Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

The attacker only has to be right once - another information protection fallacy

In one day at one conference, I heard this myth twice before I spoke up. I have heard it time and again, and enough is enough. It's an offshoot of the old fear, uncertainty, and doubt approach to drive up the level of fear and make your message of resolution all the more acceptable. But false premises lead to bad decisions.

Let's suppose we did the same thing with physical crime

Where can we find an analogy... 9/11? Nope - they were wrong again and again - they just kept on trying and the defenders didn't stop them, and the result is a war that is killing most of the people they worked with and destroying many of the things they were trying to protect. The Christmas bomber? Nope - he was reported on and detected in several ways - wrong again and again and the defenders just didn't stop him, and he is now in jail and reporting on those who were behind it. The as yet unidentified assassins caught on surveillance videos in Dubai? Nope - caught on tape - and now being hunted by the world - now they have to be right again and again or end up in jail or dead.

Lots of people get away with crimes, and lots of people get caught. The bad guys don't have to be right only once. They have to be right again and again, and that's why so many of them get caught. But of course a lot of them also get away with it. But it's not because the bad guys get it right - it's because the good guys don't catch the bad guys when they get it wrong.

They cyber world - only right once?

Suppose the claimants are right. They assert that an information-based attacker actually only has to be right one time. What does that mean?

- Of course it must be their first time, because otherwise, they would have to have been right again and again. Or perhaps they were wrong again and again, had lots of chances to get caught, and weren't. Or were they caught and released?
- They defeated all of the protection in place, all at once. Instead of running through the maze of protective measures, they make one lucky or highly skilled guess and win it all (whatever that "all" is). There are lots of enterprises with poor protection that can be defeated by a single step, but as a rule, that's not what happens. In most cases, you have to do at least two or three things right to get past protection without being caught.
- They win everything they ever will in one shot, and walk away fat, dumb, and happy. That's because, if they have to try again, they are no longer just getting it right once.
- They get away completely clean, with no apparent magical change in anything that will be noticed relative to criminal acts - which means either that they were rich before, poor afterwards, or somehow managed to conceal their tremendous success over the remainder of their lives. Of course not all attackers want to steal money.
- The target they are going after must have either no redundant security measures, no

layered defenses, and incredibly obvious ways for unauthorized parties to directly gain access to do whatever the attacker wanted to achieve - or the attacker is an insider with so much access that they can get whatever it is without a problem - but also not be suspected of whatever it was.

Now, to me, there are two possibilities here.

1. The defenders are completely inept. Maybe an employee about to be fired just wanted to disrupt a company for a few minutes, and cut the power at the main switch panel, and there was no uninterruptible power in place, no physical security, no procedure for employees being terminated, I guess they only had to be right once. But how much did the defenders actually lose from this?
2. The defenders are doing a reasonably good job and there is no such person. After all, that is some kind of a brilliant scam - one step gains all that is ever needed for a lifetime. Done right the first time with no practice rounds, it must also be a very gutsy individual. And the planning and foresight for someone with no relevant experience seems to imply an astonishing level of intellect. And... my point is...

There is no such person!

That's why it's a fallacy!

Yes - that's right - it's a fallacy! No such person exists. To be a successful attacker you need to get it right again and again and again. And that means you need to practice, develop skills, and make the mistakes that all people make when learning. Then, after you get very skilled, you can get it right again and again, and perhaps succeed in something substantial.

- Attackers don't get it right all the time. In fact, they generally try lots and lots of things that don't work before doing something that does work.
- In practice, attackers almost never defeat all of the protection is in place all at once.
- In practice, few thefts are big enough to allow anybody to live well for long from them.
- In practice, individuals get caught later when they brag about exploits, resell something stolen, get turned in by an ex-partner or competitor, or use the ill-gotten gains.
- Some targets are very weak, have no redundant (or primary) protection, and incredibly obvious ways for unauthorized parties to gain unlimited access. And the vast majority of losses still apparently involve insiders. And lots of insiders get detected and caught.

Why then do they succeed so often?

The problem is not that attackers only have to be right once. The problem is that, after getting away with things again and again, after betting caught and released, after being fired but allowed to keep the money, after getting detected millions of times, they are still free to keep attacking. And eventually, they do succeed. That's the problem.

It's not that they only have to be right once.

It's that they get to be wrong so many times and get to keep on trying!