There are several aspects to telecom network security. Internally, misconfigurations and insecure coding practices render telecom and IT infrastructure vulnerable, and externally, telecom companies face issues like cable and diesel theft. The equipment used for setting up the telecom network is another key area of concern.

Telecom operators as well as other large enterprises are following a moat-and-castle approach to ensure security. Network security elements like firewalls and intrusion detection systems are used to defend internal assets from threats from third-party interconnected networks. System security elements such as antivirus and content filtering are deployed for mitigating risks from viruses, spyware and trojans.

As far as equipment is concerned, the government has been insisting on rigorous telecom equipment security procedures. Communication breaches in the past have prompted such action. Moreover, some government agencies have raised concerns about malicious software in foreign equipment that could pose a threat to national security. Thus, in June 2011, the Department of Telecommunications tightened the rules for telecom equipment, holding service providers responsible for any security breach in the operators' networks. It has imposed a penalty of up to Rs 500 million for every breach in the network that arises due to telecom companies failing to take necessary precautions.

Telecom operators

To meet users' future demand for bandwidth, operators need to constantly expand their radio access networks (RANs). IP RAN, the core-IP mobile network, significantly helps in optimising 2G network architecture and implementing 3G access networks. Its usage has gained momentum in India with nine operators deploying 3G networks. However, IP RAN-bearer networks should be able to effectively prevent various kinds of attacks, viruses and frauds to ensure mobile network security and stability. In addition, it is essential to provide better connectivity on private lines and redundancy functionality for mobile services. A common example of network security breach is the denial-of-service attacks that flood the network with non-productive traffic, preventing routers and switches from properly responding to production data. Compared to non-IP RAN, IP-based RAN faces several security threats and, therefore, it is important for operators to be vigilant and deploy security solutions.

In India, almost all operators have outsourced their network operations to vendors like Ericsson, Nokia Siemens Networks, Alcatel-Lucent, Huawei and ZTE; and IT operations to companies like Wipro, IBM and Tech Mahindra. These players ensure the security of telecom operators' backhaul and access networks as well as their IT operations.

Recently, Vodafone extended its contract with IBM to manage the IT systems of Vodafone's Indian unit until 2017. The deal is estimated to cost $1 billion. In 2007, IBM had signed a contract worth approximately $600 million to manage Vodafone's IT functions. In July 2011, Bharti Airtel had awarded a 10-year contract to IBM for providing IT solutions across its operations in 16 countries in Africa. This was the second 10-year contract between the two companies over the past few quarters. In September 2010, IBM received a $1.5 billion contract from Airtel for managing its IT requirements across 16 countries in Africa. IBM also signed an outsourcing contract with Idea Cellular for $800 million.

Tech Mahindra and Wipro have contracts with some of the new players in the multi-billion dollar Indian telecom market. For instance, Tech Mahindra has a $400 million IT outsourcing deal for a period of 10 years with telecom operator Etisalat DB.

On the access side, data security is of paramount importance to users, especially for newer mobile applications like mobile payment systems and online financial transactions. Mobile operators need to determine the most efficient way to deliver new services for capitalising on consumer demand without compromising on the reliability and security of services.

Enterprise segment

While the number of operators that need to secure their networks is limited, there are a million small and large enterprises in India that need a secure communication network.

Companies today are looking for a wide range of communication technologies from virtual private networks and IP telephony to network security and remote access. Over the past one year, tele.net has surveyed a number of enterprises across various industry verticals to assess the key trends in their network security (see table). The survey showed that the most popular security solutions deployed by enterprises are access logs, proxy servers, intrusion detection and prevention systems, and firewalls. A large number of enterprises have also opted for

security audits. Smaller organisations prefer deploying and maintaining their networks and security solutions. On the other hand, larger enterprises outsource these requirements in order to reduce capital expenditure while increasing their focus on core competencies.

Managed security services (MSS), thus, represent a rapidly developing market driven by the internet's ubiquitous influence as well as the companies' need to maintain and track emails, network logs and other data.

Internet security threats today range from curious stalkers to savvy intruders, from simple pranks to espionage. Without a plan to protect the entire network and connection points, a company's defence mechanism is only as strong as its weakest link.

According to a recent research study titled "Managed Security Services: A Global Strategic Business Report", by Global Industry Analysts, expenditure on network security is expected to reach $8.4 billion by 2015.

According to Voice&Data, the network security market segment in India witnessed a growth of 21.6 per cent, with the total network security revenue touching Rs 9 billion. Next-generation services such as SaaS and hosted services like cloud computing are reducing both upfront capital expenditure as well as operating costs, thereby leading to greater adoption of MSS.

Vendors like HP, Cisco and IBM have been providing managed network security services to companies not just in India but globally as well. Operators such as Orange, AT&T and Verizon are also committed to expanding their portfolios with managed services, especially in the area of network security.

The way forward

The evolution of security solutions involves achieving the right mix of technology that is properly implemented and effectively managed. In order to effectively address these challenges, organisations will have to move beyond the constraints of obsolete approaches to security.

As more enterprises move towards cloud-based networks, a shift in mindset is required from a point-protection approach to an approach that encompasses both the premises and the extended enterprise cloud. Most importantly, the complexity of today's security requires an in-depth knowledge and understanding that only a few IT departments can claim to possess.

Moreover, with enterprises adopting 3G/BWA/LTE TD services in the near future and the growing uptake of smart devices, there is an increasing need for security services.

However, given their limited experience with security mechanisms, enterprises will increasingly opt for MSS. Thus, the increased awareness of security threats combined with the growing need to secure branch office networks, and the focus on cloud-based security services present a strong case for the growth of network and content security appliances, and the software market in India.

About Us We are Hiring Contact Us

Subscribe Privacy Policy Advertise Terms & Conditions

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