Global Information Assurance Certification Paper

Implementing Least Privilege in an SMB

GIAC GSEC Gold Certification

Author: Tim Ashford, tcashford@gmail.com
Advisor: Dr. Eric Cole

Abstract

Weekly headlines brim with stories of cyber breaches that target the enterprise. But SMB's need to beware: They are just as much at risk, and perhaps more so. SMB's are an easier target, and hackers know it: Smaller businesses have limited security resources and expertise. To make matters worse, they are often unaware of the dangers. It is time to take action, and SMB's can start with one key area: Fix the misuse of elevated privileges. Armed with administrative rights, threat actors have free rein over desktop systems. Once they compromise these systems, the very survival of the business is at stake. With a few strategic moves, smaller businesses can mitigate these risks, by utilizing some of the tools and strategies of their larger counterparts. The good news is that one of the best enterprise tools is free and already available in every Windows domain: Group Policy. With Group Policy, SMB's can automate tasks like limiting desktop privileges, installing and patching software, and whitelisting applications. The time is now for SMB's to enlist such readily available tools in their defense. Learning Group Policy security features will go a long way toward making the environment more secure.

1. Introduction

To better understand the problem at hand, it is perhaps best to look at how SMB's got to where they are today, in terms of privileged account access at the desktop. Together with the widespread adoption of Windows XP in the enterprise, many software programs were designed to be installed, run and updated by a local administrator. In particular, software needed access to the Program Files directory, which could only be modified by local administrators or Power Users by default (A. Beuhring, personal communication, April 4, 2015). As a result, many users were simply left to be local administrators of their own machines. With the advent of Windows Vista, User Account Control was introduced, giving IT management the option to elevate privileges as needed from a standard user account, but there were still many problems with installing and running popular programs, such as Intuit software. SMB's lacked the expertise to handle the complexity of balancing usability with security in such instances, and the easy answer became clear: continue to allow users to be local administrators. Even through the arrival of Windows 7 and later editions, it is common to find this practice.

Large enterprise security departments have known for years of the dangers of such a posture: Not only can malware execute on a single desktop, but more sophisticated versions can pivot to resources around the network, and steal large amounts of data. SMB's face the same risks as their larger counterparts, but may not have fully reckoned with those risks. The question to SMB leadership is: What would happen to your business and its reputation if your customer's data were found on the Internet? And what if a large percentage of your customers dropped you, once the news broke that you were breached, and that their data may not be safe on your network?

How are SMB's in particular affected by rising security threats? Unfortunately these businesses have it the worst, in some ways. First, they are open to the same avenues of attack as any other business, such as phishing scams, and infected web traffic, while lacking the best systems to thwart these dangers, such as host based intrusion prevention systems, or application layer firewalls. This means that opening emails and

browsing the web from an SMB endpoint is potentially more dangerous than from an enterprise workstation. Here's an example: A compromised website leaves behind a malicious program on an unsuspecting SMB user's desktop, but that danger goes undetected until long after sensitive corporate data has been stolen. Second, SMB's lack the sophisticated tools found at larger businesses, such as SIEM's (security information and event management tools), which are used to detect when systems are compromised. For example, a point of sale (POS) terminal at an SMB may be breached, but the company has no tools in place to detect that credit card data is being exfiltrated. Third, with their limited resources, SMB's tend to be easier targets overall, and require less expertise on the part of the hacker to get in. As the Verizon Data Breach Report (DBIR) from 2012 put it, "Smaller businesses are the ideal target…and money-driven, risk-averse cybercriminals understand this very well. Thus, the number of victims in this category continues to swell." (Verizon RISK Team, 2012) According to Symantec's most recent Internet Threat Report from April of 2015, 60% of the previous year's **targeted attacks** (emphasis mine) were against small and medium businesses. (Symantec, 2015) These dangers simply cannot be ignored. On the bright side, Verizon's report said that "97% of breaches were avoidable through simple or intermediate controls." (Verizon RISK Team, 2012)

What follows are some simple to intermediate controls that can limit many of these dangers that SMB's face. These controls center on reducing privileges for users at the desktop. While that may sound oversimplified, consider the finding of the Australian Government's Department of Defense report from 2014: The top four out of thirty-five recommendations (for mitigating cyber intrusions) involved least privilege access for users. In fact, if these top four recommendations were followed, they said, over 85% of the risks they discovered would be mitigated. (Defence Signals Directorate, 2014) In an ancillary report, they went on, "Adversaries often use malicious code to attempt to exploit vulnerabilities in workstations and servers. Restricting administrative privileges makes it more difficult for an adversary's malicious code to elevate its privileges, spread to other hosts, hide its existence, persist after reboot, obtain sensitive information or resist removal efforts." (Defence Signals Directorate, 2014)

Author: Tim Ashford, tcashford@gmail.com

Here is an outline of the controls that will be covered to tackle least privilege, together with several of its implications.

1. Before any technical actions are taken, formulate policy requirements with company management approval, documenting enforcements for the controls that mitigate the highest level risks in terms of privilege access.
2. Implement key Group Policy Objects relating to security from Active Directory. Group Policy Management is a free tool integrated into the Windows servers that are used to authenticate users in the typical Windows Domain.
    a) Take users out of the Local Administrators group on their systems. This can be automated in Group Policy using the "Restricted Groups" Group Policy Object (GPO).
    b) Enable the GPO to "turn off local group policy objects processing"; this prevents users or clever malware from tampering with domain-wide GPO settings.
    c) Turn off PowerShell at the local workstation level (there are several ways to do this, including the use of AppLocker, a Windows feature available in selected systems). PowerShell is a powerful Windows tool that has lately been weaponized by sophisticated hackers. It is hard to detect when it is misused, and since it is rarely needed on most desktops, should simply be turned off.
    d) Configure GPO's for specific UAC settings (User Access Control) in Group Policy. These settings insure that all desktop users are prompted for administrator credentials whenever a software installation is attempted.
3. Use Group Policy Software Installation (GPSI) to install and update standard software packages like Oracle's Java. This moves SMB environments toward standard configurations, and insures that updates are handled in a timely manner.
4. Deploy the GPO's that have been designed, once they have been tested on a small number of VM's. GPO's should always be configured first without being attached to any organizational units, and then tested, because actual behavior cannot always be predicted in real-world environments.

Author: Tim Ashford, tcashford@gmail.com

5. Explore alternatives and additions to GPSI. For some SMB's, it may be advantageous to augment the use of GPSI with third party software like PowerBroker for Windows, since it adds features like auditing.
6. Enforce application whitelisting. AppLocker is an excellent choice, because it is an extension of Group Policy. Additional costs may be involved, since many organizations don't have Windows Enterprise licenses on each desktop, which is a requirement for AppLocker to work.

These steps take into consideration the need to contain cost and complexity, which is a must for SMB's.

2. Start with Written Policy

The first step toward limiting what users can do on their desktops is not actually technical; it is procedural. SMB's need a clear and concise written security policy. This must include a strategic look at the need for least privilege, and give an outline of what to do. Armed with a short document that is actionable and enforceable, company leadership has made a statement to employees about how serious they are about protecting their environment. The reality is, most SMB's admit that they don't have policies in place. In a study conducted in October, 2012 by the National Cyber Security Alliance together with Symantec, 87% of smaller businesses interviewed admitted that they didn't even have a formal written Internet use policy for their employees. (National Cyber Security Alliance, Symantec and JZ Analytics, 2012) Specific cyber issues like least privilege, by inference, are even less likely to be addressed in writing by SMB's.

Our SMB security policy should state the rationale for moving users away from unrestricted privileges. It could say something like, "All desktop users will have Standard User accounts for their desktops. Since users have access to email and the Internet, they will invariably be exposed to malware that is not easily caught or contained. This move will limit damages, since most malware will not run without elevated privilege." To make this policy enforceable, the following could be added: "IT leadership is required to produce a quarterly report to company management, with an output showing that all employees have Standard User rights on their desktops. Any

single failure to produce this report will result in a warning letter. A second infraction will result in loss of compensation, at the discretion of company management."

3. Move on to Group Policy

Once leadership has moved to create and enforce a policy, it is time to get to work on the technical side. What can SMB's do to restrict user privileges at the desktop level, especially with limited budgets? They can do a whole lot, it turns out. It is assumed that a given SMB runs a Windows network with Active Directory. The first and perhaps most powerful tool is Group Policy. Group Policy is a smart move, because it comes freely including with a Windows server environment. SMB's don't have big security budgets, and need to use what they already have in place. Group Policy is an excellent tool that many organizations already have, but simply may not be using. While at first Group Policy can be daunting, due to the myriad of options, a few key settings can make desktops significantly more secure, without greatly hindering users. With some effort, and no additional software purchases, a working knowledge of Group Policy allows us to configure settings that make an attacker's job much harder. What follows is a walk through the basics of navigating Group Policy, to get to those settings. First, within the Group Policy Management interface, each organization needs its OU's, or organizational units. In a smaller sized firm, it is likely that only a few OU's will be used, or perhaps just one. Policies can then be associated, or linked, with these OU's.

To forge new policies, create them under the "Group Policy Objects" folder in the Group Policy Management console. See Figure 1. Here, configuration options are considered and chosen, without any immediate impact on the environment. Policies can then be applied to an OU at a later time. In order to create our first security-related policy object, here are a few assumptions. First, there will be several Group Policy Objects once finished, so they must be named as clearly and intuitively as possible. Second, after right-clicking on "Group Policy Objects", and choosing "New", use a convention to group similar policies together (J. Moody, Microsoft MVP, personal communication, April 27, 2015).

Author: Tim Ashford, tcashford@gmail.com

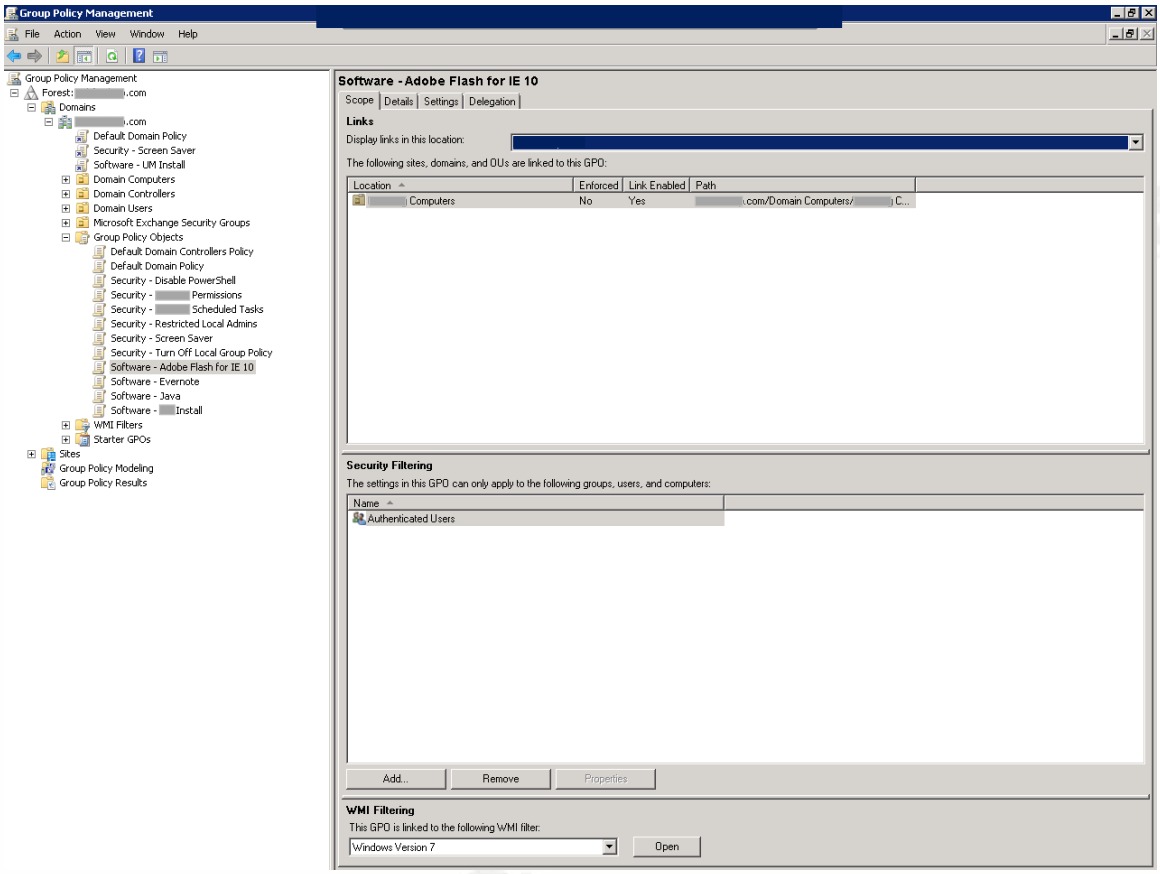

Figure 1: Group Policy Management Console

For example, for software installations, choose "Software - [name]", while a permissions-related setting could be labeled "Security - [setting]". Finally, assume that each major policy setting will get its own Group Policy Object, in order to isolate tasks. These assumptions help in three ways: First, GPO's are easier to understand for those who did not originally design them; second, they are easier to troubleshoot; and third, they are simpler to audit.

3.1 Automate the Removal of Local Admins

Our first GPO will automate the removal of users from the Local Administrator's Group. For starters, create a new policy object, and call it "Security - Restricted Local Admins". Once created, right-click and edit. Here, drill down to Computer Configuration→Policies→Windows Settings→Security Settings→Restricted Groups. Next, right click on Restricted Groups and choose "Add Group..." Name this

group "Administrators". By designating only Domain Administrators or those with similar roles here, all other domain users are restricted from having administrative rights at the local level (once this policy is linked to a particular organizational unit - OU - of computers. This will be covered later.)

However, at least one local administrator account must be left on the system. For best practice, several options should be considered. To start with, one option is to keep the local administrator account disabled, which is the default. If this account were activated, it should be renamed, and a complex password should be assigned to it. Regarding this password, it is urgent that it be kept unique; if a single password is used across all machines, this greatly increases the risk that malware could pivot around the network. An easy but less secure option is to concatenate a unique machine identifier together with a base password. This static password allows for a straightforward "break the glass" option (A. Beuhring, personal communication, April 10, 2015). Such scenarios would be situations where an employee or IT support person is at a workstation, and needs a relatively easy way to access the system as an admin. In this case, they simply need to know the base password, plus a unique identifier like the system serial number. The more secure option for password protecting a local admin account is to automate the assignment of a randomized and regularly updated password (Fossen, 2013) Microsoft has an interesting tool called LAPS, which was most recently updated in May of 2015 (Berkouwer, 2015). It is a sophisticated way to protect the local administrator account on each workstation, and best of all, it is free (Microsoft, 2015).

3.2 Enforce Group Policy Objects

As a safeguard to insure that domain level policies are forcefully applied, our next suggested policy object is "turn off local group policy objects processing", found under Computer Configuration→Policies→Administrative Templates→System→Group Policy (J. Moody, Microsoft MVP, personal communication, April 24, 2015). Once again, create this as a separate policy object, and isolate this step, to allow for future troubleshooting. It is widely known that Local GPO's are processed before any domain-based GPO's. By turning off Local Group Policy Objects processing, machines are better

protected against the risk of malware that adjusts local policy settings before the next time that domain level policies are applied. In other words, this insures that the settings in place for our entire domain can't be tampered with on a single desktop, either by malware or an unauthorized user. For example, malware has been known to block access to the Control Panel, the Task Manager, the Registry Editor, and the Command Prompt in Windows, using Local Group Policy (ESET, 2014). With this setting enabled, local policies can never be edited. Therefore, important areas like the registry will remain off limits to standard users. SMB's don't have tools to detect subtle changes like registry tweaks, and need the assurance that such changes are kept from happening in the first place.

3.3 Document Changes

As GPO's are implemented, it is important to document each new step, or each new item, added to Group Policy. This is part of the overall Change Management process that every organization needs (Stickel, n.d.). Even with the most prudent design and intuitive naming conventions, organizations need a thorough explanation of what was changed, by whom, and when. For SMB's with limited IT staff, this is especially important. Why? Without the benefit of many eyes on the implementation process, there is a far greater risk of error. Even a basic change log in Excel, with several columns listing date/time, change agent, item, date tested, and expected result, can be simple enough for an SMB to implement.

3.4 Lock Down PowerShell

In terms of securing the desktop, what are some other key Group Policy objects that SMB's can explore? Some of the more sophisticated attacks against Windows desktops involve the PowerShell framework. SMB's should look into ways to disable PowerShell from executing on desktops at all, since most users will never need this functionality. AppLocker, mentioned later, is an option for disabling PowerShell. Stealthy hackers like PowerShell for its ability to execute powerful commands, while leaving little evidence of its use. (Hastings & Kazanciyan, 2014)

Author: Tim Ashford, tcashford@gmail.com

SMB's in particular would have a difficult time knowing that an intruder was using this tool, so it is all the more important to disable it.

3.5 Enforce User Account Control

User Account Control settings are another area to consider. When UAC settings are turned on and elevated, they require administrator passwords to be entered every time software is installed by someone directly in front of the machine. By configuring a few simple UAC settings in Group Policy, SMB's can mitigate the risk of unauthorized software installation by forcing credentials for each. For example, under Computer Configuration→Policies→Windows Settings→Security Settings→Local Policies→Security Options, there are a few policy objects that affect how and when the UAC elevation prompt executes. Further to this, when either Standard Users or even Administrators try to install software manually, a prompt appears on the secure desktop that requires credentials before proceeding.

3.6 Use Group Policy Software Installation (GPSI)

Speaking of software installation, SMB's have an important consequence to consider after implementing least privilege at the desktop: Users can no longer install or update their own software. This is a problem, because when users have administrative privileges, they can add or change any software they please. The problems faced by implementing least privilege from a software standpoint are really twofold: First, software installations must be automated so that limited IT staff is not overly burdened. Since users no longer install software themselves, IT would otherwise be expected to manually attend to each software installation, which is not feasible. Second, there needs to be a central way to run security updates for vulnerable software in a timely manner, without involving users, since users can no longer apply critical software updates themselves. This is a relief on some level, due to the fact that counterfeit updates have compromised systems. But there is nevertheless an urgent and important need to install security updates for Java and Adobe software, in particular. Hardly a month goes by without hearing about a new vulnerability in one of these software packages, and those with security risks pose a significant threat to a Windows desktop. That means that as

users browse the web on computers with unpatched versions of software add-ons, they risk infections that may not even register with the detection capabilities typically found in an SMB. Group Policy is once again a great way to solve these challenges. Group Policy Software Installation, or GPSI, is free, well documented, and well integrated into the Windows world, making it a great fit for SMB's.

3.7 Inventory All Software

Before learning how to apply Group Policy for software installation, IT management needs to meet the requirements of the second Critical Security Control, which is to inventory all software currently in the environment. How can IT know what needs to be protected and patched, if they don't even know what they have in terms of software? Especially in an SMB, where a formalized software management process has likely been lacking, there may be surprises: an inventory of all currently installed software may discover some items that require immediate removal. While an evaluation of all the options for implementing this control is beyond the scope of this paper, one third party software option for automating this discovery process will be discussed later. For further reading, the latest elaboration of Critical Control 2 can be followed at: http://www.cisecurity.org/critical-controls.cfm

3.8 Use GPSI to Install Java

Using Java as an example, here are the steps needed to install the latest update. First, note that by default, Group Policy can only process MSI files. This is because MSI files behave much more predictably than EXE files, and thus provide more options as far as installation, removal, and configuration with Group Policy (Moody, Extracting MSIs for Software Deployment, 2013). Some software installation files are available in MSI format by default, but in the case of Java, there are some steps to perform in order to extract the MSI. First, find the Oracle download that is free of unwanted add-on software. This can be done by Googling "Oracle Technetwork Java", look for Java downloads, and then choosing the JRE (Java Runtime Environment).

Since Oracle does not offer an easy way to grab the MSI, there is a workaround to get it. Download the EXE file that corresponds to the correct desktop operating system, and run it on a single desktop (Moody, Extracting MSIs for Software Deployment, 2013). But before proceeding all the way through the install, browse to %appdata&\LocalLow\Sun\Java\[Java version folder] and find the MSI file here (Pace, 2015). Even if Oracle changes where the MSI is temporarily parked, search the local drive for an MSI from that day, while the executable is open. Some software deployments need more than a single MSI (Moody, Extracting MSIs for Software Deployment, 2013), but in this case, proceed with this one file.

Now that the correct MSI is captured, create a folder hierarchy from which Group Policy can deploy this package and any further software packages needed. This folder should be easily accessed across the network, with permissions that make it accessible to both users and computers, so "read" and "execute" privileges should be granted to both. As a best practice, create separate folders for each software deployed, and then within each software folder, distinct sub-folders for each version (J. Moody, Microsoft MVP, personal communication, April 27, 2015).

Back at our Group Policy Management interface, create a new Group Policy Object for automated deployment. Assume that the software is tied to a machine rather than a user, and therefore create a new policy under Computer Configuration→Policies→Software Settings→Software Installation. Here, right click and choose New...Package, and browse to the location of the MSI on the network. Though it is beyond the scope of this project, all kinds of other options are available in this section, such as a tab for accomplishing upgrades of software that Group Policy has previously deployed, and even a tab for making granular adjustments to the installation files, using an MST file with the Microsoft Orca tool (Moody, Deploy Java Runtime Environment with Group Policy, 2013). Incidentally, other key applications like Microsoft Office can utilize this free MST tool (Moskowitz, 2011).

Author: Tim Ashford, tcashford@gmail.com

Group Policy Software Installation (GPSI) offers real advantages to SMB's, both in terms of security and utility, provided that IT personnel are willing to learn the nuances of proper execution. In terms of utility, SMB's can centrally deploy exactly the software that the business wants users to have, and nothing else. This removes hours of manual attention spent at each user's desktop, considering what is legitimate, and what is not. Once the kinks are worked out, desktop software will stay up to date and secure, and from the user' perspective, will simply work. In terms of security, GPSI insures that only authorized versions of software are installed, and can even enforce the removal of vulnerable software, like older versions of Java. This gives SMB's the same tools that are leveraged by much larger firms. Granted, in some cases, packaging the correct MSI deployment takes extra effort and research. But for smaller businesses, there are likely only a handful of applications requiring regular security updates. Once these are mastered, the process for automating all software installs can be developed over time. For those software packages where the updates are less critical, more time can be left between updates, assuming that there are no must-have feature enhancements. And if there are, the investment of time must be made to learn the steps to use GPSI for those updates as well.

3.9 Deploy Group Policy Objects (GPO's)

Up to this point, Group Policies have only been configured. How are they deployed? Once the logical OU's are in place that align with our users and business units, simply right click on an OU, choose "Link an Existing GPO..." and select one of the available objects. There are a few more steps to keep in mind. To insure that policies work as designed, double-check settings like Security Filtering under the Scope tab, whether the policy is enforced, and what order in which they are processed (Microsoft, 2003). In particular, Security Filtering allows the policy object within the OU to apply to a specific number of users or computers. Enforcement of policies is not recommended in general, due to the fact that enforced policies take precedence over all others, making policy application less predictable. In other words, when no policies are enforced, they routinely apply in the following order: local policies first, then site policies, then OU policies, then domain policies. A single enforced policy "adds complexity to the

predicted flow of how policies are applied by making the Group Policy client process back up the Active Directory hierarchy," (J. Moody, Microsoft MVP, personal communication, May 7, 2015). For a summary, from the Settings tab, see all the unique options chosen for each policy object by clicking on "show all".

For more advanced options, consider WMI filtering, which allows policy objects to be filtered on parameters such as operating system. For example, since 2014, Microsoft has provided automated Adobe Flash updates for Windows 8 and IE 11, through Microsoft Update or Windows Server Update Services (WSUS). If, however, there are older Microsoft operating systems or browsers in the environment, such as Windows 7 or IE 10, updates that patch Adobe Flash updates can be automated selectively, by applying a WMI filter in Group Policy. In other words, Group Policy can check the operating system or browser of each desktop, and when a Windows 7 machine with IE 10 is discovered, the Adobe Flash patch can then be applied. This is a fairly advanced topic, but not difficult to implement. And once a few parameters are scoped, SMB's can deploy policies for different subsets of computers based on specific variables, without the need to create further OU's.

Now that the process has been described, how should policy objects be deployed? First, test them before they go live - for an SMB, this should involve using a single desktop or small test OU (Beckman, 2012). Virtual machines work best for testing, rather than physical boxes. The reason is obvious: Rebuilding a virtual machine from snapshots is the easiest way to recover from a botched group policy update, and VMWare Player offers a free tool for this. From an SMB perspective, always use the tools that are free and easily available. One expert suggests using a virtual machine that mimics a live system from the environment, and already has policies that are applied around the network (Beckman, 2012). This not only tests the new policy in action, but reveals how that policy addition inter-operates with other existing policies. Such testing verifies that the policy object works as expected. If not, Microsoft TechNet and many other helpful websites like http://www.deployhappiness.com offer troubleshooting tips and best practices for Group Policy.

Author: Tim Ashford, tcashford@gmail.com

With experience, SMB IT will learn to navigate the further implications of using Group Policy. For example, there is an option to suppress pop-ups that notify users when updates are available. Or there may be a need to modify or uninstall existing software. Installing printers is another area needing attention among users without admin rights. Whatever can be automated will help streamline the work of limited IT personnel, and prevent users from getting frustrated while waiting for needed changes. With further study, Group Policy tools and tips exist, given that enough time and energy are devoted to the task. And when Group Policy objects don't seem to be working, two built in tools offer a good place to start troubleshooting: The Event Viewer, and the "gpresult" command at a command prompt on a desktop in the environment.

4. Alternatives to GPSI

Stepping back for a moment, what if a small to medium-sized organization decides they simply don't want their IT support to master Group Policy, and especially Group Policy Software Installation (GSPI)? Or perhaps, IT decides to invest in Group Policy only for the few software packages in need of the most critical and frequent security updates? In such cases, there are commercially available alternatives. Keep in mind at the outset, however, that no third party software will prevent the need for managing and troubleshooting the overall process of software deployment. One package from Secunia called Corporate Software Inspector (CSI) scans systems for known vulnerabilities in EXE's, DLL's and OCX files, and offers remediation through available updates, based on a database that Secunia manages of existing patches (Secunia, 2013). Agents at each desktop would report to a central web console, from which patches could be deployed. As an added feature, reports can also be generated, revealing which systems and their corresponding software are in need of updates. (Secunia, 2013). Incidentally, Microsoft does not offer any kind of central reporting in Group Policy by default. Better auditing and reporting provides a more documented picture of what is happening in the environment, which will become increasingly important as further compliance-regulatory attention is focused on cybersecurity.

Author: Tim Ashford, tcashford@gmail.com

Because of the frequency and urgency of software security updates, Secunia's product may be an important consideration for handling laptops and any other desktops that are not connected to the corporate environment. This is an important problem that SMB's must solve: With or without Group Policy Software Installation, how is software deployed and managed for computers outside the corporate LAN? With Secunia as part of that solution however, the cost to a smaller business with fewer than 100 endpoints could still be in the thousands of dollars. For a less expensive alternative, PDQ Deploy from Admin Arsenal is a simple and intuitive option. It can be centrally deployed and even handles EXE file deployments, given that the administrator correctly implements parameters for a silent install. This can vary from software to software. Pricing is only a few hundred dollars per year for a single admin, no matter how many endpoints are supported. Consult http://www.adminarsenal.com for more information.

Another software package to consider is called PowerBroker for Windows from BeyondTrust. Part of a suite of options from the company, this software deploys a desktop agent that promises to perform the following: Remove admin privileges from end users; audit any applications across the network that require admin rights to run; automatically generate group policies; and effectively automate the elevation of applications, installers and system tasks that need those admin privileges. This works by elevating the privilege of a task or application, rather than a user (Schmitt, n.d.) Two clear security advantages of using this product over Group Policy alone are: One, all modifications can be audited, and extensive reports are offered on everything related to the rules and policies that PowerBroker manages; and two, PowerBroker can feed this type of data to a Security Information and Event Management (SIEM) system, which can capture what is happening in the realm of privileged use on the desktop, and correlate these data points with other security events around the network. While many smaller businesses would be unlikely to invest in a SIEM, they may find SIEM options available through cloud security providers. SMB's need to be on the lookout in the long run for SIEM offerings as they become more practical and affordable, since they are an important way to monitor privileged access.

Author: Tim Ashford, tcashford@gmail.com

Unlike Secunia CSI, PowerBroker does not actually deploy software updates; IT management would still need to employ GPSI or other third party software application to install and update software. Importantly, PowerBroker is integrated right into the Group Policy management console, so SMB customers would still be required to be competent with Group Policy. The benefit of PowerBroker is that it extends the functionality of Group Policy by allowing for sophisticated auditing and reporting on events surrounding least privilege. In addition, it was noted earlier that an inventory of all applications around the environment is critical to a successful implementation of least privilege; PowerBroker for Windows promises to automate that inventory process. The added value of this is that an audit of all existing software and the impact of implementing least privilege can be conducted before any change is made to the rights of desktop users, insuring a smooth transition. For example, PowerBroker could detect that a desktop is running scheduled tasks, which would break once that user can no longer run them as an administrator.

4.1 Enforce Application Whitelisting

The PowerBroker product introduces another critical need for all businesses seeking to manage the process of least privilege: Application whitelisting. Even though the removal of admin rights at the desktop reduces the amount of amount of malware that can run, The importance of this discipline is hard to overstate: In the most recent version (5.1) of the 20 Critical Controls, application whitelisting was listed as **the number one** action item or sub-control that can have "the most immediate impact on preventing attacks." (Council on Cyber Security, n.d.) To put it simply, application whitelisting will prevent all applications from running on desktops, except those that are whitelisted or authorized. This is extremely helpful for an SMB, since it further simplifies the management and security of software installation: Rather than worry about the many varieties of software that could possibly be considered legitimate, IT has a short list of what is approved, and can enforce that list easily. PowerBroker's application whitelisting determines which applications have permissions to run, and blocks all others. Again, the added advantage of a PowerBroker installation is the additional auditing and logging capabilities, which satisfy an increasing array of compliance requirements.

Author: Tim Ashford, tcashford@gmail.com

In order to stay with built-in Windows tools, AppLocker is the best option for application whitelisting. AppLocker is an excellent extension of Group Policy, and is also free, with one caveat: Only desktops with Enterprise Windows licenses can utilize it. For environments where Windows 7 or Windows 8 desktop Pro licenses have already been deployed, Enterprise upgrades are available, but may cost a few hundred extra dollars per desktop.

AppLocker settings already reside in Group Policy, which is a plus if Group Policy has been used to tackle least privilege. It is the successor to Software Restriction Policies, which still exist in Group Policy (and may be utilized under some circumstances where desktops do not have Enterprise licenses). AppLocker has the added benefit over Software Restriction Policies of an "Audit only" mode, which drops notifications in the Event Viewer on each affected local workstation (Shields, 2009) (unlike PowerBroker for Windows, which provides centralized reporting, AppLocker only adds audit events to an individual Event Viewer installation). To find AppLocker settings in the Group Policy Management Console, browse to Computer Configuration→Policies→Windows Settings→Security Settings→Application Control Policies→AppLocker. There, see three sub-folders for AppLocker settings. As the recommendation suggests from the Critical Controls, AppLocker is most useful at whitelisting only those applications that are allowed to run in the environment. This is highly suited to an SMB, because only a limited number of applications are needed. By configuring AppLocker settings in Group Policy, all other unauthorized software can be restricted by default. Microsoft TechNet offers step by step directions on the various features of AppLocker (Microsoft, 2012), which are beyond the scope of this discussion. As mentioned before, any AppLocker policies should be documented and tested in a virtual environment before deployment.

Once some of the best practices already mentioned are implemented, SMB's can investigate further tools to monitor the use of privileged access. For example, companies like Netwrix and ManageEngine each have a tool to monitor how administrative rights are actually utilized around the network (Netwrix Auditor and ManageEngine

ADSolutions). (Incidentally, ManageEngine also produces the Desktop Central application, which can be considered for automating software deployment, among the other options mentioned earlier. It is, however, limited to only a few supported software packages.) Auditing privilege use helps SMB IT to answer the question, who has administrative privileges, and who has merely standard rights? In order to verify the policies discussed earlier, there must be a way to prove that users don't have admin rights, and also that such rights have not been elevated without IT leadership's knowledge. With the increasing number of security options mentioned, IT security should always be guided by questions like: What problem needs to be solved? How can these problems be solved at the lowest cost? And, how can the solutions be executed while adding the least complexity? This takes us back to where we started, which is to limit our tools to only a few, or even just one: Group Policy.

In the future, SMB's may opt for a managed client from a larger cloud-based provider. Several security practitioners in private conversations have noted that the future of security for SMB's will be cloud-based services like InTune from Microsoft. These promise one day to outsource the security management of SMB desktops, by offering the kind of granular options discussed here, together with competitive pricing. At the most basic level, however, they will still likely utilize some form of Group Policy.

5. Conclusion

The above steps tackled an extremely common problem among SMB's today, which is the unmanaged use of privileged access. Such unrestricted use at the desktop level must be stopped. This starts with taking administrative privileges out of the hands of users. Even application whitelisting, as powerful as it is, cannot prevent blacklisted malware from running, once an endpoint has administrative privileges. As Derek Melber, Microsoft MVP, has said, a workstation logged in as administrator can run anything, and therefore should be considered unmanaged (Melber, 2012). As a local admin, he goes on, "even with the most sophisticated and complex array of Group Policy and other management settings being delivered from Active Directory and the network,

the local user [or remote malicious operator] can subvert the settings with ease." (Melber, 2012)

SMB's have many tools available to manage the implications when desktop privileges are reduced. These options must be weighed carefully though, to prevent the sprawl of too many systems, each requiring monitoring, management and updates – not to mention sprawling costs. Some tools like Microsoft LAPS and Netwrix Effective Permissions Reporting are optional ways to add depth to a SMB security posture, and are free. Others like Secunia CSI or PowerBroker for Windows by BeyondTrust cost several thousand dollars, and must be planned carefully to insure that the business has the appropriate time and resources to manage them actively, in order to justify the cost. With proper oversight, CSI and PowerBroker offer powerful ways to automate key tasks like software installation and privilege elevation. PDQ Deploy from Admin Arsenal should also be considered, since it is cheaper than Secunia, and centrally pushes software updates once users can no longer run them on their own.

Best of all is Group Policy. Though it requires effort to learn, it offers a tremendous array of granular security options, giving SMB's the same sophisticated GPO options deployed in larger enterprises. For example, in conjunction with AppLocker and some of the UAC-specific GPO's, an SMB admin can use Group Policy to lock down a desktop nearly as tightly as much larger firms would. Furthermore, with the onset of sophisticated PowerShell script attacks at the endpoint, Group Policy can be employed with AppLocker to prevent an attacker from running a shell. SMB's can tackle privilege management decisively, and work toward automating many of its implications.

Author: Tim Ashford, tcashford@gmail.com

6. References

Beckman, K. (2012, January 31). *Troubleshooting Group Policy – Part 2: Test and deploy*. Retrieved from 4SYSOPS: https://4sysops.com/archives/troubleshooting-group-policy-part-2-test-and-deploy/

Berkouwer, S. (2015, May 2). *The Things that are Better Left Unspoken*. Retrieved from The DirTeam.com / ActiveDir.org Weblogs: https://dirteam.com/sander/2015/05/02/security-thoughts-microsoft-local-administrator-password-solution-laps-kb3062591/

Council on Cyber Security. (n.d.). *The Critical Security Controls for Effective Cyber Defense*. Retrieved from Center for Internet Security: http://www.cisecurity.org/documents/CSC-MASTER-VER5.1-10.7.2014.pdf

Defence Signals Directorate. (2014, June). *Restricting Admin Privileges*. Retrieved from Australian Signals Directorate: http://www.asd.gov.au/publications/protect/Restricting_Admin_Privileges.pdf

ESET. (2014, April 16). *An infiltration is blocking access to the Control Panel, Task Manager, Registry Editor, and Command Prompt—what should I do?* Retrieved from ESET: http://kb.eset.com/esetkb/index?page=content&id=SOLN721

Fossen, J. (2013, August 1). *Reset Local Administrator Password Using A Different Random String On Each Computer And Recover The Passwords Securely*. Retrieved from SANS.org: http://cyber-defense.sans.org/blog/2013/08/01/reset-local-administrator-password-automatically-with-a-different-password-across-the-enterprise

Hastings, M., & Kazanciyan, R. (2014). *Investigating PowerShell Attacks.* Retrieved from Black Hat: https://www.blackhat.com/docs/us-14/materials/us-14-Kazanciyan-Investigating-Powershell-Attacks-WP.pdf

Melber, D. (2012). *Windows Endpoint Security is Least Privilege and Data Loss Prevention*. Retrieved from BeyondTrust: http://www.beyondtrust.com/Content/whitepapers/Windows-Endpoint-Security-is-Least-Privilege-and-Data-Loss-Prevention.pdf

Microsoft. (2003, March 28). *Application of Group Policy*. Retrieved from TechNet: https://technet.microsoft.com/en-us/library/cc736313(WS.10).aspx

Microsoft. (2012, August 8). *AppLocker Step-by-Step Scenarios*. Retrieved from Microsoft TechNet: https://technet.microsoft.com/en-us/library/ee791835(v=ws.10).aspx

Microsoft. (2015, May 1). *Local Administrator Password Solution (LAPS)*. Retrieved from Microsoft Download Center: https://www.microsoft.com/en-us/download/details.aspx?id=46899

Moody, J. (2013, August 26). *Deploy Java Runtime Environment with Group Policy*. Retrieved from Deploy Happiness: http://deployhappiness.com/deploy-java-runtime-environment-with-group-policy/

Moody, J. (2013, November). *Extracting MSIs for Software Deployment*. Retrieved from Deploy Happiness: http://deployhappiness.com/wp-content/uploads/2013/11/Extracting-MSIs-for-Software-Deployment.pptx

Moskowitz, J. (2011, August 18). *Deploying Microsoft Office Using a Microsoft Transform File*. Retrieved from IT Ninja:

Author: Tim Ashford, tcashford@gmail.com

http://www.itninja.com/blog/view/deploying-microsoft-office-using-a-microsoft-transform-file

National Cyber Security Alliance, Symantec and JZ Analytics. (2012, October). *2012 NCSA / Symantec National Small Business Study.* Retrieved from Stay Safe Online: https://www.staysafeonline.org/download/datasets/4389/2012_ncsa_symantec_small_business_study.pdf

Pace, M. (2015, March 11). *Oracle Java 8*. Retrieved from IT Ninja: http://www.itninja.com/software/oracle/java-8/8-update-40

Schmitt, J. (n.d.). *Power Broker for Windows Desktops*. Retrieved from Demos on Demand: http://goo.gl/HPMiMU

Secunia. (2013, September 10). *CSI 7.0 Walkthrough*. Retrieved from YouTube: https://www.youtube.com/watch?v=-1u1Ma4pms4

Shields, G. (2009, October). *AppLocker: IT's First Security Panacea?* Retrieved from Microsoft TechNet: https://technet.microsoft.com/en-us/magazine/2009.10.geekofalltrades.aspx

Stickel, E. (n.d.). *Change Control vs. Change Management: Moving Beyond IT*. Retrieved from Technology Executives Club: http://www.technologyexecutivesclub.com/Articles/management/artChangeControl.php

Symantec. (2015, April). *Internet Security Threat Report.* Retrieved from Symantec: https://www4.symantec.com/mktginfo/whitepaper/ISTR/21347932_GA-internet-security-threat-report-volume-20-2015-social_v2.pdf

Verizon RISK Team. (2012). *2012 Data Breach Investigations Report.* Retrieved from Verizon Enterprise: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf

Author: Tim Ashford, tcashford@gmail.com

Last Updated: June 26th, 2017

Upcoming Training

SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Community SANS San Diego SEC401	San Diego, CA	Aug 21, 2017 - Aug 26, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS