Question: Modern operating systems, such as Red Hat Linux, Apple macOS, Ubuntu Linux, and Microsoft Windows, frequently distribute patches, and some application and utility software developers also distribute patches for their products. However, the number of developers that distribute patches is relatively small when compared to those who do not. Many programs and apps never receive any patches or security updates. Should programs and applications be required to provide security updates for a specific period of time after the program is released? What should happen when a software company goes out of business and leaves your product without an option to be patched or updated? Should organizations charge for updates and patches?

Answer:

When it comes to if I think programs and applications should be required to provide security updates, for a period of time after the program is released, my answer would be yes. The reason being is most programs and applications look to provide security updates for there customers to help protect them from known cyber threats and various vulnerabilities that can be exploited by attackers, if not already patched. This allows the programs and application to maintain user trust, and continue operations through its support lifecycle, in which programs such as Windows, RedHat, and even Ubuntu have implemented for there community's.

When it comes to what a individual should do if the product they utilize, provider goes out of business and is neither patched or updated, The individual should immediately stop using the product. The reason being is that they run a major security risk on there devices, due to the vulnerabilities that could be exploited by attackers that they are unaware of, especially if this program is connected to the internet.

I feel that organizations should not charge for updates and patches, as this seems a little unethical. This is due to minor vulnerabilities and crucial vulnerabilities, needing to be patched

immediately, for continued operations of various projects of organizations and users. And if users or organizations aren't able to pay, this would leave there devices vulnerable and making them victim of various cyber-attacks.