Peter Wullinger
Rechenzentrum
Abteilung Kommunikations- und Informationsdienste

Christian-Albrechts-Universität zu Kiel
Rechenzentrum

Autor	Peter Wullinger
Letzte Änderung	2022-09-27
Version	1.3
Revision	19

Festlegung Mailversendender Systeme an der CAU

Einsatz des Sender Policy Frameworks

Inhaltsverzeichnis

Änderungen

Version 1.3: Subdomain _spfx → spfx

Einleitung

Das *Sender Policy Framework* ist ein Verfahren, dass es erlaubt, die *erlaubten Versender* für E-Mails festzulegen. Festgelegt wird hierbei, welche Systeme (IP-Adressen, Servernamen) innerhalb einer E-Mail-Domäne E-Mails verwenden dürfen.

Peter Wullinger
Rechenzentrum
Abteilung Kommunikations- und Informationsdienste

Auf diese Weise erhalten Empfänger von E-Mails die Möglichkeit zu prüfen, ob eingelieferte Nachrichten über die dafür deklarierten Systeme des Absenders versendet wurden, oder ob möglicherweise eine Absender-Fälschung vorliegt.

Geprüft wird an dieser Stelle der Absender auf Protokollebene (SMTP-From, Envelope-From), nicht der in der E-Mail genannte Absender (Header-From). Die Überprüfung kann aus diesem Grund vor Annahme der E-Mail durchgeführt werden. Eine Prüfung ist daher resourcenschonend möglich.

SPF findet immer mehr Verbreitung und wird insbesondere von diversen großen E-Mail-Anbietern eingesetzt. Uns erreichen auch Berichte aus dem Campus, dass einige Einrichtungen E-Mails ohne SPF-Eintrag (d.h. wenn der SPF-Eintrag fehlt, nicht wenn die SPF-Prüfung negativ ausfällt) ganz ablehnen.

Trotz auch kritischer Stimmen[1] erscheint eine Einführung von SPF auch an der CAU dennoch notwendig und sinnvoll.

Konzept

SPF-Richtlinien (Policies) werden für jede DNS-Domäne separat definiert. So haben SPF-Richtlinien für `@uni-kiel.de` keinen Einfluß auf z.B. `@tf.uni-kiel.de`.

Basis-Regelsatz

SPF erlaubt über einen domänen-spezifischen Regelsatz die Festlegung, ob E-Mails mit Absender innerhalb der Domäne, die von einem bestimmten Rechner (IP-Adresse) ausgehen, in eine von drei Kategorien fallen:

erlaubt, pass, +	Der Rechner ist berechtigt E-Mails (für diese Domäne, mit diesem Absender) einzuliefern.
neutral, ~	Keine Angabe darüber, ob der Rechner berechtigt ist, E-Mails einzuliefern.
verweigern, fail, -	Der Rechner ist *nicht* berechtigt, E-Mails einzuliefern.

Die entsprechenden Richtlinien werden im DNS des Absenders hinterlegt und von dort abgerufen.

Grundsätzlich soll der Versand von E-Mails innerhalb von E-Mail-Domänen, die durch das Rechenzentrum verwaltet werden (RZ-E-Mail-Domänen) ausschließlich über die Systeme des Rechenzentrums versendet werden. Im Großteil des Campus wird diese Regelung erzwungen, indem die beiden relevanten Ports SMTP (25) und SMTPS (465) für den E-Mail-Versand nach außen gesperrt sind

1 z.B. https://www.heinlein-support.de/blog/news/gmx-de-und-web-de-haben-mail-rejects-durch-spf/

Der SPF-Basisregelsatz sieht daher vor, dass wir zunächst nur die Mailtransportrechner (Relays) und den/die Listserver des Rechenzentrums für den Versand freischalten. Die betroffenen Rechner befinden sich alle im Netzbereich *134.245.11.192/27*, bzw. *2a0a:6200:0:3::/64*.

Wir setzen diese Basisregeln als Standard für RZ-E-Mail-Domänen um. Einrichtungen mit eigener E-Mail-Anbindung (TF, Informatik) sind gebeten, eigene Regeln zu definieren.

Um Probleme bei bestehenden Systemen zu verbinden, setzen wir für alle anderen Rechner das Ergebnis der Bewertung auf *neutral* (~). Eine Verschärfung hin zum Verbot des Versands über nicht explizit freigegebene Rechner ist mittelfristig angedacht.

Anforderungen für Einrichtungen

Mit der Festlegung von SPF-Regeln erhöhen sich die Anforderungen für Institute der CAU, sofern

- die DNS-Einträge von E-Mail-Domänen extern gehostet werden. Hierbei müssen die SPF-Einträge dann entsprechend unserer Beratung selbst gepflegt werden.
- E-Mails über andere Systeme als die im Basisregelsatz vorgesehenen versendet werden sollen. Insbesondere ist entweder ein dauerhafter Kommunikationskanal zwischen externem Betreiber und Institut/Rechenzentrum oder eine Delegation der SPF-Einträge notwendig.

Fehlende oder fehlerhafte SPF-Richtlinien führen sonst unter Umständen dazu, dass E-Mails mit Absendern für Domänen der Universität, die auf anderen als den definierten Wegen bei Empfängern eingehen, abgelehnt oder als SPAM erkannt werden.

Dementsprechend ist eine Abstimmung immer notwendig, sobald einer der obigen Fälle eintritt. Dies erhöht auch die Anforderung an externe Dienstleister, da diese mit den entsprechenden Verfahren umgehen können müssen.

Ausnahmen und Erweiterungen

Der Basisregelsatz sollte für die meisten Versendevorgänge ausreichend sein. Allerdings gibt es unterschiedliche Ausnahmefälle, die beim Regelkonzept berücksichtigt werden müssen. Insbesondere relevant ist hierbei der Versand über separate Server, sowohl aus dem Campusnetz als auch über externe Anbieter.

Die beantragende Institution ist hierbei für die Absprache mit dem externen Dienstleister verantwortlich. Wichtig ist, dass Änderungen den Postmastern möglichst vor der Umsetzung mitgeteilt werden, damit die nötigen Einträge im DNS aktualisiert werden können.

Wir definieren unterschiedliche Freigabe-Varianten:

EXT-DOMAIN Freigabe eines externen Rechners anhand seiner IP-Adresse für den Mailversand mit beliebigen Absender-Adressen unterhalb einer Domäne.

Es ist notwendig, den Postmastern die IP-Adresse(n) der versendenden Systeme mitzuteilen. Bei Änderungen ist eine Information über die Änderung an die Postmastern nötig.

EXT-ADDRESS Freigabe einer oder mehrerer E-Mail-Adressen für den Mailversand.

Hierbei werden nur einzelne E-Mail-Adressen für den separaten Versand für eine Liste von IP-Adressen freigegeben.

Es ist notwendig, den Postmastern die betroffenen E-Mail-Adressen sowie die IP-Adresse(n) der versendeten Systeme mitzuteilen. Bei Änderungen ist eine Information über die Änderung an die Postmastern nötig. die nötigen Einträge im DNS aktualisiert werden können.

EXT-RANGE Freigabe eines Adressbereichs für den Mailversand mit beliebigen Absenderadressen unterhalb einer Domäne.

Es ist notwendig, den Postmastern die Adressbereiche der versendenden Systeme mitzuteilen. Bei Änderungen ist eine Information über die Änderung an die Postmastern nötig.

EXT-HOST Freigabe eines oder mehrerer Rechner auf Basis Ihres Rechnernamens (DNS-Eintrag). Diese Vorgehen ermöglicht gegebenenfalls eine Teil-Delegation der Freigabe an Externe, sofern die DNS-Einträge extern vorgehalten werden.

Es ist notwendig, den Postmastern die DNS-Namen der versendenen Systeme mitzuteilen. Es ist durch geeignete Maßnahmen sicherzustellen, dass die entsprechend DNS-Einträge mit der nötigen Sorgfalt gepflegt werden. Bei Änderungen ist eine Information über die Änderung an die Postmastern nötig.

DELEGATE Vollständige oder Teil-Delegation der SPF-Einträge an Externe. Hierbei wird in der SPF-Richtlinie ein Verweis auf eine extern gepflegte Richtlinie eingetragen.

Es ist notwendig, den Postmastern die Domänen (TXT-Einträge) für das Ziel der Delegation anzugeben. Änderungen können eigenständig im Abstimmung mit dem externen Dienstleister abgesprochen werden. Die Postmaster behalten sich bei konkreten Verdacht auf Missbrauch eine Rücknahme der Delegation vor. In diesem Fall wird die betroffene Einrichtung über die Sperre informiert.

Es sollen bevorzugt die Varianten EXT-DOMAIN und EXT-ADDRESS verwendet werden. Hierfür ist allerdings sicherzustellen, dass Änderungen bei externen Dienstleistern mit ausreichend Vorlauf an das RZ weitergegeben werden. Veraltete Einträge führen gegebenfalls zur Klassifikation von E-Mails als Spam oder zur Ablehnung von E-Mails.

Die Varianten EXT-RANGE, EXT-HOST und DELEGATE sollen sparsam verwendet werden. Das RZ setzt entsprechende Einträge nur, wenn eine dauerhafte, fachlich ausreichende Betreuung durch die Einrichtung sichergestellt ist.