INFOWATCH®
BECAUSE YOUR DATA IS YOUR BUSINESS

www.infowatch.com

CTOFORUM
Technology for Growth and Governance

Need for Multi-Layered Protection

19 October 2012 14:04 pm by Varun Aggarwal

Natalya Kaspersky, CEO InfoWatch, co-founder of Kaspersky Lab talks to Varun Aggarwal about how enterprises need to manage new age threats

Data leakages are becoming increasingly common among even the supposedly secure enterprises. Experts suggest that since most of these cases are highly targeted attacks, there is little companies can do about avoiding them. Your views.

That's a wrong approach. If you do not protect your confidential information at all you will be the first target of the malefactors and all your sensitive data will leak! That will inevitably bring reputational losses as well as huge damage to your business. Remember the June incident with Samsung and LG when some of their confidential technologies have been stolen and smuggled out of their manufacturing plants by employees of a subcontracted firm? It is likely that these pieces of top-secret information have got into the hands of rival TV makers, wiping out any advantage Samsung and LG had hoped to gain through their R&D investment in OLED television technology!If you stop fighting you will be shot!Butif you care about defense you have a chance to survive.

There are two major approaches to security of confidential data. The first one is drastic and promotes total security that means blocking all the channels of data transfer outside the company. It is highly efficient in terms of security but absolutely unacceptable if we talk about business processes.

Another approach is a multi-layered conceptof data protection which includes organizational measures, data classification, access rights management and data leakage prevention. Many companies do not understand the key factor of the efficiency of DLP systems and think that DLP is low efficient software. It is only soif the company doesn't know what information it possesses, what part of it is confidential and should be controlled. The problem is that almost 80% of all information in modern companies is unstructured data. That's why efficient DLP systems should include a "pre-dlp" stage - categorizationof corporate data to define what exact information is sensitive and needs to be protected. It is done auto-manually and includes a big part of consulting. After that the DLP software is installed and starts monitoring corporate data. All together this gives quite a high result, about 90 percent of efficiency. Though nobody guarantees absolute security.

The recent case of identity theft of Mat Honanfrom from Wired.com has brought to fore some of the weaknesses in the cloud security. Since most of the cloud vendors dictate their security terms, what can enterprises do to secure their data in the cloud? Also, what should individuals do to protect their digital identities?

As for the companies cloud services are still not widely used though the topic is already 12 years old. The main reason is the problem of IT security in the cloud. The thing is that when you give your data to the

cloud services provider the latter operates and stores the data but it doesn't want to take high responsibility for its safety. Provider can only include limited responsibility into the cloud agreement because otherwise it'll quickly be out of business. So now when you put your data into the cloud you can mentally say "Goodbye" to it. That's why few large enterprises use cloud services and SMB companies use them by force to save costs. So my advice to companies is either not to use cloud services at all or to put only non-sensitive data into the cloud which is not very convenient but secure.

As for the home users I would advise people again not to put confidential data into the cloud. And unfortunately, if you still use the cloud than Mat Honan's case shows us a necessity to make a backup copy of all important information and store it in inaccessible place which makes the cloud concept senseless.

Companies are choosing to keep mum about their preparedness for a cyberattacks to avoid undue attention from the hackers. While this clearly reflects the growing fear for Anonymous, do you think this is the right strategy to take?

If you are talking too much about how you protect your company's network, what security measures you undertake and what solutions you use than your company becomes vulnerable to attacks. Such transparency may also lead to the reputational damage. On the other hand we see an obvious lack of experience in field of IT security and data protection. Therefore IT security experts share their experience at specialized IT security events which are many in the world or at numerous web resources where professional matters are discussed anonymously, without the risk of data leakage.

Do you have any India specific data detailing the number of breaches or the state of security among Indian enterprises? Please share.

The topic is evidently kept silent and a rare Indian incident is discussed in the press. Still the problem of data breaches is more than relevant since there are lots of manufacturing companies in India and their industrial secrets and intellectual property need protection. Besides the national feature of Indian enterprises is a huge number of employees which means big volumes of personal data and thus higher risk of losses. Nobody knows how efficiently this data is protected. According to The Cost of a Data Breach Study among Indian organizations in 2011 by Ponemon Institute, the average total cost of a breach to an organization was INR 53.5 million ($1 million), with malicious breaches by hackers or criminal insiders being the most expensive type at INR 4,224 ($ 80) for one compromised record.

What do these numbers say? Let's take for example two Indian software development enterprises HCL and Infosys which develop custom software. If they face a data leak incident they put at risk not only their own internal information but also the confidential data of their numerous customers. In this case the two companies will suffer grave reputation damage with a high probability of lawsuits.

Unprecedented number of employees in Indian enterprises dramatically increases the data leakage risk. National mentality doesn't allow Indians to cry stinking fishthus we see only few data leakage incidents announced in the press. But keeping mum about the problem only scales it up.

http://www.thectoforum.com/content/need-multi-layered-protection