Engineer

E-post

post som skickas mellan brevlådor över internet

Vad det är

E-post är systemet som bär ett skrivet meddelande till en adress av formen `namn@domän` och lämnar det i en brevlåda tills ägaren läser det. I vardagligt tal heter det ofta mejl, och standarderna som definierar det säger för det mesta bara mail. Mottagaren behöver inte vara uppkopplad när meddelandet skickas: servrar tar emot meddelandet, håller det och skickar det vidare, och därför beskrivs e-post som lagra och vidarebefordra, på engelska store-and-forward, snarare än som ett samtal.

Två dokument står för det mesta av definitionen. RFC 5322 säger vad ett meddelande är: ett block av huvudfält, en tom rad och sedan själva texten. RFC 5321 beskriver SMTP, det nätverksprotokoll som en sändande server använder för att lämna meddelandet till nästa server på vägen. För att hitta nästa server slår avsändaren upp domänens MX-poster i DNS, poster som namnger de maskiner som är villiga att ta emot post för domänen.

Ett komplett meddelande kan vara mycket kort:

```
From: Ana Holm <ana@example.org>
To: orders@example.com
Date: Fri, 16 Oct 2026 09:14:00 +0200
Subject: Invoice 114 has the wrong VAT number
Message-ID: <20261016.0914.ana@example.org>

Hello, could you send a corrected copy?
```

Bara två av de huvudfälten är obligatoriska: datumet och avsändarens adress. Allt annat är frivilligt enligt standardens bokstav, men ett meddelande som saknar ämnesrad eller meddelandeidentitet ser slarvigt ut för de program som sorterar

post. En rad får vara högst 998 tecken lång och bör hålla sig inom 78, eftersom många e-postprogram fortfarande klipper av eller bryter allt som är längre.

Det finns ett andra, dolt lager. SMTP flyttar meddelandet inuti ett *kuvert*: en returadress, dit rapporter om misslyckade leveranser går, och en lista med mottagare. Kuvertet och de rader med `From:` och `To:` som läsaren ser är separata och skiljer sig ofta åt. En dold kopia fungerar eftersom mottagaren står på kuvertet men saknas i huvudfälten. En sändlista fungerar eftersom kuvertets returadress pekar på listan, så att studsen från en prenumerant vars brevlåda har stängts når listprogrammet och inte personen som skrev inlägget.

Använd begreppet i ett beslut

Använd ”Vad är e-post?” i ett konkret beslut. Vi kan knyta begreppet till systemet ni bygger eller köper. En webbplats som är snabb, lätt att hitta och går att redigera av din egen personal, utan en faktura för varje ändrad formulering.

Se våra tjänster Hör av er →

Granska antagandena bakom ordet

Använd förklaringen och det länkade arbetet för att formulera frågor till projektet. Vi kan undersöka antagandena tillsammans innan ett verktyg väljs. Utvecklade 100 webbapplikationer med HTML/HTML5 — 100 byggda webbapplikationer

Utvecklade 100 webbapplikationer med HTML/HTML5 Hör av er →

Varför det spelar roll

En e-postadress är den identitet som större delen av webben faller tillbaka på. Bekräftelser vid registrering, återställning av lösenord, kvitton, fakturor och meddelandet om att en betalning har studsat färdas alla som e-post, så en produkt vars post försvinner har användare som är utelåsta utan att någon märker det. Den som aldrig fick sin bekräftelselänk skriver sällan för att berätta det. Hen går därifrån.

E-post har heller ingen ägare. Varje domän kan driva sina egna servrar, och varje server kan tala med varje annan. Den öppenheten är skälet till att e-post har överlevt nästan alla meddelandetjänster som har byggts sedan dess. Priset är förtroendet. Den ursprungliga designen låter en avsändare skriva vad som helst på raden `From:`, så mottagande servrar avgör numera själva om de ska tro på ett meddelande. De avgör det utifrån bevis som den sändande domänen publicerar i DNS: vilka värdar som får skicka för domänen (SPF), vilka nycklar som signerar dess post (DKIM) och vad mottagaren ska göra med ett meddelande som påstår sig komma från domänen men saknar båda (DMARC).

För ett företag går den användbara gränsen mellan två slags trafik. Transaktionell e-post går till en person på grund av något som den personen just gjorde: en kod, ett kvitto, en länk för att återställa lösenordet. Massutskick går till många personer för att avsändaren valde att skicka dem. De två bygger upp sitt rykte var för sig, drar på sig klagomål i olika takt och skickas ofta från olika domäner. Blandas de kan ett nyhetsbrev som irriterar folk bromsa återställningen av ett lösenord.

Till sist finns frågan om var posten bor. Att driva en egen e-postserver innebär lagring, skräppostfilter, säkerhetsuppdateringar och ett avsändarrykte som måste förtjänas och behållas. En hostad brevlåda för läsning och en leverantör av utskick för automatiserad post är det vanliga svaret, och det är ett val som är värt att göra med avsikt snarare än av slentrian.

Så ser det ut i praktiken

På en plattform bar e-posten verifiering, aviseringar, sammandrag och kampanjer, och med en enda leverantör blev varje avbrott totalt. Lösningen var att lägga tre leverantörer bakom ett gemensamt gränssnitt med automatisk failover: SendGrid först, därefter SMTP2GO och Azure Communication Services. Inkommande webhooks rapporterar vad varje leverantör gjorde med ett meddelande, och båda sidorna hamnar i en utskickslogg och en tabell för leveranshändelser, så att den leveransstatus som leverantören rapporterar kan hämtas med en databasfråga i stället för att gissas. Kampanjer till segment av användare körs i ett separat schema för massutskick med 5 tabeller och 24 funktioner, byggt vid sidan av den transaktionella posten eftersom det är ett annat problem. En kontroll vid uppstart skickar ett verkligt meddelande genom hela stacken bakom en flagga: ett fel loggas som en varning i utveckling, men stoppar processen i staging och produktion. Sidan anger också priset: tre integrationer att hålla vid liv och leveransloggar som växer och måste rensas.

Företagets egen e-post börjar i DNS. Zonen innehåller ungefär tjugo poster, bland dem e-postroutning via en leverantör av hostade brevlådor, en avsändardomän för transaktionsmejl och autentiseringsposterna för båda, och hela zonen hålls som data i repot och stäms av mot leverantörens API. En ingång för granskning rapporterar skillnaden mellan deklarationen och det som faktiskt serveras, utan att ändra något, och det är den del som används mest.

Var företagets egen post bor avgjordes av aritmetik. De publika tjänsterna körs på en enda värd med 512 MB minne, och e-posten hålls medvetet borta från den maskinen: en e-postserver behöver marginal som värden redan har förbrukat, så den är skriven som ett installationsskelett som väntar på en egen värd. Under tiden läses brev till företaget i företagets egen brevlåda, som ligger hos Apple iCloud, och det finns ingen sändlista bakom den.

Var det går fel

Posten hamnar i skräpposten samma vecka som leverantören byts. Applikationen är densamma, men mottagarna blir misstänksamma. Domänens publicerade poster namnger fortfarande den gamla avsändaren, så post från den nya kommer fram osignerad eller från en värd som domänen aldrig har godkänt. Lägg till den nya avsändaren i posterna före bytet, behåll den gamla tills dess sista meddelande har gått iväg och läs, om domänen begär dem, de samlade rapporter som mottagarna skickar tillbaka.

Applikationen startar, och ingen tar emot något. En utgången nyckel eller ett avstängt konto hos leverantören ser precis ut som en fungerande konfiguration tills en verklig person sitter och väntar på en kod. Skicka ett verkligt meddelande vid uppstart överallt där tystnad är farlig, och registrera vad leverantören säger har hänt med varje meddelande, så att ett mejl som saknas kan spåras i stället för att diskuteras.

Studsarna samlas i en brevlåda som ingen läser. Kuvertets returadress pekar på en låda av typen `no-reply`, så permanenta leveransfel kommer fram och förblir olästa. Avsändaren fortsätter att skriva till brevlådor som stängdes för ett år sedan, och mottagarna tolkar det som en vana hos den som skickar skräppost. Låt returadressen peka på något som behandlar rapporterna, och sluta skicka till en adress efter ett permanent fel.

Ett tillfälligt nej behandlas som slutgiltigt. SMTP-svar som börjar med 4 betyder försök igen senare; svar som börjar med 5 betyder sluta. En avsändare som ger upp vid första 4xx tappar post som en upptagen eller försiktig server hade tagit emot en halvtimme senare. RFC 5321 ber om nya försök med minst 30 minuters mellanrum och om att avsändaren ger upp först efter minst fyra till fem dagar. Transaktionell e-post vill oftast ha snabbare omförsök med backoff, och en tydlig anteckning när avsändaren till slut slutar försöka.

Läs mer

- RFC 5322: Internet Message Format — huvudfälten, den tomma raden, gränserna för radlängd och de två fält som varje meddelande måste bära.
- RFC 5321: Simple Mail Transfer Protocol — kuvertet, svarskoderna, uppslagningen av MX-poster och råden om nya försök.
- RFC 7208: Sender Policy Framework (SPF) — hur en domän listar de värdar som får skicka e-post i dess namn.
- RFC 6376: DomainKeys Identified Mail (DKIM) Signatures — signering av huvudfält och text med en nyckel som mottagaren hämtar från DNS.
- RFC 7489: DMARC — som knyter båda kontrollerna till domänen i den synliga raden `From:`, med en policy och rapporter; ett informativt dokument snarare än en standard.

Ordlista

Välj utifrån era faktiska förutsättningar

Beskriv arbetsflödet, befintliga gränssnitt och användarna som behöver förändringen. Vi kan definiera en testbar leverans och en överlämning som gör att teamet kan underhålla lösningen.

Se vad det kostar Hör av er →

Gör begreppen praktiska

Fråga hur ”Vad är e-post?” gäller i er organisation. Ett konkret exempel från ert nuvarande system räcker för att börja samtalet.

Se våra tjänster

welcome@engineer.company +45 50 10 61 84 Köpenhamn, Danmark

Ta med dig den här sidan

Visitkort

Omsorgsfullt skapad med kärlek av D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Upphovsrätt © 2025 – nu · Engineer ApS · Alla rättigheter förbehållna.

Utskrivet från https://engineer.company/sv/glossary/email/