The Top 8 Critical Security Components for User Accounts

Modern operating systems are organized to meet the needs of various users. User accounts, from the standpoint of a consumer, are meant to be configured and customized based on the needs of the individual who will be in control of the account. Regardless of the ultimate purpose of the account, several security-related considerations come into play that need to be addressed by proper information technology (IT) infrastructure.

What follows are the 8 leading critical security components for user accounts that every organization should put into practice.

1) **Training** – Immediately upon hire, training should take place before any network credentials are distributed. The training should then be repeated on an annual basis. This will ensure that every person knows the current practices and the specific details of what a user should and should not be accessing with their accounts.

2) **User account**s – Users are the weakest link in any organization. Without advanced IT infrastructure in place, security professionals cannot ensure that users will remain protected. In most cases, securing user accounts is the first step in developing a protected infrastructure.

3) **Separation between normal and privileged user accounts** – System administrators and other types of privileged users should have separate accounts for their day-to-day work and for performing their special functions. These administrative (admins) accounts should have additional security controls. For certain types of accounts (such as accounts that have access to production environments), there should be a rights escalation process to ensure that even admins do not have unfettered, always-on access to sensitive areas. This way, preventative measures will be in place so that sensitive data and environments do not encounter malicious or unintentional damage.

4) **Multifactor authentication** – Many high-profile breaches are instigated when an attacker acquires compromised credentials (usernames and passwords). Using an additional layer of security, such as hard or soft tokens, makes it much more difficult for an attacker to gain complete access to an organization's network. Including multi-factor authentications significantly reduces the risk posed to an organization from compromised credentials.

5) **Up to date information** – Updating contact details, job titles of personnel, managers and program stakeholders is crucial. This way, whenever there is an organizational change or security incident, organizations can quickly access any needed information.

6) **Review of group memberships –** Every organization should have an operating procedure in place that reviews and revises group memberships and other access privileges. Reviews should occur periodically (at least once a quarter) or when a user changes positions. If a user's new role does not require access to resources that their old role gave them, that access should be removed.

7) **Development, test and production account management** – Within multiple environments, there is a temptation to share accounts in order to streamline the development process. However, this greatly increases the risk to your production environment and thus, your client's data and publicly facing software. Using sensitive production data in test environments should always be avoided, and

responsibilities for development, testing and production should be separate and performed by separate resources.

8) **Disable stale accounts** – Recently inactive accounts should be disabled and accounts that have been dormant for longer periods of time should be deleted. Accounts that have been dormant for more than 90 days should probably be removed completely.

Implementing these security measures is the best way for organizations to protect against data breaches and ensure that user accounts are managed in an effective manner.