Source : www.thehindu.com Date : 2023-02-25

CYBERATTACKS ARE RISING, BUT THERE IS AN IDEAL PATCH

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

February 25, 2023 12:08 am | Updated 01:13 am IST

‘With most cyberattacks originating from beyond India’s borders, international cooperation would be critical to keep India’s digital space secure’ | Photo Credit: Getty Images/iStockphoto

The past few weeks have highlighted the soft underbelly of our fast expanding digital networks. The first was the ransomware attack on the servers of India’s premium institute, the All India Institute of Medical Sciences. Nearly 40 million health records were compromised and it took over two weeks for the systems to be brought online. Soon afterwards, a ransomware gang, BlackCat, breached the parent company of Solar Industries Limited, one of the Ministry of Defence’s ammunition and explosives manufacturers, and extracted over 2 Terabyte of data.

Ransomwares have emerged as the most predominant of malicious cyberattacks. Here, the perpetrators demand hefty payments for the release of withheld data. Data show that over 75% of Indian organisations have faced such attacks, with each breach costing an average of 35 crore of damage. There are other malwares that could infect all kinds of computer systems. With the lines between the physical and digital realms blurring rapidly, every critical infrastructure, from transportation, power and banking systems, would become extremely vulnerable to the assaults from hostile state and non-state actors.

Cyber capabilities are also playing a pivotal role, as seen in the ongoing conflict in Ukraine, where electronic systems in warheads, radars and communication devices have reportedly been rendered ineffective using hacking and GPS jamming. With cyber threats capable of undermining our critical infrastructure, industry and security, a comprehensive cyber security policy is the need of the hour.

In 2022, the Indian Computer Emergency Response Team (CERT-In), which is India’s cybersecurity agency, introduced a set of guidelines for organisations to comply with when connected to the digital realm. This included the mandatory obligation to report cyberattack incidents within hours of identifying them, and designating a pointsperson with domain knowledge to interact with CERT-In. India’s draft Digital Personal Protection Bill 2022 proposes a penalty of up to 500 crore for data breaches. Recently, India’s armed forces created a Defence Cyber Agency (DCyA), capable of offensive and defensive manoeuvres. All Indian States have their own cyber command and control centres.

However, most organisations lack the tools to identify cyberattacks, let alone prevent them. India

also faces an acute scarcity of cybersecurity professionals. India is projected to have a total workforce of around 3,00,000 people in this sector in contrast to the 1.2 million people in the United States.

Most of our organisations are in the private sector, and their participation remains limited in India's cybersecurity structures. They would be advised to look at the Digital Geneva Convention, where over 30 global companies have signed a declaration to protect users and customers from cyber breaches, and collaborate with like-minded intergovernmental and state frameworks. With the introduction of 5G and the arrival of quantum computing, the potency of malicious software, and avenues for digital security breaches would only increase. India's cybersecurity strategy would do well not to overlook these actualities and trends.

With most cyberattacks originating from beyond our borders, international cooperation would be critical to keep our digital space secure. It would also be a cause which would find resonance abroad. This year, cybercrimes are expected to cause damage worth an estimated $8 trillion worldwide. India has already signed cybersecurity treaties, where the countries include the United States, Russia, the United Kingdom, South Korea and the European Union. Even in multinational frameworks such as the Quad and the I2U2 (which India is a member of) there are efforts to enhance cooperation in cyber incident responses, technology collaboration, capacity building, and in the improvement of cyber resilience. Yet, there is no truly global framework, with many operating in silos.

Also read | **Cyberattacks on Indian healthcare industry second highest in the world: CloudSEK**

Previous years have seen the United Nations General Assembly establish two processes on the issues of security in the information and communication technologies (ICT) environment. One is the Open-ended Working Group (OEWG), comprising the entire UN membership, established through a resolution by Russia. The other is the resolution by the U.S., on the continuation of the Group of Governmental Experts (GGE), comprising 25 countries from all the major regions. The two antagonistic permanent members of the UN Security Council, counted among India's most important strategic partners, differ vastly on many aspects of the Internet, including openness, restrictions on data flow, and digital sovereignty. Yet, based on adoption, member-states have found the two resolutions to be complementary, and not mutually exclusive. Amidst the turbulent current world events, these UN groups would struggle to have effective dialogues.

The G-20 summit this year in India, which will see participation by all the stakeholders driving the global levers of power, is a rare opportunity to bring together domestic and international engagement groups across the spectrum, and steer the direction of these consultations. India could make an effort to conceptualise a global framework of common minimum acceptance for cybersecurity. This would be one of the most significant contributions made by any nation towards collective security in modern times.

Anil K. Antony is a technology entrepreneur, and a Munich Young Leader, 2023, Korber Stiftung and Munich Security Conference. Tweets@anilkantony

Comments have to be in English, and in full sentences. They cannot be abusive or personal. Please abide by our community guidelines for posting your comments.

We have migrated to a new commenting platform. If you are already a registered user of The Hindu and logged in, you may continue to engage with our articles. If you do not have an account please register and login to post comments. Users can access their older comments by logging into their accounts on Vuukle.

END