One of Today’s Most Overlooked Security Threats—Six Ways Auditors Can Fight It

By Calum MacLeod

What is today’s biggest IT security threat? The answer is IT staff members, according to reports from IDC and Carnegie Mellon University/US Department of Defense (DoD). IDC research finds that enterprises rank insider sources as their top security threat. In addition, research from Carnegie Mellon University for the DoD finds that when it comes to insider attacks, 86 percent of perpetrators held technical positions. Of these, 57 percent performed the attack after termination.

Both reports found that insider attacks result in costly outages, lost business, legal liability and, inevitably, failed audits. In one case study, it took 115 employees 1,800 hours to restore data deleted by a disgruntled insider. At the time of the attack, the perpetrator was a former employee of the IT department who was able to remotely access key systems. According to these reports, IT insiders commonly acquire and maintain powerful system access even after termination.

The following are six of the best practices for battling this menace:

1. Create an inventory of privileged passwords. Privileged passwords are the nonpersonal, shared passwords that exist in virtually every device or software application in an enterprise, such as “root” on a UNIX server, “Administrator” on a Windows workstation and an application ID used by a script to connect two databases. Many companies begin the process of securing their privileged passwords by taking an inventory of how many exist and how often they are updated.

In this effort, it is important to note that privileged passwords exist in many places within the enterprise, such as:

- Administrative accounts that are shared by multiple IT professionals and come predefined by the manufacturer. These include UNIX root, Cisco enable, database administrator accounts and Windows domain.
- General shared administrative accounts, such as help desk, fire-call, operations and emergency accounts
- Hard-coded and embedded application accounts, including resource database IDs, generic IDs, batch jobs, testing scripts and application IDs
- Service accounts, such as Windows service accounts and scheduled tasks
- Personal computer accounts, including the Windows local administrator on laptops and desktops

Many organizations still manually update these passwords, if they change them at all. For example, a recent study showed that 42 percent of application passwords are never changed.

2. Define the role of identity and access management (IAM). When it comes to managing privileged passwords, a common first misstep is to import all administrator or shared IDs into a system built for managing human identities. The benefit of this approach is that organizations can automatically update the privileged passwords. The drawback is that the organization still has no way of assigning individual responsibility. For example, the reports may show that the administrator identity downloaded the database of top clients at 1:47 a.m. Sunday morning. However, that action—or its consequences—cannot be tied to a particular individual.

To deliver true accountability, the system for privileged password management (PPM) must tie individual identities to shared accounts. This is incredibly sensitive data—a hacker’s dream list of all the privileged passwords—so this information must be stored in an exceptionally secure place. IAM solutions are not designed to store sensitive data and typically partner with a PPM solution for the privileged accounts and passwords.

3. Apply change policies to privileged passwords. This may sound obvious, but one would be surprised how often policies for privileged passwords are not as explicit as those for their human counterparts. For instance, a password for a laptop may be changed every 30 days; however, surveys show that a workstation has a 20 percent chance of never having the administrator ID changed from its default. In other words, if a laptop is lost, the finder may not know who the owner is or at what company he/she works—but the finder can search the web to find the default administrator password that ships with a Dell Latitude D600. Within seconds, the laptop’s new owner will have more access to the systems than the legitimate owner had.

It is recommended to have an explicit policy that names all the password types uncovered during the privileged password internal survey and spell out update policies for each. Best practices dictate that these policies should be at least as stringent as those for individual employees.

4. Ensure that privileged passwords are stored securely. Again, this may seem obvious, but it is imperative that organizations store their privileged passwords in the most secure vaulting system available. Placing the passwords in wallet-sized cards are not acceptable alternatives (unfortunately, this author has observed all of these methods in use).
5. Create a staged approach to deployment. Privileged passwords are literally the keys to the kingdom and must be controlled properly. One common stumbling block for projects around privileged passwords is that once the password inventory is created, the sheer volume and prevalence of these codes is overwhelming. Personnel can throw up their hands, saying: “We never secured these before, so why bother now?” In these situations, the most successful auditors take a deep breath, drink a tall latte and start putting together a stepped plan with reasonable deadlines, deliverables and consequences.

6. Remember that computers are people, too. While 99 percent of enterprises change passwords for employees, up to 42 percent never change hard-coded and embedded passwords for application IDs, testing scripts and batch jobs. According to Mark Diodati of the Burton Group, this creates an App2App password problem that is “exponential. For example, 300 hosts multiplied by two applications per host multiplied by five scripts per application equals 3,000 stored passwords.” Often, these passwords are in cleartext and readily available to every developer or database administrator in an organization.

All in all, no privileged password management system is complete without an App2App component. However, since application passwords are stored in scripts that must be recoded, tested and deployed, many organizations neglect fixing past code that would prevent future mistakes. Once again, a stepped plan can be the organization’s best friend.

One final note to consider is that no policy for managing privileged passwords would be complete without related reporting structures. Audit reports for privileged passwords often cover such topics as when passwords are updated, any update failures and which individual identities performed tasks under a shared account.

In conclusion, the greatest threat now posed to IT security is due to the smallest of things, a tiny code embedded in virtually every piece of hardware and software. However, armed with a strong plan and the knowledge that they are protecting their organizations, auditors can become successful warriors against today’s top IT security menace.

Endnotes
1 Hudson, Sally; Privileged Password Management: Combating the Insider Threat and Meeting Compliance Regulations for the Enterprise, IDC, 2007
2 Cappelli, Dawn; Akash Desai; Andrew Moore; Timothy Shimeall; Elise Weaver; Bradford Willke; Management and Education of the Risk of Insider Threat (MERIT) CERT3 Program, Software Engineering Institute and CyLab at Carnegie Mellon University, 2006
4 Ibid.
5 Ibid.

Calum MacLeod is European director of Cyber-Ark Software. He has more than 30 years of experience in the IT industry. Prior to joining Cyber-Ark, he was a PKI and VPN consultant and business development and product manager in several venture capital-funded companies in the US and Europe.