IP-Blacklists sinnvoll kombinieren

Blockwerk

Christian Rossow, Christian Dietrich, Norbert Pohlmann

Trotz eines Spam-Anteils jenseits der 90 Prozent funktionieren die Mailserver bei Providern, Unternehmen und anderen größeren Organisationen, und die Anwender nutzen ihr Lieblingsmedium weiterhin unverdrossen. Großen Anteil daran haben IP-Blacklists, von denen viele Postmaster sogar mehrere einsetzen.

Blacklists sind umstritten. Doch solche Verzeichnisse von IP-Adressen Spam-versendender Rechner bilden anerkanntermaßen einen wichtigen Schutzmechanismus im Kampf gegen den Missbrauch von Internet-Ressourcen. Eine Reihe von ihnen lässt sich kostenlos nutzen. Bei der Auswahl von Blacklists zur Spam-Abwehr auf einem Mailsystem verlassen sich viele Systemadministratoren und IT-Entscheider aufs Hörensagen oder auf ihr Gefühl. Die Erfahrung anderer ist – wie so oft – ein wichtiger Gesichtspunkt bei der Auswahl von Blacklists. Das Folgende stellt, basierend auf empirischer Inhaltsanalyse einiger frei verfügbarer Blacklists, weitere Anhaltspunkte dar, die bei der Auswahl und insbesondere beim Kombinieren von Blacklists helfen können.

Das Markieren, mehr noch das Blockieren von Spam anhand der IP-Adresse des Absenders hat den Vorteil, dass es enorme Ressourcen sparen kann. Der SMTP-Dialog wird dann in der Regel bereits in einem frühen Stadium durch das annehmende Mailsystem unter Angabe eines Fehlercodes beendet (Reject). Es findet also keine Übertragung des Inhalts der E-Mail statt, und der annehmende Mailserver muss sich gar nicht erst um die Verarbeitung kümmern. Dies macht sich umso vorteilhafter bemerkbar, je stärker der Mailserver ausgelastet ist. Anti-Spam-Maßnahmen wie Inhalts- und Virenfilter erfordern sehr viel I/O- und Rechenleistung.

Blockieren als zweischneidiges Schwert

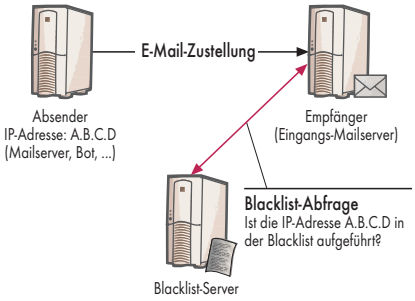
Allerdings ergibt sich ein potenzieller Nachteil beim Einsatz von IP-Blacklisting. Wer beispielsweise – wie es immer wieder vorkommt – einen eigentlich legitimen Ausgangs-Mailserver blockiert, den Spam-Versender missbrauchen, enthält seinen Anwendern auch erwünschte E-Mails von dort vor. Der gelistete Provider gerät dadurch unter Druck und muss sich um eine Austragung seiner IP-Adresse kümmern, will er seine Kunden behalten. Blacklist-Betreiber und -Anwender müssen insbesondere bei großen Providern mit Augenmaß vorgehen, da sonst möglicherweise ein einzelner Benutzer durch den Versand von Spam Tausende von Anwendern desselben Mailservers in Mitleidenschaft ziehen kann. Andererseits hilft dieser Druck mitunter, dass Provider schnell reagieren und den Spammer aus ihrem Netz befördern. Leider gibt es aber auch viele Beispiele, in denen Provider weder auf Beschwerden über spammende Kunden noch auf Blacklistings reagieren.

Es ist daher für Anwender von IP-Blacklisting umso wichtiger, auf eine nachvollziehbare und vertretbare Art und Weise Spam-Abwehr zu betreiben: Zum einen, um den eigenen Kunden und Anwendern einen angemessenen Schutz zu bieten, zum anderen, um im Falle eines Listings eine klare Begründung geben zu können.

Blacklists arbeiten unterschiedlich

Vor diesem Hintergrund ist es interessant, inwieweit die Inhalte, also die gelisteten Adressen verschiedener Blacklists, einander überschneiden oder auch ergänzen. Dies könnte Administratoren Hinweise darauf geben, wie viele und vor allem in welcher Kombination Blacklists sinnvoll zur Spamabwehr geeignet sind.

Blacklists unterscheiden sich hinsichtlich der Policy, die darüber bestimmt, welche IP-Adressen auf die



Mithilfe einer während des SMTP-Dialogs abgefragten, oft von externen Dienstleistern betriebenen IP-Blacklist können Mailserver darüber entscheiden, welche E-Mails sie als spamverdächtig markieren oder gleich ablehnen. Fürs Filtern nach der Zustellung beim Endanwender sind sie weniger gut geeignet (Abb. 1).

Liste gelangen können. Oft sind Blacklists in mehrere Subzonen mit speziellen Policies unterteilt. Darüber hinaus unterscheidet sich die Dauer des Listings einer IP-Adresse. Manche Blacklists entfernen IP-Adressen nach einer definierten Zeit, beispielsweise die Blacklist der *iX*-Redaktion (www.nixspam.org) nach derzeit vier Tagen. Andere lassen IP-Adressen für unbestimmte Zeit in der Blacklist und entfernen Einträge allenfalls bei begründeten Beschwerden der Gelisteten.

Blacklists weisen unter anderem wegen der unterschiedlichen Policies deutliche Unterschiede in ihrem Umfang auf. Einige führen lediglich einzelne IP-Adressen unabhängig voneinander auf, die beispielsweise nur dann Eingang in die Liste finden, wenn sie tatsächlich als Spam-Quelle auftreten. Andere listen dagegen ganze IP-Adressbereiche, etwa dann, wenn in bestimmten Subnetzen eine gewisse Zahl einzelner IP-Adressen als Spam-Quellen aktiv und ein Kollateralschaden in der „Adressnachbarschaft“ unwahrscheinlich ist. Solche Blacklists können wesentlich größere IP-Adressbereiche abdecken, ohne dass tatsächlich von jeder einzelnen IP-Adresse Spam ausging.

Der Anteil der gelisteten Adressen lässt sich an der theoretischen Gesamtzahl von IP-Adressen messen. IPv4 stellt rund 4,2 Milliarden zur Verfügung. Für die Praxis ist allerdings der Anteil der gelisteten Adressen an der praktisch nutzbaren Menge zugewiesener IP-Adressen aussagekräftiger (siehe Tabelle), die derzeit etwa bei der Hälfte der Gesamtzahl liegt.

Umfang einiger IP-Blacklists

Name	Adressbereich	Einträge	IPv4-Anteil	Nutz-Anteil
pbl.spamhaus.org	320 152 000	130 000	7,4541 %	18,3826 %
xbl.spamhaus.org	5 789 000	5 789 000	0,1348 %	0,3324 %
CBL	5 212 000	5 212 000	0,1214 %	0,2993 %
all.dnsbl.sorbs.net	5 090 000	2 836 000	0,1185 %	0,2923 %
dnsbl.njabl.org	4 459 000	4 459 000	0,1038 %	0,2561 %
dnsbl.ahbl.org	3 488 000	3 132 000	0,0812 %	0,2003 %
dnswl.org (Whitelist)	2 867 000	9 000	0,0668 %	0,1647 %
sbl.spamhaus.org	1 807 000	5 000	0,0421 %	0,1038 %
UCEPROTECT L1	801 000	801 000	0,0187 %	0,0460 %
NiX Spam	78 000	78 000	0,0018 %	0,0045 %

Optimieren durch Vergleichen

Eine besondere Stellung nimmt in der Vergleichstabelle die Liste dnswl.org ein. Es handelt sich nicht um eine Black-, sondern um eine Whitelist mit dem Ziel, die Zahl von Fehlalarmen durch gelegentlich auf Blacklists auftauchende „richtige“ Mailserver zu reduzieren. So gibt es eine Menge Spam, der zum Beispiel von Google- oder Yahoo-Accounts ausgeht, aber nicht jeder möchte solche namhaften Mail-Provider aussperren, wenn sie mal wieder die Aufnahme in eine Blacklist ausgelöst haben. dnswl.org listet gezielt solche Server, denen man zutrauen kann, vor allem tatsächlich erwünschte E-Mails zu versenden.

Eine Vergleichsmatrix zeigt den Anteil, der sich in zwei zu vergleichenden Blacklists überschneidet. Die Angabe der Werte erfolgt prozentual, gemessen an der Blacklist der Zeile.

Beim Interpretieren der vorliegenden Auswertung ist zu beachten, dass es sich bei der Analyse von Blacklists stets um eine Momentaufnahme handelt. Sie ändern sich durch zum Teil sehr schnelles Hinzufügen und Entfernen von Adressen laufend. Die Zahlen der hier aufgeführten Blacklists stammen vom 12. Juli 2007. Nicht alle Blacklist-Betreiber bieten von sich aus ihren kompletten Datenbestand zum Download an. Bei einigen war viel Überzeugungsarbeit dafür notwendig, ausnahmsweise Zugriff auf die Listen zu erhalten.

Die Listen in Form von DNS-Zonen oder als Text-Downloads komplett anzubieten, ergibt aber aus mehreren Gründen Sinn. Einerseits motiviert man Vielnutzer, die Listen zu spiegeln und dadurch sowohl viel Traffic zu sparen als auch die Informationen über Kommunikationspartner zurückzuhalten, die sie sonst mit den DNS-Anfragen preisgeben. Zum anderen sind die Nutzer weniger abhängig vom Anbieter, falls dessen eigene DNS-Server ausfallen.

Im Vergleich zeigen sich deutlich die Beziehungen der Blacklists von Spamhaus untereinander. Offensichtlich umfasst die XBL (xbl.spamhaus.org) die CBL komplett. Außerdem enthält die PBL einen Großteil der CBL (circa 74 %). Darüber hinaus deckt die PBL große Teile anderer Blacklists ab. So sind beispielsweise IP-Adressen der von der *iX* gepflegten Blacklist NiX Spam zu mehr als 55 % in der Liste von Spamhaus enthalten. Umgekehrt führte NiX Spam zum Zeitpunkt der Erhebung mit 0,007 % nur einen kleinen Bruchteil der PBL, was wegen des enormen Umfangs der PBL immerhin rund 21 600 Einträge ausmachte.

iX-TRACT

- Zum Entlasten von Mailservern, Verbessern der Filterquote und um Druck auf spammerfreundliche Provider auszuüben, setzen viele Postmaster Blacklists mit IP-Adressen ein, von denen Spam ausgeht.
- Diverse Blacklists bieten sich für den Einsatz an, doch nicht jede Kombination eignet sich für einen effizienten Mailserver-Betrieb.
- Selbst umfangreiche Blacklists decken weniger als 10 Prozent des gesamten IPv4-Adressbereichs ab und treffen über den Rest keine Aussage.
- Zukünftig dürften Verfahren an Bedeutung gewinnen, die allen IP-Adressen eine mehr oder weniger gute Reputation zuordnen können.

Einige IP-Blacklists im Vergleich (gemeinsame Anteile in %)

Blacklist	all.dnsbl.sorbs.net	UCEPROTECT L1	NiX Spam	dnsbl.ahbl.org	sbl.spamhaus.org	dnsbl.njabl.org	CBL	pbl.spamhaus.org	xbl.spamhaus.org	dnswl.org	Bogus ranges
all.dnsbl.sorbs.net	–	1,83	0,28	10,17	10,67	11,03	8,03	36,92	17,92	0,002	7,73
UCEPROTECT L1	11,61	–	2,34	1,97	0,58	2,93	64,14	69,96	64,79	0,026	0,01
NiX Spam	18,32	23,80	–	1,79	0,64	2,58	41,02	55,36	42,58	0,064	0,02
dnsbl.ahbl.org	14,83	0,45	0,04	–	0,56	64,32	3,74	66,38	13,87	0,002	0,22
sbl.spamhaus.org	29,15	0,25	0,03	1,04	–	0,88	1,23	5,49	1,49	0,003	9,68
dnsbl.njabl.org	12,59	0,53	0,05	50,31	0,37	–	4,75	67,11	21,03	0,003	0,28
CBL	7,84	9,86	0,62	2,50	0,44	4,07	–	73,91	100,00	0,001	0,00
pbl.spamhaus.org	0,58	0,17	0,01	0,72	0,03	0,93	1,19	–	1,36	0,000	1,48
xbl.spamhaus.org	15,39	8,76	0,57	8,17	0,47	15,83	88,05	73,92	–	0,001	0,01
dnswl.org (Whitelist)	0,003	0,007	0,002	0,003	0,002	0,005	0,001	0,002	0,002	–	0,027
Bogus ranges	0,03	0,00	0,00	0,00	0,01	0,00	0,00	0,34	0,00	0,000	–

Beim Kombinieren von Blacklists spielen die jeweiligen Schnittmengen für die Gesamtwirksamkeit eine große Rolle. Die Tabelle zeigt den prozentualen Anteil an IP-Adressen der Blacklist A (Zeile), den auch Blacklist B (Spalte) abdeckt.

Die PBL umfasst alle von Providern als „Mailserver-frei“ gemeldeten Adressen, die in der Regel dynamisch an Einwahl- und DSL-Kunden vergeben werden, also nicht nur verifizierte Spamquellen.

Es zeigt auch auf, welche Kombinationen von Blacklist-Abfragen sinnvoll sind. Zwei Blacklists mit geringen Überschneidungen zu vereinen, ist wesentlich effektiver, als solche zu kombinieren, die eine hohe Anzahl von IP-Adressen übereinstimmend aufführen. So erscheint es wenig sinnvoll, Spamhaus’ XBL mit der CBL zu kombinieren, die in der XBL enthalten ist. Andererseits lässt sich die NiX-Spam-Liste gut zusammen mit den Listen von SORBS einsetzen, da mehr als vier von fünf Einträgen der NiX-Spam-Liste nicht von SORBS gelistet sind.

Abbildung 2 zeigt den gesamten Adressraum von IPv4. Die obere Hälfte der Grafik repräsentiert die NiX-Spam-Blacklist, der untere Teil stellt den Inhalt der PBL grafisch dar. Die Horizontale ist in 256 Adressblöcke mit jeweils 16 777 216 (2^{24}) IP-Adressen unterteilt. In der CIDR-Schreibweise entspricht dies sogenannten /8-Netzen. Die Y-Achse gibt logarithmisch an, wie viele IP-Adressen in der jeweiligen Blacklist (oben NiX Spam, unten PBL) gelistet sind. Die Länge der senkrechten Linien verdeutlicht, dass es zwar hinsichtlich der Anzahl der Einträge Unterschiede gibt, dass jedoch kaum Adressblöcke nur in einer der beiden Listen vertreten sind.

Black- versus Whitelists

Whitelists eignen sich hervorragend zum Schutz vor falschen Einträgen in Blacklists. Bei auf Whitelists gelisteten IP-Adressen handelt es sich meistens um legitime E-Mail-Server. Von ihnen ausgehende E-Mails sollen von Black- oder Greylisting unbehelligt bleiben. Da aber auch gewöhnliche Mailserver gelegentlich zum Versenden von Spam missbraucht werden, können durchaus manche IP-Adressen sowohl auf Blacklists als auch auf Whitelists gelistet sein.

Wie bereits erläutert, kann ein einziger Anwender eines E-Mail-Systems den Ruf des gesamten Systems und somit all seiner Nutzer schädigen. Im schlimmsten Fall führt dies zur Eintragung des Servers in Blacklists. Solche Systeme kann man durch Whitelisting schützen und dadurch das verbindungsorientierte Blacklisting umgehen. Deshalb ist es sinnvoll, neben Blacklisting andere Filter einzusetzen, darunter Inhaltsfilter, die eine Entscheidung pro individueller E-Mail treffen und auch beim Aussetzen von Blacklisting noch Spam filtern können. Die Vergleichsmatrix zeigt, dass sich die

CBL: Zuordnung zu autonomen Systemen

AS	Bezeichnung	Einträge	lokaler Anteil [%]
9121	TTNET	234 145	2,393
4134	Chinanet-Backbone	205 120	0,298
27699	Telecom. de Sao Paulo	157 017	6,347
7738	Telecom. da Bahia	152 159	3,034
8167	Telecom. de Santa Catarina	148 816	6,894
8151	Uninet S.A. de C.V.	135 221	1,101
4837	China169-Backbone CNC Group	112 558	0,531
9829	BSNL National Internet Backbone	106 412	1,527
7643	Vietnam Posts and Telecom.	101 770	10,492
3269	Telecom Italia	99 629	0,826

dnsbl.njabl.org: Zuordnung zu autonomen Systemen

AS	Bezeichnung	Einträge	lokaler Anteil [%]
4134	Chinanet-Backbone	708 818	1,031
4837	China169-Backbone CNC Group	285 048	1,344
4766	Korea Telecom	193 308	0,782
27699	Telecom. de Sao Paulo	164 522	6,650
9318	Hanaro Telecom	161 925	1,849
7132	AT&T Internet Services	126 151	0,404
7738	Telecom. da Bahia	112 192	2,237
22927	Telefonica de Argentina	102 464	13,192
3462	HINET Data Comm.	84 589	1,094
8151	Uninet S.A. de C.V.	76 139	0,620

Überschneidungen zwischen diversen Blacklists und der Whitelist dnswl.org mit Werten unterhalb des Promillebereichs in Grenzen halten.

Verbotene Zonen im Internet

Ebenfalls interessant ist der Vergleich von Whitelists mit sogenannten Bogons, nicht zugewiesenen und damit eigentlich nicht aktiven Netzbereichen. Sie umfassen neben per Definition nicht benutzbaren oder reservierten Netzadressen auch von der IANA noch nicht vergebene IP-Adressen. Externer IP-Verkehr aus diesen Bereichen kann also ohne Auswirkungen auf die Erreichbarkeit komplett und schon am Router blockiert werden. Für Blacklists hat es somit keine negativen Auswirkungen, falls sie Bogons umfassen. Gänzlich anders ist die Ausgangssituation bei Whitelists: Für Bogons ist eine Listung zum Umgehen von Blacklisting kontraproduktiv.

Beim Blick auf die Vergleichsmatrix fällt auf, dass die Whitelist dnswl.org eine gewisse Überschneidung mit den als Bogon deklarierten Netzadressen aufweist. Auf Anfrage hat der Betreiber der Whitelist diese Einträge inzwischen gelöscht. Es handelte sich wahrscheinlich einfach um Tippfehler. Der Betreiber will zukünftige Einträge auf Bogons prüfen, um neue derartige Fehleinträge zu vermeiden.

Fehlerhafte Listungen einer Whitelist wie dieser können fatale Folgen haben. Schafft es ein Spammer, von einer IP-Adresse auf der Whitelist aus E-Mails zu versenden, verzichten je nach Bekanntheits- und Nutzungsgrad der Whitelist viele Eingangs-Mailserver auf ein Blacklisting. Das kann zur starken Mehrbelastung nicht nur des Servers, sondern auch der Empfänger führen, zu denen dann mehr Spam durchdringt.

Vergleich mit Routing-Informationen

Das Analysieren von Blacklists erlaubt auf bequeme Weise eine Zuordnung von unangenehm auffallenden IP-Adressen zu Ursprungsländern oder autonomen Systemen (AS). So lassen sich Statistiken über die Provider und Länder mit den meisten Spam-Quellen erstellen, ohne auch nur eine einzige Spam-Mail selbst empfangen zu müssen. Hier dienten die Blacklists CBL und dnsbl.njabl.org diesem Zweck. Die CBL enthielt zum Zeitpunkt der Analyse etwa 5,2 Millionen, dnsbl.njabl.org umfasste rund 4,5 Millionen IP-Adressen.

Ein autonomes System ist eine Einheit mit gemeinsamen Routing-Informationen – etwas vereinfachend, aber meist korrekt mit „Internetprovider“ beschrieben. Die zehn am häufigsten von Blacklistings getroffenen AS sind aufgeführt. Es fällt zum Beispiel auf, dass sich das chinesische AS 4134 auf beiden Blacklists weit oben befindet. Bei den meisten handelt es sich um asiatische oder amerikanische AS, aber auch die europäische Telecom Italia ist in der Listung der CBL zu finden. Die Spalte rechts gibt an, welchen Anteil des jeweiligen AS die Blacklist enthält. So ragen beispielsweise das AS 7643 auf der CBL mit 10,5 % und das AS 22927 auf dnsbl.njabl.org mit 13,2 % des gesamten für das AS verfügbaren Netzbereichs hervor.

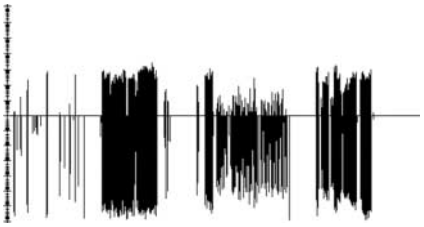
Eine etwas abstraktere Sicht ermöglicht die Zuordnung von IP-Adressen zum Herkunftsland. So kann man teilweise die regionale Ausrichtung einer Blacklist erkennen und schwarze Schafe unter den Ländern ausmachen. Negativ fallen in beiden Blacklists die Länder China, Brasilien und die Vereinigten Staaten auf. Aber auch europäische Länder gibt es innerhalb der „Worst 10“: Deutschland und Polen sind – wenig schmeichelhaft – oft in der CBL vertreten, Frankreich hat viele Einträge in dnsbl.njabl.org. Darüber hinaus fällt in der NJABL-Liste der hohe Anteil (3,9 %) an gelisteten IP-Adressen im Verhältnis zu Argentiniens gesamtem verfügbaren Adressraum auf. Das als ergiebige Spam-Quelle bekannte China ist in absoluten Zahlen tatsächlich jeweils

dnsbl.njabl.org: Zuordnung zu Staaten

Land	Einträge	Anteil dort [%]
China	1268571	0,977
USA	476130	0,019
Korea	448338	0,772
Brasilien	441364	1,881
Indien	194092	1,412
Argentinien	186102	3,884
Frankreich	131657	0,099
Mexiko	118733	0,612
Taiwan	113741	0,607
Japan	96239	0,043

CBL: Zuordnung zu Staaten

Land	Einträge	Anteil dort [%]
Brasilien	563159	2,400
China	424435	0,327
USA	359369	0,014
Türkei	235375	2,867
Russland	223684	1,391
Indien	219334	1,596
Deutschland	196971	0,283
Korea	196485	0,339
Mexiko	152294	0,785
Polen	142674	1,169



Eine grafische Gegenüberstellung der PBL (unten) mit NiX Spam macht deutlich, dass Spammer oft ähnliche Adressblöcke zum Versenden der Nachrichten verwenden (Abb. 2).

recht weit oben angesiedelt. Im Vergleich zu anderen Ländern sind dort jedoch relativ kleine Teile des verfügbaren Adressraums gelistet.

Globale IP-Reputationsdatenbank

Angesichts der zum Teil stark voneinander abweichenden Inhalte diverser Blacklists stellt sich die Frage, welcher Anteil des insgesamt im Internet genutzten IPv4-Adressraums sich durch die Vereinigung aller Blacklists überhaupt abdecken ließe. Es stellt sich heraus, dass die genannten Black- und Whitelists zusammen gerade einmal zu 20 Prozent aller nutzbaren rund 2 Mrd. IP-Adressen überhaupt eine Aussage treffen. Der theoretische IPv4-Adressraum beläuft sich sogar auf rund 4,2 Mrd. IP-Adressen, die also von Black- und Whitelists heutzutage nur zu etwa 10 % abgedeckt sind.

Umgekehrt zeigt dies leider, dass Spammer durch die Nutzung von „frischen“, ungelisteten IP-Adressen in mindestens 80 % aller Fälle nicht von einer Blacklist gesperrt werden können. Es verdeutlicht aber auch das hohe Potenzial künftiger IP-Reputationssysteme. (un)

CHRISTIAN ROSSOW

ist Mitarbeiter im Forschungsbereich E-Mail-Sicherheit des Instituts für Internet-Sicherheit an der FH Gelsenkirchen.

CHRISTIAN DIETRICH

ist Mitarbeiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen und für den Forschungsbereich E-Mail-Sicherheit verantwortlich.

PROF. DR. NORBERT POHLMANN

ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der FH Gelsenkirchen.

Literatur

[1] Bert Ungerer; Eingeschränkt; IP-Blacklists gegen unerwünschten Datenverkehr; *iX* 4/2007, S. 102

[2] Manuel Schmitt; Entlastungsfrage; Echtzeit-DNS-Blacklist als Mittel gegen Spam; *iX* 12/2007, S. 112