A VULNERABILITY ASSESSMENT IS NOT A RISK ASSESSMENT The next time you are hiring for an open-information security position, if you want to watch the candidates squirm, ask them to describe the difference between a vul- nerability assessment and a risk assessment.Further, a comprehensive risk assessment needs to account for any compensat- ing controls that already exist.Sometimes the risk exposure is referred to as the "impact" or "consequence" of the risk, and it should always be tied to a particular threat/ vulnerability pair.Notice that this description helps us rate the severity of the exploit by indicat- ing how much data (all client data from the United Kingdom) will be affected, and the sensitivity by the scope of which data will be disclosed (sensitive, regu- lated customer data). It also indicates that a notification to clients will be required which affects reputation, costs money, and could expose the organization to civil legal action. A dollar value of financial loss is also stated in order to quantify the impact to the organization. When articulating a risk, it is not enough to just describe the lack of a control and call it a risk. For example, you may see someone with no formal risk assess- ment training describe the risk in the previous example as "TLS/SSLv3 is not required for all communications."In the case of the Web server sup- porting weak SSL ciphers, a compensating control might be that the Web server is only ever accessed over a secure VPN connection, thus not relying on the SSL encryption to protect the communications.The combination of the likelihood that the threat will exploit the vulnerability, and the severity of the exploit, combined with the sensitivity of the asset itself yields the risk exposure rating.Too many organizations think that if they get a pretty report out of Qualys or Nessus scanners listing all the running services, missing patches, and possible vulnerabilities that they have performed a risk assessment.It may seem like splitting hairs, but this casual use of terminology is usually a symptom of information security inex- perience that leads to some very ineffective security programs.A typical vulner- ability assessment will identify weaknesses and flaws through some kind of active means such as scanning or configuration analysis.Attackers typically use vulnerability scans as part of their reconnaissance, so it is good to run the same tests yourself to identify which weaknesses would be visible to an attacker.A risk assessment is the superset of activities for taking that vulnerability data, mapping it to likely threats, evaluating the severity for the given environment, and articulating the risk(s) that might result.Vulnerabilities are identified and rated based on a very general knowledge of how they might be exploited; however, no real analysis of applicability or threat analysis is included.Risk Assessment In general, a technical risk assessment is going to include a vulnerability assess- ment of some kind; however, there is much more to a risk assessment than just identifying weaknesses.Similarly, any scanning or assessment tool may provide some guidance about the applicabilityof a vulnerability, but you are going to get a very one-dimensional risk score from a vulnerability assessment.The impact statement describes two potential threat activities, unauthorized reading of communications and intentional modification of messages in transit.Just like running a vulnerability scan isn't a penetration test, it isn't fair to equate a vulnerability scan to a risk assessment.That just isn't good enough.

Summarized by © lakhasly.com