CASE STUDY

Linxo verdoppelt mit einem sicheren E-Mail-Produkt seine User-Base innerhalb eines Jahres

ZUSAMMENFASSUNG:

Linxo ist eine Plattform die es Nutzern ermöglicht, ihre Finanzkonten von einer einzelnen Schnittstelle aus in Echtzeit zu verfolgen und zu verwalten. Das Tool wickelt Ersparnisse, Überweisungen und Guthaben ab, um das Haushalten einfacher und transparenter zu machen. Zugang zu Linxo bekommen die Nutzer über die Web App oder den Download der mobilen App. Sie können zudem auswählen, ob sie bei bestimmten Aktivitäten, wie bei hohen Ausgaben oder dem Risiko des Kontoüberzugs per Mail oder Push-Mitteilung benachrichtigt werden möchten.

Die Benutzer von Linxo legen großen Wert auf Privatsphäre und Sicherheit, vor Allem da sie persönliche Informationen wie Bankkonten, PIN-Nummer und andere Details teilen. Durch eine steigende Anzahl an Datenschutz-Schlagzeilen - von den ***Foto-Hacks bei Sony*** über den kontroversen Film „Das Interview" bis zu ***Gerüchten zu einem über das Entertainment-System an Bord gehacktem Boeing-Flugzeuges*** - sind die meisten Tech-Nutzer mitttlerweile mehr als vorsichtig damit, welche Information sie teilen, wohin sie gesendet und wie sie genutzt werden.

Gleichsam mit dem eigenen Wachstum wird sich Linxo auch stärker der Verschiebung des Consumer Mindsets sowie der ansteigenden Nachfrage nach Cyber-Sicherheit bewusst. Seit seiner Gründung im Jahr 2011 ist das Unternehmen auf 700.000 Nutzer gewachsen, von denen die Hälfte in 2014 allein hinzugestoßen ist. Linxo sucht weiter nach Wegen, um die Sicherheit des Data Hosting zu verbessern und seinen Kunden einen ruhigen Schlaf zu schenken.

HERAUSFORDERUNG:

E-Mail-Sicherheit war eines der ersten Anliegen, das Linxo nach seiner Gründung addressieren wollte. Das Herzstück des Produktes basiert auf E-Mail-Benachrichtungen, da die meisten Nutzer über ihre Konto-Aktivitäten auf dem Laufenden gehalten werden möchten. Das Team begann, nach einer verlässlichen und einfach zu bedienenden E-Mail-Lösung zu suchen, bis es schließlich 2012 auf Mailjet stieß und sich entschied, mit dieser Software die monatlich 2.5 Millionen E-Mails zu versenden.

Das System deckte ihre Anforderungen perfekt ab: Überdurchschnittliche Zustellbarkeit („deliverability"), unterstützt durch eine eigene Technologie und ein Experten-Team zum Thema Deliverability. Linxo konnte sich also beruhigt zurücklehnen, wissend, dass Ihre E-Mails zur richtigen Zeit in den richtigen Postfächern landen würden.

MAILJET UND LINXO,
EINE BEZIEHUNG DIE AUF SICHERHEIT AUFBAUT

Die Nutzer von Linxo können sich aussuchen, ob sie per E-Mail oder Push-Mitteilungen über ihr Konto auf dem Laufenden gehalten werden. „***E-mail scheint der Favorit bei unseren erfahreneren Nutzern zu sein, die Ihr Konto etwas gründlicher ins Auge nehmen"***, sagt Bruno Van Haetsdaele, Co-Founder und CEO von Linxo. Möglicherweise liegt es auch daran, dass Benutzer vergangene Transakationen einfacher organisieren, archivieren und einsehen können.

Mailjet's Tech-Team arbeitete eng mit Linxo zusammen, um die Sicherheitsbedürfnisse des Unternehmens zu verstehen und eine maßgeschneiderte Lösung zu entwickeln, die sowohl die Benutzer schützt als auch die gesetzlichen Regulationen vor Ort beachtet. Das in Paris ansässige Unternehmen Linxo fand es hilfreich, dass Mailjet auch in Frankreich gehostet wird. ***„Das bringt uns Vorteile im Hinblick auf Datensicherheit und Privatsphäre"***, sagt Bruno Van Haetsdaele. Insgesamt ist die französische Gesetzgebung strenger, wenn es um Datenschutz und -sicherheit geht, sowohl was physische als auch digitale Dateien angeht. Der Ankauf von Kontaktlisten von Drittanbietern ist verboten und „ Opt-In " ist verpflichtend, was bei CAN-SPAM oder dem australischen Spam-Gesetz nicht der Fall ist.

Mailjet hostet alle Benutzerdaten auf hochsicheren Servern in Frankreich. Der Co-Founder des Unternehmens Julien Tartarin, der seine Karriere als Developer begann, hatte bei der Entwicklung Mailjets vom ersten Tag an globale Sicherheit im Kopf. ***„Wir nutzen TIER IV Datenzentren - welche die höchsten Sicherheits-Level bieten. Unsere Server werden in Frankreich gehostet, sodass unsere Daten nicht von den „ Black Boxes" des Intelligence Authorization Act betroffen sind"***, ergänzt Julien Tartarin. Mailjet besitzt absolute Kontrolle über die Verbindung zwischen Datenzentren und Dienstleistungen.

Zudem fügt Linxo eine zusätzliche Sicherheitsebene hinzu, um Informationen zu schützen, die von ihrem Mailjet-Konto an ihre internen Server gehen. „Die Kommunikation zwischen unserer API und den APIs von Mailjet wird mithilfe einer SSL-Technologie, die normalerweise von Banking-Anwendungen genutzt wird, verschlüsselt.

AN VORDERSTER FRONT

Als eine erste Gefahrenabwehr empfehlen die Deliverability-Experten von Mailjet den Sendern stets, die ***Authentifizierungs-Tools*** SPF, DKIM und DMARC einzusetzen. Dies ermöglicht es ISPs wie Gmail, Yahoo und AOL Ihre Identität als Sender zu validieren. Zudem schützt es Sie vor E-Mail „ Spoofing", einer Art von Spam, bei der ein falscher Sender eine Marke oder eine Person imitiert. „ Spoofing" ist eine ernsthafte Gefährdung für die Glaubwürdigkeit Ihres Brands.

In einer in diesem Jahr veröffentlichten ***DMARC Preseemitteilung*** teilte Twitter mit, während eines 45-tätigen Beobachtungszeitraumes unfassbare 2.5 Milliarden "gespoofter" E-Mails entdeckt zu haben, die mit ihren Domänen verbunden waren. Dieses verbreitete Phänomen trägt dazu bei, dass Konsument vermehrt das Teilen von persönlicher Information meiden. Tatsächlich ***gaben 62% alle Konsumenten an, sie seien besorgt darüber, wie Marken ihre Informationen verwenden.***

DMARC ermöglicht es Sendern anzuzeigen, ob sie SPF oder DKIM Schlüssel verwenden sowie welche spezifischen Maßnahmen - Bericht, Quarantäne, Zurückweisung - der empfangende E-Mail Server ergreifen sollte, falls eine E-Mail bei der Authentifizierung nicht besteht. Wenn zum Beispiel ein Spammer

versucht eine Linxo E-Mail zu „spoofen“ um die Kreditkarteninformation eines Benutzers zu erfragen, wird mithilfe dieser Schlüssel die „Spoof-E-Mail“ die Authentifizierung nicht bestehen und von Gmail zurückgewiesen werden.

Eine weitere „Best Practice“ für den Versand großer E-Mail-Volumen ist eine eigene oder „dedizierte“ IP-Adresse. Im Vergleich zu einer gemeinsam genutzten IP-Adresse bietet diese eine größere Kontrolle über Ihren Ruf als Sender. Das bedeutet einerseits, dass ihre Adresse nicht von dem Senderverhalten der anderen Nutzer beeinflusst wird, andererseits aber auch dass Sie die Verantwortung tragen, hohe Standards im E-Mailing beizubehalten, da sich dies sonst negativ in Ihrem Ruf als Sender niederschlägt.

ERGEBNISSE

„Seit 2012 verlassen wir uns auf Mailjet, vor Allem weil man sich flexibel nach unseren Bedürfnissen gerichtet hat,“ schließt Bruno Van Haetsdaele ab. „Da Mailjet service-orientiert ist, brauchen wir uns keine Sorgen um die Skalierbarkeit unseres E-Mail-Programms machen. Und da unser Sendevolumen stetig wächst, ist es einfach gewesen unseren Traffic zu vergrößern und gleichzeitig eine gute Service-Qualität zu behalten.“ Im Laufe eines einzigen Jahres hat Linxo seine User-Base und sein E-Mail-Sendevolumen verdoppelt.

Der erste, wichtige Schritt ist Vertrauen mit den Kunden aufzubauen, indem man ihre Daten schützt. Transparenz und der Antrieb, kontinuierlich an einem besseren Produkt zu arbeiten, gehören zur Vision von Linxo.

Van Haetsdaele sagt: „Mailjet hat sofort unsere Anliegen in Sachen Sicherheit und Privatsphäre begriffen. Der persönliche Support den wir erhalten haben war außerdem sehr hilfreich. Diese und andere Faktoren machen Mailjet zu dem Dienstleister nach dem wir gesucht haben. Dank dieser Elemente konnte unser Unternehmen zu der Größe wachsen, die es heute besitzt.“

mailjet™