Get Ahead of Your Next Security Breach

Five Steps to Mitigate the Risks of Privileged Accounts

Abstract

Privileged accounts are a necessity in any enterprise IT environment, since they enable administrators to manage the environment. But as news reports constantly remind us, granting privileged access increases the risk of a security breach, no matter what industry your organization represents. However, your organization does not have to become the next statistic. By taking the five concrete steps outlined in this paper, you can help protect your organization from the risks inherent in privileged accounts.

Introduction

Privileged accounts are a necessity in any enterprise IT environment: administrators must have enhanced privileges to manage the environment. But privileged accounts also introduce serous compliance and security risks. In particular, privileged accounts are often "all or nothing." For example, in Unix, enabling a help desk member to perform even simple password resets requires granting them full administrative rights, which can be misused either intentionally or accidentally. Moreover, privileged accounts are inherently difficult to manage; since many people and systems need access to the same credentials, it is difficult to keep the credentials secure, change them regularly, and hold individuals accountable for actions taken using the credentials.

These risks are serious, since they do lead to security breaches. In fact, Verizon's "Data Breach Investigations Report" found that 76 percent of breaches exploited weak or stolen credentials, and 13 percent resulted from privilege misuse and abuse. How can you help protect your organization? This paper outlines five clear steps your organization can take to mitigate the security risks of privileged accounts.

Ensuring that privileged passwords are changed on a regular basis will go a long way toward tightening security in your environment.

Step 1: Take an inventory of your privileged accounts, including the users and systems that use them.

You can't mitigate the risks of privileged accounts if you don't know how many accounts you have or who needs access to them, so take a careful inventory. Also inventory the individuals who use those privileged accounts, and remember that privileged passwords are often hard-coded in many scripts and applications.

With a comprehensive list of all privileged accounts and the people and systems who need access to them, your organization can assess where it is most vulnerable to internal or external security breaches, so you can focus on those areas first.

Step 2: Ensure your privileged passwords are stored securely.

Once you have created an inventory of all your accounts and passwords, be sure to store those credentials securely. One good option is a solution that creates a "password safe" to secure privileged credentials using multiple security layers, including encryption, firewalls and secure communication.

Password safe technology can also help ensure that privileged credentials are provided to users who need them in a timely manner with appropriate approvals. If you don't want to use a password safe, at least ensure that all privileged passwords are encrypted, and that accessing them requires multiple layers of authentication.

Step 3: Enforce strict change management processes for privileged passwords.

Most organizations recognize the importance of requiring strong passwords with regular changes, but often they are better at enforcing this policy for everyday users than for privileged accounts—often for good reason. Since privileged credentials are often hard-coded in scripts and applications, changing privileged passwords introduces the risk of important applications failing.

Creating a complete and accurate inventory of the scripts and applications that use privileged credentials, as explained in Step 1 above, is a good start. You may also want to consider investing in a software solution that can replace hard-coded passwords with programmatic calls that dynamically retrieve the account credentials.

Ensuring that privileged passwords are changed on a regular basis will go a long way toward tightening security in your environment.

Step 4: Whenever possible, ensure individual accountability and least privileged access.

Good security, as well as many compliance regulations, requires both individual accountability and least privileged access. Organizations must know exactly who had access to what and when, and they should grant only the level of access a user needs in order to perform the task at hand. Doing so limits harmful actions, whether unintentional or malicious.

However, not all systems provide native tools that enable you to enforce individual accountability and least-privileged access. In those situations, you might want to look into third-party solutions that provide granular delegation and control.

Step 5: Audit use of privileged access on a regular basis.

It's not enough to simply control what privileged users are allowed to do; you also need to audit what they actually do. On a regular basis, generate and review reports that note when privileged

passwords were changed and what potentially harmful commands have been used on each system, and by whom.

In addition, institute a process for periodic certification to ensure users who can gain or request access to privileged accounts should retain those abilities. Through regular auditing, reporting and certification, your organization can better understand how well it is securing privileged accounts, discover areas for improvement and take steps to reduce risk.

Conclusion

Privileged access represents a serious security risk that must be addressed in a thoughtful, practical and balanced way. There is no silver bullet for IT security, but by taking the five steps outlined here, your organization can assess its current situation, identify gaps and mitigate the risks involved in providing privileged access.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

It's not enough to simply control what privileged users are allowed to do; you also need to audit what they actually do.

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.