Blacklist-Analyse

Von schwarzen Listen und schwarzen Löchern

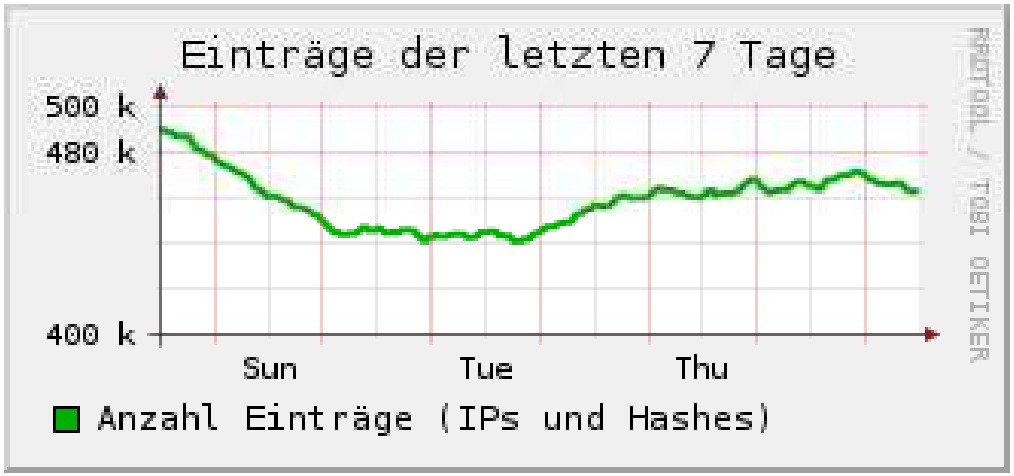
Christian J Dietrich
dietrich [at] internet-sicherheit . de

Christian Rossow
rossow [at] internet-sicherheit . de

Institut für Internet-Sicherheit
https://www.internet-sicherheit.de
Fachhochschule Gelsenkirchen

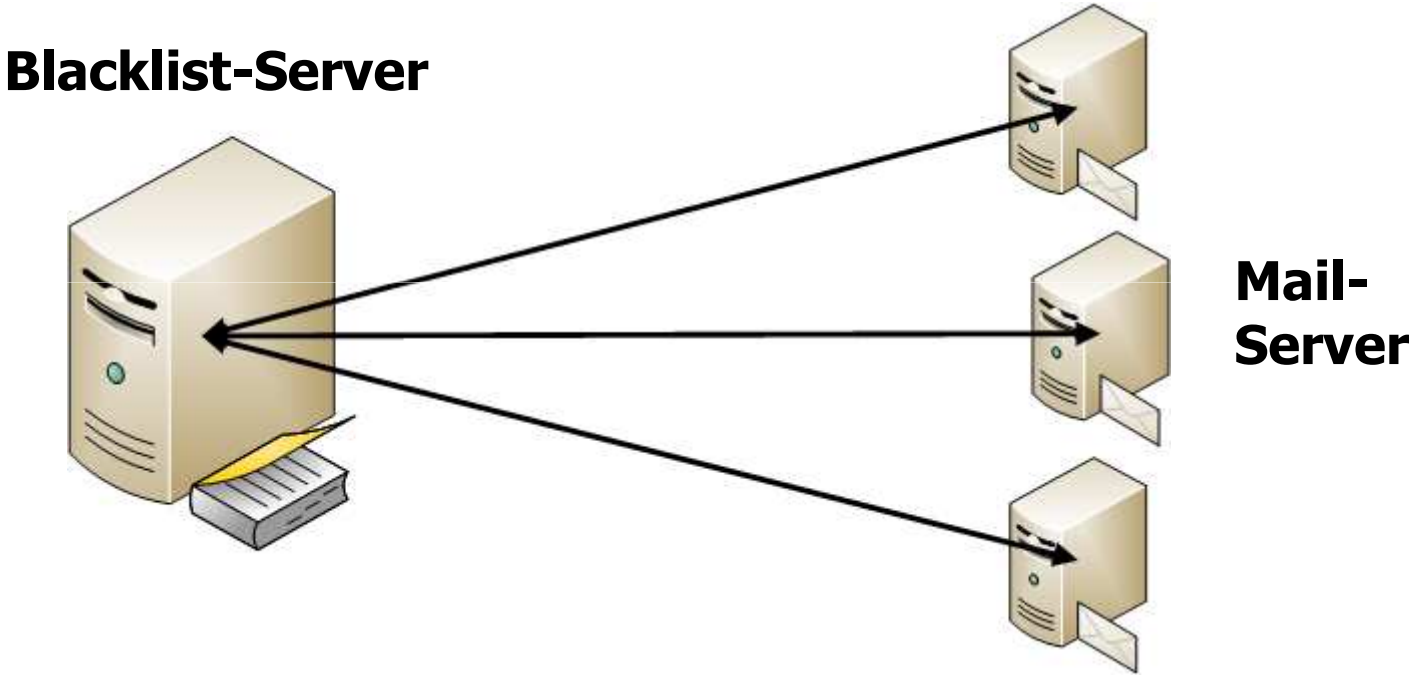
NiX Spam – Die Blacklist der iX

- Speicherung von **IP-Adressen** und Prüfsummen
- Spammer werden anhand von Spamtraps aufgespürt
- NiX Spam speichert Daten mit Spam-Aktivität innerhalb der vergangenen 3 Tage
- Wenig Daten = ineffektiv?
- Etwa 2000 Einträge werden sekündlich abgefragt

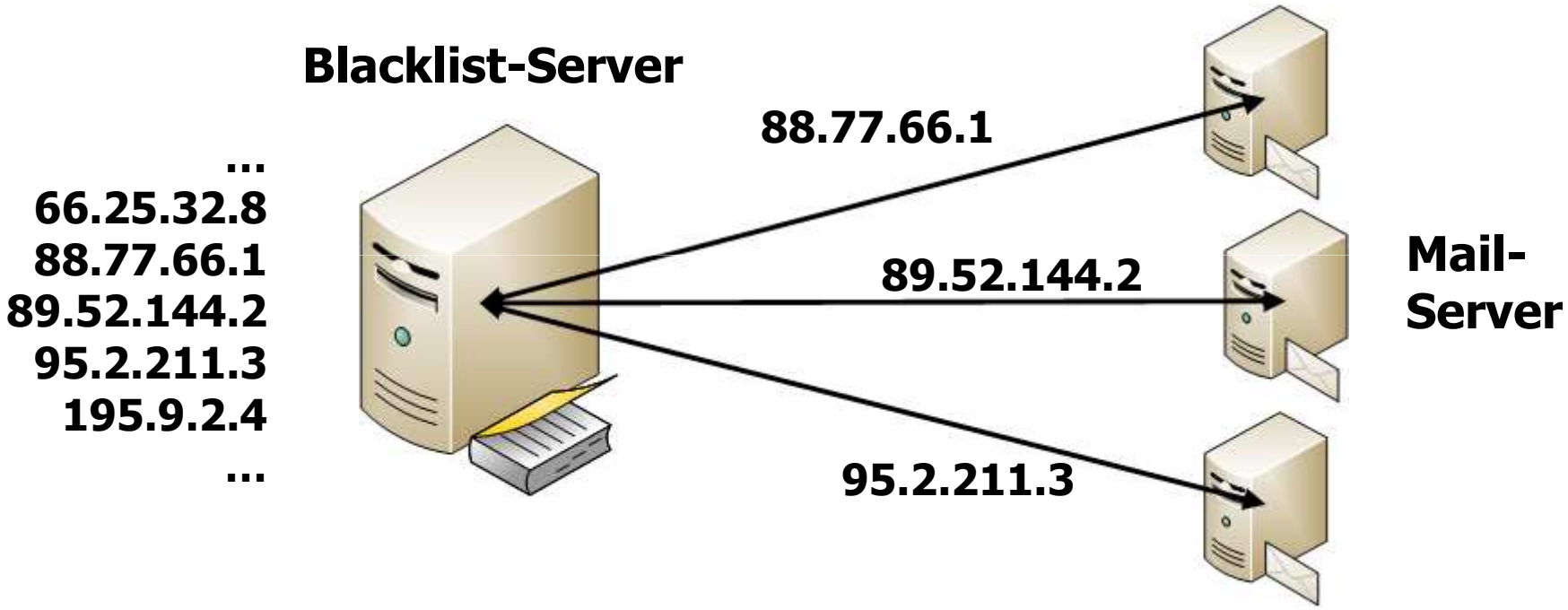


- Analyse des **Inhalts** sowie des **Abfrageverhaltens**

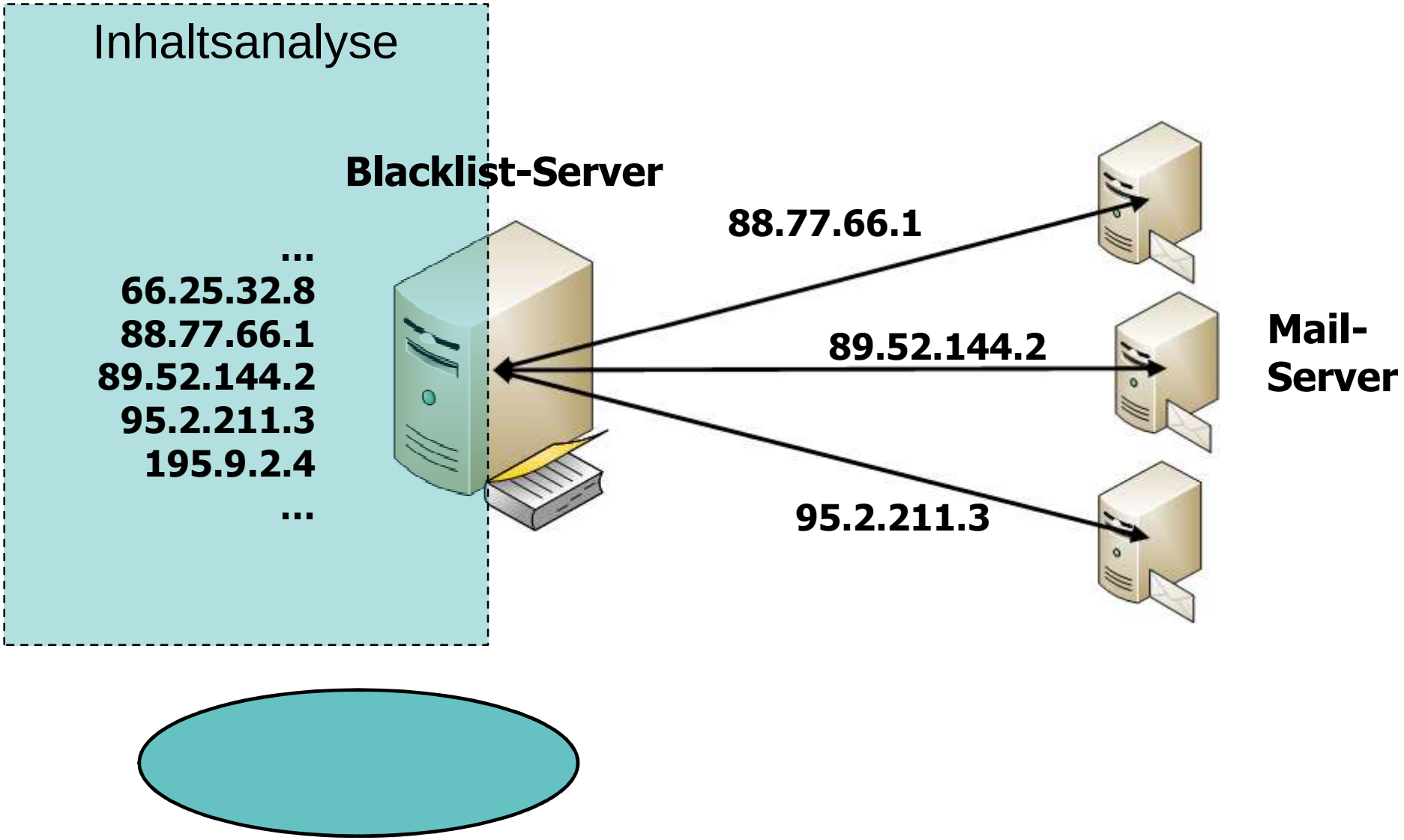
Inhalts- vs. Verhaltensanalyse



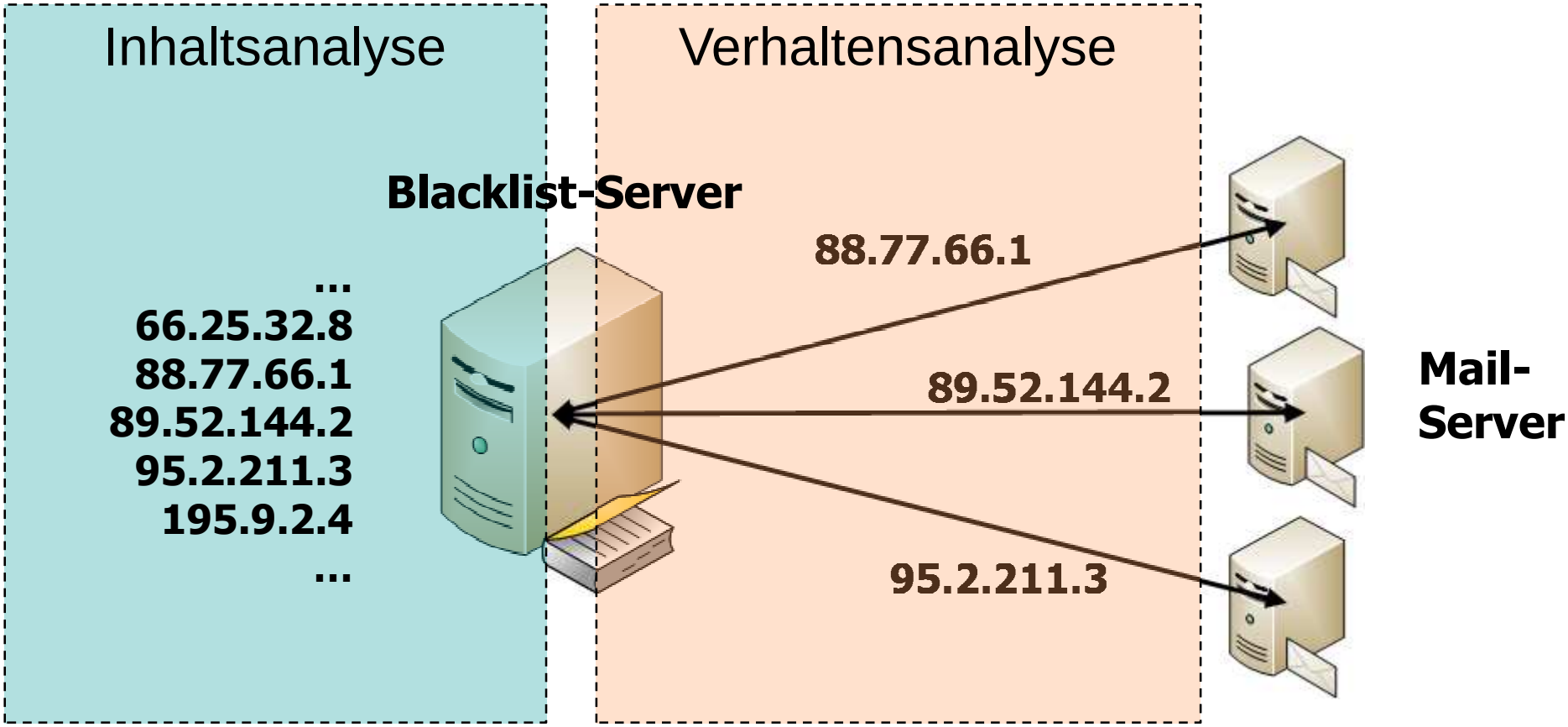
Inhalts- vs. Verhaltensanalyse

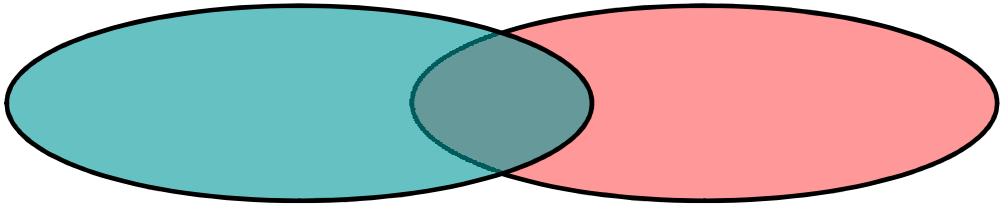


Inhalts- vs. Verhaltensanalyse



Inhalts- vs. Verhaltensanalyse





Top 15 Autonome Systeme auf der NiX Spam BL

Rang	AS ID	AS Name	Einträge	% v. ges.
#1	9121	TTNET TTnet Autonomous System	34816	0.358%
#2	4134	CHINANET-BACKBONE No.31,Jin-rong Street	15262	0.024%
#3	5617	TPNET Polish Telecom's commercial IP network	13571	0.342%
#4	3269	ASN-IBSNAZ TELECOM ITALIA	13457	0.102%
#5	6147	Telefonica del Peru S.A.A.	12941	0.930%
#6	4837	CHINA169-BACKBONE CNCGROUP China169 Backbone	12634	0.055%
#7	22927	Telefonica de Argentina	9596	1.054%
#8	7738	Telecomunicacoes da Bahia S.A.	8190	0.131%
#9	4766	KIXS-AS-KR Korea Telecom	7708	0.031%
#10	19262	VZGNI-TRANSIT - Verizon Internet Services Inc.	7704	0.052%
#11	8359	COMSTAR COMSTAR-Direct Moscow region network	6734	0.945%
#12	7418	Terra Networks Chile S.A.	6390	1.040%
#13	8167	TELESC - Telecomunicacoes de Santa Catarina SA	5963	0.266%
#14	3320	DTAG Deutsche Telekom AG	5873	0.020%
#15	27699	TELECOMUNICACOES DE SAO PAULO S/A - TELESP	5356	0.187%

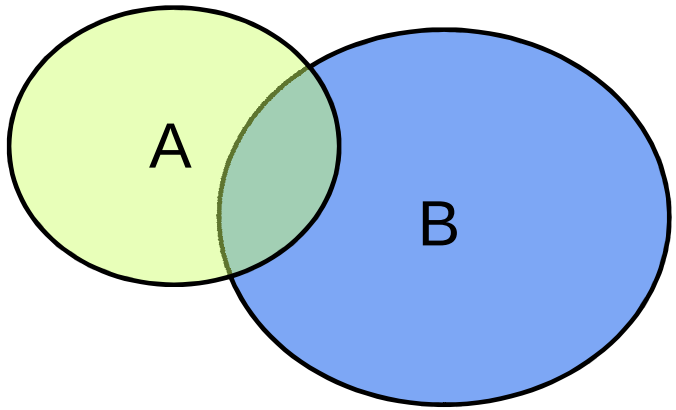
Top 15 Länder auf der NiX Spam BL

Land	IP-Adr.	% v. ges.
RUSSIAN FEDERATION	38343	0.223%
CHINA	35794	0.026%
TURKEY	34979	0.415%
UNITED STATES	33581	0.001%
BRAZIL	26002	0.111%
POLAND	20660	0.169%
COLOMBIA	17952	0.579%
GERMANY	17878	0.025%
ITALY	16668	0.069%
SPAIN	16285	0.079%
ARGENTINA	15801	0.304%
UNITED KINGDOM	15076	0.010%
KOREA, REPUBLIC OF	15011	0.025%
INDIA	14033	0.101%
PERU	13201	1.053%

Überschneidungen zwischen Blacklists

- Blacklists ähneln sich
  - Spammer triggern mehrere Sensoren (z.B. Spamtraps)
  - Datenaustausch zwischen Blacklists
  - Gleiche Datenquellen

- Überschneidungsanalyse
  - Wie groß ist die Schnittmenge zwischen zwei Blacklists?
  - Was kann daraus gefolgert werden?



Überschneidungsmatrix

reference \ comparison	all.dnsbl.sorbs.net	UCEPROTECT L1	NiX Spam	sbl.spamhaus.org	dnsbl.njabl.org	dul.sorbs.net	CBL	pbl.spamhaus.org	xbl.spamhaus.org	dsbl.org	ubl.lashback.com	dnswl.org	Bogus ranges
all.dnsbl.sorbs.net	--	0.18	0.07	0.08	0.87	99.09	0.77	78.03	0.75	2.73	0.33	4.852	0.00
UCEPROTECT L1	47.16	--	18.54	0.14	2.72	44.84	75.01	79.99	16.66	11.59	27.01	0.000	0.00
NiX Spam	43.94	45.61	--	0.10	2.24	40.18	71.70	73.37	19.14	7.64	32.99	0.001	0.00
sbl.spamhaus.org	19.31	0.12	0.04	--	1.20	3.54	1.04	7.01	0.98	2.26	0.13	0.000	0.00
dnsbl.njabl.org	57.76	0.70	0.23	0.34	--	56.47	3.78	71.77	6.70	82.49	0.95	0.000	4.42
dul.sorbs.net	100.0	0.18	0.06	0.02	0.86	--	0.75	78.61	0.72	2.72	0.31	4.457	0.00
CBL	41.73	15.77	6.13	0.24	3.09	40.26	--	83.22	15.53	9.80	15.52	0.000	3.61
pbl.spamhaus.org	58.24	0.23	0.09	0.02	0.81	58.14	1.15	--	1.08	2.44	0.40	3.246	2.75
xbl.spamhaus.org	44.97	3.89	1.82	0.25	6.07	42.63	17.24	86.18	--	11.94	4.62	0.000	8.01
dsbl.org	61.18	1.01	0.27	0.22	28.04	60.61	4.08	73.41	4.48	--	1.25	0.000	0.00
ubl.lashback.com	52.80	16.94	8.41	0.09	2.31	49.03	46.32	85.75	12.42	8.96	--	0.003	5.38
dnswl.org	0.024	0.001	0.001	0.000	0.005	0.022	0.003	0.002	0.004	0.010	0.011	--	0.000
Bogus ranges	0.00	0.00	0.00	0.00	1.57	0.00	1.57	8.62	3.13	0.00	7.83	0.000	--

Überschneidungsmatrix: NiX Spam

reference \ comparison	all.dnsbl.sorbs.net	UCEPROTECT L1	NiX Spam	sbl.spamhaus.org	dnsbl.njabl.org	dul.sorbs.net	CBL	pbl.spamhaus.org	xbl.spamhaus.org	dsbl.org	ubl.lashback.com	dnswl.org	Bogus ranges
all.dnsbl.sorbs.net	--	0.18	0.07	0.08	0.87	99.09	0.77	78.03	0.75	2.73	0.33	4.852	0.00
UCEPROTECT L1	47.16	--	18.54	0.14	2.72	44.84	75.01	79.99	16.66	11.59	27.01	0.000	0.00
NiX Spam	43.94	45.61	--	0.10	2.24	40.18	71.70	73.37	19.14	7.64	32.99	0.001	0.00
sbl.spamhaus.org	19.31	0.12	0.04	--	1.20	3.54	1.04	7.01	0.98	2.26	0.13	0.000	0.00
dnsbl.njabl.org	57.76	0.70	0.23	0.34	--	56.47	3.78	71.77	6.70	82.49	0.95	0.000	4.42
dul.sorbs.net	100.0	0.18	0.06	0.02	0.86	--	0.75	78.61	0.72	2.72	0.31	4.457	0.00
CBL	41.73	15.77	6.13	0.24	3.09	40.26	--	83.22	15.53	9.80	15.52	0.000	3.61
pbl.spamhaus.org	58.24	0.23	0.09	0.02	0.81	58.14	1.15	--	1.08	2.44	0.40	3.246	2.75
xbl.spamhaus.org	44.97	3.89	1.82	0.25	6.07	42.63	17.24	86.18	--	11.94	4.62	0.000	8.01
dsbl.org	61.18	1.01	0.27	0.22	28.04	60.61	4.08	73.41	4.48	--	1.25	0.000	0.00
ubl.lashback.com	52.80	16.94	8.41	0.09	2.31	49.03	46.32	85.75	12.42	8.96	--	0.003	5.38
dnswl.org	0.024	0.001	0.001	0.000	0.005	0.022	0.003	0.002	0.004	0.010	0.011	--	0.000
Bogus ranges	0.00	0.00	0.00	0.00	1.57	0.00	1.57	8.62	3.13	0.00	7.83	0.000	--

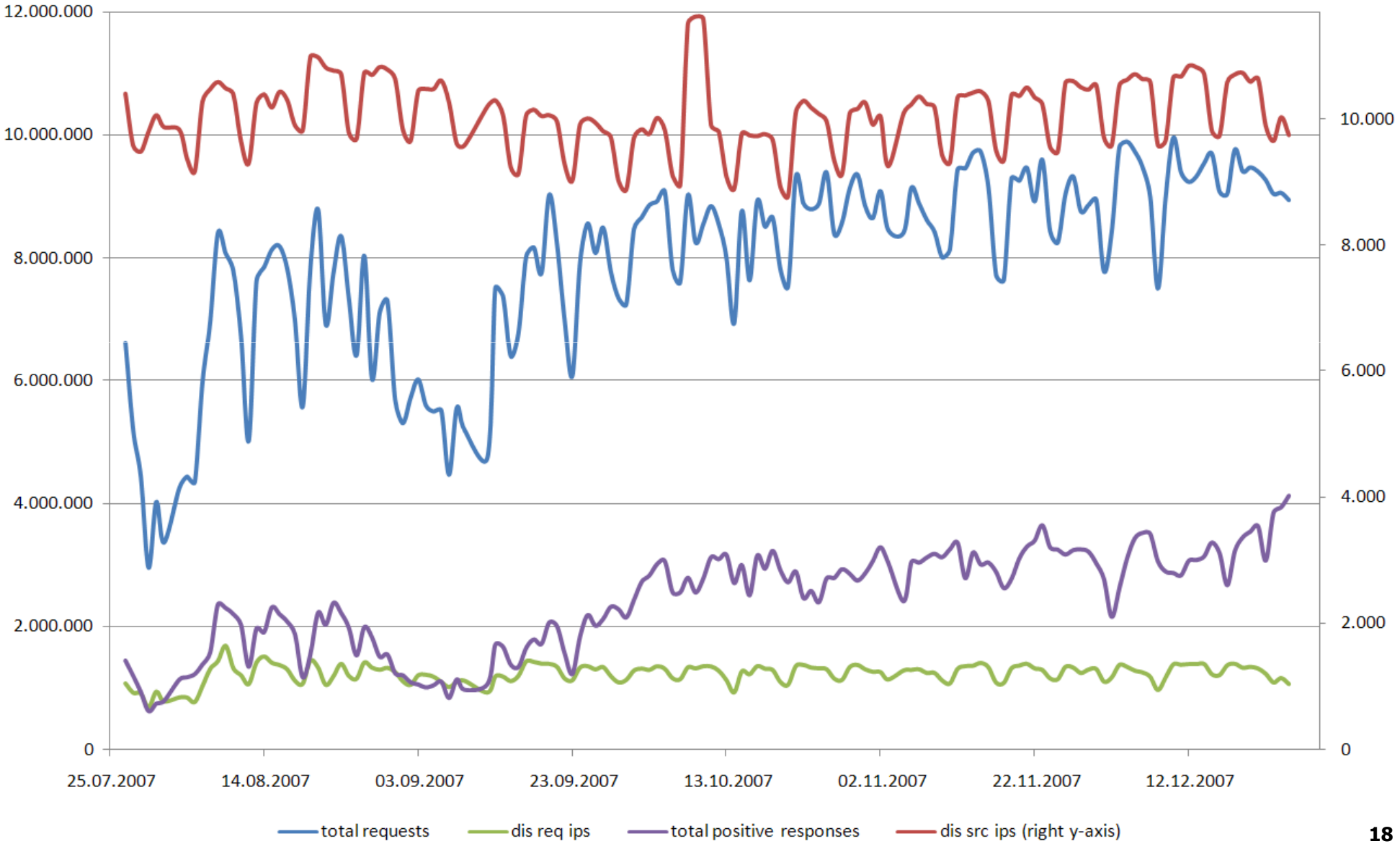
Überschneidungsmatrix: dnswl.org

reference \ comparison	all.dnsbl.sorbs.net	UCEPROTECT L1	NiX Spam	sbl.spamhaus.org	dnsbl.njabl.org	dul.sorbs.net	CBL	pbl.spamhaus.org	xbl.spamhaus.org	dsbl.org	ubl.lashback.com	dnswl.org	Bogus ranges
all.dnsbl.sorbs.net	--	0.18	0.07	0.08	0.87	99.09	0.77	78.03	0.75	2.73	0.33	4.852	0.00
UCEPROTECT L1	47.16	--	18.54	0.14	2.72	44.84	75.01	79.99	16.66	11.59	27.01	0.000	0.00
NiX Spam	43.94	45.61	--	0.10	2.24	40.18	71.70	73.37	19.14	7.64	32.99	0.001	0.00
sbl.spamhaus.org	19.31	0.12	0.04	--	1.20	3.54	1.04	7.01	0.98	2.26	0.13	0.000	0.00
dnsbl.njabl.org	57.76	0.70	0.23	0.34	--	56.47	3.78	71.77	6.70	82.49	0.95	0.000	4.42
dul.sorbs.net	100.0	0.18	0.06	0.02	0.86	--	0.75	78.61	0.72	2.72	0.31	4.457	0.00
CBL	41.73	15.77	6.13	0.24	3.09	40.26	--	83.22	15.53	9.80	15.52	0.000	3.61
pbl.spamhaus.org	58.24	0.23	0.09	0.02	0.81	58.14	1.15	--	1.08	2.44	0.40	3.246	2.75
xbl.spamhaus.org	44.97	3.89	1.82	0.25	6.07	42.63	17.24	86.18	--	11.94	4.62	0.000	8.01
dsbl.org	61.18	1.01	0.27	0.22	28.04	60.61	4.08	73.41	4.48	--	1.25	0.000	0.00
ubl.lashback.com	52.80	16.94	8.41	0.09	2.31	49.03	46.32	85.75	12.42	8.96	--	0.003	5.38
dnswl.org	0.024	0.001	0.001	0.000	0.005	0.022	0.003	0.002	0.004	0.010	0.011	--	0.000
Bogus ranges	0.00	0.00	0.00	0.00	1.57	0.00	1.57	8.62	3.13	0.00	7.83	0.000	--

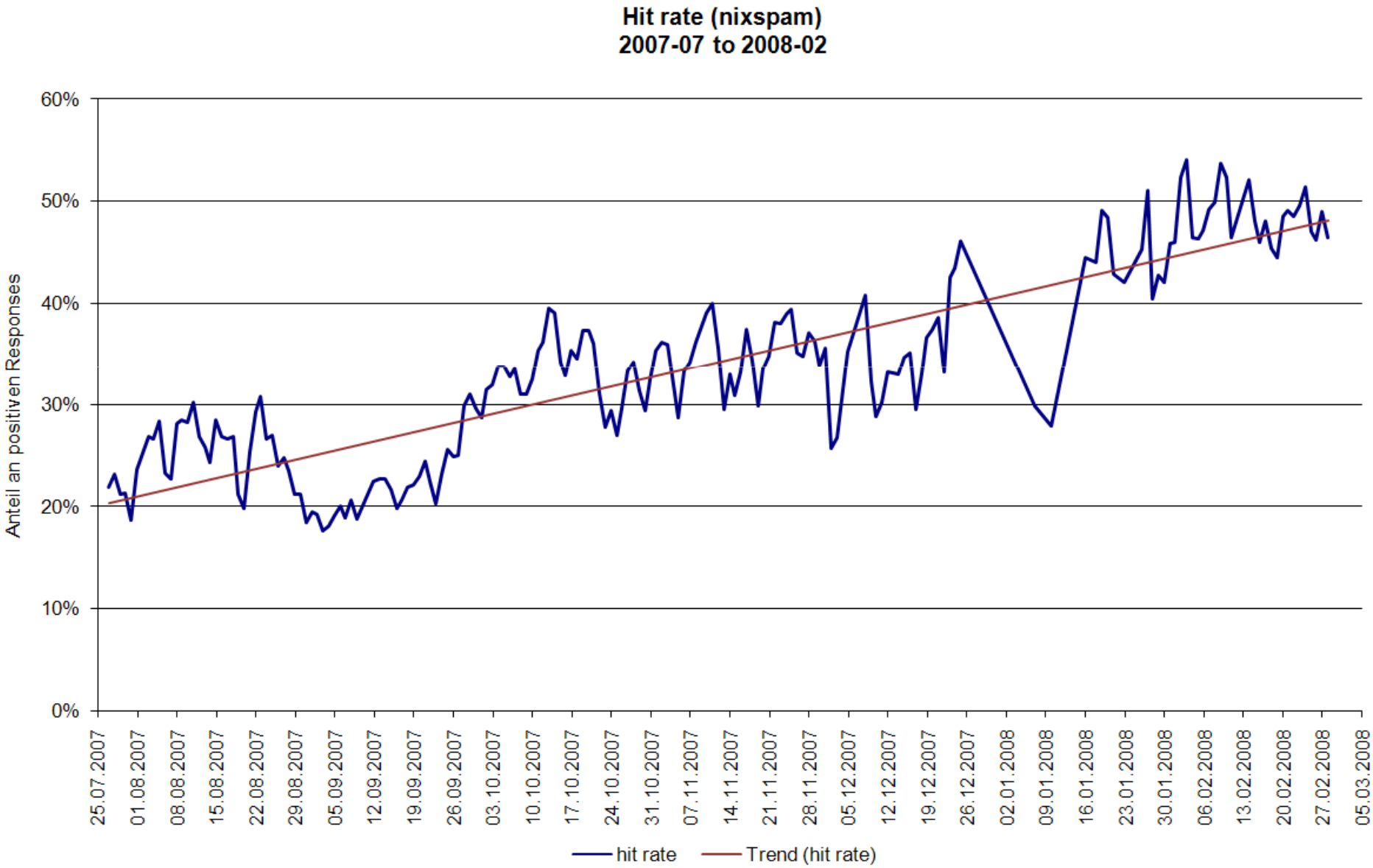
Überschneidungsmatrix: Spamhaus PBL

reference \ comparison	all.dnsbl.sorbs.net	UCEPROTECT L1	NiX Spam	sbl.spamhaus.org	dnsbl.njabl.org	dul.sorbs.net	CBL	pbl.spamhaus.org	xbl.spamhaus.org	dsbl.org	ubl.lashback.com	dnswl.org	Bogus ranges
all.dnsbl.sorbs.net	--	0.18	0.07	0.08	0.87	99.09	0.77	78.03	0.75	2.73	0.33	4.852	0.00
UCEPROTECT L1	47.16	--	18.54	0.14	2.72	44.84	75.01	79.99	16.66	11.59	27.01	0.000	0.00
NiX Spam	43.94	45.61	--	0.10	2.24	40.18	71.70	73.37	19.14	7.64	32.99	0.001	0.00
sbl.spamhaus.org	19.31	0.12	0.04	--	1.20	3.54	1.04	7.01	0.98	2.26	0.13	0.000	0.00
dnsbl.njabl.org	57.76	0.70	0.23	0.34	--	56.47	3.78	71.77	6.70	82.49	0.95	0.000	4.42
dul.sorbs.net	100.0	0.18	0.06	0.02	0.86	--	0.75	78.61	0.72	2.72	0.31	4.457	0.00
CBL	41.73	15.77	6.13	0.24	3.09	40.26	--	83.22	15.53	9.80	15.52	0.000	3.61
pbl.spamhaus.org	58.24	0.23	0.09	0.02	0.81	58.14	1.15	--	1.08	2.44	0.40	3.246	2.75
xbl.spamhaus.org	44.97	3.89	1.82	0.25	6.07	42.63	17.24	86.18	--	11.94	4.62	0.000	8.01
dsbl.org	61.18	1.01	0.27	0.22	28.04	60.61	4.08	73.41	4.48	--	1.25	0.000	0.00
ubl.lashback.com	52.80	16.94	8.41	0.09	2.31	49.03	46.32	85.75	12.42	8.96	--	0.003	5.38
dnswl.org	0.024	0.001	0.001	0.000	0.005	0.022	0.003	0.002	0.004	0.010	0.011	--	0.000
Bogus ranges	0.00	0.00	0.00	0.00	1.57	0.00	1.57	8.62	3.13	0.00	7.83	0.000	--

Kennwerte (2007/07 – 2007/12)



Hit rate (Trefferquote) 2007/07 – 2008/02



Fazit

- Je höher die Abfragehäufigkeit einer IP-Adresse, desto eher Spam (mit entscheidenden Ausnahmen)!
- Blacklisten überschneiden sich
  - Überschneidungsmatrix liefert Hinweise
- 36% der IP-Adressen sind nur sehr kurz aktiv (weniger als eine Minute)
- 33% aller IP-Adressen tauchen nur ein einziges Mal auf
- Deutschland ist größter Nutzer der NiX Spam (regionale Ausrichtung)

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

Besuchen Sie uns: Halle 9, C16

Christian J Dietrich
dietrich [at] internet-sicherheit . de

Christian Rossow
rossow [at] internet-sicherheit . de

Institut für Internet-Sicherheit
https://www.internet-sicherheit.de
Fachhochschule Gelsenkirchen