AGS Encryptions Ltd.

‘Target’: Missing Abstraction

As long as we lack a cyber security theory, “Target”, “Heartland”, and worse will keep coming

Bridges kept falling until Newton formulated his mechanics: the underlying principles that keep high rises standing, ships sailing, and rockets flying. None of these could have happened without Newton’s abstraction of the myriad of observations regarding the dynamics of material things. Maxwell did the same to give us television, radio, cell phone and everything electronic. ***And what is needed -- urgently -- is a “Cyber Newton”, a “Security-Maxwell”: a sound and effective theoretical foundation for the challenge of security in cyber space.***

Patch work, our present strategy, is woefully inadequate. All those extensive malware logs never stop the next flavor. There are several thousands distinct credible attack pathways pointing into the heart of every, so called, secure system. It is theoretically impossible for the security team to identify each and every such attack pathway. The hackers, on their part, have all those multitude of attack options available to them, and all they have to do is to spot one attack scenario that was missed by the security team. One is enough! I have not personally analyzed the Target situation but reportedly that is what happened. I have done some work on the Heartland breach, and there, I know, that it was a case of the hackers spotting a way to compromise the system, a way which the security team missed, as they missed many other attack scenarios, as anyone else would have missed so many effective ways to inflicting data-harm.

Tactics, Specificity, and patching holes after the fact, do not work. Imagine that we would have built bridges by simply not repeating a design of a bridge that fell in the past. The more bridges we would have spun, the more would have fallen, and we would have logged an ever longer list of ‘what not to do’ which is of little help. Luckily our design is guided by the first principles formulated by Newton.

Similarly in security, huge logs of known signatures of bad code, and long lists of lessons as to ‘what not to do’ is the wrong, wrong strategy.

Another analogy: every chess player looking at a board, will quickly appraise whose position is stronger. Have they identified all possible game sequences? No, even IBM Deep Blue can't do that. The strength of a position of a chess board is *abstracted* from the details. Grand masters abstract better than the rest of us.

And that is what we need for cyber security: first principles to abstract the threat. Everything that we do in security is driven and justified by the threat. The less we understand the threat, the weaker our defense. Most security consultants rush to build walls, deploy intrusion detectors, set up burdensome identity verifiers, but they rarely stop to seriously analyze the threat, estimate, appraise, quantify it. And that is because we don't have the tools, we don't have a cyber security theory.

It is beyond 'Target', it is further than payment; as we move in to our new world, the cyber world, the need for sound security is growing. It is our civil order that we are talking about here; it is our national defense that is in play. We mouth a lot about the asymmetric war, where we have a disproportionate vulnerability amplified by our total lack of theory.

Here and there someone is raising this issue, mostly in pure academic terms, it is not enough, it is pathetic really, in light of our growing vulnerability. It starts with leadership. Reading Einstein's letter on the threat of unprecedented proportions, President Roosevelt, handed Einstein's warning of the Atomic bomb over to his secretary of War stating clearly: "This Needs Action!"

We need a Presidential level summon of a Cyber-Oppenheimer, charging him with putting together a Cyber-Manhattan Project, and turning the table on the barbarians at our cyber gates.

Any delay will be judged by history as dereliction of duty.

*Prof. Gideon Samid, PhD, PE, Chief Technology Officer, AGS Encryptions Ltd * gidoen@AGSgo.com*
AGSgo.com is doing its share with it AbstracThreat^{TM} service.