heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Die Bedrohung kommt von innen:

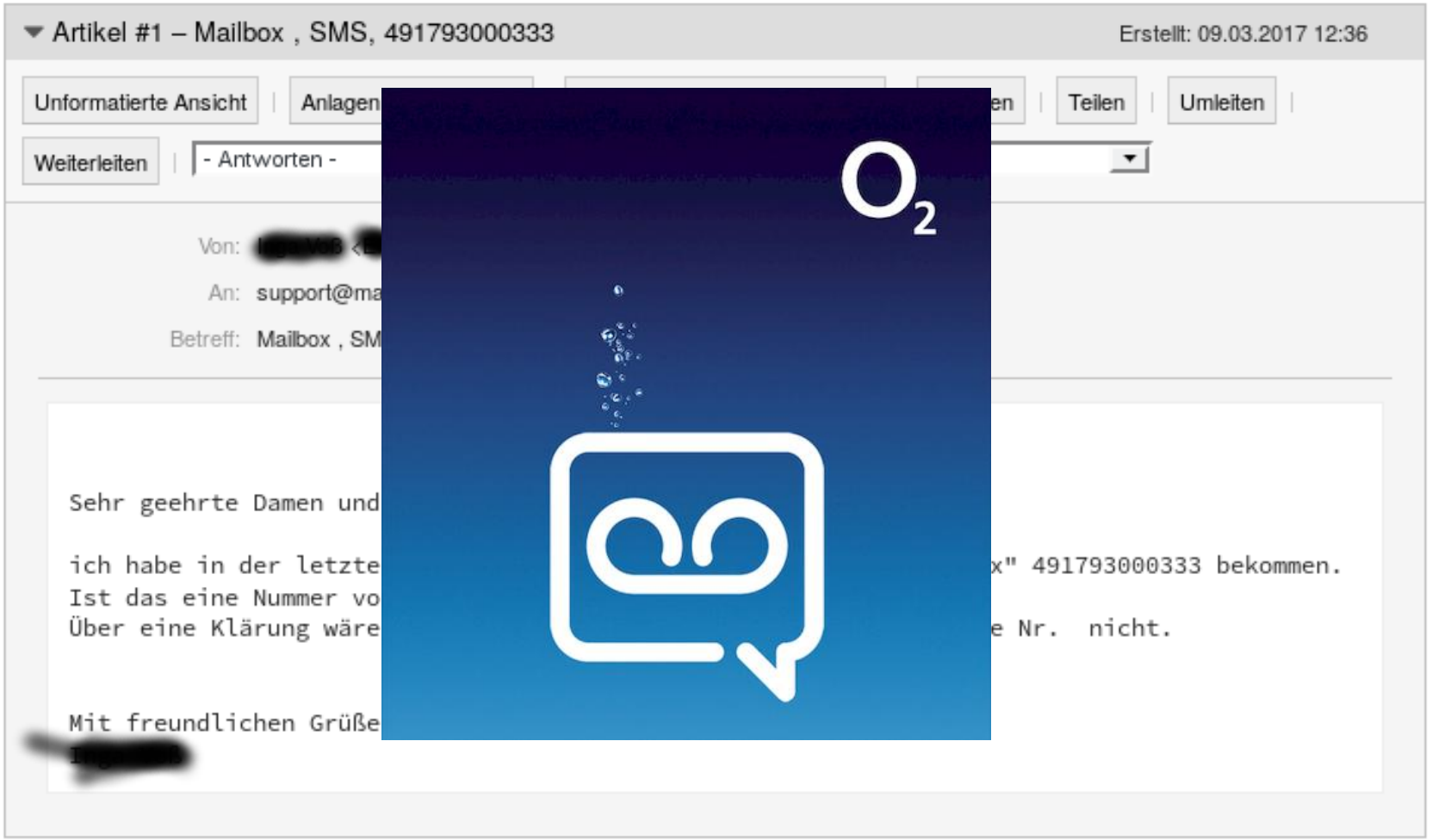
Outbound Spam Prevention

Peer Heinlein <p.heinlein@heinlein-support.de>

Geht's um E-Mail-Security...

- Heinlein Support GmbH / Peer Heinlein
  - Linux Security Consultant seit 1995
  - Spezialist für Mailserver und Anti-Spam/Anti-Virus seit 1992
  - Diplom-Jurist
  - Kunden:
    - ISPs > 100.000 Kunden und > 1.000.000 Kunden
    - Universitäten, Forschungseinrichtungen
    - diverse Landesrechenzentren (ITDZ, Stuttgart, Baden-Franken, Thüringen)
    - Massenversender
    - Eigene E-Mail ISPs: mailbox.org (Stiftung Warentest Testsieger)
  - Heinlein Support GmbH: 35 Mitarbeiter mit Sitz in Berlin

Wer oder was ist mailbox.org?



Peer Heinlein <p.heinlein@heinlein-support.de>

Mailbox.org

- Besonders auf Sicherheit und Privatsphäre bedachter E-Mail-Provider
  - Vollständig anonyme Nutzung
  - Prepaid-Modell
  - Bezahlung u.a. per Bargeld, Paypal, Bitcoin & Co
  - Kein Usertracking
- Zweimaliger Testsieger der Stiftung Warentest

- Einfache Testaccounts mit eingeschränkter Nutzung
- Frei, offen, anonym für jedermann

Peer Heinlein <p.heinlein@heinlein-support.de>

Die Situation

Peer Heinlein <p.heinlein@heinlein-support.de>

Das Problem der Mailprovider

- Spammer öffnen bei Freemail-Providern automatisiert massenhaft Accounts
  - Google-Captchas werden dabei immer wieder systematisch überwunden
  - Spammer eröffnen tagelang alle 15 Sekunden einen neuen Account

- Auch Bezahlaccounts sind kein Problem:
  - Bezahlung durch geklaute Bankdaten
  - Bezahlung durch geklaute Paypal-Daten
  - Bezahlung durch eigenes Paypal
    - Paypal-Accounts der Spammer durch Kreditkarten gedeckt
    - Spammer stornieren 4-6 Wochen später bei ihrem Kreditkartenanbieter
    - Kreditkartenanbieter entzieht Paypal das Geld
    - Paypal leitet Rückabwicklung ein, verlangt 10,- EUR Strafgebühren

Peer Heinlein <p.heinlein@heinlein-support.de>

Spam 2016: Back to the roots

- Weniger Versand direkt durch Botnetze
  - Das läßt sich recht einfach und effizient filtern!
- Wieder zunehmend gehackte + gephishte Accounts
  - Ganz gezielte Kampagnen gegen Provider und Universitäten
  - Normale Accounts mutieren zu Spam-Accounts
  - Normale Mailserver mutieren zu Spamschleudern
- Gehackte Accounts werden ausgenutzt:
  - Durch Botnetze
  - Durch Client-Zugriffe (Einzel-IPs)
  - Ferngesteuerte Webmailer-Zugriffe auf Roundcube & Co.

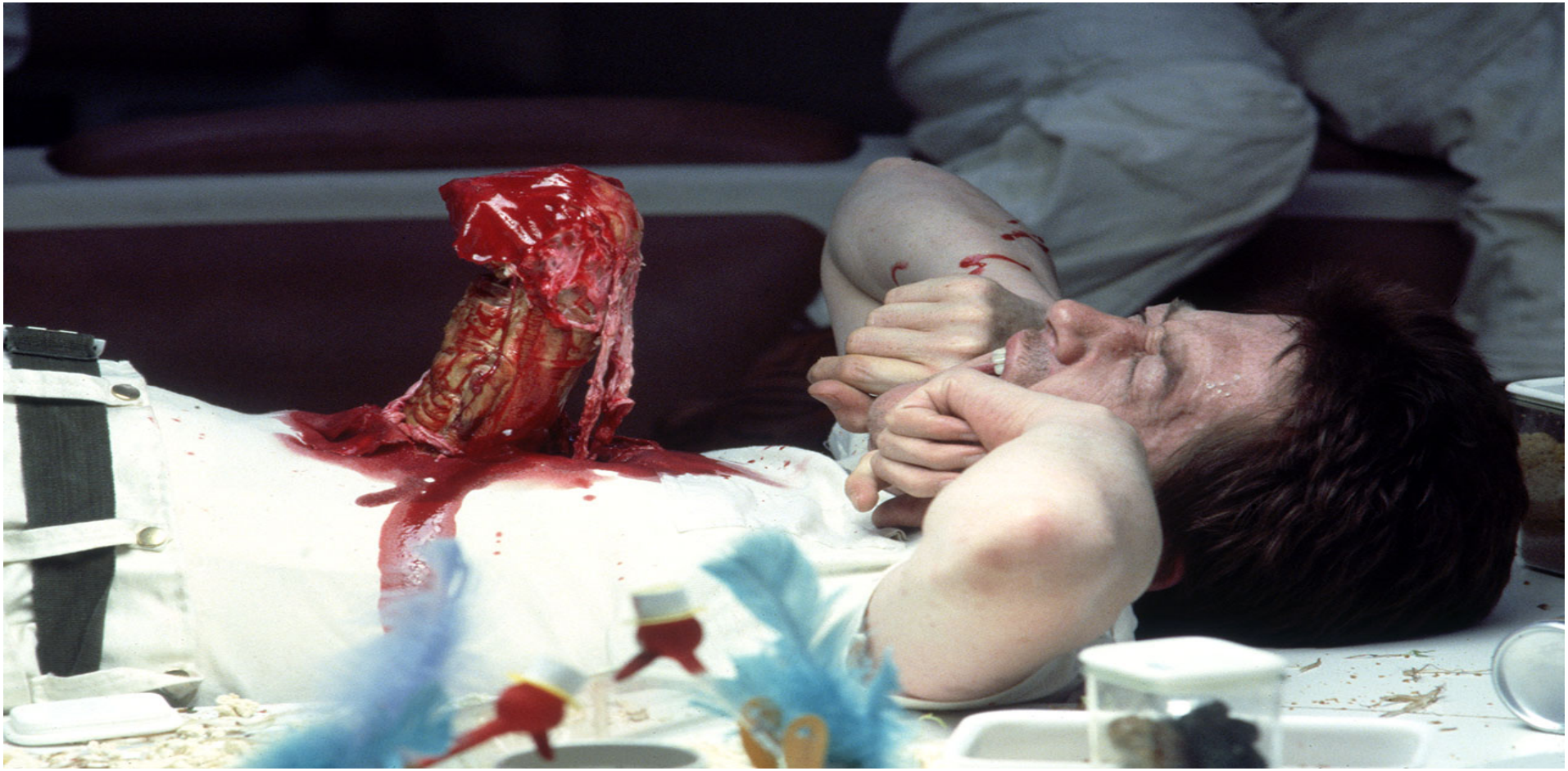
Peer Heinlein <p.heinlein@heinlein-support.de>

Outbound-Spam ist unternehmenskritisch!

- Outbound-Spam-Mails belasten die Ressourcen
  - Sorgen für Alarme (gerne Nachts + am Wochenende)
- Bringen Mailgateways auf RBL-Sperrlisten
  - User sind sauer, verursachen $upport-Aufwand, kündigen
  - Arbeitsbeschaffungsmaßnahme, echter finanzieller Impact
- Bringen echte Mails woanders in die Spam-Quarantäne
- Ist so oder so auch einfach verantwortungslos anderen gegenüber.
- Ist ein echtes Problem für die betroffenen Postmaster.

Peer Heinlein <p.heinlein@heinlein-support.de>

Kurzum: Die Bedrohung kommt von innen!



heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Schutz gegen Phishing und Spam-Accounts

Peer Heinlein <p.heinlein@heinlein-support.de>

Gegen Phishing-Attacken wehren

- Guter eingehender Spamschutz (sowieso)
- Eigene Spamtraps installieren und auf Phishing-Mails auswerten
- Bei Incidents: Phishing-Mails schnell aus INBOXen löschen
  - Wettlauf gegen die Zeit!
  - doveadm expunge -A mailbox INBOX subject „MAILBOX WARNING: Account update“
  - URL + Absender-Mailadressen outbound in der Fireall sperren?

- Support-Mails per PGP signieren?

Gegen Phishing-Attacken wehren

- Echte Support-Adresse von außen sperren?
- Eigene Spamfilter-Pattern aus erkannten Phishing-Attacken
  - „Your XXXX team“
- RegExp-Filter auf eigene Phishing-Absender
  - support.*@meinedomain.example
  - support.*\ .*@meinedomain.example

Peer Heinlein <p.heinlein@heinlein-support.de>

Wenn‘s zu spät ist

- Irgendwer fällt immer darauf hinein. Immer.
- Was tun bei anonymen Prepaid-Accounts...
  - ...die aus Paranoia keine Passwort-Reset-Methode hinterlegt haben?
  - Wird das Passwort von uns zurückgesetzt ist der User ausgesperrt

- Außerdem: Crypto-Inboxen mit Userpasswort wären dann zerstört
  - Hey: It‘s not a bug, it‘s a feature!

- Besser: SMTP-Versand deaktivieren
  - LDAP: (|(mail=%s)(status=active)(smtpAuthEnable=yes))
  - Info-Mail an Nutzer, Passwort-Rücksetzung setzt SMTP-Sperre zurück
  - Contra: Account ist kompromittiert, Inhalte können abgezogen werden

Peer Heinlein <p.heinlein@heinlein-support.de>

Automatisierte Accountregistrierungen verhindern

- Captchas, ggf. mehrere, auch doofe, zufällig rotierend?
- Anzahl der Account-Creates pro IP pro Zeitraum tracken
- Zeittracking-Analysen im Registrierungsformular
  - Kann das ein Mensch in unter 15 Sekunden das ausfüllen?
- Geo-IP-Sperren (nicht immer eindeutig)
- Monitoring der Account-Create-Zahlen
- Weitere kreative Betriebsgeheimnisse. (Sorry, ggf. nur mündlich)

- Verspätetes Löschen? Nicht in die Karten schauen lassen.

- Hilft alles nur teilweise. Spammer werden es immer schaffen.

Peer Heinlein <p.heinlein@heinlein-support.de>

Outbound under Control

Peer Heinlein <p.heinlein@heinlein-support.de>

Ausgehende Mails nach Spam/Viren filtern

- Natürlich müssen ausgehende Mails nach Spam-/Viren gefiltert werden
  - Machen viele nicht
  - Amavis/SpamAssassin/ClamAV sind schonmal was
- Outbound mit niedrigem Kill-Level arbeiten (3? 4?)
  - SMTP-Auth-Mails können kaum technische Fehlermerkmale aufweisen!
- „banned content“ auch auch ausgehend filtern
  - Exe, JavaScript & Co
- Unattraktiv sein: „.*paypal.*\ .*@example.com“ blocken!

Peer Heinlein <p.heinlein@heinlein-support.de>

Amavis als FBL im eigenen Haus

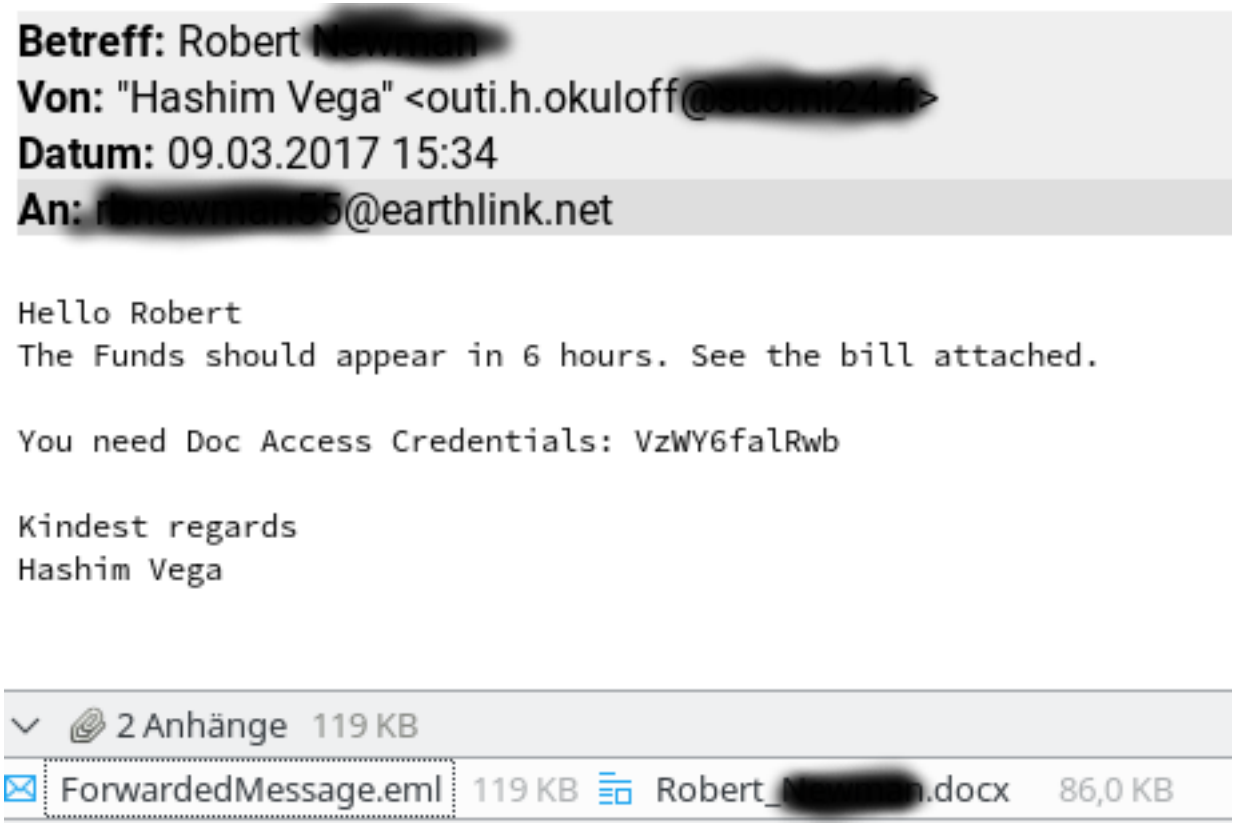
- Amavis kann bei Spam-/Virenbefund mit Alert-Mails reagieren
- Von außen sinnlos, von innen genial
  - Voraussetzung: Outbound über eigenen Amavis-Port leiten!

```
# it is up to MTA to re-route mail from authenticated roaming users or
# from internal hosts to a dedicated TCP port (such as 10026) for filtering
$interface_policy{'10026'} = 'ORIGINATING';

$policy_bank{'ORIGINATING'} = {  # mail supposedly originating from our users
 originating => 1,  # declare that mail was submitted by our smtp client
 virus_admin_maps => ["virusalert\@$mydomain"],
 spam_admin_maps  => ["virusalert\@$mydomain"],
};
```

Ausgehend filtern – logisch, aber wie?

→ Kleine E-Mails mit wenig markantem Inhalt



heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

Feedback-Loops: Der Blick ins Netz

Peer Heinlein <p.heinlein@heinlein-support.de>

Feedback Loops

- Viele Provider bieten Feedback-Loops an
  - Reporten User oder deren Systeme Spam, gibt's einen Alert an den aussendenden ISP
  - Rückkanal in Echtzeit – welchen Schrott versenden meine Systeme?
  - WER versendet von mir diesen Schrott? Absenderkennung prüfen!

- Report erfolgt im ARF, im Abuse Reporting Format
  - Einfach, ASCII, parsbar, RFC 5965
  - (Aber auf Mail beschränkt, xARF geht weiter, hier nicht relevant)
  - Google, Microsoft/Hotmail & Co haben eigene Formate

This is an automated report for an email message received by fbl@abuse.earthlink.net

---

Feedback-Type: abuse
Version: 1
Source-IP: 91.223.[redacted]
Feedback-Agent: SpoonFeed/0.1
Received-Date: Thu, 9 Mar 2017 09:35:59 -0500

—ForwardedMessage.eml

Betreff: Robert [redacted]
Von: "Hashim Vega" <outi.h.okuloff[redacted]>
Datum: 09.03.2017 15:34
An: [redacted]@earthlink.net

Hello Robert
The Funds should appear in 6 hours. See the bill attached.

You need Doc Access Credentials: VzWY6falRwb

Kindest regards
Hashim Vega

2 Anhänge 119 KB

ForwardedMessage.eml 119 KB Robert_[redacted].docx 86,0 KB

Peer Heinlein <p.heinlein@heinlein-support.de>

Feedbackloops: Eintragen, eintragen, eintragen!

- Liste wichtiger FBLs auf:
  - https://www.m3aawg.org/fbl-resources
  - https://www.abusix.com/blog/data-sources
- Deutsche IPs bieten keine FBLs
  - T-Online, GMX, web.de, Vodafone, Freenet – Fehlanzeige.

- Überall einzeln registrieren mit
  - IP-Networks oder ASN
  - Teilweise Absender-Domain

- Wichtig:
  - Abuse-Contact in den Domain-whois-Daten vorher korrekt setzen!

Peer Heinlein <p.heinlein@heinlein-support.de>

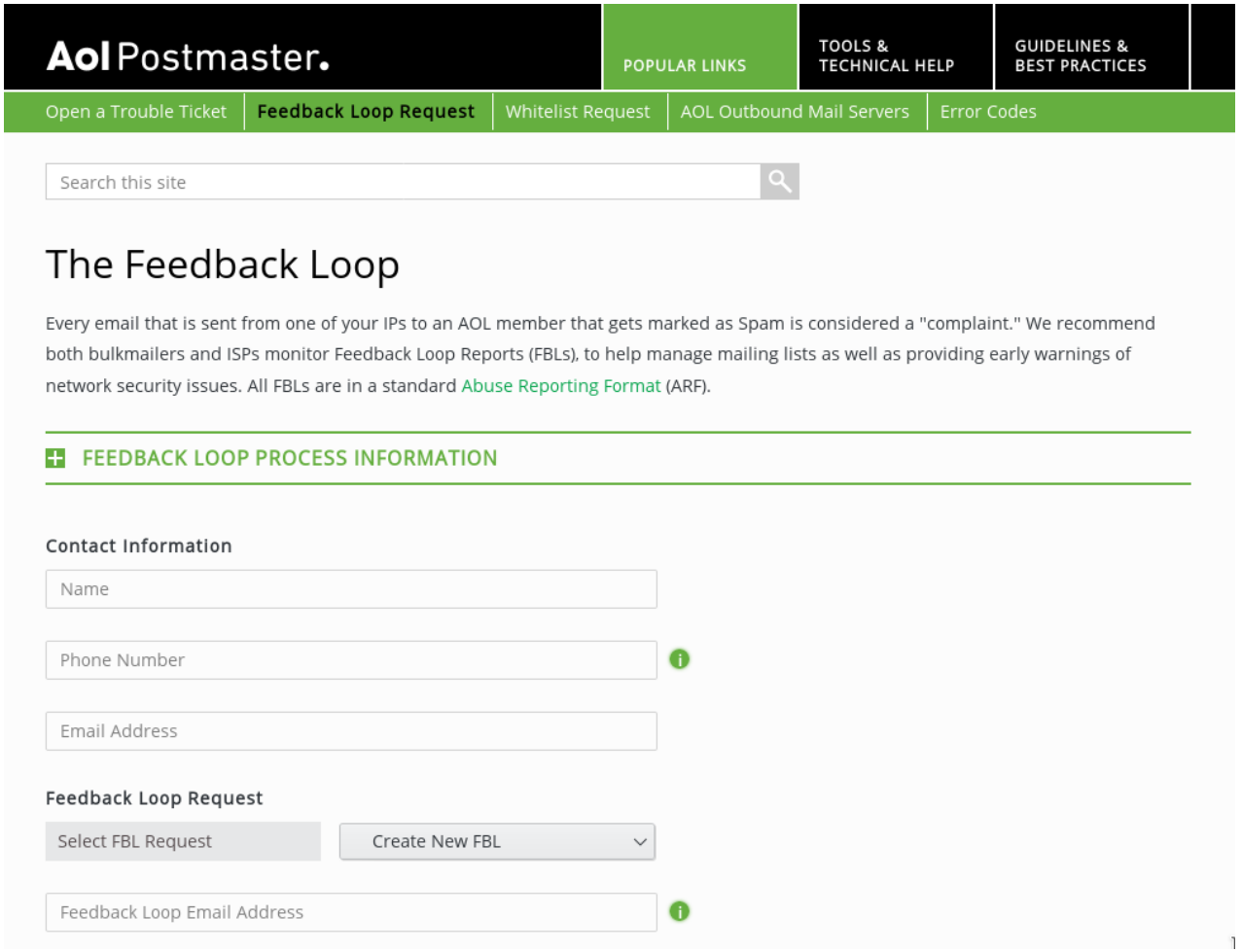
Monitoring der Outbound-Relays

- https://postmaster.aol.com/
- https://help.yahoo.com/kb/postmaster
- https://postmaster.live.com/snds/
- https://postmaster.yandex.ru/
- https://postmaster.mail.ru/

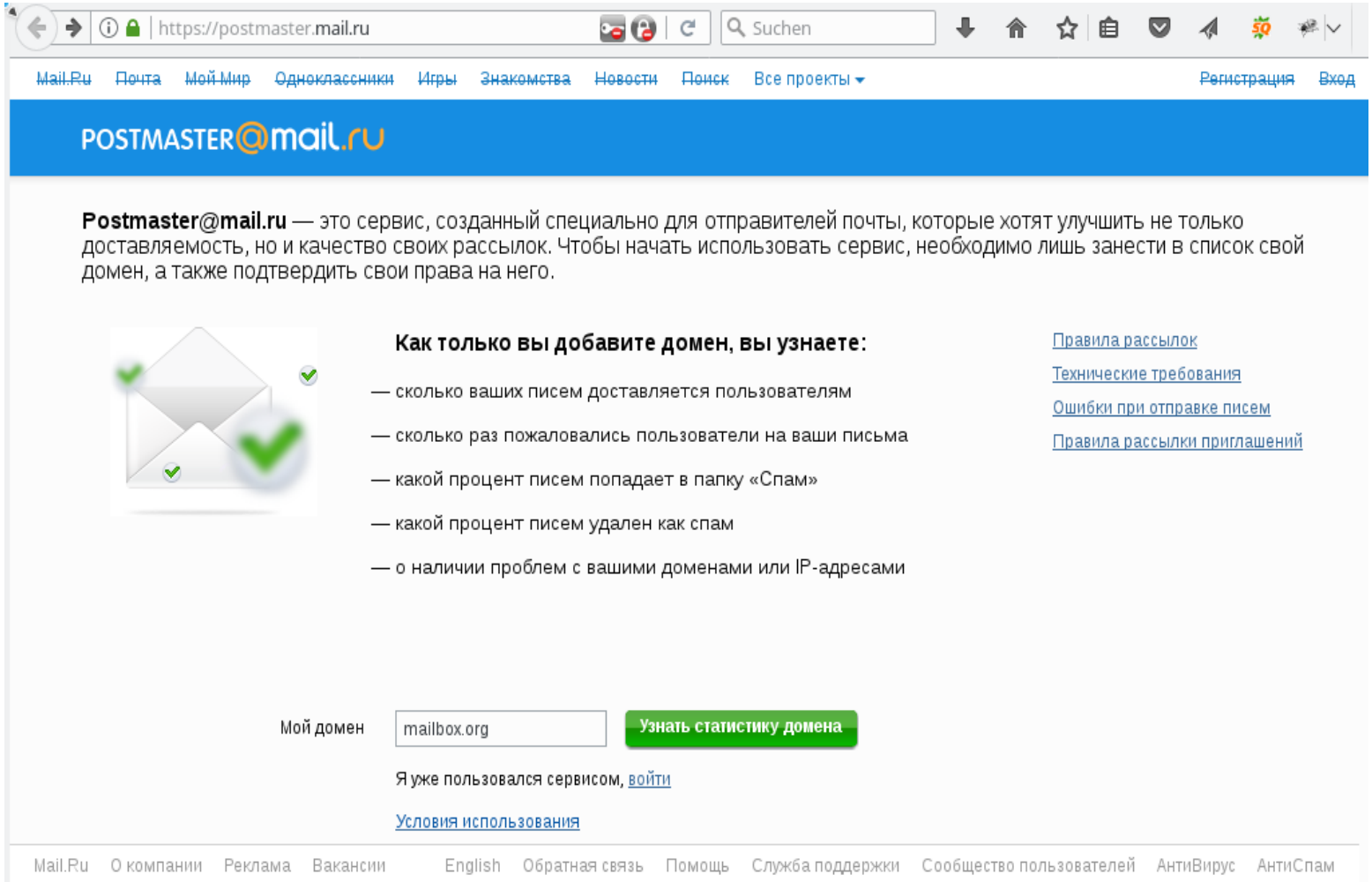
- http://www.senderbase.org

- Kommerzielle Anbieter:
  - https://250ok.com/
  - Abusix mit 240.000 Spamtraps, gut für Server-Hoster

Postmaster AOL



Mail.ru


https://postmaster.mail.ru
Suchen
Mail.Ru Почта Мой Мир Одноклассники Игры Знакомства Новости Поиск Все проекты
Регистрация Вход
POSTMASTER@mail.ru
Postmaster@mail.ru — это сервис, созданный специально для отправителей почты, которые хотят улучшить не только доставляемость, но и качество своих рассылок. Чтобы начать использовать сервис, необходимо лишь занести в список свой домен, а также подтвердить свои права на него.
Как только вы добавите домен, вы узнаете:
— сколько ваших писем доставляется пользователям
— сколько раз пожаловались пользователи на ваши письма
— какой процент писем попадает в папку «Спам»
— какой процент писем удален как спам
— о наличии проблем с вашими доменами или IP-адресами
Правила рассылок
Технические требования
Ошибки при отправке писем
Правила рассылки приглашений
Мой домен
mailbox.org
Узнать статистику домена
Я уже пользовался сервисом, войти
Условия использования
Mail.Ru О компании Реклама Вакансии English Обратная связь Помощь Служба поддержки Сообщество пользователей АнтиВирус АнтиСпам

Microsoft Smart Network Data Service

- https://postmaster.live.com/snds/data.aspx
- Hotmail nimmt auch Mails per „250 OK“ an, stellt sie aber nicht zu
- Office365-Plattform hat das wohl nicht mehr

IP Address [?]	Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FROM [?]
Total: 7 IPs		**18,541**	**12,079**	**17,825**	**2 Red IPs**	**< 0.1%**		**2**	**6 distinct values**	**6 distinct values**
213.203	3/9/2017 9:00 AM - 3/10/2017 8:00 AM	7676	2072	7459		< 0.1%		0		
80.241	3/9/2017 9:00 AM - 3/10/2017 7:00 AM	2677	2517	2604		< 0.1%		0		
80.24	3/9/2017 9:00 AM - 3/10/2017 8:00 AM	2447	2200	2317		< 0.1%	3/9/2017 7:27 PM - 3/9/2017 7:35 PM	2		
91.223	3/9/2017 9:00 AM - 3/10/2017 8:00 AM	1955	1862	1923		< 0.1%		0		
91.223	3/9/2017 9:00 AM - 3/10/2017 8:00 AM	1843	1750	1768		< 0.1%		0		
91.223	3/9/2017 9:00 AM - 3/10/2017 8:00 AM	1462	1267	1298		< 0.1%		0		
80.241	3/9/2017 9:00 AM - 3/10/2017 8:00 AM	481	411	456		< 0.1%		0		
Total: 7 IPs		**18,541**	**12,079**	**17,825**	**2 Red IPs**	**< 0.1%**		**2**	**6 distinct values**	**6 distinct values**

Peer Heinlein <p.heinlein@heinlein-support.de>

FBL:
Hast Du keine, bau dir eine!

- Mailheader „List-Unsubscribe“ für Mailinglisten gedacht
- Läßt sich als Header auch in andere ausgehende Mails einsetzen
- Enthält URL mit codierten Informationen zur Mail
- Austragungswunsch des Empfängers löst FBL-Complaint aus
- RFC8058 (Tobias Herkula)

heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>

spamblockd:
Spammer erkennen und stoppen

Peer Heinlein <p.heinlein@heinlein-support.de>

Missbrauch verhindern

- Egal ob gehackter oder registrierter Spam-Account: Er soll nicht 10.000 Mails versenden können.
  - Normale Nutzer schon!
  - Business-User erst recht!
  - Harte Limits helfen viel, aber nicht endgültig.

  - Ein Spammer mit 10.000 Mails am Tag richtet viel Schaden an.
  - Ein Spammer mit 1.000 Mails am Tag richtet Schaden an.
  - Ein Spammer mit 100 Mails am Tag richtet kaum Schaden an.

  - Ein Spammer mit 10.000 Accounts mit 100 Mails am Tag… naja.
    - Accountregistrierungen verhindern!

Peer Heinlein <p.heinlein@heinlein-support.de>

Statt harter Limits: Anomalie-Detection

- Wann findet Missbrauch statt?
  - Account ist neu und sendet viel
  - Account ist neu und sendet SEHR viel
  - Wird von zwei wechselnden IPs (gleichzeitig!) genutzt
  - Wird von VIELEN wechselnden IPs (gleichzeitig!) genutzt
  - Wird von verschiedenen Ländern/Kontinenten gleichzeitig genutzt
  - Sendet (deutlich?) mehr als der 30-Tages-Durchschnitt
  - Es gibt Complains aus Feedback-Loops gegen diesen Account (später mehr)
  - Sendet Mails an mehrere Empfänger gleichzeitig
  - Sendet Mails an viele yahoo-Adressen
  - Sendet Mails an Dictionary-Empfängerlisten
  - Und viele, viele weitere Betriebsgeheimnisse. Sorry.
  - Am Ende: > 25 sich selbst verstärkende Messwerte

Peer Heinlein <p.heinlein@heinlein-support.de>

Neue Ideen

- Levenshtein-Distanz bei Multi-Recipient-Mails
  - Viele Spammer arbeiten systematisch Namenslisten ab
  - Die Levenshtein-Distanz berechnet den Änderungsgrad von Adresse zu Adresse
- Client-Fingerprinting gerade bei Webmail-Access
  - SSL-Ciphers
  - OS des Clients
  - Verwendet

Peer Heinlein <p.heinlein@heinlein-support.de>

Spamblockd ist wirklich effektiv

- Ein normaler Nutzer kann 5.000 – 10.000 Mails versenden
- Botnetz-Spammer stoppen wir nach ~70 Mails
- Normale Spammer stoppen wir nach ~250-500 Mails
- Wie hoch das Limit ist, ist eigentlich gar nicht so wichtig!

- http://www.spamblockd.org (upcoming)
  - Normales Rate-Limiting: for free
  - Userindividuelle Rates aus LDAP + Anomalie-Detection: Lizenz

heinlein

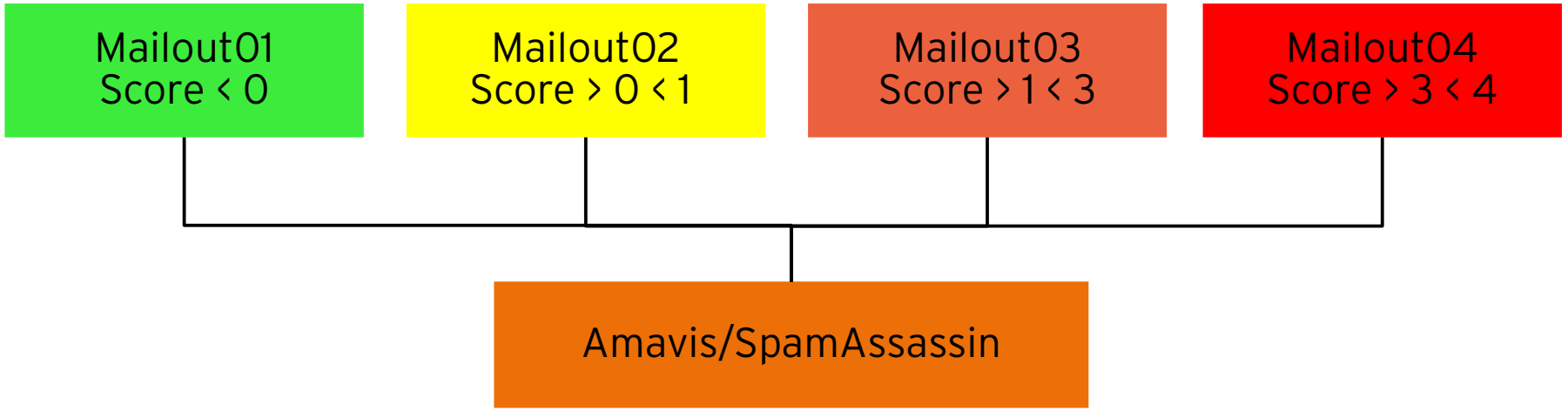
Peer Heinlein <p.heinlein@heinlein-support.de>

Mit dem unvermeidlichen arbeiten: Spam managen

Peer Heinlein <p.heinlein@heinlein-support.de>

Mit dem Unvermeidlichem Umgehen

- Zu einem gewissen Teil muß man auch Spam „verwalten“
- 2/3/4 verschiedene Outbound-Relays je nach Qualität der Mail
  - Usermails | Servermails | Massen-Mails | Scorings
- Amavis/SpamAssasssin leitet Mails je nach Score an verschiedene Relays weiter



Peer Heinlein <p.heinlein@heinlein-support.de>

Howto: Score-basiertes Routing in Amavis

```
$forward_method =      'smtp:[mailout00.example.com]:10025';  # set to undef with milter!
$forward_tag_method =  'smtp:[mailout01.example.com]:10025';  # set to undef with milter!
$forward_tag2_method = 'smtp:[mailout02.example.com]:10025';  # set to undef with milter!
$forward_tag3_method = 'smtp:[mailout03.example.com]:10025';  # set to undef with milter!

@forward_method_maps =      ( sub { Opaque(c('forward_method')) } );
@forward_tag_method_maps =  ( sub { Opaque(c('forward_tag_method')) } );
@forward_tag2_method_maps = ( sub { Opaque(c('forward_tag2_method')) } );
@forward_tag3_method_maps = ( sub { Opaque(c('forward_tag3_method')) } );

%forward_method_maps_by_ccat = (
  CC_CLEAN.',1',    sub { ca('forward_tag_method_maps') },
  CC_SPAMMY,        sub { ca('forward_tag2_method_maps') },
  CC_SPAMMY.',1',   sub { ca('forward_tag3_method_maps') },
  CC_CATCHALL,      sub { ca('forward_method_maps') },
);
```

→ Variablen müssen im Amavis-Sourcecode als dynamisch angemeldet werden!

Peer Heinlein <p.heinlein@heinlein-support.de>

Kunden-Webserver mit LAMP-Stack

Peer Heinlein <p.heinlein@heinlein-support.de>

Gehackte Kundenpräsenzen tracken

- Wordpress & Co: Gehackte Webserver sind an der Tagesordnung
- Doch woher kommt der Spam? Wer verschickt was?
- PHP protokolliert
  - Das erzeugende Script im Mail-Header
  - Die Mail in einem separaten Logfile

```
; Add X-PHP-Originating-Script: that will include uid of the script followed by the filename
mail.add_x_header = On
;mail.log = /var/log/apache2/phpmail.log
mail.log = syslog
```

```
Mar  9 22:06:55 host apache2: [09-Mar-2017 21:06:55 UTC] mail() on
[/srv/www/htdocs/.../../wp-includes/class-phpmailer.php:698]: To: user@example.net --
Headers: Date: Thu, 9 Mar 2017 21:06:55 +0000 From: WordPress <wordpress@example.com>
Message-ID: <80a16d2118c40a330c5e668a1e01bf32@www.example.com> X-Mailer: PHPMailer 5.2.22
(https://github.com/PHPMailer/PHPMailer) MIME-Version: 1.0 Content-Type: text/plain;
charset=UTF-8
```

Peer Heinlein <p.heinlein@heinlein-support.de>

Die Feedback-Loop direkt zurück zum Kunden

- Kleine Hilfe am Rande:

  Wenn schon Mails, dann mit dem richtigen Envelope-From!

```
<VirtualHost xx.xx.xx.xx>
    Servername www.example.com
    php_admin_value sendmail_path "sendmail -t -i -f kunde@example.com
</VirtualHost>
```

Peer Heinlein <p.heinlein@heinlein-support.de>

Du bist nicht alleine
Hilfe, Ideen, Anregungen

Peer Heinlein <p.heinlein@heinlein-support.de>

Austausch mit Gleichgesinnten

- Postmaster-Mailingliste
  - https://listen.jpberlin.de/mailman/listinfo/postfixbuch-users
  - https://chilli.nosignal.org/cgi-bin/mailman/listinfo/mailop
- Arbeitskreis E-Mail vom ECO
  - http://wiki.ak-email.eco.de/
- Certified Senders Alliance CSA
  - 10.-12.5.2017: CSA Summit in Köln
- M3AAWG
  - https://www.m3aawg.org/

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.

Peer Heinlein

Mail: p.heinlein@heinlein-support.de

Telefon: 030/40 50 51 – 42

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

Post-Snowden Mail-Security 2016
[SLAC 2016]
Peer Heinlein <p.heinlein@heinlein-support.de>

Ja, diese Folien stehen auch als PDF im Netz...
http://www.heinlein-support.de/vortrag

Peer Heinlein <p.heinlein@heinlein-support.de>

Soweit, so gut.

Gleich sind Sie am Zug:
Fragen und Diskussionen!

Peer Heinlein <p.heinlein@heinlein-support.de>

Wir suchen:
Admins, Consultants, Trainer!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

Peer Heinlein <p.heinlein@heinlein-support.de>

Und nun...

- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

Bis bald.

Peer Heinlein <p.heinlein@heinlein-support.de>

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln in Training und Schulung die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS

Hard- und Software-Appliances für Archivierung, IMAP und Anti-Spam und speziell für den Serverbetrieb konzipierte Software rund ums Thema E-Mail.