“PATCH GEHABT” - Sicherheitslösung für Unternehmensnetzwerke auf Basis von OSINT

Hintergrund

Täglich werden neue Schwachstellen in verschiedenster Software bekannt. Gleichzeitig werden auch Exploits, die beschreiben wie Schwachstellen ausgenutzt werden können, entwickelt und veröffentlicht.
In einer IT-Infrastruktur in der eine sehr hohe Anzahl an Anwendungen, Servern und Netzwerkgeräte betrieben werden, ist es daher sehr wichtig, existierende Schwachstellen zu erkennen und auf Relevanz zu prüfen, um zum einen ein Bewusstsein für die aktuelle Sicherheitslage der IT-Infrastruktur zu erlangen und zum anderen durch die Behebung von Schwachstellen, potentielle Angriffsflächen zu minimieren.
Es muss also jede Schwachstellenmeldung auf Relevanz und Kritikalität bewertet werden. Dieser Prozess, Schwachstellenmanagement genannt, ist nicht nur für große, sondern jegliche Unternehmen mit einer IT-Infrastruktur von Bedeutung. Die Bewertung von Schwachstellen erfolgt dabei durch den zu erwartenden Schaden, wenn eine Ausnutzung erfolgt.

Ziel

Im Projekt soll ein komplexes System zur Verwaltung von Informationen zu Schwachstellen prototypisch entwickelt werden. Hierzu soll eine modulhaft organisierte Software erstellt werden, welche Schwachstellenmeldungen aus verschiedenen Quellen einliest, mit weiteren öffentlich verfügbaren Datenquellen verknüpft und gegen eingesetzte Software in Unternehmensnetzwerken prüft. Dabei soll die in Abbildung 1 dargestellte Struktur aus [Romilla2018] oder eine ähnliche (bspw. SEPSES knowledge graph [Kiesling2019]) als Grundgerüst genutzt werden.

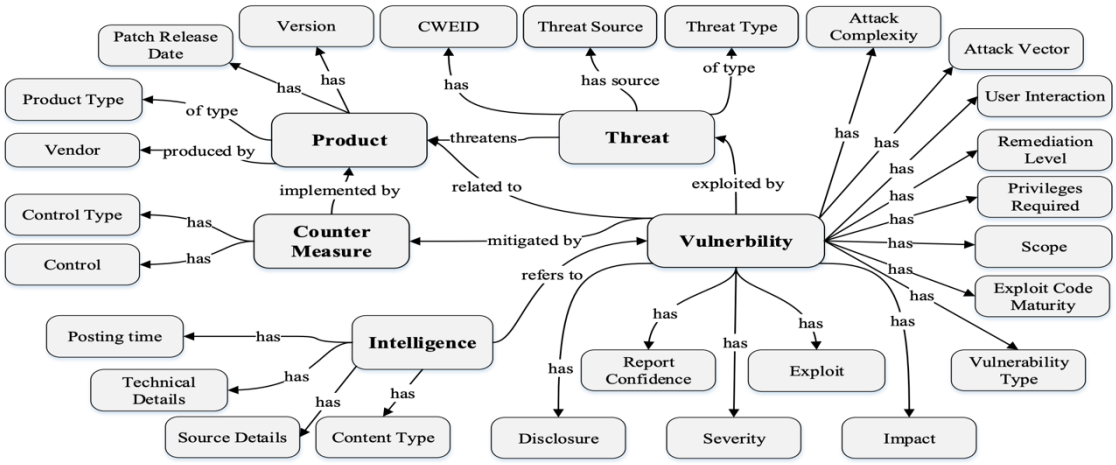

Abbildung 1: Modell eines Ontologie-basierten Schwachstellen Modells aus [Romilla2018]

Weiterhin sollen Ergebnisse von Schwachstellenscans und weiteren technischen Quellen im System verwertet werden können.

Schwachstellenmeldungen müssen immer in der aktuellsten Version zur Verfügung stehen und alle Informationen bezüglich dieser, einem Analysten dargestellt werden. Dabei soll es die Möglichkeit geben, Informationen eines Analysten, wie bspw. eine eigene Bewertung nach dem CVSS Standards oder Informationen aus Ticketsystemen von Unternehmen ebenfalls zu verwalten.

Für die Auswertung der Sicherheitslage eines gesamten Unternehmens ist eine Darstellung von Schwachstellen bspw. in „Vulnerability Quadrants“ [Leonov2017], aber auch in einer zeitlichen Entwicklung von Schwachstellen wünschenswert.

Zur effektiven Verknüpfung von Meldungen verschiedener CERTs, Software und Hardwareherstellern mit Produktinformationen ist ein Einsatz von Maschinellem Lernen notwendig, um in Texten, vollautomatisiert, zu erkennen für welche Produkte die Meldung erstellt wurde, aber auch um Kritikalität, und empfohlene Methoden zur Behebung von Schwachstellen zu erkennen. Weiterhin sollten Aktualisierungen von Informationen bzgl. Schwachstellen wie bekannt gewordene Exploits, Nachrichtenmeldungen oder Daten aus sozialen Netzwerken kenntlich und benutzerfreundlich dargestellt werden.

Um den Einsatz in Unternehmensnetzwerken zu ermöglichen, sind im Projekt auch Methoden zu evaluieren, welche eine Verarbeitung vertraulicher Informationen (der im Unternehmen eingesetzten Soft-, Firm- und Hardware) ermöglichen, ohne dass der Betreiber des Systems Einsicht in vertrauliche Informationen erhält. Wir werden die Möglichkeit haben, den Prototypen im IT Betrieb einer bekannten Bank zu testen und evaluieren.

Kontakt

Prof. Dr. Christian Dörr - Lehrstuhl Cyber Security and Enterprise Security

Referenzen

[Romilla2018] Syed, Romilla, and Haonan Zhong. "Cybersecurity Vulnerability Management: An Ontology-Based Conceptual Model." (2018).

[Kiesling2019] Kiesling, Elmar, et al. "The SEPSES Knowledge Graph: An Integrated Resource for Cybersecurity." International Semantic Web Conference. Springer, Cham, 2019.

[Lenov2017] Vulnerability Quadrants :https://avleonov.com/2017/05/10/vulnerability-quadrants/#:~:text=Vulnerability%20Quadrant%20is%20a%20simple,vulnerabilities%20crawling%20on%20the%20screen.&text=%E2%80%93%20It's%20all%20about%20CVEs.