live **mint**

18 January 2016 | E-Paper

ENCRYPTION POLICY   BLACKBERRY   DIT   ONLINE SECURITY   ONLINE STORES

Govt to play catch up on encryption norms

Govt to play catch up on encryption norms

Sahil Makkar

First Published: Tue, Mar 27 2012. 10 53 PM IST

💬   ✉   🖨 | f Share 0   y Tweet

Updated: *Tue, Mar 27 2012. 10 53 PM IST*

New Delhi: The new encryption policy to be announced by the Department of Information Technology (DIT) will tighten online security standards and bring them on par with the encryption norms that are already being followed by many government institutions and private companies.

The move has worried law enforcement agencies that may find it harder to snoop online although it has the potential to boost e-commerce. Indians are likely to spend $84 billion on online stores by 2016, compared with the $7 billion they spent in 2010, Boston Consulting Group predicted in a report released on Monday.

The policy entails increasing the encryption norms from 40 bits to 128 bits. Bits are used to define the level of coding of a message; the more the bits, the greater is the security of an online transaction or even an email.

Entities including the Reserve Bank of India (RBI), commercial banks, insurance companies, service providers, and the Indian units of Microsoft Corp. and BlackBerry-maker Research In Motion Ltd (RIM)have already switched to a minimum encryption of 128 bits, said a high-ranking government official.

"We are proposing to increase encryption level from the present 40 bits to 128 bits in the upcoming encryption policy. This will largely legitimise use of encryption (norms) in the country," said the official, who spoke on condition of anonymity.

However, the move by the DIT is likely to face resistance from the law enforcement and security agencies on grounds of national security. Officials in the security establishment argue that India is still to develop technology to crack the encryption standard beyond 50-60 bits. "By legitimising to 128 bits, this will further add to our problems in getting lawful access to email and other messages," said an official who handles such matters in the intelligence and security agencies.

Another high-ranking government official, who independently confirmed the move to legitimise use of higher encryption, said a balance needed to be struck between the requirement of industry and security agencies.

"There are two issues that needed to be addressed. One is of the security need and other is requirement of safety and security in the transactions. We will try to strike balance between the two," said the official, adding that encryption policy will change with the passage of time. Concerns increased after the alleged misuse of services offered by RIM during the the 26/11 Mumbai terror strike that killed 166 people.

RIM offers highly secured services like BlackBerry Messenger (BBM), BlackBerry Internet Services (BIS) and BlackBerry Enterprise Server (BES) in India.

After the attack, security agencies asked RIM and other service providers for lawful and real time access to their services.

RIM subsequently gave them access to BBM and BIS but still denied access to BES on grounds that it did not have the decryption key.

The services providers were asked to set up part of their infrastructure in the country.

At the same time, the government asked DIT to frame India's first encryption policy and directed National Technical Research Organisation, a technical intelligence wing, to develop capabilities to break and provide instant access to all high-end encrypted services.

"It seems the government has finally woken up to the need. The industry needs permission to decrypt up to at least 128 bits. It is a right move in the right direction," said Pavan Duggal, a cyber law expert. "It will be a tremendous boost for online activities, protection of personal data, flipping of e-commerce, banking, insurance and further growth of information security sector in India."

Amod Malviya, vice-president (engineering) at Flipkart.com, said his company welcomed this move.

"One of the main concerns consumers have while transacting online is the issue of security. The number of bits used in the key of an encryption algorithm has an exponential impact on the complexity of breaking/deciphering it. 40-bit encryption is very easily broken, especially with the significant increase in computational power in the recent times," he said.

"Legitimizing 128-bit encryption would allow businesses to be more protected, thus allowing for more security over the Internet. This would be particularly useful for e-commerce organizations, as an ever increasing number of people now transact online over this encryption."

Varghese M. Thomas, director of corporate communications at RIM India, said if implemented, this would be a welcome move, especially since e-commerce, insurance and banking transactions accessed through various modes (PCs, laptops, smartphones) are on the increase in India and require secure, encrypted communication standards.

"India is the global hub for the business process and knowledge process outsourcing industry, where secure communication is a key requirement. This move would further enhance India's image as a secure outsourcing destination," he added.

sahil.m@livemint.com

First Published: Tue, Mar 27 2012. 10 53 PM IST

💬   ✉   🖨   f **Share** ⟨0   🐦 **Tweet**

FROM THE WEB   Sponsored Links by Taboola ▷

Get the Latest Updates from the World of Business, Entertainment and Sports

NDTV

Investing Rs.1000 Per Month Can Lead to Long Term Wealth Creation.

MyUniverse

Help Your Child Get Off TV With This Educational Activity Box

Flintobox

Ayurvedic Treatment for Hair Loss Problem. Your Friends Will Not Believe This!

Lass Naturals Shampoo

Before Earning Fame, She Was Homeless

Bajaj Finserv

Skin Whitening Secret Finally Exposed

Radyance Skin Supplement

Subscribe |Contact Us |Mint Code |Privacy policy |Terms of Use |Advertising |Mint Apps |About Us |Syndication |

Mint on Sunday |RSS |Hindustan Times |Desimartini