Australian Government
Australian Signals Directorate

Marketing and Filtering Email Service Providers

First published: November 2020
Last updated: October 2021

Introduction

This publication provides high level guidance on how to use email service providers (ESPs) in particular deployment scenarios. This publication should be read in conjunction the *How to Combat Fake Emails* publication. The considerations and controls described in that publication also apply to ESPs sending email on your behalf.

Types of email service providers

ESPs help address issues ranging from managing email routing through to full email hosting solutions. The advice in this publication is primarily focussed on Marketing ESPs and Filtering and Routing ESPs (hereafter referred to as Filtering ESPs).

Marketing ESPs

Marketing ESPs typically provide business and marketing support for activities such as maintaining mailing lists, managing registrations, providing self-service features (such as subscribe and unsubscribe features), and tracking interests and engagement (such as open and click through rates).

While a Marketing ESP provides functionality for customer communications and driving product, service and program engagement, they also introduce cyber supply chain risks that can adversely affect an organisation's security posture and brand, as well as being leveraged for cybercrime.

Filtering ESPs

Filtering ESPs route and filter incoming and outgoing email flows and messages. Organisations may use them to provide availability protection (e.g. against distributed denial-of-service attacks or on-premise equipment failure) or for spam and malicious content filtering, where use of the leveraged expertise of a specialist service may provide more effective protection than an on-premise solution.

While the use of a Filtering ESP can be a wise security decision, there are particular security risks organisations should consider which relate to managing email flows and protecting the organisation's reputation.

Security risks

Reputational risks

Using an ESP to send email on your behalf, such as a Marketing ESP, or a Filtering ESP (which relays your outbound email), creates certain reputational risks:

- if the ESP is not properly authorised as a sender for a domain and email messages sent through the ESP are then classified as fake/spam email
- if the ESP is properly authorised as a sender for a domain but their policies/processes allow others to abuse the service by sending email claiming to be from your organisation (i.e. email spoofing).

The first reputational risk impacts effectiveness and reach of your communications, while the second allows malicious actors to abuse vulnerable ESP services to send email claiming to come from your domain, thus increasing the effectiveness of their phishing/malicious email campaigns.

Email spoofing via an ESP is difficult for recipients to detect or prevent since customer organisations typically authorise these vulnerable ESPs to send email on their behalf by using Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM).

Organisations must take care when authorising ESPs to send or relay on their behalf using mechanisms such as SPF and DKIM.

Data confidentiality risks

Filtering ESPs that perform mail routing/guarantee availability of mail delivery will be able to view email in plain text unless end-to-end message encryption is in place. Further, Filtering ESPs that filter email messages need to be able to view email in plain text to perform their function of filtering spam and malicious content. In both cases, this creates data confidentiality risks that organisations can most effectively manage by carefully choosing their ESP.

Choosing an email service provider

Do they have a cyber security program or certifications?

Marketing ESPs can store email subscriber information as part of their service. This might range from just email addresses, through to more identifiable preference information or click through history. Depending on the content, this may be Sensitive Information as defined within the *Privacy Act 1988* and may need to be managed in accordance with the Privacy Act.

Organisations covered by the Privacy Act are required to take reasonable steps to control the disclosure and use of personal information which they, or their service providers, collect on Australians.

To perform their function, Filtering ESPs have access to an organisation’s email flow in plain text. Choosing a partner that can be relied on to not store or disclose your information is important.

Before engaging an ESP, you should undertake cyber supply chain risk assessment of potential ESPs. Factors to consider should include:

- general reputation of the ESP in the industry
- cyber security certifications the ESP may hold
- available ESP cyber security policy and/or statements
- data sovereignty issues based on the ESP’s operating location(s) and ownership/influences
- ESP’s terms of use and privacy policy.

A Privacy Impact Assessment may also be necessary depending on the information the ESP has access to.

Do they require you to prove you own a domain before sending from it?

Before a secure ESP sends or relays email on your behalf, they will require you to create an account and prove domain ownership before associating the domain with your account.

Typical methods of proving domain ownership include the ESP providing challenge text that is:

- put in a special Domain Name System (DNS) record
- published in a web server location associated with the domain

- sent to a well-known security-related email address for the domain and needs to be confirmed via the ESP's website.

Note that publishing an ESP's mail servers in your SPF record does not necessarily constitute proof of domain ownership. While it proves the domain owner did authorise the ESP to send email on behalf of the domain, it does not prove the person currently registering the account is the domain owner. See the case study below for further information on why this is important.

You should be cautious if an ESP does not require proof of domain ownership or uses an existing configuration, such as SPF delegation to their domain, as the only proof of domain ownership.

Do they authenticate senders every time emails are submitted?

Once you have registered an account and proved domain ownership, a secure ESP will provide an authentication mechanism to allow you to verify you are the same party when you return to submit email. Depending on your use case this might be via a system-to-system authentication method, a web portal where you log in before sending messages or some other authentication arrangement.

A secure ESP will:

- require multi-factor authentication to administrative interfaces to increase the level of protection on authorised accounts and limit the effectiveness of password spraying attacks
- use an acceptable system-to-system authentication method, such as an API key or other method, to identify your systems before sending or relaying email on their behalf.

Do they provide access to logging information?

Depending on your organisation's existing security monitoring capabilities, you should investigate whether an ESP can provide you with logging or other security metrics from their service. This information can be vital to responding to cyber security incidents and is worth investigating before choosing an ESP.

Using an email service provider securely

Getting visibility on email service provider engagement

Marketing ESPs are sometimes engaged directly by business units as part of service, product or program delivery.

Cyber security teams may be able to identify Marketing ESPs used by their organisation by reviewing the organisation's SPF records and DKIM selectors. Cyber security teams should also engage with technical staff responsible for external DNS to ensure processes are in place to notify cyber security teams when changes are requested to SPF, DKIM and Domain-based Message Authentication, Reporting and Conformance (DMARC) records. This allows cyber security teams to ensure ESP engagement is appropriately authorised and risk-managed.

For Filtering ESPs, cyber security teams should review DNS MX records and consult messaging teams on email flow.

Authorise your email service provider using DKIM if possible

To allow a Marketing ESP to send email using your domains, you should authorise the ESP by providing them with a DKIM key and selector, rather than using SPF.

For a Filtering ESP, which relays your outbound email, the preferred approach to authorising in order of preference is:

- sign the message with your own DKIM key and selector before it leaves your infrastructure, or
- give the ESP a specially created valid DKIM key and selector so they can sign the message, or finally
- authorise the ESP using SPF.

Inheritance of ESP's posture when using SPF to authorise ESPs

Many ESP's will ask you to include their SPF, A record or other DNS record in your organisation's SPF record to authorise them. This is convenient as it allows the ESP to adjust their infrastructure without advising or requiring changes from you. However, it does mean your SPF posture is set by the permissiveness of the ESP's DNS records.

Before you include any DNS record from an ESP in your SPF record, you should consider and accept the security risks associated with their existing record, and that this record could change in future without you necessarily being aware of it.

Discovery risks from using SPF to authorise ESPs

Identifying an ESP as a valid sender in your SPF record will allow malicious actors to identify that you use that ESP. Subsequently, if malicious actors identify a vulnerability with the ESP's sender validation, potential misuse of your domain may be possible through the ESP.

When malicious actors identify ESPs with weak validation, they will check a large number of domains to identify any organisations using that particular ESP. This discovery activity is not complex, and can be automated and performed quickly and effectively. As an example, Rapid7's Project Sonar provides a ready enumerated dataset of TXT records of all detected internet hosts from which malicious actors can easily build a map of SPF delegations. For similar reasons, organisations should be cautious of using ESPs that publicly list their clients.

In contrast, DKIM can only be used to identify an entity's ESP if malicious actors can obtain a legitimate email sent through the ESP.

Create separate DKIM selectors and key pairs for different ESPs

Organisations should use a separate DKIM selector and key pair for each ESP so, if necessary, these can be revoked/removed without impacting other email flows.

When considering the implications for DMARC, be aware only one test (SPF or DKIM) needs to be passed for an email to be considered valid.

Legacy recipient mail servers

Organisations should also be mindful that older receiving mail servers that rely solely on SPF checking may block email which is identified only by DKIM. If a significant number of recipient's mail servers are old, you should assess the security risk of including the ESP in the domain's SPF record. Other mitigations to reduce security risk include scoping the authority given to the ESP.

Scope the authority you give to Marketing ESPs

Instead of authorising a Marketing ESP to send email on behalf of your organisation's root domain, you can limit the scope of the authority to either a subdomain or a specific program, service or product domain. For example, a Marketing ESP is being engaged to facilitate engagement for a new service. Rather than authorising the ESP to send on behalf of *<organisation>.org.au*, you could authorise the ESP to send on behalf of *<service>.<organisation>.org.au* or *<service>.org.au*.

Use of a subdomain or a specific program, service or product domain will reduce the reputational risk to the organisation's overall brand if malicious actors are able to conduct phishing attacks through a poorly secured ESP. It will also reduce the complexity of SPF, DKIM and DMARC configurations by separating them into different places, and allow removal of the associated records when changing ESPs, without the risk of impacting main email flows.

Monitor the service

If you have the capability, and your ESP provides security logs, you should ingest these into your security information and event management (SIEM) solution as appropriate.

For Marketing ESPs, a basic, but useful, technique is to make sure a few internal staff are recipients of group emails. This can increase the speed at which any misuse, information leakage or other unintended communications are detected.

Use DMARC and review your reports

DMARC provides a mechanism to request recipient mail servers on the internet notify the domain owner when they detect unauthorised email.

If you deploy DMARC, you should put in place reporting arrangements so this information can be reviewed. You may need to engage a specialist DMARC reporting service provider to help interpret these reports.

By receiving DMARC reports, organisations are more likely to identify misconfigured infrastructure and be aware of phishing campaigns which are threatening your brands.

Review and test configurations

Organisations can usually predict the interactions between SPF, DKIM and DMARC for well understood email paths. However, when attempting to implement these standards, organisations can find their email arrangements are more complex than initially thought. Organisations should use tools to verify their SPF, DKIM and DMARC configurations, as well as liaising with major email recipients to check email flows are working as anticipated after the initial implementation and any subsequent related maintenance.

There are numerous free and paid options on the internet to test your SPF, DKIM and DMARC configurations. While not an exhaustive list or a recommendation on any particular service, the following provides some examples:

- MXToolBox
- DMarc Analyzer
- Dmarcian
- Fraudmarc
- Dmarcly.

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Further information on SPF, DKIM and DMARC, as well as interacting with older recipient mail servers, can be found in the *How to Combat Fake Emails* publication.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).