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

Addressing the Big 3: Compliance, Fraud & Cyber Security

The Big 3 are called the Big 3 for a reason… they are complex issues with many facets, and no single solution will address any one of them, let alone all three. Therefore, I will focus the insider threat, which could relate to Fraud or Compliance or Cyber Security, depending on the situation. The insider threat can be divided into a number of areas to address- hiring processes, training processes, etc. but the one key fact is that there are people who will not follow the rules and will do bad things. This insider threat may exist at many functions (teller, manager, loan officer), but I will focus on a specific type of insider threat- system administrators.

System administrators are a special class of user because their business function requires them to work at the system level. This access in many cases gives them the ability to bypass the security controls put in place to prevent activities. There is no way to eliminate system level access- systems will break, need to be patched, etc. and system access is needed for these functions.

The piece that can be controlled is individual accountability. If a system administrator needs root access on your core system, you should at the very least know who is using that access. Privileged access should be monitored, and one way of providing that monitoring is by controlling privileged access through the use of Privileged Password Management (PPM).

PPM can provide individual accountability because the person who needs privilege is given the password for a limited time, and then the password is changed to remove their access. The person who requested the password is responsible for any activity done with the privileged account. This may not prevent a system administrator from taking an action, but it eliminates the ability to do it anonymously. PPM can also support the ability to enforce dual control, requiring more than one individual to be involved in the gaining of access. Though not always feasible for a small IT staff, dual control (maker-checker) has been used as a fraud control for years. PPM allows this same control to be used for privileged access.

In summary, the insider threat will not go away. You can implement strategies to screen employees and try to minimize the chance of it occurring, but if you look at the headlines, you will see that this threat will never go away. System administrators who have privileged access should have additional controls, since their access is so powerful. Individual accountability and dual control are additional tools to implement to provide these additional controls.

Kris Zupan
Chief Executive Officer

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