Do You Know Where Your Privileged Accounts Are?

by Dean Weich, Tools4ever

Enterprises of all industries, types and sizes are adopting and enforcing "least privilege" practices for account management, but privileged accounts will always be necessary and intrusion attempts are only increasing. If you must have a set of "keys to the kingdom," where do you hang them?

"Least privilege" is a fundamental access governance (AG) concept. It ensures that Tim in marketing cannot access the accounting department's files. If you ask yourself, "Does my employee need X?" and the answer is "no" remove that access. However, IT admins, C-level executives, some managers and service and application accounts all require some higher-level access rights to fulfill various role functions. If an employee ever needs to pop the hood for an enterprise's systems or operations, they will need a privileged account.

Lurking Privileged Accounts

For the purpose of this article, privileged accounts can be separated into two types: high- and low-visibility. High-visibility privileged accounts are those controlled and used by people: IT admins, C-level executives and managers. There is typically some level of protection, often requiring authentication of the operator's identity. Low-visibility privileged accounts are orphaned accounts left on your network and service accounts. Orphaned accounts have been left behind by previous employees or are unused by current ones. Service accounts are operated by the software, application or other type of service itself, and require elevated permissions to ensure the systems and applications communicate and function properly. Some services require external data to perform properly and the associated account allows for the transfer of that data as if the service was a privileged user making the request.

Vendor accounts are somewhere between, as they lay dormant unless third party support or a service vendor accesses the account for scheduled, requested or emergency maintenance and updates. Even after the uninstallation of an application or software or the discontinuation of a service, these and service accounts can remain within the network. Altogether, this means that there are more privileged accounts within an enterprise than there are privileged account users – perhaps even more than all users.

User education is critical to ensuring that the exposure of human vulnerabilities is minimized. If employees have poor security practices within their personal work environments – accounts, passwords, ignorance of malware, unsecure activity, etc. -- the enterprise as a whole is at risk. If an attack or the failure of a mobile device's endpoint security leads to a breach, an AG policy can help add a layer of security by limiting the intruder to the stolen user account's permissions. If the intruder is using Tim from marketing's account, they won't have any more access to the accounting department's files than Tim does because of the "least privilege" enforcement.

AG can make an intruder's life much more difficult, but a basic policy cannot prevent them from operating within the limited network so long as they can continue to pretend they are the stolen user and emulate their activity. Standard user accounts may be the way in, but they certainly are not the motive for a breach. Privileged accounts are high-priority targets for the intruders to gain the elevated permissions within the system to access sensitive data or wreak havoc. With the right privileged account, an intruder has free reign disguised as an admin. The danger of enterprises having so many privileged accounts is that, especially when left unaccounted for, they can be used both as system backdoors and disguised access for intruders once inside.

Preventing that original breach is difficult when those privileged accounts may actually be the source of entry. Service accounts run in the background and vendor accounts lay dormant until used by internal or external

support staff. Orphaned accounts are more likely to be permanently dormant. That dormancy obscures privileged accounts much more and increases potential entry points – ones that are supposed to exist and, therefore, are especially vulnerable. Once inside your enterprise's system or network, an intruder may not intend a smash-and-grab job, but carefully bide their time setting up for a more sophisticated, more devastating attack. Some intruders may intend solely to lurk and discover ongoing information about an enterprise. Compromised privileged accounts can provide effective concealment for these extended breaches.

Threats can also emerge from third parties if their own security has suffered a breach, compromising the systems and networks that remain connected to your enterprise through an outside account. Intruders who have breached those third parties can easily achieve authorized access by disguising themselves as support accessing a privileged account, subsequently granted entry into their network with all of the permissions they wanted. This remains the support account's intended function, so it becomes much more difficult to spot the red flags. Though vendors are used as an example, these information breaches are not limited to services provided by technology enterprises. If your enterprise electronically exchanges any kind of information with another business, independent contractor, or any third party entity, there are exposed entry points with potential risk.

Not just the biggest fish...

This problem is not limited to big business anymore, despite what many small and medium enterprises may think. The proliferation and use of enterprise technologies throughout the business world means that even solo operations likely use third party software, applications, security or solutions to some extent, which require privileged accounts. The numbers in Symantec's 2016 Internet Security Report clearly demonstrate the rising threat of spear-phishing to small (one to 250 employees), medium-sized (251 to 2,500 employees), and large (2,500+ employees) businesses. Spear-phishing is an intrusion attempt that tries to lure the victim into opening an email attachment that appears to originate from a familiar or credible source. According to Symantec, spear-phishing campaigns have risen 55 percent, from 841 in 2014 to 1,305 in 2015.

Symantec's research compiled the risk ratios for each business size, exhibiting one in 40.5 small, one in 6.8 medium-sized, and one in 2.7 large businesses were targeted by these phishing attacks – rounded to 3 percent, 15 percent and 38 percent, respectively (Figure 1).

	Small (1-250 employees)	Medium (251-2,500 employees)	Large (2,500+ employees)
Risk Ratio	1 in 40.5	1 in 6.8	1 in 2.7
Risk % (Rounded)	3%	15%	38%
Avg. # of Attacks (Per Enterprise)	2.1	2.2	3.6

Figure 1 – Enterprise Risk Ratios by Size, Symantec (https://www.symantec.com/security-center/threat-report)

While the risk ratios may portray a smaller percentage chance of small and medium-sized businesses being targeted by phishing attacks, those organizations who were targeted in 2015 from both size categories were attacked an average of 2.2 (medium-sized) and 2.1 (small) times. Large businesses that were targeted experienced an average of 3.6 attacks. These numbers indicate that while the overall chance of being attacked is less for smaller and medium-size businesses, anyone targeted must prevent multiple attacks.

Further, the smaller attack ratios may be due to the greater number of businesses with fewer employees. The size categories do not perfectly line up, but the Statistics of U.S. Businesses' (SUSB) data on firm size help portray the just how many more small businesses exist in the United States than those from the larger 2 categories. Out of a total of 5,720,160 U.S.-based firms, 18,219 had greater than 500 employees, 83,423 had between 100-499 employees, and 6,624,518 had fewer than 100 employees (Figure 2). That breakdown overwhelmingly demonstrates a much greater number of existing small businesses, representing a very high number of targets in terms of volume.

	Small (1-99 employees)	Medium (100-499 employees)	Large (500+ employees)
# of Businesses	6,624,518	83,423	18,219

Figure 2 – Statistics of U.S. Businesses Firm Size Data (https://www.sba.gov/advocacy/firm-size-data)

The following analysis is a general interpretation of the data related to gross attack volume in an attempt to compensate for the size classification disparity between Symantec's and SUSB's research. Symantec's highest risk ratio (1 in 2.7) applied to SUSB's count of large firms would project 6747 of those experienced attacks. This number includes a portion of those enterprises classified by Symantec as medium-sized due to overlap. By comparison, applying the small-business risk ratio (1 in 40.5) only to SUSB's count of firms with fewer than 100 employees, a smaller classification than Symantec's 1-250 range, would project 163,568 of those enterprises experienced attacks. Only 3 percent of small businesses may have been attacked, but 163,568 businesses remains a massive number of targets and discredits the belief that "it won't happen to us."

Perhaps most concerning is the 5-year trend demonstrating an increase in the ratio of attacks specifically targeting small businesses. The 2011 breakdown revealed that 50 percent of attacks targeted large businesses, 32 percent targeted medium-sized businesses, and 18 percent of attacks targeted small businesses. Compare to the most recent numbers in 2015: 35 percent of attacks targeted large businesses, 22 percent targeted medium-sized businesses, and 43 percent of attacks targeted small businesses (Symantec 2016).

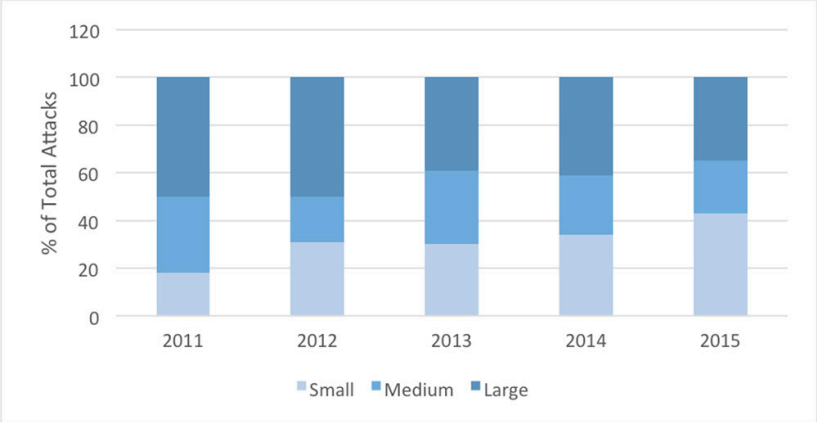

Figure 3 – Attack % Breakdown, By Year (2011-2015), Symantec (https://www.symantec.com/security-center/threat-report)

As the information reveals, the distribution of phishing attacks according to enterprise size began to equal out more in 2013 before skewing slightly more towards smaller businesses. While large and medium-sized enterprises seem to have some fluctuation in their yearly attack percentages, small businesses have shown fairly steady increases. This could be because of the generally smaller IT budgets and lower IT maturity of smaller businesses, making them comparatively easier targets. Similarly, the three-year decrease (2013-2015) in attacks on medium-sized enterprises may be because they are considered to have less valuable assets than the largest businesses but more sophisticated security than the small ones.

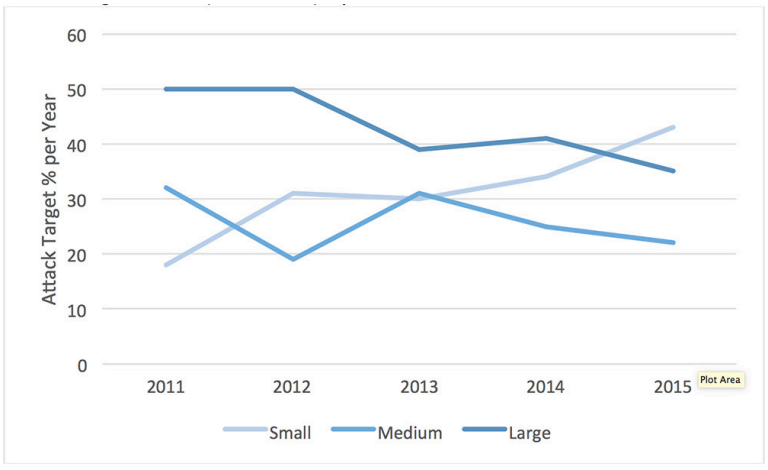

Figure 4 – Attack Target Trends (2011-2015), Symantec (https://www.symantec.com/security-center/threat-report)

Best Practices

If you must have a set of "keys to the kingdom," where do you hang them? Protecting your enterprises' privileged accounts relies on the adoption of routine auditing, usage restrictions, and fail-safe expiries as best practices.

The first step to better protection requires an internal audit of all privileged accounts on the enterprise's network: user-controlled, orphaned, service and vendor or other third party. Active Directory's Users and Computers is one of the easiest places to centrally look at all of your privileged accounts. During your audit, remove any orphaned privileged accounts and those associated with services or vendors no longer used.

Having cleaned up your domain, it is important to educate employees on proper usage and the dangers and types of security breaches. Any employee with the rights to a privileged account should only log in and use it when absolutely necessary. For all other activity, these employees – including system administrators, C-level executives and others – should log into normal accounts controlled by AG with "least privilege" enforcement.

If an employee must use a privileged account, an auto-expiry should be set to disable the account after use. Especially when linked with a workflow process, it is very simple to automatically disable privileged accounts after use and reactivate them when requested. An account could be given an expiry date of midnight the same day it was enabled for activity, disabling it until requested for future needs. Disabling privileged accounts prevents intruders from being able to use them to any effect even if accessed. Vendor accounts can also be set for expiry to disable them when not needed for third party use.

Service account require a different type of monitoring, since they cannot be disabled at any point in order to function properly. Instead of placing an automatic expiry on a service account, those accounts should prevent interactive login and then be siloed, or restricted to only their essential function according to AG and "least privilege." Service accounts operate as privileged users with the authority to request information from other network areas, and so they should be treated the same as user-controlled privileged accounts. If a service account is associated with accounting software, its permissions only need to extend to relevant accounting data. Both Tim from marketing and the accounting software only need permissions to the data essential for their enterprise roles, so their accounts should reflect such. Unrestricted service accounts with accumulated privileges can be used by intruders to go from accounting data to HR data and all over the network. If siloed, a successful intruder is still limited to the restricted scope of the service account's privileges.

Protecting privileged accounts requires upkeep, but ultimately returns to the active enforcement of "least privilege" – ensuring that all users and accounts are restricted to the exact essentials necessary for their role within the enterprise. No more, no less.

Note: The grouping were chosen with respect to the limitations of comparing the data presented by Symantec and SUSB. The original research methods utilized different classifications of small, medium, and large sizes for enterprises. For this reason, the data analysis presented here should be regarded as a more general suggestion of how Symantec's risk ratios look in terms of gross volume. To best compensate for data gaps, Symantec's large-business risk ratio was applied to a range of enterprises that contained all SUSB's large businesses and some of its medium-sized range, padding the base number and, consequently, the projected number of enterprise attacks. Conversely, Symantec's small-business risk ratio was applied to SUSB's small businesses, a lower range than Symantec's, decreasing the base number and projected number of enterprise attacks. In essence, the large-business gross numbers are mildly inflated and the small business numbers are mildly deflated, estimating the attack-volume disparity at a less severe level than what more consistent data would likely demonstrate.

Dean Weich

Dean Wiech joined Tools4ever in April 2006 and is responsible for the Tools4ever, Inc. operations the United States. His duties include direct sales as well as the responsibility for the sales, technology and consulting team along with the day-to-day operations for the company.

Dean has been involved with sales and sales management in the software arena for over 20 years – before joining Tools4ever he was Vice President of Sales for a Manhattan based Software Company that is specialized in cost allocation and spend optimization. He attended the University of Akron and studied Chemical Engineering before deciding to pursue a career in technology.

Contributions

- Do You Know Where Your Privileged Accounts Are?
- Password Management: History, Costs, Problems and Pain Points, and Solutions
- Identity Management and Enterprise Service Bus a Happy Marriage Does Not Make