HelpSource Q&A

We invite you to send your information systems audit, control and security questions to:
HelpSource Q&A
bgansub@yahoo.com or
publication@isaca.org

Fax to: +1.847.253.1443
Or mail to:
ISACA Journal
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Ganapathi Subramaniam is an accomplished professional with 25 years of industry experience, Subramaniam's passion and profession have always been information security. He lives and works in India. As a conference speaker and columnist, he has addressed numerous gatherings of chief information officers and chief information security officers worldwide.

Q My company uses a cloud-based email service provider for corporate email. The same vendor also provides storage space for all the employees to store data. Please let me know the controls that ought to be in place from a security point of view. For obvious reasons, I am not naming the vendor. My company deals with a great deal of sensitive information that we have a legal obligation to protect.

A While there are many advantages of using a cloud service provider (CSP) for handling emails, they come with a few shortcomings. Your company must be cognizant of both these advantages and shortcomings. In most instances, the email service provider is a shared infrastructure environment. Your organization may not get a dedicated infrastructure environment. This shared tenancy arrangement means that access controls must be quite strong. Here are some indicative steps to ensure that the controls are in place to protect your organization's information:

- Integrate the mail authentication credentials with your active directory (assuming that you are using a Windows-based network). Having separate credentials will require users to remember a different password and username for accessing the mail system, an outcome you will wish to avoid.
- Allow access to mail only with at least a two factor-based authentication. For example, they may get a one-time password (OTP) on their mobile device, which will help to ensure that no third party is able to impersonate and access. I am aware of a particular cloud-based email system that sends alerts of suspicious login attempts to the administrators.
- Consider restricting specific users from sending email outside of your company if there is no business need for them to do so. They must be able to send email within the company domain only. While this cannot be made a universal control, this must be implemented for users based on your business needs.
- Consider restricting users from sending emails with attachments.
- For individuals accessing their corporate email using their smartphones, have a mobile device management (MDM) system in place. You need an MDM platform that can work on all types of mobile device operating systems—Windows, Apple and so on. Your tool must have the capability to wipe the data—only your company's data and not any personal data—from the phone of the individual leaving the organization. One of the big challenges is implementing "containers," in which corporate data cannot be comingled and stored alongside personal data.
- Update sender policy framework (SPF) records on your domain name system (DNS) to ensure that only authorized servers are allowed to send emails representing your company's domain. An SPF record is a type of DNS record that identifies the various email servers that are authorized to send email using your company's domain. The key aim of SPF records is to prevent spammers from sending messages forged from addresses belonging to your company.
- Impose device-level restrictions for users handling confidential or sensitive information. This means that only authorized devices can actually connect to your email system irrespective of whether they are connected to your office network or their home network. Some form of media access control (MAC) ID restrictions must be in place to ensure that only company-provided desktops/laptops are used to connect.
- Consider imposing time restrictions in terms of access. If some employees do not need around-the-clock access, then impose time restrictions.
- Ensure ability to implement IP address-based restrictions. This means that certain users must be able to access the email system from your office network only and not from any other location.

FORUM

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article, and choose the Comments tab to share your thoughts.

Go directly to the article:

- Ensure ability to implement information rights management (IRM). IRM controls help to ensure that emails do not get forwarded or copied, rather, they self-delete or disappear after a certain length of time. This will ensure that emails do not get forwarded further to unauthorized recipients.

Many cloud-based email service providers offer simplified versions of their solutions and offer those at lesser prices. In many cases, they dial back security controls. Security controls that ought to be present by default are then made add-on features.

Above all, your company must take a holistic approach to implementing controls aimed at preventing potential data leakages. There is no point in imposing controls on one particular system and keeping all the other holes permanently open.