Zürcher Hochschule
für Angewandte Wissenschaften

School of Engineering

InIT Institut für angewandte Informationstechnologie

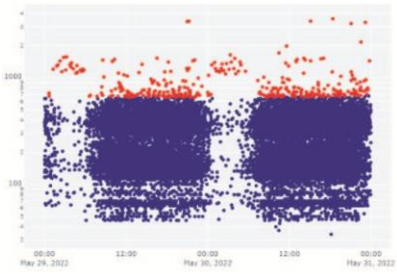
ISpot: Anomalie-Erkennung bei REST APIs

Bei der SWICA Krankenversicherung werden viele interne und externe Schnittstellen als REST-APIs über einen zentralen Enterprise Service Bus angeboten. Diese Schnittstellen werden über ein klassisches Monitoring-System überwacht und es wird nach statischen Schwellenwerten alarmiert. Das Ziel dieser Thesis war darum herauszufinden, ob anhand von detaillierten Loginformationen der Schnittstellen wie Payload und Metadaten ein Standardzustand definiert werden kann und ob entsprechende Abweichungen (Anomalien) erkannt werden können. Anomalien werden bei potenziellen Cyberattacken, ungenügender Datenqualität und fehlerhaften Umsystemen erwartet. Zur Prüfung dieser Hypothesen wurde in einem ersten Schritt eine Logdatenbank erstellt und mit den entsprechenden Daten befüllt. Danach wurden die Logs manuell mit einem eigens hergestellten Log-Viewer ausgewertet und entsprechende Schwellenwerte für den Standardfall ausfindig gemacht. Mittels komplexer SQL-Abfragen wurde ausserdem nach kontextuellen Anomalien gesucht. Nach ersten Erkenntnissen wurden davon Features ausgewählt und mit zwei verschieden Unsupervised Machine Learning Algorithmen geprüft. Mit dem Isolation Forest-Algorithmus konnten gute Ergebnisse bei der Anomalieerkennung bei Häufungen von Anfragen und längeren Antwortzeiten erzielt werden. Anhand dieser Resultate konnte der SWICA Krankenversicherung ein Massnahmenkatalog überreicht werden. Dieser enthält Vorschläge zur weiteren Verbesserung der REST-Schnittstellen sowie Hinweise auf mögliche Sicherheitsprobleme. Als Weiterentwicklung wäre wohl die Verwendung eines Neuralen Netzwerks, wie z.B. ein Autoencoder, ebenfalls zu prüfen und es könnten entsprechende Vergleiche mit den bereits guten Resultaten des Isolation Forest gemacht werden. Als Limitation der Arbeit kann die relativ kurze Dauer der Datenerhebung angesehen werden. Da die Datenakquise ebenfalls Bestandteil der Thesis war, konnten nur Daten von drei Monaten analysiert werden. Somit konnte keine Saisonalität untersucht werden.

Diplomierende
Riccardo Somma
Lukas Stieger

Dozent
Andreas Weiler

Dashboard der Anomalie-Erkennungssoftware iSpot



Die roten Punkte sind die erkannten Anomalien im logarithmisch skalierten Graph.