

CU SECURITY: BEYOND THE MOAT - COMPREHENSIVE SECURITY STRATEGIES

Credit unions are under strict regulatory controls which too often forces them into reactionary mode instead of being able to take a proactive and strategic approach to security. Protecting the credit union's assets is not an 8 - 5 job, it requires 7 x 24 diligence. It also means moving away from isolated point products and implementing comprehensive defense-in-depth solutions.

With years of information security experience within the Financial Services Sector, we know that there is a gap between best practices for the management of firewalls and IDS devices in general, and what is deployed in the field. There are so many connections coming into and out of a typical credit union that is a challenge to design and deploy a security environment properly. We specialize in assisting IT departments design secure perimeter security networks that are properly configured, managed, and monitored on a 24x7x365 basis.

e-DMZ Security is also a strong proponent of network segmentation meaning the configuration of a set of firewalls designed to protect internal servers and the applications and data that they contain. Internal segmentation, when coupled with strong authentication, represent very effective security tools especially when combating blended threats that can originate from the inside of the credit union.

The biggest difference in our approach versus a typical Managed Security Service Provider is that we are a Co-Managed Security Service Provider. This is a significant point, not just semantics. We help the credit union's IT staff understand and manage their network by augmenting, supporting and training, while allowing the customer to retain as much administrative control as they choose. Knowledge transfer is a huge part of what we do and believe in. We augment their internal IT skill sets, and help them adjust and react appropriately to the ever-changing security landscape- we do not advocate handing over the keys to their castle.

Another area of security that we offer a unique solution in is the realm of shared privileged access: "root" for UNIX systems and "Administrator" for Windows systems. This is a complex and troubling problem that every organization faces. In order to manage this critical "super user" access, we developed the Password Auto Repository™ (PAR). This is a specifically designed and hardened appliance that addresses the storage, release, and update of administrative passwords. PAR ensures that individual accountability and an audit trail are preserved, and that passwords are changed periodically in accordance with the credit union's security policy.

Whether it is our ESMS+ program for smaller organizations that includes 24 x 7 firewall and IDS monitoring and management by e-DMZ personnel or our Enterprise offerings that include the Password Auto Repository and Vulnerability Management Services, we have a security solution that fits every credit union's requirements, regardless of size.



Kris Zupan is CEO/CTO of e-DMZ Security and a CISSP. A seasoned veteran in the field of distributed security, Kris Zupan built and managed one of the largest Firewall and UNIX Security deployments while in tenure with a Fortune 10 Financial Services Organization. The UNIX Security Model he established there earned laudatory comments from Regulatory Agencies. Zupan founded e-DMZ Security on his visionary concept of Co-Managed Security Services, building on his extensive experience in providing the highest level of security for practical, 'real-world' applications. He has presented on the topic of UNIX Security and is active on various product advisory boards for security companies.