Proper Data Security

DEAN WIECH, Managing Director at Tools4ever

In today’s complex corporate and business network environments, controlling access to sensitive data is of utmost concern. The amount of security-related data stored across a network is immense for many organizations, and relating all this data to the user’s account information in Active Directory can be tricky and time consuming.

There are really three sides to proper data security. The first step is ensuring that new employee accounts are created with the proper access rights when an employee joins the organization. The second is making sure those access rights remain accurate during the employee’s tenure, and the third is revoking all access rights when the employee leaves.

Let’s take a more in-depth look at solutions for all three of these phases of data security.

Solutions

By using a role-based access control matrix in conjunction with an identity management solution, companies can ensure that accounts for new employees are always created with proper access rights.

The first step of this stage is to define the roles that employees should have in the organization. This is usually a combination of department, location and job title. While establishing the data access rights, group memberships and application requirements for each role can be time consuming, the end result will allow a template for both new employee creation and an audit point in the future.

Software applications are available that will allow the linking of a human resource system to Active Directory for automatic account creation with all proper rights. Additionally, if there are special requirements, a workflow system can easily be

established to allow manager and system owners to process approvals before access is granted.

Access rights to data often tend to creep into multiple areas over an employees' tenure with an organization. For example, rights are assigned to one employee for special projects while one employee is covering for another on leave or when an employee changes departments and responsibilities. The revocation of these special or historical rights occurs infrequently at best. Again, software solutions are available to analyze the rights of employees and make the information actionable. For the product to provide value, there are several items that should be considered as mandatory including the ability to detect:

- Direct access to a file/directory rather than access through a group membership;
- Access to a file/directory through multiple or nested group memberships;
- Groups and user accounts that are no longer present in Active Directory;
- Duplicate access privileges to a file/folder of a user or user group;
- Access to files/directories through a local or file system user account.

Once an audit of access rights is performed, it can be compared against the baseline template for each employee role initially established. Any deltas can then be sent to managers and systems owners for verification or revocation of the rights.

The final step in the data security process is one that is often overlooked or not performed in a timely fashion: The termination of access rights to the network, data and all applications, including cloud-based solutions, must be accomplished immediately upon an employee's termination.

Recently, a sales manager at a large organization that's also a client of Tools4ever told a horror story about this very topic. A terminated sales rep had his network access revoked immediately upon departure, but the organization did not have a process in place to disable access in a timely manner to a cloud-based business intelligence application. The terminated employee realized the account was sill "live" and proceeded to download more than 10,000 records over the course of the next 30 days at a cost to the company of more than $6,000.

The point of this story: Imagine the costs if 20, 30 or 100 terminated employees did this very same thing in a short period of time.

When putting a process in place to handle terminated employees, the most common scenario is, once again, a link to the HR system. When an employee is terminated, a synchronization process needs to be in place to handle the decommissioning of accounts in all internal and external systems. If feasible, using web services or application programming interfaces (API's) to automate the process will save time and money in the long run. Where not feasible, an email workflow process should be established whereby system owners are notified to terminate the account and positive feedback required to establish the work has been completed.

Summary

It is imperative that organizations implement the necessary security measures to insure that access to data, groups and applications are right sized for an employee during their tenure. Equally critical is the revocation of all account access when they depart. Failure to meet these criteria can lead to theft of secure data and costly access to external applications.

For more information, please visit www.tools4ever.com *[1].*

Links:
[1] http://www.tools4ever.com/