Contribution ID: **47** Type: **Poster**

Testy penetracyjne systemu zarządzania energią elektryczną OpenEMS —identyfikacja i mitygacja podatności w otwartoźródłowych systemach energetycznych

Thursday 24 April 2025 10:45 (30 minutes)

W odpowiedzi na rosnącą popularność rozproszonych systemów zarządzania energią oraz integrację odnawialnych źródeł energii (OZE), w projekcie przeprowadzono kompleksową analizę bezpieczeństwa otwartoźródłowego systemu OpenEMS. System ten, napisany w języku Java, wspiera monitorowanie, kontrolę i optymalizację przepływów energii elektrycznej w instalacjach przemysłowych i prosumenckich. Celem projektu była identyfikacja krytycznych podatności w systemie oraz ocena ryzyka dla integralności, dostępności i poufności danych w kontekście systemów zarządzających infrastrukturą energetyczną. Zidentyfikowano problematykę związaną z brakiem powszechnie dostępnych analiz bezpieczeństwa otwartoźródłowych systemów EMS, mimo ich rosnącego znaczenia w przemyśle i energetyce. W trakcie badań przeprowadzono testy penetracyjne obejmujące, analizę kodu źródłowego i komponentów backendu, testy dynamiczne interfejsów REST API, ocenę bezpieczeństwa warstwy komunikacji Modbus TCP, badanie podatności na typowe błędy programistyczne i konfiguracyjne. Do realizacji testów wykorzystano m.in. środowiska OWASP ZAP, Burp Suite, a także specjalistyczne narzędzia dedykowane testowaniu systemów OT i aplikacji webowych. Przeanalizowano krytyczne błędy w kodzie źródłowym oraz zaproponowano zmiany w konfiguracji komunikacji sieciowej, zwiększające odporność systemu na ataki. Projekt dostarczył istotnych wniosków naukowych, pogłębiając wiedzę z zakresu cyberbezpieczeństwa otwartoźródłowych systemów klasy EMS. Wyniki badań wykazały powtarzalne wzorce podatności charakterystyczne dla tego typu rozwiązań i potwierdziły konieczność łączenia podejścia IT z praktykami ochrony infrastruktury krytycznej (OT). Z perspektywy praktycznej i komercyjnej projekt przyniósł mierzalną wartość dla podmiotów wdrażających OpenEMS w rzeczywistych instalacjach przemysłowych i prosumenckich. Opracowane rekomendacje mogą zostać bezpośrednio wykorzystane w audytach bezpieczeństwa oraz jako podstawa dla dalszego rozwoju systemu, zwiększając jego odporność na zagrożenia cybernetyczne.

Author: GORLOWSKI, Kacper

Presenter: GORLOWSKI, Kacper

Session Classification: Session B (Poster)