The InfoSec Conundrum. Keep Playing Until You Lose.

Don MacVittie, 2011-13-05

Lori and I received the new Blackberry Smart Phones that F5 ordered for us last week, and have spent about a week familiarizing ourselves with all that has changed since our several-year-old ones came out. There is certainly a lot of change. The Social Media add-ons bundled into these phones are certainly much nicer than the ones we had installed on our older phones, texting has its own app rather than being a part of the email package, the screen is more crisp, and photo quality is light-years ahead of previous incarnations, but still doesn't compete with high-end digital cameras. Oh yeah, and it takes calls too.

One little bundled application was Word Mole, a game where you try to pick words out of a six by six array of letters. You can use any letters, the words have to be in their dictionary, and the larger the word, the more points. And the less common the letters the more points you are awarded. The game is surprisingly (for me) addicting, and takes very little time to play – each level is timed to two minutes, so you can complete a level in two minutes or less. And since you get extra points for any time left on the clock, most levels take less than half a minute.

An interesting implementation choice in this game is that you "win" by "losing later" than your last time. There is no finale to the game, you just keep going through levels (with occasional breaks to do a little something else that is speed based) until you don't get enough points before the timer runs out. Since the timer is set to two minutes, and the required number of points goes up with each completed level, it is pretty much inevitable that you're going to lose. The only question is how far you will get before you fail.

Word Mole Menu, Compliments of Crackberry.com

And that got me to thinking about how we deal with information security, even today. It is not generally considered ***if*** you will get compromised, we approach InfoSec like you ***will*** fail, the only questions are "when?" and "did you do enough to try and stop it?"

That just is not a viable way to run a business over the long-term. Particularly not with the sanctions and pressures governments are putting on ***the victims*** of hackers. Organizations are under increasing pressure as if they were the culprit, whilst the ne-er-do-wells are sometimes apprehended, sometimes not, sometimes hiding away in countries that will not pursue them. Disclosure laws are good, you should warn people if their identity has been compromised, but looking to see if an organization is "culpable"? Even if a company was stupid enough to have zero information security in place, that is akin to a company failing to lock its front door and being robbed… While stupid, and an insurer may have an issue with it, the authorities certainly wouldn't blame the company for having forgotten to lock their door (though a lenient judge may give the robber a lighter sentence for it). They didn't ask to be robbed.

And yet we are still running on "do all you can to protect…" where "protect" has the known double meaning of "customer data from hackers" and "the organization from exposure if a hacker gets in".

Eventually, your organization will fail. "Guaranteed failure with minimized risk" is not the answer, and it leaves us in a untenable position, both as organizations and as customers of said organizations.

So I've pointed out the obvious, next you want to know my answers. I wish I had them. We here at F5 have some great products to support you and lend better protections, but the problem is much more comprehensive than that. It requires international relations, standards on when you've crossed the line from innocent poking around to outright lawbreaking, and governments the world over to track down and prosecute the evildoers. For some reason we (the world in general) are much more accepting of criminals that steal from a keyboard than those who steal with a brick through a window, and it is far past time when that must end. But ending it will not be easy or quick.

I'd start by forging solid international agreements on what constitutes violation of an organization's presence on the Internet. Certainly attempting to connect to one port is not a violation, but if that connection includes a malicious script or the attempt is to connect to a thousand different ports, it is a different story all together. From there, punishment guidelines must be agreed upon, and enforcement… Enforced. There is very little in this world that I truly believe needs international cooperation on a grand scale, but the Internet is anywhere, and ingress/egress points in different countries is not only common, it is largely the norm in some parts of the world, so any attempt at Internet regulation must involve a massive scale of national cooperation, making it a tough problem.

Still, it is a worthy effort. There are enforcement techniques available to force international cooperation, assuming the other parts mentioned above are taken care of. Cutting off rogue countries that harbor Internet lawbreakers is entirely possible on an international scale, as are several other enforcement tools.

Let's stop treating InfoSec like a game of Word Mole. Because when you lose in InfoSec, someone generally gets fired, even if everything was done right, and that impacts people in a very real way. That doesn't even touch upon the type of harsh treatment the corporations that are compromised suffer at the hands of press, bloggers, and governments, and the impact that has on the overall organization.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com