Cybersecurity concerns grow as e2Ws gain pace

ANJALI SINGH
Mumbai, 11 September

As the electric two-wheeler (e2W) market continues to gain momentum, manufacturers are increasingly turning their lens on the critical aspect of cybersecurity.

With the potential for hackers to gain unauthorised access to vehicles and sensitive data, companies like Ather Energy, Ola Electric, Kabira Mobility, and GT Force are taking steps to safeguard their products and customer information.

Ather Energy, in its recent Draft Red Herring Prospectus (DRHP), highlighted the potential risks associated with cybersecurity breaches. The firm acknowledged the possibility of unauthorised access to its systems, which could lead to significant consequences, including legal claims, brand damage, and disruptions to operations. To mitigate these risks, Ather Energy has implemented security measures and continuously monitors its networks for vulnerabilities.

ON THE DEFENSIVE

ATHER ENERGY
Implemented security measures and is monitoring its networks for vulnerabilities

OLA ELECTRIC
Invested in insurance policies to cover potential losses arising from cyberattacks

KABIRA MOBILITY
Integrated tamper-resistant hardware security modules

Ola Electric has addressed cybersecurity concerns in its DRHP. It has invested in insurance policies to cover potential losses arising from cyberattacks, but it recognises that such coverage may not be sufficient for all eventualities. It acknowledged the risk of uninsured liabilities, which could impact its financial condition and operational stability.

"The electronics and software components of vehicles are rapidly increasing, driving features like engine management, ADAS, and automated functions. While this offers more comfort, it also raises significant cybersecurity concerns. Two-wheeler makers need to prioritise hardware and software security measures to protect their products and customer data," Anurag Singh, MD at Primus Partners, said.

Kabira Mobility, another E2W manufacturer which sells around 500-600 units per month, is taking steps to ensure the safety of its E2Ws. It is focusing on hardware and software security measures. "We have integrated elements such as tamper-resistant hardware security modules in our E2Ws to protect sensitive data by using physical unclonable functions for unique device identification. We are implementing secure boot processes to ensure the integrity of the vehicle's software," said Akash Siwach, chief technology officer, Kabira Mobility.

More on business-standard.com