

SEPPmail®

Die wichtigsten Vorteile von SEPPmail auf einen Blick

August 2008

Inhalt

Die wichtigsten Vorteile von SEPPmail auf einen Blick	3
Enhanced WebMail – Technologie.....	3
Domain Encryption.....	5
Queue-less Betrieb.....	5
Vorteile einer Appliance	6
Hochverfügbarkeit	7
Verbreitung.....	7

Die wichtigsten Vorteile von SEPPmail auf einen Blick

Enhanced WebMail – Technologie

Das Hauptproblem beim Versenden von sicheren E-Mails ist, dass die Gegenseite in der Regel (noch) keine „Standard“- Verschlüsselung wie PGP oder S/MIME im Einsatz hat. Eine Secure E-Mail – Lösung muss deshalb eine Möglichkeit bereitstellen, auch mit Kommunikationspartnern ohne vorhandene Verschlüsselungslösung zu kommunizieren.

SEPPmail bietet eine patentierte Technologie, die eine sichere Kommunikation mit beliebigen Empfängern ermöglicht.

Diese Technologie verlangt nur, dass ein Web-Browser und eine Möglichkeit E-Mails zu empfangen vorhanden ist. Weitere Anforderungen an die Infrastruktur des Benutzers bestehen nicht.

Soll der Benutzer ein „Enhanced WebMail“ erhalten, so verschlüsselt SEPPmail die Nachricht und schickt dem Benutzer diese Nachricht in einem html-Mail. Der Benutzer öffnet den html-Anhang und die verschlüsselte Meldung wird automatisch an den SEPPmail Server transportiert. Nach Eingabe des Passworts, das der externe Empfänger bei der Registration selber vergeben hat, wird ihm der Inhalt der E-Mail angezeigt.

Der Vorteil dieses Verfahrens liegt auf der Hand: wie bei allen WebMail Lösungen sind die Anforderungen an die Infrastruktur des Empfängers minimal. Im Gegensatz zu anderen Systemen ist die Sicherheit aber deutlich höher: Dadurch, dass für den Zugriff auf die Daten das Passwort alleine nicht mehr genügt, sondern die Mail-Meldung zusätzlich notwendig ist, schlagen die üblichen Phishing-Methoden fehl – ganz im Gegensatz zu den üblichen Secure Web-Mail Lösungen, die gegen Phishing Methoden konzeptbedingt machtlos sind.

Ein weiterer Vorteil liegt auf der Seite des Betreibers: Dadurch dass die E-Mail im Mail-Client des externen Benutzers gespeichert ist und nicht auf seiner eigenen Infrastruktur, sind die Anforderungen an benötigtem Speicherplatz sehr bescheiden. Würden diese E-Mails auf der Infrastruktur des Betreibers gespeichert, müsste er jedes Jahr zusätzliche Festplatten anschaffen und immer grössere Mengen von Daten archivieren. Oder der Betreiber würde die Benutzer verärgern, in dem deren E-Mails regelmässig gelöscht würden. Sind die E-Mails im Mail-Client des externen Benutzers abgespeichert, existieren diese Probleme nicht. Der Empfänger ist selber

für alle Backup-Massnahmen zuständig und besitzt zusätzlich die Kontrolle über seine Daten.

	Normales "secure Webmail"	PDF-Verschlüsselung	Selbstextrahierendes Archiv	Spezieller Client	SEPPmail mit "enhanced secure Webmail"
Keine Speicherung ausgehender E-Mails					✓
Phishing-Resistent					✓
Resistent gegen Brute Force – Attacken					✓
„Eingeschriebenes E-Mail“ möglich					✓
Keine Installation beim Empfänger					✓
Auf den gängigen Plattformen lesbar					✓
"Two-Factor Authentication"					✓

Wie aus der Tabelle ersichtlich wird ist es nicht unproblematisch eine „normale“ Secure WebMail-Lösung zu betreiben. Abgesehen davon, dass diese Systeme alle ausgehenden verschlüsselten E-Mails zwischenspeichern müssen, sind sie vor allem eines nicht - sonderlich sicher ! Ein Secure WebMail ist mit einer Phishing-Attacke relativ einfach auszuhebeln und bietet damit ein erhöhtes und seit langem auch bekanntes Angriffsrisiko. Vor allem Firmen im Bankenumfeld, die einem ausgeprägten Phishing-Risiko ausgesetzt sind, profitieren deshalb ausserordentlich von der zusätzlichen Sicherheit, die das patentierte „Enhanced Secure Webmail“ von SEPPmail bereitstellt.


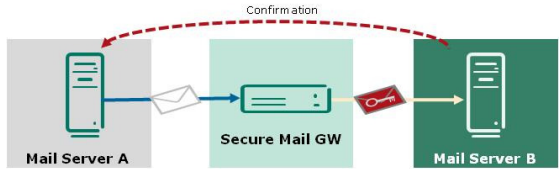
Domain Encryption

Zwischen SEPPmail-Geräten kann der gesamte E-Mail-Verkehr automatisch und für den Benutzer vollständig transparent verschlüsselt werden. Schon heute sind mehr als 300 Domänen an dieses „E-Mail-VPN“ angeschlossen. Jede neue SEPPmail Installation kann – muss aber nicht – an diesem Verbund teilnehmen – ohne Konfiguration oder Schlüsselmaterial-Austausch.

Selbstverständlich können auch Domain-Keys anderer Hersteller – ob PGP oder S/MIME - eingebunden werden.

Queue-less Betrieb

SEPPmail hat eine einzigartige Funktionsweise, bei der E-Mails nie in einer Queue zwischengespeichert werden. Dies führt zu einer erheblichen Erleichterung bei der Fehlersuche im Mailsystem. Ausserdem kann eine Appliance bei Hardwareausfall garantiert ohne Datenverlust ausgewechselt werden.

<p>Funktionsweise anderer Secure Mail Lösungen (bei SEPPmail ebenfalls implementiert)</p>	<p>Queue-Less Betrieb von SEPPmail.</p>
<p>Normalerweise sind Secure E-Mail – Lösungen wie „normale“ Mailserver aufgebaut. Der schrittweise Ablauf beim Verarbeiten von E-Mails sieht deshalb folgendermassen aus:</p>	<p>Um ein wirklich sicheres Clustering zu ermöglichen, beherrschen die SEPPmail-Appliances deshalb einen speziellen „Queue-less“ Modus. Die Verarbeitung der E-Mails erfolgt dann nach folgendem Ablauf:</p>
	
<ul style="list-style-type: none"> ▶ Mailserver A sendet ein E-Mail an das Secure E-Mail Gateway ▶ Der Secure E-Mail Gateway empfängt das E-Mail und bestätigt Mail- 	<ul style="list-style-type: none"> ▶ Mailserver A sendet ein E-Mail an den Secure E-Mail Gateway ▶ Der Secure E-Mail Gateway empfängt das E-Mail. Das E-Mail wird

<p>server A den Empfang</p> <ul style="list-style-type: none"> ▶ Das E-Mail wird vom Ent- bzw. Verschlüsselungsmodul des Secure E-Mail Gateways verarbeitet. Nach der Verarbeitung wird das Mail an die lokale Mailqueue des Secure E-Mail Gateways weitergegeben. ▶ Die lokale Mailqueue liefert die zwischengespeicherten E-Mails sequentiell an Mailserver B aus 	<p>vom Ent- bzw. Verschlüsselungsmodul des Secure E-Mail Gateways verarbeitet. Nach der Verarbeitung wird das E-Mail an Mailserver B weitergegeben.</p> <ul style="list-style-type: none"> ▶ Erst jetzt wird Mailserver A der Empfang des E-Mails bestätigt. Während der gesamten Transaktionszeit ist für Server A die Übertragung im Prozess.
<p>So werden im normalen Betrieb immer E-Mails auf dem Secure E-Mail-Gateway zwischengespeichert. Ein Clustering der lokalen Queue ist hingegen technisch kaum realisierbar. Bei einem Ausfall eines Gerätes in einem Secure E-Mail Gateway-Cluster muss daher damit gerechnet werden, dass E-Mails verlorengehen.</p>	<p>Bei einem Ausfall eines Gerätes eines SEPPmail-Clusters gehen durch diese Funktionsweise nie E-Mails verloren. Ausserdem wird die Fehlersuche einfacher, da bei einem „vermissten“ E-Mail nur die Logs der Mailserver A und B berücksichtigt werden müssen.</p>

Vorteile einer Appliance

Durch den Appliance – Ansatz ist die Installation von SEPPmail extrem rasch und unkompliziert durchgeführt. Updates sind einfach durchzuführen und bereiten keine Probleme.

Die SEPPmail Appliance basiert auf spezialisierter Serverhardware mit redundanter Stromversorgung und mehrfach vorhandenen Lüftern. Darauf aufbauend ist ein stark gehärtetes OpenBSD UNIX System mit der SEPPmail Applikation installiert.

Diese Kombination von Hardware und Software, zusammen mit dem Multimaster LDAP Clustersystem, ist Garant für höchste Stabilität und 100-prozentige Verfügbarkeit.

Hochverfügbarkeit

Hochverfügbarkeit ist, insbesondere im unternehmenskritischen Umfeld der E-Mail – Kommunikation, unabdingbar. Dem Thema „Cluster“ wird bei SEPPmail deshalb besonders viel Beachtung geschenkt.

Clustering ist eine Grundfunktion von SEPPmail. Ein neues Gerät ist innert Minuten in einen bestehenden Cluster integrierbar, und ein defektes Gerät ist innert Minuten ersetzt. Da auf einer SEPPmail-Appliance generell nie E-Mails gespeichert werden, ist ein sehr effizientes Clustering möglich, praktisch in Real-Time auch auf einen entfernten Standort über eine „langsame“ Leitung.

Das Clustering ist zweistufig: Einerseits wird die im Gerät integrierte LDAP-Datenbank auf jedes Mitglied des Clusters repliziert. Somit hat jede Instanz alle Daten praktisch verzögerungsfrei zur Verfügung. Andererseits kann ein beliebiges Gerät die IP-Adresse eines anderen automatisch übernehmen, falls dieses ausfällt. Ebenso können natürlich die bestehenden und bewährten Fail-Over Funktionen der Mail-Systeme weiter eingesetzt werden.

Die Inbetriebnahme eines neuen Clustermitgliedes geschieht in wenigen Schritten:

- ▶ Aufstarten des neuen Gerätes, Einstellen der Netzwerkparameter (IP, ev. Failover-IPs, Gateway, DNS etc.)
- ▶ Export der Cluster-Credentials per WebGUI eines bestehenden Mitgliedes des Clusters
- ▶ Angabe der IP eines bestehenden Mitgliedes des Clusters und Hinaufladen der Cluster-Credentials auf dem neuen Gerät
- ▶ Das neue Gerät ist betriebsbereit.

Da nie E-Mails auf einem Gerät gespeichert werden („Queue-less Betrieb“) kann bei einem Ausfall eines Gerätes kein Datenverlust auftreten.

Verbreitung

SEPPmail ist die in der Schweiz heute am meisten eingesetzte Lösung. Sie können auf mehr als 20 geschulte Integrationspartner in der Schweiz zählen.