CSO

RISK AWARENESS

By Robert C. Covington, Contributor, CSO

JAN 2, 2019 10:49 AM PT

OPINION

5 steps to simple role-based access control (RBAC)

RBAC is the idea of assigning system access to users based on their role in an organization. It's important to remember that not every employee needs a starring role.

Despite all of the advanced attack scenarios we face in cybersecurity today, it seems like we continue to shoot ourselves in the proverbial feet with the simple things.

Case in point: the 2017 Verizon Data Breach Investigations Report found that 81 percent of hacking-related breaches involved compromised credentials. Further, a simple failure can have systemic impact, as was documented recently in the Crowdstrike Intrusion Services Casebook 2018. As part of their research, they documented a case of a large, multi-national apparel company user working on a public network, while in a coffee shop. The user's credentials were compromised, resulting in the compromise of the company's entire infrastructure.

[Keep up with 8 hot cyber security trends (and 4 going cold). Give your career a boost with top security certifications: Who they're for, what they cost, and which you need. | Sign up for CSO newsletters.]

Why do we find something as seemingly simple as access control to be such a challenge? Perhaps it is because it only seems simple. As an example, consider a company with just 20 employees and 5 systems. Let's also assume that for each system, a given user might need to

use it only to read files, for read/writing of files, for administrative access, or no access at all. The number of possible permutations of access settings in such a small environment is huge.

Add to the problem the fact that in a typical smaller company, management of access rights is casual at best, even "one size fits all" in some cases. It seems that this simple problem is not so simple at all. Yet, if we can't get this right, our chance of having even reasonably secure systems is pretty small.

The solution to this problem is not new. It dates back to the 1970s, long before information security was on anyone's radar. The approach is called role-based access control (RBAC). According to a National Institute of Standards and Technology (NIST) document, the first formal **RBAC model** was proposed in 1992. Thus, we have been sitting on a strong approach to this problem for many years.

What is RBAC?

RBAC is nothing more than the idea of assigning system access to users based on their role within an organization. The system needs of a given workforce are analyzed, with users grouped into roles based on common job responsibilities and system access needs. Access is then

assigned to each person based strictly on their role assignment. With tight adherence to access requirements established for each role, access management becomes much easier.

The question therefore is why, with an achievable and time-honored approach, we can't seem to get a handle on access control. We are certainly being pushed in that direction of RBAC, with all of the major standards, including PCI DSS, HIPAA and Gramm-Leach-Bliley all requiring some form of it.

I would suggest that one reason RBAC is not used more frequently is that for small to medium companies, it seems easier to just do this on an ad-hoc basis as each employee joins the company. The challenge is that with as many permutations as can exist with just a few systems involved, the approach becomes unsustainable.

What is the benefit of role based access control?

With the proper implementation of RBAC, the assignment of access rights becomes systematic and repeatable. Further, it is much easier to audit user rights, and to correct any issues identified.

RBAC may sound intimidating, but it can in reality be easy to implement, and will make the ongoing management of access rights much easier and more secure.

The data breach you prevent may be your own.

RBAC vs. ABAC vs. ACL

There are some alternatives for/variations of RBAC, including:

Access control lists (ACL) — An ACL is a means of defining access rights by a given user or user group, to a specific object, such as a document. As a simple example, an ACL could be used to allow users from one department to make changes to a document, while only allowing users from other departments to read the document.

Attribute-based access control (ABAC) — ABAC, sometimes known as policy-based access control, can use a variety of attributes, including user department, time of day, location of access, type of access required, etc. to determine whether a user's access request should be granted.

Both of these options provide additional granularity of controls beyond the basic concept of RBAC, but can also greatly expand the effort required to create and maintain the necessary permissions. RBAC arguably offers a more simplified and manageable approach, given that the privileges of a user in a given position are granted with a simple effort, to all others in the same role. These methods can, however, be used in tandem to increase control.

RBAC implementation

Hopefully I have convinced you to take a closer look at RBAC. If so, consider the following simplified five-step approach to getting it implemented:

1. Inventory your systems

Figure out what resources you have for which you need to control access, if you don't already have them listed. Examples would include an email system, customer database, contact management system, major folders on a file server, etc.

2. Analyze your workforce and create roles

You need to group your workforce members into roles with common access needs. Avoid the temptation to have too many roles defined. Keep them as simple and stratified as possible.

For example, you might have a basic user role, which includes the access any employee would need, such as email and the intranet site. Another role might be a customer service rep, that would have read/write access to the customer database, and a customer database administrator, that would have full control of the customer database.

3. Assign people to roles

Now that you have a list of roles and their access rights, figure out which role(s) each employee belongs in, and set their access accordingly.

4. Never make one-off changes

Resist any temptation to make a one-off change for an employee with unusual needs. If you begin doing this, your RBAC system will quickly begin to unravel. Change the roles as required or add new ones when really necessary.

5. Audit

Periodically review your roles, the employees assigned to them, and the access permitted for each. If you discover, for example, that a role has unnecessary access to a particular system, change the role and adjust the access level for all employees in that role.

As an example, many healthcare organizations, given the need for regulatory compliance in controlling access to medical records, use RBAC to define exactly what access to medical records each type of clinician may need. While a doctor might have almost unlimited access to the records of patients he/she manages, a receptionist might be limited to basic contact information needed to manage appointments. Given the large number of staff members in well stratified roles, RBAC is an efficient way to control record access in compliance with HIPAA, and other regulations.

There are tools that can help with setting up RBAC. Many systems, such as Microsoft Active Directory, have built in roles that you can use as a starting point, which you can extend to fit your unique situation. You can also use an identity management system to automate the assignment of privileges based on role.

More on access control:

- **What is access control? A key component of data security**
- **5 steps to simple role-based access control (RBAC)**
- **Role-based access control is fine – who needs attribute-based access control?**
- **HP gives software robots their own IDs to audit their activities**
- **What is identity management? IAM definition, uses, and solutions**
- **The best identity management advice right now**
- **What is SAML? How it works and how it enables single sign on**
- **What is OAuth? How the open authorization framework works**

Next read this

- *24 best free security tools*
- *8 hot cyber security trends (and 4 going cold)*
- *Top cyber security certifications: Who they're for, what they cost, and which you need*
- *The 10 Windows group policy settings you need to get right*
- *10 essential enterprise security tools (and 11 nice-to-haves)*
- *How to perform a risk assessment: Rethinking the process*
- *6 steps for building a robust incident response plan*

Robert C. Covington, the "Go To Guy" for small and medium business security and compliance is the founder and president of togoCIO.com. Mr. Covington has BS in Computer Science from the University of Miami, with over 30 years of experience in the technology sector, much of it at the senior management level.

Follow