CREDIT UNION tech-talk
LEADER'S FORUM
SPECIAL ROUNDTABLE SECTION
TECHNOLOGY NEWS FOR CREDIT UNIONS SINCE 1988
WWW.CUNEWS.COM

Addressing the Big 3: Compliance, Fraud & Cyber Security

How credit unions can best prioritize spending in regards to compliance, fraud and cyber security is probably the most important question facing every organization in the financial services market today. While all three of these areas are vitally important, our perspective is that the best strategy to address all three requirements is to first build an effective cyber-security architecture. That is where protection starts, and if you can get that right, it will inherently provide the added benefits of significantly reducing the risk of fraud while also helping organizations meet their compliance requirements.

But we all know that building an effective cyber security architecture is much easier said than done. The continuous evolution of malware, advanced persistent threats, and other types of cyber attacks has put every organization on the defensive, and created intense pressure on IT organizations to quickly discover, diagnose, and solve the problem. This is hard enough to do in a Fortune 500 company where you typically have very large, dedicated IT security teams. But the same attacks are also targeting credit unions where the entire IT team might consist of only a couple of people. It is unreasonable to think they have the time or resources to respond effectively to every possible cyber attack.

So how can a credit unions develop and implement an effective cyber security architecture? I would suggest, and in fact what I believe is absolutely essential, is to change our mindset about how to approach the challenge of cyber security. If you look at what's happening in most financial services organizations – even large global banks – they typically focus on a "defense-in-depth" strategy, where they rely on multiple security tools and technologies, each providing an additional layer of defense and protection in the event of a cyber attack. The general idea is that, if the threat penetrates one layer, it will hopefully be stopped by the next layer.

Unfortunately, there are two problems with this strategy. The first problem is obvious – the strategy doesn't work, which is why we continue to see very large organizations become victims of cyber attacks. The second problem is the fatal flaw in all of these defense-in-depth strategies. They are, by design, focused on reactive protection. By that I mean they are like the defensive line of a football team, trying to keep the opponent out of the end zone when they are on the 1-yard line. By the time your opponent is at the 1-yard line, prospects for success are grim despite your best efforts to provide reactive protection. Good luck with that.

I believe that a better response starts with a fundamental change in thinking. Rather than focusing on reactive protection, we need to focus on proactive prevention. In other words, rather than treating the symptom of the problem, focus on fixing the root cause of the problem.

Here's a specific example. We know that more than 90% of all malware attacks that infect end user devices enter the system through the web browser. Historically, we have tried to solve this problem by installing various endpoint security, AV, and detection technologies to the network gateway and/or on each endpoint device in an effort to discover and stop threats. But this is the reactive protection approach, and it doesn't work.

In this scenario, the best solution is to shift the focus from reactive protection to proactive prevention. And to accomplish that, you really need to transform the browser itself, from a malware delivery tool to a first line of security defense that effectively stops all browser malware from infecting endpoints. That might sound like fantasy, but the good news is that Spikes Security's innovative AirGap security solution is delivering this proactive prevention right now. It is being deployed in many large enterprise organizations, but it is also an affordable, effective solution for smaller credit unions as well.

Branden Spikes
CEO, CTO and Founder

SECURITY SPIKES™

Branden Spikes is the CEO, CTO, and Founder of Spikes Security, a Silicon Valley startup focused on preventing browser-borne malware from penetrating enterprise networks. Previously, Branden worked alongside Elon Musk for 15+ years at PayPal, SpaceX, where he was responsible for designing and implementing advanced IT systems. He also helped architect the software that provides security for Tesla electric cars. Branden's unmatched experiencing in building secure, high performance IT systems gives him a unique perspective and advantage as the CEO and visionary of Spikes Security.

Contact Info

www.spikes.com