Thinking Like the Bad Actors and Prioritizing Security

Assume you've been breached. Period.

The reason that I start there is because I've learned from practice, that we have to work on the assumption that we have had our systems violated in one way or another. The reason that this is important is that we have to start with a mindset to both discover the violation, and prevent it in future.

Who is it that has breached our systems? Well, we have a fun name for them…

Bad Actors

Hey, I like Kirk too, but you have to admit…he's not really a good actor

No, not the kind that you see in SyFy remakes of popular movies, but the ones that have been infiltrating your infrastructure for nefarious purposes. Bad actors are those who have the single-minded purpose of breaching your security, and doing something either inside the environment, or taking something back out.

All too often we hear about breaches long after they have happened. I'm a big fan of Troy Hunt's web site Have I Been Pwned? It's a helpful resource, and a reminder of just how important it is that we understand that bad actors exist and are pervasive in the world of internet connected resources.

Bad actors love the internet of things. Just imagine how much simpler it is to access resources when they are interconnected and internet accessible. Physical security is the first place to look, and all the way up the stack to the application layers. Using your mobile to access your bank site when you're in Starbucks? Not a good idea. Seem paranoid to say that? That's what every bad actor hopes you say.

Assume security is failed. Assume you've been breached. The next step comes with how you plan and prepare to discover and recover.

White Hat (aka Ethical) Hacking

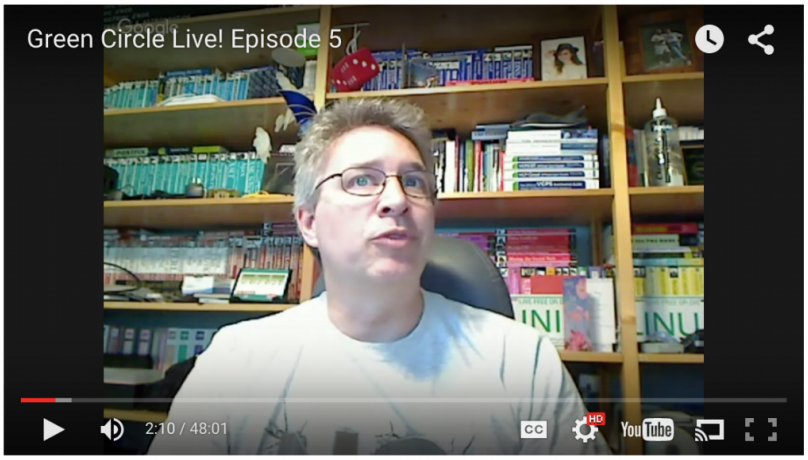
Just under a year ago, I attended the BSides Delaware event. This was a very interesting opportunity to go outside of the normal conference circuit that I am used to attending. I would liken this to the VMUG equivalent where DefCon is the VMworld of security. These are great events, and touch on every aspect of security from application, to network, to physical, and even security of yourself including self-defense tactics.

One thing that you learn about hacking, is that it takes a hacker to find and prevent a hacker. White Hat hacking has been a practice for many years, and it is an important part of the security and networking ecosystem. If you aren't already engaging an organization to help with penetration testing or some form of security analysis, you absolutely should.

The same skills that drive the bad actors have been embraced by white hat hackers to provide a positive result from that experience. We use real users to provide UX guidance, so it only makes sense that we should use the same methodology for our security strategy.

Make Security Part of Infrastructure Lifecycle

Whether it's your application lifecycle, or your infrastructure deployment, security and automated testing should very definitely be a part of the workflow. I was lucky to have a great conversation on my Green Circle Live! podcast recently with Edward Haletky.



We chatted about how there is a fundamental flaw in both the home and the data center. The whole podcast is a must listen if you ask me, and I encourage folks to rethink security as something that should be top of mind, not an after thought.

There are lots of bad actors out there. I prefer to keep them in the movies and out of my data, how about you?