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

Online, Mobile, Network & Physical - Securing the Spectrum

These aspects of security - online, mobile, network and physical - are completely different from each other and each of them requires very specific attention. Where physical security is concerned, my comment would be that, "everyone seems to understand this is a highly specialized area which requires dedicated and specialized personnel, and no one hires a security guard on staff anymore, we all subcontract them from specialized companies; so why not make the same considerations when it comes to cyber security?".

When we look at online security for credit unions we need to think of their members; these are usually the most vulnerable because many of them are usually completely outside of the tech world, they are end users.

They have no idea of the dangers they can run into; they simply want to make a financial transaction without walking into a credit union, from their own computer, and often do not realize that, without proper protections, someone could be snooping into their keyboard to steal their credentials, which, of course, could lead to disastrous consequences. Yes, federal law protects the consumer, but there have already been cases wherein the financial institution has won because it was able to demonstrate complete negligence on the part of the consumer. That said, these are exceptions because for the most part, the law protects the consumer and the credit union is truly the entity at risk here.

So the question is ~ how can the credit union protect itself where this issue is concerned?

Red flags have been in use for a while now and though they are not yet completely ironed out, they do help quite a lot - spotting unusual transactions and blocking them before they cause damage is a great starting point. But some credit unions are going further, by providing a free license for anti-theft software to their members. In this situation, the member installs it as a plug in, and this software watches on the username and password for their account. If that information is trying to go "somewhere else" because the browser page has been hijacked or spoofed, it will immediately block the transaction and raise an alert.

In fact, I would go all the way to propose that making use of such software be mandatory, i.e., Mr. Member, you either install this software and USE it, or you cannot bank online! Actually, I would also add here that the credit union should ensure end users take proper care in securing their own devices as well. Too many end users do not use properly updated AV on their computers. And as those computers are often infected with multiple threats, when used to connect to the credit union, the likelihood of a leak of information is far too high a risk for the credit union to accept lightly.

Mobile security can be separated into 3 segments: end users banking online from their smart phones or tablets; credit union employees accessing applications and/or information via a mobile device; and BYOD. Each of these topics would deserve a white paper of its own. End users and smart phones - I would treat them just as explained above; the credit union needs to have some form of assurance that nothing can hijack that conversation or steal

Pierluigi Stella
Chief Technology Officer

NETWORK BOX
Managed Security Services

Pierluigi Stella co-founded Network Box USA (the American division of Network Box Corporation Ltd) in 2003, after 15 years with IBM. In his capacity as CTO, he has acquired extensive knowledge of security issues with emphases on the financial; banking; hospitality and travel; healthcare; and education sectors. Stella has authored articles for such reputable publications as Communications News; PC Today; CU Times; Processor; and Tech Port. He is a frequent Featured Expert Contributor on CUinsight.com and has also been profiled in the Houston Business Journal as well as Houston Public Radio. A regular sight at premiere trade shows and industry conferences, he has presented, among others, at the ISACA/IAOP 2011 Risk Management & Data Security World Conference in Denver. In 2008, Stella was a contributor to the ENISA's "Cloud Computing Risk Assessment" project which analyzed data protection and data security issues. He holds a Master's Degree (Magna Cum Laude) in Electrical Engineering from the University of Naples, Polytechnic School of Engineering in Naples, Italy. He has received many industry recognitions for notable career achievements in addition to being the recipient of excellence awards for innovative design.

Contact Info

www.networkboxusa.com

Online, Mobile, Network & Physical - Securing the Spectrum

those credentials. Mobile employees using company issued devices - there are plenty of apps that attempt to protect these devices; the relevant data should be encrypted - some apps encrypt everything, some only the important data; either way, encrypting is important because the device can be lost or stolen.

Passwords - they need to be strong; I am not a fan of changing them frequently; but they need to be long and strong. I advocate adopting bio devices if they are available (I am surprised I have yet to see an app that will lock my iPhone unless I stick my thumb on it). There are also AV apps and other forms of protection available; all should be adopted as security. In truth, it is never "enough". Finally, BYOD - at a minimum - have a policy, a properly set policy giving the credit union the right to wipe the device if it is lost, that ensures the device is treated like a corporate issued device, with proper security and proper attention. If this is unacceptable, don't allow BYOD. Whatever you do, do not just ignore the issue - not having a proper policy is the equivalent of having a completely open policy. Do write one, and use it.

Network security is a separate issue; no credit union has enough resources and personnel to do this properly in house. I am absolutely convinced that this should always be outsourced. I do this for a living, I see and know what it takes to do this properly; I see no way that a small private company whose business is NOT security could ever do this properly. Even if you do attract one single, smart, security professional … how long do you think that they will stay on board before a managed security services company makes them a better offer? And what prospects of carrier does he/she have? And how much will he/she cost you? In the end, what can the poor person do when the only visibility he/she has is that of your Internet connection? There is a whole world out there, and it is a dangerous one. Looking at that single bomb about to hit you is not the right way to ensure your security; you want to know what is going on around the world, before any threat comes even remotely close to your doorstep; and this can only be done by a MSSP with good global reach.

Outsourcing is the only way that credit unions can effectively prioritize securing these four channels. I have outlined that Network Box USA is a managed security services company and the reasons why this aspect of security should be completely outsourced. What I would like to stress is that managed security is not just a person behind a screen watching over your firewall and making some configuration changes here and there. Network Box has 3 ISO security certifications; it runs a security response center where our people watch the entire Internet 24/7/365 and create signatures to protect our customers in real time. Currently we produce over 75,000 signatures per week, and push them out to our boxes about 300 times a day. Real time protection is fundamental because of the speed of the Internet, and how rapidly new threats are released, to the tune of about 500,000 new threats per day. A small MSSP with one NOC and no security response is not the answer to this aspect of your security; you want a global corporation that is truly aware of what is going on with the Internet, hours, if not days, before the danger shows up anywhere near you.

Pierluigi Stella
Chief Technology Officer

NETWORK BOX
Managed Security Services

Pierluigi Stella co-founded Network Box USA (the American division of Network Box Corporation Ltd) in 2003, after 15 years with IBM. In his capacity as CTO, he has acquired extensive knowledge of security issues with emphases on the financial; banking; hospitality and travel; healthcare; and education sectors. Stella has authored articles for such reputable publications as Communications News; PC Today; CU Times; Processor; and Tech Port. He is a frequent Featured Expert Contributor on CUinsight.com and has also been profiled in the Houston Business Journal as well as Houston Public Radio. A regular sight at premiere trade shows and industry conferences, he has presented, among others, at the ISACA/IAOP 2011 Risk Management & Data Security World Conference in Denver. In 2008, Stella was a contributor to the ENISA's "Cloud Computing Risk Assessment" project which analyzed data protection and data security issues. He holds a Master's Degree (Magna Cum Laude) in Electrical Engineering from the University of Naples, Polytechnic School of Engineering in Naples, Italy. He has received many industry recognitions for notable career achievements in addition to being the recipient of excellence awards for innovative design.

Contact Info

www.networkboxusa.com