ZDALNY DOSTĘP SECOMEA

DLA UTRZYMANIA RUCHU – ESENCJA IIOT

Prawdopodobnie Przemysł 4.0 oraz IIoT to obecnie najbardziej nośne hasła, które na swych sztandarach umieszczają dostawcy wszelkiej automatyki – od sensorów po systemy PAC. Rzecz w tym, że aby te idee wdrożyć potrzebny jest system bezpiecznej komunikacji – prosty, skalowalny i cyberbezpieczny. Potrzebny jest prawdziwy zdalny dostęp.

TEKST: KRZYSZTOF ZAJDEL,
COMPART AUTOMATION

PRAWDZIWY ZDALNY DOSTĘP A VPN

Koncepcja IIoT jest atrakcyjna dla utrzymania ruchu, ponieważ umożliwia szybką zdalną interwencję serwisu (często zewnętrznego) na poziomie linii produkcyjnych i pojedynczych maszyn. Zdalny dostęp przez Internet nie jest rzeczą nową. Zakłady produkcyjne od dawna wykorzystują sieci prywatne VPN, by zapewnić dostęp serwisu do urządzeń. Takie rozwiązanie wymaga jednak dużego zaangażowania działu IT i jest trudne w praktycznym zarządzaniu. VPN sprawdza się bowiem dobrze tylko w prostych scenariuszach, gdy uczestnicy komunikacji należą do jednej organizacji.

Remedium na te bolączki są systemy zdalnego dostępu oparte na chmurze. Jednym z przykładów jest system **Secomea**. Umożliwia on zdalny dostęp przez Internet do dowolnych urządzeń. Ponadto, posiada system zarządzania uprawnieniami użytkowników na zasadzie drag and drop. Co to oznacza dla utrzymania ruchu? Można błyskawicznie dołączyć nową osobę jako uprawnioną do zdalnego dostępu i precyzyjnie określić, do jakich urządzeń ma mieć dostęp (na poziomie pojedynczych sterowników, paneli itp., z uwzględnieniem konkretnych usług – np. dostęp tylko do webserwera sterownika bez możliwości zmiany programu w PLC). Ma to olbrzymie znaczenie, gdy serwis urządzeń w zakładzie zlecany jest firmom zewnętrznym (np. producent maszyny, integrator systemu czy samodzielny automatyk). Nierzadko takich firm w zakładzie jest wiele.

BEZPIECZEŃSTWO PONAD WSZYSTKO

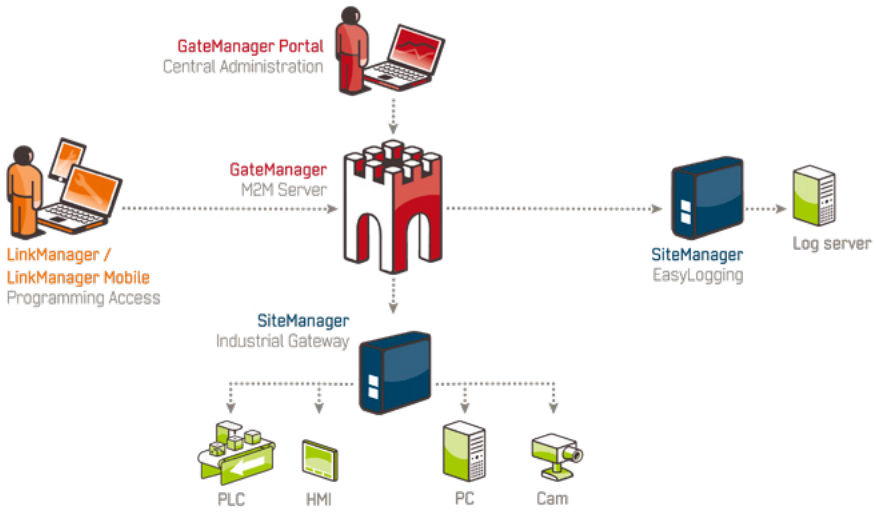
Nie wystarczy zaszyfrować przesyłanych danych, by mówić o bezpieczeństwie zdalnego dostępu. System powinien być odporny na nieuprawniony dostęp. Secomea oferuje możliwość dwu lub nawet trzyskładnikowego uwierzytelnienia (login-hasło, certyfikat X.509, jednorazowy kod SMS). Ponadto, system powinien być wolny od luk funkcjonalnych. Przykładowo, powinien dawać łatwą możliwość skutecznego zarządzania uprawnieniami, a więc łatwego ich nadawania oraz, co jeszcze ważniejsze, odbierania. Musi być również jak najmniej podatny na błędy i niedbalstwo użytkowników.

Secomea to system certyfikowany przez organizację ProtectEM, badającą holistycznie zagadnienia związane z bezpieczeństwem systemów informatycznych na podstawie uznanych w świecie IT standardów, np. NIST SP800-115.

JAK TO DZIAŁA?

Schemat działania przedstawia rysunek nr 1. Centralnym elementem systemu jest **GateManager** - serwer M2M. GateManager może być zainstalowany na serwerach Secomea (hosting) lub na własnym serwerze. GateManager pozwala na rozbudowane zarządzanie prawami dostępu poszczególnych użytkowników do urządzeń, archiwizuje informacje dotyczące wykonywanych połączeń i pozwala na szybką diagnostykę stanów wszystkich urządzeń w sieci. GateManager jest zarządzany i konfigurowany zdalnie przez administratorów za pomocą portalu administracyjnego z poziomu przeglądarki internetowej.

Urządzenia obiektowe, do których chcemy mieć dostęp, podłączone są do Internetu przez **SiteManager** - rodzaj routera niewymagający w czasie eksploatacji żadnych lokalnych konfiguracji.



Rys. 1. ?????

SiteManager może być podłączony do Internetu stacjonarnego przez sieć zakładową (przez port **Ethernet** lub **WiFi**) lub/i mobilnego (wbudowany modem **3G** lub dołączany modem **3G/4G** przez USB). SiteManager automatycznie nawiązuje łączność z serwerem GateManager. SiteManager udostępnia w sieci Internet urządzenia i usługi oparte o sieć **Ethernet**, a także urządzenia z interfejsem szeregowym **RS232** oraz **USB**. SiteManager dostępny jest jako router sprzętowy lub w wersji software'owej do instalacji na komputerze PC.

Aby operator mógł połączyć się ze zdalną instalacją niezbędny jest **LinkManager** - program uruchamiany na komputerze PC. Po zalogowaniu się na swoje konto użytkownik może za pomocą kilku kliknięć wybrać spośród udostępnionych mu obiektów ten, z którym chce nawiązać łączność, wybiera konkretne urządzenie (sterownik, panel, itp.) i jest już online. Korzysta ze standardowych narzędzi tak, jakby był na miejscu.

Za pomocą funkcji **LinkManager Mobile** użytkownik może połączyć się ze zdalną instalacją za pomocą urządzenia mobilnego (tablet, telefon) i uzyskać dostęp do WWW, VNC oraz RDP. To szczególnie ciekawa możliwość z punktu widzenia utrzymania ruchu i kadry zarządzającej produkcją. Można podejrzeć stany pracy maszyn z dowolnego miejsca w świecie.

GDZIE SĄ NASZE DANE?

Sercem zdalnego dostępu jest serwer **GateManager**, który pełni rolę centralnego węzła komunikacyjnego i wyposażony jest w interfejs zarządzania zdalnym dostępem. Unikalną cechą systemu Secomea jest to, że daje użytkownikowi wybór czy chce korzystać z serwera GateManager w hostingu w chmurze, czy wyposażyć się we **własny serwer**. Ta druga opcja daje pełną gwarancję poufności wszelkich danych, ponieważ cała infrastruktura jest wyłączną własnością posiadacza serwera, a Internet jest jedynie medium transmisyjnym do przesyłania szyfrowanych informacji. Żaden zewnętrzny podmiot nie ma dostępu ani do przesyłanych danych, ani do kont użytkowników, logów serwera, statystyk, ani żadnych innych danych przechowywanych w systemie.

Więcej na: **www.secomea.pl**