Securing digital India

Cyber threats are regarded as bloodless wars. Is India ready for them?

GN Bureau

Every day is a new day in terms of security as new threats keep emerging. In such a landscape cyber attack is going to be one of the major global risks. This was highlighted by Srikant Shitole, managing director - India, Symantec, at the 'Secure Digital India' conclave in April in New Delhi. The conference was organised by Governance Now in collaboration with Symantec.

"Globally, hackers attack sectors like healthcare, retail, education, government and financial. But in India, the government is one of the most prominent sectors under threat," Shitole said.

In order to ensure cyber security one needs to be aware about the threats first. "The more we know, the more we would be able to protect ourselves from the threat," he said. Also, by knowing the threats in advance an organisation can better prepare itself to protect its critical infrastructure and information.

Vinit Goenka, member (IT) taskforce, ministry of shipping, road transport and highways, highlighted various areas that will raise security concerns for the government, for example, smart cities and smart railways. "In India, 41 percent of e-commerce sales are done through mobile phones. With each purchase, data goes to the cloud via a mobile phone. And every time this data goes into the system there is a chance to compromise it," he said.

Highlighting the increasing cases of espionage by business competitors, he said, "As we go into tomorrow's market, the boundaries of ethics and morals are getting blurred. Competitors are trying to destabilise their counterparts. The future war will be digital." However, he said, a right blend of people, processes, and technology can help address such cyber threats.

Vinit Goenka¸ member (IT) taskforce, ministry of shipping, road transport & highways

Shrikant Shitole, managing director - India, Symantec

The session on 'Secure Digital India' was moderated by Vikas Aggarwal, executive director, Ernst & Young. Various panellists deliberated upon how India must take the lead in cyber security through innovation. Intense government and industry interactions were held during the session for development of advanced and intelligent solutions for securing the cyber space.

Rudra Murthy KG, chief information security officer - digital India, ministry of home affairs, admitted that the country is not yet fully ready to deal with various kinds of cyber attacks. "Security should be part of every principle of Digital India," he said. But lack of trained human resource in cyber security is a big challenge. "The way technology is evolving, the current human resource is not able to adapt and move to the next version," he added.

Loknath Behra, director general, Kerala Fire and Rescue Services, said that the government should not take help of the private sector in investigating cyber crimes. "We need to figure out the actual readiness of our police system to investigate these kinds of applications." He highlighted this lacuna by giving an example. Recalling the Delhi high court blast of 2011, he said, "We received some evidence from a computer in Kashmir. But in transit the hard disk broke. I went from Kanyakumari to Kashmir to retrieve information from that broken hard disk but could not. Ultimately, we got permission to send it to the FBI in San Diego, US, and they recovered the data." This incident clearly highlights that the states lack infrastructure, human resources and training.

Moreover, a right kind of framework is also needed to make the country cyber secure. "We need robust IT laws so that judiciary plays a key role to create right kind of judicial framework," said Alok Vijayant, director (cyber security), NTRO.

In the process of providing government services under the umbrella of Digital India, issues of security cannot come as an afterthought. "It should not be implemented at the later stage.

(L-R) Rudra Murthy KG, chief information security officer - Digital India, ministry of home affairs; Vijay Devnath, general manager (infra & security) & CISO, CRIS; Alok Vijayant, director (cyber security), NTRO; Vikas Agarwal, executive director, Ernst & Young; Sanjiv Mittal, CEO, NiSG; Loknath Behera, director general, Fire and Rescure Department, government of Kerala; Ravi Vijayvargiya, DDG (network security), NIC; Atul Anchan, systems engineer - manager, India, Symantec.

Security must go in parallel with creation of data," Vijayant said.

He also highlighted that transferring huge amounts of data on a small bandwidth can be a challenge and can affect dissemination of some essential services. "So we have to ensure fallback options. If the normal internet does not work there should be another plan to transfer the data either by shifting non-emergency or emergency services to different network," he added.

Vijayant also noted that most of the internet service providers (ISPs) are not interested in protecting citizens from malware. "Business consideration overpowers consideration on security," he said. He suggested that such ISPs can be penalised for any kind of malware on their network. As an intermediary they have a role to play in security. "Data protection and standardisation of data structure is a major exercise," he added.

"In most of the projects typically we come across first time computerisation. Our major focus remains on how we will be able to make it work. How will the data come? Will the change that we are trying to bring in the government department happen?" asked Sanjiv Mittal, CEO, National Institute for Smart Government (NISG).

He elaborated that unless there is computerisation one cannot even think of information security. "We keep on adding layers of security with more products and tighten the whole process to ensure that we are safe. But security is not just about building firewalls. One thing that is often ignored is threat from internal sources. A study has been done which says more and more threats happen from internal sources than external ones," he said.

Mittal urged the industry experts to come out with an action plan which will take care of future requirements. He also shared that NISG is building a team – a centre of excellence for information security. "As we realise that we are in e-governance we cannot let the security exist only on papers. We have to have experts who can help various ministries and keep on upgrading year-on-year as new threats keep on getting uncovered," he said.

Ravi Vijayvargiya, senior technical director (network security), NIC, said that security threats also occur during dissemination of government services to citizens. "Most of the services which the government delivers are mostly located in the government data centres. There are sensitive applications from the health or education department, which the government is trying to deliver under Digital India. So any breach in the application will create havoc."

Concluding the conclave, Atul Anchan, systems engineer-manager, India, Symantec, said that security is an ongoing process."As attacks against business and nations hit the headlines with much regularity, it is clear that cybercriminals have evolved and use more sophisticated tactics to target governments, public sector organizations, and critical infrastructure. Hence it is imperative that security should be implanted in the design of Digital India and not as an afterthought. As the global leader in cybersecurity, Symantec is committed to securing India's critical information infrastructure, and making the 'Digital India' initiative successful." ■

feedback@governancenow.com