SPF, DKIM, DMARC usw

Neue Herausforderungen bei E-Mail und Spam

Kurt Jaeger, pi@opsec.eu

https://cccs.de

Stuttgart, 9. Juli 2015

Übersicht

- Vorwissen notwendig: Mail, IP, DNS, SMTP
- Mailheader
- Verarbeitung
- Verfahren
- Probleme
- Lösungsskizze

Vorwissen

- Mail: Austausch von langen Textnachrichten, Absender/Empfangsadressen
  Beispiel: test@dom.ain
- IP: Internet Protokoll
  Austausch von Datenpaketen, Quell/Zieladressen
  Beispiel: 212.71.205.21
- DNS: Domain Name System
  Verteilter, hierarchischer Key/Type/Value Speicher
  Beispiel: Key = opsec.eu, Type = MX, Value = 10 home.opsec.eu.
- SMTP: Simple Mail Transfer Protokoll
  Übertragung von Mails zwischen zwei Rechnern
  It's not simple anymore

Was ist Spam ?

- unerwünschte Mails
- Werbung: Attention Economy
- Ausforschen persönlicher Daten
- Vorspielung einer persönlichen Mail
- Click-Baits
- Phishing (Angriff auf den Rechner)
- Spionage
- Warum ? Geld verdienen, whatever works

Wie dagegen vorgehen ?

- Spam filtern
- Spambekämpfung: Gegen den Verursacher vorgehen
  Nicht Teil dieses Vortrags!
- E-Mail-Adressen stringent verwalten
  - Für jeden Lieferant/jeden Vertrag/jede Kennung eine Mailadresse
    Beispiel: juniper@einkauf.nepustil.net
  - Falls zuviel Spam kommt: Adresse kann deaktiviert werden

Wer verteidigt sich ?

- Mailserver
- Mailclients (teilweise), nicht Thema

Wie funktioniert Mail ?

- Mailclient (Mail User Agent, MUA), nicht Teil des Vortrags
- Mailserver
  - Mailübertragung (Mail Transfer Agent, MTA)
    - Versand
    - Empfang
- Wer einen Mailserver betreiben möchte, bekommt hier Hinweise
- Envelop-From – Absender laut Umschlag

```
From absender@opsec.eu Wed Jul 08 21:25:17 2015
Return-path: <absender@opsec.eu>
Envelope-to: empfaenger@opsec.eu
Delivery-date: Wed, 08 Jul 2015 21:25:17 +0200
Received: from home.opsec.eu ([193.105.105.1] ident=spamd)
        by home.opsec.eu with spam-scanned (Exim 4.85 (FreeBSD))
        (envelope-from <absender@opsec.eu>)
        id 1ZCuy5-0006jy-M9
        for empfaenger@opsec.eu; Wed, 08 Jul 2015 21:25:17 +0200
X-Spam-Checker-Version: SpamAssassin 3.4.1 (2015-04-28) on home.opsec.eu
X-Spam-Level:
X-Spam-Status: No, score=-0.0 required=5.0 tests=NO_RELAYS autolearn=ham
        autolearn_force=no version=3.4.1
Received: from pi by home.opsec.eu with local (Exim 4.85 (FreeBSD))
        (envelope-from <absender@opsec.eu>)
        id 1ZCuy5-0006js-K9
        for empfaenger@opsec.eu; Wed, 08 Jul 2015 21:25:17 +0200
Date: Wed, 8 Jul 2015 21:25:17 +0200
From: Kurt Jaeger <absender@opsec.eu>
To: empfaenger@opsec.eu
Subject: Einfache Mail
Message-ID: <20150708192517.GA25903@home.opsec.eu>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
Content-Length: 90
Lines: 4

Und ?

--
pi@opsec.eu           +49 171 3101372                        5 years to go !
```

Einfache Checks

- einfache DNS/Domain Checks
- Blacklist-Lookup
- Greylisting
- SpamAssassin (u.a. Content-Rating)
- Sender-Verify (-Callouts)
  https://en.wikipedia.org/wiki/Callback_verification
- SMTP-Auth (User/Passwort)

Komplexe Verteidungsverfahren

- SPF
- SRS
- DKIM
- DMARC
- DANE
- Ratelimiting

SPF: Sender Policy Framework

- RFCs 7208 und 7372
- Realisierung: DNS Eintrag
- Beispiel:
  "v=spf1 mx ip4:212.71.205.21 ip6:2001:14f8:1:1::15 -all"
- Sagt grob: Nimm Mail von dieser Absender-Domain von MXen und diesen IPs an, alle anderen Server dürfen nicht
- exim Prüfung bei eingehender Mail per ACL
- Details siehe
  https://github.com/Exim/exim/wiki/SPF

SPF: Probleme

- Mailverteiler und Weiterleitungen tun nicht mehr
- Subdomains müssen beachtet werden
- Webserver und Webformulare
- Spammer fügen SPF-Records für ihre Domains hinzu

SRS: Sender Rewriting Scheme

- SPF Problem:
  user1@dom1 sendet an 2@dom2, dort Weiterleitung an 3@dom3
- Reject, weil dom2 keine Mails von @dom1 versenden darf
- Lösung: Absender umschreiben auf
  SRS0=HHH=TT=dom1=user1@dom2
- Hash, Zeitstempel in Datenbank merken
- Antwort Mails nur weiterleiten, wenn Vorgang bekannt
- Problem: alle weiterleitenden Mailserver müssen SRS implementieren
- Details siehe
  https://github.com/Exim/exim/wiki/SRS

DKIM: DomainKeys Identified Mail

- RFC 6376
- Public-Key-Cryptographie
- Absender-Domain veröffentlicht Public Key im DNS
- Signiert alle ausgehende Mail mit dem Private Key
- Signatur im Mailheader
- Empfänger-Mailserver überprueft und verwirft, falls unpassend

DKIM: Beispiel DNS-Eintrag

- _domainkey.mail.complx.org.
- IN TXT "r=hostmaster@complx.org; s=nn"

- nn._domainkey.mail.complx.org.
- IN TXT "v=DKIM1; k=rsa; p=MIIBIjANBg[...]"

- p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCg
  KCAQEArtSIKw258tcYisMb/4yX4MjyI710fnavudVOvSCm
  J4cwFy3RRcluKm5wtEjs0XjsN3DS8gpJ+MwbaNH8CUDH40
  lVDy+uR+MfLMjrVKjv/ypAhtcPFDcR3nsKldvRwmq4DOFz
  qPlCtTjkTlCbUAY5ryuDyrrVz5XAVjxUHXIsdrrR1OAaRH
  LDnd03EiIVmZF+CSv1UsPg2g/5i4+LhlysLT/ioA3K9hyY
  iB3HXs7qY9sW6q0YjhMAL7s8OEJ0O5O2wAMqqbN5dtNvw6
  +HIyA4P/3yznc3xl+CcFfZr8G2iLeBpPvIJYi8kMeGFGyk
  dwTbyYjZQ2Jxytac1CuOafKGSQIDAQAB

DKIM: Erzeugen der Keys und DNS Einträge

- openssl genrsa -out dkim.key 2048
- openssl rsa -in dkim.key -out dkim.pub -pubout -outform PEM
- Script, um daraus einen DNS RR zu machen: https://opsec.eu/src/dkim/pub2rr

DKIM: exim config (1) Router

```
dnslookup_dkim:
  driver = dnslookup
  condition = ${perl{senderdomhasdkim}{'exists'}}
  domains = ! +local_domains
  transport = remote_smtp_dkim
  no_more
```

DKIM: exim config (2) Transport

```
remote_smtp_dkim:
  debug_print =
        "T: remote_smtp_dkim for $local_part@$domain"
  driver = smtp
  dkim_domain = $sender_address_domain
  dkim_selector = nn
  dkim_private_key =
        /var/mbx/$sender_address_domain/Conf/dkim.key
  dkim_canon = relaxed
  dkim_strict = false
  #dkim_sign_headers = DKIM_SIGN_HEADERS
```

DKIM: Probleme

- Mailverteiler und Weiterleitungen tun nicht mehr
- Subdomains müssen beachtet werden
- Webserver und Webformulare
- Spammer fügen DKIM-Records für ihre Domains hinzu
- Key-Management
- Mail-Formate sind komplex

DMARC

- Domain-based Message Authentication, Reporting, and Conformance
- RFC 7489
- Absender definiert, wie ein Empfaenger mit Mail umgeht, falls SPF/DKIM/... scheitert
- Ebenfalls in einem DNS Eintrag
- Beispiel: "v=DMARC1;p=reject;pct=100;rua=mailto:postmaster@compl
- Dienstleister, die die Ergebnisse auswerten https://dmarcian.com/dmarc-status/
- Config siehe https://github.com/Exim/exim/blob/master/doc/doc-txt/experimental-spec.txt

DANE: DNS-Based Authentication of Named Entities

- RFC 6698
- Public-Key-Cryptographie, Verwendung von TLS Zertifikaten
- TLS == Transport Layer Security (alter Name: SSL)
- Absender-Domain veröffentlicht Zertifikat im DNS
- Authentizität sollte dann aber DNSSEC gesichert sein
- Empfänger: Fragt DNS nach Zertifikat bzw. Unterschrift einer Certification Authority (CA)
- DANE-TA(2), Trust Anchor, daher: Traue dieser CA
- DANE-EE(3), End Entity, letztlich: self-signed Certificate
- Nur bei Übereinstimmung ist Absender-Server OK
- Config siehe https://github.com/Exim/exim/blob/master/doc/doc-txt/experimental-spec.txt

Ratelimiting

- Eigentlich wichtig für ausgehende Mail
- ... wenn der Server missbraucht wird
- Problem: Missbraucher senden nur noch wenige Mails und wechseln dann den Server
- Implementierung: Komplex, wenn individuell zu konfigurieren

Probleme

- False Positives
- Das Reihenfolgeproblem
- Auslieferungsproblem-Problem (Failed Mail)
- Das Mehrempfaenger-Problem
- Das Key-Management Problem
- Das Mailinglisten-Problem
- Das Mailforwarding Problem
- Backscatter
- Silent Discard: Zulassen oder nicht ?
- Juristische Probleme

False Positives

- Wenn eine Mail als Spam erkannt wurde...
- ...obwohl sie erwünscht war ?
- Lösung: Spam-Quarantäne

Das Reihenfolgeproblem

- Mailserver bedienen mehrere Domains und mehrere Postfächer
- Regeln werden nacheinander abgearbeitet
- Server-weite Regeln
- Domain-weite Regeln
- Postfach-spezifische Regeln
- Was tun, wenn sich einzelne Regeln wiedersprechen ?
- Ansatz: Scoring Regel-Liste
- Problem: Ergebnis für User nicht einfach nachvollziehbar
  Beispiel: SpamAssassin
- Sieve: An Email Filtering Language, RFC 5228

Das Auslieferungsproblem-Problem

- Wenn eine Mail vom Empfänger zurückgewiesen wurde, wird eine 'failed mail' erzeugt
- Der Absender dieser failed mail ist envelop-from: <>
- Die Fehlermeldung: Leider: Freies Format
- Korrelation versendete Mail mit Failed Mail ?
- Sonst: Offen für Spam

Das Mehrempfänger-Problem

- In einer SMTP-Transaktion kann eine Mail an mehrere Empfänger eingeliefert werden.
- Wie teilt SMTP dem Absender mit, wenn einer der Empfänger die Nachricht nicht will, der andere aber explizit ?
- Per-Recipient Data Response
- Wurde nie ein offizieller Standard http://www.ietf.org/mail-archive/web/ietf-smtp/current/msg07655.html

Das Key-Management-Problem

- Bei vielen Verfahren werden Crypto-Verfahren verwendet
- Diese Verfahren verwenden öffentliche und private Schlüssel
- Sicher erzeugen, verwalten, speichern und übertragen

Das Backscatter-Problem

- Spammer versendet viele gefälschte Mails
- Aber leider mit einem gefälschten Absender meiner Domain ?
- Und die Empfängeradressen sind ungültig
- Viele Failed Mail
- Oder empörte Empfänger
- In der Praxis selten eskaliert (Spammer wollen nicht auffallen)

Das Silent Discard-Problem

- Eingehende Mail wird als Spam erkannt
- Löschen, ohne sie dem Absender zurückzuschicken ?
- Wegspeichern in Spampostfach/Quarantäne ? Wie lange ?
- Open Source Software, die diese Funktion bereitstellt ?

Juristische Probleme

- Einige Juristen sagen, dass eine Aufbewahrungspflicht für Geschaeftskommunikation besteht.
- Laufzeit: 10-11 Jahre
- Auch fuer Spam ?
- Muss man daher alle Spam annehmen ?
- Hört sich etwas abseitig an
- Aber: Wo kein Kläger, da kein Richter

Das Markt-Problem

- Mailserver-Betrieb wird so komplex, dass sich der Markt auf Grossanbieter konzentriert.
- Der Markt regelt alles, nur nicht immer im Interesse Aller
- Verbraucherschutz

Lösungsskizze: Spam-Polizei

- Staatliche Stelle
- Missbrauchsreports sammeln (freiwillig!)
- automatische Verfahren (Open Source usw)
- Nach Häufigkeit ordnen
- Die grössten Verstösse...
- ... zur Quelle verfolgen
- offen, nicht verdeckt
- Im Inland: abstellen
- International: kooperieren
- Die Marktlösung ist volkswirtschaftlich teurer

Zum Nachlesen

- https://www.heise.de/artikel-archiv/ix/2015/07/110_Mailwehr

Vielen Dank für Ihre Aufmerksamkeit