Battling Security Fatigue – Working Towards Usable Security

NIST recently conducted a study on security fatigue (http://bit.ly/2dYJFLC), which also published by IEEE (http://bit.ly/2dxLpJj).

Conducted by cognitive psychologists, this study unearthed a sense of resignation and loss of control, an air of fatalism, unavoidability, all of which lead to avoiding even making a decision (why bother if it's all useless!), as well as a tendency to almost intentionally underestimate the risk (the mindset being "if I can't see it, it's not there"). Users become reluctant to deal with the situation. I'm not a psychologist, of course, so I shan't pretend to attempt explaining why people behave this way, but the fact is, they do. And this can lead to disastrous consequences.

We all bank online, shop online, deal with our health issues online. If we become disenchanted and jaded, we'll stop what already little care we put into these activities, and hackers will have an even easier time attacking all of us. If I leave my house door unlocked because, in my mind, a skilled thief can easily open it anyway, guess what? The dumbest of thieves can now walk in and steal whatever they want!

One vital point cited by a user in the study said, "We used to have 1 password to keep up with at work; now we're being asked to remember 25 or 30 passwords" (edited). Let's think about that for a second. Personally, I have no idea how many passwords I have out there. I can't even begin to count them. And according to best practices, (and because I'm a security professional), I "try" to make each one different, and change it as often as necessary. How many users outside of our industry (and let's face it, within our industry as well) are actually doing that?

This situation has its equivalent in the work environment, of course. We're all human and we bring to work, our habits, and our frustrations. Only to have someone else add on to them because now we work in a FI, and we're more of a target than we were at home! Now, it isn't wrong telling users that your FI is a target. By all means, awareness is half the battle won. Should users cease clicking, you'll stop getting ransomware and other nasty stuff. After all, they're the most vulnerable layer in your defense-in-depth. But to what extent can you really stress your users before you wind up with a result the complete opposite of what you desire?

I'm not sure I have the answer, let alone a solution. However, I firmly believe we need to lay off a little and, as we continue to train our users, it's equally vital for us to realize we can't continue to scare them until they're nauseated by the very topic of security. Security is OUR concern, not theirs. WE need to do our job, and keep them safe despite themselves!

The questions for this roundtable ask how our solution can assist a FI in identifying the appropriate security actions. This question isn't quite in line with the previous two, wherein we're asked about security fatigue. No product or service or solution can help with that situation because it's an human issue, and thus it should be dealt with.

Network Box can help the IT professional with the knowledge that your perimeter is being vigilantly and proactively guarded, that someone (a large and capable team) is watching relentlessly every second of every day, and that at least that specific part of your job is taken care of. You can then fully focus on other aspects of your security issues. Network Box also provides you with tools to see what's going on, day by day, hour by hour. And when dealing with security fatigue, it can certainly be immensely useful to have instant reports on hand, which you can use for a (nice) conversation with a colleague whose actions are possibly endangering the security of your network and data.

Pierluigi Stella
Chief Technology Officer

NETWORK BOX
Managed Security Services

Contact Info

www.networkboxusa.com

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.