Otwarta architektura – przyszłość elektronicznych systemów zabezpieczeń

artykuł firmy „ID Electronics" – ZOFIA KOLCZYŃSKA

Jednym z najważniejszych czynników, które mają wpływ na jakość elektronicznego systemu zabezpieczeń, jest właściwa realizacja funkcji zdefiniowanych przez jego użytkowników. Dlatego precyzyjne określenie wymagań, jakie powinien spełniać system, jest jednym z najważniejszych zadań, jakie stoi przed jego projektantem oraz przyszłymi użytkownikami. Większość problemów pojawiających się w czasie eksploatacji wynika z nieumiejętności sprecyzowania oczekiwań. Niewłaściwie dobrany system może być źródłem irytacji użytkownika, zmuszonego do korzystania z rozwiązań, które nie zawsze odpowiadają jego rzeczywistym potrzebom. Szczegółowe określenie potrzeb oraz zdobycie odpowiedniej wiedzy przed dokonaniem zakupu umożliwią wybór systemu, którego infrastruktura nie zamyka możliwości dalszego rozwoju.

Wybierając rozwiązanie o ograniczonych możliwościach, użytkownik powinien mieć świadomość, że w pewnym momencie rozwój systemu zostanie zakończony. Istnieje zagrożenie, że swobodna rozbudowa systemu, niezbędna na danym etapie rozwoju firmy, nie będzie już możliwa. Natomiast zastosowanie rozwiązania integrującego różne systemy pozwala na dokonanie swobodnego wyboru wśród producentów i produktów, które w danym momencie najbardziej odpowiadają potrzebom użytkownika obiektu. Jednocześnie gwarantuje, że gdy te potrzeby ulegną zmianie, nie będzie kłopotu z dostosowaniem systemu. Dzięki temu użytkownik będzie mógł korzystać z zainstalowanego systemu przez długi czas, bez ponoszenia nadmiernych kosztów związanych z dokonywaniem koniecznych zmian.

Integracja

Integracja może być realizowana na wielu poziomach. Najczęściej systemy są łączone ze sobą za pomocą interfejsów. W tym przypadku każdy z systemów działa niezależnie, każdy zarządza własną bazą danych, jest oddzielnie konfigurowany i administrowany. W konsekwencji jest to rozwiązanie bardzo nieefektywne. Może ono zostać ulepszone przez wprowadzenie np. współdzielenia danych między systemami. Jednak podstawowy problem pozostaje nierozwiązany, ponieważ nadal istnieją dwa różne systemy, które powinny ze sobą ściśle współpracować. Użytkownik musi pokonywać trudności związane z synchronizacją danych, administracją i aktualizacją systemu, zawodnością oraz relatywnie wysokimi kosztami utrzymania.

W pełni efektywnym rozwiązaniem może być wykorzystanie wspólnej bazy danych dla wszystkich systemów, opartej na skalowalnej architekturze rozproszonej. W ramach tej bazy różne elementy mogą być spójnie łączone dzięki dobrze zdefiniowanym „otwartym interfejsom", zachowując się jak integralne części systemu.

Uzyskanie w pełni spójnego połączenia wszystkich wymaganych podsystemów nie jest zadaniem łatwym. Tak naprawdę rzadko się zdarza, aby jedna firma produkowała wszystkie elementy potrzebne do utworzenia pełnowartościowego systemu zabezpieczeń. Także niewielu producentów potrafi złożyć wszystkie elementy składowe w jeden spójny system, którym można sterować za pomocą jednego interfejsu użytkownika.

Pełna integracja może być uzyskana dzięki połączeniu w systemie trzech podstawowych elementów:

1. **Wspólna baza danych.** Dzięki zastosowaniu wspólnej bazy danych można zagwarantować, że niezbędne informacje będą dostępne w odpowiednim momencie dla wszystkich użytkowników systemu.
2. **Jeden interfejs użytkownika dla wszystkich operacji.** Kluczem do skutecznego wykorzystywania systemu jest uzyskanie prawidłowej reakcji operatora, opartej na właściwym połączeniu zachodzących w systemie zdarzeń z dostępnymi informacjami. Używając różnych rodzajów oprogramowania, pochodzących z kilku źródeł, trudno jest połączyć je ze sobą tak, aby uzyskać niezawodny, a jednocześnie łatwy w obsłudze system, który sprawnie przetwarza informacje i skutecznie wspomaga interwencję ochrony.
3. **Otwarta architektura.** W systemie mogą być wykorzystywane urządzenia różnych producentów. Jeżeli system nie może współdziałać z urządzeniami więcej niż jednego producenta, jest wielce prawdopodobne, że w przyszłości możliwości rozwoju systemu będą bardzo ograniczone. →

Doświadczenia ostatnich lat pokazują, że rozwiązania oparte na otwartej architekturze dynamicznie zdobywają rynek systemów zabezpieczeń.

Współdziałanie

Wybór systemu o otwartej architekturze to zaledwie połowa sukcesu. Ważne jest także, aby był zaprojektowany w sposób umożliwiający jego stały rozwój i łączenie różnych technologii. Odpowiedni system jest gwarancją zrealizowania koncepcji pełnego zarządzania bezpieczeństwem obiektu. Oznacza to, że wszystkie podstawowe systemy, połączone w odpowiedni sposób, tworzą rozwiązanie, które działa skuteczniej niż poszczególne systemy działające samodzielnie.

Dobrym przykładem ilustrującym powyższe zdanie jest zarządzanie systemem telewizji dozorowej. Telewizja dozorowa jest jedną z technologii, którą najtrudniej zintegrować z systemem kontroli dostępu. Kluczową wartością jest możliwość udokumentowania, za pomocą zarejestrowanego obrazu, ważnych zdarzeń zachodzących w systemie. Przy pełnej integracji zarządzania telewizją dozorową, zdarzenia alarmowe lub związane z kontrolą dostępu mogą być łączone z obrazem z kamery, nagranym w miejscu występowania zdarzenia. Odbywa się to bez konieczności interwencji operatora systemu. Informacja o alarmie oraz związany z nim obraz z kamer jest wysyłany do wskazanego użytkownika.

Kolejnym przykładem integracji jest kontrola dostępu połączona z monitorowaniem gości i nadzorowaniem przenośnych urządzeń o dużej wartości. Aplikacja do monitorowania gości pozwala w prosty sposób zarządzać wizytami w obiekcie. Korzystając z komputera, recepcjonista może zaplanować wizytę, zarejestrować odwiedzającego, wykonać identyfikator oraz monitorować poruszanie się gościa po obiekcie. Po zakończonej wizycie gość zostaje wyrejestrowany, a wizyta zarchiwizowana. Kolejna aplikacja umożliwia monitorowanie działania użytkowników przenośnych urządzeń. Jeżeli zachodzi taka potrzeba, istnieje możliwość zlokalizowania danego urządzenia. System zapisuje informacje o tym, w którym czytniku ostatnio dane urządzenie zostało zarejestrowane, a także o osobie uprawnionej, która w danym momencie była w jego posiadaniu. Jeżeli osoba przenosząca urządzenie nie jest do tego uprawniona, zostanie wywołany alarm. Sygnał alarmowy może uruchamiać system telewizji dozorowej, który w momencie pojawienia się urządzenia w punkcie kontrolnym, zarejestruje jego aktualnego posiadacza.

Istnieje także możliwość integracji technologii IT, która nie jest tradycyjnie związana z zabezpieczeniami. Na przykład tworząc konto użytkownika karty w systemie zabezpieczeń, administrator automatycznie tworzy jego konto w systemie Windows. Nazwa konta jest pobierana ze wspólnej bazy danych systemu. Jeżeli konto w systemie Windows jest kasowane, automatycznie dezaktualizuje się karta użytkownika systemu zabezpieczeń, a użytkownik, który został pozbawiony praw dostępu do obiektu, ma automatycznie zablokowany dostęp do sieci komputerowej.

Wysoki poziom integracji oraz wpływ technologii IT radykalnie zmieniają pewne elementy systemu zabezpieczeń. Na przykład to, co tradycyjnie było nazywane zarządzaniem kartami identyfikacyjnymi, jest obecnie zarządzaniem wszystkimi danymi związanymi z użytkownikami systemu – tj. produkcją identyfikatorów, przechowywaniem informacji biometrycznych, autoryzacją logowania do PC oraz monitorowaniem urządzeń przenośnych o dużej wartości.

Dzięki ścisłej integracji możliwe jest stworzenie interfejsu użytkownika o małym stopniu komplikacji. Pracownicy ochrony czy recepcji nie muszą być tak biegli w obsłudze komputera jak administratorzy, którzy zarządzają systemem. Prawidłowa integracja powinna sprawić, że obsługa nawet najbardziej zaawansowanych funkcji będzie bardzo prosta. W przypadku występowania wielu aplikacji, wspólna baza danych i ujednolicony interfejs graficzny sprawiają, że system jest bardziej skuteczny niż kilka oddzielnych systemów realizujących te same zadania.

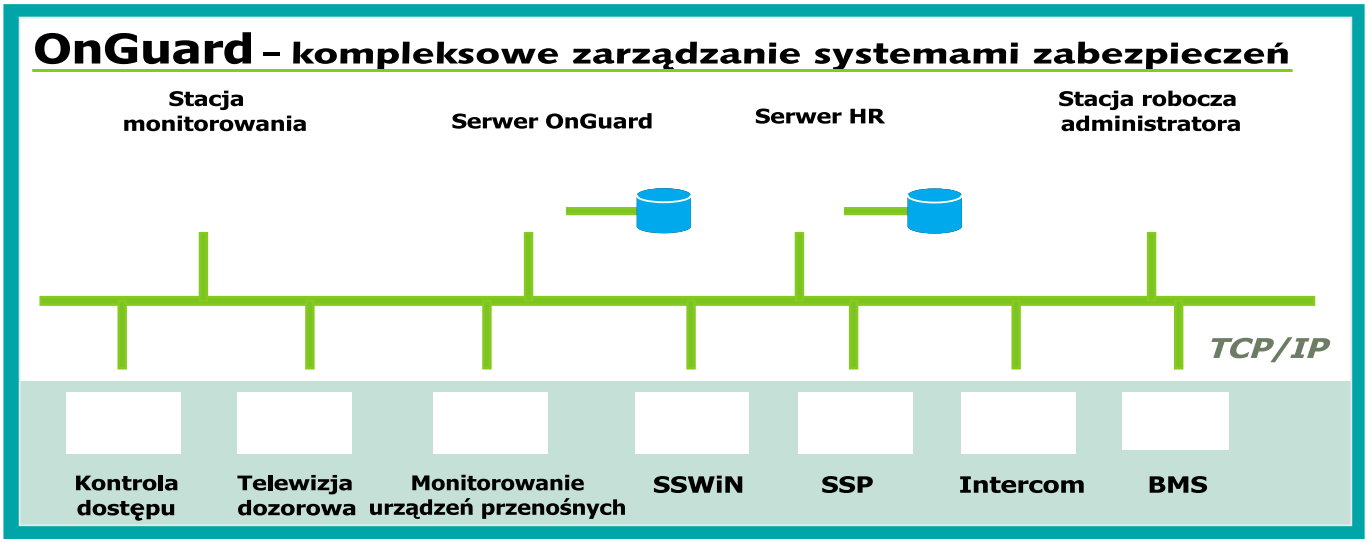
System LENEL OnGuard

Wykorzystanie otwartej architektury do zbudowania rozwiązań kompleksowego zarządzania systemami zabezpieczeń obiektu, oferujących użytkownikowi najnowszą technologię w najprostszy sposób, jest podstawowym celem firmy LENEL. Opracowany przez firmę LENEL system OnGuard ściśle integruje współdziałające ze sobą technologie, wykorzystując standardy otwartej architektury. Jest kompatybilny z systemami operacyjnymi Windows 2000 oraz XP, oferuje zaawansowane funkcje kontroli dostępu, monitorowania alarmów, telewizji dozorowej, sygnalizacji włamania, monitorowania przenośnych urządzeń, produkcji identyfikatorów oraz zarządzania pracownikami i wizytami gości. Wszystkie aplikacje dostępne są jako indywidualne moduły, a także mogą być łączone w dowolnych konfiguracjach w celu stworzenia optymalnego rozwiązania.

System OnGuard został zaprojektowany zgodnie ze standardami obowiązującymi w przemyśle informatycznym. Może współdziałać z wieloma dostępnymi na rynku technologiami: systemami operacyjnymi *(Windows 2000/XP),* platformami baz danych *(Microsoft SQL Server, IBM DB2 Universal Server oraz Oracle Server),* katalogami użytkowników *(MS Active Directory, LDAP),* sieciami *(Ethernet),* generatorami raportów *(Crystal Reports)* oraz narzędziami administracyjnymi. OnGuard może być także ściśle zintegrowany z zewnętrznymi aplikacjami i urządzeniami peryferyjnymi. Istnieje możliwość dwukierunkowej wymiany danych z każdym systemem kompatybilnym ze standardem ODBC *(Open Database Connectivity),* tj. z systemami zarządzania personelem, rejestracji czasu pracy oraz z systemami ERP. System OnGuard obsługuje urządzenia peryferyjne za pomocą przemysłowych sterowników komunikacji, np. drukarki do identyfikatorów *(Nisca, Eltron, Ultra),* urządzenia łączności sieciowej *(Lantronix),* czytników kart (zbliżeniowych, z paskiem magnetycznym, standardu Wieganda, z kodami kreskowymi) oraz czytników biometrycznych.

Wszystkie moduły aplikacji systemu mogą być ze sobą integrowane w dowolny sposób, przy użyciu wspólnej bazy danych oraz jednego interfejsu użytkownika. Oprogramowanie może być konfigurowane i zarządzane z jednego komputera, a wszystkie zdarzenia mogą być monitorowane z dowolnej stacji roboczej w systemie. Rozproszona architektura pozwala na rozmieszczenie stacji roboczych oraz inteligentnych kontrolerów bezpośrednio w istniejącej sieci. Wszystkie lokalne decyzje są podejmowane i wykonywane w modułach, minimalizując ruch w sieci oraz zapewniając dostęp do danych w czasie rzeczywistym.

Istnieje możliwość zintegrowania systemu z aplikacjami sieciowymi. System może być połączony ze standardową prze-



glądarką sieciową, dzięki czemu każda aplikacja jest dostępna przez Internet lub Intranet.

Korzystając z aplikacji udostępniania oprogramowania, administrator może udostępniać niektórym stacjom roboczym tylko określoną część oprogramowania, zwiększając w ten sposób bezpieczeństwo danych oraz ułatwiając pracę operatorom.

Dostęp do zestawu standardowych interfejsów programowania aplikacji (API) umożliwia producentom elementów składowych systemu zabezpieczeń (np. systemów sygnalizacji pożaru, włamania i napadu, telewizji dozorowej) oraz oprogramowania integrację z produktami firmy LENEL.

Aplikacje OnGuard

Onguard Multi-Server Enterprise. Wieloserwerowy system charakteryzujący się zsynchronizowaną bazą danych, umożliwiający monitorowanie zdarzeń związanych z bezpieczeństwem w dużych organizacjach, z siedzibami rozsianymi na całym świecie. Dzięki tej aplikacji np. manager IT może sprawować kontrolę nad całym zintegrowanym systemem, przy jednoczesnym zachowaniu niezależności działania systemów lokalnych.

OnGuard Open IT. Zaawansowana aplikacja integrująca, która pozwala na dwukierunkowe połączenie systemu OnGuard z aplikacjami IT w czasie rzeczywistym. Umożliwia łączenie rekordów użytkowników kart z ich kontami Windows Login, dzięki czemu aplikacje systemu OnGuard mogą być zastosowane (w wersjach pełnych lub okrojonych) na innych platformach programowych i z innymi systemami informatycznymi, takimi jak: Tivoli, HP OpenView czy IBM WebSphere Message Adapter.

OnGuard Area Access Manager. Program umożliwiający autoryzowanym osobom kontrolę dostępu użytkowników do wybranych obszarów w obrębie firmy. Po zalogowaniu się do programu na wybranym komputerze PC, wyświetlana jest lista obszarów, które dany operator może kontrolować oraz lista osób, które mają dostęp do tych obszarów. W łatwy sposób operator może przydzielić lub skasować prawa dostępu.

OnGuard Visitor. Program służący do monitorowania gości przebywających na terenie obiektu. Jeszcze przed przybyciem gościa operator może wprowadzić do systemu wszystkie niezbędne informacje, np. dane osoby odwiedzającej, czas wizyty itp. oraz zdjęcie i podpis. Przybycie gościa potwierdzane jest jednym kliknięciem myszy.

OnGuard Credential Center oferuje zintegrowane funkcje zarządzania kartami identyfikacyjnymi. Aplikacja obsługuje wszystkie możliwe przemysłowe standardy produkcji identyfikatorów oraz wyposażona jest w wiele funkcji kompresji i przetwarzania obrazu.

OnGuard Biometrics pozwala na niezwykle prostą rejestrację wzorów biometrycznych użytkowników. Czytniki wzorów podłączone są bezpośrednio do stacji roboczej, a wzory biometryczne użytkowników pobierane są podczas ich rejestracji w systemie. Nie jest wymagany żaden dodatkowy program do obsługi tego procesu.

Onguard Intrusion oferuje pełną integrację systemu z panelami alarmowymi Radionics oraz z systemami detekcji zdarzeń, dzięki czemu użytkownik może monitorować urządzenia rejestrujące zdarzenia alarmowe i mieć nad nimi pełną kontrolę z poziomu centralnego systemu monitorowania alarmów.

OnGuard Video LDVR umożliwia oglądanie na żywo obrazów z miejsc występowania alarmów. Kamery można podłączyć bezpośrednio do urządzeń kontroli dostępu w terenie i rejestrować zdarzenia w bazie danych systemu. Jeśli wybrane urządzenie zarejestruje alarm lub inne zdarzenie, przypisana do niego kamera rozpocznie rejestrację obrazu. Dla każdego alarmu lub zdarzenia może zdefiniować odpowiednie czasy nagrywania.

OnGuard Video LNVR jest to rozwiązanie bazujące na kamerach adresowalnych (IP), dostępne tylko w wersji programowej. Aby zaopatrzyć się w najnowsze funkcje systemu telewizji dozorowej, należy jedynie zainstalować najnowszą wersję oprogramowania.

OnGuard Mobile Enterprise umożliwia dostęp do wszystkich funkcji systemu OnGuard z poziomu komputera przenośnego. Komputer komunikuje się z siecią i serwerem OnGuard za pomocą łącza bezprzewodowego Ethernet. Jest to doskonałe rozwiązanie dla wszelkiego rodzaju stałych i przemieszczających się punktów kontrolnych.

W pełni zintegrowany system dostarcza rozwiązań, które najbardziej odpowiadają rosnącym potrzebom użytkowników systemu zabezpieczeń. Wszystkie funkcje są dostępne w jednym systemie, administrator zarządza wspólną bazą danych, operator musi opanować posługiwanie się tylko jednym interfejsem użytkownika, a brak duplikacji serwerów, konfiguracji, stacji monitorującej, bazy danych oraz interfejsu użytkownika, ogromnie redukuje całkowity koszt utrzymania systemu.

ID Electronics Sp. z o.o.
ul. Przy Bażantarni 11, 02-793 Warszawa
tel.: (22) 649 60 95, fax: (22) 649 61 00
e-mail: sales@ide.com.pl http://www.ide.com.pl