Publication – The Economic Times

ET THE ECONOMIC TIMES

As India steps towards increased digital dependency, the importance of cybersecurity comes into the forefront. The sector is thus coming up with several new technologies to make the space safer. Here are a few key ones

Technologies to make your online experience safer in 2023

POOJA.MAHIMKAR
@timesgroup.com

According to PwC's Global Digital Trust Insights – India Edition survey, organisations across the globe have expressed concerns regarding increased cyber threats in 2023. 65 per cent of surveyed business executives feel cybercriminals will significantly affect the organisation in 2023 compared to 2022. In India, cloud-based pathways (59 per cent) and the Internet of Things (58 per cent) are the top areas of concern, followed by mobile devices and software supply chains (54 per cent). It is thus quite evident that new security paradigms are required to secure the virtual space. Here are some steps, which could play a significant role in the next few years.

➤ Understanding user behaviour

Behavioural analytics is one such technology making cyberspace more secure. "It uses AI and machine learning for a real-time, cognitive approach for fraud detection. Behavioural analytics can help seamlessly authenticate users by building models based on patterns of mouse movements, keyboard typing, and mobile touch-screen swipes in real time," explains Tushar Haralkar, IBM security software, technical sales leader, India / South Asia Region. This understanding of behavioural patterns helps detect potential threats as well as predict any future attacks. For example, it may find that unusually large amounts of data are coming from one device. This may mean a cyberattack is looming or actively happening. Other indicators of malicious activity include odd timing of events and actions that happen in an unusual sequence.

"As newer, more sophisticated cyber attacks try to overcome existing protection, it is crucial to mount layered defences, covering different levels of infrastructure and applying multiple protection layers of varied nature to every protected asset," says Dipesh Kaura, GM, South Asia Kaspersky.

➤ Heightened verification process

According to a report by Nord Security's password manager arm NordPass, 'password' is still the most common password used. Followed by "123456" and "12345678". This shows how vulnerable our personal data is. Traditional cybersecurity technologies provide access once we enter our username and password. However, the biggest challenge in a virtual world is that it is difficult to determine if it is a stolen credential or a legitimate user. "Instead of relying on just username and password or OTP, context-aware security uses machine learning and AI to analyse key parameters like the user, device, activity, environment, and behaviour in context to determine holistic risk scores," adds Haralkar.

"Two-factor authentication, i.e. a password together with a generated key, is now commonplace. Biometric authentication is also becoming more prevalent as mobile app usage grows," adds Abhinanda Sarkar, academic director, Great Learning.

Payment/digital frauds are also on the rise, while banks and financial institutions are doing their bit to secure their apps and websites; consumers too need to keep up and educate themselves on how to be safe online. "In this digital era where customer experience and ease of transaction have taken centre-stage, the challenges associated with fraud are increasing every day. The industry is thus working towards making apps safe and secure for the users," says Bipin Preet Singh, founder and CEO, MobiKwik.

➤ Cloud safety is important

As work-from-home (WFH) becomes a norm now across the globe, cloud has become a key component. Cloud encryption is thus seeing an increased demand to secure data across the virtual world. "Cybersecurity professionals use a mathematical algorithm to complete cloud encryption. Only authorised users with an encryption key can unlock the code, making data readable again. This restricted access minimises the chance of data breaches by unauthorised attackers," informs Haralkar.

"With digital taking the cloud-native route, Secure Access Service Edge (SASE) offers a secure way to connect users, systems, and endpoints to applications and services anywhere. It enables Zero Trust Network Access and brings cloud-native security technologies together with Wide Area Network (WAN) capabilities. It not only monitors the identity of a device or entity, but also combines it with real-time context, security, and compliance policies to avoid hampering the user experience," explains Srikanth Chakkilam, CEO and non-executive director, Cigniti Technologies Limited.

➤ Blockchain on the horizon

"Based on the principles of decentralisation and cryptography, blockchain can have a potentially revolutionising impact on the security architecture. While there is still a lot to uncover in terms of blockchain's capabilities, a few blockchain cybersecurity cases could be device-to-device encryption for IoT, protecting data transmission, DNS protection, and preventing DDoS attacks. As the decentralised structure eliminates single-point failures, blockchain may become the default cybersecurity technology for everyone in the coming years," says Chakkilam.