DAWN

10th September, 2020

Sumaira Jajja

K-Electric struck by 'ransomware'

KARACHI: K-Electric on Wednesday said it experienced an attempted cyber-incident earlier this week. "The KE teams have initiated consultation with international information security experts and are also collaborating with local authorities in this regard," the company said in a statement.

The admission came days after customers across the city complained that they were unable to lodge power outage and technical fault complaints using 118 helpline, 8119 SMS service and KE Live App or check the company's website for duplicate bills.

On Tuesday, KE had issued a statement telling customers to expect disruptions to some online services but made no mention of the "cyber-incident".

Hacked

"All critical customer services including bill payment solutions and 118 call-centre are operational and fully functional, to ensure the integrity of our systems, as a precautionary measure, we have isolated few non-critical services.

Some services frozen but power supply unaffected; hackers demand $3.8m ransom to unfreeze

As such customers may experience some disruption in accessing duplicate bills from the KE website," the statement released on Wednesday said.

Word of the hack was already in widespread circulation by the time the utility officially acknowledged it. An information security and technology news publication 'BleepingComputer' published a story on Tuesday with the headline 'Pakistan's largest private electricity provider, K-Electric, hit by Netwalker ransomware'.

Ransomware is a relatively recent form of hacking in which the attackers insert malicious code into a computer that encrypts all the data in the system. They then demand payment via online platforms in return for providing the decryption key.

The report said that Netwalker is demanding $3.8 million ransom and if payment is not made in seven days, the ransom will increase to $7m.

BleepingComputer is a partner in the No More Ransom Project which was started in 2016 as an alliance between Europol's European Cybercrime Centre, the National High Tech Crime Unit of the Netherlands police, and McAfee in order to battle ransomware.

When reached out, the report's author, Lawrence Abrams told Dawn, "it is not known how much or what files were stolen before encrypting K-Electric's systems." His report says the attack seems to have happened on Monday.

"As K-Electric is exhibiting actual disruptions to their online services and billing, my guess is that they had at least some devices encrypted."

What's at risk?

Though KE has not shared details of the attempted hack and adds that it is following cybersecurity protocols, concerns remain on whether any data was leaked, and if so whether it was encrypted.

Tech experts say that currently, there is no redressal mechanism in the country for such data breaches — that have happened in the past as well — leaving consumers at a greater risk.

"When a data breach happens, it is worth asking if the data encrypted and what has been leaked," said Shahzad Ahmed, director Bytes For All — NGO that works on technology and human rights.

The draft Pakistan data protection bill is there but it does not offer adequate protection of citizens in case of data breaches, he added.

KE has access to consumers' names, addresses, CNIC and NTN numbers — information that is also published on bills — some more if you pay bills online.

"Financial data is linked to your CNIC (including with bank accounts, credit card). Many consumers pay their bills online. This is sensitive information. NIC details can reveal date of birth, your mother's name (in records) and place of birth. This makes you more vulnerable. If any point hackers [in any data breach] are not given ransom, they can sell this to dark web and this can have repercussions."