The recent CrowdStrike software bug incident was caused by a faulty update pushed out by CrowdStrike to 8.5 million devices. Although a large number the aftermath of this faulty update caused more damage than the numbers seem to indicate. CrowdStrike is a cyber security company which produces software to protect organizations from attacks. The update rolled out was on their Falcon software which monitors computers for attacks. Computers with this software are normally holding crucial information or executing important processes. The outage caused airlines, hospitals, financial, and media services to all suffer from technological issues. Flights had to get delayed and medical records could not be accessed. All these computers that were compromised by these updates were all Microsoft windows 10 computers. Microsoft, to aid in this situation worked closely with CrowdStrike to release recovery tools to allow these computers to be reset to the past version before the crash so they could still be utilized.

The bug was caused by a sensor configuration update to windows system. This update resulted in system crashes and shutting down multiple flights because of technical issues. More than 10,000 flights were shut down and many public transit systems were also affected. CrowdStrike's outage also disrupted multiple appointment systems for hospitals which caused many people to not be able to get the help that they needed. Financial institutions were also heavily affected many people were getting pay checks later than they were supposed to because systems were down. In the media department multiple outlets were taken off the air such as British broadcaster Sky News was taken off the air because of the update.

To prevent this from happening in the future CrowdStrike and companies like them need to have rigorous testing and quality assurance processes before rolling out an update.

CrowdStrike did not follow the industry standard of rolling the update out to a limited number of users at a time which would have caused millions less in damages that CrowdStrike users suffered. The importance of rigorous testing is shown in this situation if this update was tested more, then this situation never would have happened, and medical appointments and flights would never have had to get cancelled and rescheduled.

In conclusion, CrowdStrike did do a lot wrong but also a lot right concerning this situation. CrowdStrike's damage control was very good and effective, and they made sure to be completely transparent during so. They had contacted Microsoft, AWS, and other services that their platform is normally used in combination with and had those companies help them fix their issue. Although they had great damage control and fixed the problems that the users had this situation should never have happened to begin with. CrowdStrike's tactic of pushing an update out to everybody at once without having a slow release which makes sure each group is able to test the new update and make sure it doesn't crash before sending it out to more critical systems is a large oversight. Especially with how CrowdStrike's program is used mainly on critical computers that if they malfunction there are very large conflicts that arise.

Citations

Kerner, S. M. (2024, October 29). *Crowdstrike outage explained: What caused it and what's next*. WhatIs. https://www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next

Thornton, K. (2024, August 19). *Crowdstrike incident: What happened and how can we learn from it?: UMGC*. University of Maryland Global Campus. https://www.umgc.edu/blog/crowdstrike