SPOTTED

Systematic mapPing Of deTecTion approaches on data sources for Enhanced cyber Defence

Programm / Ausschreibung	FORPA, Forschungspartnerschaften NATS/Ö-Fonds, FORPA OEF2020	**Status**	abgeschlossen
Projektstart	01.10.2021	**Projektende**	30.09.2025
Zeitraum	2021 - 2025	**Projektlaufzeit**	48 Monate
Keywords	Incident, Detect, Response, Cyber-Attack, Detection, SIEM, IDS, Honeypot, Usable-Security		

Projektbeschreibung

Im letzten Jahrzehnt gab es einen klaren Paradigmenwechsel von Prävention und Schutz zu Erkennung und Reaktion. Es wird davon ausgegangen, dass Angreifer die Systeme bereits bis zu einem gewissen Grad kompromittiert haben ("Presumption of Compromise"). Die Implementierung einer organisationsweiten Erkennung und Reaktion auf dieses Problem ist ein sehr ressourcenintensives Unterfangen. Die erforderlichen Softwarelösungen sind komplex in Betrieb und Wartung, die für das Unterfangen notwendige Sicherheitsexperten sind eine sehr gefragte Ressource. Dies spiegelt sich auch in aktuellen Beschäftigungszahlen wider, es ist ein deutlicher Mangel an IT-Sicherheitsspezialisten in Österreich und weltweit erkennbar. Eine vollständige Erkennung und Reaktion erfordert eine dedizierte Infrastruktur mit enormen Leistungsanforderungen. Hinzu kommt, dass die Trends aus Wirtschaft, Umwelt und Technik die Digitalisierung drastisch beschleunigt haben. Die Sicherheitsaspekte der laufenden Systemintegration sind komplex und werden bei unternehmerischen Entscheidungen in der Regel nicht vollständig berücksichtigt. Die Implementierung von infrastrukturweiten Erkennungssystemen kann schnell das gesamte IT-Sicherheitsbudget verschlingen. Es besteht eine hohe Wahrscheinlichkeit, dass Erkennungs- und Reaktionsprojekte von vornherein verworfen, abgebrochen oder unvollständig durchgeführt werden. Dies ist in der Tat ein ernstes Problem, da eine effektive Erkennung und Reaktion erfordert, um die Zeit von Cyberangriffen zu verkürzen und den wirtschaftlichen Schaden und die Auswirkungen auf die menschliche Sicherheit so gering wie möglich zu halten. SPOTTEDs Mission ist es, diesen Problemen entgegenzuwirken. Es werden Methoden und Modelle im Bereich der Erkennungs- und Reaktions-Prozesse entworfen, die sich mit folgenden Fragen beschäftigen: Welche Datenquellen und Erkennungstechniken sind besonders gut geeignet, um möglichst viele, häufige oder besonders gefährliche (in Bezug auf den Schaden) Cyber-Angriffe zu erkennen? Ist eine generalisierte Anwendung von Erkennungstechniken auf Datenquellen möglich? Wie sieht eine Methodik aus, die es Unternehmen ermöglicht, die optimale Kombination von Erkennungsalgorithmen und Datenquellen für die Erkennung mehrstufiger Angriffe auszuwählen? Wie müssen Erkennungsereignisse angereichert werden, um die Qualität (Zeit bis zur Entscheidung, Falscherkennungsrate) der Erkennung und den Entscheidungsprozess bei der Reaktion auf einen Vorfall zu verbessern? Es wird ein Prototyp entwickelt, der die Methoden, Modelle und Konzepte implementiert. Die Ergebnisse werden in einer virtuellen Umgebung validiert, die reale Dienste aktueller und zukünftiger Unternehmensumgebungen sowie anspruchsvolle simulierte mehrstufige Angriffe emuliert. Darüber hinaus werden die Ergebnisse mit realen Angriffen während des Einsatzes neuartiger Honey-Pot- und Honey-Network-Konzepte sowie der

Expertenvalidierung durch Industriepartner kreuzvalidiert.

Projektpartner

- AIT Austrian Institute of Technology GmbH