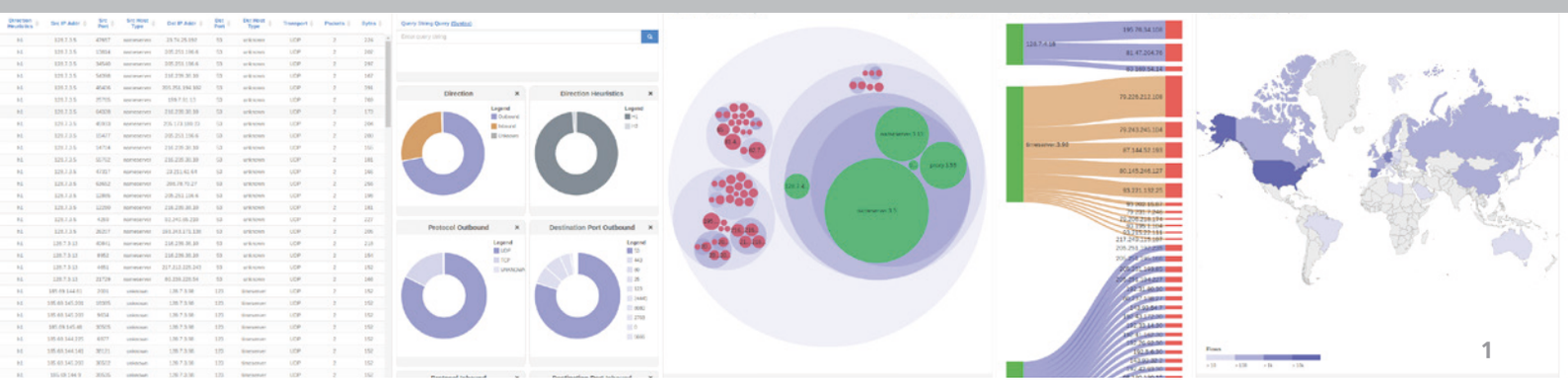
Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE



HUMAN-CENTRIC SECURITY VISUALIZER

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie FKIE

Fraunhoferstraße 20
D-53343 Wachtberg

ANSPRECHPARTNER
Henning Perl
Telefon +49 228 73-54208
henning.perl@fkie.fraunhofer.de

Dr. Carsten Winkelholz
Telefon +49 228 9435-494
carsten.winkelholz@fkie.fraunhofer.de

www.fkie.fraunhofer.de

EINE NEUE VERTEIDIGUNG GEGEN CYBER-ANGRIFFE

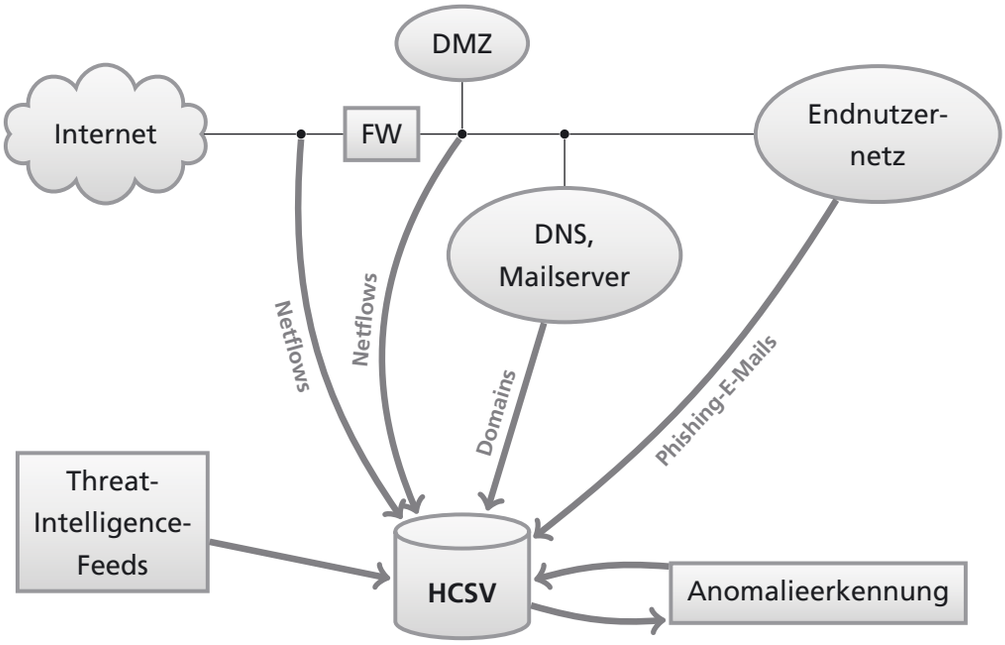
Die Gefahr durch Cyber-Angriffe hat in den letzten Jahren stark zugenommen. Vermehrt sind diese Angriffe genau auf ein Ziel zugeschnitten, so dass Standardabwehrmaßnahmen wie Firewalls und Intrusion Detection keinen automatisierten Schutz mehr bieten. Mit unserem Ansatz soll der Mensch wieder in den Mittelpunkt gestellt werden. Die Handlungsfähigkeit von Administratoren und Sicherheitsexperten soll dadurch unterstützt werden, dass ihnen ein Lagebild über verschiedene Bedrohungssensoren bereitgestellt wird.
Das Ziel des Human-Centric Security Visualizers ist es, die Handlungsfähigkeit von Systemadimistratoren zu erhöhen, indem die Daten, die jetzt schon vorhanden sind (Logdaten, IDS-Systeme) visuell aufbereitet werden. Zudem werden weitere Datenquellen wie die Annotation von Domains oder die Analyse von E-Mail-Texten eingebunden. Des Weiteren ist es nach Kundenwunsch möglich, zusätzliche Datenquellen in das System zu integrieren.

ZIELE DES PROJEKTES

Der Human-Centric Security Visualizer unterstützt den Netzwerkadministrator darin, sicherheitsrelevante Aufgaben durchzuführen.

Zu diesen Aufgaben zählen
- das Erkennen und Analysieren von Anomalien,
- das Erkennen von Schwachstellen,
- die Visualisierung von Meldungen von Warnsensoren (IDS, Firewalls, Honeypots),
- das Einschätzen und Berichten von Risiken, und
- das Ableiten von Maßnahmen.

Das System ist modular aufgebaut. Zunächst werden sicherheitsrelevante Daten über Sensoren gesammelt. Nachfolgend werden diese Daten mittels Machine-Learning und NLP-Verfahren aufbereitet, wobei auch Daten aus einer Datenbank



2

bekannter Malware-Domains hinzugezogen werden. Die aufbereiteten Daten bilden dann den Ausgangspunkt für die Visualisierung der Gesamtlage für den Administrator.

ARBEITSWEISE

Bei der Datenerhebung wurde darauf geachtet, dass das System mit einer großen Menge an unterschiedlichen Daten umgehen kann. Da Log- und Netflowdaten in Echtzeit aggregiert, gespeichert und indiziert werden müssen, sind dabei Technologien wie Elastic Search zum Einsatz gekommen. Es wurde ein Backend-System entwickelt, welches die Daten sammelt und für die Datenanalyse vorbereitet. Des Weiteren werden die Daten über eine JSON-API dem Visualisierungs-Frontend, zur Verfügung gestellt. Beim Einlesen der Netflows werden diese mit weiteren Meta-Informationen, wie z. B. der Gefährlichkeit der angefragten IP-Adresse oder geographischer Informationen, angereichert. Die Bewertung der Gefährlichkeit von IP-Adressen ist möglich, weil aus bekannten Schadsoftwarefamilien mittels Analyse die von dieser Schadsoftware verwendeten Domänen extrahiert wurden (mittels Reverse Engineering des Domain Generation Algorithmus). Dadurch können z. B. pro Tag für die bekannten Schadsoftwarefamilien sämtliche verwendeten Domänen im Voraus berechnet werden. Verwendet man nun diese Domänen in einer Blockliste (z. B. an einem Proxy), so kann der Schaden durch die Schadsoftware verhindert und das infizierte System identifiziert werden. Darüber hinaus wird über versuchte Zugriffe auf die Steuerdomain der Schadsoftware die Art der Infektion des Rechners bestimmt. Mittels dieser Information ist es dann möglich, eine Signatur und Desinfektionsmethode für den infizierten Rechner bereitzustellen. Die durch das Tool bereitgestellten Informationen werden dann geeignet visualisiert und bieten dadurch nicht nur effektiven Schutz gegen bekannte Schadsoftware, sondern bilden auch einen wertvollen Beitrag zu einem Lagebild der aktuellen Bedrohungslage.

BENUTZEROBERFLÄCHE

Für die Konzeption des Benutzerinterfaces wurde zunächst mit den Systemadministratoren des FKIE der genaue Nutzungskontext identifiziert. Hierzu wurden die Vorgehensweisen des Administrators bei der Analyse des Netzwerkes erfasst und darauf basierend das Konzept der Oberfläche entwickelt, das in einem ersten Prototypen umgesetzt wurde.
Kernelemente der Oberfläche sind interaktive Visualisierungen, mit denen sich für die identifizierten Nutzungskontexte intuitiv informative Grafiken erzeugen lassen. Die Oberfläche ist mit aktuellen Webtechnologien umgesetzt und lässt sich damit leicht in verschiedene Systemlandschaften integrieren. Es werden aktuelle Techniken in der Informationsvisualisierung wie Transitionen verwendet, die ein verbessertes Nutzerlebnis erzeugen sowie eine verbesserte Aufmerksamkeitssteuerung bei Wechsel der Informationsdarstellung und damit ein besseres Verständnis von Zusammenhängen ermöglichen.
Das System wurde in die Infrastruktur des FKIE integriert, um es an Livedaten zu testen und die Arbeitsweise von Adminstratoren mit diesem Werkzeug weitergehend zu evaluieren. Auf Basis der Erkenntnisse werden dann die Anforderungen und Use-Cases erweitert.

1 *Benutzeroberfläche des Security Visualizers.*

2 *Darstellung des modularen Systemaufbaus.*