computer dimensions

520.743.7554
info@computerdimensions.net
www.computerdimensions.net

Malicious Activity in the Office 365 Cloud

The accelerating migration to the cloud is creating an attractive target for cybercriminals. One of the primary cloud offerings is Microsoft Office 365 which is being heavily targeted. I have provided a brief history of Office 365 attacks in order to illustrate the challenges of effectively protecting employees from danger once your company makes the move to a cloud offering such as Office 365. It is also worth pointing out that Office 365 is considered to be one of the more secure cloud offerings.

Let's start by taking a look at some recent history of publicly recorded attacks.

In June 2016 at least ***57 percent*** of all Office 365 customers received at least one malspam attempt that contained an infected Cerber ransomware attachment. It took Microsoft several hours to update their levels of protection to stop the attack coming into the environment. At the time they had 18 million subscribers. That number increased to 120 million in 2017, and they expect to have at least two-thirds of business customers in the Office 365 cloud by the end of fiscal 2019. Clearly, this is an increasingly juicy target for all sorts of threat actors.

In July 2017 there was a sophisticated attack targeting high-level employees of Fortune 2000 organizations. Within each organization, the attackers targeted a small number of senior employees across multiple departments. It revealed that attackers know that Office 365 is ripe to be exploited and that we should anticipate that attacks against Office 365 will proliferate in the foreseeable future.

In March 2018 millions of Office 365 accounts were hit with Password Stealers, a wave of malspam attacks that tried to dupe users and ***steal their passwords*** by disguising malicious emails as tax-related notifications from the IRS.

In May 2018 researchers spotted in-the-wild attacks using a method to bypass the advanced threat protection features in Office 365. Dubbed BaseStriker, the attack was tested against several configurations and found that "***anyone using Office 365 in any configuration is vulnerable,*** "be it web-based client, mobile app, or desktop application of Outlook.

Last year **Microsoft** saw malware attempts targeted at Office 365 increase ***600 percent*** and even higher numbers are projected for 2018.

520.743.7554
info@computerdimensions.net
www.computerdimensions.net

Conclusion

You should expect breaches to occur when under attack from constantly evolving threats, especially when dealing with environments full of untrained employees and lacking multi-tiered security. With this conclusion in mind, here are ***3 top tips*** for securing Office 365.

1. ***Use Multi-Factor Authentication***. Even if credentials are stolen, it restricts the attacker from moving forward with the attack.

2. ***Trust no URL or attachment***. It is always best to avoid clicking URLs or attachments in your email.

3. ***Apply best practice, implement Defense in Depth***. Augment Microsoft's own security controls. You can be sure that sophisticated threat actors will already have tested any malicious attack targeting the Office 365 environment against Microsoft's own security tools to increase their success rate. Utilize multi-tiered security with a business class firewall, additional email security and regularly tested backup measures.