

Ryzyko wycieku poufnych firmowych informacji przez e-mail, przypadkowo czy też przez działanie malware, to jedno z najgroźniejszych niebezpieczeństw dzisiejszych firm. Nie jest łatwo znaleźć rozwiązanie które zabezpieczy komunikację email skutecznie a jednocześnie w prosty sposób.

Mimo, że istnieje możliwość zaszyfrowania i podpisania wiadomości przy użyciu klienta poczty, pracownicy muszą znać jak właściwie z takiego rozwiązania korzystać. W konsekwencji, ciągła implementacja firmowych polityk bezpieczeństwa silnie zależy od wiedzy i dyscypliny indywidualnego pracownika – nie jest to ani praktyczne, ani skuteczne.

Sophos SafeGuard MailGateway upraszcza ochronę email dzięki integracji procesów kryptograficznych zaangażowanych w procesy szyfrowania/odszyfrowania a także podpisu elektronicznego i jego weryfikacji w jeden punkt firmowej sieci. Takie rozwiązanie gwarantuje pełną transparentność pracy dla użytkownika i automatyczną implementację wewnętrznych polityk bezpieczeństwa dla komunikacji e – mail. Nadawca i odbiorca mogą porozumiewać się za pomocą wiadomości elektronicznych tak, jak robili to do tej pory bez obaw o poufność wymienianych treści.

Aby zaszyfrować lub odszyfrować wiadomość i wygenerować podpis elektroniczny SafeGuard MailGateway korzysta ze standardów S/MIME i OpenPGP Internet.

Dla odbiorców, którzy nie posiadają infrastruktury zabezpieczającej email, innowacyjny SafeGuard PDFMail automatycznie przekształca wiadomość, wraz z załącznikiem, w zaszyfrowany plik PDF. Taki plik jest następnie przesyłany w wiadomości do odbiorcy gwarantując bezpieczeństwo transmisji danych.

Odbiorca nie wymaga niczego więcej poza oprogramowaniem czytającym PDF i odpowiednim hasłem do odszyfrowania otrzymanego dokumentu. Załączniki zawarte w dokumencie PDF zachowują swój oryginalny format (np. .doc, .xls, .ppt), mogą zostać rozpakowane i zmodyfikowane. Następnie odbiorca może odesłać zaszyfrowaną odpowiedź korzystając ze zintegrowanej funkcji odpowiadania, dołączając także załącznik.

Alternatywnie, SafeGuard PrivateCrypto i SafeGuard WebMail mogą także zostać wykorzystane do ochrony zewnętrznej komunikacji sieci nieposiadających infrastruktury zabezpieczającej.

SafeGuard MailGateway jest rozwiązaniem skalowalnym – od małych instalacji, przez zapasowe po klastry sieci.

### SafeGuard MailGateway gwarantuje:

Prosty i bezpieczny sposób zabezpieczenia i autentykacji pracy opartej na wymianie email

Ciągle wzmocnienie firmowych polityk bezpieczeństwa dzięki implementacji szyfrowania i podpisu elektronicznego z jednej, centralnej lokacji

Automatyczne odszyfrowanie przychodzącej i wychodzącej poczty dla odbiorców wewnątrz firmowej sieci bądź zaszyfrowanie dla odbiorców zewnętrznych.

[www.sophos.com.pl](http://www.sophos.com.pl)

**Kluczowe funkcje****Bezpieczeństwo**

- Centralna implementacja polityk bezpieczeństwa dla szyfrowania email i podpisów na całą firmową sieć

- Elastyczne i granularne definiowanie reguł szyfracji i podpisów

- Wsparcie dla S/MIME, OpenPGP, SafeGuard PrivateCryptio, SafeGuard WebMail i SafeGuard PDFMail

- Zintegrowana autoryzacja certyfikatów (CA) dla automatycznego generowania kluczy i certyfikatów

- Możliwość skanowania wirusowego zaszyfrowanych wiadomości

- Idealne rozszerzenie dla systemów ILP i CMF

**Uproszczone wdrożenie**

- Szybka instalacja i dystrybucja za pomocą koncepcji software appliance
- Bezproblemowa integracja z istniejącą infrastrukturą PKI i email
- Integracja key server dla S/MIME i OpenPGP
- Zintegrowany z Company Director Services jak Microsoft Active Directory
- Alternatywna metoda szyfrowania email bez potrzeby certyfikowania infrastruktury
- Niezależny od serwera pocztowego jak Lotus Notes, Microsoft Exchange itp.
- Skalowalny – od małych instalacji po klastry sieciowe

**Uproszczona praca**

- Transparentny dla użytkownika
- Interoperacyjny ze standardami bezpieczeństwa email
- Centralny zestaw reguł i zarządzania kluczami dla bezpiecznego ruchu pocztowego
- Wygodny i intuicyjny interfejs administracyjny
- Prosta skalowalność, migracja i utrzymanie

**Kluczowe korzyści****Bezpieczeństwo**

Ochrona cennych informacji firmowych i osobistych w wymianie wiadomości

Skalowalne, centralne rozwiązanie zabezpieczające do wykorzystania w infrastrukturze pocztowej opartej na

**SMTTP**

Elastyczne i szczegółowo definiowane zestawy reguł

Elastyczne i szczegółowo definiowane zestawy reguł

Wsparcie dla S/MIME, OpenPGP, SafeGuard PrivateCryptio, SafeGuard

WebMail i SafeGuard PDFMail (SafeGuard PDF Mail, SafeGuard

PrivateCryptio i SafeGuard WebMail to rozwiązania do komunikacji bez wsparcia dla S/MIME lub OpenPGP)

Automatyczne szyfrowanie i rozszyfrowywanie oraz podpis elektroniczny

Automatyczne generowanie kluczy i certyfikatów dla S/MIME i OpenPGP

Zintegrowany key server dla S/MIME i OpenPGP

Zintegrowany system zabezpieczający

Wsparcie dla usług directory i key server

**Wymagania systemowe****Hardware**

- Intel CPU
- Minimum 512 MB RAM
- Twarde dyski IDE/SCSI/SATA
- Napędy CD – ROM

**IDE/SCSI/USB**

- Adapter sieci Ethernet

**Opcje systemowe****System operacyjny**

- CentOS
- Wsparcie Vmware

**Instalacja**

Kompletna instalacja z CD – ROM

**Zarządzanie**

Zarządzanie webowe wraz ze szczegółowym wsparciem online