NETWORKWORLD

This story appeared on Network World at
http:// www.networkworld.com/columnists/2008/031008-jericho-forum-horn.html

Data-leak prevention and encryption: Tools that can work together

The Jericho Forum Outlook By Joerg Horn , Network World , 03/10/2008

The Jericho Forum is an organization pushing for innovation in e-commerce security. In this essay, Joerg Horn, head of gateway solutions at Utimaco, a Jericho Forum member, discusses combining data-leak prevention and encryption technologies for enterprise information protection.

Data leakage incidents generally occur when workers are performing everyday tasks, such as sending e-mail that inadvertently contains sensitive information. When this happens, data-leak prevention (DLP) products -- in theory — should be able to flag it for sensitive keywords, fingerprinted documents or data structures, thereby helping to mitigate the risk of data leakage.

Once flagged, data-leak prevention technology analyzes the content, classifies the data and decides whether the data needs to be protected. It can then automatically enforce a pre-determined data protection policy.

The Jericho Forum is an organization with stated principles for fostering innovative security approaches. Principle No. 11 states: "By default, data must be appropriately secured when stored, in transit and in use." The sub-clauses for this principle state: "Removing the default must be a conscious act" and "High security should not be enforced for everything; 'appropriate' implies varying levels with potentially some data not secured at all'".

Today, most people who use encryption on their computer hard disk tend to send data via e-mail, USB, CD-ROM or network to a file-share unencrypted.

Disk encryption technology is designed to protect against external threats, both those that result from malicious insiders trying to steal data (including lost or stolen laptops) and from employee errors. If implemented properly, data-leak prevention offers the tantalizing prospect of being able to apply encryption to sensitive data whenever it is exported, thus protecting against misuse (intentional or unintentional) by people with authorized access to data.

DLP products should be "smart" enough to be selective about encryption, using it only when needed. In practice, if a user puts a confidential database on a USB stick, or sends out an e-mail

containing sensitive data, DLP should automatically recognize that the content needs to be protected and would trigger encryption based on the content. In this case, data-leak prevention should work in concert with encryption by supporting compliance requirements, reducing the cost associated with encryption and streamlining many of the administrative tasks associated with encryption.

Some organizations have tried to solve the problem of data security leakage by placing an appliance in the data center to inspect outgoing traffic from the company network. However, in a de-perimeterized world, there is rarely a consistent "choke-point" to place any such appliance, so this approach fails.

Today, many employees do not work within the walls of the organization. While this mobile workforce can increase productivity, it can also increase the risk that corporate data will be inadvertently exposed. To combat this very modern threat, enterprises should examine their current and future architectures, and where appropriate combine client-based and gateway-based data-leak prevention so that it is close to both the data and the users.

A key component to successful data-leak prevention and encryption deployments is an organization's understanding of which types of data need to be protected, and where that data resides. This is a task not to be underestimated. However neither encryption nor DLP magically begins protecting data. Encryption and DLP can only enforce policies once the policies have been determined and implemented.

In order to be successful with DLP, a company needs to prepare, identify and understand where the data leakage risks are within its organization, as well as determine what its security policies are around the management of sensitive data.

Once policies and the technology are in place, the combination of encryption and DLP then offers the prospect of protecting not only information that is already on hand, but also providing protection for new data as it comes into the organization. Perhaps the greatest advantage to deploying DLP technology is the ability to help companies better understand where sensitive data is located in their organization, classify data so that they understand the different levels of sensitivity they are dealing with, and then apply the right set of controls to that data.

All contents copyright 1995-2008 Network World, Inc. http://www.networkworld.com