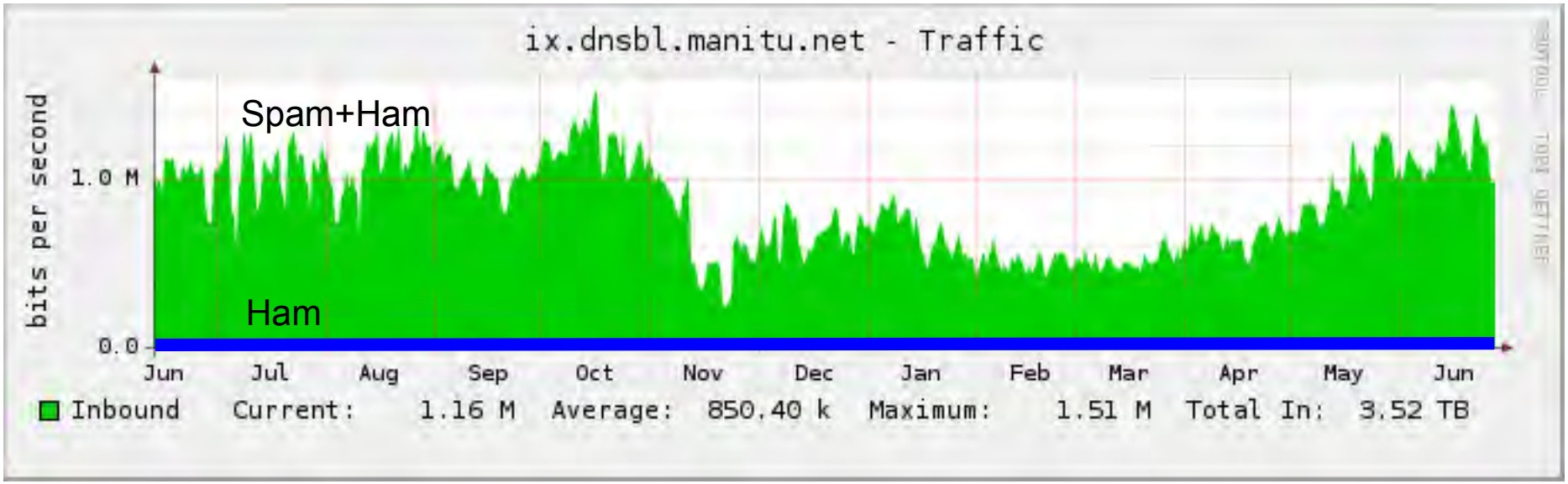
Blacklist-Projekt "NiX Spam"

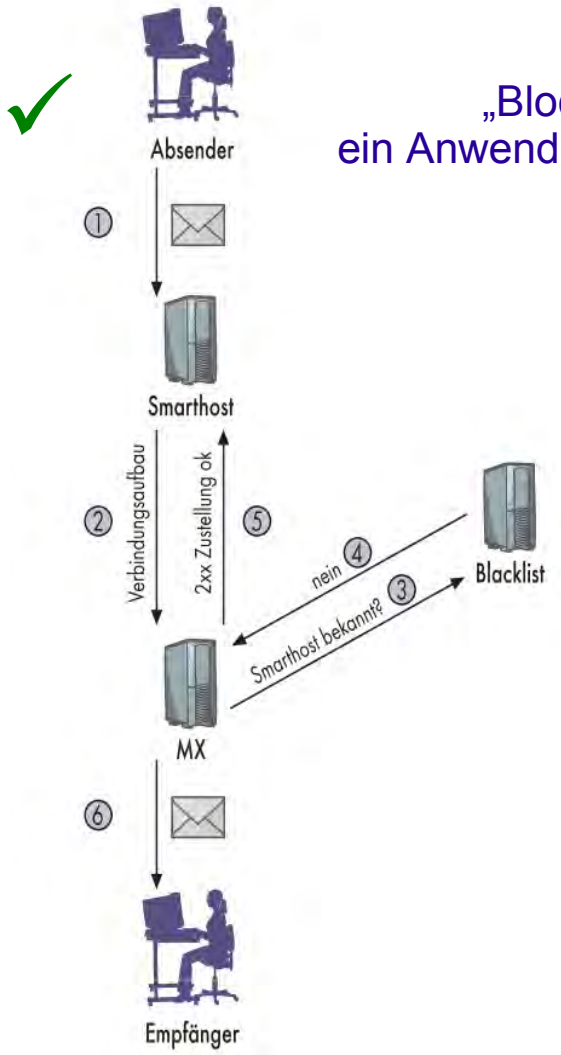
Bert Ungerer, Redaktion *iX*
Mailserver-Konferenz 2009

E-Mail-Datenverkehr von Spam dominiert

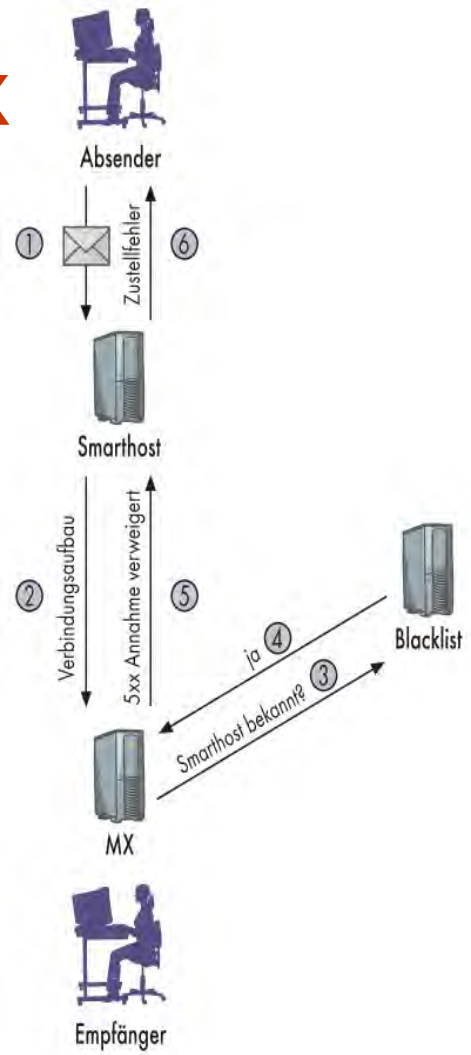


Quelle: Dr. Bülow & Masiak + eigene, stark vereinfachte Schätzung

DNS-basierte Blacklist (DNSBL) gegen E-Mail-Spam



„Blocken“ -
ein Anwendungsbeispiel



DNS-basierte Black(hole) / Blocking List (DNSBL)*

- ✓ Abfrage per DNS spart Ressourcen
- ✓ Nicht nur gegen E-Mail-Spam einsetzbar
- ✓ Mehrere DNSBLs lassen sich in Scoring einbinden
- x Policy und Identität der DNSBL-Betreiber oft unklar
- x Viel Spam über ISP-Smarthosts mit Millionen von Kunden - aggressive Blacklists erfordern parallelen Whitelist-Einsatz
- x DNSBL-Anwender geben Kommunikationsdaten preis - §!

*alias RBL™ by Trend Micro™

Positive Nebenwirkungen des DNSBL-Einsatzes

- ✓ Abweisen während des SMTP-Dialogs gibt Rückmeldung
- ✓ „Blocken“ schafft anders als „annehmen - markieren - zustellen - speichern - übersehen“ rechtlich klare Verhältnisse.
- ✓ Blacklistings als Druckmittel gegen spamfreundliche ISPs und ESPs
- ✓ Blacklists können Funktionsweise von Botnetzen und Verhaltensweisen von Spammern aufklären.
- ✓ Blacklists als Frühwarnsysteme für Malware-Befall

NiX Spam

- ✓ Analyse mehrerer Mio. E-Mails pro Tag an Mitarbeiter und diverse Spamtraps (u. a. web.de, GMX, eigene und gespendete Domains)
- ✓ Automatische Blacklist-Eintragung binnen Sekunden
- ✓ ca. 700.000 „neue“ IP-Adressen pro Tag, 400.000 in 12 h (Juli 2009)
- ✓ kostenlose Nutzung per DNS (Zone ix.dnsbl.manitu.net)
- ✓ Austragung per E-Mail oder Web-Formular jederzeit kostenlos möglich (wenige IP-Adressen pro Stunde)
- ✓ DNSBL-Anwender filtern rund 200 Mio. Spam-Mails pro Tag
- ✓ Alternative Text-Liste zum Herunterladen (40.000, TTL < 1 h)
- ✓ Änderungstolerante Hash-Werte („Fuzzy Checksums“) verfügbar

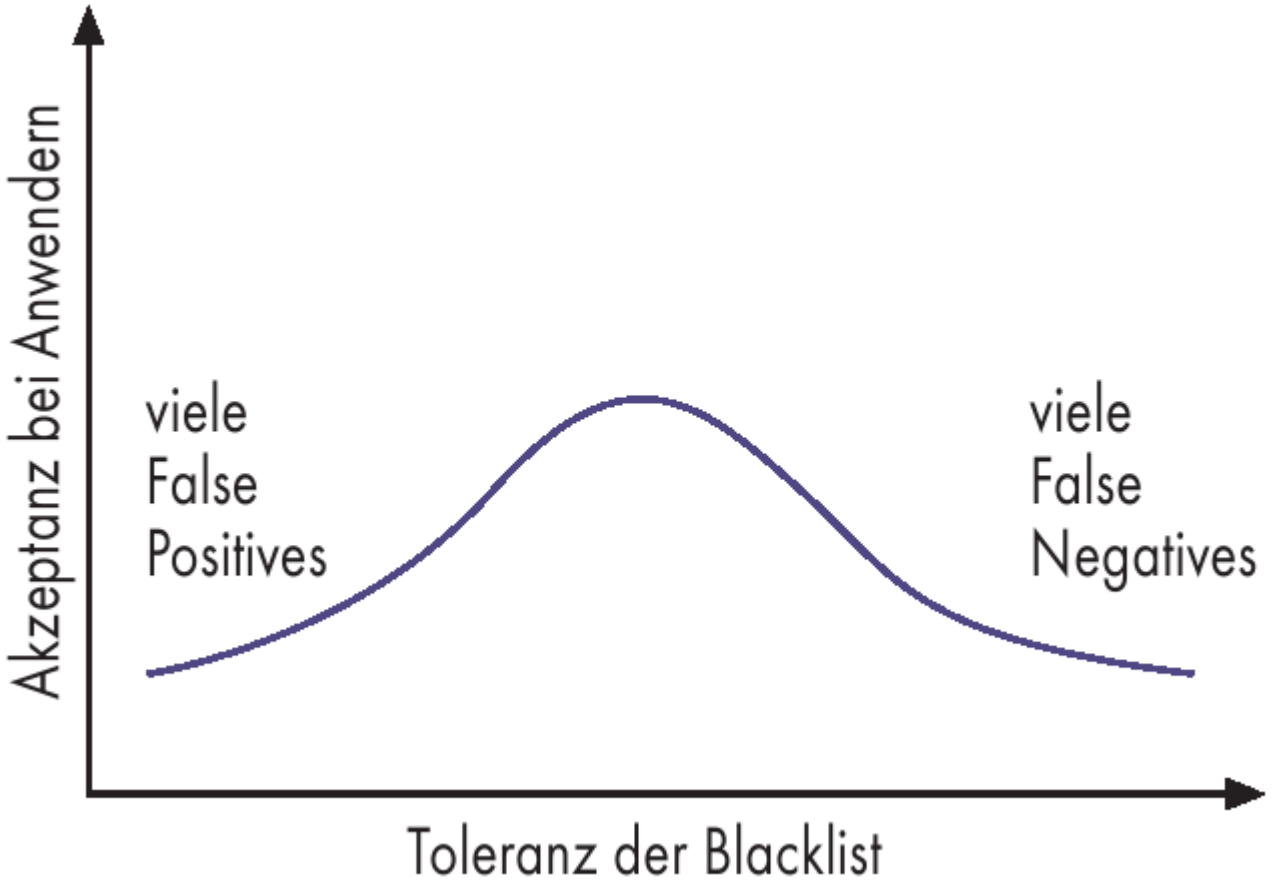
Alternative: Hash-Vergleich

- ✓ Hohe Genauigkeit (siehe z. B. bei Intra2net)
- ✓ Nebenwirkungen bei Fehleinschätzungen gering
- ✓ Interessant als Ergänzung zu IP-DNSBLs
- x Hoher Ressourcenbedarf, da Mail komplett vorliegen muss
- ✓ SpamAssassin-Plugin verfügbar: ixhash.sourceforge.net, wiki.apache.org/spamassassin/iXhash

NiX Spam: Besonderheiten

- ✓ Nur tatsächlich aktive Adressen gelistet, keine „verdächtigen Netze“
- ✓ TTL nur 12 h - keine „Langzeitbehandlung“ einzelner Täter oder spamfreundlicher Provider
- ✓ Keine „Strafeintragungen“ aus Nicht-Spam-Gründen
- ✓ Primär zur Entlastung/Unterstützung von Mailservern/Postmastern
- ✓ weitgehend automatisiert, insbesondere das Austragen
- ✓ Austragen nicht an Bedingungen (etwa Zahlungen) geknüpft
- ✓ Infrastruktur und Netztraffic gesponsert
- ✓ MX-Einträge und Spam-Weiterleitungen ebenfalls auf Spendenbasis
- ✓ Deep Header Inspection, daher geeignet für Analyse aller Received-Zeilen, nicht nur der IP-Adresse des direkt verbundenen SMTP-Clients

Toleranz einer Blacklist beeinflusst Akzeptanz



Vorsichtsmaßnahmen

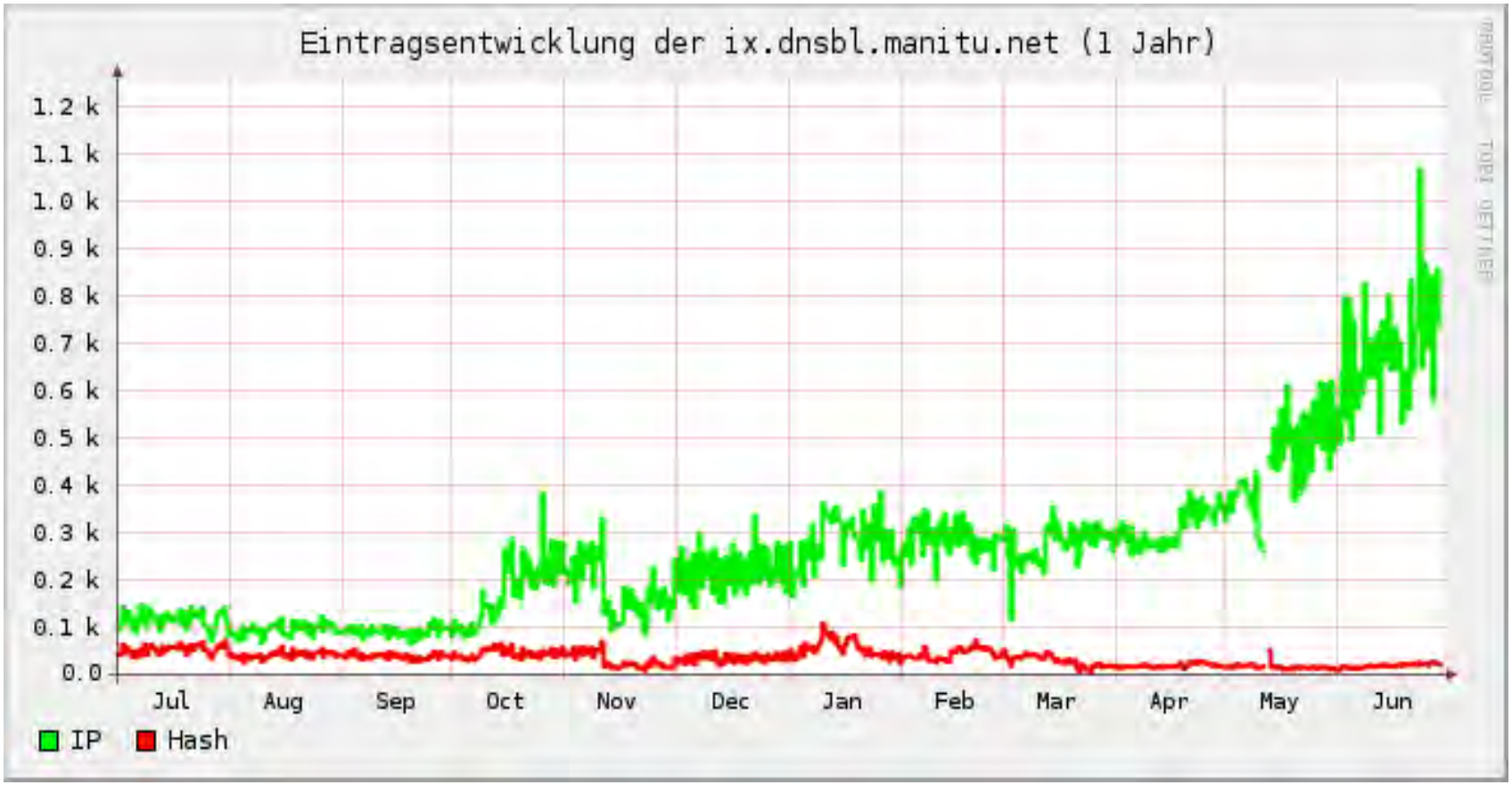
- ✓ Derzeit rund 32.500 Mailserver auf interner Whitelist (+ /24-„Nachbarn“) sowie etliche große Adressbereiche
- ✓ Sofortiges Austragen durch Anwender möglich
- ✓ Automatische Austragung nach nur 12 Stunden
- ✓ Automatische Whitelist-Eintragungen
- ✓ Keine automatische Austragung von Whitelist-Einträgen
- ✓ Hinweis auf Listing-Ursache schon im TXT Record (bitte mit 5xx im SMTP-Dialog ausgeben!)

„Blockender“ Mailserver muss Infos liefern

554 Service unavailable;
Client host [72.#.#.#] blocked using
ix.dnsbl.manitu.net; Spam sent to the mailhost
mail.ixlab.de was detected by NiX Spam at Wed,
01 Jul 2009 09:03:40 +0200, see
http://www.dnsbl.manitu.net/lookup.php?value=72.#.#.#

553 5.3.0 Mail from 202.#.#.# rejected - black list;see
http://www.heise.de/ix/nixspam/dnsbl/

ix.dnsbl.manitu.net: Eintragungen pro Minute



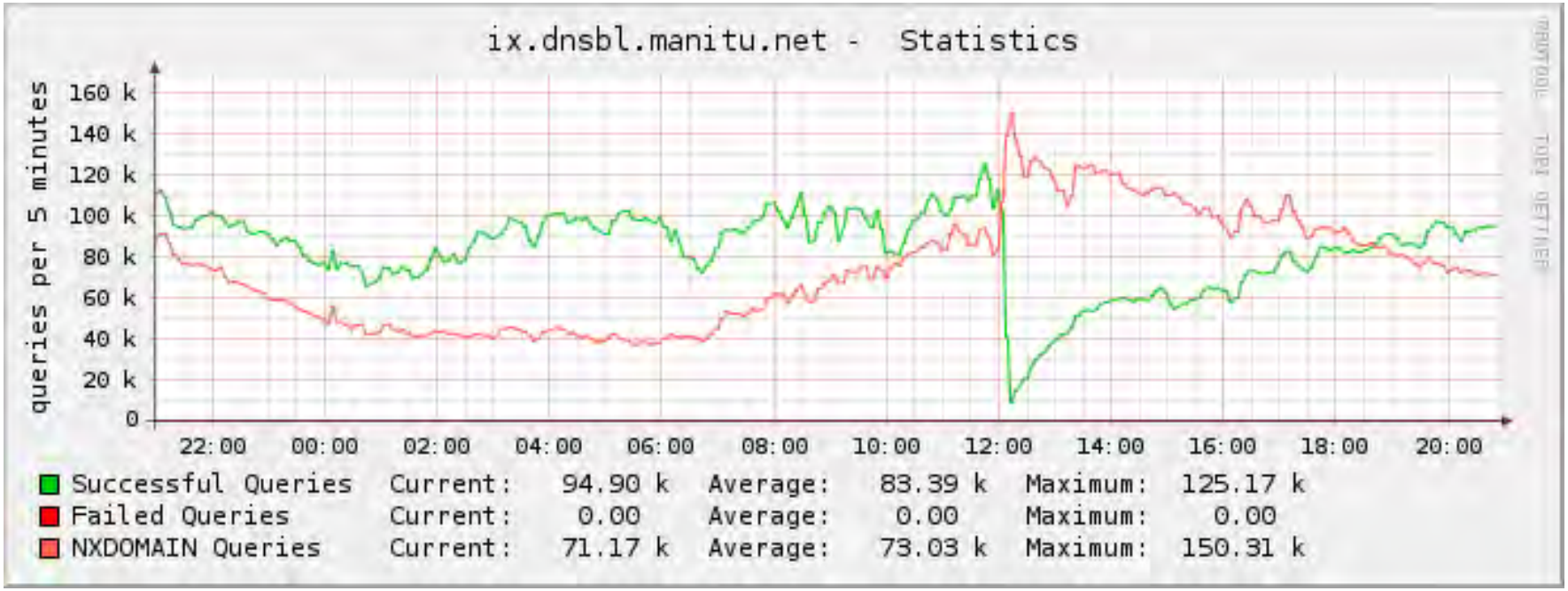
Stand: 30. Juni 2009

Traue keiner Statistik!

Trefferanteile Quelle	NiX Spam	Spamhaus PBL	Spamcop	Spamhaus SBL-XBL
Q-Space 30.6.2009	65 %	28 %	4 %	2 %
Jeff Makey KW 25, 2009	19 %	70 %	23 %	67 %
dihe's IP-Index ab Sept. 2006	59 k	58 k	58 k	79 k
Intra2net KW 25, 2009	66 % 0,1 % FP	70 % 0 % *	62 % 0,1 %	77 % 0 % *

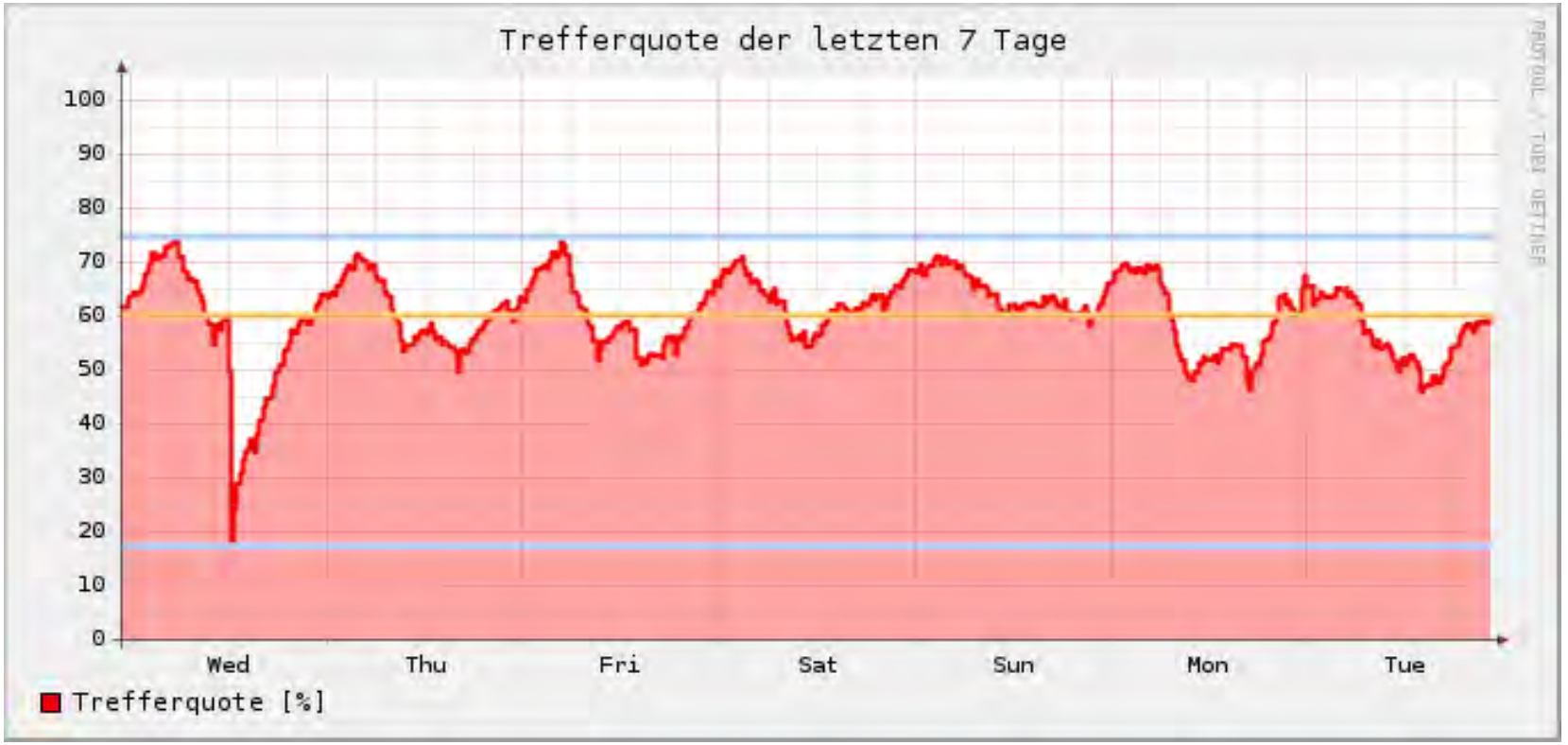
*** Geänderte Fassung: Die im Vortrag zitierten höheren False-Positive-Werte basierten auf von Spamhaus nicht empfohlenen SpamAssassin-Einstellungen. Für die ebenfalls erwähnte CBL bleibt es bei 77 % Wirksamkeit und einem FP-Anteil von 0,2 % im Vergleichszeitraum 14. bis 20. Juni 2009.**

Wirksamkeit nach „Reset“: Nach 8 h wieder „voll da“



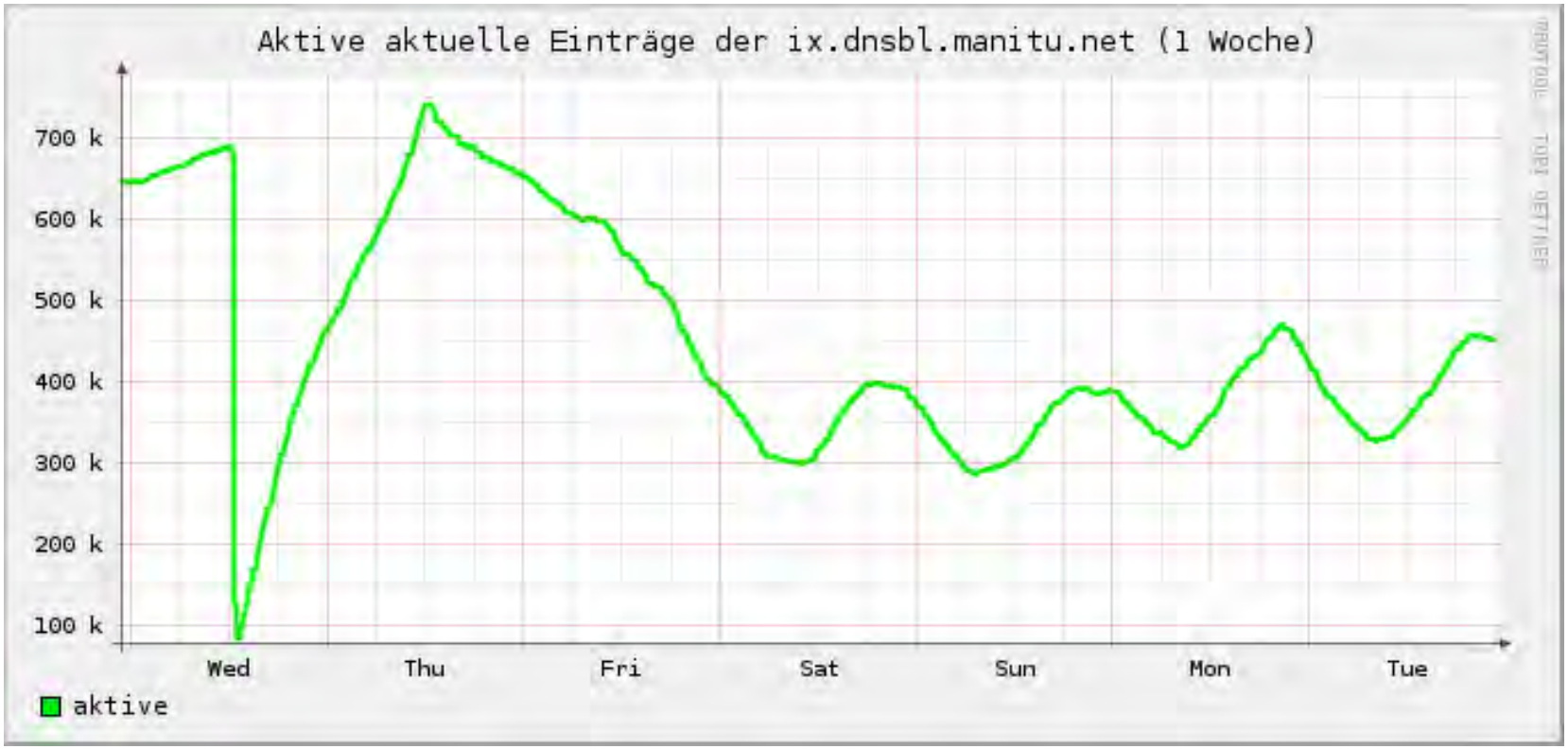
Quelle: Dr. Bülow & Masiak, 24. Juni 2009

Wirksamkeit nach „Reset“



Stand: 30. Juni 2009

NiX Spam: Zahl der Einträge



Stand: 30. Juni 2009

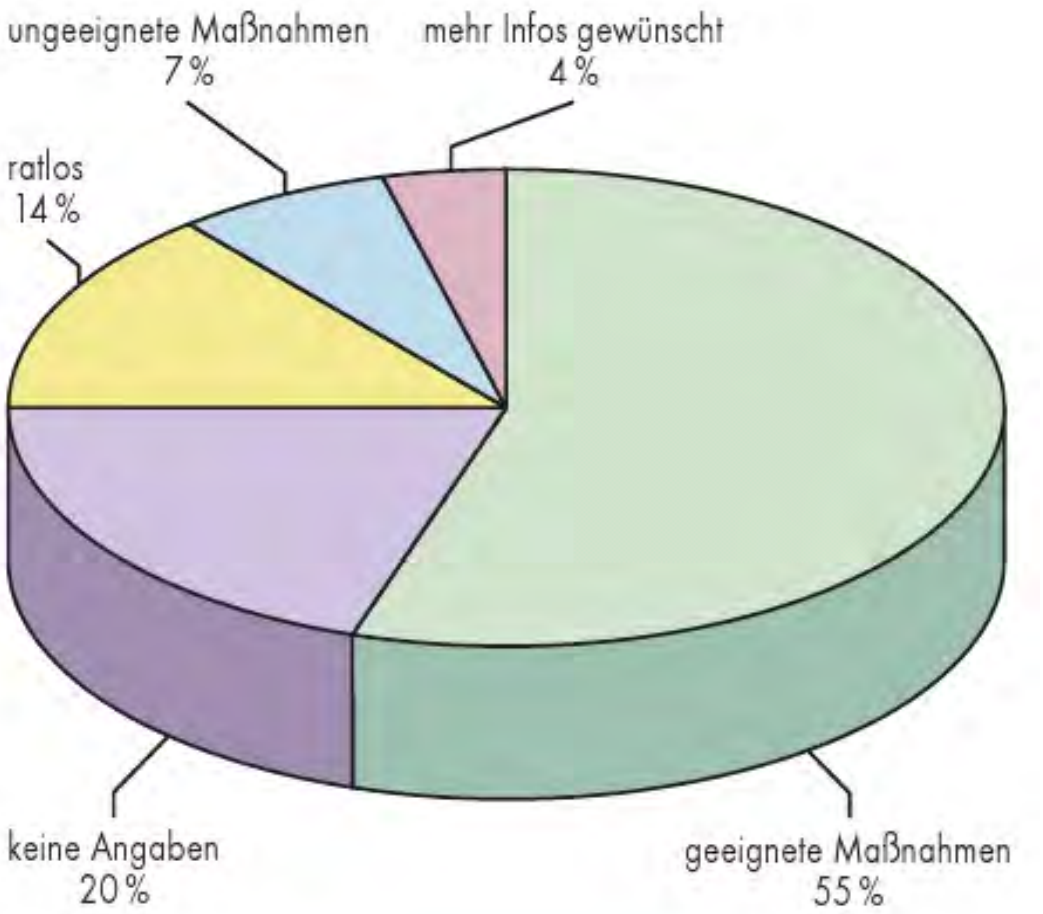
Verständnis für Blacklistings

- ✓ „Blocked port 25 for intranet hosts“
- ✓ „Offenes Relay gefunden, Problem behoben“
- ✓ „Deleted mk09trap@nixspam.org from mailing list“
- ✓ „Mitarbeiter wurde abgemahnt“
- ✓ „Bounces sollten jetzt nicht mehr vorkommen.“
- ✓ „Offending host disconnected and reformatted“
- ✓ „Trojan found and removed“
- ✓ „Killed spamming customer“
- ✓ „Verseuchtes Besucher-Notebook vom Netz genommen“

Weniger sinnvolle Reaktionen auf Blacklistings

- „Purchased Firewall / Barracuda / GFI / ...“
- „Idiot! This is the 12th time I fill this form!“
- „You are blocking a large Estonian ISP!“
- „I have Kaspersky.“
- „I call my lawyer if you block my email again.“
- „Ich informiere BND, Presse und meine Botschaft darüber, dass Sie meine E-Mails lesen und blockieren.“
- „Our Exchange host does not spam! No log entry!“
- „The blocked IP address is not being used for emails!“
- „Dear Barracuda Central / Spamhaus / Spamcop / ...“

Blacklist-Beschwerden im Überblick



Quelle: *iX* 6/2009

Wie man sich selbst auf Blacklists bringt - ganz ohne Malware

- Alle E-Mails erst annehmen, dann schauen, wohin damit - wozu gibt es Bounces? Die Absenderadresse wird schon stimmen.
- Filtern während des SMTP-Dialogs könnte zum Engpass werden. Spam- und Virenschutz brauchen Zeit und Unerwünschtes kann man ja zurücksenden.
- Mein Mailserver ist unter dem coolen Namen cust-host-0815.example.com erreichbar. Da kann ich mir den Pointer Record für Reverse Lookups sparen.
- Spamfilter sind nicht 100-prozentig sicher und daher im Urlaub *alle* E-Mails mit Abwesenheitshinweisen zu beantworten.
- Unsere neue Challenge-Response-Lösung ist genial: Zum Filtern nutzen wir jetzt die Arbeitskraft unbeteiligter Dritter.
- Aus rechtlichen Gründen müssen wir den Absender darüber informieren, dass seine Mail im Spam-Ordner gelandet ist.

E-Mail-Marketing kann zu Blacklistings führen

- Wir kaufen diese billige CD mit Adressdaten, dann können wir sofort loslegen.
- Hinter info@, webmaster@, support@ und alle@ stecken doch bestimmt interessierte Empfänger.
- mk09@htmlpost.de hat sich vor fünf Jahren angemeldet und nie etwas bestellt, der braucht attraktivere Werbemails.
- mk09@weiternicht.de ist seit zwei Jahren nicht erreichbar, aber vielleicht klappts beim nächsten Mal.
- Gültige Absenderadressen in eingehendem Spam bilden eine prima Datenbasis für unser nächstes Mailing.
- Single-Opt-in genügt, das macht doch sogar Apple so.
- Dafür muss das Opt-out so kompliziert wie möglich sein.

Vielen Dank fürs Unterstützen von „NiX Spam“

- ✓ Viele Spam-Forwarder
- ✓ Diverse Spender von MX Records
- ✓ Etliche Betreiber von DNS-Slaves
- ✓ Dirk Bonengel (iXhash-Plugin)
- ✓ Dietmar Braun (NetCologne)
- ✓ Thorsten Kraft (United Internet)
- ✓ Marcel Lohmann (malowa)
- ✓ Manuel Schmitt (manitu)
- ✓ und viele andere ...

Informationen, Ressourcen, Kontakt

- ✓ DNSBL-Zone: ix.dnsbl.manitu.net
- ✓ Test-Eintrag: 2.0.0.127.ix.dnsbl.manitu.net
- ✓ Statistiken, Lookup, Austragung: www.dnsbl.manitu.net
- ✓ Projekt-Webseite: ix.de/nixspam/dnsbl/
- ✓ Anwenderforum: ix.de/foren/forum-48292/list/
- ✓ Twitter: twitter.com/nixspam
- ✓ Artikel „Eingeschränkt“, *iX* 4/2007, S. 102
- ✓ Artikel „Schwarzhüter“, *iX* 6/2009, S. 86
- ✓ E-Mail: Bert Ungerer <un@ix.de>