Andrey Kiselev, 123RF

Antispam-Blacklisten

Dunkle Mächte

Das Blacklisting auffälliger Hosts gilt als probates Mittel im Kampf gegen Spamversender. Doch nicht jeder, der auf einer Blackliste landet, hat sich vorher als Spammer unmöglich gemacht. Zunehmend geraten die Böse-wichte-Katalogisierer selbst in die Kritik. Wolf-Dieter Mergenthaler

Das System der Schwarzen Listen funktioniert genau umgekehrt wie die Gästeliste in der Disco: Findet der Türsteher des Lokals den Namen des Einlass Suchenden auf der Gästeliste, darf der passieren. Gelangt aber jemand auf eine Schwarze Liste, dann wird er abgewiesen, sei es eine Fluggesellschaft, deren Maschinen Europa nicht mehr anfliegen dürfen, oder sei es ein Host, der als Spammer aufgefallen ist und von dem darum prophylaktisch niemand E-Mails empfangen will.

Door Policy

Das Schwarze-Liste-System leuchtet schnell ein und wird in der Praxis oft und gern eingesetzt. Seine Wirksamkeit und Akzeptanz steigen und fallen allerdings mit der Art und Anwendung der Kriterien, wie jemand auf eine Schwarze Liste gelangt. Während eine auf Flugsicherheit spezialisierte Organisation anhand von wohldefinierten Standards und offen publizierten Regeln über die Landerechte eines Carriers entscheidet, herrscht andernorts bei den Betroffenen der Eindruck einer großen Willkür vor – ähnlich wie an der Discotür, wo der Clubbesitzer die Gästliste nach Gutsherrenart verwaltet.

Bei Antispam-Blacklisten stellt sich heraus, dass viele Anbieter auf dem Transparenzniveau der Discotür agieren. Noch am sympathischsten arbeiten die, die im Internet E-Mail-Adressen streuen, um gezielt Spammails auf sich zu ziehen. Kommt eine Mail bei so einer Adresse an, gilt sie als Spam und die IP des absendenden Hosts landet auf der Schwarzen Liste. Der Kasten „Do it yourself" erklärt, wie ein Admin selbst so einen Spamdetektor aufsetzen kann.

Viele große Provider und Antispam-Filter, zum Beispiel Ironport [1], setzen ähnliche Verfahren (auch) ein und genießen dabei den Vorteil der Größe, mit ihr verstärkt sich der Nutzeffekt: Jede Mail, die das Ziel nicht erreicht, spart Rechenleistung. Das Risiko bei solchen Listen sind Autoresponder: Sendet ein Angreifer in großem Umfang E-Mails an ein Postfach, das eine Vacation-Nachricht reflektiert, und verwendet er eine gefälschte Absenderadresse, dann landet die automatische Antwort im „Blockade-Postfach". Daraufhin landet ein legitimer Absender auf der Backlist. Davor kann nur eine Whitelist oder das gelegentliche Überwachen durch einen Menschen schützen.

Sippenhaft nach Herkunft

Wer durch einen solchen Autoresponder auf eine Blackliste gekommen ist, darf sich als Teil der Völkergemeinschaft fühlen: Eine Menge Blacklists sperren gleich ganze Länder aus [2][3][4]. Forschungskooperationen mit Hochschulen in Fernost oder Geschäftskontakte nach Südamerika müssen die Betroffenen dann über Facebook abwickeln.

Das häufig gehörte Argument: In diesen Ländern stünden die meisten Spamrechner. Doch das stimmt gar nicht: Die meisten Spammails stammen aus der westlichen Welt, die USA und europäische Staaten spielen ganz weit vorne mit [5] [6]. Doch keiner käme auf die Idee, das eigene Land zu blocken.

Auch die Statistik meint es mit den Schwarzen Listen nicht besonders gut: Auf der MIT Spam Conference [8] stellten Mitarbeiter des Instituts für Internetsicherheit der FH Gelsenkirchen die Ergebnisse ihrer aktualisierten Untersuchung zu Blacklists vor [9]. Dabei stellte sich heraus, dass sich die Blacklists untereinander weniger stark überlappen als vermutet, beispielsweise 80 Prozent zwischen Nix-Spam-List und Spamhaus.
Die Wissenschaftler glichen die Blacklisten zudem die mit einer expliziten Whiteliste ab. Eigentlich dürfte keine Blackliste solche IPs enthalten. Tatsächlich schlugen manche Blacklisten bei bis zu 5 Prozent aller legitimen IPs (falschen) Alarm. Da sind einem die Antispam-Dienstleister fast lieber, die schon auf der eigenen Webseite warnen, ihre Verfahren seien experimentell und aggressiv und mithin im Alltag ungeeignet [10].

Wie komme ich dort wieder runter?

Das Business der Spamversender ist trotz der großen Streuverluste und der Strafverfolgung lukrativ. Nicht wenige Beobachter meinen, dass die Strukturen denen der organisierten Kriminalität ähnlich seien. Die Betreiber der Schwarzen Listen sind die natürlichen Gegner der Spammer und befürchten persönliche Repressalien der Kriminellen. Wohl darum nennt kaum eine Blackliste ihren Betreiber genau, Spamhaus [11] zum Beispiel ist auf seine Anonymität stolz.
Das Nachsehen haben legale Mailserver-Betreiber, die versehentlich auf eine Schwarze Liste gelangt sind. Sie tun sich schwer, einen Kontakt zum Betreiber herzustellen, ganz zu schweigen davon, ihn wegen Unterlassungs- und Schadensersatzansprüchen vor Gericht zu bekommen. Das Zivilrecht kennt kein Verfahren gegen Unbekannt.
Wie an der Discotür sieht sich der Abgewiesene auf die Gnade des Betreibers angewiesen. Freundliches Nachfragen und viel Geduld sind nötig, aber nicht immer erfolgversprechend. In der Regel existiert ein Webformular, in das der Geschmähte die eigene IP-Adresse eintragen muss, so zum Beispiel bei Spamhaus und Spamcop [12]. In simplen Fällen fällt die Sperre dann 45 Minuten später.
Einspruchsmöglichkeiten sehen die Regeln meist nur wenige vor. Spamcop sagt dazu auf der Webseite: Nach 24 Stunden ohne Spamreport fiele die falsch gelistete IP sowieso von der Liste – für Spamcop lohne es nicht, vor Ablauf dieser Zeit tätig zu werden. Klar macht Spamcop auch, dass die Firma bereit ist, den Schaden durch Aussitzen notfalls zu vergrößern: „Wenn Sie mit rechtlichen Schritten drohen, müssen wir Ihre E-Mail an unsere Rechtsabteilung geben. Das wird dann jede Aktion verzögern, die wir vielleicht sonst unternommen hätten."
Ein extrem beratungsresistenter Fall ist APEWS [13], eine weitere Blacklist. Hier sehen die FAQ auf der Webseite gar keine Verfahren vor, die zum Austragen einer IP führen könnten. Auch gibt es keine sonstige Kontaktmöglichkeit zu den Betreibern. Da es offenbar genügend Blacklisting-Opfer gibt, bildet sich auch gleich ein passendes Geschäft dazu: UCE Protect beziehungsweise Whitelist.org [14] setzt einzelne IPs oder ganze Adressbereiche (die so genannten Level 1 bis 3) erstmal auf seine Blackliste. Nach Zahlung eines Betrages schaltet der „Dienstleister" die IPs auf seine Whitelist (Abbildung 1).

Dynamisch

Wenn ein DSL-Kunde sich bei seinem Provider einwählt, bekommt er seine IPs dynamisch zugewiesen. Einen Tag später kriegt sie ein anderer Kunde – oft genug einer mit einem ungepflegten Windows-PC, auf dem sich eine stattliche Malwaresammlung ansammelt. Wegen solcher Spamschleudern kann man verstehen, dass Blacklisten und Mailserver dynamische IPs grundsätzlich blocken.
Sie verfolgen dabei unterschiedliche Ansätze, um die dynamischen IPs zu ermitteln: Einigen testen per einfachem DNS-Reverse-Lookup, ob im Rechnernamen etwa »DSL«, »dynamic« oder »pool« auftaucht – was die Betreiber dabei vorverurteilter Hosts mit statischer IP, die vielleicht »dynamic.cloud.*tld*« heißen, nicht freut. Andere Betreiber sind umsichtiger und lassen sich von den großen Providern die Adressblöcke ihrer dynamischen IP-Pools geben. So ist der Ausschluss wenigstens sinnvoll begründet.

Eine feste IP soll helfen

Das Problem der Blockade dynamischer IPs lässt sich umgehen, zumindest für Unternehmen. Denn die finden bei allen größeren Providern in der Aufpreisliste die Option „Feste IP". Auf einer solchen wird ein Kunde erwarten, einen Mailserver störungsfrei betreiben zu können, und wird das vielleicht sogar zur Vertragsbedingung mit seinem Anbieter machen. Die meisten Provider trennen diese statisch vergebenen IPs von ihrem dynamischen Adressbereich, was Blacklistern die Unterscheidung erleichtern sollte.
Manchmal erweist es sich trotzdem für DSL-Kunden mit statischer IP als unerwartet schwierig, einen Mailserverbetreiber vom Gegenteil zu überzeugen, der die eigene IP fälschlich als „dynamisch" einstuft. Vor einigen Monaten traf es ironischerweise ausgerechnet einen Antispam-Experten, der auch seine Dissertation über Maßnahmen gegen illegale Werbemails geschrieben hat: Auf der MIT Spam Conference [8] berichtete der Hamburger Professor und regelmäßige Linux-Magazin-Autor Tobias Eggendorfer, dass Dataport, der IT-Dienstleister der Stadt Hamburg, seinen Mailserver mit statischer IP blockt. Dadurch kann er mit keiner Einrichtung seiner Heimatstadt kommunizieren.
Eggendorfer fand heraus, dass die IP seines Servers auf keiner öffentlichen Blacklist auftaucht. Das legt nahe, dass

Do it yourself

Mailserver-Betreiber, die selbst eine Blackliste verwalten möchten, werden zum Beispiel bei Open BSDs Spamd [7] fündig. Der Daemon kann auf bestimmten Mailkonten einlaufende E-Mails direkt auf seine Schwarze Liste setzen. Dazu konfiguriert sich der Admin lediglich ein paar E-Mail-Adressen, die er sonst nicht verwenden will, und publiziert sie eifrig auf Internetseiten, sodass die Harvester der Spammer sie finden.

Jetzt muss nur noch der Spamd über den Befehl

```
spamdb -T -a 'spamtrap@mydomain.org'
```

erfahren, dass das die Adressen sind. Ab sofort landen alle IPs, die versuchen dorthin eine Mail zu senden, auf der Liste. Das Verfahren ist nachvollziehbar und für jeden, der Drittanbietern misstraut, leicht zu implementieren.

Abbildung 1: Whitelisted.org – nützlicher Service oder ein dreist erpresserisches Geschäftsmodell?

Dataport eigene IP-Listen benutzt. Das sollte ein Entfernen ja besonders einfach machen, vermutete er anfangs.

In seinem Vortrag belegte er aber, dass für ihn über mehrere Monate und Eskalationsstufen hinweg keine Besserung erzielbar war – was wohl kein Einzelfall ist [15]. Mittlerweile beschäftigt der Streit die Anwälte (siehe Kasten „Kein Kommentar"). Immerhin: Da Eggendorfer eine Meldeadresse des Anbieters besitzt, weiß er, gegen wen er juristisch vorgehen muss – gegen Spamhaus oder APEWS wäre sein Ansinnen versandet.

Verworrene Rechtspraxis

Wie das zuständige Gericht in Hamburg am Ende entscheidet, ist weitgehend offen, weil die Materie ziemlich vertrackt ist: So sind Mittel als legitim einzuschätzen, die eigene Infrastruktur gegen Spam zu schützen. Im vorliegenden Fall bedeutet das eingesetzte Antispam-Blacklisting auf der anderen Seite, dass ein Hamburger Bürger mit eigenem Mailserver nicht mit seiner Stadtverwaltung per Mail kommunizieren darf – im speziellen Fall Eggendorfer sogar ein Beamter nicht mit seinem Dienstherrn.

Das Amtsgericht Lüneburg hatte 2007 den Fall eines Multilevel-Marketing-Anbieters zu verhandeln, den sein Provider über Blacklists ausfilterte. Obwohl solche Werbefirmen in Sachen unverlangter E-Mail nicht per se unverdächtig sind, gab das Gericht dem Kläger Recht. Es hielt das Blacklisting für wettbewerbswidrig und untersagte die Sperre [16].

In der Literatur oft diskutiert ist zudem die Frage, ob Blacklisten generell dem Unterdrücken von Nachrichten entspricht, was nach §206 StGB eine Verletzung des deutschen Fernmeldegeheimnisses bedeutete und damit strafbar wäre. Die Gegenposition lautet: Der Mailserver, der die Blacklist nutze, unterdrücke die Mail gar nicht, sondern lehne nur die Zustellung ab.

Die Gegner dieser Auffassung bemühen den Versand eines Briefes als Vergleich und sagen, dass der Absender durch das „Einwerfen" der Mail in seinen Mailserver bereits soweit geht wie ein Briefversender, der das Kuvert in den Postkasten wirft. Die Sendung gelte als aufgegeben. Wenn nun ein Mailserver die Annahme der Nachricht verweigere, sei das so, als ob der ausliefernde Postbote keine Lust habe, den Brief zuzustellen. Wegen der Unterdrückung der Sendung müsse der Bote mit Strafe rechnen.

Blacklist-Hölle

Als Fazit lässt sich sagen: Blacklisten widersprechen einander, Einspruch gegen einen Eintrag ist nur schwer möglich, auch weil die meisten Betreiber bewusst anonym agieren. Die Rechtslage für Betreiber wie Kunden ist verworren. Betreiber eines großen Mailservers sollten darum überdenken, ob sie Mails nur auf Basis einer Blacklist ablehnen sollen.

Salomonisch wirkt der Ansatz von Spamassassin: Ein Eintrag auf einer Blacklist bewirkt für eine E-Mail hier zwar einen Negativ-Score, führt aber nicht allein zur Ablehnung. Auch als guter Weg erscheint es, Mails erstmal anzunehmen und pro User in verschiedene Ordner wie »Spam«, »Spamverdacht« und »Geprüft« zu verteilen. Hier kann und soll der Empfänger selbst entscheiden. Der Provider entgeht damit auch dem Vorwurf, Nachrichten zu unterdrücken. *(jk/ofr)* ■

Infos

[1] Ironport: [http://www.ironport.com/de/]

[2] Material zur „The Abusive Hosts Blocking List": [http://www.ahbl.org/documents]

[3] Listings for all known Korean net blocks: [http://www.okean.com/antispam/korea.html]

[4] The South Korean Network Blocking List: [http://korea.services.net]

[5] The 10 Worst Spam Countries: [http://www.spamhaus.org/statistics/countries.lasso]

[6] Spam Sources by Country: [http://www.m86security.com/trace/spam_statistics.asp]

[7] Stephan A. Rickauer, „Spamd bekämpft Spam unter Open BSD", Linux-Magazin 02/09, S. 64

[8] MIT Spam Conference: [http://projects.csail.mit.edu/spamconf/]

[9] „Detecting Gray in Black and White": [http://www.internet-sicherheit.de/uploads/media/Christian-Rossow-Thomas-Czerwinski-Christian-J-Dietrich-Detecting-Gray-in-Black-and-White-MIT-spam-conference-2010.pdf]

[10] What is the Spamcop Blocking List: [http://www.spamcop.net/fom-serve/cache/297.html]

[11] Spamhaus: [http://www.spamhaus.org]

[12] Spamcop: [http://www.spamcop.net]

[13] APEWS: [http://www.apews.org]

[14] Whitelist.org: [http://www.whitelisted.org]

[15] Heise-Meldung zu Dataport: [http://www.heise.de/newsticker/meldung/Was-war-Was-wird-948045.html] (3. Meldung)

[16] AG Lüneburg, Az. 7 0 80/07, Urteil vom 27.9.07 ([http://www.amtsgericht-lueneburg.niedersachsen.de])

Der Autor

Wolf-Dieter Mergenthaler hat in den 80ern Informatik studiert und arbeitet schon einige Jahren im Antispam-Bereich. Das dabei gern eingesetzte Blacklisting sieht er seit einiger Zeit überwiegend kritisch.