Mobile strategies increase need for data loss prevention technology in Europe

Mobile strategies increase need for data loss prevention technology in Europe

Data loss prevention technology that covers all popular mobile platforms and is easy to use and implement is called for as mobile strategies evolve

Mobile has entered business strategy from two directions. The business wants to grab the opportunity to better serve the mobile masses, while employees want to mobile devices as part of their work
This has created an environment that security teams have had to come to terms with quickly.

Roman Foeckl, CEO at security supplier CoSoSys, says the increasing number of mobile devices in the enterprise, and new versions of an operating system, is forcing organisations to rethink ways of securing corporate data.
It is not just about mobile the applications, he says, but also how employees interact with other organisations and people. Mobile provides low-cost computing power that is available to everyone and enables staff to collaborate with others, but this is a recipe for security breaches in businesses.
Foeckl says traditional security is irrelevant in many cases. For example, he says the shift from open file systems (Windows 7) to application sandboxes (Android, iOS, Windows Phone/Pro/RT), is making traditional antimalware, especially antivirus, less relevant.
For example, on iOS, there is little need for antimalware or antivirus products because neither they, nor any other app on the device, can access another app's storage or memory.
According to Foeckl, when planning a mobile security strategy there is no one size fits all: "Every company has to choose a cross-platform solution that works on Apple iOS, Android mobile devices, Windows, Mac OS X and Linux computers to cover the entire fleet of workstations."
Sufficient resources for data loss protection
But what are companies doing to incorporate endpoint and mobile security tools in applications to make sure they are secure?
"This can be achieved by implementing data loss prevention (DLP) features into applications and more," says Foeckl. "However, the administrators have to be sure that IT resources under their control are ready to co-operate with advanced features like file tracing and file shadowing."

With DLP, the amount of data being monitored and the number of copies stored could quickly absorb a sizeable chunk of the available IT resources.
"In European countries, sometimes we are faced with the situation that a CIO or administrator evaluates resources as insufficient for DLP use," says Foeckl. "In such cases it is recommended to look at cloud-managed DLP and mobile device management [MDM] that offer easy evaluation, implementation and scalability. It's also a good way to safely reap the benefits of the cloud protecting data."
In central and eastern European countries, one obstacle is the fact that many companies still prefer their own datacentres or computing power over cloud services, says Foecki.

Authorisation and security awareness
The software being used in enterprises is changing, so security teams must understand different security features and their limitations.
Foeckl says CoSoSys increasingly supports Macs and iOS devices. It has experience with preventing data breaches that could happen with the use of Google Drive, One Drive, Dropbox, on Windows and Mac OS X computers, for example.

Réagissez à cet article

Source : *Mobile strategies increase need for data loss prevention technology in Europe*