Date: 01-12-2022

DevOps in-class assignment

I want each one of you to do some online research and select one real industry case study where operational and software security has failed and about the consequences of such failures. Analyze the root causes and understand in-depth reasons for failure and present it in class. (don’t send me your answers)

\*Select a Company and note down the points and you can present them (verbally) in the class in live.

Note: Don’t choose Rogers outage issue as we already discussed in class. Think out of the box. 

The software security failure I choose was actually against the internet. Back in the 80s, you know, the internet was new, there was only around 60,000 computers connected to the internet and in 1988, which was the year of when this attack took place, the use of computers, especially programming wasn’t very familiar in the US. So, the attack was called The Morris Worm, named from its creator, a Cornell University computer science student Robert Tappan Morris. So, on November 2, 1988, the day computer science lost its innocence, he rapidly infected an estimated of 6,000 machines, which was a lot in that day. The worm depleted itself throughout these computers and shut them down completely, made them inoperable. This was actually one of the most costly software bugs ever that was caused by a single student. In perspective, the internet was as much has a hazardous territory as it was mostly for learning and doing back then, less security means easier holes, the internet was a lot more vulnerable.

But the funny thing is that the attack wasn’t meant for malicious intent people say, but kind of was. What happened was Robert Morris, was interested to learn the potential and limitations of computers. He developed his self-replicating program to test the boundaries of the network, a sort of penetration testing. He concealed his activities by hacking into the MIT (Massachusetts Institute of Technology) network to launch his worm, attempting to cover his tracks somehow. A friend of his, accounts say, tipped off The New York Times saying there was a worm separating through the internet and giving them Morris’s initials, he paid a price for his actions. In 1989, the first to be indicted under the US Computer Fraud and Abuse Act (CFAA), he was sentenced to a fine of $10,000 plus costs of his supervision, three years of probation, and 400 hours of community service, although the cost of the mess he created was estimated to be as high as $10 million. You can also say that this was the first DoS (denial-of-service) attack ever, they didn’t call it that back then, but it was actually the first internet worm because it goes from to computer to computer.

Years later, history has forgiven Morris though, with the attack now widely credited for exposing a vulnerability and improving digital security. These days, Morris is a professor at MIT, which is the place/network he hacked, and the worm’s source code has been kept at the University of Boston as a museum piece on a floppy disc. Funny how things can turn out.

It kept running through computers until they eventually captured one of the programs and found out how to stop it, the program was also only 99 lines of code of caused chaos.

Back then with the internet being new everyone worked together as academics trying to get the internet to work, solving problems, helping each other and stuff. It was a free nice open culture, but this changed it in a big way, was a wakeup call for the internet and started to get more serious about security.