

CU SECURITY: BEYOND THE MOAT - COMPREHENSIVE SECURITY STRATEGIES

The threats to credit unions are coming more quickly everyday. The industry has seen an explosion of attacks including phishing, Trojans, worms, viruses and keystroke loggers - not to mention new blended threats that combine phishing scams with malicious spyware. Increased employee awareness about these types of attacks and ongoing security training are critical as users still remain the weakest link in the security chain.

On the technology side, financial institutions can no longer rely on outdated signature-based systems. These systems are reactive by nature and can take days or even weeks to be updated. That is why WholeSecurity's solutions incorporate patent-pending behavioral technology so that they can operate in a proactive manner to identify and eliminate both known and unknown threats. Without this kind of sophisticated technology in place, organizations simply cannot protect against zero day and targeted attacks.

Securing endpoint PCs for any employee or vendor who accesses a credit union's internal systems from the outside via SSL VPNs, Citrix®, Outlook® Web Access or portals is a particularly important security requirement. WholeSecurity specializes in protecting these endpoints, even non-corporate systems like home PCs, Internet kiosks, and public computers. This on-demand technology is seamlessly delivered by our Confidence Online product in just a few seconds via ActiveX® and Netscape® plug-ins. After this quick download, Confidence Online scans the endpoint machine to identify any malicious eavesdropping and remote control software on the system and then takes action based on the configuration set by the credit union's IT and Audit/Compliance departments.

WholeSecurity also offers always-on protection that runs as a Windows service on managed PCs in the LAN or connecting via IPSEC VPNs. Always-on protection prevents the propagation of worms, eavesdropping software and malware from inside the network. Confidence Online complements traditional AV software to form a proactive first line of defense that protects PCs from threats that AV software is not able to stop, such as new worms, targeted attacks, and a multitude of malware variants. By providing zero-hour defense against these threats, Confidence Online also helps the IT Department with their patch management efforts - they no longer have to operate in "fire truck mode" and can take the time to properly test and deploy their patches knowing that their PCs are safeguarded.

Financial institutions need to look beyond standard security systems, such as firewalls, IDS/IPS and anti-virus, and extend the security perimeter to their endpoint machines - both inside and outside their physical walls. WholeSecurity provides protection against today's most dangerous threats by augmenting traditional systems and adding a new layer of zero hour defense that can protect any computer, at anytime.



Michael Vien is Chief Information Security Scientist at WholeSecurity, an Austin-based software vendor that provides behavioral, on-demand security solutions to protect against malicious threats like worms, phishing, Trojan horses, keystroke loggers, and other eavesdropping programs. With over 13 years of experience in Information Technology, Michael Vien is considered one of the foremost security experts on malicious code in the United States, with ranking in the top five by several leading white hat security groups. Vien has consulted for over 35 government agencies, taught classes on security for Fortune 500 companies, and developed attack and penetration methodologies for global telecommunications corporations.

