FEATURE

Effective Interactive Privileged Access Review

Most organizations would agree that it is a good practice, albeit not an easy one, to establish rules relating to the amount and type of access to provide to particular job roles. Access control is a key element in protecting enterprise information. It requires focused analysis to identify all the activities a role may need to undertake to perform its function and what information or applications the role may need to do the job thoroughly and well. Life would be so much simpler if, after investing the time and effort in identifying roles and associated access rules, nothing ever changed and no exceptions were ever needed.

But, life rarely cooperates. Occasionally, certain individuals must be given privileged access to certain tools or information to accomplish a specific, discrete purpose—some aspect of their role that is outside the ordinary list of tasks. Organizations may need to assign privileged access to take advantage of an unexpected opportunity or to address a hitherto unknown threat; it is part of doing business in a digital world. However, great care must be taken in understanding the legitimate reasons for assigning privileged access, assigning it in a controlled way, and monitoring its ongoing use and discontinuance to ensure the privilege is not abused. This article covers the broad aspects of the importance of interactive privileged access review; how it should be done, including some tips on frequency of the access reviews; and expected outcomes as benefits. It will not, however, cover the entire spectrum of log reviews end to end.

What Is Privileged Access?

As the word "privileged" indicates, this is an access for a special purpose that requires more than a normal access. Some examples of privileged access roles are administrator, root or superuser. People assigned these roles can do much more than normal users or end users, such as granting/revoking access, changing the level of access and resetting credentials.

Providing privileged access must be aligned with the least privileged access needed to perform a defined job role or on a need-to-know basis. A document outlining separation of duties should be kept as a reference for who should have what access and to ensure no conflict of access or roles.

Privileged access must be provided based on demonstration of a legitimate business need and the advance approval of access by the data asset owner or an authorized delegate (**figure 1**, column 1.0).

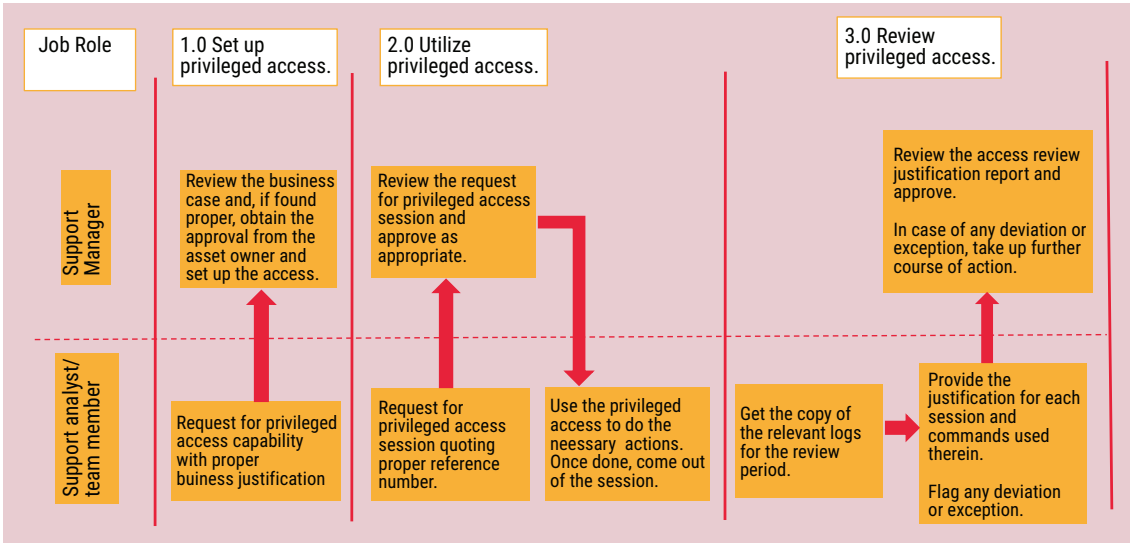
Generally, there are two modes of privileged access:

- Through a graphical user interface (graphical user interface [GUI], user interface screens) on the front end, typically for application access administrations
- Through the back end (also called interactive access), used typically by IT support professionals or IT professionals in general, as part of their assigned application support role. In cases of application outage or issues, people assigned this role need this access to do the required repair work, to recover from a business or application failure. Some examples of this repair work are changes/updates to the code (bug fix), changes/updates to the data and making configuration corrections/updates.

Examples of Interactive Privileged Access
Examples of interactive privileged access include Unix-ID for shell script updates in the production region, Job Control Language (JCL) access in the mainframe for mainframe job submission/resubmit in production, interactive access to a job scheduler such as CA7 or autosys, and back-end production database updates as part of operations support requirements.

Sundaresan Ramaseshan, CISM, ITIL-Foundation, ITIL-SO
Is an IT supervisor supporting security tools at Ford Motor Private Limited, located in Chennai, India. He has more than 25 years of experience performing various roles in the software development life cycle in the IT industry. He is interested in enhancing his depth of knowledge in the security domain and sharing some of the things he has found to be effective in his day-to-day operations that could benefit the community as a whole.

Figure 1—Establishing Privileged Access



Potential Risk

While privileged access would benefit the organization to effectively come out of a production outage as part of "run and protect" the business, it also has an inherent risk.

Even if access is by an authorized person, that individual could make a mistake, for example, updating the data incorrectly or bringing down application(s), which could impact the business, resulting in production loss and/or monetary loss. The organization could also lose its reputation in the market or be perceived as weak in protecting its own competitive advantage. Customers' data privacy could be compromised, for example, through loss of personally identifiable information (PII) or, in some cases, secret personally identifiable information (SPII). The organization may end up paying hefty fines due to various governmental regulations while losing customers' confidence and brand image.

It has been reported that more than half of cybercrimes or cyberattacks happen due to the weakest link in the chain: internal employees whose credentials are either intentionally (for personal gain or other illegal reasons) or unintentionally (phishing or malware) compromised.

One methods of securing privileged access is Privileged User Access Management (PUAM).

Any need for privileged access to the production area should be addressed through the workflow for requesting credentials for privileged access with proper approval processes (**figure 1**, column 2.0).

Privileged account credentials should be stored in a common password repository, with static or dynamic password resetting capabilities.

"WHILE PRIVILEGED ACCESS WOULD BENEFIT THE ORGANIZATION TO EFFECTIVELY COME OUT OF A PRODUCTION OUTAGE AS PART OF "RUN AND PROTECT" THE BUSINESS, IT ALSO HAS AN INHERENT RISK."

How to Monitor

Interactive privileged access for IT personnel must be monitored and their activities should be audited in an appropriate and timely manner to ensure the effectiveness of the control (**figure 1**, column 3.0).

It must be done in such a way that any unauthorized access can be detected as quickly as possible and also be able to give some indication of the size of the impact. Ultimately, management must be comfortable that it has a line of sight to critical access and actions. This could incorporate the responses to two broad questions:

1. Who needs such interactive privileged access?
2. Who uses the interactive privileged access and for what reason?

Logging Mechanism and Protecting the Integrity of the Logs

An appropriate standard should be set and applied when configuring logs. Utmost care should be taken to make the logs read-only with proper archival setup. Proper archiving is highly recommended to ensure that the size of the log file is not impacting the performance of the operating system. Important logs can also be stored at a backup location in case of specific legal retention requirements.

> “THE FREQUENCY OF LOG REVIEWS SHOULD BE DIRECTLY PROPORTIONAL TO THE FREQUENCY OF INTERACTIVE ACCESS AND THE CRITICALITY OF THE ASSET.”

Frequency of Log Reviews

The frequency of log reviews should be directly proportional to the frequency of interactive access and the criticality of the asset. Ideally, if the log review uncovers any issues, it should be as close as possible to the origin of the event, which could help in recovering from it.

Flagging vulnerable and nonvulnerable commands is a good practice for performing log reviews.

Vulnerable commands can be defined as those such as data copying, data edit/manipulation or delete. Viewing the data is a nonvulnerable command provided it is done by authorized personnel. Accordingly, it is necessary to focus on the vulnerable commands when performing log reviews (**figure 2**).

For the period in review, the dump of the logs is obtained from the respective server teams. The team member then parses the log file into structured line items (probably in an Excel spreadsheet), lists out one command in a line, the time of checkout of the ID, who checked it out and a reference ticket number for which the access was obtained (**figure 2**). The team lead then reviews the log for appropriateness. Once the leader is convinced that the privileged access activities were in line with the expectations, he or she forwards the review with the findings to a supervisor for approval. The supervisor then provides the approval (**figure 1**, column 3.0). If an exception is found, the supervisor must use his or her judgment and consults with the security compliance team for further corrective actions. If there is an explanatory comment, as shown in **figure 2**, it should be addressed by fixing the gap and monitoring for consistency in adoption as part of maintenance.

Figure 2—Interactive Access Review Sample		
Command	**Vulnerable**	**Ticket # / Comment**
#DTS Wed Jan 29 00:08:26 EST 2014	Date and time of access	Used by Duraisamy for editing as part of commenting on the command as per request ID: 123456
pwd	No	
crontab -l	No	
date	No	
pwd	No	
crontab -e	Yes	
date	No	
crontab -l	No	
date	No	
pwd	No	
ls -l	No	
exit	No	
#DTS Thu Jan 30 03:16:35 EST 2014	Date and time of access	Used by Kevin from the password management team to change the password as per request ID: 345667
pwd	No	
ls	No	
cd bin	No	
ls	No	
cd /proj	No	
ls	No	
exit	No	
#DTS Thu Jan 30 23:28:19 EST 2014	Date and time of access	
passwd	Yes	
exit	No	

Improvement Example

Sometimes, the support analyst may push back, saying unrestricted back-end interactive access is required as part of operations support simplification. Proper care should be taken to separate out read-only privileges and other high-level privileges such as edit, update, delete or execute. While activities done through read-only can be quickly reviewed, provided they are done by authorized service personnel, other commands such as update, delete or copy need to be scrutinized for specific ticket reference. This prioritizes the log review area effectively and reduces the risk accrued to previously unrestricted back-end privileged ID access.

Conclusion

As IT transforms into a key driver for business enablement, privileged access review should demonstrate the existence of controls and uncover any shortfalls therein. It should result in meaningful actions based on feedback about the overall IT process as part of continuous improvement.