CU t-t CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Online, Mobile, Network & Physical - Securing the Spectrum

At the end of the day, online, mobile, and network all rely on the same underlying technology- servers. Whether they are web servers, app servers, or core systems, many of the fundamental security practices still remain the cornerstone of controlling these systems. Rallypoint Solutions focuses on Privileged Account Management, controlling the access for the superuser accounts on these systems. Co-Managed Privileged Password Service (CP2S) is a service designed specifically for Credit Unions to address the issue of controlling who has access to the Administrator or root accounts on these servers.

While the spectrum keeps getting wider, it makes it even more important to understand that the days of a hard shell with a soft chewy center are gone from a network perspective. APTs and other threats have increasingly penetrated the perimeter. This is why the simple and fundamental processes become even more important. Ensuring that privileged passwords are not shared and are changed frequently is a compensating control against the APTs that are looking to harvest passwords through key-loggers or viewing cached credentials. Ensuring that IT administrators use non-privileged accounts by default can make malware less effective.

My analogy is pro football. While new schemes are introduced (whether Wildcat, West Coast, etc) the games are won or lost based on blocking and tackling - the fundamentals.

This is even more important when you have limited time, money, and manpower. The fundamental controls have continued to exist because they work. Too many people think that old security is bad security- I think just the opposite. If you look at the SANS Top 20 Security Controls, most of these were in infosec policies twenty years ago. The controls around inventory, control of network ports, controlled use of administrative privilege and others continue to work whether the attack is from across the room, across the street via wireless, or across the globe.

Rallypoint Solutions focuses on Critical Control 12: Controlled Use of Administrative Privilege, controls that have been around since the 1990s, but are still making headlines today:

From http://www.net-security.org/secworld.php?id=13992

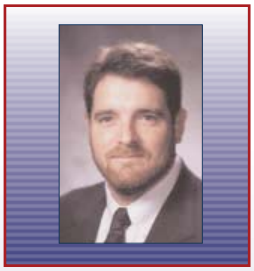
"Privileged accounts have served as the root cause of some of the most significant breaches in recent months, including:

- The Flame virus - Flame, a virus considered the 'mother of all cyberweapons', had a sniffer component that scans traffic on an infected computer's local network, collecting usernames and passwords. From here, attackers were able to hijack administrative accounts and acquire high-level privilege to other computers and network locations.

- Subway data breach - In New Hampshire, two men plead guilty to stealing payment information from Subway restaurants and according to the court documents, the men "remotely scanned the Internet to identify POS systems with remote desktop software applications on them. They logged into the systems over the internet and cracked the passwords to gain administrative access." Once they gained access, they simply installed key logging software to capture data being input."

At the end of the day, if you have limited time and resources- work on blocking and tackling- the fundamentals will never become obsolete.

Kris Zupan
CEO



RALLYPOINT solutions

Kris Zupan is CISSP, Chief Executive Officer and Chief Technology Officer for Rallypoint Solutions. Kris has been a leader in bringing attention to Privileged Account Management and bringing innovative solutions to market. 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. e-DMZ Security was purchased by Quest Software in February, 2011.

Contact Info

www.rallypoint.us.com