CxO Trust Newsletter - March 2022

Bias and Noise in the Decision-Making Process: Why Zero Trust Will Help You

Daniele Catteddu, Chief Technology Officer, CSA

The Zero Trust approach has become extremely popular in recent years. This has been the result of a series of events in the market. The pandemic has accelerated the need for organizations to adopt a modern and flexible approach to information technology, the vendors of Zero Trust products are spinning their marketing wheels, and some governments, especially in the USA, have adopted a policy of Zero Trust first as a part of their cybersecurity strategy.

Zero Trust is a combination of the adoption of continuous risk management best practices and the application of skepticism when evaluating the trustworthiness of an entity, be it a human or a machine. So, at its essence, Zero Trust is about the decision-making process.

For those of you familiar with some foundational concepts of behavioral economics, cognitive bias and noise (or unwanted variability) are two of the contributing factors that most negatively influence a decision. Bias and noise pollute our analysis process and lead systems (and humans) to make wrong decisions and estimations of, for instance, the level of trust that should be assigned to a certain entity when interacting with information and communication technologies.

Bias and noise plague the decision-making process by introducing wrong assumptions, over/underestimation of the value and weight of certain data in the decision-making process, variability, etc.

The advantage of the Zero Trust philosophy is that it approaches the problem of defining and assigning trust by adopting the principles of 'making no assumptions' and 'trust but verify.' In other terms, that means that the key driving principles behind Zero Trust go in the direction of eliminating or reducing at the source those factors that generate system bias and noise.

Clearly, technology plays a role in Zero Trust, but as always, the technology is an enabler of the solution, and not the solution itself. Technologies such as mTLS, Single Packet Authorization (SPA), and drop all firewalls, and architectures such as Software Defined Perimeter (SDP), ZTNA, and BeyondCorp/Prod, are certainly key enablers for a Zero Trust approach. However, what appears to be paramount is an understanding of the cultural shift that the Zero Trust philosophy proposes.

The spirit of Zero Trust is to move away from the idea that there are users or machines that can be always trusted because they live in a certain location (e.g., internal network or Country X), or because they have certain initial attributes, or because they have certain roles. Of course, this goes against the consolidated cybersecurity and network security old/current 'moat and castle' and 'defense in depth' models, and this is exactly the organizational shift needed within companies.

The access to resources shall be regulated based on the idea that each trust-based decision is ephemeral,

and it should be renegotiated depending on the context in which a certain user/entity/resource operates. A server to which I have access now might not be allowed to me in 30 minutes if, for instance, the security hygiene of my endpoint has changed, or if the recourse I want to have access to requires additional permission, etc.

Of course, there is more to Zero Trust than just a cultural and organizational shift. There are a number of actions that a company has to put in place for a successful implementation, i.e., mapping of users, identifying management, resource mapping, data flow mapping, continuous monitoring, data analytics, etc., but since the end goal is to improve the accuracy, efficiency, and effectiveness of the decision-making process, then the revision of the current conceptual model behind the definition and attribution of trust should be the starting point.