

Forslag til system for automatisk kryptering av utgående sensitiv e-post v/Erik Skinstad Infinigate AS.

Bakgrunn:

Datatilsynet har vurdert at lønsslipp som inneholder fødselsnummer må være kryptert om den sendes pr e-post. Tidligere har Datatilsynet uttalt at dersom lønsslipp sendes i åpen e-post kan den ikke inneholde fødselsnummer. Skattedirektoratet på sin side sier at lønsslipp må inneholde fødselsnummer for å tilfredsstille skattebetalingsforskriften.

<http://norsis.no/nyheter/2010-02-24-Lonsslipp-kryptert-e-post.html>

Lønsslippar kan berre sendast på kryptert e-post

Datatilsynet har tidlegare meint at arbeidsgjevarar må utelate fødselsnummer for lønsslippar sendt i e-post. Etter at fleire arbeidsgjevarar har fått reaksjonar frå skattestyresmaktene, har Datatilsynet innhenta ei avklaring i saka.

http://www.datatilsynet.no/templates/Page_3349.aspx

Skattebetalingsforskriften § 5-10-20 første ledd oppstiller krav til hvilke opplysninger dokumentasjonen (lønsslippen) til skattyter skal inneholde. Det fremgår direkte av bestemmelsen at skattyters fødselsnummer skal fremgå av dokumentasjonen. **En lønsslipp som ikke inneholder fødselsnummer er derfor i strid med bestemmelsen.** Bestemmelsen inneholder ikke krav om opplysninger om bankkontonummer, slik at en utelatelse av denne opplysningen er ikke i strid med bestemmelsen.

<http://www.datatilsynet.no/upload/Skattedirektoratet.pdf>

Dette kan løses på forskjellige måter, i mitt oppsett har jeg tatt hensyn til at mottaker av kryptert epost ikke skal behøve å installere spesialprodukter, men kun benytte adobe PDF leser for å lese kryptert epost. Løsningen vil være fleksibel for å lage eget regelsett for kryptering.

Jeg har valgt å benytte Symantec Brightmail epost filter som epostfiltrering, og Sophos (Utimaco) Secure email gateway for kryptering. Epost klient er Outlook, epost server er Exchange.

Løsningen er helt epost klient og epost server uavhengig.

For mer informasjon, kontakt



Erik Skinstad
Systems engineer

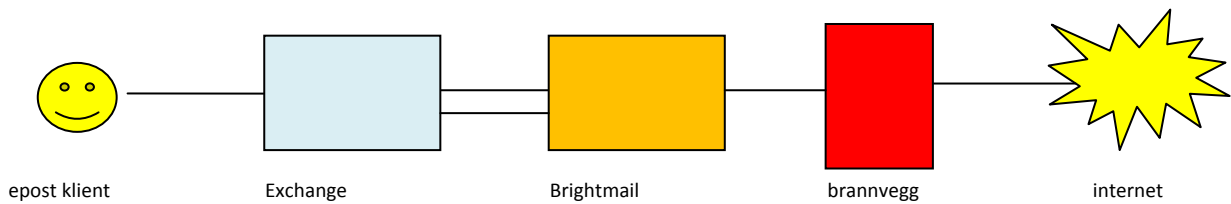
Infinigate Norge AS
Martin Linges Vei 17
N-1367 Snarøya

Phone +47 67 10 18 00
Fax +47 67 58 15 60
Mobile: +47 93 01 68 18

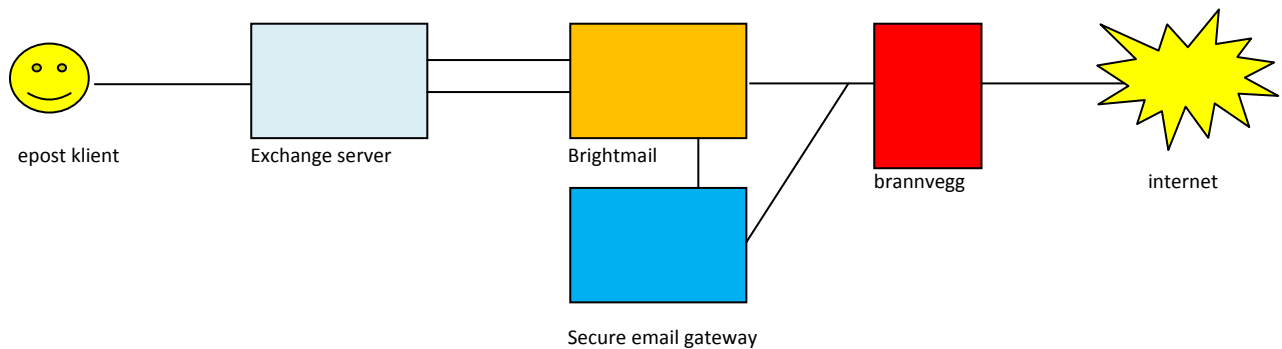
erik.skinstad@infinigate.no
www.infinigate.no
[Map](#)

erik.skinstad@infinigate.no

I oppsettet mitt fantes det allerede en Microsoft Exchange server og en Symantec Brightmail. Brightmail blir benyttet til å filtrere inngående og utgående epost for spam og virus.



I dette oppsettet introduserte jeg en Sophos (Utimaco) Secure email gateway, eksisterende oppsett er urørt.



Med innebygget funksjonalitet i Brightmail, sjekker jeg utgående epost for direktiver for kryptering. Direktiver kan eksempelvis være ord i emnefeltet. For å styre epost som skal krypteres til Secure email gateway introduserte jeg noen direktiver som bestemmer hvilke eposter som skal krypteres. I mitt oppsett valgte jeg – hvis følgende ord er i emnefeltet i eposten skal eposten krypteres: "lønsslipp" eller "pdfkrypt". Så et emnefelt i epost "lønsslipp for oktober" eller "Her kommer tilbudet pdfkrypt" vil bli kryptert. I det siste eksemplet er det brukeren selv som bestemmer at denne eposten skal krypteres ved å legge til pdfkrypt i slutten av emnelinja.

Endringer ved ny funksjonalitet:

epost klient

Ingen, men gir brukeren mulighet til å kryptere utgående epost med å legge til "pdfkryp" i slutten av emnelinja.

exchange server

Ingen.

Brightmail

Ingen endring, men tar i bruk funksjonalitet som sjekker emnelinje i eposten. Ved treff på disse, sendes mailen via Secure email gateway.

Brannvegg.

Tillater Secure email gateway å sende epost ut på port 25.


Mer om Symantec Brightmail.

I tillegg til å være en av markedets beste løsning for antivirus og antispam for epost, er det moduler for Compliance. Denne modulen kan benyttes til å sikre at epost bruk er i samsvar med retningslinjer og standarder som eks. HIPAA (including PHI) . Denne kan også benyttes til egendefinert sjekk av innhold, slik som i mitt eksempel hvor jeg innfører regler for kryptering av epost.

eks :

Email Content Compliance Policies						
Manage Email Content Compliance filter policies for your organization.						
Add	Edit	Delete	Move Up	Move Down	Enable	Disable
<input type="checkbox"/>	Email Content Compliance Policies				Enabled	Applied To
<input type="checkbox"/>	Delete Executable Files Violations				✓	Outbound only
<input type="checkbox"/>	Delete Email Policy Violations				✓	Outbound only
<input type="checkbox"/>	Legal Disclaimer				✓	Outbound only
<input type="checkbox"/>	Delete True Type Executable Files Violations				✓	Outbound only
<input type="checkbox"/>	pdfmail				✓	Outbound only

fra filter pdfmail:

<input type="checkbox"/> Conditions	
<input type="checkbox"/> If text in Subject part of the message contains 1 or more occurrences of "pdfmail"	
Actions	
Perform the following action:	
[Select an action]	
<input type="button" value="Add Action"/>	
<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="checkbox"/> Actions	
<input type="checkbox"/> Route the message to *12345678901.88:25*	

Mer om Sophos (Utimaco) Secure email gateway .

Denne gatewayen kan kryptere epost med flere metoder, den har kryptering med S/MIME, OpenPGP, Utimaco Private Crypto og Kryptert PDF.

S/MIME:

Krever distribusjon av digitale sertifikater. For utstedelse av disse er det en CA innebygget i serveren hvis man ikke har en PKI på plass fra før.

OpenPGP:

Denne krever utveksling av nøkler.

Utimaco Private Crypto:

Denne krever installasjon av Utimaco Private Crypto hos mottaker av kryptert epost.

Kryptert PDF:

Ved å benytte denne krypteringen, vil mottaker kunne lese denne i Adobe Acrobat. Denne finnes allerede hos de fleste mottakere.

Resten av denne beskrivelsen vil forholde seg til kryptert PDF på et overordnet plan.

For å kryptere epost, vil man måtte forholde seg til hva (hvilken epost), avsender (har denne brukeren tilgang til å kryptere) mottaker (hvilken nøkkel skal benyttes for kryptering) .

Hva:

Denne belutningen er allerede tatt i Brightmail siden eposten er sendt til denne serveren.

Avsender:

Brukere som skal benytte kryptering må være registrert i serveren. Dette kan gjøres i server, eller man kan importere fra AD.

Mottaker:

eks: erik.skinstad@infinigate.no. Her er erik.skinstad mottaker i domene infinigate.no.

Her bestemmes krypteringsnøkkel. Det kan lages faste eller tilfeldige krypteringsnøkler for mottakere, grupper av mottakere, domener, eller for alle mottakere i alle domener. Hvis man benytter tilfeldig nøkkel, vil eposten sendes kryptert til mottaker og den tilfeldige nøkkelen som er generert vil sendes til avsender av eposten. Avsender vil måtte kommunisere denne nøkkelen til mottaker slik at denne vil kunne åpne eposten. PDF dokumentet som sendes, vil sendes som vedlegg. Ved åpning av dette vil bruker bli spurt etter passord. Ved riktig passord, vil dokumentet åpnes i Acrobat. Ved krypteringen vil server legge til en forside i PDF dokumentet (cover sheet), bruker vil måtte bla ned i dokumentet for å lese innhold. Vedlegg leses ved å trykke 'bindersens' i Acrobat.