Source : www.thehindu.com Date : 2022-02-12

TAKING A BYTE OUT OF CYBER THREATS

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

Cyber attacks may be a relatively new phenomenon, but in a short time frame have come to be assessed as dangerous as terrorism. The world was possibly made aware of the danger and threat posed by cyber weapons with the advent of the Stuxnet Worm in 2010, which resulted in large-scale damage to Iran's centrifuge capabilities. Two years later, in 2012, a bank of computers belonging to the Saudi Aramco Oil Company were targeted, reportedly by Iranian operatives, employing malware that wiped out data on 30,000 computers. A few weeks later, Iran was again believed to have been behind a targeted attack on the Qatari natural gas company, RasGas. The string of instances appear to have provoked then United States Defence Secretary, Leon Panetta, to utter the warning that the world had to prepare for a kind of 'cyber Pearl Harbour', highlighting a new era of potential vulnerabilities.

In the decade that followed, and while preparing for a 'potential Pearl Harbour' type of strike, including seeking ways and means to retaliate in the eventuality of such attacks, the West seemed to lose its way on how to deal with the emerging cyber threat. Each succeeding year, despite an increase in cyber threats, witnessed no change in the method of response. The years 2020 and 2021 have proved to be extremely difficult from the perspective of cyber attacks but no changes in methodology have been seen. In 2021, cyber attacks that attracted the maximum attention were SolarWinds and Colonial Pipeline in the U.S., but these were merely the tip of a much bigger iceberg among the string of attacks that plagued the world. Estimates of the cost to the world in 2021 from cyber attacks are still being computed, but if the cost of cyber crimes in 2020 (believed to be more than $1 trillion) is any guide, it is likely to range between $3trillion-$4 trillion. What is not disputed any longer is that soon, if not already, cyber crime damage costs would become more profitable than the global trade of all major illegal drugs combined.

As 2022 begins, the general consensus is that the cyber threat is likely to be among, if not the biggest, concern for both companies and governments across the globe. In the Information age, data is gold. Credential threats and the threat of data breaches, phishing, and ransomware attacks, apart from major IT outages, are expected to be among the main concerns. Results are also likely to far eclipse the damage stemming from the COVID-19 pandemic or any natural disasters. A little publicised fact is that the vast majority of cyber attacks are directed at small and medium sized businesses, and it is likely that this trend will grow.

According to experts, among the most targeted sectors in the coming period are likely to be: health care, education and research, communications and governments. Health-care ransomware has been little publicised, but the reality is that ransomware attacks have led to longer stays in hospitals, apart from delays in procedures and tests, resulting in an increase in patient mortality.

Far more than merely apportioning costs linked to cyber crime is the reality that no organisation can possibly claim to be completely immune from cyber attacks. While preventive and reactive cyber security strategies are needed — and are essential to mitigate cyber risks — they are proving to be highly illusive in an increasingly hyper-connected world. Comprehending the consequences of this reality could be devastating.

For instance, despite all talk about managing and protecting data, the reality is that ransomware is increasing in intensity and is tending to become a near destructive threat, because there are many available soft targets. Statistics in this regard are also telling, *viz.*, that new attacks are taking place every 10 seconds. Apart from loss of data, what is also becoming evident is that

ransomware criminals are becoming more sophisticated, and are using ransomware to cripple large enterprises and even governments. Talk of the emergence of ‘Ransomware as a Service’ (RaaS) — a business model for ransomware developers — is no mere idle threat.

The huge security impact of working from home, dictated largely by the prevailing novel coronavirus pandemic, must again not be underestimated as it is likely to further accelerate the pace of cyber attacks. A conservative estimate is that a rash of attacks is almost certain to occur on home computers and networks. Additionally, according to experts, a tendency seen more recently to put everything on the Cloud could backfire, causing many security holes, challenges, misconfigurations and outages. Furthermore, even as Identity and Multifactor Authentication (MFA) take centre stage, the gloomy prognostication of experts is that Advanced Persistent Threats (APT) attacks are set to increase, with criminal networks working overtime and the Dark web allowing criminals to access even sensitive corporate networks.

Unfortunately, and despite the plethora of such evidence, cyber security experts appear to be floundering in finding proper solutions to the ever widening cyber threat. There is a great deal of talk among cyber security experts about emerging cyber security technologies and protocols intended to protect systems, networks and devices, but little clarity whether what is available can ensure protection from all-encompassing cyber attacks. Technology geeks, meanwhile, are having a field day, insisting on every enterprise incorporating SASE — Secure Access Service Edge — to reduce the risk of cyber attacks. Additional solutions are being proposed such as CASB — Cloud Access Security Broker — and SWG — Secure Web Gateway — aimed at limiting the risks to users from web-based threats. Constant references to the Zero Trust Model and Micro Segmentation as a means to limit cyber attacks, can again be self-limiting. Zero Trust does put the onus on strict identity verification ‘allowing only authorized and authenticated users to access data applications’, but it is not certain how successful this and other applications will prove to be in the face of the current wave of cyber attacks. What is most needed is absent, *viz.,* that cyber security experts should aim at being two steps ahead of cyber criminals. This is not evident as of now.

Missing from the canvas is that cyber technology presents certain unique challenges which need particularised answers. Instead of attempting to devise standard methodologies, and arrive at certain international norms that govern its use, a decade of misplaced effort by the West in preparing for a ‘potential Pearl Harbour type of strike’ has enabled cyber criminals to gain the upper hand. While the West focused on ‘militarization’ of the cyber threat, and how best it could win with its superior capabilities, valuable time was lost. It led to misplaced ideas and erroneous generalisations, resulting in a decade of lost opportunity.

This situation needs to be reversed. A detailed study of the series of low- and medium-level proactive cyber attacks that have occurred during the past decade is clearly warranted. It could reinforce the belief that when it comes to deterrence in cyber space, what is required is not a piece of ‘grand strategy’: low and medium tech, low and medium risk targeted operations could be just as effective. A related aspect is to prevent individual companies from attempting their own tradeoffs — between investing in security and maximising short-term profits. What many companies and even others fail to realise is that inadequate corporate protection and defence could have huge external costs for national security, as was evident in the SolarWinds attack.

Nations and institutions, instead of waiting for the ‘Big Bang cyber attack’, should actively prepare for a rash of cyber attacks — essentially ransomware — mainly directed at available data. The emphasis should be on prioritising the defence of data above everything else. Consequently, law enforcement agencies would need to play a vital role in providing effective

defence against cyber attacks.

On the strategic plane, understanding the nature of cyber space is important. While solving the technical side is ‘one part of the solution, networks and data structures need at the same time to prioritise resilience through decentralised and dense networks, hybrid cloud structures, redundant applications and backup processes’. This implies ‘planning and training for network failures so that individuals could adapt and continue to provide service even in the midst of an offensive cyber campaign’.

The short answer is to prioritise building trust in systems — whether it is an electrical grid, banks or the like, and creating backup plans including ‘strategic decisions about what should be online or digital and what needs to stay analog or physical, and building capacity within networks to survive’ even if one node is attacked. Failure to build resilience — at both the ‘technical and human level — will mean that the cycle of cyber attacks and the distrust they give rise to will continue to threaten the foundations of democratic society’. Preventing an erosion of trust is critical in this day and age.

M.K. Narayanan, a former Director, Intelligence Bureau, a former National Security Adviser and a former Governor of West Bengal, is currently Executive Chairman of CyQureX Pvt. Ltd., a U.K.-U.S.A. cyber security joint venture

Our code of editorial values

END