Policy Analysis #3

Omar Branch

Department of Cybersecurity, Old Dominion University

Cyber Strategy and Policy

Professor Malik A. Gladden

2/25/2024

As we dig deeper into access control policy lets have a little refresher before we get into this topic, which is the ethical implications of access control policy. As we know by now, access control policy secures highly important data and minimizes the risk of an attack. Why yes it is important to keep all data stored safely, but when does all become a problem? Which is why we're here for today's topic which is the ethical implications.

When it comes to cybersecurity there will always be a problem deciding when enough is enough. Ethical implications by definition states what's right and wrong actions in specific situations. In access control we run into a few issues and we're going to briefly get into one by one. Let's start with something simple, when you first apply for a company in IT you are given the credentials needed in order to do your job. These credentials can be your badge, email, username, and password that you can eventually change to something you can remember. But let's say you use that email to send something out somewhere, due to policies in place someone has access to monitor and see what you're sending which technically is an invasion of privacy. This can somewhat lead to an issue later down the road but in reality they're just trying to make sure things are following the company's rules.

When it comes down to the cost of an access control system the prices can vary depending on the size of your company and the set goals/values within the company. Just to put into perspective on how much something will cost imagine you own a tech building and roughly have 12 keypad controls just on the first floor. Each keypad is going to need some type of security attached to it right? So lets say it'll cost $900 per keypad to install a security policy/system. That comes out to a total of $10,800 per

keypad and let's keep in mind that just the first floor. So yes, this type of security raises the issue that companies tend to run into which is something that is cost efficient. But the more you spend though the more benefits you can get. A few benefits that come from implementing an access control policy are simplified management and enhanced control, real time tracking in all systems, elimination of traditional keys, and of course the obvious which is increase in security and risk mitigation.

One access control that I like specifically is the role based access control also known as RBAC. This access control policy is in charge of the level of access that employees have in a network. It restricts employees to the point where they can only access the information that allows them to perform their job duties. Then of course you're gonna have your select few that can oversee all the employees in the company. For this instance I don't believe employees' rights are violated at all. The company usually informs the employees in this instance and gives a heads up in regards to what they can and cannot see. The manager and CEO will be the ones that look behind these employees to make sure protocol is being followed as well.

In conclusion the access control policy is something that to me doesn't have any major problems against individuals rights, just besides maybe privacy of companies emails. I don't believe that there are any negatives of having these policies either as they are there to provide a guideline and give companies a format to build on. The cost of the measures can become extremely pricey which is why it is vital that businesses look at all the information before making a decision that could possibly cost them more than they can chew. I do believe though that as we continue to grow inside the cyber world we are going to possibly run into policies that need to be revamped but nothing major.

References

Kashmar, N., Adda, M., Atieh, M., & Ibrahim, H. (2021). Access Control in Cybersecurity and Social Media. *Cybersécurité et Médias Sociaux*.

Badsha, S., Vakilinia, I., & Sengupta, S. (2020, January). Blocynfo-share: Blockchain based cybersecurity information sharing with fine grained access control. In *2020 10th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 0317-0323). IEEE.

Hugot, V., Jousse, A., Toinard, C., & Venelle, B. (2021, December). A safe dynamic access control providing mandatory automotive cybersecurity. In *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (pp. 848-851). IEEE.