

Platforma RSA enVision

Systemy i aplikacje wewnętrzne

Systemy i aplikacje wewnętrzne

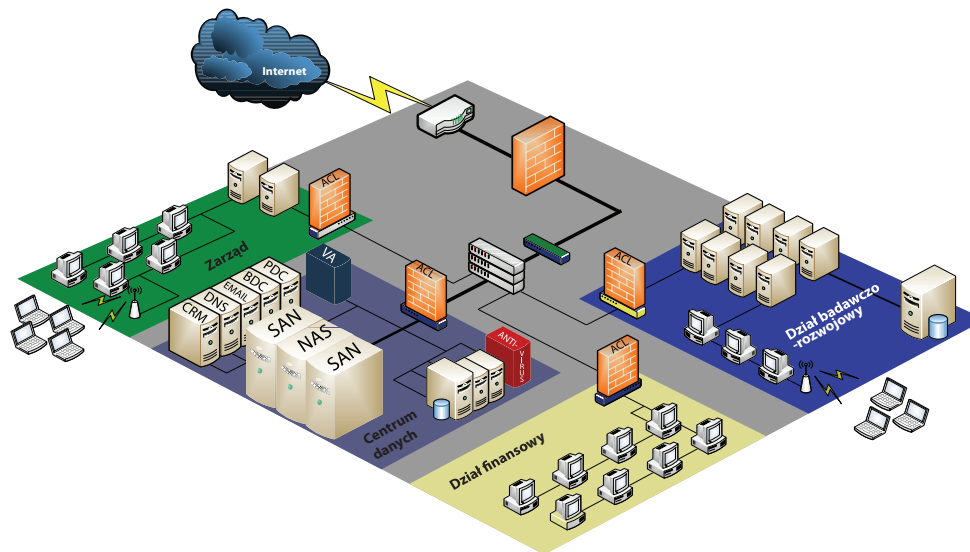
Nawet najlepsze mechanizmy ochrony na styku z internetem nie mogą powstrzymać wszystkich wyrafinowanych zagrożeń bezpieczeństwa pochodzących z zewnątrz, jakie mogą się pojawić w dzisiejszych czasach, a w przypadku zagrożeń wewnętrznych są one prawie beużyteczne. Zmusiło to firmy do tworzenia nowych strategii zabezpieczania swoich sieci wewnętrznych zarówno przed umyślnym, jak i przypadkowym wtargnięciem.

Zabezpieczenie systemów wewnętrznych i aplikacji jest złożonym przedsięwzięciem, które musi brać pod uwagę wszystkie przypadki komunikowania się użytkowników ze wszystkimi wewnętrznymi lub zewnętrznymi usługami w sieci. Typowe środowisko sieciowe w takiej sytuacji to tysiące interfejsów systemowych, prędkości analizy ruchu 100 Mbps/1 Gbe/10 Gbe i niezliczone technologie, takie jak sieci VLAN, bardzo szybkie przełączanie, routery podstawowe, platformy hostów, sieci bezprzewodowe, IDS oraz serwery analizujące słabe punkty. Typowe środowisko aplikacji oznacza często tysiące programów – aplikacje typu klient/klient oraz klient/serwer – i setki protokołów. Wreszcie, istnieje zwykle środowisko zarządzania obejmujące setki grup użytkowników wymagających przyporządkowania do różnych zasad postępowania.

Zabezpieczanie sieci wewnętrznej za pomocą enVision

Platforma enVision™ firmy RSA jest jedynym rozwiązaniem do zarządzania informacją i zdarzeniami bezpieczeństwa, które daje stuprocentowy wgląd we wszystkie zagrożenia bezpieczeństwa mogące wystąpić wewnątrz sieci – począwszy od przełączników i routerów przez urządzenia zabezpieczające, aplikacje i serwery, aż po urządzenia do przechowywania danych.

Platforma enVision zapewnia bezpieczeństwo poprzez agregację i analizę wszystkich danych (All of the Data™) ze wszystkich elementów infrastruktury sieciowej w czasie rzeczywistym. Wykorzystuje przy tym możliwości bazy danych protokołu internetowego Internet Protocol Database™ (IPDB) LogSmart®. Używając systemu uczenia się na podstawie poziomu bazowego przez platformę enVision, użytkownik dokładnie widzi zwyczajne – albo odbiegające od normy – wzorce powstające w sieci, dzięki czemu może zidentyfikować zagrożenia bezpieczeństwa dosłownie w każdym miejscu sieci, nawet w przypadku oddalonych lokalizacji.



The Security Division of EMC



Baza danych protokołu internetowego firmy

Dzięki wykorzystaniu zaawansowanej architektury LogSmart IPDB stosowanej przez setki przedsiębiorstw na całym świecie, urządzenie jest w stanie przechwytywać wszystkie dane (All the Data) z sieci, mechanizmów zabezpieczających, hostów, warstw aplikacji i urządzeń do zapisu danych zainstalowanych w obrębie całego przedsiębiorstwa. LogSmart IPDB umożliwia analizę danych zarówno w czasie rzeczywistym, jak i archiwalnych, oraz ich prezentację w formie przeglądów i raportów dostosowanych do różnorodnych potrzeb każdego działu przedsiębiorstwa – np. działu IT, działu bezpieczeństwa, osób odpowiedzialnych za zapewnienie zgodności i zarządzanie ryzykiem czy wreszcie zarządu.

Zalety bazy danych LogSmart IPDB:

- Zaprojektowana w celu przechowywania i zapewnienia efektywnej pracy z wykorzystaniem danych nieusystematyzowanych, bez konieczności ich filtrowania lub normalizowania
- Zapewnia utrzymanie cyfrowego łańcucha ochrony danych, dzięki czemu dane raz wprowadzone do bazy nie mogą zostać zmienione – w odróżnieniu od większości schematów danych wykorzystywanych w rozwiązaniach opartych na RDBMS
- Nie są konieczne programy typu agent
- Rozproszona architektura typu „peer-to-peer” umożliwia dużą skalowalność i wydajność

Dzięki zastosowaniu platformy enVision użytkownicy mają możliwość gruntownej poprawy wewnętrznych systemów i aplikacji przez:

- **Wdrożenie kontroli dostępu** – Możliwość kompleksowego kontrolowania i raportowania w celu wdrożenia zasad kontroli dostępu pozwala klientom na natychmiastowe wykrycie nadużyć i wprowadzenie odpowiedzialności zarówno za uprawniony, jak i nieuprawniony dostęp do sieci, zasobów obliczeniowych i składników na poziomie obiektów.
- **Zmniejszenie liczby błędnych klasyfikacji** – Automatyczna korelacja zgłaszanych ataków z zasobami i danymi podatnymi na uszkodzenia znacznie ogranicza koszty powstałe w wyniku incydentu i umożliwia skoncentrowanie strategicznych zasobów analizy bezpieczeństwa na ważnych zdarzeniach.

- **Monitorowanie w czasie rzeczywistym** – Ujednolicony podgląd wzajemnych zależności pomiędzy zdarzeniami następującymi w obrębie przedsiębiorstwa znacznie usprawnia praktyki klienta zdefiniowane i stworzone na podstawie ciągłego monitorowania sieci w czasie rzeczywistym oraz informacji o systemie i zdarzeniach bezpieczeństwa. Dzięki temu użytkownik może bardzo szybko ustalić, „co się dzieje” w sieci firmowej.
- **Wykrywanie nieautoryzowanych usług sieciowych** – Wykrywanie niedozwolonych usług wykorzystujących „otwarte ścieżki” w zabezpieczeniach sieci umożliwia klientom zamknięcie dróg dostępu do sieci, które mogłyby umożliwić wypływ informacji, naruszenie prywatności oraz przepływ nielegalnych treści przez sieć przedsiębiorstwa.
- **Wdrożenie listy obserwacyjnej** – Analiza parametryzowanych zdarzeń i ostrzeżeń umożliwia uzyskanie większej wydajności działania, a także pozwala klientom na zdefiniowanie ryzyka narażenia na zagrożenia zewnętrzne i wewnętrzne ze strony przestępców identyfikowanych za pomocą adresów sieciowych i nazw użytkownika, atakujących określoną usługę i systemy w sieci przedsiębiorstwa.
- **Skorelowane wykrywanie zagrożeń** – Cel zapewnienia bezpieczeństwa całej sieci przedsiębiorstwa realizowany jest poprzez zautomatyzowany proces sprawdzania sieci, bezpieczeństwa i zdarzeń systemowych pod kątem słabych punktów oraz oceny ryzyka i zagrożeń we wszystkich lokalizacjach firmy.

O firmie EMC RSA

Firma RSA – oddziału firmy EMC zajmującej się bezpieczeństwem – jest uznanym na rynku liderem w przekształcaniu danych występujących w całej sieci przedsiębiorstwa na informacje bezpieczne i zgodne z przepisami. Baza danych LogSmart® Internet Protocol Database (IPDB)™ oferuje architekturę, która jako jedyna umożliwia efektywne gromadzenie i ochronę danych o kluczowym znaczeniu w działalności klientów. Dzięki firmie Network Intelligence setki klientów na całym świecie zapewniają sobie zgodność i bezpieczeństwo bez zwiększania kosztów i złożoności.



RSA Security Inc.
RSA Security Ireland Limited
www.rsa.com

The Security Division of EMC

© 2007 RSA Security Inc. Wszelkie prawa zastrzeżone.
RSA, RSA Security, RSA Secured, SecurID, SecurCare oraz logo RSA są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy RSA Security Inc. w Stanach Zjednoczonych i/lub innych krajach. Microsoft i Windows są zastrzeżonymi znakami towarowymi lub znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i/lub innych krajach. EMC jest zastrzeżonym znakiem towarowym EMC Corporation. Wszystkie inne produkty i usługi wymienione w niniejszej publikacji są znakami towarowymi odpowiednich podmiotów.