1105 MEDIA PAPER

Redmond MAGAZINE

THE DANGERS OF NOT DEPROVISIONING

IT can't forget to close the door once an employee departs by fully deprovisioning their systems.

backupify
a datto company

www.backupify.com

When an employee resigns or is otherwise let go, it’s easy to lose sight of the potential damage that can be done with the departed employee’s active credentials. While IT might focus more closely on technology provisioning for new hires, deprovisioning departing workers is equally critical.

Employees leave a company and leave behind their company-owned PCs or notebooks. The log-in credentials associated with those employees and their equipment can still give them access to sensitive data on the corporate network. And former e-mail accounts often remain active for weeks if not months. While setting up new hires to get them productive is indeed important, leaving the door open after an employee leaves is simply asking for trouble.

The Sony Pictures data breach in late 2014 is a cautionary tale about the consequences of deprovisioning failure. “This boiled down to a disgruntled ex-employee who discovered that he or she was able to gain access to their company data even though they were not with the company anymore, and they leveraged that access to devastating results,” says Tim Warner, author evangelist with Pluralsight.

The woes Sony experienced following that extremely public data breach were numerous. “The corporation was publicly embarrassed. There was a lot of personally identifiable information exposed, and their intellectual property. At least one movie was released to the public and there was lost public trust,” says Warner. “Those are truly devastating things … Sony is big enough they’re still around, but it still cost them a lot.”

Similar data breaches constantly fill the headlines, making a cautious and consistent deprovisioning policy and procedures more important than ever. The good news is that deprovisioning is a relatively straightforward process; it just can’t be ignored or delayed.

AVOID A “RESUME GENERATING EVENT”

During a recent webcast, Warner focused on what IT can do to properly accomplish deprovisioning in the cloud-based Software as a Service (SaaS) world, especially with the widespread adoption of application stacks Microsoft Office 365 and the Google G Suite. This is a whole new world compared to the relatively recent past

Cover Image: jijomathaidesigners / Shutterstock.com

when all the operating systems and applications were stored and managed onsite.

The failure to get deprovisioning right and leaving security gaps in your infrastructure can be what Warner calls an RGE—a resume generating event. If your company goes down, you might need to make a career change, or at the very least a job change. Warner recounted the days of primarily on-premises storage, where closing the door after employee departures was a much simpler process. "The employee leaves the company and you immediately disable their Active Directory user account, assuming you are a Microsoft shop," he says. "You take ownership of their computer. You take ownership of their files, pretty much done and done."

Deprovisioning was easier to handle in this type of setting, because you were dealing simply with on-premises infrastructure, which you own and manage directly. With cloud-based SaaS, application management is quite different. Warner advises IT pros start learning how to do deprovisioning in the cloud world. "Let's say we are using Office 365 and we've got a lot, maybe even a majority of our actual property stored in this cloud," he says. "What can we do to protect it in the context of user deprovisioning?"

WHERE IS YOUR DATA?

It is important to remember that while cloud vendors provide high availability and storage scalability, they are also storing data at various locations around the world. "It's no secret the vendor in most of these cases is not backing up that data themselves," says Warner. "You need to do that. You need to provide the security of your data as well as for disaster recovery."

"WE ARE USING OFFICE 365 WITH OUR ACTUAL PROPERTY STORED IN THIS CLOUD. WHAT CAN WE DO TO PROTECT IT IN THE CONTEXT OF USER DEPROVISIONING?" —TIM WARNER, PLURALSIGHT

Back then, organizations owned the entire lifecycle of employee technology—their hardware, their software, and their credentials. As far as compliance with government or industry-specific regulations, companies were required to backup and archive data to fulfill those mandates. Organizations might also have to transfer data to the employee's replacement or the rest of his or her work team.

Using a cloud service provider to store corporate data is an effective strategy, but it does not absolve the organization of the responsibilities of protecting and managing their individual users' data. Data backup must be part of a larger disaster recovery strategy when relying on cloud service providers.

Companies need to research how their cloud provider handles deprovisioning. They need answers to questions like: what happens when you decide to move away from Office 365 and cancel your account? How long do you have to get your data back?

AFTER AN EMPLOYEE LEAVES, MOST COMPANIES WILL RETAIN DELETED DATA FOR A SPECIFIC PERIOD. ONCE THAT EXPIRATION DATE HAS PASSED AND DATA IS DELETED, IT MAY UNRECOVERABLE.

Office 365 operates on a subscription model, which is significantly different from the on-premises world when there were licenses for a certain number of seats and software was stored on discs. What do you do about a departing employee's apps when working in a cloud subscription model? "It's not as easy as just disabling an Active Directory account," says Warner. "You've got money being paid to a vendor for that license. What are you going to do? Release the license? Just keep it there? What else?"

When running Office 365, there are also many other locations where data may be stored. There is OneDrive, SharePoint online, and Exchange mailboxes. All those aspects of the Office 365 infrastructure are affected when deprovisioning a departing employee.

After an employee leaves, most companies will retain deleted data for a specific period. Once that expiration date has passed and data is deleted, it may unrecoverable. Organizations working with cloud-based storage and applications like Office 365 have to take control of and responsibility for the data lifecycle and for backing up data they need to retain.

RESPONSE OPTIONS

There are a few options for how to respond when an employee leaves the company. IT first needs to identify what is going to happen with that employee's cloud identity and license. Office 365 allows for a litigation hold on all of their data, but that can be expensive. Companies will need to consider upgrading Office 365 subscriptions to get those options. Exporting an Exchange Mailbox to a PST (Personal Storage Table) can be difficult. It's advisable to see if a cloud service provider has tools available to help with data backup, archival and deprovisioning.

The overall transition to SaaS is not always as straightforward as cloud vendors claim. IT staff may need additional training because:

- SaaS apps operate differently from their historical counterparts, and each have their own learning curve
- Office 365 and G Suite exist within wider frameworks that need contextual understanding from the Microsoft and Google ecosystems
- The SaaS solution likely has no “turnkey” deprovisioning capability

Warner recommends IT departments seek out vendors for help with data and deprovisioning-related functions, such as cloud backup, data retention and user account deprovisioning.

SIMPLY DELETING THE PLATFORM LICENSE ISN’T THE BEST OPTION EITHER, ESPECIALLY IF YOU DON’T HAVE THE DATA BACKED UP.

Fortunately, there are vendors such as Backupify (now a part of Datto) that can help IT departments back up data and help with the other tasks required to safely deprovision departing employees. “Backup can actually assist and make this process more seamless,” says Joseph Ochs, Sales Engineering Team Lead for Backupify.

Partnering with a backup vendor can also save an organization valuable time and money. While there is always the option of maintaining a platform license for a former employee, Ochs points out this has associated costs as well. It can also make data access more difficult because you have to log-in to the former employee’s account to get to the data. It is usually easier to access that data from a central repository where it has already been backed up.

Simply deleting the platform license isn’t the best option either, especially if you don’t have the data backed up. Exporting the data locally is another option, but Ochs points out that you lose some of the cost-savings you gain from moving to the cloud because you are going back to maintaining data on an on-premises server. Data access can also be an issue if you have to upload a PST before you can search an ex-employee’s email.

The option of going to a third-party backup vendor, while adding some costs, can eliminate the unnecessary price of maintaining platform licenses for employees who no longer work for the company. This can add up to substantial costs, especially for companies that experience more than 30 percent employee turnover per year and maintain licenses for all of those departed workers. SaaS backup can archive data for all employees both active and departed. “I’ve worked with companies that have seen massive cost savings,” says Ochs.

THE OPTION OF GOING TO A THIRD-PARTY BACKUP VENDOR, WHILE ADDING SOME COSTS, CAN ELIMINATE THE UNNECESSARY PRICE OF MAINTAINING PLATFORM LICENSES FOR EMPLOYEES WHO NO LONGER WORK FOR THE COMPANY.

For companies with traditionally high employee turnover, Ochs has seen cases where a company had 1,500 active employees and 1,500 former employees for whom the company was still paying licensing fees. “They were able to pay for Backupify with the money they saved on the licenses for former employees. In addition, it provided backup for the data being created by the active employees,” says Ochs.

The security benefits and cost savings point out that deprovisioning is not something to take lightly or put on the back burner. When an employee shuts the company front door for the last time, the door on their access to company resources should be shut as well.

Find out more

http://www.backupify.com

backupify

a datto company