://www.ftc.gov/bcp/workshops/spamsummit)

(10) Microsofts SenderID: (http://www.microsoft.com/mscorp/safety/technologies/senderid/default.mspx)

(11) SpamAssassin-Homepage: (http://spamassassin.apache.org)

Der Autor

Julian Mehnle ist als selbstständiger Softwareentwickler und -designberater tätig. Seit 2003 ist er an der Entwicklung, Standardisierung und Implementation des Sender Policy Framework beteiligt und war im vergangenen Jahr Mitglied des SPF Council. Im Übrigen kennt er sich auf den Gebieten E-Mail-Technik und speziell E-Mail-Sicherheit, sowie SQL-Datenbanken, Perl und I18N besonders gut aus.