Making Ethical Decisions That Prioritize Systems' Security and Stability: Ethics Analysis Essay

Hassan Alshehri

Kenneth Corpus

11/27/2023

Scenario:

A system administrator is asked to grant access to a sensitive system to an employee who needs the proper credentials or authorization.

Essay Topic:

How does the System Administrator Code of Ethics guide the actions of a system administrator in this scenario, and what steps should they take to ensure the security and integrity of the system while still fulfilling their professional obligations?

Introduction

Most companies that have invested in information systems have ethics policies that guide their staff in protecting the security and integrity of these systems. While these policies apply to all users, system administrators are considered privileged/unique users because they can access sensitive information that others cannot (Limoncelli et al. 323). Their privileged position means their standards are higher, thus requiring them to be more careful in applying and enforcing these policies. However, in their day-to-day activities, they usually encounter scenarios where they have to make ethical decisions that prioritize the system's security and integrity. For instance, the administrator in the scenario described above is being asked to do something that can compromise the security of a sensitive system. Granting access to an unauthorized user or a person with limited access rights would undermine the system's integrity and the confidentiality of data contained in it. Therefore, this essay critically analyzes this case using the System Administrator Code of Ethics to shed light on the administrator's steps to ensure system security and integrity without neglecting their professional duties.

Analysis

The administrator in this scenario should be guided by three principles described in their code of ethics: privacy, system integrity, and ethical responsibility. The privacy guidelines/principles require system administrators to preserve and safeguard the confidentiality of any information they are entrusted with. In this case, if the administrator allows the employee to access the system without proper credentials or authorization, they would expose sensitive information to possible manipulations by unauthorized entities. The system integrity guideline also requires system administrators to avoid actions that undermine system integrity. Furthermore, in deciding whether to grant access, they should remember the ethical responsibility guideline, which requires them to make decisions that do not compromise the community's safety, privacy, and well-being.

Based on the three guidelines, the system administrator should take several steps to fulfill their professional obligations without compromising the system's security and integrity. First, he/she should seek clarification about the request to ensure it is legal and consistent with the company's policies. If these policies need clarification, the administrator should seek advice from a competent company member. Seeking clarification and reading the company policy help determine whether the employee's request is legal or illegal. If it is against the policy, the administrator should be bold in communicating it and turn down the request respectfully.

The next step is to engage a higher authority, especially if the employee making the request is a senior person in the organization and is persistent/insistent on getting access. Some organizations, especially the bigger ones, have an office dedicated to addressing such problems when they arise (Limoncelli et al. 338). In such organizations, the administrator should consult the office to establish an amicable solution. Other institutions have explicit guidelines detailing what the administrator is supposed to do in such scenarios and how they are supposed to do it (Fagernes and Ribu 969). If a small company does not have those guidelines or structures, engaging the human resource (HR) department or any other relevant department could help by letting them know that there is an issue that requires their intervention.

Keeping records of all the events is also critical in such a scenario to ensure that the administrator has enough evidence to validate his/her claims in case he/she is asked to do something illegal by a senior person in the company. Records that should be kept include phone calls, request dates, and commands given. One of the most effective ways of securing these records is to ask the employees to make their requests in writing. This technique ensures that the

request is explicit and that the administrator has a paper trail on which he/she can depend in case of a policy violation dispute. Limoncelli et al. (399) note that putting a request in writing ensures that something that could have been misinterpreted is clarified and that the administrator has a trail. He also argues that people fear putting unethical things in writing, meaning that if a request is against the company's policy, an employee would fear to make it.

Conclusion

This case presents a critical analysis of a scenario in which the system administrator requests access to a sensitive system from an employee who needs the proper credentials or authorization. It has been demonstrated that such a request can lead to privacy/confidentiality violations or compromise system integrity. To this end, the administrator must follow the principles of privacy, system integrity, and ethical responsibility described in their code of ethics to make an informed decision to safeguard the system's security and stability. The three steps the administrator should take to fulfill these guidelines have also been described. They include seeking clarification regarding the request and ensuring that it is consistent with the company's policies, engaging a higher authority in case the person making an unethical request is a senior employee, and keeping records of events if the request must be accepted.

Works Cited

Fagernes, Siri, and Kirsten Ribu. "Ethical, legal and social aspects of systems." *Handbook of network and system administration*. Elsevier, 2008. 969-997.

Limoncelli, Thomas A., et al. *The practice of system and network administration*. Pearson Education, 2007.