The Objectives Of Policy Makers

Posted on May 13, 2020

In organizations where information is a critical asset, it is required to define some rules and regulations to protect the information assets from unauthorized access. The policymakers of such organizations should define cybersecurity objectives and establish a regulatory framework. The policy makers should properly analyze the organizational environment and operations and then define the objectives as it is the backbone of the bill. It is the responsibility of policy makers to take into account the threats, vulnerabilities and risks related to ICT infrastructure and to make policies accordingly. The policies should be strong enough that while adopting them, the risks and threats would be minimized. The policies reflect the organization's overall approach towards the business operations and related risks. (Pascoe et al., 2024)

Limitation To Vehicle Cybersecurity:

Although there has been no such malicious cyber attack on autonomous vehicles till now, the real danger was seen when two hackers tried to access the jeep and intended to remotely control it. They succeeded and interrupted its transmission halfway. It was done for research purposes. However, this shows that autonomous vehicles are vulnerable, and hence, they need to adopt strategies and mitigate such risks.

One of the major limitations of cybersecurity is because of the numerous electrical components present in the car, which are connected through the internal network. If the hackers succeeded in accessing the Bluetooth or infotainment system of the car, then they will definitely succeed in gaining control of the critical components such as brakes or engines.

Autos today have up to 100 ECUs and in excess of 100 million lines of code — an enormous assault surface. Additionally confusing issues, car producers source ECUs from a wide range of providers, implying that nobody player is responsible for, or even acquainted with, the greater part of a vehicle's source code.

The risk of car cyberattacks will just increasingly pose a threat as society advances to independent vehicles. In any case, even before self-governing vehicles end up boundless, auto hacking is as of now an undeniable threat: In 2014, the greater part of the vehicles sold in the United States were associated, implying that they are powerless against cyberattacks.

Steps To Improve Cybersecurity In Autonomous

Cars:

A standout amongst other approaches to shield associated autos from this developing risk is by building security into the outline of the vehicles. This implies, for instance, guaranteeing that there are no contentions, blunders or misconfigurations in singular segments. Completely amassed autos ought to be tried all the more thoroughly to guarantee the last item lives up against security hacks, utilizing strategies, for example, penetration testing, whereby frameworks are deliberately assaulted to uncover flaws. This thusly would mean better instruments and measures that would drive everybody in the business to factor in security appropriately from the beginning. (National Highway Traffic Safety Administration, 2022)

The following enormous test is probably going to outline vehicles that match security with well-being. As self-driving innovation develops to utilize more computerized reasoning and profound learning systems, we will depend on yet more programming to control our autos and settle on choices on security grounds as human drivers would. This will make it much more essential that the autos are secure so they additionally ensure drivers' well-being.

FISMA:

FISMA defines policies related to IoT. But its policies are not enough for the "Internet of things" (IoT). FISMA directs NIST to establish guidelines and standards to maintain the security of IT-related infrastructure. FISMA defines steps that will move the organization toward NIST compliance. NIST has well-structured policies related to IoT, which include policies related to the cybersecurity of autonomous vehicles. By following those policies organizations can ensure security in their IoT's.

References

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29 https://doi.org/10.6028/NIST.CSWP.29

National Highway Traffic Safety Administration. (2022). Cybersecurity best practices for the safety of modern vehicles. https://www.nhtsa.gov/automated-vehicles-safety/published-reports-and-documents