Demystifying Threats of Privilege Users

–**Sanil Nadkarni**,
CISO & VP - SLK GLOBAL SOLUTIONS, sanilnadkarni@yahoo.com

As the IT infrastructure is becoming increasingly sophisticated and size of the application and system proliferating each day, one of the most fundamental problems the IT Security team today is to manage and monitor the threats of privilege users accounts.

Traditionally, a "Privileged User" has been defined as someone (i.e. IT administrator) with authorized access to sensitive networks, machines, applications, to perform his mundane tasks. Access to these users are often given in a perfunctory manner

These users typically posses an unrestricted access not only to the pivotal system , but also have access to vital classified , company secret information , such as credit card , bank account. Details etc. These users can be malevolent and pose an inherent risk to company without adequate controls deployed to effectively manage, monitor their access.

Let's take a deep dive to demystify the risk emitting out of privilege users.

Local user accounts: local user's accounts are ubiquitous. Build in by default in operating system; network IOS, applications, databases. Organization finds themselves on a sticky point, as they cannot delete nor disable them due to system constrains, or their requirement for troubleshooting.

Typically the IT staff has local admin privilege to all the desktops and server systems; hence inevitably they get access to user's profiles / documents, shared files etc.

With the local admin they have privileges to install unauthorized software, application and even install a malicious malware, network monitoring tools or even plant a logic bomb

The local user account are generic in nature and often the passwords are not changed regularly, they can be easily compromised or exploited thus posing a huge security risk to the security posture of the company.

Network devices: the network devices such as routers / firewalls / IPS / switches are overlooked for privilege access. They are key to the entire infrastructure as all of the data traverses through these devices. These network devices have inbuilt admin account which can be exploited by the nefarious hackers, thus giving an unrestricted access to the corporate network.

Data base servers: Most of the company's important data resides on the database servers. Due to the complexity of the databases, managing the privilege user account in database is a cumbersome task. For example, University administrator whose job requires only the ability to change student contact information may take advantage of excessive database update privileges to change grades. With thousands of such database servers this is a considerable risk to the vital company data residing on the database servers.

Logs: Most of the organizations do not log the administrator's accounts .Being a privilege account logging of these users becomes imperative .however one has to be conscientious of granting modify access to the logs. As the users may be treacherous since they have capability of abusing the system and later wipe out the logs.

Application users: there are multiple application used by each business function, all these applications may hosts Privilege user accounts. These privilege users have access to tweak the application, change the settings, and have access to the backend data along with the logs. Without monitoring and understanding the access level of the privilege users could expose the company to the perils of sabotage or data theft.

The privileged IDs are usually shared among a pool of users, can cause accountability and compliance issues, and can thus increase the risk for sabotage and data theft

Solution:

Stock of user accounts: Users' accounts on the network devices should be accounted for privilege access. One has to keep an inventory of all the privilege users' accounts. These users should be monitored and access rights of these users should be granted only on need to know basis. Renaming the admin accounts is a wise way to keep amateur hackers at bay.

Monitoring the access: IT team should take a stock of all the privilege users' account in the enterprise. Organization should consider monitoring these accounts regularly. A process can be put in place to regularly change the passwords.

Although it's a cumbersome task to do this manually, there are off the shelf product available in market which can automate the activity.

Unauthorized changes: having an elevated access gives a privilege to the administrators to carry out unauthorized changes to the systems or the application. Hence all these unauthorized changes should be logged and thoroughly investigated. It would be wise decision to have the investigation conducted by a third party.

Logging: privilege user's activity should be logged. One has to enable logging to key system and applications. Logging would give enough evidence to detect any suspicious activity carried out by any privilege user account. As the size of the logs are proliferated each days , to find a log is like a needle in a haystack hence Centralize log management is a good way of collecting all the logs centrally to manage and monitor the logs for any suspicious activity and avoid it been altered.

Separation of duties: users should be granted privilege access only on need to know basis. One should very carefully in designing the access to the privilege users. Separation of duties concept should be wisely integrated while giving the access. The monitoring activities should not be managed by the privilege users as they might alter the logs.

Security audits: continuous security audit reviews should be carried out for privilege user's access. The internal audit team should have user access management audits embedded into their existing audit plans

Products can be handy: there are hosts of products available in the market which can assist one in monitoring, reviewing, and logging access rights of the users. These products can integrate into the existing infrastructure can add teeth to the existing information security framework

Policies and procedures: organizations should indite policy on privilege users access management. Having a robust policy assists organization not only to protect it from the iniquitous hackers but also built a framework to have unobtrusive way of adhering of information security asset

Regulations and Standard for help: Most of the organizations will be attracting one or more regulation or compliance which will enforce one to demonstrate the efficacy of management to manage the privilege accounts. Regulations such as SOX / HIPPA, PCI DSS mandate user access management to be diligently monitored for assuring safety of vital data. Regulations and compliance can propel to have a rigor around the user access management. ■

Sanil Nadkarni is a executive level management professional with more than 13 + years of core Information Security, Fraud & Risk Management experience with leading Fortune 500 multinational companies. He has authored several articles and news letter in various national and international magazines. He is a speaker and an avid reader.

sanilnadkarni@yahoo.com