All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Stupid security getting stupider still - and falling into denial

I am amazed at the fact that stupider is not caught by my spelling checker. Is it a real word? This morning I was typing on my cell phone and put in the word lunch (or I thought I did) and it came out Lynch! Taking someone out to lynch is really bad compared to lunch – depending on who they are they might be a tad offended. Just saying...

What is "security" all about?

I heard two angel pitches in the last day or so and had one form or another of my secure cyber question (I am the lead for "secure cyber" in the group). I gave a hint to one of them at the start of my question indicating that the phrase "block chain" in response would constitute a wrong answer. I started the other question by pointing out that the big company they were planning to partner with had lots of published vulnerabilities in its cyber-systems and more coming out quite often. In each case, the response I got back indicated deer in the headlights level understanding of the issues. In one case they indicated that they were going to depend on me to evaluate it for them – and I pointed out privately afterwards that invoking my name has a nasty way of getting people to call me, and since I didn't know what they actually did yet, there was every chance the result could come out undesirable.

Of course we don't know what we will find until we look. But Jon David, who I haven't heard form in a long time, one told me (correctly) that (approximately) "If you don't know, you are not secure". His theory was that, even if by some rare trick of fate you were secure at some point in time, by the next day you would no longer be, unless you knew and could show you were.

But my question runs a bit deeper. I keep hearing the term "security" and "secure". For those who have read my previous articles on the subject, you know that few even understand a definition for the term they are using. Of course if you don't know what you are aiming at, you are unlikely to hit the target.

Denial

Which brings me to an apparently fundamental misunderstanding of "security" today. While denying the need for security is bad, even worse is security that ends up denying legitimate services. And that appears to be the approach of the day. Potential problem detected? Deny services until resolved. Stupid! Stop it!

Availability of authorized services is a fundamental security requirement.

If you are denying legitimate services, the harm may be, and often is, higher than granting unauthorized access. Costing me time will cost you my business. Costing enough of your customers enough time will put you out of business.

Find a better way

Warning: If you are a CISO or otherwise in charge of protection, you need to find a better way than denying services to legitimate users. As a start, find a way to assess the tradeoffs between availability and whatever else you are trying to achieve.

