

CU SECURITY - ESTABLISHING A PROACTIVE APPROACH

There are four separate pieces to the security puzzle: 1) policy development, 2) firewall and VPN (virtual private network) configuration and management, 3) risk assessment and penetration testing, 4) intrusion detection / prevention. Credit unions must take into account each piece and ensure that all of their bases are covered on the security front.

Security policy and employee manual development are critical first steps every credit union needs to take, that is why we send an experienced security/network engineer on-site to help the credit union with this process. Their infrastructure and physical environment are analyzed, as well as the way that they do business at their particular credit union. We then help them develop a custom tailored security manual that fits their network and operations while meeting and exceeding NCUA requirements.

Firewalls are the credit unions first line of defense, so it is absolutely essential to have them properly configured and maintained. We carefully scrutinize their firewalls and help the credit union tighten up their perimeter defenses. That may mean setting up three zones: external - DMZ (demilitarized zone) - and internal; or even more zones in some cases depending on the credit union's connections to the outside world. If the credit union is running a VPN, that is an area where we really focus on as well. That is because a VPN essentially punches a hole through the firewall, thereby creating an easy entryway for (worms, trojans, spyware, etc) via an unprotected remote user.

As for risk assessments and penetration testing, we perform thorough external and internal tests for credit unions of all sizes. Threats are characterized as High, Medium or Low and a report is generated that includes remediation steps. Internal assessments go through every device on the credit union's network looking for weaknesses. We often find machines needing service packs, spyware, file sharing tools, outdated router software and much more.

Finally, we are seeing a lot of interest in intrusion detection and prevention systems from our hundreds of credit union clients. Over the years, we have developed a finely tuned intrusion detection system that we use to monitor our customers' networks 24/7. This in-line IDS is a powerful tool for detecting and blocking unusual or malicious traffic trying to enter the credit union.

With over 10 years of experience working with credit unions installing and maintaining servers, routers and switches, ECCT is uniquely qualified to assist credit unions with securing their networks and systems. This hands-on experience with credit unions and their core processors, coupled with our certifications from Cisco, Microsoft and Citrix, gives our credit union partners from across the country a great deal of peace of mind.



Gerard Heege Jr. is President/CEO and founder of ECCT. Since 1992, ECCT has been providing the latest technological innovations to the credit union industry. ECCT's services have been tailored to accommodate the unique characteristics of credit unions and their data processing vendors. ECCT's clients include credit unions using processing vendors such as EDS, Summit, USERS, XP Systems, and many others. ECCT has developed business partnerships with credit union vendors and manufacturers to deliver premium consulting services in Network Security, Thin-Client technology, LAN servers, firewalls and routers. Mr. Heege leads a team of expert consultants implementing the latest in security and networking products & services.