CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

It seems that there is a new poster child for privileged password management - Sony. Many in the industry (including myself) have been talking about APTs and the damage they can cause, but it has normally been done with broad brush strokes and not a lot of specifics. The recent hack on Sony has changed all of that by providing painfully detailed examples of their processes. I am not going to spend this article rehashing what has already been published, I am going to focus on one simple part of the incident.

“On Thursday, writers at Buzzfeed noticed that within a trove of stolen Sony files being shared online in the wake of the recent high-profile hack of the company’s network is a folder named “Password” containing, predictably, dozens of documents purported to allow access to dozens of accounts used by the movie studio.” http://rt.com/usa/211903-sony-hack-password-folder/

Put yourself in Sony’s shoes for a moment. How many Credit Unions have similar lists and files ‘hidden’ in their organization? How many spreadsheets with passwords to admin accounts protected with an excel password or worse, not protected at all? How many passwords used by Network administrators to gain privilege are used across multiple systems, so that as soon as the password is known, the attacker has the ability to access multiple sensitive servers?

The hackers attacking Sony weren’t able to grab the amount and type of data without the use of privileged accounts. Sony made it easy when they provided a file called “systems user IDs and paswords.xlsx”(http://gawker.com/sonys-top-secret-password-lists-have-names-like-master_-1666775151). Can I say definitively that a Privileged Password Management (PPM) system would have prevented this attack? Absolutely not, but it sure would have made it more difficult.

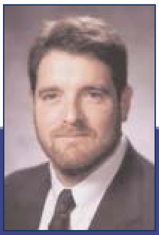
There has been some discussion of how the APT first got into Sony, but the point is that how the network is breached is no longer the real issue. With enough time and money, a determined attacker will get into a network. As shown in this and almost every other APT attack, the target is privileged passwords. The privileged passwords are the key to getting the ‘good’ data. Since every system has at least one privileged account, and you have to assume that the password can be compromised, the defense against APTs as it relates to privilege comes down to two questions:

1. How long is the credential valid?
2. Where can the credential be used?

How long a credential is valid is based on how often that password is changed. If an APT steals a password through a keylogger or ‘pass the hash’ method, the timer starts for how long that password is valid. If you are using a PPM system that changes the passwords frequently and after use, this time could be 2 hours. If you are like many organizations, this password may be good for 30-90 days. This is a huge difference in the likelihood of an attacker being able to use the stolen credential.

Where the credential can be used is the second factor. If you use AD accounts to gain privilege, then the compromise of that credential puts every member server in the organization at risk. If you use a local account for privilege (a growing trend due to APTs), then the credential can only be used on a single device.

As Credit Unions decide how to best use resources to protect their organization, I think that the Sony example demonstrates the need for Privileged Password Management. There are numerous solutions (some that cost nothing at all) that can make sure that your Credit Union doesn’t have to explain why it has a password file in Excel sitting in their network.



RALLYPOINT solutions

Contact Info

www.rallypoint.us.com
Phone: 302.543.8087

Kris Zupan
CEO/CTO

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.