Cybersecurity Research

T-Mobile recently had a data breach that exposed personal information of over 47-million people. The investigation is still currently ongoing but this isn’t the first time where T-Mobile has had a data breach. In fact, T-mobile has had several data breaches dating all the way back since 2018. These breaches have included personal information such as social security numbers, driver’s license numbers, phone numbers, and billing addresses that can be used against the customer. Furthermore, the breach was used to sell user’s information for a price tag of $270,000 on an online forum. The motivations were pretty clear that the hacker just wanted money and didn’t care who would get affected from such information being leaked. Based on the articles, hackers tend to usually attack companies with a lot of consumer data. This leads to them trying to hack T-Mobile’s servers in order to retrieve such data. T-Mobile has said that they’ve been able to close the illegal entrypoint that the hacker was able to get into. T-Mobile has tried in the past to tighten their security and also be transparent with their customers by making sure they know what is going on. One strategy that T-Mobile is bringing in, is to make sure that the technology that they use is tested and reassured for safety and implementation. They have a zero trust posture where they don’t trust anything from the inside and outside. This means that they have to verify anything and everything before users can be granted access to sensitive info.