F5- Business Information

F5 is a technology company that specializes in delivering cybersecurity and networking solutions. They have recently expanded to include security services to businesses and enterprises through malicious bot automation protection, multi-cloud services. Such as protection from DDoS, ransomware, and data leaks.

Enterprise Vulnerability Management

The goal of a company when managing vulnerabilities is to monitor the status of the enterprise's security. Identifying and patching vulnerabilities as they become known. Operational processes are put in place by identifying and patching vulnerabilities. The security team also monitors systems so alerts on specific vulnerabilities can be detected and acted on. There are four ways a company a company can work to improve security changes over time through monitoring and patching vulnerabilities. The first step is preventative, to ensure vulnerabilities are compensated for and patched before they can be exploited by attackers. Detective includes monitoring all enterprise security automation systems to detect incidents. Forensic, involves logging event and incident information to be correlated, cross-checked, and investigated. Audit- involves centrally collecting forensic data to be analyzed by auditors and investigators.

Vulnerability Predictability and Cost Model

The purpose of this model is to create a cybersecurity vulnerability cost model that predicts the costs of each vulnerability and how much impact each vulnerability will cost each to prevent a potential attack if the network is infiltrated. Enterprises use common vulnerabilities to secure their companies and to prevent attacks. This model will estimate the cost to fix each vulnerability as a preventative measure. The model will be using the Monte Carlo Simulation to predict the likely hood of an attack if the vulnerability is not fixed. The model uses the data from each published CVE[1] that is provided by the national institute of standards and technology. This data will use the vulnerabilities that are present for the company F5 networks to show how to predict the cost and likelihood of each vulnerability.

Simulation of the Model

To simulate the model the event occurrence was calculated by using a 1 for yes and 0 for no. The model used was the Bernoulli distribution was used with a binomial distribution to calculate the predictability of each vulnerability over the course of 12 months.

To estimate the cost of each vulnerability I used the industry data from bug bounty programs to determine the low, best case, and high cost of each CVE. Then I simulated the information in a triangular distribution to identify the total estimated cost of each vulnerability.

I calculated the average cost by using the mean of the estimated cost. Then I calculated the average monthly cost by dividing the average cost yearly by 12. Lastly, I calculated the vulnerability probability for each month by taking the event occurrence divided by 12. These gave me the results of the simulation.

CVE- Common Vulnerabilities and Exposures

A CVE stands for common vulnerability and exposure. The purpose is to identify vulnerabilities that are present in specific versions of code bases. “It is defined as a weakness to the logic or code in software or hardware components. When exploited it results in negative impact to confidentiality, integrity, or availability. Mitigation of vulnerabilities includes making changes to codes to protect the code or network. [2]

CVSS- Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) has a rating of 1 (lowest) to 10 (most severe). This predicts the damage a vulnerability if not address will cause to your company. These scores represent the time that each vulnerability needs to be addressed. In 2019 the department of Homeland Security (DHS) issued an operational directive to all federal agencies describing how they need to patch Critical vulnerabilities. Vulnerabilities that have a score of 10 must have a patch in 15 days of detection, for high severity vulnerabilities those with a CVSS score over 7 there must be a patch within 30 days of detection. [3].

EPSS- Exploit Prediction Scoring System

Mike Roytman and Jay Jacobs of Cyentia Institute released a “Exploit Prediction Scoring System (EPSS) model in 2019. This model looked at 25,159 vulnerabilities that were published by MITRE’s Common Vulnerability Enumeration (CVE) between 2016-1018. Based on the machine learning analysis there were 16 significant factors usable to determine predictability. Those factors were observed and analyzed using a machine learning to predict the likelihood of an exploitation of a vulnerability. By running a log calculation, they could predict the probability percentage of the exploitation in the next 12 months. The higher the probability the higher priority the patch[4].

Bug Bounty Cost Assessment

The model uses the predictions of the cost to identify the amount of money that it would cost to patch a vulnerability. To find the cost of each vulnerability type bug bounties gave an estimate of the cost it would take to fix each vulnerability. A bug bounty is a program put on by a company to pay ethical hackers for finding weaknesses in their networks. There are different award amounts for the size of the company and the specific vulnerability. Through this information and the severity of the vulnerability a prediction can be made of the cost of each vulnerability.

Works Cited

[1] NVD - Vulnerabilities. (n.d.). Https://Nvd.Nist.Gov/Vuln. Retrieved December 14, 2021, from https://nvd.nist.gov/vuln

[2] CVE - CVE. (n.d.). Http://Cve.Mitre.Org/. Retrieved December 14, 2021, from http://cve.mitre.org/

[3] cyber.dhs.gov - Binding Operational Directive 19–02. (n.d.). Https://Cyber.Dhs.Gov/Bod/19-02/. Retrieved December 14, 2021, from https://cyber.dhs.gov/bod/19-02/

[5] Pompon, R. (2021, October 12). Prioritizing Vulnerability Management using machine learning. F5 Labs. Retrieved December 14, 2021, from https://www.f5.com/labs/articles/cisotociso/prioritizing-vulnerability-management-using-machine-learning