

INSTANT MESSAGING SECURITY SERVICE

WAT ANALISTEN ERVAN ZEGGEN

"Gebleken is dat IM in zakelijke scenario's als callcenters of situaties waarin tijd van cruciaal belang is, een zeer effectief hulpmiddel is voor de verspreiding van informatie en het snel oplossen van problemen"

Gartner MarketScope voor Instant Messaging, 2007

"Er is en blijft een markt voor een gebruiksvriendelijke beveiligingsoplossing voor openbaar IM."

Osterman Research, Presence, IM and Real Time Communication Trends, 2007-2010, 2007

KUNT U DE VOORDELEN VAN IM GEBRUIKEN EN DE GEVAREN ERVAN VERMIJDEN?

Omdat IM (Instant Messaging) directer is dan e-mail en veelzijdiger dan de telefoon, kan het de snelheid, het gemak en de efficiency van zakelijke communicaties aanzienlijk verbeteren. Door de vele voordelen is communicatie via IM een van 's werelds snelst groeiende internetmedia geworden. En de verwachting is dat het totale aantal gebruikers in 2009 de 1 miljard zal overschrijden. In het bedrijfsleven neemt het gebruik van expresberichten – vooral het ongecontroleerde gebruik ervan – heel snel toe, wat in gelijke tred is met deze wereldwijde trend.

Door het ongecontroleerde gebruik, bevoegd of onbevoegd, van openbare IM-netwerken bent u blootgesteld aan risico's die de productiviteit, winstgevendheid, bedrijfscontinuïteit en het klantvertrouwen in gevaar kunnen brengen. En dit is niet alleen een kwestie van potentiële problemen als gevolg van malware die via expresberichten wordt verspreid. Ook onbedoelde of opzettelijke gegevenslekage, oneigenlijk gebruik en onwettelijk gebruik zijn gevaren waarmee zeker rekening gehouden moet worden.

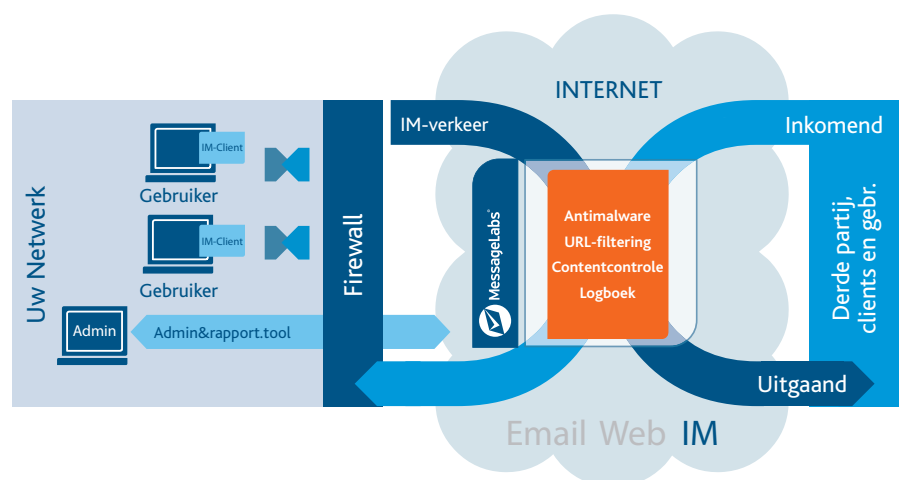
MessageLabs Instant Messaging Security Service (IMSS) kan uw werknemers helpen de openbare IM-netwerken veilig te gebruiken. Door zijn functionaliteit op het gebied van bescherming en beheer kunt u volledig en met meer vertrouwen profiteren van de interne en externe realtimecommunicatie via compatibele openbare IM-systemen, en de werkdruk van uw IT-team verlichten.

IMSS helpt de kosten, complexiteit en beperkingen van interne oplossingen op basis van software en hardware te vermijden. Bovendien biedt het bewezen mogelijkheden om te voldoen aan de urgente behoefte van het tegenwoordige bedrijfsleven aan een veiliger, beter beheersbaar en controleerbaar gebruik van openbaar IM.

MESSAGELABS – HET VERSCHIL

- Een unieke en uitgebreide service voor de beveiliging, de beheersing en het beheer van expresberichten, met gebruikmaking van bewezen technologie en expertise.
- De implementatie van eigen Skeptic™-technologie die maatstaven biedt voor de bescherming tegen nieuwe, opkomende en samengestelde bedreigingen.
- Maximale functionaliteit gecombineerd met minimale onderhoudsvereisten.
- Een toonaangevende klantenondersteuning die wereldwijd 24 uur per dag, 7 dagen per week voor u klaar staat.
- Een intuïtieve mogelijkheid voor het opzetten van beleid is onderdeel van de service.
- Lage eigendomskosten vergeleken met interne oplossingen op basis van software of hardware.

IM ALS PLUSPUNT, NIET ALS RISICO – MESSAGELABS INSTANT MESSAGING SECURITY SOLUTION



Deze volledig beheerde en volledig aanpasbare service biedt een uitgebreide, kosteneffectieve verzameling moderne mogelijkheden, waaronder antimalware, URL-filtering, contentbeheer, berichtregistratie en -rapportage. IMSS is niet alleen snel en handig in te stellen en te gebruiken, het is ook eenvoudig toe te passen via een gebruikersvriendelijke webportal.



HOE WERKT DE SERVICE?

- Elk expresbericht naar of afkomstig van uw organisatie wordt door onze infrastructuur gevoerd.
- Inkomende berichten (inclusief tekstbestanden of andere bijlagen) worden onmiddellijk en uitgebreid gescand op:
 - bekende en onbekende virussen, wormen, trojaanse paarden en andere malware
 - weblinks die leiden naar websites die met malware zijn geïnfecteerd.
- Alle inkomende en uitgaande berichten worden vergeleken met uw controleregels en beleidsregels voor aanvaardbaar gebruik van IM.
- Berichten die schadelijk of verdacht zijn, of de beleidsregels schenden, worden automatisch geblokkeerd.
- Alle andere berichten gaan naar de IM-inbox van de beoogde ontvanger zonder dat enige vertraging merkbaar is.
- Elk bericht wordt veilig in onze beveiligde infrastructuur geregistreerd.

MESSAGELABS IN DE PRAKTIJK

- Gebruikers van expressberichten: de MessageLabs-service veroorzaakt geen merkbare vertraging in de aflevering van expressberichten en geen ondermijning van IM-functionaliteit
- T-managers: IMSS biedt volledige controle over (en volledig inzicht in) het gebruik van expressberichten in uw bedrijf. De service werkt ook naadloos samen met onze services voor e-mail/webbeveiliging en enterprise IM.
- Servicebeheerders: IMSS is eenvoudig te beheren via een enkele webportal; een uitgebreide

DE VOLGENDE STAP

Contact met een productspecialist:
Nederland: +31 (0)20 799 7929
info@messagelabs.com

Zie voor vestigingen en telefoonnummers in andere landen: www.messagelabs.nl/contact

IMSS draait op ons bewezen, ondernemingsgerichte en wereldwijde webbeveiligingsplatform. Al uw inkomende, uitgaande en interne expresberichten (inclusief bijlagen) worden door een ultramoderne en uitgebalanceerde infrastructuur gevoerd, die de best mogelijk beveiliging en controle mogelijkheden biedt. U kunt ook heel eenvoudig firewallregels toevoegen die voorkomen dat uw medewerkers de service kunnen ontwijken.

Een bericht/bijlage met malware wordt door onze scantorens geblokkeerd nog voordat het zelfs maar de grens van het netwerk van de beoogde ontvanger bereikt. Een belangrijke rol hierin is weggelegd voor Skeptic™, onze unieke voorspellingstechnologie die van elk expresbericht, elke e-mail en webpagina die het scant leert en zo constant zijn ongeëvenaarde detectiemogelijkheden verder uitbreidt.

Wanneer een bericht of bijlage een link naar een geïnfecteerde of ongeschikte website lijkt te hebben, of trefwoorden of uitdrukkingen bevat die u in uw controleregels opgeeft, wordt dit bericht of deze bijlage automatisch geblokkeerd. Hierdoor kunt u uw netwerk tegen infectie beschermen en uw medewerkers afschermen van ongeschikt materiaal dat van buiten uw organisatie afkomstig is, en bent u beschermd tegen onbedoelde of opzettelijke gegevenslekage en tegen onjuist gebruik van expresberichten door uw medewerkers.

Alle expresberichten worden in een logboek bijgehouden en kunnen naar uw bestaande archiveringsoplossing worden verzonden. Zo kunt u alle communicatie via openbare IM bijhouden, zodat uw gegevens altijd opvraagbaar zijn en u aan de regelgeving op dit gebied voldoet.

FUNCTIES EN VOORDELEN VAN IMSS

FUNCTIES	VOORDELEN
Werkt met AIM van AOL, Yahoo! Mail en Microsoft MSN.	Biedt veiliger en gecontroleerd gebruik van toonaangevende openbare IM-netwerken.
Leverd meerlaagse bescherming tegen bekende, nieuwe en samengestelde bedreigingen die via openbare IM-netwerken worden verspreid.	Dicht beveiligingsgaten in uw bedrijfsnetwerk door te voorkomen dat malware via expresberichten kan binnenkomen.
Bevat intuïtieve functionaliteit voor het opzetten van beleid, inclusief het stapelen van meerdere regels	Maakt het snel opzetten van beleid voor aanvaardbaar gebruik van IM, op groepsniveau of per gebruiker mogelijk.
Kan volledig worden geïntegreerd met directory's die aan LDAP voldoen.	Zorgt dat groepsgegevens altijd up-to-date zijn waardoor op beheertaken kan worden bespaard.
Bevat instelbare/aanpasbare regels en meldingen.	Zorgt dat aan uw specifieke behoeften kan worden voldaan zonder nadelige gevolgen voor de gebruikerservaring.
Het downloaden van een agent of software naar uw netwerk is niet nodig.	Eenvoudig in te stellen, te gebruiken en toe te passen.
Omvat een dashboard, samenvatting en gedetailleerde rapportage.	Is overzichtelijk, laat zien wie verantwoordelijk is en geeft vertrouwen in de effectiviteit van de service.