Reputation und Threat Information als Ergänzung zu Blacklists

Jannis Ohms[1] · Ina Schiering[2] · Philipp Wentscher[2]
Roland Kaltefleiter[3]

[1]Ostfalia HaW
Institut für Kommunikationssysteme und Technologien
jannis.ohms2@ostfalia.de

[2]Ostfalia HaW
Institut für Information Engineering
{i.schiering | p-th.wentscher}@ostfalia.de

[3]NetUSE AG
rk@netuse.de

Zusammenfassung

Durch die einfache Zugänglichkeit und effiziente Nutzung sind Blacklists ein wichtiger Bestandteil des IT-Sicherheitsmanagements von Organisationen. Sicherheits-Bewertungen von Domains oder IP Adressen stehen aber auch aus anderen Quellen zur Verfügung. In diesem Beitrag werden dabei Threat Intelligence Management Plattformen, die Zugriff auf aggregierte Informationen ermöglichen, am Beispiel X-Force und kollaborative Web Reputation Systeme am Beispiel Web of Trust (WOT) untersucht. Als Beispiele für Blacklists wird eine Auswahl von Blacklists aus dem Intel Marketplace von Critical Stack betrachtet. Diese Quellen für Informationen zu Sicherheits-Risiken, die mit einer Domain verknüpft sind, werden im Rahmen einer Fallstudie basierend auf Domain Name Service (DNS) Anfragen eines mittelständischen Internet Service Providers evaluiert.

1 Einleitung

Blacklists sind eine wichtige Basis-Komponente im IT-Sicherheitsmanagement von Organisationen. Sie können zentral eingesetzt werden, um DNS-Anfragen oder Web-Requests zu bewerten. Dabei sind Sie besonders ressourcenschonend und liefern eine einfache Möglichkeit des Risiko Managements auch für kleine und mittlere Unternehmen (KMU), ergänzend zu typischen Schutzmaßnahmen wie z.B. Firewalls und Anti-Viren Software, etc. (siehe [BMWI12] zu typischerweise umgesetzten Sicherheitsmaßnahmen von KMUs).

Gemäß des Infoblox DNS Threat Index [Inf16] wird weiterhin der Domain Name Service (DNS) stark als Basis für Angriffe genutzt. Da nach einem erfolgreichen Angriff gemäß einer Darstellung von Trustwave [Trus15] der Median bis zur Entdeckung einer Infektion in Organisationen bei ca. 86 Tagen liegt, ist es wichtig zu untersuchen, welche Daten-Quellen zur Bewertung der Reputation von Domains und Websites im Rahmen des Risiko Managements

P. Schartner (Hrsg.) · D•A•CH Security 2016 · syssec (2016) 87-97.

genutzt werden können. Das Ziel dabei ist es Hinweise auf Infektionen zu erhalten, die ressourcenschonend genutzt werden können.

Sicherheits-Bewertungen von Domains im DNS werden hauptsächlich in Form von *Blacklists* bereit gestellt. Beispiele für öffentliche, frei zugängliche Blacklists sind z.B. die Informationen über das Zeus-Botnetz [Zeus] oder aus dem Open Source Intrusion Detection System Snort [Snor]. Daneben existieren kommerzielle Services z.B. von Herstellern von Anti-Virus Software, wie McAfee SiteAdvisor oder Norton Safe Web. Als Basis für die Untersuchung wurde eine Auswahl von Blacklists aus dem Intel Marketplace von Critical Stack [cri] betrachtet.

Andere Formen der Sicherheits-Bewertung werden durch *Threat Intelligence Management Plattformen* realisiert, die Zugriff auf aggregierte Informationen über Vorfälle, wie z.B. die Nutzung als Command & Control Server in Bot-Netzen ermöglichen [BrGS15], [Kamp14]. Von dieser Gruppe von Plattformen wird beispielhaft X-Force [XFor] untersucht. Diese Systeme sind insbesondere interessant, da sie einen Datenaustausch auf Basis von Standards wie STIX, TAXII [enis14] ermöglichen. Damit ermöglichen Sie die kooperative Bereitstellung von Informationen über Sicherheitsvorfälle.

Als weiterer Ansatz werden *kollaborative Web Reputation Systeme* untersucht [AyJe11], [ChCh12], [LNAW+15]. In diesen Systemen wird auf Basis von Community Ratings die Vertrauenswürdigkeit bewertet und dazu die Sicherheit dieser Einschätzung angegeben. Zu dieser Gruppe von Services wird als Beispiel Web of Trust (WOT) [wot] betrachtet.

In Form einer Fallstudie wird untersucht, inwieweit diese ergänzenden Datenquellen sinnvoll für die Sicherheits-Bewertung in Organisationen im Rahmen des Risiko Managements genutzt werden können. Diese Fallstudie basiert auf DNS-Anfragen eines mittelständischen Internet Service Providers (ISP) aus Deutschland und einer Auswahl an Blacklists aus dem Intel Marketplace von Critical Stack. Um die Datensätze einzuordnen, wird die Alexa Top 500.000 Liste [Alex] verwendet. Dabei werden die folgenden Aspekte untersucht:

- *Datensätze*: Domains aus DNS-Anfragen eines ISP, Domains der Alexa Top 500.000 Liste, Zusammenstellung von Blacklists
- *Ergänzende Daten-Quellen*: die Services WOT, X-Force
- *Abdeckung von WOT, X-Force* bezogen auf die Datensätze
- *Vergleich der Bewertungen* von WOT und X-Force für die gewählten Datensätze

Diese Arbeit ist wie folgt organisiert: Nach der Übersicht bekannter Ergebnisse für die Datenquellen Blacklists, Threat Intelligence Management Plattformen und kollaborative Web Reputation Systeme in Abschnitt 2 wird die Methodik der Fallstudie in Abschnitt 3 vorgestellt. Es folgt die Zusammenstellung der Ergebnisse der Analyse in Abschnitt 4 und in Abschnitt 5 eine kritische Betrachtung und Einordnung.

2 Related Work

In bisher bekannten Arbeiten wurden die drei Arten von Informationsquellen, Blacklists, kollaborative Web-Reputationsdienste und Threat Intelligence Management Plattformen im wesentlichen getrennt untersucht.

Zur Bewertung von Blacklists wurden Untersuchungen von Metcalf et al. [MeSp14] durchgeführt, die festgestellt haben, dass erst die Kombination verschiedener Blacklists eine sinnvol-

le Abdeckung darstellt. Kührer et al. [KüRH14] haben untersucht, in welchen Zeitintervallen Updates erfolgen. Sie geben an, dass es im Mittel ca. 30 Tage dauert, bis eine Domain, die erstmalig aufgefallen ist, in Blacklists aufgenommen wird. Dabei bestehen jedoch große Unterschiede zwischen verschiedenen Anbietern.

Dietrich et al. [DiRo09] untersuchten die Nutzung von Blacklists im Kontext von Spam-Mails. Daneben werden Blacklists als Basis-Information eingesetzt, um bei Systemen, die eine Bewertung basierend auf überwachtem maschinellen Lernen durchführen, ein Labelling der Trainingsdaten vorzunehmen. Beispiele für solche Systeme sind NOTOS [APDL+10], EXPOSURE [BSBK+14], oder neuere Ansätze zur Ergänzung von Blacklists von Stevanovic et al. [SPDR+15] beim Labelling von Daten.

Die Bedeutung von *Threat Intelligence Management Plattformen*, Standards zur Kooperation und die Notwendigkeit eines Informationsaustauschs wurden von Kampanakis [Kamp14] und Dandurand, Serrano [DaSe13] dargestellt. Brown et al. [BrGS15] haben die aktuellen Herausforderungen im Bereich des Threat Managements untersucht.

Kollaborative *Web Reputation Systeme* sind typischerweise in Communities entstanden. Ein wichtiger Vertreter dabei ist der Service WOT [wot], [AlTo12]. Die Benutzer und Strukturen solcher Communities wurden von Chia und Chuang [ChCh12] untersucht. Von Liu et al. [LNAW+15] wird die Weiterentwicklung zu einem personalisierten Web Content Recommendation Model diskutiert.

Ein Vergleich zwischen WOT und dem McAfee SiteAdvisor aus Nutzersicht von Ayyavu und Jensen [AyJe11] stellt einen der wenigen Vergleiche zwischen den beiden Gruppen von Systemen dar. Dabei werden die beiden Datenquellen in Form von Plugins für Web-Browser betrachtet, während in der vorliegenden Arbeit die Betrachtung der zugrundeliegenden Daten für die Risiko-Bewertung im Unternehmen im Fokus steht.

3 Methodik der Fallstudie

Die vorliegende Fallstudie basiert auf DNS-Daten, die bei einem mittelständischen ISP aus Deutschland aufgezeichnet wurden. Dabei handelt es sich um DNS Anfragen des ISP selbst und Anfragen einer größeren Anzahl von Kunden, die im wesentlichen der Gruppe der KMUs zuzuordnen sind. Die Daten wurden anonymisiert, indem alle Informationen zu den anfragenden Clients entfernt wurden. Über einen Zeitraum von 3 Tagen wurden im November 2015 ca. 51 Millionen DNS-Pakete aufgezeichnet.

Als Domain wird typischerweise die Second-Level Domain betrachtet, im Falle von z.B. Content Delivery Networks oder Top-Level Domains wie *co.uk* die Third-Level Domain. Die daraus resultierenden Domain-Namen werden als *Relevant Level Domain (RLD)* bezeichnet.

Der betrachtete Datensatz enthält eine große Anzahl von Anfragen, die einem Domain Generation Algorithm (DGA) zugeordnet werden können. Diese werden herausgefiltert, da sie weder in der Blacklist noch in WOT oder X-Force enthalten sind. In dem Datensatz sind 173.762 verschiedene RLDs enthalten. Nach dem Herausfiltern der DGA-Domains besteht der resultierende Datensatz aus 60.832 verschiedenen RLDs (siehe Datensatz *ISP* in Tabelle 1).

Der Datensatz *Critical Stack* ist eine aus mehreren Quellen zusammengestellte Blacklist aus dem Intel Marketplace von Critical Stack [cri]. Die Alexa Top 500.000 [Alex] ist eine Zu-

sammenstellung der weltweit am häufigsten verwendeten Domains und wird hier als Datensatz *Alexa 500* betrachtet. Beide Datensätze wurden ebenfalls im November 2015 erhoben.

Tab. 1: Datensätze der Fallstudie

Datensatz	Beschreibung	Größe
ISP	DNS eines mittelständischen ISP	60.832
Alexa 500	Alexa Top 500.000	500.000
Critical Stack	Critical Stack Blacklist https://www.binarydefense.com https://snort.org http://www.us.openbl.org https://greensnow.co http://www.chaosreigns.com/iprep http://emergingthreats.net http://autoshun.org http://danger.rulez.sk/index.php/bruteforceblocker https://www.badips.com http://dragonresearchgroup.org/insight http://www.bambenekconsulting.com https://zeustracker.abuse.ch https://www.packetmail.net http://malc0de.com/database https://www.damballa.com https://sslbl.abuse.ch/blacklist https://virbl.bit.nl https://securelist.com https://palevotracker.abuse.ch http://security-research.dyndns.org	ca. 600.000

Für eine erste Einordnung der Daten wird in Tabelle 2 die Verteilung der Datensätze in Bezug auf Top-Level Domains untersucht. Im *ISP*-Datensatz sind deutsche bzw. deutschsprachige Domains deutlich stärker vertreten, als in allen anderen Datensätzen. Besonders die Daten aus *Critical Stack* haben einen deutlichen Schwerpunkt bei den *.com* Domains. Damit scheinen Aspekte wie eine Vielfalt von Ländern und Sprachen, wie sie in Europa wichtig sind, derzeit in den hier betrachteten Blacklists nicht angemessen abgebildet zu werden.

Tab. 2: TLD Verteilung der Datensätze

Kategorie	ISP	Critical Stack	Alexa 500
Amerika	0,75%	0,56%	3,51%
Asien	0,58%	5,53%	10,05%
Australien, Ozeanien	0,16%	2,07%	1,31%
COM	75,57%	75,23%	41,20%
DACH	13,97%	0,30%	2,43%
Deutschland	13,52%	0,25%	2,00%
Europa	15,78%	2,06%	12,16%
Öffentlich	3,99%	12,90%	9,11%
Sonstiges	3,15%	1,65%	22,67%

Für die Domains aus diesen drei Datensätzen wurden Anfragen bei den Services WOT [wot] und X-Force [XFor] gestellt. X-Force ordnet jeder Domain einen Wert zwischen 0 und 10 zu. Dabei handelt es sich um das Risiko, mit dem die Domain behaftet ist, auf Basis von aufgezeichneten Vorfällen. Ein hoher Wert entspricht einem hohen Risiko. Ein Wert von 0 bedeutet, dass zu der Domain noch keine Informationen vorliegen.

WOT dagegen liefert für jede Domain einen Wert zwischen 0 und 100, der die Reputation der Domain angibt. Anders als bei X-Force, bei dem ein hoher Wert ein hohes Risiko angibt, bedeutet hier ein hoher Wert eine hohe Reputation. Um die Ergebnisse leichter vergleichen zu können, werden die Reputationswerte von WOT in Intervallen zusammengefasst und so umgestellt, dass vergleichbar zu X-FORCE der Wert 0 ein geringes Risiko und der Wert 9 ein sehr hohes Risiko darstellt. Im weiteren werden die so normalisierten Daten betrachtet.

4 Ergebnisse der Fallstudie

Auf Basis der erhobenen Daten wird untersucht, welcher Anteil der Datensätze überhaupt Bewertungen in WOT, bzw. X-Force besitzt. Für die Datensätze, die eine Bewertung besitzen, wird die Verteilung der Bewertungen für die drei Datensätze untersucht und geprüft, inwieweit die Bewertungen für diese Datensätze übereinstimmen.

Auf Basis der oben dokumentierten Datensätze bestehend aus RLDs wird zunächst in Abbildung 1 untersucht, welcher Anteil der drei Datensätze Bewertungen in WOT, bzw. X-Force besitzt.

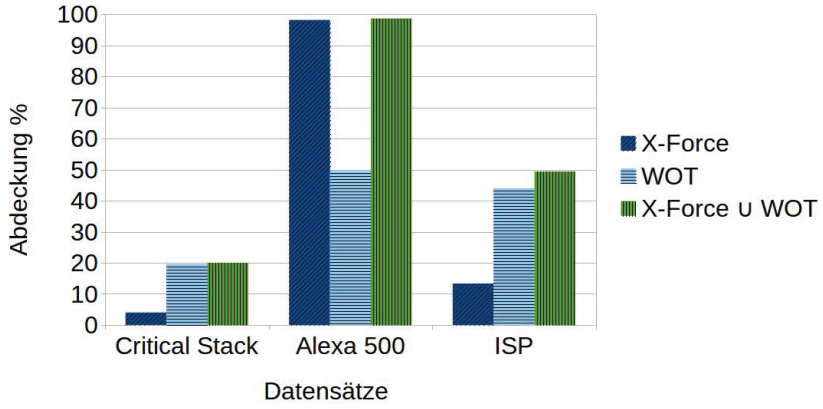

Abb. 1: Abdeckung der RLDs aus den Datensätzen durch X-Force, WOT

Dabei wird deutlich, dass sowohl WOT, als auch X-FORCE einen deutlichen Fokus bei den weltweit häufig angefragten RLDs aus der *Alexa 500* haben. Eher aus globaler Sicht selten angefragte Domains, wie Domains der *Critical Stack* Blacklists oder z.B. Domains aus dem *ISP* Datensatz, die einen eher regionalen Bezug haben, wie lokale Zeitungen, Vereine oder Sportinformationen, wurden weitgehend nicht abgedeckt.

Die geringe Abdeckung des *Critical Stack* Datensatzes war zu erwarten, da ein großer Teil dieser Domains nicht erreichbar ist. Sie wurden z.B. in der Vergangenheit kurz für illegale Aktivitäten verwendet. Die Abdeckung von WOT ist in allen Fällen größer, da der Service WOT bereits länger existiert und das Ziel darin besteht, generell die Reputation von Websites aus Nutzer-Sicht herauszustellen. Durch den Community-Ansatz und die Datenbasis, die hauptsächlich auf der Sammlung von Vorfällen beruht, ist zu erwarten, dass die Abdeckung von

X-Force wachsen wird. Hier stehen jedoch sicherheitskritische Vorfälle im Fokus, anders als bei WOT, wo auch die gute Reputation einer Site dokumentiert wird.

Tab. 3: TLD Verteilung der WoT, X-Force Abdeckung der Datensätze

Kategorie	ISP WoT	Critical Stack WoT	Alexa 500 WoT
Amerika	2,00%	1,97%	4,79%
Asien	1,67%	2,80%	8,19%
Australien, Ozeanien	0,46%	0,89%	0,72%
COM	35,56%	35,02%	54,61%
DACH	34,82%	1,30%	3,05%
Deutschland	33,57%	1,01%	2,53%
Europa	39,93%	3,76%	12,91%
Öffentlich	10,46%	7,95%	12,90%
Sonstiges	9,92%	47,61%	5,87%
Kategorie	ISP X-Force	Critical Stack X-Force	Alexa 500 X-Force
Amerika	1,69%	1,01%	4,82%
Asien	1,89%	3,67%	7,89%
Australien, Ozeanien	0,46%	2,06%	0,70%
COM	36,83%	34,28%	50,87%
DACH	40,52%	0,42%	4,62%
Deutschland	39,03%	0,31%	3,90%
Europa	45,47%	1,85%	16,20%
Öffentlich	10,82%	7,85%	14,29%
Sonstiges	2,85%	49,28%	5,22%

Als ersten Schritt für die Untersuchung der durch WOT, X-Force abgedeckten RLDs wird die Verteilung der TLDs in Tabelle 3 betrachtet. Dabei fällt auf, dass besonders die Anzahl der *Sonstigen* TLDs im Datensatz Critical Stack stark wächst. Diese Kategorie beinhaltet TLDs, die keinem Land zugeordnet sind, sondern z.B. wie *tv, .mob, .me* auf spezifische Dienste ausgerichtet sind oder z.B. TLDs für Städte wie *.berlin*. Im ISP Datensatz zeigt sich, dass häufig genutzte deutsche Domains bereits breit in den beiden betrachteten Services vorhanden sind.

Im nächsten Schritt werden für die RLDs, die in WOT und X-Force eine Bewertung besitzen, die Bewertungen normalisiert, wie in Abschnitt 3 dargestellt und in Relation gesetzt. Die Ergebnisse werden für die drei Datensätze in Abbildung 2, 3 und 4 zusammengefasst, indem die Verteilungen der Bewertungen gegenüber gestellt werden.

Für die beiden Datensätze *ISP, Alexa 500* die eher normales Nutzerverhalten repräsentieren, zeigen die Verteilungen ein vergleichbares Spektrum an Bewertungen der beiden Services WOT und X-Force. Lediglich bei dem Datensatz *Critical Stack*, der aus Domains besteht, die extrem selten und meist nur für eine kurze Zeit in Verbindung mit illegalen Aktivitäten eingesetzt wurden, gehen die Häufigkeiten der Bewertungen weit auseinander.

Dazu stellt sich die Frage, wie stark die Bewertungen einzelner Domains voneinander abweichen. Nach der Gegenüberstellung der Häufigkeitsverteilungen der Bewertungen werden für RLDs, die in beiden Services eine Bewertung haben, diese Bewertungen verglichen. Dazu wird die Verteilung des Absolutbetrags der Differenz zwischen beiden Werten betrachtet. Auch diese Auswertung wird für alle drei Datensätze in Abbildung 5, 6 und 7 dargestellt.

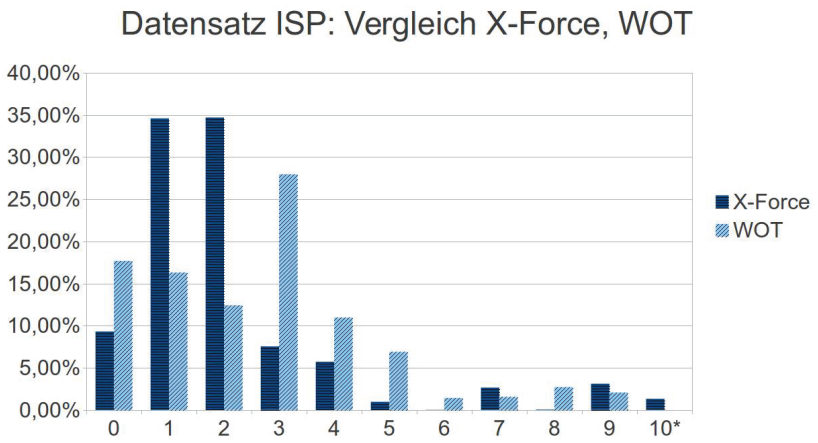

Abb. 2: Vergleich der Risikoeinschätzung des ISP Datensatzes von WoT und X-Force

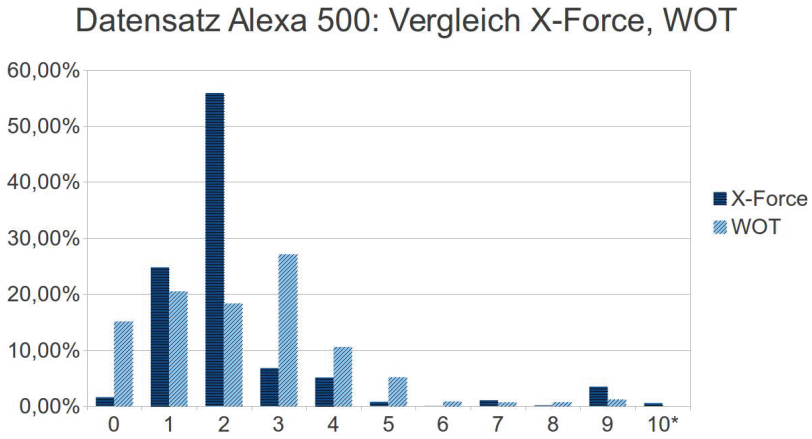

Abb. 3: Vergleich der Risikoeinschätzung des Alexa 500 Datensatzes von WoT und X-Force

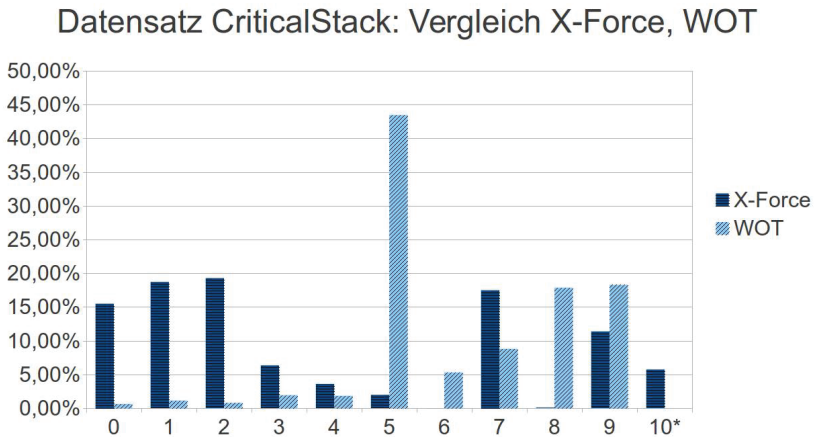

Abb. 4: Vergleich der Risikoeinschätzung des Critical Stack Datensatzes von WoT und X-Force

Diese Betrachtung unterstützt die bisherigen Ergebnisse. Die Einschätzungen der beiden Dienste WOT und X-FORCE stimmen für Domains der Datensätze *ISP* und *Alexa 500* sinnvoll überein. Bei dem *Critical Stack* Datensatz weichen die Bewertungen der beiden betrachteten Dienste für viele RLDs sehr weit voneinander ab.

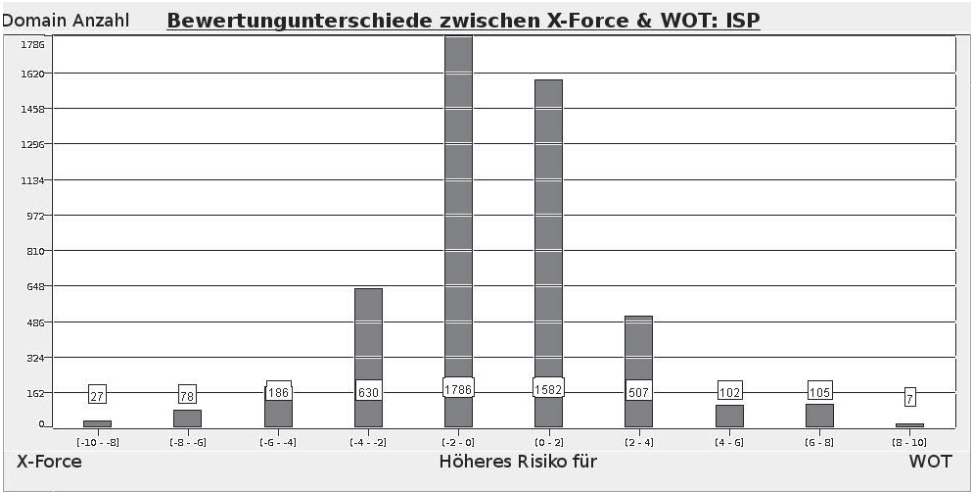

Abb. 5: Übereinstimmung der Bewertung von WOT, X-Force beim Datensatz ISP

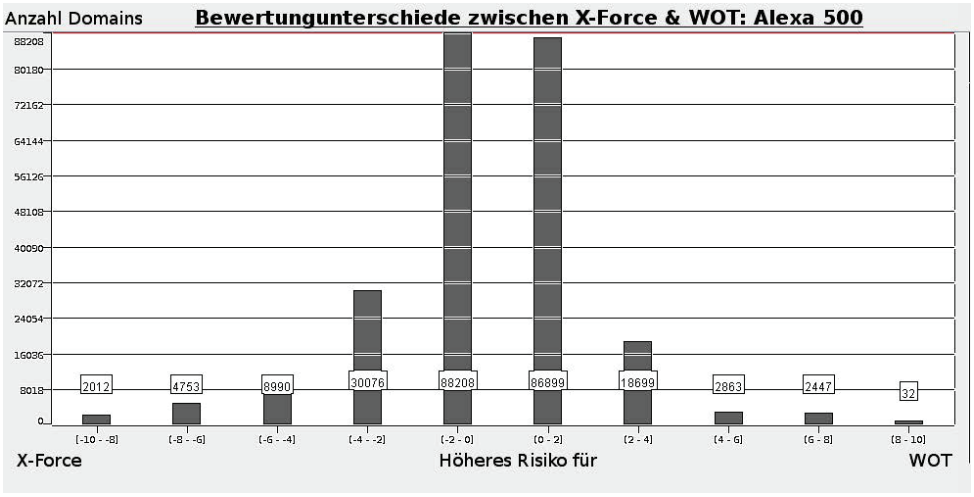

Abb. 6: Übereinstimmung der Bewertung von WOT, X-Force beim Datensatz Alexa 500

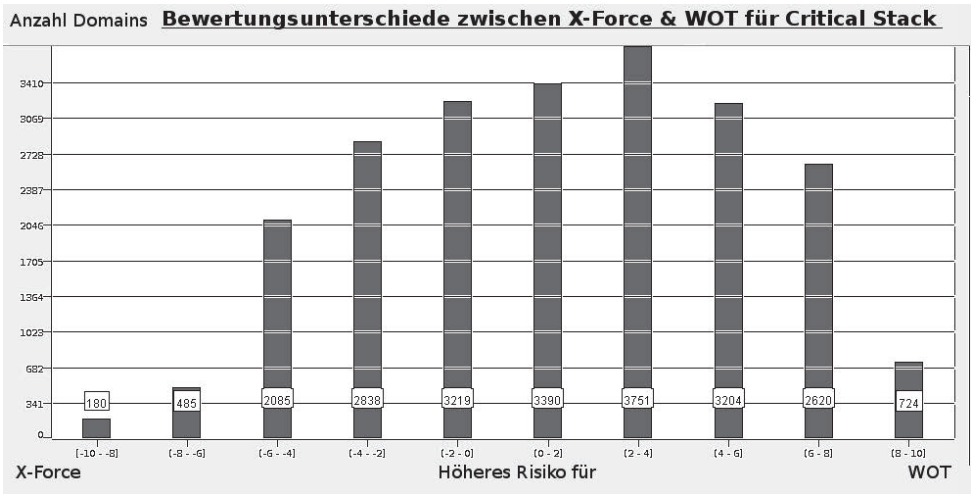

Abb. 7: Übereinstimmung der Bewertung von WOT, X-Force beim Datensatz Critical Stack

Diese Differenz lässt sich begründen durch die unterschiedlichen Ausrichtungen der Dienste WOT und X-Force. Der Fokus von WOT ist die Nutzer-Sicht auf eine Domain als Website, während X-Force die Sicht der Organisation einnimmt und ausschließlich auf Basis von Sicherheits-Vorfällen wertet. Häufig genutzte Domains wie z.B. *wetter.com* sind aus beiden Sichten unkritisch. Dagegen ist eine Domain wie *goggle.com* für Nutzer extrem ärgerlich und ist bereits durch den Versand von Spam und die Verteilung von Malware aufgefallen. Da bei X-Force nur ein konkreter Vorfall bisher hinterlegt ist, wird die Domain hier eher vorsichtig als Risiko-Level 1 bewertet, während die WOT Bewertung umgerechnet einen Risikolevel von 9 darstellt. Domains wie *raidrush.ws*, ein Nachrichtenportal, das als TLD Samoa nutzt, wird von Nutzern eher als neutral bis gut bewertet, während X-Force hier ein hohes Risiko darstellt, begründet durch Vorfälle.

5 Diskussion

Insgesamt stellen Threat Intelligence Management Plattformen und kollaborative Web Reputation Systeme interessante Quellen für Informationen dar, die im IT-Sicherheitsmanagement eines Unternehmens ressourcenschonend genutzt werden können.

Der Einsatzbereich dieser Informationen ist vergleichbar mit dem Einsatzbereich von Blacklists. D.h. mögliche Einsatzbereiche sind die Reduktion der Risiken von Phishing, infizierten Websites, Malware, ggf. auch Kommunikation mit Command & Control Servern. Damit ist der Einsatzbereich vergleichbar mit dem Einsatzbereich von Blacklists.

Zur Zeit sind Blacklists nicht transparent, d.h. es ist nicht transparent, aufgrund welcher Vorfälle eine Domain auf einer Blacklist genannt wird und wann und weshalb sie dort gelöscht wird. Auf der anderen Seite geht man davon aus, dass eine Domain auf einer Blacklist gesichert nicht vertrauenswürdig ist und deshalb z.B. automatisch geblockt werden kann. Deshalb werden Domains vor dem Eintrag sorgfältig verifiziert und zwischen einem konkreten Vorfall und der Aufnahme in eine Blacklist vergeht eine signifikante Zeitspanne (siehe Kührer et al. [KüRH14]).

Hier kann ergänzend besonders eine Threat Intelligence Management Plattform von Nutzen sein. Da dort lediglich Vorfälle gesammelt werden, kann schneller eine Information über potentielle Risiken bereit gestellt werden, als es im Rahmen einer Blacklist möglich ist. Auf der anderen Seite sollte man erst bei signifikant hohen Risiko-Bewertungen eine Domain aufgrund einer derartigen Bewertung sperren. Web Reputation Systeme haben den Fokus Nutzer vor Risiken im Web zu warnen, indem automatisiert Informationen im Browser angezeigt werden.

Beide Konzepte bieten hohes Potential durch den Ansatz mit Unterstützung einer Community transparent Informationen zu sammeln und der Community bereit zu stellen, während Blacklists meist von einzelnen Organisationen erstellt werden. Critical Stack ist hier ein Ansatz, konsolidiert Zugriff auf verschiedene Informationsquellen zu bieten. Im Laufe der Zeit ist durch wachsende Communities hier auch mit einer größeren Abdeckung zu rechnen.

Da die Anfragen einzeln online an den Betreiber gestellt werden müssen, erhalten Betreiber solcher Plattformen potentiell Informationen über Partner oder Interessensgebiete einer Organisation. Außerdem muss es zu einer Domain zunächst Vorfälle gegeben haben, bevor Threat Informationen zur Domain über die Community eingestellt werden können. Zu Domain Generation Algorithms, die breit im Rahmen der Steuerung von Bot-Netzen durch Command & Control Server genutzt werden, bestehen solche Informationen typischerweise nicht. Hier bestehen Grenzen der betrachteten Ansätze. Dabei handelt es sich um Bedrohungen, die auch durch

Blacklists derzeit nicht adäquat adressiert werden können.

Lever et al. [LWND+] weisen in einem bisher nicht veröffentlichten Artikel auf das generelle Risiko hin, dass eine Reputationsbewertung basierend auf Domain-Namen beinhaltet: Wenn eine Domain den Besitzer wechselt, bleiben Einträge in Blacklists oder Reputationsdatenbanken bestehen. Somit wird die Reputation mindestens in einer Übergangszeit vererbt, während die Domain für kriminelle Zwecke verwendet wird.

6 Zusammenfassung

Sinnvolles Risiko Management im Bereich IT Sicherheit basiert auf einem möglichst breiten Ansatz mit einer Mischung von Informationsquellen und weiteren Maßnahmen, z.B. im Bereich der Prävention.

Sowohl Threat Intelligence Management Plattformen, als auch kollaborative Web Reputation Systeme bieten wichtige ergänzende Informationen für das Risiko Management in Organisationen. Keine der hier betrachteten Quellen WOT und X-FORCE sollte allein verwendet werden, da bei beiden die Abdeckung von nationalen und regionalen Besonderheiten in der hier dargestellten Fall-Studie bisher nicht ausreichend abgebildet ist. Beide stellen jedoch interessante Zusatzinformationen dar, die im Rahmen der Risikobewertung ergänzend hilfreich sind, und bieten hohes Potential durch den zugrundeliegenden Community-Gedanken.

Danksagung
Dieses Vorhaben wird aus Mitteln des Bundesministeriums für Wirtschaft und Energie im Rahmen des Zentralen Innovationsprogramms Mittelstand (ZIM) unter den Förderkennzeichen KF2842905KM4 und KF3297501KM4 gefördert.

Literatur

[Alex] Alexa: http://www.alexa.com.

[AlTo12] T. Ala-Kleemola, S. Tolvanen: Reputation management system (2012), US Patent 8,112,515.

[APDL+10] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, N. Feamster: Building a Dynamic Reputation System for DNS. *In: USENIX security symposium* (2010), 273–290.

[AyJe11] P. Ayyavu, C. Jensen: Integrating user feedback with heuristic security and privacy management systems. *In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM (2011), 2305–2314.

[BMWI12] BMWI: Bundesministeriums für Wirtschaft und Technologie, IT-Sicherheitsniveau in kleinen und mittleren Unternehmen (2012), http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Redaktion/PDF/it-sicherheit-studie-publikation,property=pdf,bereich=itsicherheit,sprache=de,rwb=true.pdf.

[BrGS15] S. Brown, J. Gommers, O. Serrano: From cyber security information sharing to threat management. *In: Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, ACM (2015), 43–49.

[BSBK+14] L. Bilge, S. Sen, D. Balzarotti, E. Kirda, C. Kruegel: EXPOSURE: a passive DNS

analysis service to detect and report malicious domains. In: *ACM Transactions on Information and System Security (TISSEC)*, 16, 4 (2014), 14.

[ChCh12] P. H. Chia, J. Chuang: Community-based web security: complementary roles of the serious and casual contributors. *In: Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, ACM (2012), 1023–1032.

[cri] Critical Stack. https://intel.criticalstack.com/.

[DaSe13] L. Dandurand, O. S. Serrano: Towards improved cyber security information sharing. *In: Cyber Conflict (CyCon), 2013 5th International Conference on*, IEEE (2013), 1–16.

[DiRo09] C. J. Dietrich, C. Rossow: Empirical research of IP blacklists. *In: ISSE 2008 Securing Electronic Business Processes*, Springer (2009), 163–171.

[enis14] enisa: Standards and tools for exchange and processing of actionable information (2014).

[Inf16] Infoblox, Infoblox DNS threat index, Quaterly report Q4 2015 (Whitepaper) (2016), https://www.infoblox.com/dns-threat-index.

[Kamp14] P. Kampanakis: Security automation and threat information-sharing options. In: *Security & Privacy, IEEE*, 12, 5 (2014), 42–51.

[KüRH14] M. Kührer, C. Rossow, T. Holz: Paint It black: Evaluating the effectiveness of malware blacklists. *In: A. Stavrou, H. Bos, G. Portokalidis (Hrsg.), Research in Attacks, Intrusions and Defenses: 17th International Symposium, RAID 2014, Gothenburg, Sweden, September 17-19, 2014. Proceedings*, Springer International Publishing (2014), 1–21.

[LNAW+15] X. Liu, R. Nielek, P. Adamska, A. Wierzbicki, K. Aberer: Towards a highly effective and robust Web credibility evaluation system. In: *Decision Support Systems*, 79 (2015), 99–108.

[LWND+] C. Lever, R. Walls, Y. Nadji, D. Dagon, P. McDaniel, M. Antonakakis: Domain-Z: 28 Registrations later. In: , http://www.cc.gatech.edu/ ynadji3/docs/pubs/domain-z-2016.pdf.

[MeSp14] L. Metcalf, J. M. Spring: Blacklist ecosystem analysis update: 2014. In: *Software Engineering Institute, CERT Coordination Center, Pittsburgh, PA, Tech. Rep. CERTCC-2014-82* (2014).

[Snor] Snort: https://snort.org/.

[SPDR+15] M. Stevanovic, J. M. Pedersen, A. D'Alconzo, S. Ruehrup, A. Berger: On the ground truth problem of malicious DNS traffic analysis. In: *Computers & Security*, 55 (2015), 142–158.

[Trus15] Trustwave: Trustwave Global Security Report (2015).

[wot] Web of Trust. https://www.mywot.com/.

[XFor] X-Force: http://www.ibm.com/security/xforce/.

[Zeus] Zeustracker: https://zeustracker.abuse.ch/.