

ENZ 2000 – Aplikacja. Bezpieczeństwo danych na serwerze modemowym

Jako oprogramowanie sieciowe Client-Serwer ENZ-2000 przedstawia rzeczywiste siły powiązań otoczenia sieciowego.

Wymaga to specjalnego zabezpieczenia sieci przed wtargnięciem z zewnątrz, gdyż właściwe zadania systemu – czyli komunikacja z urządzeniami peryferiami – zapewnione są przez przyłączenie modemu do sieci.

Właśnie to miejsce (przyłączy) jest najbardziej zagrożone potencjalnym, niedozwolonym wtargnięciem z zewnątrz.

Mimo to można systematycznie atestować wszelkie rozwiązania, jednak tak, żeby można było (założyć odpowiednie zastosowanie) zapewnić odpowiednie zabezpieczenie przed manipulacją i zapewnić ochronę wszystkim częściom systemu przed wtargnięciem z zewnątrz.

W ramach przeprowadzonych badań pod uwagę były brane trzy istotne założenia:

- 1) Programy komunikacji i obsługi będą funkcjonować same – we własnym wydzielonym obszarze procesora, który będzie pracował niezależnie od innych części, mogą być kontrolowane i zainstalowane w nadzorowanym systemie komputerowym.
- 2) Konstrukcja oprogramowania umożliwia obsługę modemów jedynie za pośrednictwem oprogramowania wspomagającego protokoły, inne próby komunikowania się będą odrzucane.
- 3) Użytkownik musi być konsekwentny w administrowaniu systemem. Poprzez to mechanizmy zabezpieczające, stosowane w innych systemach użytkownika nie będą wprowadzały zakłóceń lub nie będą przebiegały, a stała kontrola konfiguracji urządzeń będzie przeprowadzana przez użytkownika lub jego dział –DV (Przetwarzanie Danych).

Co to dokładnie oznacza?

Magazynowanie procesów komunikacyjnych:

Krytycznym momentem (miejscem) w bezpiecznym otoczeniu DV jest wyjście na zewnątrz systemu. Do tego miejsca należą modemy, jak również łącza internetowe, oraz inne sieci robocze, przez które potencjalni hakerzy mogą próbować dostać się do sieci przedsiębiorstwa.

ENZ-2000 wykorzystuje do komunikacji odpowiednie serwery modemowe.

Będą one, jeżeli chce się rzeczywiście zabezpieczyć system, obsługiwane przez własny komputer. Na serwerze modemowym oprócz programu sterującego MOD 2000 nie powinno się instalować innych pakietów programowych, wejść sieciowych czy bazy danych.

Jeżeli MOD 2000 będzie samodzielnie i systematycznie kontrolowany, wtargnięcie z zewnątrz nie będzie możliwe.

Windows NT proponuje odpowiednie mechanizmy, które kontrolują i odpowiadają za określony system.

Stale normy protokółów:

Serwer modemowy pozwala uruchomić jedynie określone protokoły transmisji. Są one ujęte w oprogramowaniu protokółów licznikowych i magistrali komunikacyjnych takich jak FNP, SCTM, IEC-870/5, DLMS, LSV1 lub innych. Protokoły te zawierają ogólne obiektywne opracowania informacji.

Transmisja danych przebiega przez odpowiedni raster, a przebiegi mogą być kontrolowane i sterowane programem.

O tym jak wysokie jest ryzyko manipulacyjne w praktyce decyduje, staranny stosunek do numerów wejściowych jak i do przewidzianych protokółów.

FNP (zdalny protokół sieciowy) proponuje największe zabezpieczenie pod względem zastosowanych protokółów licznikowych, gdyż identyfikacja nadajnika i odbiorcy ujęta jest w informacjach. Inne protokoły przeważnie nie posiadają (IEC, DIN) lub posiadają tylko jeden nadajnik (SCTM, ISV-1). Zazwyczaj połączenie z programem serwera modemowego nie jest „wolne”, a więc nie ma możliwości odpytania czy skopiowania programu.

Administracja systemu:

Trzecim najważniejszym punktem jest zadbanie o to by dająca pewność konstrukcja programu nie została utracona przez niewłaściwą obsługę.

Administrator użytkownika musi dokładnie i konsekwentnie zapobiegać (jak przy wszystkich innych systemach), by na serwerze modemowym nie zostały zainstalowane obce programy, gdyż modemy użytkowane niezgodnie z ustaleniami są podstawowym punktem dostępu do sieci.

Dystrybutor:

Lackmann Metering Sp. z o.o.
ul. Popularna 4/6
02-473 Warszawa

Tel.: 022 863 51 17
Fax: 022 863 51 18
e-mail: info@lackmann.pl
www.lackmann.pl

Lackmann Metering Sp. z o.o.
LICZNIKI + SYSTEMY POMIAROWE
PRĄD • GAZ • WODA • CIEPŁO