NOWA WIZJA BEZPIECZEŃSTWA

Secure Mail Intelligence!® for Domino

Problem

Większość pracodawców nie zdaje sobie sprawy z tego, że cyfrowe zagrożenia zazwyczaj nie pochodzą z zewnątrz, a z wewnątrz firmy.
Zgodnie z najpopularniejszym scenariuszem pojawiają się one wewnątrz, przez lekkomyślność lub zamierzone i szkodliwe działanie jednej z zatrudnionych osób, a później rozszerzają się na inne departamenty, aż w końcu, na przykład elektronicznym listem, zostają przesłane na zewnątrz. Takie działania powodują następujące zagrożenia:

:: utrata poufnych informacji zawierających dane osobowe, finansowe, strategiczne projekty, idee i plany rozwojowe,

:: niepożądane treści na przykład związane z pedofilią, rasizmem; przechowywanie (nawet nieświadome) takich treści pociąga za sobą konsekwencje prawne,

:: nielegalne załączniki pliki zawierające muzykę, filmy , oprogramowanie nie tylko zabierają pracownikom czas ale także „zapychają" łącze,

:: infekcje wirusowe zapoczątkowane przez pliki dostarczone poprzez pocztę elektroniczną, przyniesione na laptopach, dyskach USB, urządzeniach PDA. Wirusy mogą spowodować całkowitą utratę wszystkich danych, uniemożliwić dostęp do serwerów, rozsyłać spam, przesłać ważne, tajne dane do konkurencji itp.

Rozwiązanie – SMI! for Domino

SMI! for Domino równoważy lekkomyślność i przeciwdziała złym intencjom pracowników. Zapobiega wyciekowi ważnych dla firmy informacji.
Nie pozwala na przeciążanie sieci dzięki skutecznym narzędziom do regulowania ruchu pocztowego. W pełni zabezpiecza serwery poczty i pracy grupowej IBM Lotus Domino. Zintegrowany wewnętrznie z serwerem chroni korespondencję i aplikacje Lotus Domino/Notes. Eliminuje również wiele zagrożeń pochodzących z wewnątrz przedsiębiorstwa. Najważniejsze funkcje SMI!:

:: Kompleksowe bezpieczeństwo, pełna ochrona przed wszystkimi zagrożeniami.

:: Prosta konfiguracja, zarządzanie i utrzymanie systemu.

:: Osiem silników antywirusowych zintegrowanych wewnętrznie (Authentium, ArcaVir, Kaspersky, Norman, Quick Heal, Sophos, Symantec, ClamAV).

:: Możliwość dołączenia nieskończenie wielu innych silników antywirusowych.

:: Zaawansowana analiza i kontrola treści.

:: Kontrola treści załączników, także zagnieżdżonych.

:: Analiza binarna plików.

:: Analiza binarna obrazów (opcja).

:: Archiwizacja poczty (w bazach Lotus Domino, IBM DB/2 lub Firebird), a także za pomocą Tivoli Storage Manager.

:: Graficzne raporty.

:: Wygodny i przejrzysty interfejs WWW.

:: Obsługa klastrów i serwerów partycjonowanych.

:: Otwarta architektura umożliwiającą dodawanie własnych filtrów i zdarzeń.

:: Dowolnie definiowane polityki, które są tworzone i stosowane w zależności od użytkownika, odbiorcy, nadawcy, typu pliku, wielkości, rozszerzenia, adresu.

CHARAKTERYSTYKA

- chroni pocztę przed atakami (wirusy, robaki, konie trojańskie itp.)
- chroni bazy danych Domino przed wirusami
- jednocześnie pracuje kilka silników antywirusowych
- chroni pocztę przed spamem, wykorzystuje dwadzieścia różnych technik antyspamowych
- uniemożliwia rozpowszechnianie zagrożeń wewnątrz i na zewnątrz firmy
- blokuje dystrybucję wirusów i niepożądanych wiadomości
- pomaga zapewnić bezpieczeństwo informacji zgodnie z polityką firmy
- obsługuje klastry Domino
- wyposażony w prosty, intuicyjny interfejs modułu zarządzającego (WWW)
- łatwy w użyciu moduł raportujący wykryte i zneutralizowane zagrożenia

Za trzy czwarte wszystkich naruszeń bezpieczeństwa w firmie odpowiedzialni są jej pracownicy

(„Information Age")

SMI! Series
SECURE MAIL INTELLIGENCE!®

NOWA WIZJA BEZPIECZEŃSTWA

Secure Mail Intelligence!® for Domino

Jak pracuje **SMI! for Domino**

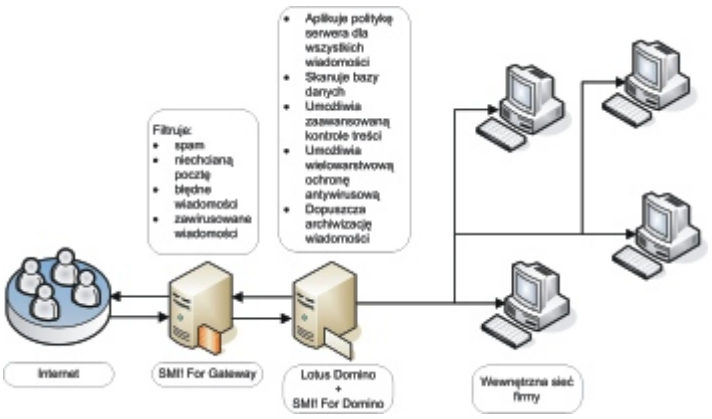
Poczta elektroniczna

Secure Mail Intelligence!® for Domino został stworzony dla wszystkich serwerów IBM Lotus Domino. Praca tego systemu polega na poddaniu kilkustopniowej analizie każdej wiadomości e-mail przechodzącej przez serwer:

:: ochrona antyspamowa i firewall – ochrona realizowana przez moduł zainstalowany przed serwerem Domino,
:: rozpoznawanie polityki – system rozpoznaje właściwą dla każdej wiadomości politykę opierając się na regułach między innymi nadawcy, odbiorcy, domenie, własnoręcznie zdefiniowanej formule Domino,
:: dzielenie wiadomości na podstawie zdefiniowanych kryteriów – identyfikuje treść i typ pliku na podstawie zbioru gotowych wzorców lub dodanych przez użytkownika,
:: analiza zawartości wiadomości – skanuje wiadomości pod kątem zawartości wirusów, używając wybranych przez administratora silników antywirusowych, usuwa zainfekowane załączniki, analizuje treść, dołącza stopki itp.,
:: klasyfikacja i przetwarzanie wiadomości – wybiera właściwą dla danej wiadomości ścieżkę, w zależności od zakwalifikowania do odpowiedniej polityki np. blokuje lub dostarcza wiadomość, usuwa załączniki, wysyła powiadomienie do nadawcy lub administratora itp.

Bazy danych

Secure Mail Intelligence!® for Domino analizuje również bazy danych IBM Domino Lotus. Program uruchamia się zgodnie z wcześniej zdefiniowanym harmonogramem lub w czasie rzeczywistym.



Rodzina produktów **Secure Mail Intelligence!®**

:: Secure Mail Intelligence!® for Gateway
:: Secure Mail Intelligence!® for Domino
:: Secure Mail Intelligence!® for Exchange
:: Secure Mail Intelligence!® Managed Service
:: Secure Mail Intelligence!® Encryption Key Manager

PODSUMOWANIE

Secure Mail Intelligence!® for Domino przeciwdziała lukom w zabezpieczeniach przez zastosowanie kompleksowej ochrony treści dla wiadomości zewnętrznych i wewnętrznych oraz dokumentów baz danych Domino

Jest najprostszym rozwiązaniem zabezpieczającym przed całym spektrum zagrożeń:

- blokuje niepożądane i niebezpieczne wiadomości
- blokuje wyciek informacji
- uniemożliwia przesyłanie niedozwolonych plików i dokumentów zawierających np. treści o charakterze seksualnym i rasistowskim
- zwiększa wydajność pracy przez eliminację nadużyć mailowych
- zabezpiecza przed spadkami wydajności sieci i zużywaniem przestrzeni dyskowej
- dzięki politykom bezpieczeństwa wymusza przestrzeganie określonych zasad w korporacji

Ready for IBM Lotus. Domino. software

Wymagania techniczne

- IBM Lotus Domino wersja 6.0 lub wyższa
- Microsoft Windows 2000/2003 Server lub nowszy
- Linux (i586 Intel lub w 100% kompatybilne w tym Red Hat, Fedora i SuSE, glibc w wersji 2.5)
- co najmniej 512 MB pamięci RAM dla każdej instancji SMI!
- 140 MB wolnego miejsca na dysku + ok. 500 MB na przetwarzane listy
- procesor Pentium III 800 MHz lub szybszy (lub odpowiednik)

M2 NET
+48 22 311 18 18, www.m2net.pl