FIRESIDE CHAT PAPER

Redmond MAGAZINE

PROTECTING EXCHANGE ONLINE MAILBOXES FROM SPAM AND PHISHING ATTACKS

By Nathan O'Bryan

The move to Office 365 can be an exciting and rewarding experience for organizations looking to improve the quality of IT services. Exchange Online provides many features that are not available in any on-premises email product. Exchange Online provides bigger, better, faster, and more reliable mailboxes than are available to most organizations though any other offering.

Using an Exchange Online mailbox means using Exchange Online Protection (EOP). Like it or not, all mailboxes in Exchange Online sit behind EOP. There is a thriving community of third-party anti-virus solutions available to use with Exchange Online.

In this whitepaper we're going to cover some of the common mistakes customers make with their malware protection while using Exchange Online. We'll talk about configuration errors that are made both with EOP and with third party malware solutions. After reading this paper, you'll know the step you need to take to ensure that your Exchange Online mailboxes are well protected, safe, and secure.

EXCHANGE ONLINE PROTECTION ADMINISTRATION

One of the issues new customers to Office 365 have with Exchange Online Protection is the administration of the service. It is not clear to customer where to find the GUI for setting EOP functions.

One of the major selling points for Office 365 is that it is a constantly updated service. The update cadence that IT departments expect includes major versions of software being released on a two to five-year cycle. With Office 365 updates come constantly, and sometimes without warning or notification from Microsoft.

The update cadence in Office 365 can mean that keeping up with the administration interfaces can be challenging. The interface for Exchange Online Protection is no exception.

The main GUI for EOP administration is located in the Exchange Admin Center of your Exchange Online tenant. The "protection" and "advanced threats" sections of the EAC contain most of the interface for EOP settings.

The EAC allows you to define specific EOP policies for your organization as a whole, or for smaller groups of your end-users. Exchange Online is deployed with default settings for EOP that are intended to provide standard protection.

If your organization decides to use a third-party malware protection product, you will likely want to modify the default

Cover: faithie / Shutterstock.com

policies in EOP. Many customers choose to turn down the functionality of EOP as low as they can when using a third-party malware solution. This action is intended to keep false positives to a minimum and give the end-users a single place to look for quarantined messages when expected email does not arrive.

The problem with this EOP management interface is that it is not easy to use, and it is poorly documented. It's very common for customers to not modify EOP defaults at all, or if they do it's often not done well. Microsoft knows this is an issue and is working to address it.

SECURITY & COMPLIANCE CENTER

Office 365 is a suite of products that were not originally designed to work together. Exchange, SharePoint, and Skype for Business were all developed individually. Since the introduction of Office 365 Microsoft has been putting considerable development resources into making these products work together.

One example of where this development work has been happening is the Security & Compliance Center within Office 365. Microsoft has been working to put together a single interface that allows administrators to control the security and compliance features of all Office 365 products in this single console.

Recently included in the Security & Compliance Center is a new interface for controlling Exchange Online Protection settings. This new interface is designed to be easier to understand and use than the existing control panel within Exchange Online.

The vision of the Security & Compliance center is not yet complete, but Microsoft is working toward that goal. Eventually the Security & Compliance Center will be a centralized GUI for security settings across all of Office 365. As of this writing, that vision is not yet fully implemented. It's still necessary to understand the EOP settings in the Exchange Admin Center as well as the settings in the Security & Compliance Center at this time.

Being aware of the Security & Compliance Center and taking the time to learn the controls that are moved there will go a long way to ensuring that your organization makes the best use of this admin center.

BEING AWARE OF THE SECURITY & COMPLIANCE CENTER AND TAKING THE TIME TO LEARN THE CONTROLS THAT ARE MOVED THERE WILL GO A LONG WAY TO ENSURING THAT YOUR ORGANIZATION MAKES THE BEST USE OF THIS ADMIN CENTER.E

SPF, DKIM, AND DMARC

SPF, DKIM, and DMARC are three technologies designed to help prove email coming from your domain is actually from you. These technologies make it more difficult for spammers to send email pretending to be you.

Customers often think that because they have migrated their email into Office 365, they do not need to setup these protections. This is not the case. Microsoft does not setup any of these systems for you and failing to set them up yourself can cause your organization's email to be marked as junk mail on the receiving end.

Sender Protection Framework (SPF) is the oldest of these three systems. SPF is based on a DNS record added to your public DNS zone. This DNS record gives those receiving your email a way to verify that the email messages are from your organization.

If your email is completely within Exchange Online with no mail flow to other third-party services or on-premises Exchange, then setting up SPF records is easy. Microsoft provides a default SPF record for this situation in the DNS setup wizard.

If your organization has a more complex email routing path, setting up your SPF record is considerably more complicated. It is necessary to take into account where email enters and leaves your messaging system, which may work with the default record Microsoft provides.

Domain Keys Identified Mail (DKIM) is a newer technology that takes domain verification one step further than SPF does. SPF relies on a public DNS record that the recipient organization can use to verify that a message came from the IP address matching your organization, DKIM uses encryption technology to sign messages ensuring they came from your organization.

Used in conjunction with SPF, DKIM adds a level or verification for email from your domain. Neither of these technologies reduce the spam your organization receives but they do help others verify messages from you as valid.

Domain-based Message Authentication, Reporting & Conformance (DMARC) is the third technology designed to verify messages with your organization's name on them are real. DMARC works as an additional validation for both SPF and DKIM.

DMARC also includes some reporting on the delivery and acceptance of messages from your environment. The feedback on how your message traffic is handled by other organizations can be very valuable.

As previously stated, these technologies are easy to setup up for a default Office 365 configuration. If you're environment has additional routing requirements, then setting up these technologies can be very complicated.

CUSTOMERS OFTEN THINK THAT BECAUSE THEY HAVE MIGRATED THEIR EMAIL INTO OFFICE 365, THEY DO NOT NEED TO SETUP PROTECTIONS. THIS IS NOT THE CASE.

Microsoft recently made changes in their Advanced Threat Protection (ATP) suite that were causing valid email from domains that do not have these technologies configured to be marked as spam. Microsoft did not announce this change was being implemented, causing considerable difficultly for some Office 365 customers.

Implementing SPF, DKIM, and DMARC is highly recommended. If your organization routes message traffic though another service, implement these technologies with care.

THE PROBLEM OF SORTING EMAIL IS NOT SIMPLY A BLACK AND WHITE QUESTION. THIS EMAIL IS GOOD, THAT EMAIL IS BAD DOESN'T WORK FOR EVERYTHING.

CLUTTER, FOCUSED INBOX, AND JUNK

The problem of sorting email is not simply a black and white question. This email is good, that email is bad doesn't work for everything. "Grey mail" is a category of email that isn't quite junk mail, but it also isn't email that end-users want clogging up their inboxes.

Grey mail is hard to define, but it tends to be newsletters and marketing type email that users sign up for. Different users are going to have different levels of tolerance for grey mail. A single user might even have different levels of tolerance for newsletters from different sources. The problem of grey mail can be very complex.

Microsoft made an early attempt to handle the grey mail problem with Clutter. Clutter was a system that tried to sort grey mail out of user's mailboxes and into a separate folder. In theory Clutter was a great tool to help sort messages by taking grey mail out of your inbox and putting it in a different folder you can look at when you have time.

Unfortunately Clutter never really worked. Many customers had problems with Clutter never really figuring out what email should be sorted out to a separate folder. This caused a lot of end-user confusion, and further eroded customer confidence in Microsoft's malware protection.

Through an acquisition Microsoft purchased the technology that turned into Clutter's replacement, Focused Inbox. Focused Inbox has a similar goal to Clutter in that its meant to sort out grey mail from the primary view of your inbox.

Once your tenant is fully moved to Focused Inbox, your end users will need to "train" the system by marking messages they do not want to see in their primary inbox for movement to the "other" inbox. After a bit of training, Focused Inbox will be able to sort end-user's messages so that grey mail is less of an issue.

Focused Inbox still does not present

OFFICE 365 ADMINISTRATORS WILL NEED TO MAKE IT A PART OF THEIR ROUTINE TO INVEST THE TIME NEEDED TO KEEP UP-TO-DATE WITH CHANGES TO OFFICE 365 AS THEY HAPPEN.

the same experience in all common clients. Using OWA will not show Focused Inbox at all, which is disappointing. Once your end-users figure out Focused Inbox, where and how it works, they will find this a very helpful feature.

NEW FEATURES

One of the biggest selling points for "the cloud" is the constant innovation of new features and functionality. Often the first point brought up in the sales cycle for Office 365 or other cloud services is that the customer will receive the benefit of constant improvement to the service.

While new features and functionality within our IT services are great, IT departments need to adjust to this reality or this situation can become negative quickly. IT pros who grew up on a cadence of new versions of software on a three-year cycle must adjust to a constant update cycle for multiple various products.

IT managers and pros who are moving their organizations to the cloud need to ensure that their move to Office 365 includes a plan for keeping up the high rate of change in cloud services. Beyond just training, IT departments need to have a plan for knowing what changes are coming, and how to make sure their end-user communities can take advantage of those new features.

It does take some effort to keep abreast of new features as they roll into Office 365. Office 365 administrators will need to make it a part of their routine to invest the time needed to keep up-to-date with changes to Office 365 as they happen.

PUTTING IT ALL TOGETHER

Office 365 is a great service that offers significant benefits for users and administrators alike. Following best practices will ensure a successful transition for your organization.

There are a lot of benefits to moving to Office 365, and the built-in technologies that keep your data safe are very good. It is still important to educate yourself about how they work, and ensure that your organization has the protection it requires to maintain access, and the ability to work normally.

Find out more

www.kaspersky.com