Strefa przedsiębiorcy

2018-02-01

Cyberbezpieczeństwo stacji paliw - specjalnie dla miesięcznika "Paliwa Płynne" komentuje Dawid Przewodowski z PetroConsulting Sp. z o.o.

Rosnąca świadomość Klientów, a także powszechność ataków hakerskich na wszelkie systemy informatyczne, zmuszają ich twórców do odpowiedniego zabezpieczania swojego oprogramowania przed włamaniami i kradzieżą danych. Firma PetroConsulting przykłada do tego zagadnienia ogromną wagę czego dowodem są odpowiednie zabezpieczenia systemu.

Można tu wymienić kilka z nich:

- System PetroManager zawsze wymusza korzystanie z szyfrowanych połączeń HTTPS, dzięki czemu hasła i loginy użytkowników na żadnym etapie nie są przesyłane niezabezpieczone. Wyjątek stanowi sytuacja, gdy system działa w infrastrukturze informatycznej klienta. Wówczas to od jego decyzji zależy czy szyfrowanie połączeń będzie wymuszane.

- Z kolei w bazie danych hasła nigdy nie są przechowywane bezpośrednio, a jedynie w formie bezpiecznego, kryptograficznego skrótu (SHA-256) utworzonego dodatkowo z użyciem losowej soli. Jest ona specjalnym ciągiem znaków tworzonym z wykorzystaniem znacznika czasowego oraz danych użytkownika, co zapewnia jej odpowiednią unikalność. Celem jej stosowania jest utrudnienie ataków wykorzystujących kolizje funkcji skrótu. Dodatkowo wydłuża ona pozornie hasło, co utrudnia inne formy ataku.

- Posiadamy również zabezpieczenia przed atakami CSRF (Cross-Site Request Forgery), polegającymi na fałszowaniu żądań do serwera z użyciem wcześniej przechwyconej prawidłowej komunikacji. Przy każdym wyświetleniu formularza w interfejsie systemu generowany jest jednorazowy kod weryfikacyjny, który pozwala na jednokrotne jego zatwierdzenie. Uniemożliwia

to ataki poprzez ponowne przesłanie przechwyconej, poprawnej komunikacji między klientem a serwerem. Niezależnie od powyższego stosowanie szyfrowania komunikacji (HTTPS) wymuszane przez system PetroManager, również znakomicie utrudnia ataki typu CSRF.

- Ponadto bezpośredni dostęp do serwerów, na których działa system PetroManager, jest możliwy jedynie z użyciem kryptograficznych kluczy dostępowych, które są ściśle strzeżone. Natomiast same serwery działają w zintegrowanym klastrze obliczeniowym, który wewnętrznie chroni dane przez ich replikację w czasie rzeczywistym na wszystkie węzły klastra oraz przeprowadza pełny backup baz danych regularnie co 6 godzin.

Wymienione powyżej elementy są tylko niektórymi zabezpieczeniami, które stosujemy dla maksymalnej ochrony danych naszych Klientów. Z oczywistych względów nie możemy podać więcej szczegółów.

Źródło: PetroConsulting

WIĘCEJ czytaj w marcowym wydaniu miesięcznika "Paliwa Płynne"

Źródło:
http://www.paliwa.pl/strona-startowa/archiwum/cyberbezpieczenstwo-stacji-paliw-specjalnie-dla-miesiecznika-paliwa-plynne-komentuje-dawid-przewodowski-z-petroconsulting-sp-z-o