IDC TECHNOLOGY SPOTLIGHT

Protecting Your SaaS Applications

June 2015

Adapted from *IDC FutureScape: Worldwide IT Security Products and Security Services 2015 Predictions — Moving Toward Security Integration* by Charles J. Kolodgy, Pete Lindstrom, Christian A. Christiansen, et al., IDC #253026

Sponsored by Trend Micro

IDC believes that in the 3rd Platform era, the best approach to protecting email services like Office 365, which reside in the cloud, is one that synergistically ties together the embedded security mechanisms offered by the email service provider with adjacent security technologies and strong processes and policies managed by the business owner of the data. This Technology Spotlight examines the security risks of software as a service (SaaS) in the era of expanding cloud use. The paper also looks at the growing security capabilities of SaaS applications and the efforts by Microsoft to better secure its SaaS offerings through partnerships with third-party cloud and security solution providers.

Security in the 3rd Platform Era: Risks and Rewards

The future of security is being driven by massive change, fueled by a highly mobile workforce that demands access to productivity applications and the adoption of cloud-based services from just about any location. These trends are part of the current stage in the evolution of corporate IT innovation and growth, which IDC calls the "3rd Platform." It's an era in which risk is shared across multiple organizations.

Many businesses are struggling with the long transition period. Instead of making risk-based decisions, some organizations are quick to move forward without consideration of how to maintain adequate protection of key assets. Small and midsize businesses are prime examples of organizations that need to move quickly to lower costs, boost employee productivity, and outsource IT support. But in this period, security is also adapting to cloud, big data/analytics, mobility, and social business — the key areas that broadly make up the 3rd Platform.

In this new era, the threat reduction paradigm long associated with mainframes and PCs is requiring businesses to consider taking on additional risk to improve user experience. Enterprises are also increasingly seizing the opportunity to outsource their email infrastructure, migrating on-premises deployments of Microsoft Exchange to Office 365, for many of the same reasons early adopters began using these services.

The classic model of protecting employees from email attacks and other threats is changing with new promises of security being "built in" and data being contained in hardened datacenters managed by a few "trusted" specialists.

Adoption of SaaS services shouldn't be followed by a decrease in the budget for information security technology and services. IDC's recent *Cyber Threat Survey* of more than 300 security practitioners found that despite the adoption of SaaS-based services that have embedded security capabilities, 53% of those surveyed said their budget for security increased by 25% or more.

Email, File Sharing Risks Require Attention

The threat landscape is supported by a global network of organized criminal gangs that prey on organizations that are not taking security into consideration when outsourcing traditional on-premises systems to cloud-based services. Email continues to be the main mechanism used by attackers to gain initial access into an organization, with an estimated 90% or more of threats emanating from email. Targeted email messages and spam campaigns can deliver malicious URLs and file attachments that evade traditional antivirus and network security appliances.

File sharing also introduces security risks that could put critical corporate data in jeopardy. There have been documented cases of spyware, worms, and other malware embedded into files shared using popular consumer-based file sharing services. One risk is sharing files with users or devices where IT doesn't control security, such as remote users on personal devices or trusted partners. Criminals can move from a partner-used shared system, which is what happened in the Target data breach (a billing system in that case). In fact, Verizon's *2015 Data Breach Investigations Report* indicates that 75% of attacks spread from victim 0 to victim 1 within 24 hours.

While most services have bolstered their security posture to identify and block fraudulent activity, no service is immune to threats. Employees themselves pose a data leakage threat. Unfamiliarity with file sharing service settings can cause share folders to be inadvertently made publicly available. Services also have their own privacy policies, often enabling technical support to gain access to user data. File sharing accounts are also susceptible to account hijacking or fraudulent access through the use of stolen passwords.

The rising level of attacker sophistication and the increasing complexity of corporate environments have lengthened the time it takes to identify and eradicate threats. IDC's survey data found that it takes a week or more on average to detect a successful attack. Nearly half of those surveyed indicated that it took another month before the threat was remediated. According to the survey, the top targets for these attacks are customer or patient information, proprietary business data, intellectual property, and bank account and credit card data.

Adopters of Office 365 and other SaaS-email services must consider the following threats:

- **Phishing.** Criminals have improved their social engineering skills and have the ability to craft convincing messages to lure victims into opening file attachments or clicking on malicious links. Scrubbing technologies provided by SaaS-based email providers are not 100% effective. Techniques to evade detection have become increasingly sophisticated. One of the latest discoveries uses digital steganography to embed malicious code within an image, audio, or video file to bypass traditional network security defenses.
- **Account hijacking.** Criminals can steal and use stolen account credentials in seconds to gain access to sensitive email messages and other files associated with an employee account. An attacker who successfully hijacks an account appears as a legitimate user and can leverage the email or file sharing account of subordinate employees to social engineer a convincing attack against managers and other executives with higher privileges.
- **Insider threats.** This threat category includes employees with malicious intentions and employee gaffes. The potential for bypassing security controls maintained by the SaaS services provider is high. Unintentional employee errors can also arise as a result of an erosion of internal enforcement mechanisms and visibility into the SaaS provider's environment. In addition, an organization that is placing its trust in an outside service to manage email and protect sensitive data must also manage potential changes in employee behavior with regard to how messages and sensitive data are protected.

Trust Is a Two-Way Street

Support and cost are significant factors for businesses in determining whether to migrate from an on-premises Exchange deployment to Office 365. Security has been a secondary issue, but the growing number of high-profile data breaches and the continued focus on so-called advanced threats have caused security and privacy to be a significantly growing concern among senior leadership and boards of directors.

Word, Excel, and PowerPoint have been favorite targets of attackers who use the popular applications to gain a foothold into corporate environments. The application files are frequently used as phishing lures in email attachments. If the attachment gets past Microsoft's scanners and network monitoring capabilities, the risk is high that the file attachment will stealthily deliver a malicious payload. Furthermore, malicious campaigns documented by security researchers have uncovered sophisticated redirects and other malicious techniques that can serve to steal account credentials and gain unfettered access to an employee account.

The attack surface of SaaS offerings is increasing, and IDC predicts that additional feature sets and connections to other technology partners will raise the risk profile of Office 365. Microsoft has already begun building out partnerships with Web-based file sharing and collaboration services. It struck a deal with Dropbox to integrate the file sharing service's cloud storage into Office 365. The partnership enables users of Dropbox to link their account directly with Word, Excel, and PowerPoint and also provides mobile access.

As more third-party partners have the ability to tap into some Office 365 data to support users of the service, the attack surface of Office 365 increases, giving criminals a potential avenue to probe for weaknesses and use when targeting an employee. Security incidents have already been well documented in file sharing services, with criminals taking advantage of a high level of employee trust in cloud-based services and using those services to spread malicious links or as a platform to conduct broader attacks.

The benefits of direct cloud-to-cloud integration using Office 365 are substantial. Microsoft provides malware protection for email, SharePoint, and OneDrive. Microsoft uses a malware signature engine, still the primary way most malware is detected, which updates hourly. Many endpoint security platform makers can find tens of thousands of threats in that one-hour window and offer customers much faster update times. Security vendors are also adding a mixture of on-premises and cloud-based sandboxes for the analysis of suspicious files. These sandboxes can identify so-called advanced threats that are often hidden inside standard office file formats and associated with targeted attacks.

Conclusion and Recommendations

Businesses that consume SaaS services must continue to maintain effective security measures, which means proactively assessing the status of the security program. Ultimately, the final responsibility for data governance and enforcement of security policies and effective processes lies with the business owner, not with the SaaS services provider. In the event of a data breach, business owners can no longer point a finger at their third-party partner as the cause of a lapse. A security assessment should thoroughly review the state of the organization's security program in the following areas and incorporate the risk tolerance of senior executives and boards of directors:

- **Security policy.** Ensure that security policies are thoroughly reviewed and clearly communicated to employees on a regular basis. Incorporate how the adoption of Office 365 and other SaaS services could disrupt policies created for on-premises infrastructure. Establish a policy review process that incorporates impacted data owners and a representative from the IT team. Internal security controls should be in place to enforce policies.

- **Security technology.** Thoroughly assess your current security technologies and determine whether they can be extended to safeguard messaging and file sharing traffic associated with Office 365. Scan the environment for configuration weaknesses and vulnerabilities that are exposed as a result of the migration to Office 365. Decide the efficacy of the security technology in place and whether it requires additional components or adjustments to handle changes to the environment associated with SaaS services adoption.
- **Security culture.** A corporate environment that has a strong security-minded culture is not fostered overnight; however, if precautions are not taken, that culture can quickly erode when security is outsourced. The SaaS services provider security commitment can instill a false sense of security and foster changes in employee behavior that result in security incidents and, potentially, a costly breach. Review current data handling protocols and communicate employee responsibility for proper data handling. Establish a security awareness training program that is sustained throughout the year.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com