IDC Analyst Connection

Sponsored by: **Vade Secure**

Author: Konstantin Rychkov

January 2019

Email Security: Maintaining a High Bar When Moving to Office 365

Introduction

Communication and collaboration has become a cornerstone of effective business today. It involves both internal and external parties and demands continuity, flexibility, and user-friendly experience. We see a rise in collaboration platforms and messaging tools used by teams across industries, but email remains the single most effective and ubiquitous means of digital communication for business, with over half of the world's population as users (3.7 billion). The flipside of this popularity is that email is the number 1 threat vector used by cybercriminals. The reason for this and at the same time the key challenge for security professionals is the amount of trust that users have in their inbox content. This trust needs a strong security foundation, which for today's modern, increasingly cloud-based infrastructure means a shift from traditional perimeter-oriented controls and the use of layered continuous protection models fit for not only detection but also reverification of email and remediation of new emerging threats.

The following questions were put to Konstantin Rychkov, research manager at IDC European Security Solutions, by Vade Secure.

Q. Has adoption of cloud email — and Office 365 in particular — reached a tipping point, particularly for cybersecurity threats?

A. Email, being a backbone of business communications, has over time become a utility. Cloud technology has enabled organizations to lift the burden of in-house mail server maintenance off the shoulders of internal IT, introducing flexibility, scalability, and operational efficiencies, and reducing costs. These are the main reasons for worldwide cloud email spending growing from 22.9% in 2013 to 68.4% in 2018 (80.4% in the U.S. and 59.6% in Western Europe). This is indeed a tipping point in preferred infrastructure.

Speaking of Office 365 and Microsoft's email applications offering in general, IDC's data confirms that it is the most adopted enterprise email solution, with a 54.0% share of the overall email applications market and 47.6% of cloud deployments in the first half of 2018 globally.

In 2016 cloud email just tipped over the 50% mark in share of deployments, but by 2022 IDC expects this share to be as high as 89.4% of a $6.3 billion market. The transition is led by Microsoft's and Google's solutions implementation. Such standardization around the platforms of choice inevitably leads to increased interest from cybercriminals and greater risks associated with careless deployments. This of course does not mean that organizations should freeze or start to roll back

migration projects. On the contrary, cloud migration is an opportunity to reevaluate email security architecture and optimize it for business continuity.

Q. How are email attacks evolving in the context of Office 365 environments?

A. For the past few years, email attacks overall have remained the number 1 entry point with over 80% of attacks beginning with an email. Using email as a highway, phishing remains the most pervasive attack, yet with cloud expansion the threat surface is growing, as does the sophistication of attacks both in terms of payloads and staging. Consequently, deriving from business email compromise (BEC), there is a growing number of internal and external impersonations used as a weapon of choice by attackers.

Traditional approaches rely on gateway protection designed to operate within the perimeter boundaries as a single point of entry and defense. For cloud platforms, such as Office 365, this security architecture introduces the vault issue. Once behind the gateway, attackers can get access not only to email communications but can also effectively spread into the application layer and reach the data, files, and contacts housed within it. This makes business cloud email a major and potentially lucrative target for hackers.

As mentioned above, email impersonations are on the rise. In fact, data from Vade Secure shows that Microsoft has been the number 1 most impersonated brand in phishing attacks for three straight quarters[1]. Starting with harvesting Office 365 (or alternative platform) credentials, malicious actors then analyze and mimic communications internally or externally (to partners and clients). These multiphased attacks are aimed at making a financial gain in the form of wire transfers or invoices paid to accounts controlled by the perpetrators of the scheme. A report by SEC highlights that one such attack resulted in 14 wire payments over several weeks, at a cost of more than $45 million in non-retrievable losses.[2]

Q. Native Office 365 security offers sufficient email protection. Why do we need extra security?

A. For the past few years Microsoft has invested heavily in its security capabilities, and the assumption that its inbuilt email protection is robust is a valid one. But native out-of-the-box capabilities of O365 or the Exchange Online Protection (EOP) service are aimed at spam filtering and catching all known malware traveling to or from your organization. Anti-spoofing with Composite Authentication (combined SPF, DKIM, and DMARK protocols) is only available for E5 or Office 365 ATP, with some functions enabled in EOP since the end of 2018.[3]

Reputation-based defenses are effective against known threats, but the growing sophistication of messaging attacks requires layered controls for unknown, highly dynamic threats and/or BEC impersonation attacks. The latter broadens the attack

[1] https://www.vadesecure.com/en/phishers-favorites-q4-2018/
[2] https://www.sec.gov/litigation/investreport/34-84429.pdf
[3] https://docs.microsoft.com/en-us/office365/securitycompliance/protect-against-threats

surface of the organization, and while in on-premise environments internal email scanning was a "nice to have," in a cloud environment, it's a must-have.

Cloud email security filters for both Office 365 and G-Suite (by far the most used cloud email platforms) are robust but not impregnable, and attackers are continuously expanding their arsenal to bypass native protection mechanisms. Therefore, augmenting O365 deployments with an additional layer of messaging protection — but by no means replacing it, in line with traditional on-premise approaches — is a good insurance for secure email architectures.

Q. For organizations with an existing email gateway, what concerns or limitations does migrating to Office 365 introduce?

A. Interestingly, IDC's *CloudView 2018* global survey (April 2018, n = 5,740) has highlighted that 7.5% of organizations have moved email application/workload from a public cloud back to an on-premise delivery model (8.7% in Western Europe). At the same time, security is rated one of the top 3 concerns for SaaS, PaaS, and multicloud deployments. So, the question of secure migration is critical for enterprise transformation.

Secure Email Gateway (SEG) is one of the traditional technologies often referred to in this paper. Using a binary good/bad model, SEG architecture first came into the market in the late 1990s when the gateway was in a DMZ (demilitarized zone). Rapid cloud adoption challenges this model as SEG controls are either non-sufficient or, when tightened too much, generate a flood of false-positives, interrupting business operations.

Because SEG requires an MX (Mail Exchange) record change, it poses the following limitations:

- Cannot layer effectively with native Office 365 security because it renders reputation-based defenses useless (e.g., for EOP), or introduces additional sophistication to integrate seamlessly
- Cannot scan inter-organization email traffic because it sits in line in the email flow
- Requires setup and (re)configuring of external spam quarantine, introducing management overhead for internal IT
- May need additional end-user training
- The product is publicly visible through a simple MX lookup; hackers can use this information to tailor their attacks in an attempt to bypass the specific vendor

Q. Accepting that it is impossible for any email security product to block every threat, what's the best approach to dealing with false-negatives?

A. Frankly, remediation has never been the strongest trait of email security solutions, stemming from the traditional approach to messaging protection. Dealing with false-negatives would involve additional technologies for detection and response which should integrate with the overall security stack to achieve security unification.

Deperimeterization of enterprise infrastructure, driven by broader acceptance and utilization of cloud, along with the dynamic threat landscape organizations face today, puts an ever-increasing burden on security teams. The scale and speed of contemporary enterprises requires primarily the automation of threat remediation and response, which in turn has visibility as a prerequisite. The same is valid for email security in particular. Continuous email protection, as mentioned, is a must for cloud-based infrastructure and this includes dynamic ruleset updates.

Another key element of effective email false-negative remediation is integration with SOC and/or SIEM tools and workflows, so that threat detection results could be leveraged to update incident response playbooks on top of ruleset tweaks.

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.