Themenbeschreibung Wintersemester 2023/2024

Freitag, 22. September 2023 09:11

Titel: Frühwarnsystem für Cybergefahren

Beschreibung:

Im Internet gibt es diverse Quellen für aktuelle Angriffsversuche, aktuell ausgenutzte Malware, Hersteller unter „Beschuss" sowie andere Trends.

Beispielhaft wären die folgenden Quellen:

- Kaspersky: https://cybermap.kaspersky.com/de/stats
- SANS Internet Storm Center: https://isc.sans.edu/data/threatfeed.html
- Shodan: https://www.shodan.io/
- Warnmeldungen des LKA BW: https://lka.polizei-bw.de/warnmeldungen/
- Metasploit: https://www.metasploit.com/
- Virustotal: https://developers.virustotal.com/reference/overview
- …

Ziel:

Trenderkennung aus unterschiedlichsten Quellen, um eine Art von Frühwarnsystem darzustellen. Mögliche Parameter wären:

- Welche Hersteller werden aktuell häufig angegriffen?
- Sind die Angriffe einer bestimmten Branche zuzuordnen?
- Sind Muster/Angriffsarten erkennbar (Erhöhte Anzahl an Uploads von Malware auf Virustotal zu einem bestimmten Typ, Erhöhte Anzahl an neuen Metasploit-Modulen zu einem Hersteller/Software,….)

Randbedingungen:

Aufgabenstellung kann aufbauend bearbeitet werden (mehrere Semester und/oder Bachelor oder Master-Thesis).

möglicher Lösungsansatz: ChatGPT für Quellenscan und Bewertung

Betreuer EnBW:

Sebastian Grupp, OT Security

Titel: automatisierte Bewertung von Security-Schwachstellen

Beschreibung

sog. CVEs (Common Vulnerabiltites and Exposures) bewerten Schwachstellen und mögliche Security-Risiken von Software-Systemen (Applikationen, Libraries etc).

Eine unternehmensspezifische Bewertung erfordert zusätzlich ein Mapping auf Kritikalität (Business-Sicht) der konkreten Appilikations/Systemlandschaft

Ziel:

Automatisierte Bewertung der CVEs im internen Kontext über Security-Zonen

Teilaufgaben

- Datenmodellierung (Systeme, Standorte. Zonen, CVEs, …)
- Simulation Produktionsumgebung (Server, Applikationen, Netzwerke)
  - Simulation / Interface zu CMDB
- Visualisierung Zonen (Zuordnung System zu Zone)
- Mapping von CVEs auf Standorte. Zonen und Systeme, Visualisierung

Input EnBW:

- Architektur der Security-Zonen
- Darstellung ITIL-Prozess und Datenhaltung der Konfigurationdaten ("CMDB")
- …

Randbedingungen:

Themenstellung auf Gruppen aufteilbar und/oder über mehrere Semester

Betreuer EnBW:

Ralf Fischer, Enterprise Architektur Management

Titel: NoCoding mit ChatGPT

Beschreibung

Mit ChatGPT functions können externe APIs in Prompdialoge integriert werden

Ziel:

Bewertung von ChatpGPT als Alternative zu LowCode/NoCode Entwicklungsumgebungen sein (zB für Prototypen-Entwicklung)

Input EnBW:

Mögliche UseCases

- Automatisierte Bereitstellung von IT-Ressourcen (Virtueller Server mit Eintrag in CMDB)
- Visualisierung von Energieerzeugungsdaten (siehe EnBWApp "E-Cockpit")
- …

Randbedingungen:

UseCases in Abstimmung erweiterbar

Betreuer EnBW:

Ralf Fischer, Enterprise Architektur Management

Titel: EnergyMap

Beschreibung

Energieerzeuger (national und international) veröffentlichen Produktions - und Verbrauchsdaten in diversen öffentlich zugänglichen Webseiten in unterschiedlichen Formaten. Eine konsoldierte Darstellung zb von "PV-Leistung in Deutschland" erfordert manuelle Recherche zu Quellen, Export und Normierung der Daten und Zusammenfassung zu einer zentralen Übersicht.

Ziel:

Automatisierte Erfassung von Erzeugungs- und Verbrauchsdaten von Energieerzeugern

Teilaufgaben

- Automatisches Auffinden der Datenquellen
- Exportieren der Daten und normierte Speicherung
- Bereitstellung der Daten für Prognosen und Auswertungen

Input EnBW:

- Glossar Energiewirtschaft
- Darstellung Wertschöpfungskette Energieerzeugung und Marktteilnehmer
- UseCases / Abfragen gegen Datenbestand wie zb "PV -Erzeugung in Deutschland Mai 2023"

Randbedingungen:

Themenstellung auf Gruppen aufteilbar und/oder über mehrere Semester
Möglicher Ansatz für Auffinden von Datenquellen/Infos: ChatGPT

Betreuer EnBW:

Christian Sander, Digital Office

Titel: Pre-Checks für Software-Updates

Beschreibung

Software-Hersteller dokumentieren Updates i.d.R über Releasenotes in denen Abhängigkeiten und Voraussetzungen bzgl. SW/Library/Frameworkversionen in Textform beschreiben. Funktionale Erweiterungen und Einschränkungen werden ebenfalls in Textform beschrieben. Zur Einschätzung auf die konkret installierten Systeme müssen diese Dokumente von System-Admins/Applikationsverantwortlichen gelesen und bewertet werden.

Ziel:

Automatisierte Auswertung der Relasenotes ("Scan") und Zuordnung auf betroffene Syteme; zusätzlich Aufzeigen möglicher Inkompatibilitäten

Titel: Visualisierung des Herkunftsnachweis von Strom auf Basis von anlagenscharfen Zeitreihen-Daten auf der Blockchain

Beschreibung:
Aufbauend auf Erfahrungen mit diesen prototypischen Anwendungsfällen, hat die EnBW in einem Whitepaper[1] beschrieben, wie die Distributed Ledger Technologieals Basis für ein dezentrales Energieökosystem fungieren könnte. Der in einem Token-Modell abgebildete Ansatz zeigt, wie Objekte aus der realen Welt vertrauensvoll in digitaler Form auf einer Blockchain abgebildet werden können und wie eine vertrauenswürdige Dokumentation von Energieaustauschen auf einer Blockchain erfolgen kann. Der im Whitepaper vorgestellte Smart-Contract-Stack wurde bereits exemplarisch für Ethereum-basierte Blockchains implementiert und auf GitHub unter der MIT-Open-Source-Lizenz veröffentlicht[2].

[1] https://it-architecture.enbw.com/whitepaper-energy-token-model/
[2] https://github.com/B2E2/b2e2_contracts

Aufgabenstellung:
Anlegen eines Beispielszenarios für die Strombelieferung eines Kleinen Gewerbekunden auf der Blockchain unter Anwendung einer bereits implementierten Blockchain Infrastruktur mit Hilfe bereitgestellter API Endpunkte. Der Fokus liegt in der nutzerzentrierten Visualisierung des Herkunftsnachweises unter Verwendung der dokumentierten Qualitäten und

Ziel:

Automatisierte Auswertung der Relasenotes ("Scan") und Zuordnung auf betroffene Syteme; zusätzlich Aufzeigen möglicher Inkompatibilitäten

Teilaufgaben

- Automatisierter "Text-Crawler" (inkl. Scan nach Hersteller-Produktseiten)
- Simulation CMDB der Produktionsumgebung (Server mit OS und SW-Installationen)
- DB-Modellierung (Output Crawler und Mapping gegen CMDB + Bewertung)

Input EnBW:

- Servicestruktur / Betriebsmodell zu Server-Betrieb und -Dokumentation
-
- …

Randbedingungen:

Möglicher Ansatz für Extrahierung Herstellerinfos aus Dokumente: ChatGPT

Betreuer EnBW:

Ralf Fischer, Enterprise Architektur Management

[2] https://github.com/B2E2/b2e2_contracts

Aufgabenstellung:
Anlegen eines Beispielszenarios für die Strombelieferung eines Kleinen Gewerbekunden auf der Blockchain unter Anwendung einer bereits implementierten Blockchain Infrastruktur mit Hilfe bereitgestellter API Endpunkte. Der Fokus liegt in der nutzerzentrierten Visualisierung des Herkunftsnachweises unter Verwendung der dokumentierten Qualitäten und Energiemengentransfers.

Teilaufgaben:

- Anlegen Digitaler Identitäten für Erzeugungs- und Verbrauchsanlagen
- Dokumentation der Eigenschaften über Verifiable Credentials
- Dokumentation der Zählwerte als 15min Zeitreihen
- Abbilden einer Verteillogik wie Erzeugte Energie an Verbraucher verteilt wird.
- Aufnehmen der Anforderungen an die Nachweisführung
- Entwickeln von Ideen zur Visualisierung der Nachweisführung.
- Visualisieren der Belieferung der Verbrauchsanlage über den Zeitverlauf über eine Web oder mobileApp.

Input EnBW:

- Erzeugungs- und Verbrauchsanlagen und deren Eigenschaften
- Zeitreihen der Erzeugungs- und Verbrauchsanlagen
- Implementierte Private Blockchain mit deployem Smart Contract Stack
- Business API zum Anlegen der Assets und Dokumentation von Eigenschaften und Zählwerten. Sowie dem Mengentransfer.
- Scanner API zum Auslesen der Information aus den Blockchain
- IT-Architektur - Whitepaper: Energy Token Model

Randbedingungen:

Fokus für Teilaufgaben Visualisierung vs. Backend-Entwicklung wird zum Kickoff festgelegt
Themenstellung auf Gruppen aufteilbar und/oder über mehrere Semester

Betreuer EnBW:

Christian Sander / Klaus Winter, Digital Office / Enterprise Architektur Management