

Secure Mail Service

Funktionsbeschreibung

1 Grundsätzliche Mail-Topologie – SMTP

In der DNS-Zone der Domain des Kunden werden als Mail-Exchanger (MX-Record) die Mailserver von weblucid eingetragen. Diese werden dann von den Versendern von Emails angesprochen, wenn Mails an die Domain gesendet werden sollen.

Die Server von weblucid senden die Mails dann – nach erfolgter Prüfung und Filterung – an den Mailserver des Kunden weiter. Dazu ist keine Konfigurationsänderung auf dem Kunden-Mailserver erforderlich, da dieser die eingehenden Mails protokolltechnisch genau wie ohne den weblucid Secure Mail Service empfängt. Mit dem Unterschied, dass alle Mails zunächst über weblucid geleitet werden.

Um seinen Mailserver vor Angriffen auf IP- und SMTP-Ebene besser zu schützen, kann und sollte der Kunde seine Firewall so einstellen, dass aus dem Internet nur noch die Server von weblucid Verbindung via SMTP (TCP Port 25) aufnehmen können.

Ausgehende Mails kann der Mailserver des Kunden nach wie vor direkt versenden. Es ist jedoch sehr empfehlenswert, auf dem Kunden-Mailserver die Server von weblucid als sogenannten Smarthost einzutragen, so dass alle ausgehenden Mails ebenfalls über weblucid laufen. Dies hat mehrere Vorteile: Die Mails werden einer Virenprüfung unterzogen und insgesamt effizienter versendet, da die weblucid Server direkt im Internet stehen und vor allem in Problemfällen besser reagieren können. (→siehe „Bounce-Cache“)

2 Mail-Prüfmechanismen

Jede eingehende Mail durchläuft nacheinander die folgenden Mechanismen, um unerwünschte Inhalte zu erkennen und ggf. abzublocken.

2.1 Spamfilter 1 (SMTP-Blocker)

Wenn der Server eines Mailversenders die Verbindung zu einem der weblucid Mailserver aufbaut, um eine Mail an einen weblucid-Kunden zu übertragen, muss er zunächst einige Parameter übermitteln, bevor die eigentliche Mailübertragung beginnt. So sendet er zunächst unter anderem seinen eigenen Namen und die Absender- und Empfänger-Mailadressen. Diese Werte sowie die IP-Adresse des Versenders und sein protokolltechnisches Verhalten werden von den weblucid Prüfsystemen ausgewertet.

Handelt es sich um einen bekannten Spam-Versender, eine temporär genutzte (dynamische) IP-Adresse oder verstößt der Versender in erheblichem Maße gegen die SMTP-Standards, so wird die Entgegennahme der Mail bereits an dieser Stelle abgelehnt.

2.2 Malware-Filter (Anti-Virus, Anti-Phishing etc.)

Jede Mail wird auf Viren, Trojaner, Spyware, Phishing-Attacken sowie andere schadhafte Inhalte untersucht und bei einer Infektion in Quarantäne gesetzt.

2.3 Executable-Filter (optional)

Wenn der Kunde es wünscht, werden Mails, die ausführbare Programme enthalten, nicht direkt an den Empfänger ausgeliefert sondern zunächst in Quarantäne gesetzt, um dem Kunden eine Überprüfung auf mögliche Gefahren zu ermöglichen.

2.4 Spamfilter 2

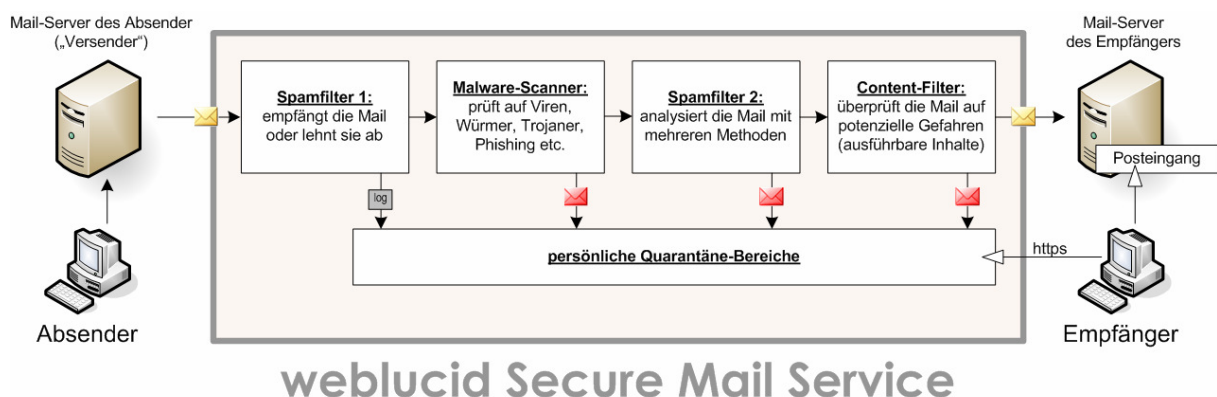
Auf jede Mail werden verschiedene Spamerkennungs-Methoden angewendet, die jeweils als Ergebnis einen Wert ergeben. Je höher dieser Wert, desto höher ist die Wahrscheinlichkeit, dass es sich um Spam handelt. Die Summe der Werte aller Methoden ergibt den sogenannten Spam-Level. Liegt dieser über einem bestimmten Schwellwert, so wird die Mail als Spam klassifiziert und in Quarantäne gesetzt.

3 Auslieferung der Mails

Nur Mails, die von allen Prüfmechanismen als sauber klassifiziert wurden, werden per SMTP an den Mailserver des Kunden ausgeliefert und landen im Posteingang des Empfängers.

4 Quarantäne

Mails, die durch einen der Prüfmechanismen als unerwünscht oder potenziell schädlich bewertet wurden, werden in Quarantäne gesetzt.



Der Empfänger findet in seinem Posteingang nur „saubere“ Mails. Er (und nur er) hat die Möglichkeit, auf sämtliche Mails, auch die in Quarantäne gesetzten Spam-Mails, zuzugreifen. So ist es per Gesetz vorgeschrieben.

Vor schadhafte Inhalten wie z.B. Viren ist er jedoch auch dann geschützt.

4.1 Rechtliche Bewertung

Bei der Behandlung von Mails gilt es, einerseits die Rechte der Empfänger auf Fernmeldegeheimnis, Datenschutz und Erhalt (Nichtunterdrückung) von Mails zu wahren, und andererseits die Rechte des Unternehmers auf Schutz seiner Werte vor Schäden zu unterstützen.

Die weblucid Internet Services unterstützt diese zum Teil recht schwierige Abwägung durch technische Maßnahmen, wo dies möglich ist.

Um den gesetzlichen Bestimmungen der Bundesrepublik Deutschland Rechnung zu tragen, wird hierbei Folgendes sichergestellt:

- **Es findet keine Nachrichtenunterdrückung im Sinne des Telekommunikationsgesetzes statt.**

Der Empfänger hat jederzeit die Möglichkeit, auf jede an ihn gesendete Mail zuzugreifen.

Anmerkungen:

Bei einer Ablehnung des Mailempfangs durch den Spamfilter 1 auf SMTP-Ebene liegt keine Mail vor, die dem Empfänger zur Verfügung gestellt werden könnte. Der Grund der Ablehnung ist entweder ein protokolltechnisches Fehlverhalten des Versenders, oder aber die Tatsache, dass es sich um einen Versender handelt, der ausschließlich und in massenhafter Weise Spams versendet, also durch eine Übertragung von Spams potenziell die Stabilität der vom Kunden genutzten Mailsysteme gefährden kann.

Bei potenziell schadhafte oder betrügerischen Inhalten hat der Kunde das Interesse, Schaden von seinem Unternehmen abzuwenden. Außerdem liegt es in der Fürsorgepflicht des Kunden, Schäden von seinen Mitarbeitern, zum Beispiel durch Passwort-Phishing oder Spyware, fernzuhalten. Daher werde derartige Mails dem Empfänger nicht ohne vorherige Prüfung durch einen sachkundigen Administrator zur Verfügung gestellt.

- **Das Fernmeldegeheimnis bleibt gewahrt. Die Datenschutzrechte des Mailempfängers werden sichergestellt.**

Durch die Art der Quarantänebehandlung wird sichergestellt, dass ohne explizites Einverständnis des Empfängers kein Dritter Kenntnis vom Inhalt der Mails nehmen kann, die durch das weblucid Bewertungssystem als Spam oder potenziell schadhaft eingestuft wurden.

Anmerkungen:

Bei Mails, die als potenziell schadhaft eingestuft wurden, erhält der Administrator des Kunden eine Benachrichtigung, um dem Unternehmer das Erkennen von Bedrohungen zu ermöglichen. Diese Benachrichtigungen beinhalten lediglich die Headerdaten der Mail (Absender, Empfänger, Betreff, protokolltechnische Details), jedoch nicht den Inhalt und auch keine Dateianhänge.

4.2 Ablauf und Funktionen des Quarantänebereichs

Grundsätzlich hat jeder Empfänger (jede Email-Adresse) einen persönlichen Quarantänebereich, in dem sämtliche an diesen adressierten aber nicht direkt zugestellten Mails bis zu 30 Tage aufbewahrt werden. Der Speicherort für die Quarantäne liegt bei weblucid.

Der Empfänger kann über ein Web-Interface auf seinen Quarantänebereich zugreifen. Die Authentifizierung wird über die Email-Adresse durchgeführt: Der Benutzer versendet dazu eine Mail an eine bestimmte Adresse, worauf er umgehend (binnen Sekunden) eine Antwort-Mail mit einem persönlichen Zugriffscode erhält.

Greift ein Benutzer 15 Tage lang nicht auf seinen Quarantänebereich zu, so erhält er automatisch eine Mail, die einen kurzen Statusbericht sowie einen Zugriffscode enthält.

Der Quarantänebereich enthält in einer Listendarstellung die Mails, die in den Quarantänebereich verschoben wurden. Der Empfänger bekommt dabei die folgenden Informationen und Aktionsmöglichkeiten:

- **„Spam1“-Mails (Empfang durch Spamfilter 1 abgelehnt)**

Infos: Datum/Uhrzeit, Absender, Grund der Ablehnung

Hyperlink [freischalten](#) bewirkt die Definition des Versenders als „Nicht-Spam-Versender“. Das bedeutet, dass der Versender der Email zukünftig von den Regeln des Spamfilter 1 auf SMTP-Ebene ausgenommen wird, nicht jedoch von den übrigen Prüfmechanismen.

- **„Spam2“-Mails (Durch Spamfilter 2 in Quarantäne gesetzt):**

Infos: Datum/Uhrzeit, Absender, Betreff

Hyperlink [ansehen](#) bewirkt eine Vorschau der Email (ohne Anhänge)

Hyperlink [zustellen](#) bewirkt die Zustellung der Mail an den Benutzer

Hyperlink [kein Spam](#) bewirkt, dass eine Musteranalyse der Mail vorgenommen, als „Nicht-Spam“ dem Lernsystem zugeführt und bei zukünftigen Entscheidungen einbezogen wird. (Dabei werden keine lesbaren oder anderweitig datenschutzrechtlich relevanten Informationen in das Lernsystem aufgenommen.)

- **Potenziell schadhafte Mails (Viren, Trojaner, Phishing, Executables):**

Infos: Datum/Uhrzeit, Absender, Betreff, Befund (gefundener Virus o.ä.)

Hyperlink [ansehen](#) bewirkt eine Vorschau der Email (ohne Anhänge)

Hyperlink [zum Admin](#) bewirkt eine Zustellung der Mail an die für diesen Fall vorgesehene Quarantäne-Adresse des Unternehmens zwecks Prüfung durch den Administrator.

4.3 Bedeutung der Quarantäne in der Praxis

Auf Grund der extrem niedrigen Rate von fälschlicherweise als Spam bewerteten Mails, sogenannter „false-positives“, spielt der Quarantänebereich in der Praxis eine untergeordnete Rolle. Abgesehen von der Einhaltung der Gesetze genießt das Interesse der Kunden, dass keine einzige Mail „verschwindet“, bei weblucid höchste Priorität. Und auch bei der Diagnose vermeintlicher oder tatsächlicher Probleme bei der Mailzustellung ist es äußerst hilfreich, zunächst die Filtersysteme als Fehlerquelle ausschließen zu können.

Die Erfahrungen der Vergangenheit haben gezeigt, das der Quarantänebereich nach den ersten Tagen von den meisten Mitarbeitern nicht oder nur noch selten genutzt wird. Die Mehrheit genießt einfach den zu über 99% spamfreien Posteingang.

4.4 Verwaltung der Benutzerkonten

Jeder Mitarbeiter des Kunden benötigt einen Account (Benutzername, Kennwort) auf dem webbasierten Quarantänebereich bei weblucid. Dieser wird durch das System vollautomatisch angelegt, wenn an eine Email-Adresse erstmalig Spam abgefangen wird. Der Mitarbeiter erhält dann eine Mail mit einem speziellen Hyperlink, über die er auf seinen persönlichen Quarantänebereich zugreifen und ein Kennwort festlegen kann.

Hat ein Mitarbeiter mehrere Email-Adressen oder Aliase, so kann er diese zu einem Quarantäne-Account zusammenfassen.

Eben so wie die Erkennung vorhandener Benutzer läuft auch die Erkennung nicht vorhandener Email-Adressen vollautomatisch. So werden Quarantäne-Bereiche nicht mehr genutzter Email-Adressen, z.B. nach dem Ausscheiden eines Mitarbeiters, nach einer Toleranzzeit gelöscht.

5 Administrationsoberfläche

Jeder Kunde kann Administratoren mit Lese-/Schreibzugriff definieren, denen über eine verschlüsselte Weboberfläche folgende Funktionen zur Verfügung stehen:

- **Domain-Konfiguration**
Grundeinstellungen zum Mailtransport, Ein-/ausschalten der Spam- und Executable-filter, IP-Adressen, Benachrichtigungsoptionen etc.
- **System-Status**
Hier kann der Administrator in Echtzeit die Funktionen sämtlicher Systeme überprüfen, such die Erreichbarkeit des eigenen Mailservers von außen.
- **Statistiken**
Jeweils pro Tag und pro Monat, als Tabelle und Grafik:
Eingehende Mails, Abgelehnte Mails an nicht vorhandene Benutzer, Spam1, Spam2, Viren, Phishing, Clean, Spam-Quote, Erkennungsquote
- **Inhalt der Bounce-Caches (s.u.)**

■ Logfiles

Jede ein- und ausgehende Mail wird mit folgenden Parametern erfasst:

Versendendes System: IP-Adresse und Name, Absender, Empfänger, Klassifizierung (Clean, Spam1, Spam2, Phishing, Virus, Executable)

Bei abgelehnten / in Quarantäne befindlichen Mails können zusätzlich Details über die Ergebnisse der Bewertungskriterien eingesehen werden.

Bei ausgehenden Mails wird angezeigt, wann die Mail versendet wurde oder wann und warum der letzte Sendeversuch fehlgeschlagen ist. Enthalten ist die positive oder negative Antwort des empfangenden Mailserver, so dass sehr einfach für jede Mail eine sichere und definitive Aussage darüber getroffen werden kann, ob die Mail ordnungsgemäß versendet wurde.

6 Zusatzfunktionen

6.1 Bounce-Cache

Alle Mailserver der weblucid sind mit einem Erkennungsmechanismus für nicht zustellbare Mails ausgestattet. Damit werden Mails, bei denen keine Chance auf Zustellung besteht, so früh wie möglich abgelehnt. Der Absender erhält unverzüglich eine aussagekräftige Fehlermeldung und vollgelaufene Mail-Queues werden vermieden.

Eingehende Mails:

Lehnt der Mailserver des Kunden eine Mail an eine bestimmte Email-Adresse ab, weil es die Adresse gar nicht gibt, so wird diese Adresse von den weblucid Systemen in eine Datenbank aufgenommen und ab sofort gesperrt. Handelt es sich nicht lediglich um einen einmaligen Tippfehler sondern wird die Adresse häufiger angesprochen, so wird sie längere Zeit gespeichert. Auf diese Weise wird der Mailserver des Kunden von der Zustellung von Fehlermeldungs-Mails entlastet.

Ausgehende Mails:

Kommt es bei der Zustellung einer vom Kunden versendeten Mail zu Problemen, wird dies von den weblucid Systemen erkannt und in einer Datenbank gespeichert. Zukünftige Mails an die gleiche Adresse werden bereits beim Empfang mit einer qualifizierten Fehlermeldung abgelehnt und der Absender erhält binnen Sekunden eine Benachrichtigung darüber. Je nach Art der Fehlermeldung wird diese für wenige Minuten bis einige Tage lang gecacht. Dieses Verhalten entlastet nicht nur die Mailserver und erhöht den Komfort für die Mitarbeiter, es vermeidet auch Mail-Schleifen, die häufig zum Überlaufen von Postfächern oder gar Mailserver-Festplatten führen können.

Domains:

Es gibt eine ganze Reihe von Domains, die zwar zum Mailversand (z.B. Bestellbestätigungen bei Online-Shops) genutzt werden, jedoch niemals selbst Mails entgegennehmen. Eine automatisch generierte „Ich bin im Urlaub bis ...“-Mail würde im Normalfall bis zu 5 Tage lang in der Auslieferungs-Queue des Servers warten und anschließend zurückgesendet werden. Die Systeme der weblucid erkennen dieses Verhalten, überprüfen die Erreichbarkeit der betroffenen Domain und lehnen in Zukunft Mails an derartige Domains sofort ab.

6.2 Versand übergroßer Mails

Der Versand von Mails mit sehr großen Anhängen bereitet den Benutzern in der Praxis häufig Probleme, da alle Mailserver, über die die Mail läuft, eine Größenbeschränkung pro Mail haben. Die Werte liegen meistens im Bereich zwischen 10 und 100 Megabytes.

Weblucid bietet daher seinen Kunden die Möglichkeit, Mails mit einer Größe von bis zu 700 Mbyte – eine ganze CD-ROM voll – zu versenden und zu empfangen. Die Größenbeschränkungen der beteiligten Mailserver, vom Server des Kunden bis hin zu dem des Empfängers, werden dabei umgangen: Die Email enthält anstatt dem Anhang selbst einen Hyperlink, über den der Empfänger via HTTPS verschlüsselt auf die Datei zugreifen kann.

Selbst wenn der Mailserver des Empfängers überhaupt keine Anhänge in Emails gestattet, kann damit eine 700 MB große Datei übertragen werden. Die bei gewöhnlichen Emails geltenden Sicherheitsmaßnahmen bleiben dabei selbstverständlich erhalten.

Hinweis: Dieses Feature wird voraussichtlich ab ca. Nov./Dez. 2006 allen Secure Mail Service Kunden ohne Mehrkosten zur Verfügung stehen.