Mobile, Virtualization, Cloud, and ... Anti-virus?

Each year, Credit Union tech-talk hosts an informative and interactive conference dedicated to the Credit Union IT professionals; the Credit Union InfoSecurity Conference. With its inaugural event taking place in 2002, this year’s 2011 conference marked its 9th anniversary. Comparing this year’s topics to that of the past, one might find it intriguing that AV (anti-virus) still tops the list.

In 2002, the main topics included best practices in security policy, security lifecycle management, and applying security to the real world problems faced by the Credit Unions. From a research perspective, topics included understanding security threats, and the other side of the coin, the impact of a security breach to a Credit Union. From an operational perspective, the conference aided in discussions surrounding protecting the core datacenter, online banking security, and the use of biometrics.

In 2011, a number of the topics were certainly more advanced in terms of how Credit Unions must provide additional technology-driven business services to their members whilst protecting them across their use of an ever-increasing set of technologies and communication channels. For example, mobile banking, cloud computing, virtual desktops, bi-directional authentication, and anti-phishing protections captured some of the spotlight during the sessions and on the vendor show floor.

Having been involved in the anti-virus space for a number of years, I found it fascinating that there was a dedicated focus on different technologies and processes designed to protect against viruses and similar threats. Clearly, the 10-year-old (or more) idea that “AV is dead” is about as far from the truth as possible; it is still top of mind for many representing the Credit Union Info Sec group this year. To this end, there were 3 sessions and as many vendors speaking to blacklisting, whitelisting, behavioral-based protections, and other malware protection trends.

Setting the AV trend aside, there was one session in particular that caught my attention this year – it was a presentation and demonstration highlighting a collection of technologies from multiple vendors implemented together to solve some of the most important security challenges faced by Credit Unions – user management, policy management, and access control; all pulled together in an effort to protect against internal fraud. This was a well-received topic as many of the attendees noted that internal theft exceeds, and will likely continue to exceed, that of externally-driven fraud.

Going beyond the piece-meal efforts presented by most vendors, JCS and Associates, Inc. (www.jcsinc.com) worked with several of their vendors to demonstrate – live – the use of VDI (virtual desktop infrastructure), combined with a zero-client device, coupled with strong multi-factor authentication/sign-on, all feeding a comprehensive log management/SIEM solution. Respectively, the vendors in play during the demonstration were Microsoft, VMware, Pano Logic, Indigo Identityware, and LogRhythm.

The end-to-end solution presented would allow Credit Unions to define roaming policies for each of their users and apply those policies, including controlling and launching the applications available to the user, only when the user logged in to one of the CU’s zero-client devices using strong, two-factor authentication. When the user completed their work and locked their PC for lunch, or even moved to
another zero-client device mid-stream in the day, the instance, including all running applications, would follow them to each of the zero-client devices they successfully logged in to. At the end of the day, or when the user left at the end of their shift, the virtual desktop instance would be cleared and re-set to a known good state, and even updated with the latest protections and patches. The instance and related policy would be ready for action for the next shift or the next day. This was a huge hit for a number of the attendees sitting in on the session, with one of them even claiming that “it is good to see this working - roaming profiles usually make me want to hang myself.”

The logging capabilities included in the demonstration captured all of the activities performed by the users, at each device, for each application used, providing deep views into who’s doing what, to which assets, where, and when; this is great for identifying internal attempts to conduct various forms of fraud.

While not a formal part of the presentations and vendor show floor, data integrity was another topic running throughout the conversations by many of the attendees, revolving primarily around standard banking transactions through new channels (via SMS, online, and mobile channels), proactive logging and monitoring (for fraud detection, insider attacks), and regulatory compliance (for auditing and forensics). It seems that most vendors, and therefore the Credit Unions that use the vendors’ products, are rolling the dice here to some degree. It will be interesting to see how the Integrity leg of the Confidentiality/Integrity/Availability (CIA) security triad plays out over time. Will fraudsters win out because the staff can’t prove something did or didn’t happen? Will the Credit Unions lose because they can’t prove to their members, partners, internal auditors, examiners and legal counsel that their security measures did in fact work?

Switching topics dramatically, the most entertaining part of the conference is usually the behind-the-scenes tour of a volunteer organization. In most cases, it is a Credit Union that offers a view into how they manage their security programs, delivered through a group visit to their offices located near the conference site. This year, however, the conference attendees were given a special treat; a behind-the-scenes tour of the security monitoring program for the Stratosphere Hotel and Casino located in downtown Las Vegas.

During the tour, the group learned that there are over 1,500 cameras recording and archiving nearly every visual and electronic transactional aspect of the property, from the casino to the hotel, and from the parking lot to the observation platform sitting near the top of the 1,149 foot tower.

The security staff will monitor the cameras, looking for “JDLR,” a term used by the staff meaning “Just doesn’t look right.” More specifically, the staff will leverage facial recognition technologies to identify players that have been banned from their casino, or all casinos. They will also look for cheating players and cheating employees.

As internal fraud and theft are a key source of risk and expense for the casino/hotel business, the capabilities of the system for monitoring employee activity is very important, and therefore, turned out to be very impressive. For example, the security staff are able to video record the actions of the bar staff as they login to the cash register, collect money from the customer, enter the transaction into the cash
register, and place the money in the till. As they are doing their job, their actions are being recorded on video and the transactions performed at the cash register are recorded in real-time and displayed on the video monitor display, in synchronized time, alongside the video. This allows the security staff to see if the bar staff have accepted money yet canceled a transaction at the till.

While the casino and hotel industry differs greatly from the financial industry, the need to monitor and identify fraudulent activity and other forms of theft is certainly common and high on the list for both.

As the Credit Union tech-talk staff prepare for their 10th anniversary conference in 2012, we’ll have to keep an eye out to see what hot security topics rise to the top for the Credit Union movement and what Credit Union speakers can cover that will help shed some light on how they manage their most pressing security risks. The big question remains: will anti-virus topics make the list again next year?

###

Sean Martin is a CISSP and founder of imsmartin consulting. Write him @ sean@imsmartinc.com.