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

Don't Let Your Security Program Live In A Bubble

Develop a Strategic, Integrated Plan that Strengthens Your Security Posture & Optimizes Costs

Unfortunately, there is no magic button that you can simply hit and "be safe and secure." Protecting your credit union from the "bad guys" is more than a technology issue – it must be a pervasive practice across your entire business and engrained in the culture of your organization.

The following concepts are good for business on their own, but when they are integrated into a cohesive strategic security plan and corresponding security framework, you will leverage and optimize the value of each, while eliminating redundant or wasted efforts. The more difficult and layered we can make our defenses and safeguards – vigilance across people, processes and technology – the less chance we will become a victim of malicious behavior. Effectively building an integrated security program doesn't have to be extraordinarily expensive if you take a strategic and integrated approach.

10 Ideas (and a few tips) to Integrate Protective Measures:

1. Multi-Factor Authentication (MFA): Having two-factor authentication in place securely verifies the external users who are coming into the organization through all sorts of devices. This is a requirement per current regulatory guidelines; and this is a simple and inexpensive solution that verifies all approved edge devices (entry points into your core networks) to let the employees who are trying to do their job in, and keep the bad guys out.

2. Network Segmentation: Simply add some intelligence to your network configuration and access points based on your employees, their profiles for access, their work hours and the relative geographies that your members are accessing your online banking from. Segment your wireless users based on members, employees, examiners and consultants. If your employees don't need access to Wi-Fi or systems after midnight to 6:00 am, then block any traffic during this time, which is typically when malicious behavior would occur. And if your members are all essentially on one continent, then maybe you don't need to allow traffic from certain countries at all.

TIP: When your auditors or consultants are working in your credit union, give them a temporary, expiring, wired or wireless access to just the areas they need, thereby demonstrating your preparedness and vigilance.

3. Monitoring, Alerting and Response, 24x7: The bad guys don't sleep when you do – they are working around the globe, around the clock and are just as dangerous (if not more so) while you are asleep than when your credit union is open for business. Unless you are planning to staff 24x7, your daily operations will need to have a team that is accountable for monitoring your entire network and systems, acknowledge alerts when something is triggered and can immediately escalate and respond accordingly at the time a possible incident is discovered.

TIP: This is not going to break the bank. You don't have to hire more people to monitor your network and systems, and you can restrict access of those monitoring to the dashboard and alert data. Your team can also benefit from the transparency and visibility of that dashboard too.

4. Data Protection: Data backup is a critical component of any security or disaster preparedness, but it is often the most common area where many organizations fail. Outdated technology, such as physical tapes or portable storage drives that are stored in an unsecure manner or even left on-site are bound to lead to problems. Create a copy of your daily incremental data and also a full weekly backup, then get it offsite and make it secure. An effective solution involves using replication software over a secure VPN tunnel that is encrypted to a secondary location that provides a long enough retention period to meet your needs for recovery of data at a specific point-in-time.

(Continued on Page 2)

Teresa Brent
Product Manager

alloya®
Corporate Federal Credit Union

OnX
Managed Services

Teresa Brent is a Product Manager at Alloya Corporate Federal Credit Union. Alloya exists to assist your credit union to perform at its best, so you can serve your members with excellence. Because the Corporate is itself a credit union, owners can be confident that their particular challenges are understood, and that their needs are met with appropriate solutions. Since launching in January 2012, Alloya Corporate's Information Technology Services, powered by OnX Managed Services, helps credit unions to design, implement and manage dependable IT infrastructures. Powered by state-of-the-art technology and available as an Alloya membership benefit, count on reliable, cost-effective IT infrastructures 24x7x365.

Contact Info

www.alloyacorp.org

5. Move core processing and member PII data to a more secure, certified provider. You are the subject matter experts at meeting the needs of your members, not managing the data center infrastructure used to power your core processing systems. If you are currently managing your own glass closet in the corner, then you are carrying the entire burden of risk and that includes all of your ever increasing audit requirements. When, in contrast, you could leverage all the physical and logical security, certifications, enterprise class technologies, ITIL processes and experienced 24x7 staff of the right hosting provider at a fraction of the cost of trying to do this on your own. Look for organizations that have credit union references and specialize with small-to-midsize financial institutions.

TIP: If a third party hosting provider allows and is consistently having regular auditor examination visits without red flags for other credit unions, then you can greatly lighten your IT compliance burden and lower your overall risk by moving PII to their hosted environment.

6. Get out of the data center business altogether: After you accomplish #5, and if you want to completely offload the accountability and responsibility of your audit and security, remove all data to offsite hosting. This means no local data on the edge devices or at credit union branches. All data is remotely stored, processed and securely accessed by authorized users – simply provide your auditors with your hosting provider's due diligence information and co-opt your partner's resources for the examination.

7. Remote or Virtual Desktop: Eliminate the possibility of data leakage and secure edge devices through properly enabling mobile and remote member services. Access all of your data through a remote virtual desktop that blocks remote enabling sessions and leverages a provider that does this as-a-service. So instead of watching for potential data leakage or exploitation – eliminate the ways it could occur and remove the data from your main and branch locations.

8. Build a program, not a one-time event: If you are paying for an annual one-time penetration test and relying on that as your burden of proof, then you are creating a false sense of security. Security is not a one-time event; it is a program that is built upon over time. Vulnerability assessment and penetration testing needs to be part of a larger picture that assesses all of your security exposures and includes social engineering to change employee behavior through ongoing education on security policies. It should also be used to frequently test the users and possibly some of your third party partners in their ability to rec-ognize social engineering vulnerabilities.

9. Security Incident Response Preparedness: Ensure you have current documentation on your environment ready to go. This will save you from having to describe your network configurations and where the most critical PII data lives after you suspect a breach has already occurred. Consider finding a qualified security forensics firm that will help you with your Security Incident Response Preparedness, tell you what you need, and take you through a mock-scenario to ensure you will be able to recognize and respond quickly when an event occurs. If you place them on a retainer, make sure they are committed to gather, document and maintain the response processes specific to your organization's IT environment. If you suspect malicious activity or a breech, they will be able to perform their forensic analysis and remediation much faster to ensure your return to normal operations.

TIP: Having a Security Incident Response retainer makes sense. A qualified forensics security firm that documents your environment, identifies a plan of action and commits to a time-frame for responding to potential threats when you suspect them does not need to be expensive.

10. The Holy Grail: Managed Security Services. Managed Security Services moves you from a reactive state to proactive state of visibility, detection and response. A truly "managed" security service should not just be sending alerts for your credit union's IT team to investigate; rather they should have a 24x7 staffed SOC (Security Operations Center) manned and ready to respond on your behalf.

Managed security services are not an insignificant investment and not everyone can afford it, but the bigger the size of your credit union the bigger the target you are, and the more you need to invest in protecting your members from malicious activity. Do you remember all those large companies breeched in the news? Those companies had expensive security alert logging and monitoring in place – what they didn't have was the staff or expertise to recognize it and respond to it while it was occurring.

TIP: Make sure any security monitoring and analysis tools are processing and identifying threats in real-time. Getting an alert on behavior happening 24 hours ago doesn't give you a chance at stopping it.

At Alloya Corporate FCU, we share the same regulations and expectations of having information protection and security as you – and with 1,600 credit union member-owners, our focus is solely on serving those in our industry. We offer consultation and recommended solutions through our IT Services that are practical to your risk and situation, and have been implemented with other credit unions with due diligence and oversight by us.

Teresa Brent
Product Manager

alloya® Corporate Federal Credit Union

OnX Managed Services

Teresa Brent is a Product Manager at Alloya Corporate Federal Credit Union. Alloya exists to assist your credit union to perform at its best, so you can serve your members with excellence. Because the Corporate is itself a credit union, owners can be confident that their particular challenges are understood, and that their needs are met with appropriate solutions. Since launching in January 2012, Alloya Corporate's Information Technology Services, powered by OnX Managed Services, helps credit unions to design, implement and manage dependable IT infrastructures. Powered by state-of-the-art technology and available as an Alloya membership benefit, count on reliable, cost-effective IT infrastructures 24x7x365.

Contact Info

www.alloyacorp.org