Office 365 Security Pain Points – Identity and Privileges

Three Ways to Stop Identity Attacks in Their Tracks

PART TWO IN A FOUR PART SERIES

CoreView

Office 365 Security Pain Points – Identity and Privileges

Smart IT shops load up on anti-virus/anti-malware, firewalls, as well as intrusion detection and prevention systems. But that still leaves Office 365 vulnerable to identity and privilege abuse and attacks.

In fact, a survey of 27 million users across 600 enterprises found that 71.4% of Office 365 business users suffer at least one compromised account each month.

Osterman Research surveyed Office 365 IT managers, and 71% of those asked struggled to "audit, manage and control privileged access into Office 365 applications."

Here are three ways hackers exploit O365 identity and privileges, and how to stop them.

In fact, a survey of **27 million** users across 600 enterprises found that **71.4%** of Office 365 business users suffer at least one compromised account each month.

Identity and Privileges

1. The Pain: Administrators Have Too Much Power

Did you know that 80% of SaaS breaches involve privileged permissions? And that admins have the most privileges of all?

So how do you mitigate/reduce the breach risk related to your Office 365 operator's rights? IT veterans may chime in with role-based access control (RBAC), low levels of which indeed exist within Office 365.

However, Microsoft simply does not provide a granular RBAC. With CoreView, you can segregate your operator responsibility by implementing a truly granular RBAC – but first ask yourself:

- Why is Segregation of Duty a must-have for your organization?
- What are the regulatory constraints?
- What is the risk if you do not implement it?
- What the business impact of not implementing it?

With Office 365, administrative rights is an all or nothing affair. Under the O365 centralized admin model, all administrators have global credentials, which means they can touch each and every user. Not only is this deeply inefficient, it creates huge security problems in two ways. First, if an O365 admin account is compromised, the hacker can access the entire environment, wreaking widespread security havoc. Second, the O365 admins themselves may have bad intentions, and become your worst security nightmare.

The native Office 365 Admin Center focuses on providing global admin rights, giving admins who tend to work locally too much power and privileges they do not need. This centralized management model of setting privileges with Office 365 entirely relies on granting "global admin rights" – even to regional, local, or business unit administrators. There is simply no easy facility for setting up regional and other geographic-based rights. Nor can you easily set up rights based on business unit, country, or for remote or satellite offices. In addition, you cannot easily limit an admin's rights granularly so they can only perform limited and specific functions, such as changing passwords when requested.

CoreView addresses these pain points with our Role-Based Access Control (RBAC) features that give you fine-grained control over what admins can, and cannot do.

Microsoft simply does not provide a granular RBAC. With CoreView, you can segregate your operator responsibility by implementing a granular RBAC – but first ask yourself:

Why is Segregation of Duty a must-have for your organization?

What are the regulatory constraints?

What is the risk if you do not implement it?

What the business impact to not implementing it?

Identity and Privileges

A proper approach to Office 365 permissions and privileges is partitioning permissions based on roles through RBAC, resulting in far fewer, truly trusted global administrators. These global admins are augmented by a set of local, or business unit focused admins with no global access, all leading to far better protection for your Office 365 environment.

Using a simple, intuitive interface, CoreView lets IT segment the Office 365 tenant in myriad ways — for example, by department, business unit, or location. After these groups are set up, IT can dive deeper, using CoreView's RBAC capabilities to define specific permissions for administrators who then can only perform certain tasks and only against a specific subset of users.

With CoreView, IT can take the entire organization served by Office 365 and break it into logical groups, or sub-tenants, perhaps based on Active Directory (AD) attributes or custom tags on the CoreView side. Once the organization is logically divided, regional admins can be assigned to the sub-tenants.

CoreView further allows you to fine-tune what actions each admin can perform, and which reports they can see. Instead of using the Office 365 Admin Center, your administrators simply log into the CoreView portal. Here, they are limited to making changes only to their assigned users, and can only perform actions they are specifically assigned. Find out more by reading our Learn to Love Office 365 Role-Based Access Control blog.

With CoreView, IT can take the entire organization served by Office 365 and break it into logical groups, or sub-tenants, perhaps based on Active Directory (AD) attributes or custom tags on the CoreView side.

Once the organization is logically divided, regional admins can be assigned to the sub-tenants.

Identity and Privileges

2. The Pain: Hit by Credential Cracking and Elevation of Privilege Hacks

Credential cracking and theft is a growing issue. "One of the big lessons organizations should take away from this year's report is that stolen credentials are becoming a bigger problem. There were many (stolen credentials incidents), including dumps of billions of stolen credentials across a number of different underground sites. It is important for organizations to monitor for stolen credentials, especially given the tendency of people to reuse passwords across personal and business accounts," according to the Verizon 2019 Data Breach Investigations Report. "60% of attacks against web applications involved the compromise of cloud-based email accounts using stolen credentials," the Verizon report concluded.

Also according to this report, 80% of all hacking-based breaches exploited weak or compromised credentials. Moreover, 29% of all breaches, including all attack types, relied on stolen credentials.

Implementing a Role-Based Access Control (RBAC) system in your Office 365 environment can mitigate these risks, as well as prevent Shadow IT and malicious IT personnel, but it is often not enough.

What exactly is privilege? "Privileged accounts are those granted privileges beyond everyday user accounts. Having access to privileged accounts provides a threat actor (or legitimate user) with access to additional systems and services. These are often among the first targets of external attackers or malicious insiders intending to cause financial loss, data loss and reputational damage," explained the Verizon Insider Threat Report.

One of the best practices is to ensure that privileged accounts are used for administrative tasks only, without any active services that can be used as attack vector. The problem is that it is not possible to monitor and enforce this easily on Office 365 standard admin tools.

In CoreView there is a dedicated report showing this problem that can be addressed with a targeted e-mail campaign to educate users, or with a workflow enforcing removal of services after notification to end users and then a grace period.

80% of all hacking-based breaches exploited weak or compromised credentials.

29% of all breaches, including all attack types, relied on stolen credentials.

Identity and Privileges

So how does CoreView address that issue both in terms of admin credentials – which is the biggest exposure because of the access that they have, and end user credentials and privileges?

Admins, given their high-level privileges, are themselves a security threat through nefarious actions (not all admins are saints). Just as important, if admin credentials are cracked, hackers have the keys to the kingdom. Knowing what is happening with ALL admin accounts is critical. "IT should have a monthly report of everybody who has performed administrative access against non-owned information assets. IT needs to know when admins accessed somebody else's mailbox. CoreView has a report for that. You can schedule that report, and you should review it on a monthly basis. If nothing else, when people know that you have the capability of watching and you are watching, they are more careful," explained Matt Smith, CoreView solution architect.

CoreView also has reports for accounts with passwords that do not expire, and can see which administrative accounts are also used as user accounts. "That is not a best practice. You should separate out your administrative access from your user access," Smith said. One solution is to grant temporary privileges for limited tasks. "CoreView has a workflow engine that can apply administrative access on the fly, which is similar to a Microsoft E5 feature. However, we can do it for any account," Smith said. With CoreView, you don't need an E5 license to give admin rights 'on the fly' and we can do it in a highly granular way

Admins, given their high-level privileges, are themselves a security threat through nefarious actions (not all admins are saints).

Just as important, if admin credentials are cracked, hackers have the keys to the kingdom. Knowing what is happening with ALL admin accounts is critical.

3. The Pain: Not Taking IT Insider Threats Seriously – and Suffering the Consequences

A common assumption many have is that IT, which controls the infrastructure, apps and data, is inherently trustworthy. The truth is, IT folks are just like everyone else, the vast majority are good and some aren't. When they go bad, the damage is immense.

Too often those in IT blindly trust others in IT, and give these workers higher level privileges than they need, and can be used to abuse access to corporate and personal information. According to a survey by Cyber-Ark, a third (35%) of IT pros spy on other company employees. Many times, it is simple human curiosity. Unfortunately, there are other times when critical and confidential data is lifted. The bottom line is just as IT controls end user privileges, IT privileges should be limited and controlled as well.

A Network World article, What to do When the Insider Threat is IT Itself, details the problem rogue IT presents. Here are the stats. A sizeable portion of insider breaches come from technical staff: 6% from developers and another 6% from admins, according to the Verizon Data Breach Investigations Report. Many insider incursions result from privilege abuse, though there are many other ways IT abuses its access.

"The first step in protecting your data is in knowing where it is and who has access to it," the report reads. "From this, build controls to protect it and detect misuse."

Great importance should be given to the moral character of your IT admins, after all, they do hold a lot of power at their fingertips, especially when a sizeable chunk of the business goes through IT systems.

Giving admins too many privileges and then not tracking what they do opens the door to IT insider malfeasance.

The first defense is using RBAC to only grant privileges that are absolutely needed, and only for the time these privileges are absolutely needed for. At the same time, have a system for tracking admin activities and let admins know tracking is in place. This alone can ward off many dangers.

External User Safety Checklist

Office 365 is an amazing productivity platform both internally and externally for your company. It helps remove barriers and simplifies interactions between people, empowering them to achieve more. This is amazing but…

Are you aware of how many external users you have in your tenant?

How many of them have been inactive in the last 90 days?

Who is taking care of removing them?

Are you monitoring external account activities?

Do you have you an automated process notifying external users that all activities are tracked, a log of accesses that is kept for several years and that employees are responsible for keeping confidential information protected?

Are you aware of files accessed by external users? Downloaded? Synchronized on their computers?

What happens if an external account is breached?

Do you have you a log of all activities performed by each external user?

If you answered no to more than one of these questions -- you really need CoreView.

Identity and Privileges

Even IT should fall under strict data access privilege policies, and all network activity, including activity from IT, should be tracked for security threats.

Meanwhile, CoreView maintains an immutable log of every administrative action, from the time the platform is put in place, for regular review by IT Security. By watching and reviewing, CoreView positively influences behavior. It is the same reason Wal-Mart and public schools have so many cameras. Not just to capture events, but to influence behavior through diligence.

CoreView maintains an immutable log of every administrative action, from the time the platform is put in place, for regular review by IT Security.

By watching and reviewing, CoreView positively influences behavior. It is the same reason Wal-Mart and public schools have so many cameras. Not just to capture events, but to influence behavior through diligence.

Learn How CoreView Protects Your Environment, and More

Get Started with CoreView – for Free

Our new CoreDiscovery solution will help admins understand, manage, secure, and drive application adoption for their O365 tenant. Learn more on the CoreDiscovery product page: https://www.coreview.com/corediscovery/.

Get your free software at the CoreDiscovery sign up page: https://www.coreview.com/core-discovery-sign-up/.

Want to learn how CoreView prevents overspending on licenses, underusing applications, or mismanaging security and configurations? Our free CoreView Office 365 Health Check diagnoses all your Office 365 problems. Sign up for an Office 365 Health Check and we will build a detailed 20-page report to cure all your Office 365 ills.

Not ready for a full custom report? You can still take a look at a Health Check sample report.

Want to see firsthand how CoreView solves Office 365 problems and tightens security, just request a demo.

Sign up for an Office 365 Health Check and we will build a detailed 20-page report to cure all your Office 365 ills.