CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Addressing Insider Threats, Cyber Attacks & Data Security

Combatting Insider Threats

Insider Threats were one of the primary drivers for the creation of Privilege Account Management products back in the mid-2000s. One of the core factors to combatting insider threat is individual accountability. Individual accountability sounds easy in theory (John Smith has a userid jsmith and therefore is accountable for all actions performed by jsmith), but in practice it can be much more complicated.

The first issue is around accounts that are not 'owned' by a single person. The most common examples of this are the 'root' account on Linux servers, or the Local Administrator account on a Windows server. These accounts always exist and have a password. This password might be needed in emergency situations (single user mode on a Linux server, or a Windows member server losing connectivity to Active Directory). The fact that multiple people (even in a Credit Union) might need this password provides the problem for individual accountability. As soon as more than 1 person has access to the password for one of these accounts, you lose the ability to assign individual accountability.

Privilege Account Management products provide a solution for the above issue. These tools take control of these shared privileged accounts. The product manages the password for these accounts and holds them securely until they are needed. When needed, an authorized person retrieves the password from the tool. This provides individual accountability because it is logged who had 'root' or 'administrator' at a specific time. Since the tool is the only one who knows the password until it is released, you know who was using the password at any given time, thus providing individual accountability.

Another issue around insider threat has been the misuse of privileged access. Most tools and applications provide an audit trail to provide information around activities, but unfortunately with enough access the user might have the ability to modify or delete the audit trail. One way of preventing this kind of action is by providing privilege access through a controlled session. Tools that provide this functionality will typically proxy the connection to the target system, and record the activities that occur within the session. The key control is that although the user has privilege access on the target system, they do not have any control over the tool recording the session. This allows the session to be recorded outside of the reach of the user. Therefore, even if the person has root privilege on a server and can modify files on that system, their session is recorded and their actions are available for review.

A typical use case for this scenario involves Remote Vendor Access (RVA). Many Credit Unions have contractors or service providers who support systems within their environment. By using a session recording tool, the Credit Union is able to see all activity that the remote vendors are performing on their systems, thus giving them a more granular view of the activity

As more systems move to cloud or remote support, the definition of 'inside' becomes blurred. By focusing on privilege, you can look to secure your information independent of where it is located or who is supporting it.

Kris Zupan
CEO/CTO

RALLYPOINT solutions

Kris Zupan is CISSP, Chief Executive Officer and Chief Technology Officer for Rallypoint Solutions. Prior to Rallypoint, Kris was the founder of e-DMZ Security. When e-DMZ was formed in 2001, it was a Managed Security Services Company, and by 2006, it was a finalist for the SC Award for Best Managed Security Service. In 2003 e-DMZ Security released the first commercial solution for Privileged Account Management, which in 2006 was selected for the SC Award for Best Password Management Solution. Kris has been a leader in bringing attention to Privileged Account Management and bringing innovative solutions to market. His 2005 ISSA journal article on Privileged Account Management was one of the first to fully detail the issue and possible solutions. He is the innovator of Privileged Session Management, with the release of the first commercial Privileged Session Management (PSM) solution in 2005. Kris is a frequent speaker and author on the issue of Privileged Account Management.

Contact Info

www.rallypoint.us.com