WHY YOU NEED TO UP YOUR GAME WITH SECURITY FOR OFFICE 365

Office 365 cloud is not without risks: What you need to know

By Brien M. Posey

Office 365 has become immensely popular because of its ability to let users work from anywhere, using any device. At the same time, however, the Office 365 cloud is not without risks. Although Office 365 provides subscribers with the tools that they need to run core business applications in the cloud, some of Office 365's security and compliance features are not enabled by default. Furthermore, many organizations have found Office 365's built-in security capabilities to be inadequate and have, therefore, opted to augment the native security and compliance capabilities with third party software.

DATA LOSS PREVENTION

While it is tempting to think of security in terms of "keeping the bad guys out," a big part of keeping data secure is preventing authorized users from leaking sensitive information. Office 365 contains a built-in Data Loss Prevention (DLP) engine that can help to prevent users from sending sensitive information through E-mail. For example, Office 365's DLP feature can be used to detect credit card numbers or social security numbers within an E-mail message and then prevent the message from being sent.

Although Microsoft's built-in DLP protection can be effective for preventing some types of data leakage, Office 365 subscribers commonly find that the native DLP capabilities do not go far enough. Microsoft's DLP feature focuses primarily on regulatory compliance (such as PCI or HIPAA) and on detecting known information types such as driver's license numbers or passport numbers. Yet, Microsoft's DLP feature has no capacity for detecting sensitive information that is unique to your organization.

Ideally, a DLP engine should provide blanket regulatory compliance capabilities, while also being flexible enough to adapt to an organization's own individual needs. This means allowing the organization to determine the types of data that it considers to be sensitive, even if the sensitive data is not of a common data type (such as a credit card number or a social security number).

A good DLP engine should also be able to detect documents that have been designated as containing sensitive information and prevent the document from being sent, even if the document

has been converted to a different file format or truncated in an effort to avoid detection. Of course, manually identifying sensitive documents is a tedious process, so a DLP engine should ideally be able to use a document's location to determine whether or not the document is sensitive.

Second, the data archiving engine needs to use policies to determine the length of time for which data must be retained. During the required retention period, the archiving engine should take steps to prevent data loss or modification. This may include steps such as encrypting archive data or using resiliency mechanisms to protect against accidental data loss.

Finally, the data archiving engine needs to be able to identify data that has reached the end of its required retention period and then dispose of that data according to the organization's policy.

AN ORGANIZATION'S SECURITY SHOULD NOT BE DEPENDENT ON A SINGLE SECURITY MECHANISM, BUT RATHER ON A VARIETY OF POLICIES AND MECHANISMS THAT WORK TOGETHER.

ARCHIVING

A big part of regulatory compliance is meeting the data archiving requirements. Microsoft Exchange Server contains a number of different features that are designed to help organizations meet their data retention obligations. The Journaling feature, for example, can capture copies of messages as they pass through the transport queue. Similarly, archive mailboxes allow for the long term retention of messages. Although these features can help with maintaining regulatory compliance, the native Exchange Server content archiving capabilities tend to be inadequate by themselves.

If a data archiving solution is to be effective, it must perform comprehensive data lifecycle management, not just archiving. This involves three key tasks.

First, the data archiving engine must be able to determine the types of data that need to be archived. It is not enough for such an engine to archive Exchange Server data. There will likely be other data types that must also be archived.

CLOSE GAPS IN SECURITY

Microsoft uses a variety of security mechanisms and procedures to protect its Office 365 assets. Yet most organizations do not operate solely within the Office 365 cloud, opting instead to create hybrid deployments that leverage resources residing on premises and in the Microsoft cloud. The problem with this is that many of the protective mechanisms that Microsoft uses to safeguard Office 365 are not able to protect resources residing on a subscriber's private network. As such, it is critically important for organizations to take steps to protect the resources residing in their own datacenters.

IT security professionals commonly advise practicing defense in depth. This concept is based on the idea that an organization's security should not be dependent on a single security mechanism, but rather on a variety of policies and mechanisms that work together to keep the organization secure.

Practicing defense in depth commonly requires an organization to use multiple security tools. While necessary, this approach can create a significant workload for admins because each tool has to be managed separately.

The solution to this problem is to take a unified approach to network security management, while continuing to use multiple security tools. This requires the use of a management tool that can accept data from a variety of security tools and then transform that data into an overall assessment of the organization's security health.

For this approach to be optimally effective, however, the security platform should be able to use the information that it has collected to provide the administrator with meaningful information. If an attack occurs the security software should be able to tell the administrator things such as which users have been attacked and whether there are any indications that the attack was successful. Such information should be presented in a meaningful and intuitive manner that does not require the administrator to go digging through log files.

While it is important for a security platform to be able to detect and report on an attack, the software should also be able to stop an attack while it is in progress. For example, the security software might initiate an automated workflow in response to an incident that has been detected.

GameChanger

GAME CHANGING STRATEGIES FOR OFFICE 365 SECURITY

PROOFPOINT PROVIDES THREAT PROTECTION FOR MICROSOFT OFFICE 365

Proofpoint Threat Protection for Office 365 safeguards users against advanced threats and targeted attacks. It provides you with threat insights to identify attacks and helps your security teams orchestrate rapid response and containment. E-mail continuity provides assurance of e-mail uptime. Proofpoint's award-winning customer support reflects its commitment to your success.

Key Benefits

- Superior blocking of malware and malware-free threats
- Actionable visibility and insights
- Respond to threats faster
- Threat Operations Center security expertise
- Ensure e-mail uptime

SUPERIOR SECURITY

Proofpoint's threat intelligence spans e-mail, network, mobile apps and social media. This next-generation approach results in industry-leading security efficacy and bulk mail management. It also detects new, never-before-seen attacks in an Office 365 e-mail environment.

Legacy techniques reliant on host, URL and attachment reputation are no longer sufficient. More is needed to combat credential phishing, business e-mail compromise and ransomware.

Proofpoint analyzes threats in several stages using multiple approaches to examine behavior, source code and protocol. Predictive analysis identifies and sandboxes suspicious URLs and attachments before users can click on them.

GAIN ACTIONABLE VISIBILITY AND INSIGHTS

Visibility is paramount to track down threats, improve cybersecurity posture and support business objectives. As security becomes a board-level conversation, it is even more critical to provide the "who, what, when, where, how" of an incident. With visibility that spans malware and non-malware attacks, knowing whether an attack was part of a broad attack campaign, targeted at your vertical or specifically at your organization, helps you prioritize actions.

PROOFPOINT'S THREAT INTELLIGENCE SPANS EMAIL, NETWORK, MOBILE APPS AND SOCIAL MEDIA.

RESPOND TO THREATS FASTER

Auto-Purge saves cleanup costs: Save hours extracting e-mail threats from Office 365 and Exchange mailboxes. This layer of protection against emerging threats takes in real-time threat alerts for malicious URLs and attachments and moves identified e-mails into a quarantine area inaccessible by end users. Each action creates a task history showing the protective action taken. You define the rules—whether e-mails are extracted automatically or on demand. You have options to retain the e-mail for review or retain for a short period then auto-delete.

Quickly assess and confirm compromise: When a target machine receives a malicious e-mail, how do you know whether it is compromised? Automated endpoint forensic collection and compromise verification provides visibility to prioritize response efforts. Organizations can remediate only the fraction of machines that require it, gaining a scalable way to reduce risk.

Threat experts: Dedicated security expertise can be hard to come by. Proofpoint's global Threat Operations Center is staffed by threat research experts working around the clock. As an extension of your security team, they leverage sophisticated threat intelligence to provide context and insights to help you understand actor/campaign activities within your environment and can help you prioritize threats.

Ensure E-mail Availability: In the event of any sort of outage, be it on Microsoft's side or an authentication issue on yours—e-mail can be readily accessed natively in Outlook via a web portal. It enables IT to regain control with always-on secondary e-mail service with a 30-day rolling inbox to eliminate single vendor dependency on uptime.

Find out more at
www.proofpoint.com/O365

proofpoint.