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

Credit unions are continually expanding the number and types of products and services that they offer to their members. This is especially evident in the online and mobile channels that continue to prove ever popular with consumers. While this is a great strategy for growing their membership base, it brings a plethora of new security challenges for credit unions of all sizes.

At GMV, we have ample experience in the performance of Security Diagnostics, Business Security and Continuity Plans. We are also focused on protecting a credit union's internal resources – whether from remote employees or members connecting to online banking systems. Guaranteeing that the computers used for remote access are malware free is therefore, at best, a tricky business when the computers are controlled by the credit union and, at worst, virtually a lost cause in the case of public or home computers under the control of members.

To counter this issue, we have developed codelogin which uses the user's cell phone to guarantee secure remote access from any computer, even if malware infected, and all in the most user-friendly way. Its innovative, patented concept can be applied to multiple cases, enabling secure access to online banking. In action, codelogin enables secure access to a local or remote system using strong two factor authentication. The program uses the online banker's everyday cell phone as the authentication device, without the hassles and expense of deploying additional tokens. The solution is unaffected by Trojans due to dual-channel authentication preventing any malware already present in the client computer from manipulating sensitive transactions of the user or carrying out any fraudulent transactions.

Credit union IT Departments will appreciate the ease of which codelogin is deployed. It makes secure access compatible with the classic password/PIN based access, allowing a progressive phase-in and also allowing access in one-off cases where there is loss of mobile coverage. There are no hassles with certificates which eliminates a great deal of management complexity for both IT works and call center agents. There is no need for major changes to existing identity management platforms; and in fact deployment enables authentication to several systems with minimum changes to these systems. We have implemented a common mobile user identity management platform which also manages mobile applications.

Another important source of fraud for the CUs are the ATMs. GMV detected years ago that the ATM fraud was starting to evolve from physical attacks and skimming, towards more sophisticated targeted cyberattacks, based on compromising the ATM by means of malware or other non-authorized accesses to the ATM file system. Traditionally, the financial institutions had tried to protect their ATMs by means of antivirus-based solutions but this approach had proved to be inadequate, since it relies on a periodical update of the virus databases, which just can't keep up with the pace of malware creation. To answer this threat, GMV developed Checker ATM Security, the first specifically designed product to protect ATMs and their networks against malware and cyberattacks. Checker is based on white listing technologies that allow to define a security policy on the ATMs which specifies the set of processes that can be executed, files and libraries that can be accessed, IP connections that are allowed to be opened, so the IT security department makes sure that whatever is not defined as allowed, will be banned. Moreover, Checker protects against the malware-based latest trend of attacks, like Ploutus in Mexico, implementing transparent full hard disk encryption that makes virtually impossible the access from any other system. Compared with a traditional antivirus, Checker has a negligible footprint on the ATMs behavior, being totally transparent to the ATM operations, and it is already protecting over 70.000 ATMs in the world.

In addition to our cyber-security solutions, we operate world class Security Operations Centers that provide financial organizations around the world with a qualified center to securely manage their information systems, to anticipate problems and to immediately resolve risks. Services provided include:

- Early Detection
- Platform, Control and Services Monitoring
- Intelligent Log Centralization and Analysis
- Vulnerability Detection and Management
- Continuous System Patching/Upgrade and Fortification
- Fast Intervention
- Forensic Analysis
- Help Desk

When CUs partner with GMV to assist them with their varied security and compliance issues, they can be assured that they are working with a global technological business group that is committed to an operating model and cultural values that focus on meeting the unique needs of each individual client.

Andres Escobero
Vice President, GMV North America

gmv INNOVATING SOLUTIONS

Andres Escobero is Vice President of GMV North America. GMV is a privately owned technological business group with an international presence. Founded in 1984, GMV offers its solutions, services and products in very diverse sectors: Aeronautics, Banking and Finances, Space, Defense, Health, Security, Transportation, Telecommunications, and Information Technology for Public Administration and large corporations. The leadership position that GMV has attained in these sectors is based on an in-depth knowledge of client needs, which allows us to deliver solutions specifically tailored to their individual requirements. GMV offers clients the best solution, fully adapted to their own requirements and including all the support necessary to achieve optimum results at a suitable price. At GMV, our employees, operating model and cultural values focus on meeting the very needs of each individual client.

Contact Info

www.gmv.com