Data Loss Protection: The Next Frontier

1/06/2012, INFORMILO
Kate Bevan

The IT security landscape was a very different place in 1997. Hardly anybody was online and computers were mostly threatened by macro viruses that arrived via infected documents that people shared via floppy disk. Spotting the potential market for software that combated the growing menace of malware, Russia-based Eugene and Natalya Kaspersky founded their eponymous company, Kaspersky Lab, to develop and distribute anti-virus software.

Fifteen years later, the Moscow-based company is ranked by technology consultancy Gartner as the sixth-biggest vendor of security software worldwide, with 2011 revenues of $612 million. And the security landscape has changed dramatically. From worrying about macro viruses, businesses are now focused on the integrity and security of their data, the managing of which has become a sector in its own right.

Small wonder then that when Natalya Kaspersky decided to spin off her own business in 2003 she chose to focus on the next frontier in security technology: data loss protection (DLP). Infowatch, a privately-held group based in Moscow, doesn't report revenues publicly, but the DLP market is a rapidly expanding sector: technology consultancy IDC forecasts the market to grow from $446.7 million in 2011 to $808 million by 2015.

"We've seen a switch from a more traditional infrastructure protection offering towards protecting data," says Ruggero Contu, a Gartner security markets analyst. And that data no longer resides solely on hard drives within a company: "Data is not resident in one area any more," he adds. "It's in the cloud, it's mobile – it's everywhere."

This shift and the sheer explosion of data presents businesses with the challenge of how to keep track of it and how to protect it. Says Kaspersky: "Companies don't know what data they have. The first problem is that the amount of data doubles every year; it becomes difficult to handle. The second problem is that data in companies is unstructured: companies don't have a system to organize their data. The third problem is data leakage: companies don't know what's getting out. And the number of channels for leakage is increasing all the time."

Those channels include everything from the malicious insider deliberately leaking information to the myriad personal devices such as mobile phones and laptops that people want to connect to their workplaces. “This is a big headache for the systems manager,” Kaspersky told Informilo during an interview. “People want to be connected to the corporate network but that means security is always playing catch-up.”

Data leakage is a constant headache for businesses of any size. It’s embarrassing at best and worse, can damage business when a company’s data is compromised. Take the case of Sony, which was hacked not once, but twice, with millions of customers’ passwords and credit card details compromised. Sony had egg all over its corporate face when it was revealed that those passwords had been stored in plain text and not encrypted.

The problem for businesses is that data gets bigger literally every minute. Every time we log in to a website, pay for something online, transfer money or otherwise leave a footprint, that data is stored somewhere.

One of the biggest problems facing businesses is how to manage data held on a myriad of devices: many businesses are moving towards a “bring-your-own-device approach,” allowing workers to choose their own hardware, which is subsidized by the company. This keeps costs down, but means that IT departments are faced with users whose devices might contain a mix of personal and business documents. IT managers are also faced with compliance issues and with the sheer variety of devices that are trying to connect to the network.

“All of these trends are forcing enterprises to move security controls close to data itself, in addition to the network and application infrastructure on which data lives and moves,” says a December 2011 report by technology consultancy IDC. “Organizations that look only to application or network-based security will have a hard time containing and controlling the use of sensitive corporate data in this de-perimeterized, open computing environment.”

Infowatch handles data for clients including the oil giant Gazprom and RusHydro, the hydropower generation company. For the latter, the issues included improving protection of data held internally and also helping it comply with international protocols on data protection.

Infowatch has thus far been focused on big infrastructure issues for businesses, but its recent purchase of Germany’s Cynapspro has given it expertise in managing the end of the infrastructure chain. Cynapspro specializes in managing permissions on mobile phones that connect to a corporate network and controlling the access points to the network. It’s a good fit for Infowatch, and should see Kaspersky’s business building a bigger presence in a market that is growing rapidly.

Symantec, McAfee (now owned by Intel), CA Technologies, Websense and RSA are ranked by IDC as the top five vendors in the DLP space. InfoWatch is still considered a niche player by analysts, but then again, no one believed that it would be possible to build a top-ten global anti-virus company from Russia when Natalya and her ex-husband Eugene first began building Kaspersky Lab. If the past is any indication of the future, Infowatch will prove to be a company worth watching.

Source http://www.informilo.com/20120531/data-loss-protection-next-frontier-609