VULNERABILITY DISCLOSURE ASSIGNMENT

Vulnerability disclosure is a policy that provides guidelines for publishing information about a particular computer security problem. It provides the vendors with the opportunity to fix any bugs found in their products and avoid any future problems that may have occurred because of it. There are many types of vulnerability disclosure policies such as full disclosure, coordinated disclosure, non disclosure, bug bounty and private vulnerability sales. Each has its own advantages as well as disadvantages. After thorough consideration of all the options I feel that the best approach that should be followed is coordinated disclosure.

In coordinated disclosure, people who find the vulnerabilities will first report it to the vendors or some trusted third party that will then later forward this information to the vendors. In this case, only the finder (the person who found the bug), any trusted third party that reports to the vendor and the vendor will have information about the vulnerability. Once the solution is developed and made available to end users the information about the vulnerability is published for public view. But sometimes this is not done. The amount of information published depends on the vendor and the type of bug found. In the coordinated disclosure policy, since the information is not released to everyone the attackers will not find out and hence this protects the software or application from being exploited. Also the vendor can choose to work with the finder in developing a solution. This proves to be a good idea sometimes as the finder will know more about the bug since they are the ones who discovered it. Everyone thinks differently and as a result with more than one pair of eyes even things that are hidden quite well can be dug up. So the finder will be able to provide better insight on what all ways the vulnerabilities can be exploited and possible ways to defend against these attacks. As the vendor comes up with solutions the finder can test them out to see if there are any loopholes.

An example of coordinated disclosure is the CERT/CC. The CERT Coordination Center was established in November 1988. It is operated by Carnegie Mellon University and is funded by US Department of Defense and Homeland security. Their goal is to “analyze the state of Internet security and convey that information to the system administrators, network managers, and others in the Internet community”. The center allows many secure ways for the public to send sensitive information. When CERT/CC receives a vulnerability report it is immediately forwarded to the concerned vendor. Therefore the center acts as a trusted third party. The information regarding the vulnerability is then disclosed to the public after 45 days of receiving the report and hence, giving the vendors a limited time to come up with patches. This forces the vendors to develop solutions, which is helpful as sometimes the vendors may choose to ignore these bugs. The disclosure date can be altered by either extending it if the vendor requires more time or releasing it earlier if active exploitation is noticed.

Full disclosure is a policy which allows full details of the vulnerability to be released publically as soon as possible. Mostly this is done without vendor involvement. The major problem with this approach is that having made the information public all the attackers will have access to this information. Since it is posted immediately after the discovery it doesn't provide the vendors with enough time to act on the information and provide fixes for the vulnerability. For example, Dan Kaminsky, a well known security researcher, found one of the most severe vulnerability in the DNS system in 2008. This vulnerability could have easily allowed attackers to carry out cache poisoning on DNS name servers. If this information was made public it would have caused a lot of problems. Dan Kaminsky knew that this issue was very severe and that the potential damages could be great. So he knew that it would have been incredibly reckless to publicly release it without giving the vendors an opportunity to issue a patch.

Non disclosure allows the vulnerability report to be shared among a small group of people or kept private. This doesn't help at all. If exploiting a particular vulnerability doesn't do much to affect the product then not sharing it may be fine. But if it causes noticeable damage to the system then it must be reported so that fixes can be made available. Bug bounty is another good method of reporting bugs. It even lets us get paid for it. The company can also restrict the amount of information available for the hackers about the product. It is a form of coordinated disclosure as the bugs are still reported back to the vendors.

In conclusion the coordinated disclosure is better for the following reasons:

- It gives enough time for the vendors to fix bugs.
- It allows both the finders and vendors to collaborate with each other.
- It prevents attackers from getting the vulnerability information before the solution is available.

Many vendors don't welcome this approach and may go against those who report bugs to them. But it is better to have the bugs directly reported to the vendors than to have them posted publicly and then find out about it later. Also, the vendors can control the amount of information that can be disclosed to the public regarding the vulnerability.