Article Title: What is Information Security?

Publisher: GeeksForGeeks

Publication Date: Apr 7, 2023

One of my favorite sources for technological information is GeeksForGeeks, so it was only natural that I turned to them for some fundamental information on information security. One of the most important concepts that this article went over was the three objectives of Information Security, also known as the CIA:

1. Confidentiality: Information cannot be shared with unauthorized individuals or entities. Authorization is a highly important tool to ensure that whoever is requesting access to information is identifiable, and their identity is verifiable.
2. Integrity: Data integrity is hugely important. There are authorized processes that result in data manipulation/mutation, and processes/individuals that are not authorized to make these changes should not have access to this ability. If they did, that could result in a lack of data integrity.
3. Availability: Up to date and accurate information should be available upon request. For example, if an employee, or individual who previously had access to secure data recently lost such authorization and made a request, the target system should be able to pull accurate data on the requester and deny access.

The article goes on to explain that organizing your systems' security posture with an information classification system offers several advantages. It results in improved security due to the ability to classify sensitive information, and the ability to follow industry compliance standards like HIPAA and PCI-DSS. Cost savings are an additional benefit because your organization can save money by not securing data that's determined "non-sensitive" (or at least loosening security restrictions on this data), being able to better manage risks by having the data sensitivity predefined and having a better understanding of the required incident response based on the sensitivity of data involved.

The article also explains the disadvantages of using an information classification system in that it introduces additional complexity, a sense of potential false security, and additional maintenance. This complexity can result in a lack of flexibility, and the possibility of inaccurate classification of data. The article continues to define some additional uses of Information Security, like disaster recovery, authentication, encryption (the ability to protect sensitive information using a cypher), network security and physical security.

Finally, GeeksForGeeks explains the potential threats to secure data, and the variety of different methods that bad actors can use to steal and threaten secure information (phishing, malware, ransomware, insider threats, human error).

This article I think has the potential to have a large impact on day-to-day activities. I think it's important to always consider information security in how you operate online. While at work, you should always be cautious about links in emails, texts, and direct messages. If you're working on building a new software system you should ask the heavy security and access control questions up front. If you're

working with networking, you should be asking questions about secure transit of information, and whether information needs to be encrypted at rest. These are all things that I personally have to maintain context of on a day-to-day basis for my work.

I think this is important information for organizations as well. I didn't get into too much detail from my summary for the security threats, but individuals in an organization should absolutely go though regular internet security training. The basics are where people slip up, like phishing emails, and plugging in USBs that you thought were safe. The article also provided valuable information in developing a security posture for your organization. The suggestion to use Authentication/Authorization (which are two separate things, but ideally used together) is a very valid suggestion. Most places are using some sort of multifactor authentication these days, and it's because it's a robust security measure. I also think that the information classification system is important in financial/health organizations. Those organizations have their own sets of compliance guidelines that can be very, very expensive if it's found that your organization is non-compliant. Having a good way to delineate between PII, and non-PII information would be beneficial to an organization dealing in secure data.

I don't personally disagree with much of what the article is saying. I think that the article didn't do a great job at organizing the information, it felt a little strange that it jumped right into information classification systems, but oh well. I was able to digest the information quickly, which is what I was looking for. The content itself I agreed with.

GeeksforGeeks. (2023, April 7). What is information security?. GeeksforGeeks. https://www.geeksforgeeks.org/what-is-information-security/