Samuel Bailey

July 26, 2021

Assignment 5-1

* Introduction
  + Whistleblower: Ubiquiti Breach “Catastrophic” – [Link](https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/)
  + January 11th, 2021
  + Ubiquiti did not do what many people believe they should have done in this incident. It was a major breach in their entire software.
* Describe the breach
  + Cloud Security & Host Security & App Security breach
  + This company was targeted for money and access to other systems. Simplistically the company is a money hole.
* Identify the threat(s)
  + Access to core systems were breached and opened.
  + If not fixed the entire company would go down.
* What could a developer have done to prevent this breach?
  + Implementing a better workflow for cloud computing and more software system checks.
* Summarize the case by explaining the role of best practices, Triple A and defense in depth in preventing future attacks.
  + Best practice for authentication is having a complex password as well as some form for MLA. For all admins on the team there needs to be a third authentication method of a flash drive or some sort of hardware.
  + Authorizations for core services should be max two admins allowed to work on service at once. Doing this with a 3rd authentication method will limit all unauthorized access.
  + Accounting is one of the main departments in all companies and needs to be protected at all costs. This is the department that people aim for. The entire goal of black hat hackers is to steal money, there’s no other reason for them to hack. Best case is to limit access for these accounts to the smallest team possible allow access only to certain people during certain times. Even if the head accountant wanted to steal money, we need to make it impossible for it to happen.
  + Defense in depth is the concept of more than one line of defense. Having just a password doesn’t cut it anymore, even the most complex password still just isn’t enough. Defense in depth is using an entire list of security defenses to stop attacks.