

CU SECURITY: BEYOND THE MOAT - COMPREHENSIVE SECURITY STRATEGIES

The objective of a hardened perimeter is to delineate inside from outside and take complete control of what crosses the boundary. By controls, I mean configuring an effective system to enforce who can cross the perimeter, how they can cross it and what they can do when they cross. Once these controls are in place, the next step requires constant auditing and diligent maintenance to keep the perimeter secure, effective and efficient.

A defense in depth strategy inherently entails layers of controls, which in turn means every layer has a gap in coverage (or else you would not need multiple layers), therefore credit unions need to ensure that their layers fill gaps. A comprehensive approach would include: Firewalls, Network Intrusion Prevention, Email/Web/IM Gateway Virus/Spam/Spyware/URL Protection, Privacy Filters, Desktop Anti-virus, Desktop Intrusion Prevention, and Strong Authentication.

Credit unions are guided by regulations as the means for deciding how to protect themselves. This is because they have traditionally lacked the resources/expertise to determine what they need to do to mitigate risk. Unfortunately regulations are not created until the risk represents an already clear and present danger. This is true of vendors as well. Product vendors do not create security products until there is a clear and present danger (anti-virus came after the first virus, IPS came after hackers, anti-spam came after spam, etc.)

As an experienced security service company, we are a CU's security partner who helps them in being forward thinking and anticipating and mitigating threats. This responsibility includes having a research and development capability that can fill the gap between when the reactive product vendors have an answer and when an answer is needed - before there is significant risk.

SecureWorks receives on average 2,000,000 alerts/day on who, how and when credit unions are being attacked. This information is delivered to our research department in order to continuously improve our services to our thousands of FI clients. We use this valuable data to strengthen the multiple layers - Network based IPS, Host based IPS, Managed Firewall, Managed VPNs, and Vulnerability Assessments - that we provide.

These broad ranging services provide the four critical components of an effective security layering framework: technology, processes to manage the technology, people to enact the process and information to help the experts decide how to change the technology following the process. And even though we are the fastest-growing Internet security service in the world, we are not content to rest on our laurels. We are always looking to improve and expand our services, so we plan to launch new services 2005 such as Email Anti-virus anti-spam Gateway, Content Filtering and Managed Wireless.



Jon Ramsey is Director of Internet Security at SecureWorks in Atlanta, GA. Ramsey has 10 years of hands-on experience at every level: system administrator, software engineer, analyst, security penetration specialist and senior engineer. Prior to joining SecureWorks, Ramsey was a member of the Computer Emergency Response Team (CERT), and worked for Siemens International and the University of Pittsburgh. Ramsey earned a Master's degree in software engineering from Carnegie Mellon University and a BS in computer science from the University of Pittsburgh. He is a member of IEEE and the Association for Computing Machinery (ACM). SecureWorks is the credit union movement's leading provider of affordable Intrusion Prevention and security services.