BLS CONSULTING
Consulenza e sviluppo informatico

SENDER ACCREDITATION

PERCHE' SERVE IL SENDERE ACCREDITATION?

Uno dei problemi di comunicazione più diffusi al giorno d'oggi nel mondo delle aziende riguarda la mancata consegna di email di lavoro perché scambiate per spam. Ciò comporta ritardi e fraintendimenti nelle comunicazioni verso clienti, fornitori e a volte persino tra rami della medesima azienda, con conseguenti disservizi, disagi e perdite economiche e di tempo.
La soluzione ideale a questo tipo di problema è l'implementazione di sistemi di SENDER ACCREDITATION.
Tali sistemi contribuiscono ad aumentare l'affidabilità del Sender (voi stessi) riducendo sensibilmente l'annoso problema di blocco per errore delle vostre email (falsi positivi). Un server ricevente potrà distinguere le email spedite effettivamente dai vostri server e utenti da quelle spam spedite da terzi. Di conseguenza le email che usurpano i vostri indirizzi verranno bloccate dai riceventi, mentre le vostre email passeranno indisturbate.

LA SOLUZIONE BLS

B.L.S. Consulting offre un sistema ottimale di SENDER ACCREDITATION, che include le più moderne soluzioni di Autenticazione delle email. Inoltre, non solo riduce sensibilmente i falsi positivi, ma include un monitoraggio dell'utilizzo del vostro nome da parte di terzi, permettendovi di provvedere a campagne spam a vostro nome che potrebbero ledere la vostra credibilità verso clienti e fornitori.
Interviene inoltre alla radice del problema dei falsi positivi, rilevando infezioni dei vostri pc da parte di virus che spediscono spam dalla vostra casella di posta, rendendola inutilizzabile, e intervenendo su pratiche errate che contribuiscono a far scambiare le vostre email per spam.

IL SISTEMA SI BASA SU:

D-KIM - DOMAIN KEYS IDENTIFIED MAIL

È un moderno sistema di autenticazione delle email che funziona sia a vantaggio di chi invia che di chi riceve.
Al momento dell'invio l'email viene autenticata con una firma criptata da un MTA (Mail Transfer Agent), che contiene le informazioni di "Header" della mail, in particolare il Dominio del mittente. Le chiavi pubbliche di decriptazione si trovano su un Server DNS specifico.
Al momento della ricezione, il MTA del destinatario rileva la presenza della firma D-KIM e ne verifica le chiavi pubbliche sul DNS, decriptando la firma e confrontandone le informazioni con quelle "in chiaro" dell'Header.

Se le informazioni corrispondono, la mail ha molte più probabilità di essere reale e dunque non scambiata per spam.
In assenza di firma D-KIM, il giudizio del ricevente rimane neutro, a meno che non sia presente una ulteriore autenticazione DMARC.
Informazioni non corrispondenti identificano immediatamente la mail come spam (possibilità piuttosto vaga, andando a totale scapito dello spammer).

SPF - SENDER POLICY FRAMEWORK

Molti Spammer falsificano il dominio delle email che inviano per renderle credibili agli occhi delle vittime.
SPF è un sistema che verifica che l'indirizzo IP del mittente dell'email ricevuta corrisponda a un HOST autorizzato a inviare posta per il dominio indicato nella mail. La lista degli HOST autorizzati viene pubblicata dal mittente su un Server DNS apposito.

D-MARC – DOMAIN BASED MAIL AUTHENTICATION, REPORTING AND CONFORMANCE

DMARC è un Sistema che si inserisce ottimamente in procedure di mail Authentication già presenti in un'azienda.
In questo caso si abbina molto bene con i precedentemente indicati DKIM e SPF.
Il sistema indica nelle mail che le mail inviate dal Dominio del mittente devono contenere obbligatoriamente le firme DKIM e SPF.
Contiene inoltre istruzioni sulle azioni da intraprendere automaticamente nel caso queste firme non siano presenti: si può infatti impostarlo in modo che le mail che non passino il controllo vengano eliminate direttamente, che siano messe in quarantena in attesa di istruzioni, oppure che vengano comunque accettate.
Una ulteriore, importante funzione del D-MARC è la reportistica: il proprietario del Dominio che lo ha implementato riceve Report periodici sulle email ricevute dalle varie caselle di posta dal suo dominio e senza le firme richieste.
Ciò permette al mittente di essere messo a conoscenza di potenziali errori nella sua configurazione, ad esempio di alcuni suoi server non inseriti correttamente nella lista di quelli autorizzati ad usare il dominio, e di potenziali campagne di attacco contro il suo dominio, contro le quali potrà dunque premunirsi.

MONITORAGGIO COSTANTE DEL VOLUME DI EMAIL SPEDITE

B.L.S. monitorerà costantemente il volume di email spedite dai vostri Server e dai vostri Domini tramite il software Senderbase.
In caso di incrementi anomali del volume di email (normalmente indice di infezioni dovute a software che spediscono email di spam) o di traffico anomalo, questo sistema di monitoraggio segnalerà il problema, consentendo l'intervento dei tecnici B.L.S.

MONITORAGGIO COSTANTE DELLE PRINCIPALI BLACKLIST

Anche l'invio di una sola email all'indirizzo sbagliato può causare l'inserimento del vostro server o dominio in una Blacklist.
È pertanto indispensabile monitorare costantemente le principali Blacklist (circa 100) e rimuoverli qualora vi fossero stati inseriti, riuscendo eventualmente a sbloccare le email nel frattempo inviate in modo che non vadano perse.
Si provvederà inoltre a individuare il motivo per cui sono state inserite in Blacklist e risolverlo.