CU t-t CREDIT UNION tech-talk
LEADERS FORUM
SPECIAL ROUNDTABLE SECTION
Technology News for Credit Unions Since 1988 www.cunews.com

Meeting the Challenges of Attacks, Breaches & Compliance

The number of successful, highly publicized data breaches in 2014 has grown tremendously. It seems just as we begin to forget one incident another major organization is breached. According to Ponemon Institute, the most costly data breaches were malicious attacks by criminals. U.S. companies experience the most expensive data breach incidents at approximately $246 per compromised record. All organizations must now, more than ever before, focus on the well established three pillars of security: people, process and technology. Organizations must implement continuous employee training, frequent process reviews and updates, and defense-in-depth with greater use of emerging security solutions.

Physical assets with sensitive information or sensitive data itself are most commonly targeted, and it is imperative to allocate appropriate budget to defend oneself or suffer serious and costly consequences. Of course, we are just barely seeing a return to a more flourishing economy so budgets are still tight, and difficult choices have to be made. It is hard to justify addition of net-new solutions that require employee training, and perhaps also changes to existing processes. But it is time. Even a cursory review of the recent data breaches reveals that most were sophisticated criminal attacks or malicious insider attacks, and many went undetected for far too long. The top three best practices are:

1. Identify and protect the highly valued, and sensitive data and IT systems. Encrypt all sensitive data, both in-transit and at-rest. By default, encrypt laptop disk drives as these are the most frequently lost or stolen physical asset.
2. Control who has access to these critical systems and minimize what each person can do. Leverage two-factor authentication for all administrative staff, and use unique account credentials for each system, rotating them regularly. Train employees, including contractors, on how best to protect these systems and establish and enforce consequences of non-compliance or security violations. Conduct impromptu checks and announce findings – sometimes peer pressure/ridicule is all that is needed.
3. The saying used to be 'trust but verify,' but organizations like Forrester now recommend a Zero Trust model for security. All access to IT systems must be recorded, and the logs must be centrally managed and protected. These logs must be automatically analyzed and alerts generated for anomalous behavior. Security staff must review these alerts daily and take investigative or preventative actions. Confirm that adequate controls are in-place and still being enforced. To state the obvious, early detection can prevent catastrophic disaster.

HyTrust delivers two solutions that can help credit unions prevent data breaches:

1. HyTrust CloudControl™ provides visibility and controls to mitigate insider threat and harden the virtualized infrastructure.
2. HyTrust DataControl™ provides encryption and key management for the virtual machines, securing data in private, hybrid and public cloud infrastructures.

With HyTrust CloudControl™ and HyTrust DataControl,™ a complete inventory of the virtualized environment is available, classified, and protected. The following controls are uniformly enforced and log records/reports are available for the auditors to examine:

- Authentication - Two-factor, and root-password vaulting
- Authorization - Attribute-based access control, and 2-Person Rule
- Auditing – Logging, real-time alerting & reporting
- Automation – Platform integrity and hardening
- VM encryption and key management

By securing the data itself, and adding strong controls for the administrators who manage these environments, HyTrust can help CUs mitigate the risk of accidental misconfiguration, malicious attacks and enable easier compliance with internal audits and regulations whilst lowering costs.

Hemma Prafullchandra
SVP and CTO

HYTRUST®
Cloud Under Control

Contact Info
www.hytrust.com
(650) 681-8100

Hemma Prafullchandra is responsible for the company's security and compliance product innovations and strategy. As an evangelist for what's possible, she drives the company and the eco-system (partners, industry & regulatory bodies, customers) to enable cost-effective, secure deployment of virtualization & cloud technologies. Hemma brings over 26 years of industry experience in the field of security. Her expertise includes Cloud, Virtualization, Solaris security, IPSec, Firewall, Certificate Authority/PKI, Java 2 Security Model, Secure Messaging, Web Services Security, Managed Security Services and Strong Authentication. Prior to HyTrust, Hemma has held senior management and technical positions at FuGen Solutions, VeriSign, Critical Path, Sun Microsystems, and the Wollongong Group. She has authored numerous patents, and is an active participant in many industry and standards bodies (IETF, OASIS, IEEE, PCI SSC Virtualization and Cloud SIGs, ODCA, Cloud Security Alliance, ISACA and NIST/NCCoE). Hemma is a frequent speaker and has presented at RSA US & Europe, VMworld, ISACA, HackerHalted, ISC2 and other industry events.