PAPER

Redmond MAGAZINE

HOW TO ENHANCE THE RESILIENCE OF YOUR OFFICE 365 DEPLOYMENT

mimecast®
unified email management

www.mimecast.com

Based on a recent webcast featuring a computing thought leader explaining the Microsoft shared responsibility model for Office 365 security.

What are we talking about when we talk about resilience in terms of Microsoft Office 365 deployments?

Tim Warner, a Microsoft MVP in Cloud and Datacenter Management, started a recent webcast on Office 365 by defining that term.

"Let's consider resilience to be the capacity for your workload to recover quickly from difficulties," he explained.

Your workload includes your line of business applications including ever vital email as well as things like your SharePoint farm, Salesforce.com, other Software-as-a-Service (SaaS) apps, and homegrown applications. All of these and more can fall victim to a range of hardware or software failures, power failures, natural disasters, or even a malicious insider or outsider attack.

"How quickly can you bounce back?" Warner asked. "Ideally, of course, the system never goes offline in the first place. But if it does, how quickly can you recover?"

That's what resilience is all about.

RESILIENCE AND AVAILABILITY

The next question when you deploy Office 365 is how much resilience will Microsoft provide you?

An Office 365 subscription provides you with services for the Microsoft apps business users need, including Outlook email, Word and Excel. But what about any homegrown or third-party applications your organization depends on?

Warner noted that even before there was SaaS or the cloud, hardware vendors bragged that their servers ran for years without going down. But infrastructure isn't the whole story when you are looking at resilience.

"How do we ensure high availability in IT?" Warner asked the webcast audience. "It's through redundancy, isn't it? Incorporating backups at various levels in your system design. And again this applies to the full stack of your services, hardware, software and data."

This is where IT departments moving to the Office 365 model need to read Microsoft's service level agreements carefully. Microsoft provides the Office apps

Cover: ra2studio / Shutterstock.com

and the infrastructure they run on, but ultimately you are responsible for your own data. Data security and availability in the event of a human-caused or natural disaster is your responsibility.

SHARED RESPONSIBILITY MODEL

To bridge the gap between what Microsoft provides and what IT needs to ensure data availability and security, Warner advocates adopting the shared responsibility model.

"In traditional IT," he explained, "you're managing the entire stack, from the physical to the software, to the applications and data. Obviously, you want to lighten that administrative burden and make your IT systems more agile. That's what led you to consider the cloud."

In his experience, he finds most IT departments are initially attracted to the Infrastructure as a Service (IaaS) model because it is similar to what they've been doing on-premises, so they are familiar with how it works. Prior to migrating to Office 365, IT may already be using IaaS via Microsoft Azure or Amazon Web Services (AWS). Azure and AWS provide the hardware, the storage, the networking, the service, all with high availability. But with IaaS, IT still needs to manage the OSs, and the software that's on the OSs. IT needs to keep the OS patched and maintain any line of business apps.

Platform as a Service (PaaS) has also been a favorite entry point to the cloud for some IT departments because the cloud vendor is providing most of the IT plumbing, so you can focus on your applications. Another step is end user application focused Software as a Service (SaaS) where with Office 365 the apps are fully hosted. However, Warner warned IT pros not to be misled by vendor sales pitches that say everything is taken care of by them.

IF A USER INDISCRIMINATELY DELETES EMAILS, DOCUMENTS OR SPREADSHEETS, OR A CYBERCRIMINAL HITS YOUR SYSTEMS, MICROSOFT IS NOT RESPONSIBLE FOR RECOVERING THAT DATA.

"That's a little misleading," Warner said, "because the customer always has responsibility for their data and security, no matter what."

He places Office 365 between the PaaS and SaaS models. But this is where shared responsibility comes in, regardless of the marketing hype. Microsoft with Office 365 will make sure that your data in Office 365 is available. However, if a user indiscriminately deletes emails, documents or spreadsheets, or a cybercriminal hits your systems, Microsoft is not responsible for recovering that data.

WHAT COULD GO WRONG?

For example, if you have an employee using your SharePoint Online solution, and they delete files and frequently empty their recycling bin, then after 30 days, you may have a problem retrieving documents that may suddenly be needed for legal, regulatory, or other business reasons.

"If you need an email back or you need a file from the SharePoint document library back and you aren't able to retrieve it," Warner said. "That's where you run into the pain point of 'Oh, man, I thought Microsoft just automagically backed-up everything.' But that's not true. That's your responsibility."

To be clear there is no evidence that Microsoft has ever accidentally lost data that is saved in Office 365, but they are not responsible for data that is accidently or purposely deleted by users, the organization, or encrypted by cybercriminals.

"The business continuity disaster recovery (BCDR) truth with Office 365 is that Microsoft provides data availability," Warner said. "They have all this documented in their Office 365 service level agreements. Your Exchange Online mailboxes will be available, your OneDrive content, your SharePoint Online content will be available, but they put limits on how long they keep data, especially deleted data." And of course this availability is an SLA, not a technical guarantee.

Microsoft takes a lot of work off the shoulders of IT professionals.

"I know from personal experience," Warner said, "that maintaining Exchange on-premises is an absolute bear. From database management to high availability and clustering, it's a lot of work. And the fact that you're paying per user licensing in Office 365, for Microsoft to take all that off your shoulders is a really appealing thing."

Microsoft provides mailbox recovery but Warner noted that there's a catch.

"Here's where you're hitting the wall by default," he said. "After 30 days, a deleted mailbox is not recoverable. Again, open a support ticket. Is it possible Microsoft could get it back? I've never heard of it happening, honestly. They're pretty hard and fast about these retention policy rules. Deleted item recovery, could be a file or email message. There's a couple of levels of that in SharePoint online and OneDrive and Outlook, but again, there's a 30-day max after which the items are not recoverable if they've been purged from that second level recycling bin." And just think what it feels like to have to execute this recovery process by opening a support ticket!

WHAT ABOUT SECURITY?

One aspect of resilience planning is preparing for downtime, unexpected downtime, and unavailable data. But how often does that occur?

"If you're not worried about the hardware and the datacenters and Microsoft is providing that high availability, what are some other ways where you could lose data?" Warner asks.

There is the issue of users deleting data accidently or on purpose as covered above. Then there is the major issue of malware and cybercriminals. Sophisticated phishing attacks can result in credential stealing and data locking and theft. Ransomware can be launched from a malicious attachment from an innocent-looking email. We've all heard the horror stories.

"Office 365 does have quite a bit of what they call threat intelligence available," Warner noted. "But once again, the catch is in many cases they're extra products with separate administration consoles and separate pricing. They'll tie into your O365 infrastructure but it's not a single pane of glass. They're also separate tools with separate learning curves."

"BUT THERE ARE GAPS IN THEIR SECURITY," TIM WARNER SAID. "THERE'S A GAP IN TERMS OF LEARNING CURVES, THERE'S A GAP IN TERMS OF SEPARATE PRODUCTS WITH SEPARATE LICENSES." THERE ARE ALSO MAJOR GAPS IN TERMS OF SECURITY EFFICACY.

Microsoft Exchange Online also has security specific add-ons such as Microsoft Exchange Online Advanced Threat Protection (ATP), which costs extra money. It is "a cloud-based email filtering service that helps protect your organization against unknown malware and viruses by providing robust zero-day protection, and includes features to safeguard your organization from harmful links in real-time," according to Microsoft.

So there are downsides in terms of added costs and the need for additional training and work for the IT department. To an extent this is counterproductive to the goal organizations have when they sign up for Office 365. The objective is to limit costs and reduce the workload.

"But there are gaps in their security," Warner said. "There's a gap in terms of learning curves, there's a gap in terms of separate products with separate licenses." There are also major gaps in terms of security efficacy.

"To summarize," Warner said, "Office 365 is a really nice, robust toolset. And as far as the security side of resilience goes, they leave that largely-to you. And they leave the data backup entirely to you."

That is why he recommends finding a third-party that will help you close those gaps without putting extra workloads on IT departments that may already be stretched thin.

MIMECAST CYBER RESILIENCE FOR OFFICE 365 EMAIL

Through its 100 percent cloud-based service, the Mimecast Cyber Resilience for Email solution delivers: Threat Protection, Adaptability, Durability and Recoverability. It does this by combining Mimecast's Advanced Email Security, Cloud Archiving and Recovery, and

Email Continuity Services into a single, integrated solution. In addition, a simple per-user subscription model eases licensing and brings cost certainty.

Threat Protection and Adaptability—Advanced Email Security

The Mimecast Advanced Email Security service, which includes Targeted Threat Protection—URL Protect—Attachment Protect—Impersonation Protect—Internal Email Protect—is a set of security services that helps organizations defend against and adapt to advanced email-borne threats. This service defends against impersonation attempts, malicious URLs and malware attachments, as well as spam and more commoditized viruses.

Recoverability—Mimecast Sync & Recover for Microsoft Exchange and Office 365

The Mimecast Sync & Recover service delivers rapid and granular recovery of mailboxes, calendar items and contacts, lost through inadvertent or malicious deletion or corruption.

Easy to deploy and as a fully integrated extension to the Mimecast Cloud Archive with one year of data recovery, it eliminates the need for standalone email backup and recovery systems. At the push of a button, Sync & Recover automates the recovery of individual emails, entire mailboxes or folders. It also enables administrators to manage archiving and data resilience from a single administrative console.

Durability—Email Continuity

Preserving the ability to conduct business during an email impacting incident, the Mimecast Continuity service eliminates email downtime by enabling employees to keep sending and receiving email in the event of an outage of the organization's primary email system. Critical security, corporate, and retention policies remain in place during a continuity event. Mimecast works with mail solutions that are on-premises, in the cloud—such as Microsoft Office 365—or with hybrid deployments.

KEY FEATURES

- 100 percent cloud-based, integrated cyber resilience for email solution
- Protects against advanced email-borne threats, including phishing, malicious URLs, malware and impersonation attacks
- Eliminates email downtime in the event of outage of the primary email system
- One Year of email data recovery
- Automated recovery of emails and associated data resulting from accidental or malicious deletion or corruption
- Simple per-user subscription model, which eases licensing and brings cost certainty

For more information:
www.Mimecast.com

mimecast®
unified email management