KOMPLEKSOWA OCHRONA INFRASTRUKTURY ELEKTROENERGETYCZNEJ

Bezpieczeństwo w sieci

Teleinformatyczne systemy zarządzania procesem wytwarzania, przesyłu i dystrybucji energii wymagają szczególnych zabezpieczeń i kompleksowej ochrony przed zagrożeniami. Nad stworzeniem prototypowego mechanizmu skutecznej ochrony infrastruktury elektroenergetycznej przed internetową przestępczością, pracuje konsorcjum naukowo-przemysłowe, którego liderem jest Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego. O założeniach interdyscyplinarnego projektu rozmawiamy z prof. dr hab. inż. Markiem Amanowiczem z Zakładu Systemów Telekomunikacyjnych Wydziału Elektroniki WAT.

Fot. Archiwum

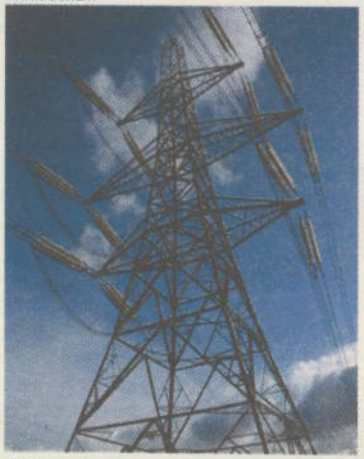
– Rozwiązanie nad którym pracuje konsorcjum ograniczy ryzyko zagrożeń?

– Zapewnienie systemowej ochrony infrastruktury teleinformatycznej sieci elektroenergetycznej przed zagrożeniami internetowymi jest podstawowym celem naszego projektu. W jego realizacji oprócz WAT uczestniczą partnerzy mający bardzo duże doświadczenie w tworzeniu rozwiązań, pozwalających zwiększyć efektywność, niezawodność i bezpieczeństwo nowoczesnych systemów teleinformatycznych. Są to: Naukowa i Akademicka Sieć Komputerowa, Wojskowy Instytut Łączności i firma Asecco Poland. Aby zapewnić skuteczność proponowanych przez nas rozwiązań musimy sprawdzić działanie prototypowego systemu ochrony w warunkach rzeczywistych. Do tego konieczna jest współpraca z podmiotami energetycznymi, przede wszystkim z operatorem sieci przesyłowej. Polskie Sieci Elektroenergetyczne (PSE) są naszym głównym interesariuszem w tym interdyscyplinarnym projekcie. Zawarliśmy stosowne porozumienie będące podstawą do prowadzenia wspólnych działań.

– Jaki jest zakres prac objętych projektem?

– Realizacja współfinansowanego przez NCBiR projektu pt. **„System zapewnienia bezpiecznej komunikacji IP w obszarze zarządzania siecią elektroenergetyczną"** podzielona została na cztery etapy. Dwa pierwsze związane są z badaniami naukowymi i polegają na opracowaniu koncepcji systemu ochrony i propozycji rozwiązań szczegółowych oraz ich weryfikacji w warunkach laboratoryjnych. Kolejne dwie fazy wiążą się z wykonaniem prototypu systemu ochrony oraz jego weryfikacji i walidacji w warunkach operacyjnych, zakończonym potwierdzeniem osiągnięcia VIII poziomu gotowości technologicznej. Rozwiązanie będzie testowane z udziałem

Fot. Archiwum



W Polsce musi być stworzony system teleinformatyczny, który zmniejszy tak zwane ryzyko energetyczne.

głównych interesariuszy projektu w wybranych miejscach w infrastrukturze technologicznej sieci elektroenergetycznych. W tym celu konsorcjum podpisało porozumienia z operatorami systemu dystrybucyjnego i przesyłowego oraz z jednostką wytwórczą centralnie dysponowaną. Ostatnie doniesienia, głównie z rynku amerykańskiego wskazują na wykrycie nowych podatności w sterownikach systemu nadzorującego procesy technologiczne związane z produkcją i dystrybucją energii elektrycznej, co może prowadzić do destabilizacji systemu, a w skrajnych sytuacjach do blockout'u. To jest bardzo poważne ostrzeżenie, ponieważ większość takich systemów jest widoczna w Internecie. Na szczęście w Polsce poziom zagrożeń jest dużo mniejszy, ale przy coraz szerszym przechodzeniu na technologię internetową opartą na protokole IP oznacza to konieczność zwiększenia poziomu ochrony kluczowej infrastruktury technologicznej sieci elektroenergetycznych.

– Jakie jest zaawansowanie prowadzonych prac?

– Czas realizacji tego projektu jest dość krótki, bo umowę z Narodowym Centrum Badań i Rozwoju na dofinansowanie projektu podpisaliśmy w grudniu 2012 roku, a zakończenie całego przedsięwzięcia przewidziane jest pod koniec 2015 roku. To wymusza na wszystkich partnerach prowadzenie intensywnych i skutecznych działań. Spotykamy się bardzo często i prezentujemy wyniki cząstkowe, poddając je wnikliwej weryfikacji. Każdy z partnerów wnosi istotny wkład w tworzone rozwiązanie. Pierwsze dwa etapy zakończymy w połowie 2014 roku. Do końca tego roku chcemy wykonać projekty wszystkich mechanizmów, czyli sfinalizować fazę projektową, Mamy już uzgodnioną i przedyskutowaną koncepcję oraz przyjęty model rozproszonego mechanizmu ochrony. Opracowany został schemat głównego komponentu systemu ochrony, zwanego koncentratorem bezpiecznej komunikacji, który będzie współpracował z innymi elementami systemu ochrony, w tym między innymi z modułami uwierzytelniania i nadzoru nad elementami, monitorowania ruchu sieciowego i produkcyjnego, powiadamiania i wizualizacji. Koncentrator ma także zapewnić ochronę przed przenikaniem złośliwego oprogramowania, które mogłyby naruszyć i zdestabilizować systemy automatyki związane ze sterowaniem i zarządzaniem siecią elektroenergetyczną. Rozwiązanie to będzie logicznym modułem grupującym wszystkie elementy systemu instalowane w ramach pojedynczego obiektu elektroenergetycznego. W skali globalnej, system będzie w głównej mierze funkcjonował jako federacja takich koncentratorów. W warunkach laboratoryjnych działanie systemu będziemy testowali na początku przyszłego roku, najpierw w postaci odrębnych komponentów, a później poprzez ich zintegrowanie w warunkach zbliżonych do rzeczywistych. To pozwoli nam na wykonanie końcowej wersji oprogramowania. Naszymi produktami będzie zbiór różnych modułów i aplikacji, które będziemy instalować i testować w wybranych obiektach systemu elektroenergetycznego. W drugiej połowie przyszłego roku rozpoczniemy prace implementacyjne związane z wykonaniem prototypu i sprawdzeniem jego działania, najpierw na platformie badawczej, a później w warunkach operacyjnych.

– Czy jest to trudne zadanie dla tak doświadczonych partnerów?

– Infrastruktura teleinformatyczna u operatorów elektroenergetycznych jest w Polsce w procesie przekształceń i zmian. Wprowadzane są nowe rozwiązania, a my te sytuacje musimy przewidzieć. To stanowi dla nas pewien problem. Stąd konieczność stałej współpracy z operatorami, aby nasze rozwiązanie uwzględniało te zmiany i było dostosowane do rzeczywistości, która pojawi się w następnych latach. Musimy stworzyć niezawodny system teleinformatyczny, który zmniejszy tzw. ryzyko energetyczne i ochroni infrastrukturę technologiczną sieci elektroenergetycznych przed skutkami działań nieuprawnionych.

– Skala i charakter takich zagrożeń są znaczne. Na jakich działaniach się koncentrujecie?

– Koncentrujemy się na działaniach najważniejszych dla uzyskania kompleksowej ochrony przed przestępczością internetową. Tworzymy pewien mechanizm, który będzie służyć ochronie i zabezpieczeniu wszystkich elementów związanych ze sterowaniem procesami wytwarzania, przesyłu i dystrybucji energii. Ten projekt nie rozwiąże globalnie problemu bezpieczeństwa w całej sieci elektroenergetycznej, ale wskaże wiarygodną i sprawdzoną w praktyce metodę w jaki sposób można zabezpieczyć taką sieć. Jeżeli wszystko się powiedzie, to będzie doskonały wzorzec do upowszechnienia i do stosowania tego rozwiązania powszechnie, w całej sieci elektroenergetycznej.

Rozmawiała Jolanta Czudak

BIPSE