Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Default deny is best practice? Not anymore!

I always rally against the folks who claim that they are using "Best Practices" in security, because I believe that protection is something you do, not something you buy, and as a result, you need to do the things that make sense for your environment, not buy into a concept that is nebulous at best and reckless in most cases. Hence I will be taking a shot across the bow of those who assert that "default deny" is the "right" way to do security.

My position in this regard actually stems from one of the oldest questions we hear is philosophical and defies solution: "Which came first, the chicken or the egg?" and the almost identical question, "If a tree falls in a forest and nobody is there to hear it, does it make a sound?". The reason these are really the same question is the same reason that default deny being the best security approach is the same question. They are all questions of definition, and the question itself is a misdirection to prevent the decision-maker from seeing the issue at hand.

- The chicken and the egg: If you mean by "egg", "something produced by a chicken", then the chicken came first. If you mean by "chicken", "something produced by a chicken egg", then the egg came first. Or as I like to answer "The egg - because there were eggs long before there were chickens. See 'dinosaur' for further details".
- The tree making a sound: If you mean by "sound", "something a person hears", then the answer is "no". If you mean by a "sound", "waveforms in the air", then the answer is "yes".
- Default deny as a best practice: If you mean by "best" that there are none better, it's not best practice. If you mean by "best" that you can claim you are doing the right thing when you don't know what the right thing is, then it may indeed be "best practice" - as in the "best practice" you could come up with given that you don't know enough to do better.

I can hear the crowds of security folks shaking their heads, blinking feverishly, and grunting that I'm an idiot and doing more harm than I will ever know. After all, if the simple "default deny" phrase can't be used with the ludicrous "best practice" phrase, how will we ever be able to explain to our users and executives why they should stop doing stupid harmful things? I have, in the minds of many, just given gobs of people the excuse they needed to not do the right thing! Life's tough.

Reality steps in every once in a while and stops the security folks from preventing the user folks from removing the barriers to productivity. Default deny is a barrier to productivity, and that's the simple truth. If a security person wants to know why they can never get the users to go along with the security program without Draconian methods, this is why: The users have work to do and you are stopping them from doing it.

To a user, default deny means that I need permission from you to do my work. And as far as I am concerned, you need permission from my boss to tell me not to do my work. So if you try to stop me, I will find a way around you so I can do my work. That's why port 80 now tunnels everything from telnet sessions to music downloads, and why when you block it in http, they will use https. Because they want the music on their desk and you can't stop them. If you try, they will turn on their cell phone with its unlimited minutes and connect it to your computer with a USB, Bluetooth, IEEE, or Ethernet splitter interface - whatever it takes - and they will play their music as they work. And if you don't support it, they will bypass it and instead of having security, you will have the fiction of security. And if you try to do the right thing and get them fired for breaking the rules, you will be fired for making the other workers unhappy.

So why is default deny a failed policy? Because, by default, you are preventing me from adapting to the world around me. Because when I am trying to get something productive done, you are stopping me. Because safety and security are not the most important things in the life of an enterprise. Taking rational risks for benefits is what enterprises do. Get with the program, or the program will crush you.

But isn't it impossible to keep the enterprise under control when you have to always chase the bad guys instead of being ahead of them? It's not impossible, once you understand that being in control is not controlling everything. The key is to understand what's really important and focus on helping the enterprise achieve that by creating a mixed strategy of deterrence, prevention, detection and reaction, and adaptation. Default deny is 100% prevention. But you can't have perfect prevention anyway, so why try to achieve it? Because the closer you get the better it is? For whom?

My opinion at this time and in this history of the world we live in, is that prevention should be practiced right up to the point where users can't do their jobs seamlessly and with a minimum of friction. And at that point, detection and reaction should kick in and dominate the day-to-day part of the approach with deterrence and deception taking on the strategic roles that they require in order to reduce the time and effort required for detection and response. And adaptation, in the form of an ongoing effort to create and adapt an enterprise information protection architecture, should be the primary long-term approach.

Default deny is dead, and information protection specialists, for the most part, just never got the obituary notice. So here it is:

Default Deny

1970s - 1990s

Died of not changing quickly enough

to meet the needs of the world around it.

Survived by its child - risk management

For more on enterprise information security architecture, follow this newsletter - or to get more of it in less time, buy and read "Enterprise Information Protection" - available at Amazon, Barnes and Noble, or other fine online booksellers near you.