A Cyberattack on Garmin: Lessons for Our App

Ransomware attacks often target large organizations like hospitals, oil companies, and other important services. These attacks happen because companies that depend heavily on their systems are more likely to pay to get everything back online quickly. While many businesses and individuals have been hit by ransomware, this article focuses on how Garmin was affected and how this impacted both its everyday users and portion of the aviation industry. Garmin's services, which include fitness tracking and airplane navigation systems, were attacked by ransomware, causing major issues for fitness users trying to log workouts and pilots who needed updated navigation tools to safely fly including flight-planning mechanisms and the ability to update mandatory Federal Aviation Administration aeronautical databases. Garmin eventually acknowledged that they were hit by ransomware but reassured their customers that their personal data was not compromised. However, they did not mention the full effect on airplane software, including critical systems like navigation and timing services. Services like flyGarmin and Garmin Pilot apps were among those affected. As a result, flight schools and instructors, like Taren Stanton, faced major challenges because their planes could not legally fly without updated navigation. "Legally, we can't fly an instrument flight plan using them for navigation if they aren't kept updated. We had one plane that was temporarily grounded because of that," Stanton shared (Newman, Wired). This situation shows how unpredictable ransomware attacks can be, and highlights the importance of strong security measures, backup plans, and a solid recovery process to maintain customer trust.

From the Garmin attack, we can learn three key lessons: the need for solid security, reliable backup plans, and preparation for unexpected events. These lessons are important for us as we develop MyCampusGym, an app where users input personal data and rely on the service provided to be secure. Although ransomware tends to target larger companies, it can affect any organization. For this reason securing our app is critical to protecting both our services and user data. Our team will make sure that MyCampusGym stays up to date with the best security practices to minimize the risk of an attack. We also need to create backup systems (aka failsafes) so that, in the event of an attack, our app can still function in some capacity. This is why failsafes are vital because they keep services running even if the main system goes down. In Garmin's case, the lack of proper backups left pilots, flight schools, and instructors unable to use essential tools, like updated navigation software. This could have been avoided if there had been a better system to handle the attack while repairs were made. For MyCampusGym, we can create an offline mode that allows users to record workouts even when the app may not be able to connect to the web services. If a ransomware attack happens, users will not lose their workout data, and once the app is back online, it can synchronize any local data changes to ensure they are included in the service going forward. This kind of feature is essential in making sure users can keep using the app, even when there may be a problem behind the scenes, ensuring users feel the service they receive is reliable and dependable.

Preparing for unpredictable events is another important lesson we have learned from the Garmin attack. In the world of technology, new threats are always appearing and becoming important to address, and companies must constantly improve their security to keep up. While no one can predict every possible attack, we need to stay ready and keep improving the defenses or our application. Our team will be using Google Firebase as the main database for MyCampusGym. Firebase offers strong security features, like encrypting data to keep it safe. Using Google Firebase gives us another advantage: we can write our own security rules. This allows us to tailor security to the specific needs of our app and its users. We will be able to control who can access what parts of the database, and we can fine-tune permissions to make sure our system stays secure. Writing our own code, instead of relying on pre-made solutions, also gives us more control over the safety of the application. While using third-party code might be faster, doing everything ourselves helps us spot potential security risks early and fix them before they can be exploited by bad actors. To further protect users, we will also implement two-factor authentication (2FA). This adds an extra layer of security by requiring users to verify their identity with both a password and a code sent to their phone or email. We also plan to limit who can sign up for MyCampusGym by requiring users to use a verified university email (such as one ending in .edu or that has a top-level domain that has been submitted by an administrator). This will help prevent fake accounts and ensure that only students, staff, or faculty members are using the app. While adding third-party apps could offer more features, it could also weaken our security, as we would not have complete control over how those apps protect data. By keeping most of the development in-house, we can ensure that we build the strongest firewall and security measures for our users.

In conclusion, the ransomware attack on Garmin shows us why security, backup systems, and being ready for the unexpected are crucial. For MyCampusGym, we are committed to taking these lessons seriously. We will focus on strong security by using Google Firebase, encryption, and two-factor authentication. To protect users during potential disruptions, we will offer an offline mode, ensuring they can continue logging workouts even if the app is temporarily down. By limiting access to verified university email addresses and handling most of the application development process and work ourselves, we will have better control over security and data protection. By taking these steps, we aim to create an app that not only meets user needs but also keeps their data safe in a world where cybersecurity threats are always evolving.