By Akanksha Mahajan Marwah

Given the recent trends in cyberspace, it is imperative that organisations build defences that can withstand increasingly sophisticated cyberattacks. Enterprises are increasingly transitioning to intelligence-driven security for a broader view of cyberrisks and vulnerabilities. However, there are certain industry verticals which are at far greater risk than others in a situation of cybersecurity compromise, owing to the sensitivity of their data, the business domain, etc. Thus, it becomes imperative, in the face of the dynamic cyberthreat landscape, that enterprises across verticals strengthen their security systems and make them as impenetrable as possible. They must focus on preventive measures and undertake monitoring at regular intervals.

tele.net takes a look at some of the highly vulnerable critical infrastructure segments targeted by cyberattacks…

Smart cities

Digital technology lies at the heart of a smart city. Advanced technologies such as IoT and sensors, coupled with the traditional information technology and operational technology systems, power smart cities to provide a higher quality of living to residents. These technologies are distributed across the entire smart city network and work in an integrated manner to generate intelligent and actionable information.

However, the use of technology in a city-like set-up widens the threat surface for cyberattacks. Devices and machines, interconnected over a network, generating and exchanging massive volumes of data, are a hotbed for miscreants and hackers continuously looking to exploit inappropriately secured endpoints.

Globally, several smart cities have faced an onslaught of cyberattacks in recent years, with such attacks becoming more sophisticated and intense over time. From loss of health data to complete network lockdown, these attacks have attempted to cripple smart cities. For instance, in Atlanta, attackers encrypted files which resulted in employees getting completely locked out of the smart city network. It is reported that the cyberattack destroyed significant volumes of police dash cam video footage. In another incident, hackers targeted Singapore-based healthcare institution SingHealth and stole the personal profiles of about 1.5 million patients

along with the details of prescriptions for 160,000 others. Estonia suffered a series of cyberattacks in which attackers penetrated and brought down key government websites, rendering them redundant. A number of techniques such as ping floods and botnets were deployed by attackers. In Sweden, a series of DDoS (distributed denial of service) attacks caused train delays and disrupted travel services.

Given that smart cities mostly comprise critical infrastructure, any compromise in cybersecurity can prove extremely risky. To this end, cybersecurity solutions and strategies need to be looked at right from the inception of a smart city. Globally, smart cities have launched cybersecurity strategies modelled around effective regulations, industry collaborations and capacity building initiatives.

The Government of India too looks committed to creating safe and secure smart cities, and has formulated a number of policies and regulations to protect smart city infrastructure from cyberattacks. The Ministry of Housing and Urban Affairs, in May 2016, had released a model framework for cybersecurity in smart cities. It covered the security of smart cities across different layers – sensor, communication, data and application.

The technology ecosystem powering smart city services in the country is highly prone to vulnerabilities, which can lead to potential social, health, economic and/or reputational risks. There is an urgent need to evaluate the existing cyber risk landscape for smart cities and ensure secure and uninterrupted transmission of data over a wide and complex network.

Energy and utility

The energy and utility sectors are undergoing significant digitalisation and modernisation with the emergence of smart grids and smart devices, which are making this critical infrastructure an attractive target for cybercriminals. These attacks can result in infrastructure shutdowns, causing economic, financial and environmental damage. Also, most utility companies have consumer details and billing information stored in their systems which can also be compromised.

Grid modernisation potentially opens up the power sector to more vulnerabilities. For instance, in September 2018, officials in Connecticut found there had been millions of attempts to hack

the state utilities' networks over the past year, although all intrusions were successfully prevented. Later, in October 2018, Russian military officials were indicted for hacking-related charges, including allegedly trying to steal login credentials from the Westinghouse Electric employees involved in advanced nuclear reactor development.

While energy companies do invest time and money in deploying network monitoring services such as antivirus, security alert software and firewalls, most of these are siloed solutions designed to fix particular issues. Gaps in siloed solutions are often the entry points for potential cyberattacks. The need of the hour is to look for solutions that are best for overall system security. To this end, energy companies can look to partner with managed service providers.

Industry 4.0

Technology-related risks in manufacturing have existed right from the time production systems were mechanised, but these threats have become more intense with the advent of Industry 4.0, which is essentially powered by digital technologies. The Industry 4.0 ecosystem combines and interconnects physical infrastructure such as supply chains and factories with customers and operations through the use of relevant digital technologies such as IoT, analytics, robotics, additive manufacturing, cognitive technologies, and augmented reality. As the traditional linear supply chain evolves with the introduction of intelligent, connected platforms and devices, it brings with it cyber weaknesses that must be overcome to prevent significant risks.

Currently, "compliance" represents the minimum security level in most organisations. However, they do not strive to achieve full security across the breadth of technologies in use, thus, provoking disruptors to look for the weakest points to gain successful entry into an organisation's systems. This challenge is likely to grow bigger as vast numbers of devices get connected under a smart factory set-up.

There is an urgent need to address cyberrisks in the manufacturing industry landscape with a secure, vigilant and resilient response strategy to capture the business value that Industry 4.0 has to offer.

Financial services

As per industry experts, the financial sector faces almost three times the number of cyberattacks as compared to other industries. Data breaches take place both internally through fraud and externally through cybercriminals. Owing to the sensitive and confidential nature of consumer data, data privacy and cybersecurity have become crucial for the efficient functioning of enterprises in the banking, financial services and insurance space. Also, given the sustained increase in digital transactions by customers, cybersecurity and customer data protection are emerging as priorities for banks.

It is imperative for organisations in the financial services space to step up investments for bolstering the security of their networks and to plug loopholes. In addition to the traditional layers of security at the network, perimeter and data centre levels, systems based on big data analytics and AI can be deployed to monitor and safeguard the information of stakeholders.

Healthcare

Technology has emerged as a boon for the healthcare sector, as it is helping hospitals improve the overall patient experience through online portals, connected medical devices and wearables, and long-distance/ remote consulting with doctors across the globe. However, such interconnected networks and devices are most vulnerable to cyber risks. These devices are often programmed to access classified information stored on hospital networks, and can easily offer an entryway into healthcare networks to cybercriminals.

During the past two years, there has been a sharp increase in the number and intensity of ransomware attacks in the healthcare sector. Security measures, thus, have become essential for protecting patients' privacy and critical infrastructure, as downtime can actually put lives at risk in a hospital.

Conclusion

While the internet has been around for several years now, interconnectivity has mostly impacted personal and professional lives, and not so much the industrial control systems, which underline critical infrastructure. Industrial control systems have traditionally remained isolated from the

internet. However, the industrial world is now steadily moving towards an era of connected everything, creating the demand for safeguarding critical infrastructure and the systems that operate it.

About Us We are Hiring Contact Us

Subscribe Privacy Policy Advertise Terms & Conditions

Copyright © 2010, tele.net.in All Rights Reserved