SysAdmin Magazine

October 2016

netwrix

Tools & Tips for Security Admins

SysAdmin Magazine

Contents

3 Top 7 Free Tools for Security Admins

5 2 Rules to Secure Office 365 Password Policy Setup

8 Group Policy: Best Practices for Troubleshooting Performance Problems

13 [Infographics]: IT Risks Faced by Large Enterprises

14 Yahoo Data Breach: What Experts Say

16 3 Pokémon GO Security Risks

19 Free Tool of the Month: Change Notifier for Group Policy

20 How-to for IT Pro: How to Detect Who Modified Mailbox Permissions in Exchange Online

Top **7 Free Tools** for Security Admins

by Ilia Sotnikov

IT Security Evangelist

It's free, master Jedi! We've gathered **top 7 security freeware tools** for sysadmins. These tools are supposed to help you make your job easier and troubleshoot security issues faster.

1. Change Notifier for Active Directory

This freeware from Netwrix provides visibility into what's happening inside your Active Directory by tracking changes to AD users, group membership, organizational units and permissions. It sends you daily reports with details about critical changes including the before and after values made during the last 24 hours.

2. KeePass Password Safe

Free open source password manager, which helps you manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one master key or a key file. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish).

3. Malwarebytes Anti-Malware

The tool finds and removes malicious software, including rogue security software, adware, and spyware. It scans in batch mode, rather than scanning all files opened, reducing interference if another on-demand anti-malware software is also running on the computer.

4. Nmap ("Network Mapper")

Network scanning and host detection tool that can be useful during several steps of penetration testing. Can be used as a vulnerability detector or a security scanner.

5. Wireshark Network Protocol Analyzer

Open source network protocol analyzer that enables users to interactively browse the data traffic on a computer network. The analyzer operates on Unix, Linux and Microsoft Windows operating systems, and employs the GTK+ widget toolkit and pcap for packet capturing.

6. Spiceworks Network Monitor

It provides real-time monitoring and statistics for your servers and SNMP-capable network devices. The tool can be used alongside Spiceworks' IT Help Desk and Inventory Management tools.

7. NetCrunch Tools

Essential free toolkit for network professionals that runs on Windows. The toolkit provides network monitoring, server and application monitoring, network mapping, diagnostic tools and reports.

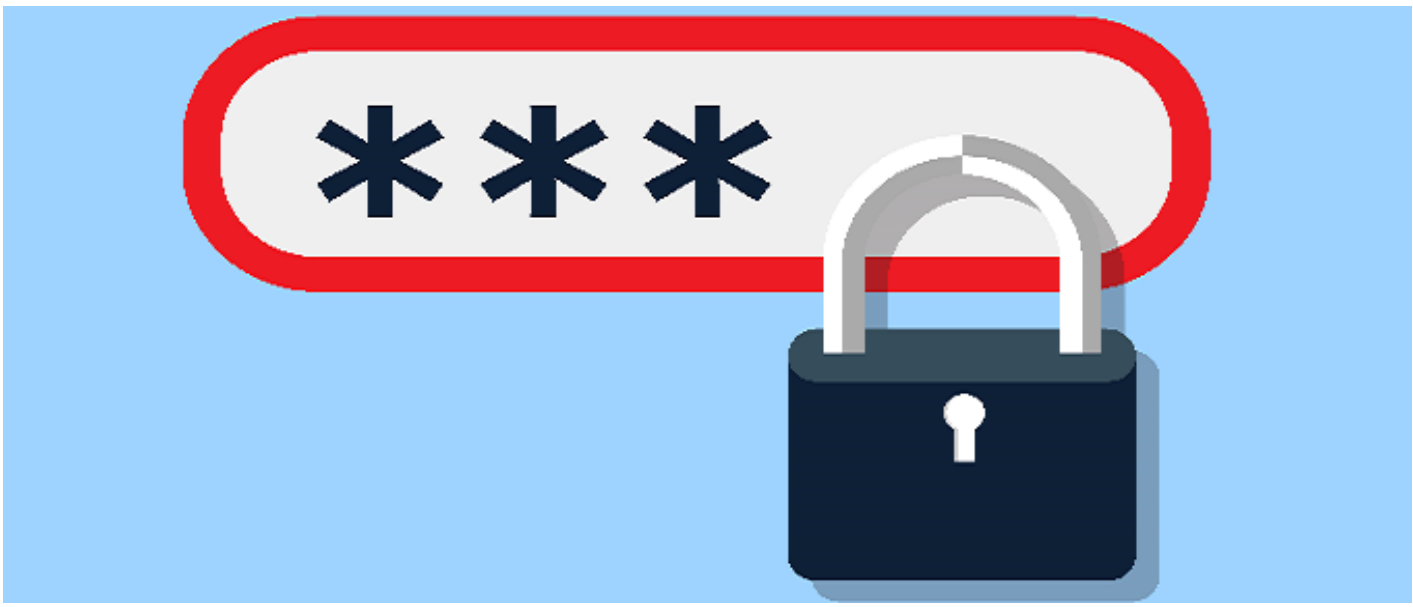
2 Rules to Secure Office 365

Password Policy Setup

by Jonathan Hassell
IT Pro, Entrepreneur

Password policy in Office 365 is much stricter and more secure than that of an on-premises application, so you no longer have to worry about setting and enforcing different authentication policies for your users. But still, you should align Office365 security settings with your overall enterprise security profile and posture.

In this blog post, I'll highlight a few rules that should be helpful for IT admins when ensure Office 365 password policy security.



Rule #1: Stay on Top of Password Expiration

By default, the password expiration period is set for 90 days. The expiration period may be increased **maximum to 730 days, but this practice is not advised as it may cause serious security risks to** business-critical data.

Here's how you can change the expiration day value:

1. Sign in to the Office 365 administrative center and go to Settings / Security and Privacy
2. Click Edit
3. Type in the number of days for a password to be valid. For most organizations I recommend this be no longer than 90 days, although if you have two factor authentication enabled you can get away with longer periods of time without compromising your overall security profile too much
4. Optionally configure when users are notified about their passwords that will soon expire
5. Click Save to retain the settings

For some accounts, like service accounts or logins used by multifunction devices to e-mail and save copies of documents scanned or faxed in, you might want to let those passwords never expire. These are typically very restricted accounts that can only do one or two things.

To get that configured, you will need to launch PowerShell and connect up to Office 365. Be sure you have both the Microsoft Online Services Sign-in Assistant for IT Professionals RTW software package as well as the Azure Active Directory Module for Windows PowerShell. Both packages are available from the Microsoft Download Center. Then, use the Connect-Msolservice cmdlet to connect to your tenant and use your credentials to authenticate.

Finally, issue the following command:

Set-Msoluser –UserPrincipalName copier@yourdomain.org -PasswordNeverExpires $true

To follow up, you can get a list of users whose passwords never expires by using:

Get-Msoluser | Select-Object UserPrincipalName, PasswordNeverExpires

NB! Beware that for accounts that you synchronize up to the cloud based on your on-premises Active Directory installation and deployment, the policies you have set and enforced on premises will carry over into the cloud and will not be affected by any changes you make in the cloud. Only cloud originating users can have their settings modified in the cloud.

Rule #2: Embrace the Two-Factor Authentication (2FA)

One of 2FA benefits is the possibility to protect a user's account even if the password is hacked. If a user's device is lost, the hacker still does not have the account password, so the impact of a loss is reduced quite a bit. Considering this, companies need to apply 2FA to Office 365 password policy setup. And here's how it could be done:

1. In the Office 365 Admin Center, go to Users / Active Users and click the 'More' menu
2. Select 'Setup' azure multi-factor authentication
3. Choose the Set up link next to 'Set Multi-factor authentication requirements', and then check the users for which you want 2FA enabled
4. Choose 'Enable' on the right

For users that use Outlook 2013 or earlier or other applications, you will need to establish an app password that bypasses 2FA since those applications don't know how to read a 2FA prompt or pass on the one-time code up to Microsoft Azure.

1. Go to the 'Service settings' link on the 2FA setup page
2. Choose 'Allow users to create app passwords to sign into non-browser applications'
3. Users will have to generate their own app passwords for use in Outlook 2013 and earlier and any other applications that use the Office 365 account

Office 2016 supports 2FA and so app passwords are unnecessary for it.

Remember that password complexity and regular password changes can help protect your data against security risks. In conclusion, let me ask you:

Group Policy:

Best Practices for Troubleshooting Performance Problems

by Joseph Moody

Deployment Engineer

There are tradeoffs to everything. In a Windows environment, users want fast logons/startups and a consistent experience across multiple devices. An efficient logon is often related to ease of use. For example, Folder Redirection and Group Policy Printer Preferences provide more unified end user experiences at the cost of slower logons. This is a classic case of speed vs. accessibility.

As more modifications are made over time, a certain amount of Group Policy bog can develop. The key to fixing Group Policy slowness is to consistently monitor its performance. In this guide, we will explore several new tools and common issues with Group Policy performance. We'll specifically focus on a Windows 10 environment.

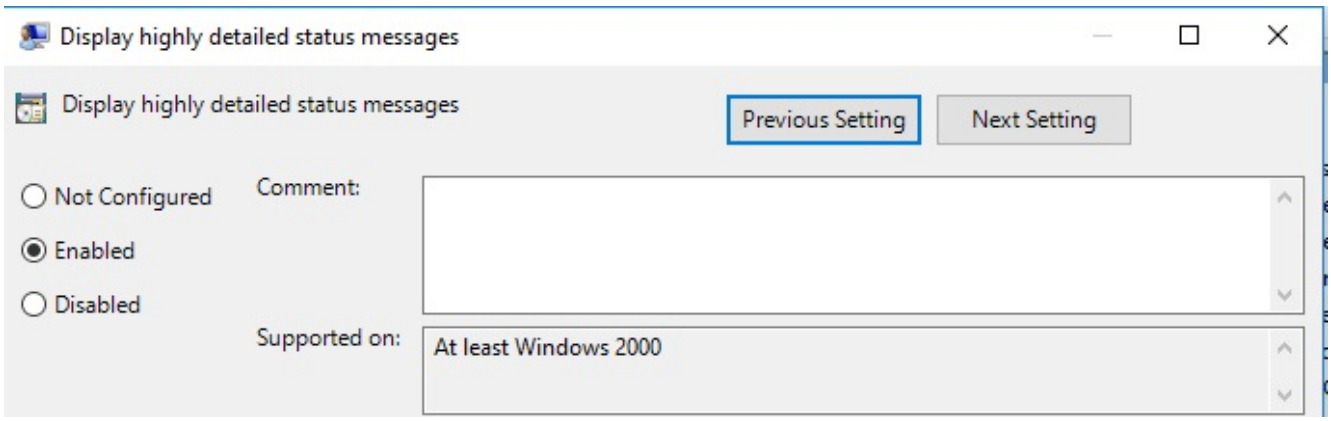
Monitoring Group Policy Performance from Clients

Very few things are more frustrating than waiting for a machine to log on...and waiting...and waiting ... and waiting. Machines with problems can often take 10+ minutes to start up or log on. The only indication that the end user receives is a *Please Wait* message or the equivalent Windows 10 *Getting things ready for you* screen.

To let users know that the machine isn't just hung up and to help you troubleshoot, you will want to enable the following two GPO settings across your machines:

- *Computer Configuration\Policies\Administrative Templates\System – Display Highly Detailed Status Messages : Setting – Enabled*
- *Computer Configuration\Policies\Administrative Templates\System\Logon\ – Show first sign-in animation : Setting – Disabled*

The first setting displays the startup component that is currently running instead of the generic startup messages. For example, you may see *Applying Group Policy Software Installation* if your machines are installing a GP deployed MSI. This setting was previously known as Group Policy Verbose mode. To make future troubleshooting easier, I prefer to enable this setting on clients and servers.



The second setting removes the *Getting things ready for you* animation that appears the first time a user logs on to a machine. The user will see some detailed status messages before the animation takes overs. This policy should be set to disabled for the user to see all messages. I prefer applying this policy to all clients. Servers do not show the first logon animation.

Monitoring Group Policy Performance from the GPMC

As a rule, administrators should always use the latest RSAT installation for the clients that they are managing. If you are managing Windows 10 clients, your administration machine should be at Windows 10 with the latest RSAT installed on it.

When running a Group Policy result within the Group Policy management Console on a Windows 10 machine, you will notice a new Component Status section under the Details tab. Components of Group Policy, such as Folder Redirection and Group Policy Printer Preferences, are known as Client Side Extensions (CSEs). This component status section will display the last evaluation status of each CSE. It will also display how long each CSE took to process. These values are also stored in the Group Policy event log on client machines.

Component Status

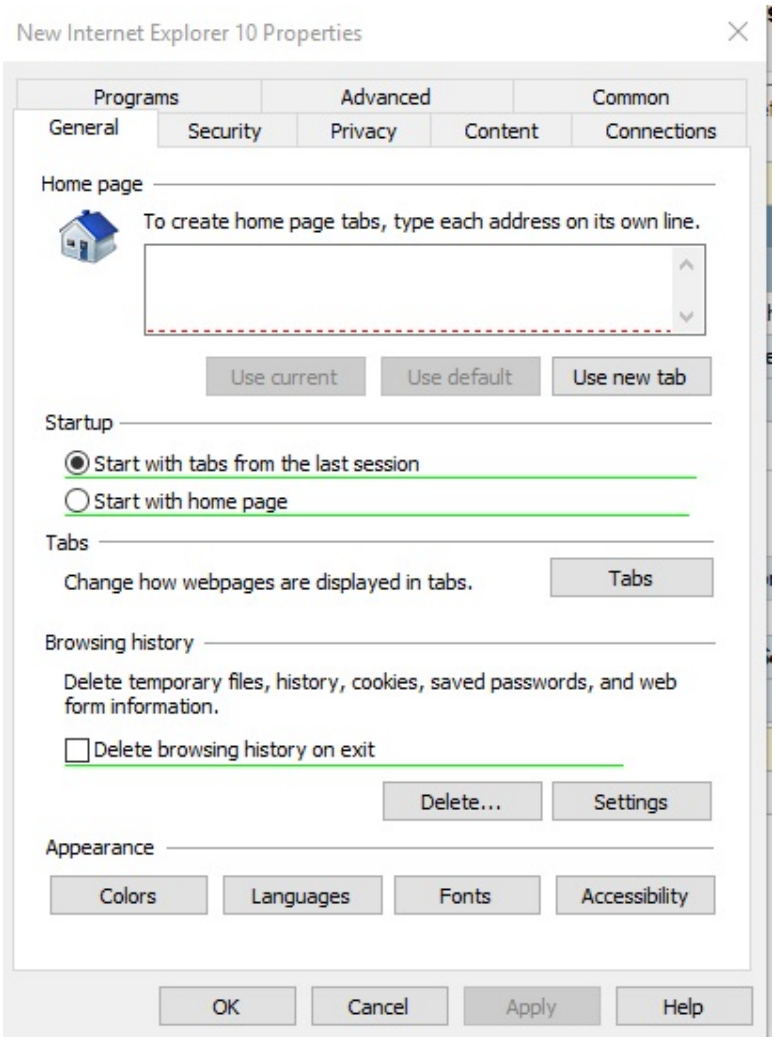
Component Name	Status	Time Taken
Group Policy Infrastructure	Success	877 Millisecond(s)
Enterprise QoS	Success (no data)	
Group Policy Files	Success	500 Millisecond(s)
Group Policy Power Options	Success	313 Millisecond(s)
Group Policy Printers	Success	485 Millisecond(s)
Group Policy Registry	Success	359 Millisecond(s)
Group Policy Services	Success	281 Millisecond(s)
Group Policy Shortcuts	Success	312 Millisecond(s)
Registry	Success	1 Second(s) 297 Millisecond(s)
Scripts	Success	
Security	Success	3 Second(s) 469 Millisecond(s)
Software Installation	Success	
Windows Search Group Policy Extension	Success (no data)	0 Millisecond(s)
Wireless Group Policy	Success	

This pane can help an administrator quickly troubleshoot Group Policy performance problems. Any item with a 600-second time failed to complete. The Group Policy service only allows a CSE 10 minutes to complete by default.

Beware the Legacy CSEs

Group Policy CSEs have evolved with each iteration of Windows or the component that they service. A perfect example of this are the CSEs that manage Internet Explorer. One of the earliest management methods involved the Internet Explorer Maintenance (IEM) extension. IEM complemented many of the features available under Administrative Templates\Windows Components\Internet Explorer. Several years later, Microsoft introduced Group Policy Preferences for Internet Explorer (IE). Having three management tools for one product became confusing for everyone!

With the release of IE10, IEM was removed from the GPMC on any machine on which IE10 was installed. This change holds true for Windows 10/IE11 as well.



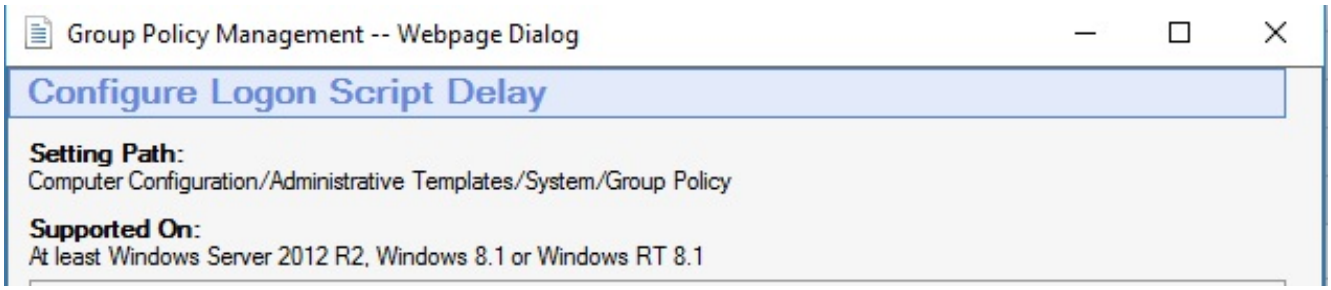
Before Group Policy Preferences (GPPs), everything in Group Policy was locked down. When GPPs were first released, many administrators treated them like an administrative template (also known as a policy setting). Many individual preference actions were changed to *Replace*, and the *Remove this item when it is no longer applied* option was set. This has the big downside of making the GPP reprocess every time Group Policy is refreshed and on every logon/startup.

Many Group Policy environments are not updated for changes in CSEs or to reflect GPP behavior. Administrators may still apply IEM settings by using the GPMC on older operating systems. When possible, administrators should look at the following alternatives for these time-inefficient CSES:

- IEM: Replace with Administrative Templates or Preferences
- Deployed Printers: Replace with Printer Preferences
- Group Policy Software installation: Replace with a software management suite such as SCCM
- Folder Redirection: Replace with an alternative such as Work Folders

You will notice that user side Group Policy scripts is not listed above. With the release of Windows 8.1, GP scripts can be configured to fire off after X seconds instead of running during the logon process.

This allows scripts to run behind the scenes after a user is already logged in. This setting can be found at Computer Configuration\Administrative Templates\System\Group Policy



Administrators should reevaluate any of their deployed preferences. When possible, preference items should use Create or Update. I personally prefer the consistency of only using the Create preference. Item-level targeting should evaluate local resources only if time is of the essence. Finally, consider shifting certain items from the user logon to the computer startup. A perfect CSE for this is Printer Preferences.

As you monitor your Group Policy's performance, you will likely find some configurations that can be undone or migrated. By using the GPMC, you can evaluate processing time across clients and focus on time-expensive CSEs. I stated earlier that there are tradeoffs to everything. Good luck in your struggle to balance speed and accessibility!

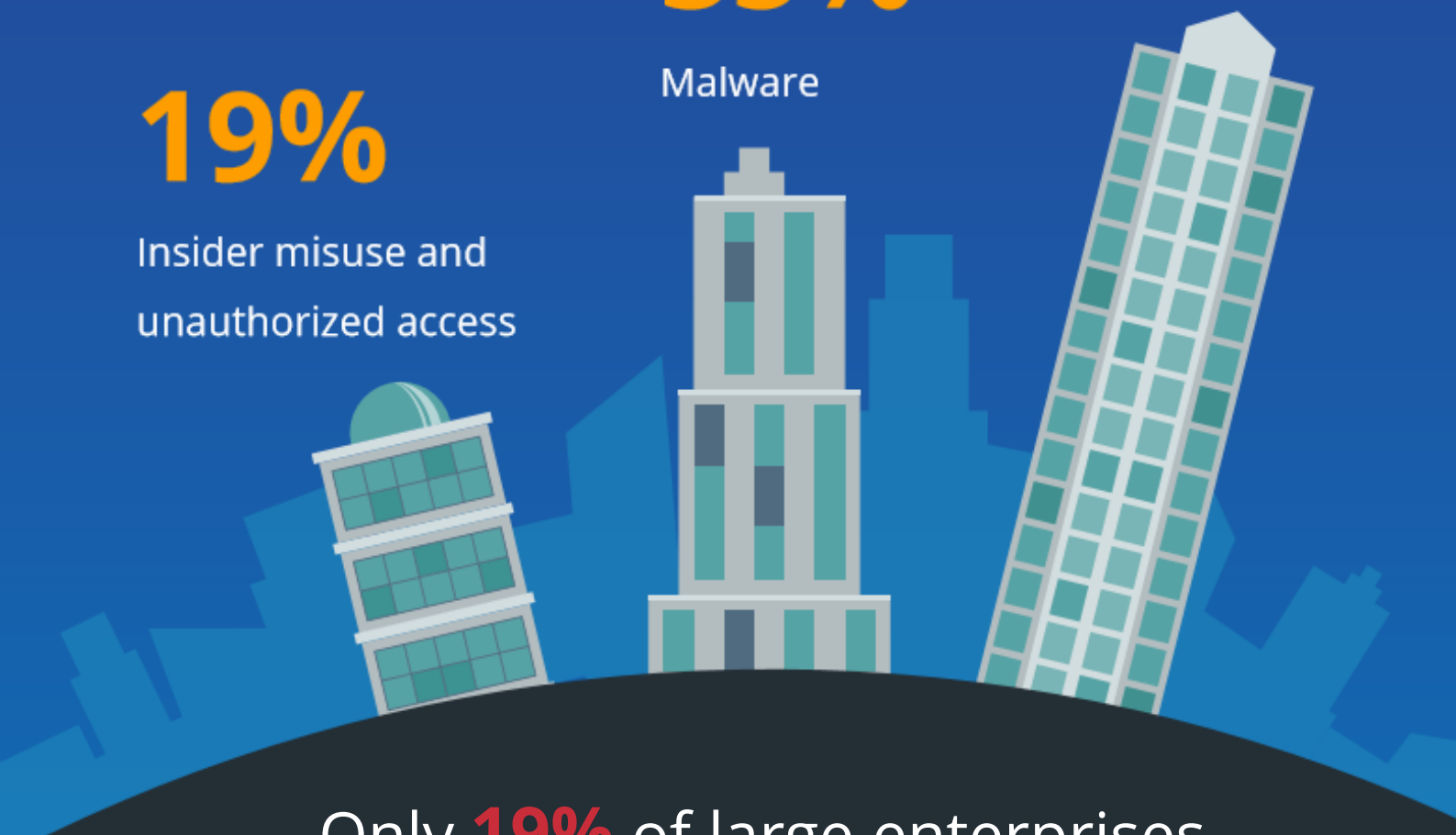
IT Risks Faced by Large Enterprises

Large enterprises worldwide experience security incidents, mainly due to

45%
Human errors

35%
Malware

19%
Insider misuse and unauthorized access



Only **19%** of large enterprises claimed they are well prepared to face cyber risks

Yahoo Data Breach:

What Experts Say

by Alex Vovk

CEO, Netwrix Corp.

It's been a few days since Yahoo confirmed a massive data breach, but we still know very little about the biggest hack in history. Who exactly was behind this attack? What the hackers obtained precisely? We still have more questions than answers. But the biggest question is about lessons businesses should learn from this catastrophe. What should they do for not being next?

In this article we have gathered insights from tech bloggers that can help companies avoid Yahoo's mistakes.

What lessons businesses should bring out of this data breach?

Brian Svidergol, IT security professional, technical consultant:

“Enterprises should spend time and money and use whatever resources are necessary to investigate cyber security incidents to minimize the potential impact to users. In Yahoo’s situation, most of the impacted accounts remained vulnerable for over 2 years.”

Richard Muniz, deployment engineer, IT evangelist:

“What should companies do? They should never assume that your security is good enough. Personally, I believe in “hacking your site”. Always probe your own defenses and see what you can do to fix those weaknesses.”

Jonathan Hassell, technical consultant:

“The most important lesson: encrypt everything. Everything. Especially personal information like names and dates of birth and security questions; not just passwords. Encrypt everything.”

Matt Hopton, IT consultant:

“Developers and enterprises remember one thing – Hash and Salt!”

Joseph Moody, deployment specialist:

“Don’t trust that you haven’t been hacked – it took Yahoo 2 years to find this out.”

Alex Vovk, Netwrix CEO and co-founder:

“Being the world’s biggest known cyber breach by far, Yahoo hack gives lots of food for thought. First, standing in the line with OPM and Blue Cross data leaks, it indicates that breaches now get more personal impact. Identity theft is on its the rise, while credit card and financial data are no longer the favorite target for hackers. Second, Yahoo has shown an unacceptable indifference to clients’ interests, putting company’s well-being above them. Holding the report on data leak suspicions back for two years is the one of the worst management mistakes that Yahoo has done – at the cost of unprecedented volume of personal data being irretrievable. While credit cards can be re-issued, the impact from privacy loss is long-lasting and has a higher risk of expansion, because stolen Yahoo accounts’ information gives enough to extract the maximum value from it. Considering this, it’s likely that government will continue working on regulations to impose stricter disclosure requirements and toughening the sentences for any organization that fails to protect personal data.”

3 **Pokémon GO** Security Risks

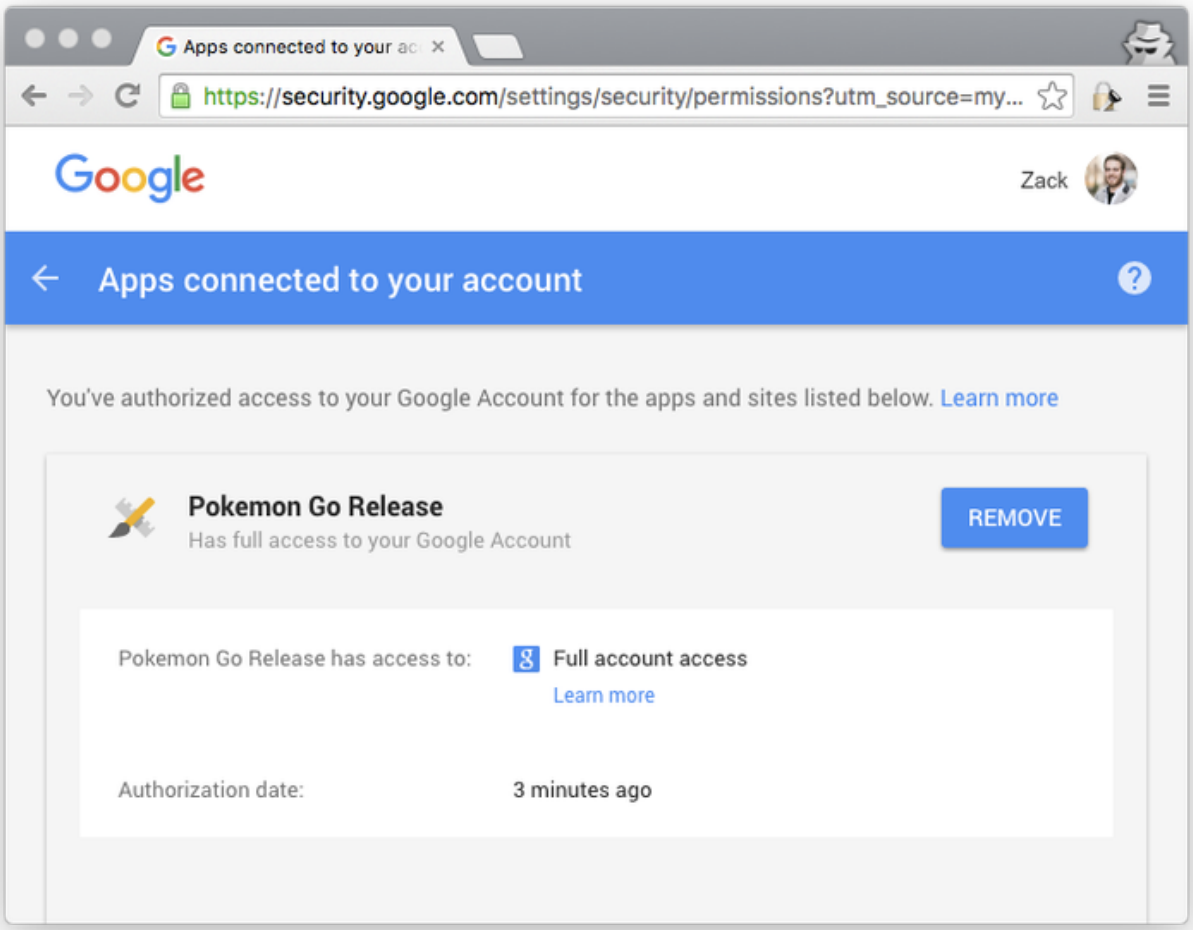
by Ryan Brooks

Product Evangelist

Are your employees or colleagues caught up in the Pokémon GO craze? Surely, most of them are. However, in the hunt to "catch 'em all," Pokémon GO users expose themselves to a variety of security risks. Moreover, playing the game presents major security risks for corporate information. In this blog post, I've listed potential risks that Pokémon GO players face as well as possible ways to avoid these risks while still participating in the game.

1. "Full Account Access"

The issue here is one of access. When a user wants to play Pokémon GO, he or she must create an account. Many users sign in using a corporate account, i.e. using corporate credentials. Doing so means that users, despite only intending to provide access to an email address and name, end up granting the Pokémon GO app full access to their Google account! This can be verified by looking at the permissions granted to the game upon logging in. What does this actually mean?



Granting "Full account access" (see the screenshot above) lets the app your emails, send emails from your account, access your Google Docs and see your photos, among many other things.

Security Tip:

Android users can edit and remove the app's "Full account access" to their Google account by going to the permissions page (check your permissions here: https://security.google.com/settings/security/permissions). For iOS users, the situation becomes a little thornier. These users must sign in using different credentials.

2. Spammy Pokémon GO Apps

Fake Pokémon GO apps are currently being heavily promoted on social media and in internet forums. It is easy to detect such fake apps because they release user information to third parties. The malicious software in these fake apps contains a script that evaluates and tracks the "victim's" online behavior. This information is then used by advertising firms to serve highly-targeted ads to the "victim."

Security Tip:

Only download the game from official sources, such as Apple's App Store or Google Play.

3. Trojanized Pokémon GO App

Hackers continue to create new malicious software and seed this software into mobile apps. In a report on Trojanized apps, Kaspersky Lab writes that this malicious software lets an attacker "bypass in-app billing to get free coins for in game items or spoof GPS locations to access areas they are not physically near." Trojanized apps may even allow attackers to remotely control a device's camera or microphone, which, in turn, could be used to enable remote recording.

Security Tip:

CheckPoint advises running security on devices that use MDM in order to detect malware or malicious apps before they embed themselves and steal data.

Naturally, these security issues will not keep people from playing the most popular mobile game in history. Nevertheless, it is very important that companies educate their employees and that people educate their colleagues about the game's potential risks. Remember, once you're empowered with caution and security consciousness, you're free to "catch 'em all!"

Free Tool of the Month

Change Notifier for Group Policy

Change Notifier for Group Policy tracks Group Policy changes, including changes made GPO links and policies, as well as software deployment changes.
It also sends daily reports with "before" and "after " values.

Example of the daily summary report

Change Type	Group Policy Object
Modified	Default Domain Policy
	Modified Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Account Policies/Password Policy
Added	Group Policy Object
	Added Computer Configuration (Enabled)/Policies/Windows Settings/Security Settings/Restricted Groups

File Server Changes Summary	
Group Policy Objects Added	1
Group Policy Objects Removed	0
Group Policy Objects Modified	1

Download

How-to for IT Pro:

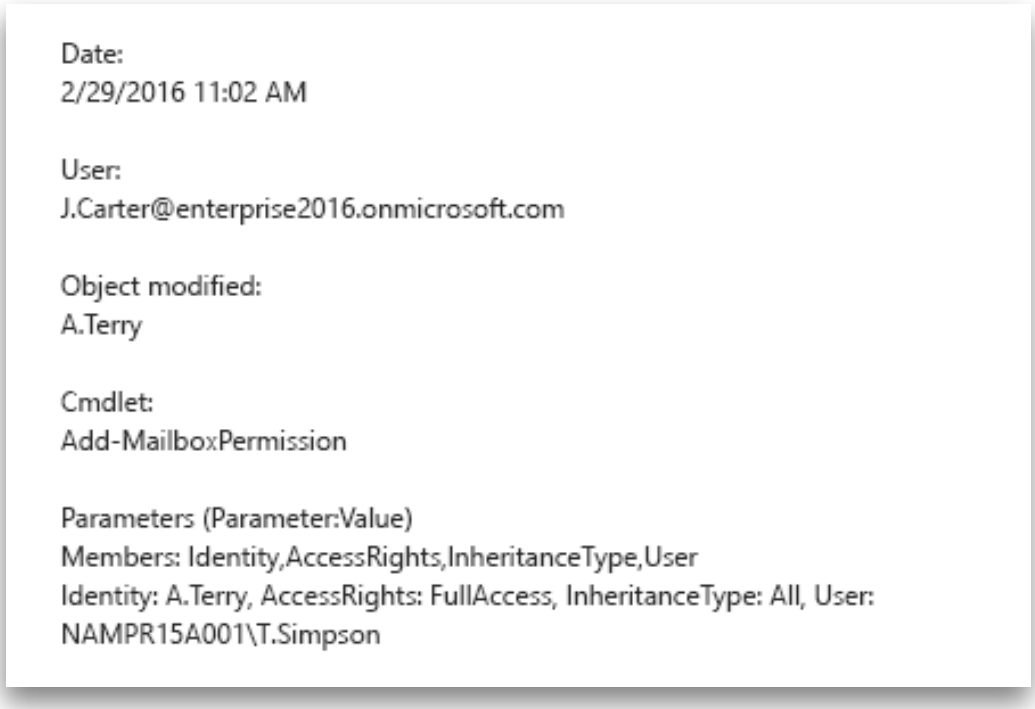
How to Detect Who Modified Mailbox Permissions in Exchange Online

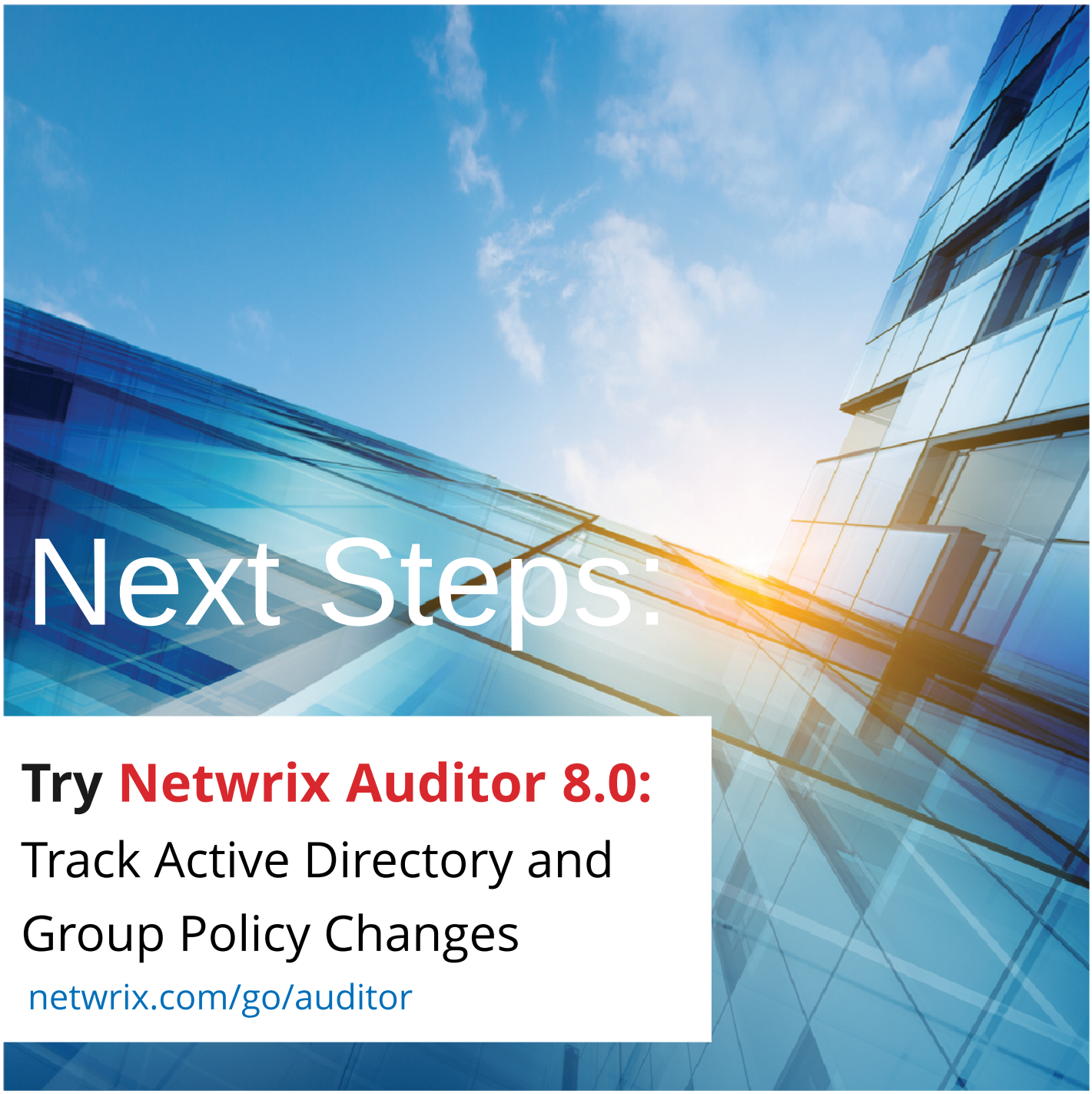
1. Open Exchange Administrative Console in Internet Explorer → Navigate to "Compliance management" → Choose "Auditing" → Choose "Run the admin audit log report..."

2. Choose a start date and end date → Click "Search". You will see all configuration changes made during the specified time period.

3. Sort the list by cmdlet and find "Add-MailboxPermission" one → Click on it for details

4. You will see who changed permissions ("User"), which mailbox permissions were changed and how ("Parameters").





Try Netwrix Auditor 8.0:

Track Active Directory and Group Policy Changes

netwrix.com/go/auditor

netwrix.com | Follow us

Corporate Headquarters: 8001 Irvine Center Drive, Suite 1100 Irvine, CA 92618

Phone: 1-949-407-5125
Toll-free: 888-638-9749
EMEA: +44 (0) 203-318-02