GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

IT-SECURITY OVERVIEW

IT-SICHERHEITSLAGEBILD ALS ENTSCHEIDUNGSUNTERSTÜTZUNG IN DEUTSCHLAND

1. MOTIVATION UND ZIEL

Die Häufigkeit von Angriffen auf IT-Systeme nimmt ständig zu, wobei sich solche Angriffe über das Internet mit vergleichsweise geringem Aufwand umsetzen lassen. Aber nicht nur die Häufigkeit von Angriffen nimmt zu, sondern auch der Aufwand, den Kriminelle und insbesondere Nachrichtendienste betreiben, um in IT-Systeme von Unternehmen und Regierungen einzudringen. Präventive Maßnahmen sind daher wichtig, um IT-Systeme abzusichern.

Ziel des Verbundprojekts „IT-Security Overview“ ist es, Fortschritte in den Gebieten Lagebilderstellung, -austausch und -korrelation zu erlangen. Ein Demonstrator zeigt die Machbarkeit der Verfahren und Probanden evaluieren die für sie ausgewählten Meldungen. Dies geschieht während der gesamten Entwicklung mit permanenter Prüfung auf Rechtskonformität.

2. DATENSAMMLUNG UND AUFBEREITUNG

Das entwickelte Werkzeug schöpft aus verschieden Quellen der *Open-Source-Intelligence*. So veröffentlichte Meldungen werden kontinuierlich gesammelt, aufbereitet und mit zusätzlichen Informationen angereichert.

Abbildung 1: Ablauf der Datensammlung und Aufbereitung.

Etwaige enthaltene personenbezogene bzw. personenbeziehbare Daten werden mithilfe von *Regulären Ausdrücken* und *Natural-Language-Processing* (NLP) erkannt und unkenntlich gemacht.

Ähnliche Meldungen können anhand von Metadaten wie Tags und Hashtags gruppiert werden. Eine statistische Beobachtung dieser Tags über längeren Zeitraum erlaubt es, einen ungewöhnlichen Anstieg in der Verwendung zu identifizieren und somit thematische Trends zu erkennen.

Des Weiteren werden Meldungen mithilfe eines hierarchisch strukturierten *Latent-Dirichlet-Allocation*-Modells (LDA) einem oder mehreren Themen zugeordnet. Folgende Abbildung visualisiert die zeitliche Entwicklung der Themenhäufigkeit in den Meldungen über einen Zeitraum von sechs Monaten. Die verschiedenen Farben stellen die verschiedenen Thermengebiete dar. Die vertikale Aufteilung zeigt ein Anwachsen bzw. Sinken der Anzahl thematisch passender Meldungen zum jeweiligen Themengebiet.

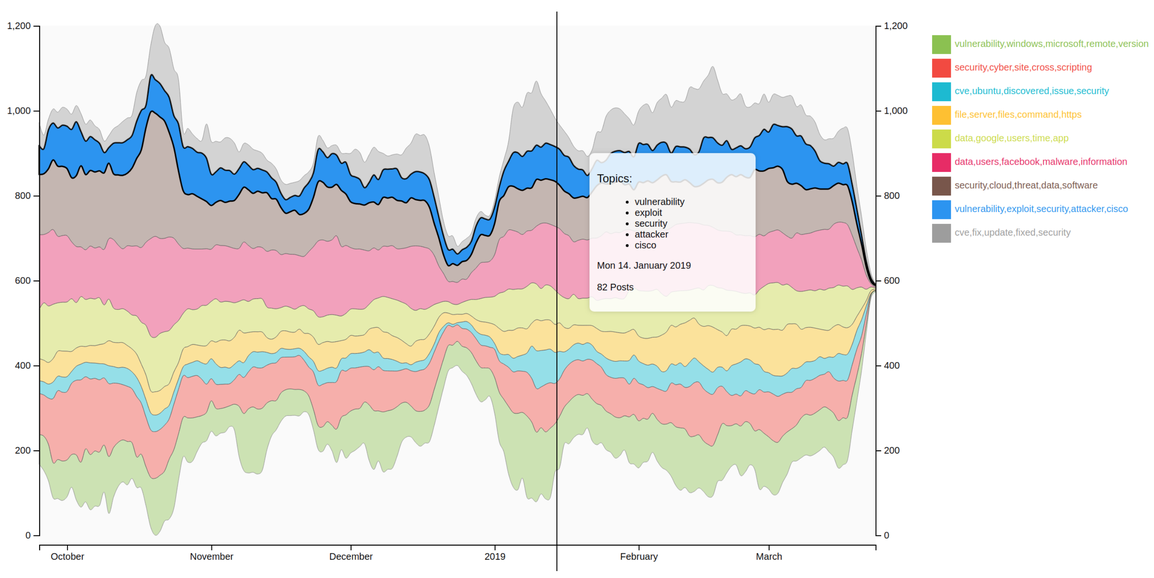


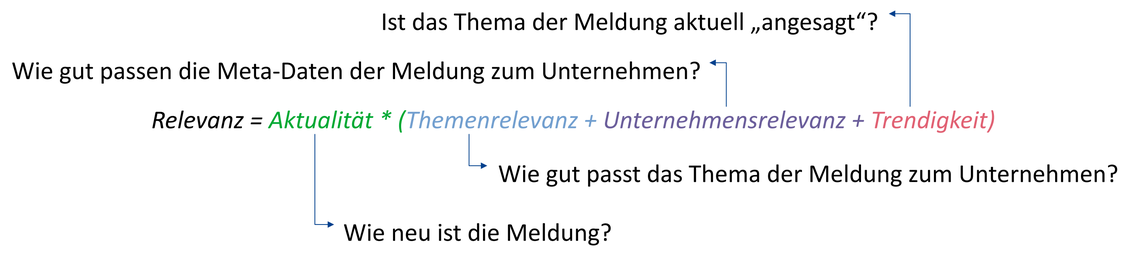
Abbildung 2: Zeitliche Entwicklung der Themenhäufigkeit in den Meldungen.

3. PARTNER

UNIVERSITÄT BONN
Karlsruher Institut für Technologie
ASW Bundesverband
HISOLUTIONS
comma soft® THE KNOWLEDGE PEOPLE

4. DEMONSTRATOR

Um der steigenden Flut an IT-Sicherheitsmeldungen Herr zu werden, wurde das Werkzeug TIER (Threat Information and Event Review) entwickelt. TIER ermöglicht einem Unternehmen aktuelle und relevante Meldungen mit IT-Sicherheitsbezug aus verschiedenen Quellen gebündelt zu betrachten. Durch kontinuierliche Interaktion auf der Weboberfläche sowie Eingabe von grundlegenden Stammdaten des Unternehmens können die angezeigten Meldungen über die Zeit stetig besser individualisiert werden. TIER „lernt“, welche Meldungen relevant sind für das Unternehmen, und nutzt dieses Wissen, um neue Meldungen nach Relevanz zu ordnen. Somit bleibt nur noch der relevante Bruchteil der eingehenden Meldungen übrig. Auf diese Weise entsteht ein unternehmensbezogenes, proaktives Lagebild zur aktuellen IT-Sicherheitslage. Dieses hat den Vorteil, dass, präventive Maßnahmen begründet ergriffen werden können, um so das Unternehmen besser gegen Angriffe zu rüsten.



Ein Benutzer kann die ihm angezeigten Meldungen in zwei Weisen beeinflussen. Durch Angabe von relevanten *Stammdaten* (z.B. verwendete Hardware/Software) und Auswahl von relevanten Themengebieten (in Form von Wortwolken) kann ein explizites Interessenprofil erstellt werden. Durch *Interaktion* mit Meldungen in der Weboberfläche durch dafür bereitgestellte Buttons und Links findet eine implizite Profilierung statt. Um die Relevanz der Meldung für einen konkreten Nutzer zu bestimmen, werden diese und andere Faktoren gewichtet zusammengerechnet.

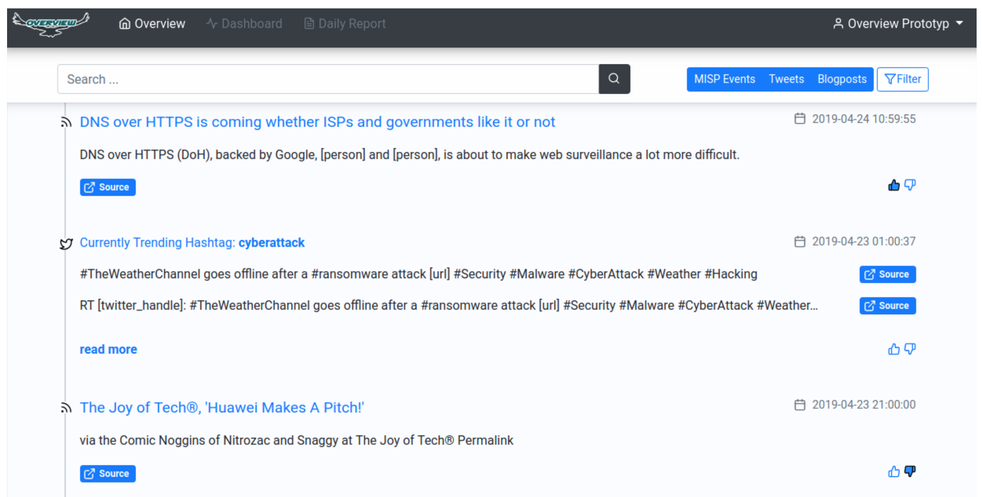


Abbildung 3: Screenshot der Weboberfläche von TIER. Verschiedene zur Individualisierung verwendete Bedienelemente sind in Form von Likes, Dislikes, etc. zu sehen.

5. DATENSCHUTZ- UND HAFTUNGSRECHTLICHE BETRACHTUNG

Der konkrete Einsatz bzw. die Aufbereitung von OSINT wirft verschiedene rechtliche Fragen auf. Eine Vielzahl der in offenen sozialen Medien allgemein zugänglichen Informationen weisen einen Personenbezug auf. Maßgeblich zur Bestimmung der Öffentlichkeit ist demnach, ob die Informationen der Allgemeinheit oder nur innerhalb einer abgeschlossener Gruppen bzw. eines Kreises ohne Verwendung von Zugangsbarrieren zur Verfügung gestellt wurden. Letztlich kommt es v.a. auf die Unterscheidung von Primär- und Sekundärdaten und dem Verarbeitungskontext an. Die bloße Kenntnisnahme, die der Verwendungsart durch Gestattung entspricht, bedarf keiner Ermächtigungsgrundlage. Das gezielte Zusammentragen und die Auswertung der Informationen geht jedoch mit einer höheren Eingriffsintensität einher, die eine Rechtsgrundlage benötigt. Bei Primärdaten ist zu beachten, dass durch die Gestattung des Öffentlichmachens und damit partieller Verzicht auf die Vertraulichkeit ein geringerer Schutz besteht und die Abwägungskriterien überwiegen können, die für eine Datenverarbeitung nach Art. 6 Abs. 1 lit. f DS-GVO sprechen. Beim konkreten Einsatz des Relevance Rankings bedarf es bei Einbindung eines Like-Buttons einer bewussten und eindeutigen Einwilligung.

Im Rahmen des Projektes werden anhand ausgearbeiteter Haftungsszenarien - u.a. Setzen von Hyperlinks; fehlerhafte Warnung; Nichtverfügbarkeit von Daten - Haftungsansprüche der beteiligten Akteure geprüft.

Als technische und organisatorische Maßnahmen werden u.a. salted Hash vorgesehen. Die Speicherung der Daten erfolgt lokal. Eine Weiterverarbeitung bzw. Nutzung außerhalb des Unternehmens (soweit MISP nicht genutzt wird) ist nicht vorgesehen.

Prof. Dr. Michael Meier, Marc Ohm, Daniel Vogel, Arnold Sykosch
Institut für Informatik 4, Arbeitsgruppe IT-Sicherheit
https://itsec.cs.uni-bonn.de/overview
overview@uni-bonn.de
Rheinische Friedrich-Wilhelms-Universität Bonn
Endenicher Allee 19A, 53115 Bonn