SEPPMAIL
SWISS E-MAIL SECURITY

PRZYKŁAD LICENCJI

Przykład:

Załóżmy że firma zatrudnia 100 osób. 50 z nich jest zobąwiązana do szyfrowania wiadomości e-mail dla bezpieczeństwa wymiany poufnych danych drogą mailową.

Z niektórymi odbiorcami firma może wymieniać zaszyfrowane wiadomości przy użyciu standardowego szyfrowania, inni odbiorcy nie posiadają żadnej technologii szyfrowania.

Firma chce również używać ochrony przed Malware oraz Spamem razem z bramkami szyfrowania poczty. Oczekuje gwarancji, wsparcia technicznego a usługi powinny trwać 12 miesięcy.

Krok 1: Wybór odpowiedniego urządzenia podstawowego.

SEPPmail oferuje dwa różne rodzaje podstawowej platfomy bramki email.

- Urządzenie sprzętowe
- Wirtualne urządzenie
  - ESX / VMware
  - Hyper-V / Microsoft
  - Hyper Hat / RedHat
  -- (Xen nie jest obsługiwane)

Nasza firma wybiera wirtualne urządzenie jako platformę w postaci rozwiązania SEPPmail.

Tutaj: Dla 50 użytkowników korzystających z szyfrowania poczty elektronicznej wybieramy licencję 1 x SEPP-VM500 wraz z obowiązkowym pakietem Care Pack* SEPP-8-500VM-MS-12. Ta podstawowa licencja posiada możliwości szyfrowania poprzez TLS lub używa szyfrowania domeny.

Jeśli nasza firma chce skonfigurować bramkę w trybie wysokiej dostępności stosując klaster, jest zobowiązana do dodania drugiej licencji oraz odpowiedniego Care Pack.

Krok 2 (opcjonalnie): Wybranie licencji szyfrowania.

Dla każdego użytkownika poczty z własnym adresem e-mail, którego chcesz używać do szyfrowania potrzebujesz jednej licencji.

Tutaj: Mamy do wyboru licencję 50 x SML-50-99 wraz z obowiązkowym pakietem Care Pack SMS-8-50-99-12. Licencja szyfrowania klienta zawiera szyfrowanie przez S/MIME, OpenPGP oraz “GINA”.

Do podstawowych funkcji szyfrowania idź do (-> Krok 1).

Krok 3 (opcjonalnie): Dodanie Self Service Password Management (SSPM) do szyfrowania GINA.

Szyfrowanie GINA jest metodą SEPPmail która zapewnia bezpieczną wymianę e-maili z odbiorcami, którzy nie mogą korzystać z norm, takich jak TLS, S / MIME i OpenPGP. Metoda ta jest metodą internetową, w której użytkownik może uzyskać dostęp do jego odbiorcy dzięki interfejsowi GINA. Dostęp jest chroniony hasłem. W przypadku gdy użytkowinik zapomni swoje hasło, musi skontaktować się z administratorem naszej firmy, aby zresetować hasło do tego adresata. Z włączoną opcją zarządzania hasłami (SSPM) odbiorca może sam zresetować hasło. SSPM musi być licencjonowane w takiej samej ilości, pozwoleń szyfrowania klienta idź do (-> krok 2).

Tutaj: Musimy dodać licencję 50 x SSPM-50-99. Za SSPM płacimy jednorazową opłatę, bez wykupowania pakietu Care Pack.

Krok 4 (opcjonalnie): Antywirus i antyspam (pakiet ochronny).

Wybór licencji jest odpowiedni do wybranego urządzenia podstawowego. Jest to opłata abonentowa, która jest odnawialna po każdym okresie rozliczeniowym. Jeśli klient chce dodać kolejne urządzenie z powodu wysokiego wykorzystania oraz posiada aktywne AV / AS - pakiet ochronny powinien być zamówiony dwukronie.

Tutaj: mamy do wyboru licencję 1 x SM-VSPP-500-12 dla 12-miesięcznej subskrypcji.

*Care Pack (ang.) - pakiet pomocy.

SEPPMAIL
SWISS E-MAIL SECURITY

Czy chcesz przetestować to rozwiązanie?

Pozwól sobie przysłać mail testowy z naszej strony internetowej:

www.szyfrowanie-poczty.pl

Poprzez demo online lub skontaktuj się ze mną:

Jan Zyber
eSafety Solutions
(+48) 32 32 311 96
kontakt@szyfrowanie-poczty.pl