Security Metric of the Week #27:
Number of times that assets were accessed without authentication or validation

Authors:
Krag Brotby, CISM, CGEIT
Gary Hinson, PhD, MBA, CISSP

This candidate metric immediately begs questions such as would you know:

- When assets are accessed? Certain accesses to some IT systems, databases, applications, data files etc. may well be monitored and logged routinely, but probably not all of them, and certainly not when it comes to non-IT information assets such as paperwork and intangible knowledge.
- Who or what was accessing them? If someone is able to access assets indirectly through a separate computer system, network connection or third party, how would you know this was taking place? What if the access was entirely automated e.g. a scheduled backup process: does that count as an access event?
- Whether the access attempts were successful or unsuccessful? The metric is ambiguous on whether it counts access attempts and/or access events.
- Whether they were 'authenticated'? Often, people are presumed to have been authenticated previously purely by dint of being in a certain place (e.g. an employee on site in the office) but what if the presumption is false (e.g. an office intruder or visitor)?
- Whether they were 'validated'? 'Validation' seems a curious term in this context. Precisely what is being validated, and on what basis?

If we're being really picky, we might wonder whether this is truly meant to be a simple cumulative count of events, or in fact a rate of accesses (i.e. the count in a defined - but currently unstated - period of time, such as a month). Going by the literal wording of the metric, we're not even entirely sure that it is measuring access to information assets, specifically!

Our concerns are naturally reflected in a poor PRAGMATIC score:

P	R	A	G	M	A	T	I	C	Score
61	78	33	16	33	0	44	35	33	**37%**

Notice the zero score

for Accuracy. It is difficult to identify, let alone measure, when someone attempts unauthorized and inappropriate access to an asset. If they are unsuccessful as a result of the identification, authentication and access controls blocking their access, that fact will hopefully be recorded somewhere. However, if they are successful due to the controls failing to prevent their access, that is unlikely to be recorded. We might take a guess at it, but that's a guess not a measure.

SMotW #27 is a typical example of a security metric that was probably crafted with some specific purpose in mind. To those who designed it, it probably meant something at the time. Unfortunately, without the background context, we have little idea what it is about. On the other hand, if the original design was properly documented or was explained by the designer/s, we would know what the measurement was trying to achieve - in other words, its purpose and the related assumptions or constraints.