PREVAILION

Focusing on Compromise Intelligence vs. Vulnerability Intelligence

Preventing Breaches Using Active Risk Posture vs. Potential Risk

TECHNICAL WHITEPAPER

Table of Contents

Introduction

Often when speaking with people about what we do here at Prevailion, discussions related to the severity and probability of exploitation of vulnerabilities comes up. People naturally want to understand what we know about the underlying vulnerabilities that are tied to the post-exploitation compromises we see globally daily. It's both natural and common, in addition to being understandable. The detection and identification of vulnerabilities in the course of establishing "root causes" of hacks, attacks, and compromises has been at the forefront of conversations related to the threat landscape for the better part of the last two decades. The question today, however, is whether or not it is prudent to focus on the vulnerability primarily in all cases and at all costs, or if it makes more sense to focus on ***active compromises*** observed within your environment – and that of your partners and suppliers in order to address and re-mediate them.

The Importance of Understanding Risk

An intelligent conversation on the subject of vulnerability is pointless if the concept of 'risk' and the formulas used to arrive at conclusions about it are not understood. Decoupling these concepts leaves you with atomic elements – which alone, though interesting, neither provides guidance nor tells a story. There are many diverse schools of thought related to this subject. Many approaches and models dedicated to the proper characterization and articulation of 'risk', it's impact to an organization, how to assess and analyze it, and how to mitigate it. Through the years multiple formulas have been devised (used and applied by risk management professionals, services providers, and vendors alike), that aid organizations in understanding their cyber-risk and broader organizational risk posture. In order to illustrate an alternate competing hypothesis this paper will provide and review some examples of the formulas that are used to calculate risk.

Risk Formulas and Vulnerability Severity Scores

There are many formulas related to the calculation of risk in cybersecurity. Traditionally, these calculations would be considered in the course of establishing and maintain over time a well-defined and implemented risk management program. Cyber risk formulas vary and will continue to do so ad infinitum. Examples include but are not limited to:

- Risk = Vulnerability x Threat / Potential for Exploitation – Organizational control efficacy[i]
- Risk = Likelihood × Impact[ii]
- Risk = Criticality (Likelihood × Vulnerability Scores [CVSS]) × Impact[iii]
- Risk = Threat / Vulnerability x possibility of occurrence x impact – control effectiveness[iv]

There is no shortage of formulas or ways to express risk from a cyber security and risk management perspective. Similarly, it is very difficult to have an intelligent conversation about risk without delving into realm of vulnerability detection and identification, scoring in terms of severity, prioritization, and remediation.

History of Vulnerability Categorization, Scoring, and Prioritization

In 1999 David E. Mann and Steven M. Christey of the MITRE Corporation presented a paper they'd written titled, "Towards a Common Enumeration of Vulnerabilities" at the 2nd Workshop of Research with Security Vulnerability Databases at Purdue University in January of 1999. This presentation was the origin of what would become world renown as the CVE List. That concept gave birth to establishing a working group that would late evolve into the initial 19-member CVE Editorial Board and led to creating the first 321 CVE entries resulting in the launch of the CVE List in September of 1999. The creation of the CVE Editorial Board would aid in changing the world of information security from both a defensive and offensive perspective in an irrefutable way forever.

Later, Common Vulnerability Scoring System (CVSS) was commissioned by the National Infrastructure Advisory Council (NIAC) tasked with supporting the global Vulnerability Disclosure Framework. It is currently maintained by FIRST (Forum of Incident Response and Security Teams). CVSS was a joint effort involving many groups, including:

- CERT/CC
- Cisco
- DHS/MITRE
- eBay
- IBM Internet Security Systems
- Microsoft
- Qualys
- Symantec

The model was designed to give end-users a complete, comprehensive score that presents both the severity of the vulnerability in question and the risk represented by its potential presence and exploitation. I say "potential" here because traditional risk assessments do not involve exploitation exercises in most cases (though perhaps they should). Formulas and metrics[v] are used to produce and deliver results to the organization being assessed and / or audited in order that they might put them prioritize and address them based on their scores and potential (probability) of exploitation. Base scoring is arrived at by the vendor or originator using the security triad (confidentiality, integrity, and availability), and once published, isn't expected to change. The base score has the most significant influence on the final score and ultimately represents the severity of the vulnerability. In addition to the base scores, temporal scores are also generated by the vendors in question and the coordinators for publication, and these temporal scores modify the base score. The temporal scores represent the urgency of the vulnerability at a point in time. There is also a score that considers the environment; however, this score is optionally calculated by organizations and, when computed, adjusts the combined base-temporal score.

The MITRE Corporation introduced the Common Weakness Enumeration (CWE)[vi], adding additional detail, depth, breadth, and classification structures from a uniquely diverse set of industry and academic sources and projects the same year. As we can see, a great deal of time and resources have been spent on the study, classification, and scoring of vulnerabilities. However, one has to ask if the research and the decision to prioritize work (post vulnerability scanning initiatives have concluded) to re-mediate vulnerabilities based on scoring in the absence of exploitation is worthwhile? And additionally, ask themselves if focusing solely on the potential for its exploitation is a good use of an organization's time and resources when real compromise (breach) and actor activity may be present and observable within the organization going unnoticed and unaddressed ad infinitum. As Mahatma Gandhi said, "Action expresses priorities."

Compromise vs. Vulnerability: Do We Choose the Chicken or the Egg?

Stephen R. Covey once said, "Most of us spend too much time on what is urgent and not enough time on what is important. " This concept is especially true when discussing matters related to defensive cyber-security strategy and the detection, identification, and mitigation of threats. It is essential to thoroughly understand (via the detection and identification processes we have at our disposal) vulnerabilities found within our network environments. It is far more critical to understand *what has been exploited and compromised than what has not yet been exploited and compromised* in terms of vulnerabilities later (not later, mind you; this isn't a Vegas odds game after all), time.

Addressing what ails you now, in terms of real-time *exploitation and compromise* (what I like to call a breach), is far more critical than addressing what has not been compromised irrespective of CVE, CWE, and CVSS. It just simply is. Failing to do so is simply irresponsible and wrong. For cyber-security leadership, it is a failure (but it doesn't have to be one). And for operational security personnel, it is the difference in addressing compromise (breach) in an evidentiary fashion proactively. The results of which include accelerated *mean time to detection* (MTTD)[vii] and *mean time to re-mediate* (MTTR)[viii], both of which have a net effect on the dwell time enjoyed by an adversary operating with impunity within their environment. So, why – if this capability, this cognition can and could be had and integrated within an organization's cyber security programs and stacks would – assuming you were aware of its existence and had the opportunity to do so, would you not take advantage of this?

Conclusions

There is no argument that it is imperative to understand the risk posture and, if detected and found to present, vulnerabilities that lie within. However, it should be obvious that is it is *more* important to focus the energy and resources of your team on those resources, where a vulnerability (irrespective of CVE, CWE, and CVSS) has been exploited already or human error (i.e. phishing attack) has already passed the gate and is preparing to detonate in the near future. At Prevailion, we are less focused on the monumental and impossible task of hardening all your systems and applications based on the vast number of old and new exploits targeting your attack surface. Even a single compromise can lead to catastrophic financial consequences. That is where Prevailion has focused on providing hard and actionable evidence of compromise in real-time and on a continuous basis to stop the various attackers that invariable find a way to slip through the gates. If you'd like to learn more about Compromise Intelligence can help you improve your security operations and programs against the unknown, you can visit us at prevailion.com

References

[i] A formula that I first encountered many years ago while a consultant with the acclaimed International Network Services (INS)

[ii] Open Web Application Security Project (OWASP), "The Free and Open Application Security Community," Conference on Information Security and Assurance, IEEE, p. 461-465

[iii] https://www.isaca.org/resources/isaca-journal/past-issues/2014/an-enhanced-risk-formula-for-software-security-vulnerabilities#7

[iv] https://stateofsecurity.com/calculating-cyber-risk/

[v] https://www.first.org/cvss/v1/faq#What-is-CVSS

[vi] https://cwe.mitre.org/about/history.html

[vii] https://www.optiv.com/cybersecurity-dictionary/mttd-mean-time-to-detect#:~:text=MTTD%20is%20the%20average%20length,done%20by%20a%20cyber%20incident.

[viii] https://www.optiv.com/cybersecurity-dictionary/mttr-mean-time-to-respond-remediate#:~:text=MTTR%20is%20the%20amount%20of,threats%20to%20their%20network%20environment.