TurboSMTP: guida tecnica alla deliverability delle email

turboSMTP

SOMMARIO

PERCHÉ QUESTO DOCUMENTO

Quando si parla di email, molti danno per scontato che inviare una mail corrisponda a recapitarla al destinatario.

Gli addetti ai lavori sanno invece che invio e recapito sono due fasi ben distinte e che il recapito è estremamente complesso.

Ed infatti quando si parla di consegna delle mail il concetto chiave è quello di **deliverability**. Con questo termine si intende il tasso medio di consegna delle mail inviate, cioè quante delle email che al mittente risultano spedite sono effettivamente arrivate nella casella di posta elettronica dei destinatari.

Pensiamo a un'attività relativamente comune nella vita di tutti i giorni: spedire un pacco. L'**invio** del pacco corrisponde a portare il pacco all'ufficio postale o a farlo prelevare dal corriere. Il **recapito** invece è tutto quello che viene dopo: la complessa logistica del trasferimento del pacco da un luogo all'altro, passando per varie tappe di smistamento e attraverso diversi sistemi di trasporto, fino ad arrivare nelle mani del destinatario. **La complessità, evidentemente, non è nell'invio ma nel recapito.** Aprire un ufficio che accetti pacchi dai mittenti è tutto sommato semplice; ma creare un sistema di logistica che li porti a destinazione è estremamente complesso, tanto che le aziende al mondo che se ne occupano sono relativamente poche.

Il recapito delle mail è un processo molto simile e, benché avvenga nel mondo digitale anziché in quello fisico, presenta sostanzialmente le stesse complessità. Anzi ne prevede una molto più grande: le email possono essere indesiderate o addirittura pericolose, motivo per cui i destinatari

trattano i recapiti con sospetto (immaginate se una percentuale elevata dei pacchi contenesse esplosivo...) ed è pertanto necessario convincerli che il messaggio in arrivo è sicuro. Il messaggio è spam? Proviene davvero dall'azienda che sembra averlo spedito? Contiene allegati o link pericolosi?

Recapitare (non semplicemente inviare) una email richiede un know-how molto specialistico, ma di cui esiste poca documentazione. Dato che questo è esattamente il nostro business, in questo documento vogliamo descrivere quali tecnologie e processi vengono utilizzati per far sì che le email giungano a destinazione. Questo ci permette di rendere più chiaro il valore aggiunto della nostra attività, e di creare qualcosa di utile per chi deve occuparsi tecnicamente dell'invio di email per implementare il proprio sistema di recapito e scegliere la soluzione migliore.

Quello che invece non tratteremo nel documento sono le cosiddette best practice che devono essere seguite da chi scrive i contenuti delle email (oggetto, contenuto, layout, ecc:) e da chi gestisce le comunicazioni (frequenza di invio, segmentazione, ecc) e le eventuali liste di distribuzione (double opt-in, pulizia liste, GDPR compliance, ecc.). Tutti questi aspetti hanno un impatto molto rilevante sulla deliverability, ma non coinvolgono le procedure tecniche di recapito e al proposito si trova moltissima documentazione sul web, dalle liste di parole da evitare nel contenuto alle statistiche sulle frequenze ideali di invio.

I destinatari di questo documento sono principalmente tecnici che abbiano già familiarità con alcune tecnologie legate alle email (ad esempio, diamo per scontato che chi ci legge sappia cosa significhi SMTP), ma dove possibile semplificheremo i concetti complessi (al prezzo di qualche approssimazione) per renderli comprensibili anche a un lettore non tecnico.

Basta mettere su un server SMTP interno... o no?

Tutte le aziende devono, per un motivo o per l'altro, inviare e recapitare molte email. La maggior parte delle aziende si rivolge a fornitori esterni (come per il resto delle attività IT) perché non ha una struttura tecnica interna. Alcune invece possiedono internamente un reparto tecnico che potrebbe proporre di gestire tutto in-house. Tipicamente, in quest'ultimo caso la proposta sarà quella di mettere su un server SMTP aziendale interno, che riceverà le mail dai mittenti e, teoricamente, le smisterà ai destinatari.

Tralasciando i rischi per la sicurezza (i server di posta interni sono prede ambitissime da spammer e autori di malware), la scelta di un SMTP aziendale interno potrebbe funzionare molto bene per le comunicazioni tra i dipendenti.

Il problema si porrà, inevitabilmente, quando invece le email dovranno uscire verso l'esterno e raggiungere caselle di posta non controllate direttamente: clienti, fornitori, partner. Con un po' di abilità tecnica i primi invii potrebbero essere recapitati, ma prima o poi cominceranno i problemi. E una volta che saranno cominciati, andrà sempre peggio: il server interno subirà un decadimento della reputazione, che a sua volta farà diminuire i tassi di consegna, che a sua volta danneggerà ulteriormente la reputazione del server e del dominio, in un circolo vizioso. Non sarà possibile prevedere quando il problema del recapito inizierà a manifestarsi (presto, ci sentiremmo di dire...) e la soluzione non sarà certo a portata di mano, soprattutto con un sistema come quello appena descritto.

È uno scenario apocalittico descritto solo per promuovere il nostro servizio? No, dovrebbe essere chiaro da ciò che abbiamo descritto in precedenza: un server SMTP interno fondamentalmente si occupa dell'invio delle email, non del loro recapito. Accetta i pacchi, per

usare il paragone precedente, non ha sofisticate procedure e strategie per recapitarli. Equivale a un fattorino a cui venga consegnata la corrispondenza aziendale, a cui però si chieda di recapitarla da solo in tutto il pianeta.

(Sul perché questo accada andrebbe fatta una lunga digressione storica sulla nascita del protocollo di trasmissione delle mail – che precede di molto la nascita stessa del web. Qui basti sapere che inizialmente il protocollo SMTP nacque come sistema di invio e recapito, ma a causa delle sue vulnerabilità – essendo stato progettato quando ancora spam e phishing non esistevano – è di fatto diventato un puro protocollo di invio e scambio, "agnostico" rispetto alla consegna).

Un server SMTP interno potrebbe comunque essere utilizzato per "accettare i pacchi", cioè le email in uscita, per passarli poi ad un servizio esterno che li smisti e recapiti. Il servizio esterno di recapito, in questo caso, prende il nome di **smarthost**. Uno scenario di questo tipo è pensabile se l'azienda, pur non volendosi occupare direttamente della deliverability per le ragioni di complessità descritte sopra, dispone comunque delle risorse per gestire in sicurezza un server che può diventare oggetto di attacchi esterni. È una soluzione ibrida molto usata nelle grandi aziende perché consente di avere un controllo interno sulla posta in uscita, allo stesso tempo assicurandosi l'elevato tasso di consegna che solo uno smarthost può garantire.

Una nota importante, forse non scontata per tutti i lettori: tutto ciò di cui parliamo qui è relativo all'invio di email legittime, cioè le email personali, transazionali o quelle commerciali inviate con il consenso del destinatario (quelle che ci si aspetterebbe venissero consegnate sempre, per intenderci). Per quanto possa apparire incredibile, le difficoltà e i processi che si descrivono sono relativi alla consegna di email legittime, non di spam. Che, vista la diffusione, merita purtroppo un paragrafo a parte.

Spam

Le aziende come la nostra, che inviano e recapitano grandi quantità di email per conto dei propri clienti, a volte vengono indicate dai non addetti ai lavori come diffusori di spam.

Nulla di più sbagliato: è vero anzi proprio il contrario, sono le aziende come la nostra che agiscono come “primo filtro” limitando la diffusione dello spam. A prescindere da ogni considerazione etica, far transitare spam sui nostri server, infatti, ne danneggerebbe la reputazione e dunque, in ultima analisi, il nostro stesso business (che, ripetiamo, è recapitare).

E infatti, semplificando molto, i grandi servizi di posta elettronica (Gmail, Outlook, Yahoo, o gli italiani Telecom, Libero, ecc.) preferiscono ricevere le email che passano dai nostri server e da quelli dei nostri competitor piuttosto che da server privati.

Per noi la battaglia contro lo spam è una vera e propria necessità di business, che determina la nostra sopravvivenza. Lo spam nella casella di un privato nella maggior parte dei casi è un fastidio che si può risolvere con un filtro antispam o cambiando fornitore di posta; sui nostri server è invece un pericolo. Per questo dobbiamo necessariamente mettere in atto strategie di prevenzione sofisticate e costose che non sono alla portata di un’azienda il cui business sia differente. Le nostre dimensioni ci consentono di combattere lo spam più efficacemente.

Se sui server di posta oltre ai messaggi legittimi transita spam, il danno di reputazione sulle email si manifesterà anche sui messaggi legittimi. Affidarsi a un’azienda con strategie antispam deboli significa mettere in pericolo le proprie comunicazioni, il proprio dominio e in ultima analisi il proprio business.

Concetti chiave

Per capire come funziona la deliverability e comprendere meglio i processi tecnici che descriveremo nel seguito, è utile introdurre subito alcuni concetti chiave:

1. Ogni mittente, ogni sistema di delivery, ogni IP, ogni server, costruisce nel tempo una propria **reputazione** presso gli attori esterni (fornitori di caselle di posta, blacklist, whitelist, ecc.), sulla base dei risultati degli invii precedenti. La reputazione può essere vista come un punteggio ponderato che, in ultima analisi, determina il tasso di consegna quanto e spesso più del contenuto del messaggio (a meno di grossolani errori nel contenuto stesso).

2. Come abbiamo visto, i fornitori di posta elettronica si trovano in una guerra perenne contro i messaggi malevoli (spam e phishing in primis). **Identificare un messaggio come legittimo o malevolo ha un costo computazionale elevato**; pertanto il tasso di consegna sarà tanto migliore quanto più il sistema di delivery faciliterà (cioè renderà economica) questa classificazione ai fornitori di posta.

3. Uno smarthost è un servizio di invio che si occupa di gestire direttamente la deliverability (a differenza di un semplice servizio SMTP, come Amazon SES o il servizio di posta in uscita del tuo internet o hosting provider).

REQUISITI DI UN SISTEMA DI DELIVERY

Cominciamo con una definizione: per **sistema di delivery** intendiamo l'insieme delle risorse tecnologiche (server, software, connettività) e umane coinvolte nel processo di invio e consegna di numerose email.

Un sistema di delivery si compone di:

- Un'interfaccia per la ricezione delle mail dai mittenti (tipicamente un accesso tramite protocollo SMTP e/o tramite API web)
- Un sistema di smistamento e gestione delle code delle mail
- Un sistema di consegna delle email in uscita dalle code (MTA, Mail Transfer Agent)
- Uno o più server su cui girano i servizi descritti sopra
- Uno o più IP dedicati all'invio
- Una o più risorse umane di amministrazione dei server e gestione degli IP (configurazione, aggiornamenti, fix, rotazione IP, analisi log)
- Una o più risorse umane che gestiscono le relazioni verso gli attori esterni, i provider di posta e le blacklist (delisting, feedback loops, segnalazioni di abuse)

La configurazione minima per inviare un numero non troppo grande di email è dunque un server

dedicato su cui siano installati i necessari componenti software (fra cui SMTP e MTA), a cui sia assegnato un IP dedicato, gestito 24/7 (per ragioni di sicurezza) da un amministratore di server esperto anche in deliverability.

È naturalmente da evitare l'utilizzo di server condivisi con altri servizi (ad esempio, usare lo stesso server su cui girano i servizi web) o con più risorse umane, sia per non sovraccaricare il sistema, sia per ragioni di sicurezza.

Al crescere del traffico o delle difficoltà di recapito si dovrà pensare a una struttura più complessa, che consenta ad esempio interventi di mitigazione e bilanciamento del carico.

(Incidentalmente, la configurazione minima necessaria già da sola spiega perché quasi tutte le aziende si affidino a servizi esterni: al di là delle considerazioni tecniche, il costo di una soluzione in-house è elevato, mentre uno smarthost può suddividere i costi fra diversi clienti)

I PROCESSI

Illustriamo di seguito i processi tecnici (automatizzati o manuali) che devono essere implementati per assicurare un recapito ottimale delle mail (cioè un ottimo tasso di consegna). Alcuni di questi processi consistono in una configurazione iniziale, altri si rendono necessari solo saltuariamente in risposta a problemi, altri infine devono essere ripetuti ad ogni ogni singolo invio.

Nel descrivere i processi useremo alcune semplificazioni (ad esempio, parleremo di firma digitale e certificazione per descrivere DKIM e SPF) che, seppur imprecise, consentiranno di comprendere meglio il processo.

Come già specificato in precedenza, i processi di cui parliamo sono procedure tecniche di competenza dello smarthost, non best practice di contenuto, invio, gestione liste, che competono a chi invia.

Configurazione dominio

Una volta scelti il dominio (o i domini) da cui inviare e lo smarthost che dovrà consegnare le mail, il dominio dovrà essere configurato per supportare i protocolli di autenticazione DKIM, SPF e DMARC. Lo smarthost, a propria volta, dovrà supportare queste tecnologie.

DKIM

DKIM (acronimo per Domain Keys Identification Mail) è un metodo utilizzato per impedire ai malintenzionati di falsificare la propria identità via email. Analizzando la parte del dominio dell'indirizzo di spedizione, il sistema DKIM verifica se il messaggio giunge dalla fonte dichiarata oppure no e se il suo contenuto (firmato digitalmente) è stato alterato. In sintesi, si tratta di un servizio di "certificazione" del messaggio.

DKIM viene implementato inserendo alcune informazioni nel record DNS del proprio dominio, in particolare nel campo CNAME; il mittente ottiene una firma digitale che ne garantisce identità e provenienza. In questo modo è possibile prevenire il phishing che tenti di abusare del proprio dominio o intercettare e manipolare il contenuto del messaggio, incrementando invece la deliverability delle email legittime.

SPF

Il Sender Policy Framework è un ulteriore metodo utilizzato per prevenire la contraffazione dell'indirizzo del mittente, ovvero l'uso di indirizzi falsi da parte di terzi. Consente al server di posta di verificare che le email in ingresso da un dominio provengano da uno smarthost autorizzato dall'amministratore di tale dominio. In pratica, il proprietario del dominio dichiara che tutte le sue mail sono trasportate dallo smarthost X, e che dunque qualsiasi mail che viaggi per altri canali è da considerare falsa.

Similmente a DKIM, anche il protocollo SPF viene implementato tramite modifiche al DNS del dominio.

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) è una tecnologia che standardizza i metodi SPF e DKIM e ne estende la funzionalità. Il criterio DMARC definisce come il destinatario deve gestire i messaggi email a seconda dei risultati di verifica di DKIM e SPF; anch'esso richiede la configurazione di un record sul dominio. In altre parole, DKIM e SPF indicano se il messaggio è legittimo (o quali parti del contenuto o del suo trasferimento non è possibile garantire); DMARC indica al server di posta del destinatario cosa fare del messaggio in base ai risultati.

Un'alternativa: il re-enveloping

Se per qualche ragione non è possibile implementare i protocolli precedenti (o non è possibile farlo rapidamente), alcuni smarthost (fra cui TurboSMTP) consentono il cosiddetto "re-enveloping" dei messaggi: in pratica, potendo garantire con certezza l'identità del mittente (dato che è stata verificata per attivare l'account), appongono la propria autenticazione al messaggio e dichiarano di stare inviando per conto del mittente.

La deliverability viene così comunque migliorata, ma c'è un prezzo: il destinatario viene informato dal proprio client di posta elettronica che il messaggio è stato inviato per conto del mittente, anziché dal mittente stesso. Questo può insospettire il destinatario. Inoltre, la reputazione del messaggio dipende interamente dalla reputazione dello smarthost e degli altri clienti dello smarthost.

Per queste ragioni, il re-enveloping è una procedura da considerare solo temporanea o di

emergenza. È giustificata come processo standard solo in casi molto particolari quando si debba inviare per conto di terzi usando ad esempio domini su cui non sia possibile l'accesso ai DNS (tipicamente, caselle di posta gratuite) - ovviamente previa verifica certa dell'identità dei mittenti. Più avanti vedremo proprio un caso di questo tipo.

Warm-up

Una volta configurato il dominio si può iniziare a spedire. Il dominio e il suo IP, all'inizio, avranno una reputazione incerta: non avendo uno storico, i provider di posta elettronica li tratteranno con particolare attenzione per capire se il traffico di email che generano è legittimo. In particolare, non vedranno di buon occhio se, da zero, cominceranno ad essere inviate di colpo moltissime email. Sarà invece necessario da parte di chi invia arrivare a pieno regime solo gradualmente, e da parte dello smarthost diluire i recapiti. Questa importantissima fase è tecnicamente definita **warm-up** (tradotto come "riscaldamento" in italiano) e può durare da qualche giorno a qualche mese.

In questa fase lo smarthost può anche adottare tecniche "smart" per velocizzare la costruzione della reputazione: ad esempio, può dirottare una parte del traffico su IP già rodati, per poi gradualmente accentrare il traffico sull'unico IP che si vuole riscaldare. Questa è la strategia più semplice, ma ne esistono di più sofisticate. L'importante è adottare tecniche di warm-up che siano viste di buon occhio dai provider di posta e non siano scambiate per tentativi di mascherare spam.

Lo scopo di uno smarthost non è imbrogliare i server di posta dei destinatari, ma al contrario

diventare loro alleato, aiutandoli a distinguere efficientemente le email legittime dallo spam (che un buon smarthost può intercettare e bloccare ancora prima che esca dai server). Smarthost e provider di posta elettronica si trovano dalla stessa parte della barricata e il tasso di consegna delle mail sarà tanto più alto quanto migliore sarà la loro relazione.

Smistamento per tipo di email

Non tutte le email sono uguali. Alcune contengono una newsletter, inviata pressoché identica a tanti destinatari allo stesso tempo; altre sono transazionali, cioè sono inviate per aggiornare il destinatario su operazioni e relazioni con i sistemi informativi dell'azienda (ad esempio le notifiche degli ordini o le richieste di cambio password), e ne riportano i dettagli. Altre ancora sono semplicemente comunicazioni personali uno a uno; ed infine, alcune si definiscono mission-critical: sono email transazionali o personali che contengono informazioni molto importanti la cui consegna è essenziale avvenga in tempi certi e prestabiliti.

Ognuno di questi tipi di email dovrebbe essere trattato in modo diverso per quanto riguarda i processi di recapito, pertanto il sistema di delivery dovrà anzitutto differenziare i messaggi basandosi sul contenuto, sulle modalità di invio (ad esempio numero, frequenza e regolarità di invio di messaggi dal contenuto simile) e su eventuali informazioni aggiuntive a disposizione del sistema (ad esempio, i messaggi dell'account X con mittente Y e oggetto Z devono considerarsi mission-critical).

Newsletter

Le newsletter sono spesso inviate in batch e normalmente non hanno una elevata priorità, quindi verranno messe in coda nell'ordine in cui sono state inviate. Per migliorarne la deliverability, lo smarthost potrebbe aggiungere o modificare alcuni header che permettano ai server di posta di identificare che tutte le mail fanno parte di un'unica campagna. In questo modo, dopo i primi recapiti, se il risultato è buono i server di posta daranno più facilmente semaforo verde al resto dei messaggi in coda che appartengono alla stessa campagna.

Email transazionali

Le email transazionali hanno di solito una frequenza più costante. Anch'esse saranno messe in coda in base all'invio; il compito dello smarthost sarà inserirle in una coda dedicata, e fare in modo che i server di posta possano facilmente identificarle come transazionali piuttosto che commerciali. Ad esempio, le email transazionali dovrebbero idealmente finire nella casella "Aggiornamenti" di Gmail, piuttosto che in quella "Promozioni". Lo smarthost non può ovviamente decidere come Gmail le classificherà, ma può fornire a Gmail dei segnali per classificarle.

Email mission-critical

Le email mission-critical devono avere la più alta priorità, cioè devono letteralmente saltare la fila: verranno inserite direttamente verso l'uscita della coda, non in base al momento in cui sono state

inviate ma in base a quando si intende recapitarle. Una coda potrebbe avere migliaia di email in attesa di essere consegnate, ma le email mission-critical usciranno sempre per prime. O, meglio ancora, lo smarthost potrebbe usare una coda dedicata ad alta priorità.

Email personali

Ci si potrebbe aspettare che le email personali vengano sempre consegnate; un tempo questo era vero ma oggi non è più così.

Il primo problema è che, essendo redatte ed inviate una ad una da un essere umano, le email personali sono poche rispetto alle newsletter ed alle email transazionali; in un certo senso si perdono in mezzo ad una quantità enorme di messaggi automatizzati e dunque la loro consegna dipende dalla reputazione degli invii automatizzati, molto più numerosi.

Ma c'è un problema molto più serio: essendo noto che le email personali sono aperte, lette e cliccate con molta più facilità rispetto ai messaggi commerciali, gli spammer e gli autori di malware generalmente cercano di comporre i loro messaggi per farli sembrare messaggi personali, nella speranza che chi li riceve si faccia più facilmente ingannare.

La conseguenza è che spesso le email personali possono essere scambiate per spam più facilmente dei messaggi commerciali automatici (newsletter e transazionali); il loro contenuto, infatti, è spesso molto simile a quello utilizzato dai malintenzionati proprio allo scopo di ingannare il destinatario.

Se ricevete una email con oggetto "Re: richiesta informazioni", cosa pensate? E' una mail

legittima o spam? Potete aprirla in sicurezza? Paradossalmente, forse potrebbe sembrarvi più sicuro aprire una mail con oggetto “Un’offerta esclusiva per te” che arriva dal vostro supermercato. È sicuramente un’email commerciale, ma quasi certamente non è pericolosa.

Lo stesso dubbio lo avranno i server di posta e, per questa ragione, la consegna delle email personali legittime sarà tutt’altro che scontata. Un buon smarthost dovrà dedicare delle risorse (IP, code, processi) a questo tipo di email, al fine di differenziarle da quelle automatiche ed evitare che siano scambiate per phishing o spam.

Smistamento per servizio

Tutti i provider di posta elettronica cercano di identificare lo spam e limitarlo secondo regole ed algoritmi propri. Possono ritardare la consegna ai destinatari e osservare che cosa fanno i primi utenti che ricevono l’email (è un comportamento tipico di Gmail), possono interrogare blacklist esterne (SpamHaus) o interne, possono limitare il numero di email accettate in un certo arco di tempo da un determinato IP o classe di IP e molto altro. Solitamente, fanno un mix di tutte queste cose, ognuno con una particolare ricetta: Gmail utilizza regole diverse da Outlook , per esempio.

Proprio perché ogni provider usa una ricetta personalizzata, è importante che le email vengano inviate secondo regole diverse per ogni provider; in particolare, potrebbe essere necessario inviare ai diversi provider con una frequenza diversa, con header aggiuntivi diversi, o usando un pool di IP differente. Di questo naturalmente non deve occuparsi chi spedisce: gestire questa complessità è invece compito specifico dello smarthost, che smisterà i messaggi in diverse code di invio non solo sulla base della loro natura, come abbiamo visto sopra, ma anche di quale provider di posta devono raggiungere.

Code di invio

Quando vengono inviate molte email, oppure email che devono essere soggette a modalità di consegna differenziate (perché di natura diversa o destinate a provider diversi, come abbiamo visto in precedenza, o ancora ad esempio perché destinate ad aree geografiche differenti), è essenziale suddividerle in diverse code che saranno processate in parallelo, distribuite su diversi server. Questo sia perché ogni coda potrebbe essere gestita con regole personalizzate, sia per evitare che un ritardo nell'uscita di una mail (ad esempio una temporanea saturazione della banda su un server) provochi lo stallo di tutte le email che devono ancora uscire. Nell'ipotesi che una coda sia bloccata, il resto delle email potrà continuare ad essere spedito senza interruzioni.

La corretta gestione delle code è l'attività che più caratterizza e impegna i servizi dello smarthost e, insieme a monitoraggio e feedback loop, costituisce la ricetta peculiare di ogni smarthost, ciò che lo distingue dai competitor.

Mail Transfer Agent

Una volta che la email è arrivata a fine coda e deve essere consegnata, lo smarthost esegue una speciale richiesta al DNS sul dominio del ricevente (detta query MX) per determinare l'indirizzo del server che si occupa di gestire la posta in entrata. Quindi contatta quest'ultimo server e chiede di recapitare il messaggio usando il protocollo SMTP.

Se la risposta è positiva, il messaggio viene consegnato al server di posta e il compito dello smarthost è terminato.

La risposta però non è sempre positiva: il server potrebbe ad esempio chiedere allo smarthost di riprovare il tentativo di consegna dopo qualche minuto o dopo qualche ora. Questa è la tipica risposta che si ottiene quando si eccedono i limiti per un IP, quando la casella del destinatario è piena, oppure quando si invia un messaggio da un nuovo dominio che il server di posta non conosce ancora. La richiesta di attendere e ripetere serve spesso anche a scoraggiare gli spammer (che normalmente ignorano questo tipo di richieste).

Se questo tipo di risposta viene fornita dopo aver trasmesso il corpo del messaggio si definisce tecnicamente **soft bounce**, per distinguerla dagli **hard bounce** che si verificano quando invece il server di posta rigetta completamente il messaggio (senza alcuna richiesta di ritrasmetterlo).

In caso di richiesta di ritentare la consegna in un momento successivo, il messaggio torna in coda, e un nuovo tentativo di consegna sarà eseguito in seguito.

L'insieme di tecnologie che gestisce code e procedure di consegna al server finale è definito Mail Transfer Agent (MTA). Esistono diversi MTA, open source e commerciali (MailerQ, Green Arrow, ecc.); non si tratta naturalmente di sistemi chiavi in mano, sono piuttosto assimilabili a framework di sviluppo che devono essere programmati e gestiti e soprattutto adattati alle regole dei provider di posta, che cambiano continuamente.

Rotazione degli IP

Se il sistema deve gestire l'invio di molte email (decine di migliaia al giorno), un solo IP in uscita non sarà sufficiente e sarà necessario invece dotarsi di più IP.

La gestione degli IP, cioè il bilanciamento delle diverse code fra più IP, è uno degli aspetti che più influiscono sulla buona deliverability delle mail. Non si tratta infatti di suddividere equamente il traffico fra i diversi IP (un'attività che potrebbe essere svolta in automatico dal Mail Transfer Agent): bisogna invece adottare una strategia in evoluzione continua che, in seguito ad esperimenti e per tentativi ed errori, consenta di massimizzare il tasso di consegna. La rotazione degli IP è quindi un'attività svolta tipicamente da una o più persone in tempo reale.

La strategia adottata da ogni smarthost è l'equivalente di una ricetta segreta e può fare una grande differenza; tuttavia è possibile identificare alcune regole generali, gli ingredienti di base della ricetta.

Anzitutto, ogni IP deve essere riscaldato, come abbiamo visto nel paragrafo Warm-up. Un IP che non abbia uno storico di invii sarà sicuramente un IP con basse prestazioni di consegna.

È inoltre necessario disporre di una buona classificazione dei propri IP: conoscere cioè in tempo reale la reputazione di ogni IP presso ogni provider di posta elettronica. Uno stesso IP in un dato momento, in funzione dello storico, può avere una cattiva reputazione per Gmail, una ottima reputazione per Microsoft e una nella media per Libero.

Allo stesso modo, un certo IP può avere buone performance per le mail personali e una cattiva per le newsletter.

Con queste informazioni a disposizione, le risorse che si occupano della rotazione degli IP osserveranno le performance del traffico e lo smisteranno dinamicamente fra i diversi IP. L'obiettivo di questo intervento non sarà quello di offuscare la provenienza delle email (una tattica adottata dagli spammer e che porterà invariabilmente al crollo del tasso di consegna), ma al contrario quello di facilitare ai server dei destinatari il riconoscimento della provenienza e

della natura dei messaggi. Sarà ad esempio una buona strategia quella di inviare lo stesso tipo di messaggi, dallo stesso mittente, per lo stesso server di destinazione, dallo stesso IP; e viceversa dirottare su un IP differente il traffico di natura differente.

Quando si parla di deliverability, gli incidenti sono frequenti ed inevitabili, anche con il traffico di migliore qualità. Ad esempio è frequente che alcuni destinatari segnalino per errore come spam un messaggio legittimo (anche solo perché l'oggetto li insospettisce o non trovano i link di cancellazione), danneggiando così l'intera campagna. Ma le cause di improvvisi cali di consegna possono essere svariate e imprevedibili. Se il numero di IP a disposizione lo consente, è una buona strategia avere un certo numero di IP in uso attivo, e un pool di IP di riserva, già riscaldati, su cui dirottare al volo il traffico (tutto o in parte) in caso di problemi.

Feedback loop

Come si è visto, uno degli aspetti più importanti per una corretta gestione degli invii è ottenere in tempo reale informazioni sui risultati di un invio e soprattutto sugli eventuali problemi ed imprevisti.

Il primo modo per ottenere queste informazioni è essere inseriti nei feedback loop dei fornitori di posta, cioè ricevere da essi in tempo reale le notifiche di eventi avversi (segnalazioni come spam, invio ad una spam trap, abusi, ecc.). Ogni fornitore ha un proprio sistema di interfacciamento: alcuni hanno un'API web, altri inoltrano le segnalazioni via mail, altri ancora richiedono un contatto diretto fra team, o un mix di tutto questo. Il team che gestisce i feedback loop dovrà costantemente analizzare le notifiche e prendere le necessarie contromisure, sia

a livello tecnico interno (ad esempio, sospendendo temporaneamente alcune code di una campagna) che, se necessario, contattando gli attori esterni coinvolti (ad esempio, richiedendo o fornendo ulteriori informazioni oppure eseguendo una richiesta di delisting ad una blacklist).

Monitoraggio

All'attività di gestione degli eventi in tempo reale (principalmente con i feedback loop) deve essere affiancata una continua attività di monitoraggio della reputazione di tutti gli elementi che compongono l'invio (dal mittente agli indirizzi IP), arrivando all'esecuzione di esperimenti ed all'invio di campagne simulate al solo scopo di verificare i risultati presso diversi provider. Idealmente, la reputazione di ognuno di questi componenti dovrebbe essere monitorata indipendentemente da tutti gli altri.

Il monitoraggio è un'attività in gran parte manuale che non è possibile automatizzare del tutto, ma esistono diversi strumenti tecnici che possono essere adottati per semplificarlo. Ad esempio, esistono servizi che forniscono liste di indirizzi email aperti a questo preciso scopo presso i principali provider, ai quali è possibile inviare qualsiasi contenuto e con qualsiasi frequenza (non si tratta di destinatari reali) per verificare i risultati dell'invio.

IL TRACCIAMENTO

Una volta che l'email sia arrivata a destinazione, tecnicamente il compito dello smarthost potrebbe considerarsi concluso.

Tuttavia la consegna di un'email, per chi la invia, non è un obiettivo a sé stante: è invece il primo passo affinché la mail possa essere aperta, letta e il destinatario possa eventualmente compiere un'azione su di essa (come seguire un link contenuto al suo interno ad esempio).

Registrare e monitorare questa attività, che tecnicamente si definisce **engagement**, è ovviamente molto utile per chi invia, ma lo è altrettanto per lo smarthost, in quanto contribuisce alla fase di monitoraggio di cui si è parlato in precedenza. Il livello di engagement sulle email può influire in modo importante sulla deliverability degli invii successivi: tutti i provider di caselle di posta, infatti, registrano le azioni che i propri utenti compiono sulle email ricevute e classificano i mittenti sulla base dell'engagement.

Il tracciamento di aperture e click è sempre opzionale e a discrezione del mittente e, se attivato, viene effettuato riscrivendo il contenuto dell'email prima di consegnarla, in modo del tutto trasparente per chi invia:

- Lo smarthost inserisce nel codice del messaggio un'immagine di tracciamento, per registrare le aperture del messaggio
- Lo smarthost sostituisce i link originali con link speciali di ridirezionamento, per tenere traccia dei click

I dati così raccolti possono essere visualizzati dal mittente in modo aggregato, utile soprattutto nel caso di campagne o email automatiche (la classica dashboard di statistiche su tassi di apertura e clic aggregate temporalmente o per campagna), oppure mostrando uno storico dell'engagement di un singolo destinatario, nel caso dei messaggi personali o commerciali uno-a-uno (a tale scopo TurboSMTP offre un prodotto dedicato chiamato TurboExecutive).

UN CASO CONCRETO

Per esemplificare i processi descritti in precedenza riportiamo un case study reale.

Veniamo contattati da un'azienda che sviluppa un software usato da professionisti sanitari, che ci presenta una serie di esigenze molto specifiche derivanti dal settore in cui opera, e che al momento di contattarci sta sperimentando con il fornitore esistente molte criticità.

Le esigenze

Il cliente ha una serie di richieste funzionali molto specifiche:

1. Dal software dell'azienda, il professionista sanitario deve poter inviare via email ai pazienti le ricette dematerializzate
2. L'invio, benché centralizzato, deve avvenire con l'indirizzo email normalmente utilizzato dal professionista nelle proprie comunicazioni personali affinché i pazienti lo riconoscano
3. Il paziente deve poter fare un "reply to" diretto al mittente della mail
4. Il professionista deve ricevere sulla propria casella di posta eventuali notifiche di mancata consegna (ad esempio dovute al fatto che il paziente ha fornito un indirizzo sbagliato)
5. È necessario usare un account di invio unico per l'azienda che sviluppa il software (anziché

creare singoli account per i singoli professionisti) per ragioni di semplicità di utilizzo da parte dei professionisti

6. Come ovvio, deve essere garantita una deliverability altissima, vicina al 100%
7. Le stesse elevate performance si devono ottenere sulle mail aziendali, inviate dall'azienda verso l'esterno con il proprio indirizzo e dominio

Le criticità

Al momento di contattarci l'azienda sperimenta le seguenti criticità:

1. Il fornitore attuale non consente l'invio da indirizzi email (le caselle di posta personali degli operatori sanitari) appartenenti a domini multipli non controllabili direttamente; dunque i pazienti vedono arrivare le ricette dematerializzate da un unico dominio (quello dell'azienda sviluppatrice) che non riconoscono (e in molti casi ignorano il messaggio o, peggio, lo segnalano come pericoloso) e non sono in grado di rispondere direttamente all'operatore
2. Le mail aziendali hanno seri problemi di consegna in particolare sui due principali provider di posta italiani
3. L'azienda non ha una figura tecnica interna con competenze specifiche su "come funzionino le email" e dunque non ha nessuna comprensione delle cause dei problemi

In sostanza l'azienda si trova in una situazione di emergenza in cui, pur avendo esternalizzato

l'invio di email, non riesce di fatto ad erogare il servizio: le mail sono tutte legittime e importanti, ma finiscono in spam e, quando comunque arrivano, non sono riconosciute dai destinatari.

La situazione è particolarmente grave data la natura delle email che devono essere inviate: non si tratta di email commerciali, ma di messaggi critici per la salute dei pazienti/destinatari.

La nostra analisi

Abbiamo subito eseguito un'approfondita analisi tecnica, comprensiva di un monitoraggio sulle performance esistenti, che ha rilevato i seguenti problemi da affrontare e risolvere urgentemente:

1. Il dominio principale del mittente è compromesso a causa di precedenti errori di gestione e, nonostante la natura delle email inviate, ha una reputazione - e dunque una deliverability - pessima
2. Il problema di deliverability è particolarmente grave nei confronti dei fornitori di posta italiani (che, accanto ai classici Gmail e Outlook, rappresentano una percentuale molto alta degli indirizzi email dei destinatari)
3. Il cliente richiede l'invio da numerosi mittenti (i professionisti sanitari), quindi da indirizzi email su domini non direttamente controllabili – dunque per forza di cose in maggioranza senza DKIM – con relativo inoltro di bounce-back su altrettante caselle, anziché solo sull'account principale

La nostra soluzione

Per soddisfare le esigenze del cliente e risolvere tutte le criticità in tempo rapido e senza gravare sulla attività dell'azienda (in particolare senza stravolgere il codice esistente e sovraccaricare gli sviluppatori), abbiamo adottato le seguenti soluzioni:

1. Per le email provenienti dagli operatori sanitari, al cliente è stato fornito un servizio in modalità "re-enveloping"; cioè il mittente viene opportunamente "imbustato" in modo che il dominio responsabile per l'invio – in termini di authority e quindi deliverability - sia quello di TurboSMTP, ma allo stesso tempo è assicurata la trasparenza per il paziente che vedrà comunque l'email provenire dal suo medico.
   Questo ha permesso di venire incontro alle esigenze 1-2-3-5-6 (mittenti multipli con domini propri ma un solo dominio responsabile della deliverability, riconoscibilità delle email inviate, possibilità per i destinatari di rispondere direttamente al mittente).
2. È stata abilitata una personalizzazione per il cliente, in virtù della quale i bounce-back vengono inoltrati al singolo operatore sanitario anziché all'email dell'account principale (esigenza 4).
3. La reputazione del dominio principale è stata gradualmente ripulita dirottando il traffico su IP ad alta reputazione, ed estendendolo gradualmente a tutti gli altri IP usati dall'azienda con un warm-up graduale e mirato. Grazie al re-enveloping, i destinatari hanno anche smesso di segnalare le mail come spam perché ne riconoscevano la provenienza
4. Per risolvere il problema specifico relativo ai provider italiani, si è scelto innanzitutto di utilizzare IP europei (cioè assegnati da RIPE); ma soprattutto, e più efficacemente, i provider

italiani sono stati contattati dal nostro team tecnico per segnalare la natura delle mail inviate dall'azienda e garantirne la legittimità, creando inoltre delle code di invio dedicate e funzionanti in modo diverso dal resto del traffico.

5. Si offre con continuità consulenza e supporto sui processi e su alcuni aspetti della logica del software, fornendo anche esempi custom di codice per risolvere la criticità 3 (mancanza di un esperto interno).

6. Si procede a un monitoraggio continuo della deliverability, cosicché le richieste di delisting (rimozione da blacklist) possano avvenire in tempo reale, e rotazione e warm-up degli IP siano ottimizzati in modo trasparente per il cliente.

Il cliente, quando ci ha contattati, partiva da una situazione "disperata" in cui una parte molto rilevante delle email inviate non arrivavano ai destinatari. In seguito al nostro intervento, il cliente ha ottenuto una deliverability ottima e le eventuali difficoltà temporanee vengono adesso monitorate e gestite in tempo reale senza problemi di continuità.

LA STRUTTURA TECNICA ED ORGANIZZATIVA DI TURBOSMTP

TurboSMTP utilizza una private cloud, cioè un insieme di macchine virtuali in configurazione cloud ospitate su server fisici che gestisce direttamente. Si tratta di server Linux IBM ospitati in datacenter IBM in Europa e negli USA.

Abbiamo a disposizione alcune migliaia di indirizzi IP assegnati direttamente da ARIN e RIPE, gli organismi (rispettivamente statunitense ed europeo) che gestiscono a livello mondiale l'assegnazione degli IP. Gli indirizzi IP sono dunque a nostra disposizione senza intermediari.

L'architettura software utilizza sia componenti di terze parti che software proprietario. Ad esempio il nostro MTA è in gran parte sviluppato internamente.

Il nostro team tecnico è composto da personale altamente specializzato diviso nelle seguenti unità organizzative:

- Team di sviluppo, che si occupa della scrittura, testing e deployment del codice proprietario e delle integrazioni fra le componenti software dell'architettura
- Team di amministrazione infrastruttura, che si occupa dell'amministrazione e gestione della private cloud e dei server fisici su cui essa risiede
- Team di gestione deliverability, che si occupa della gestione degli IP, delle code, dei feedback loop e del monitoraggio
- Team di assistenza e consulenza, inserito nella struttura tecnica in quanto spesso la gestione delle problematiche del cliente richiede analisi tecniche su misura

CONCLUSIONI

Quello che hai letto fin qui ti sembra complicato? Ci piacerebbe dirti che non lo è, ma la verità è che consegnare bene le mail è davvero, davvero complesso! Per questa ragione le aziende che al mondo si occupano di questo servizio sono relativamente poche (anche rispetto a tutte quelle che forniscono servizi web). Se perfino grandi realtà come Facebook o Booking.com, nonostante le loro immense risorse, si affidano a terzi per l'invio delle mail, significa che questo è un campo in cui sono necessarie competenze specialistiche.

Nonostante la difficoltà ci auguriamo però che questa lettura sia stata piacevole ed istruttiva, nonostante la difficoltà: non abbiamo trovato in giro molte altre risorse che ne parlino e quindi pensiamo di aver realizzato qualcosa di utile.

Se poi hai bisogno di una mano per consegnare le tue mail, non hai che da chiamarci!

LINK UTILI

Mail Transfer Agent commerciali:

- Green Arrow: https://www.greenarrowemail.com/solutions/engine-onprem-edition
  Un diffuso software MTA ad alte prestazioni, installabile on premise
- MailerQ: https://www.mailerq.com
  Un diffuso software MTA ad alte prestazioni, installabile on premise

Servizi di monitoraggio reputazione e deliverability:

- MX Toolbox: https://mxtoolbox.com
  Una suite di strumenti utili per monitorare la salute del proprio dominio, IP, e in generale la reputazione dei propri invii
- HetrixTools: https://hetrixtools.com/
  Una suite di monitoraggio integrato delle blacklist

Blacklist e whitelist:

- SpamHaus: https://www.spamhaus.org/
  La più nota ed influente blacklist
- Barracuda BRBL: https://www.barracudacentral.org/rbl
  Blacklist e suite di sicurezza utilizzata da grandi provider di posta

- Return Path: https://returnpath.com
  Il più importante servizio di certificazione delle procedure di invio per le grandi aziende

I nostri servizi:

- TurboSMTP: https://www.serversmtp.com
  Il nostro servizio di smarthost per l'invio di email commerciali e transazionali ad elevata deliverability

- TurboExecutive: https://www.turboexecutive.com
  Il nostro servizio di invio e tracciamento per email personali e aziendali, con monitoraggio delle interazioni in tempo reale su app

- EmailChef: https://www.emailchef.com
  La nostra piattaforma per creare ed inviare campagne di email

emailchef
gustose ricette per l'email marketing

emailchef.com

mailStyler
NEWSLETTER CREATOR

newslettercreator.com

SendBlaster

sendblaster.com

turboSMTP

serversmtp.com

turboexecutive

turboexecutive.com

eDisplay

Via Palmanova, 24 - 20132 Milano (MI) Italy

Tel. +39 02 89050969

Viale del Lavoro, 53 - 08023 Fonni (NU) Italy

Tel. +39 0784 1786271

info@edisplay.it

edisplay.it