CU t-t CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Addressing Insider Threats, Cyber Attacks & Data Security

Unfortunately, data breaches are not a question of "if," but "when." As a result, there is no single technology solution a credit union can deploy that will guarantee 100% information security. Data breaches are in fact only increasing in frequency and sophistication. That said, there are a number of precautions an organization can take that will mitigate the risk of a data breach.

Here are four steps organizations can take to limit the risk of a data breach:

1. Manage "Shadow IT"
Dropbox is one of the most popular file sharing services in "shadow IT"—the products and services that employees adopt without IT approval. While these solutions are easy to use, they typically lack basic security controls and hackers have exploited these limitations. While you might be tempted to block employees from using Dropbox, they will only find another Shadow IT service to fill the void. A better solution is to allow employees to use Dropbox but with required security, auditing and controls. This way, IT organizations boost employee productivity without sacrificing IT security needs.

2. Equip systems with strong user authentication passwords
According to a 2015 Trustwave research report of 574 data breaches that took place across 15 countries, 28% of those breaches were the result of weak passwords. Despite common knowledge, passwords like "1234" or "qwerty" are still often used. A strong password that uses both upper and lowercase letters, symbols and numbers that are unique and not in use for other solutions or systems, can decrease the likelihood of a breach.

3. Take ownership of encryption keys
As you would never share your house key with a complete stranger, the same concept should be applied with encryption keys. However as long as encryption keys are maintained by public cloud service providers and their architects, personal data and information that is stored in a public cloud will be at risk. So rather than focusing on the strength of an encryption algorithm, a better question to ask is where are encryption keys held and managed. An alternative is a private cloud storage solution that guarantees ownership of encryption keys for maximum protection and control over stored data.

4. Ensure proper use-policies for dated applications
Apps that once thrived in large-scale app stores but are no longer supported present an easy way for hackers to exploit and implant malware. Organizations can help protect their personal information by encouraging staff to regularly update apps when newer versions are released or to delete them altogether when they're no longer supported by their developers. IT departments can also establish and enforce a mobile app whitelist to manage which apps are safe for employees to download and use.

Yorgen H. Edholm
President and CEO

Accellion

Yorgen H. Edholm
is President and CEO of Accellion which is an award winning private company that provides the leading mobile content platform that increases enterprise productivity and ensures data security and compliance. He is also a Silicon Valley veteran with 25 years of enterprise software expertise. Accellion, Inc. is the leading provider of private cloud solutions offering enterprise organizations secure access to enterprise content wherever it is stored to enable increased enterprise productivity and ensure data security and compliance for highly regulated industries like financial services, healthcare, government and legal.
With kiteworks, all enterprise content is owned and controlled by the customer and enables organizations to keep servers, storage, applications, metadata and authentication within the firewall and not co-mingled with a third party public cloud provider. Additional security features include file tracking and reporting, anti-virus, file/folder expiration, two-factor authentication, remote wipe, app whitelisting and much more.

Contact Info

www.accellion.com