



Fact or Fiction: Debunking the Top 5 Misconceptions about Data Protection

Wednesday, March 26, 2008

www.lumension.com



Overview

One of the latest trends in IT security has been the shift in focus toward data-centric protection. Data is the most valuable asset an IT department must protect, and technology has evolved to meet this requirement. Encryption technology and data leakage protection solutions, which tend to rely heavily on content filtering technology, have helped shore up many organizations' data stores, but the problem is that as companies adjust their data protection strategies they have fallen prey to a number of misconceptions about data protection. Security officers should do their best to learn the truth so that they can develop a well-balanced data protection program.

Fiction:

The outside threat is a greater threat than the inside threat.

The Facts:

Data leakage risks can be broken down into two major categories: data loss and data theft. Most of the news stories out today usually relate to the former, typically reports of data missing through lost laptops, back-up tapes and devices.

While the loss of a laptop with thousands of personal records is certainly enough to raise an eyebrow, the likelihood that it will fall into the hands of someone who knows what to do with that data is relatively low. Even if a device or laptop is stolen, it is far more likely that the outsider that gains possession is really just in it for the value of the hardware rather than the data. The appropriate use of encryption can further diminish the risk that an opportunistic thief takes advantage of the valued information contained within.

That leaves us with the second category of data leaks. Data theft is far more hazardous to the enterprise, because in these cases the criminal understands the value of the data and hopes to steal it for their use. These malicious parties, whether they are inside or outside the organization, seek ways to gain access to the data and use it to their advantage. From the outside this is typically achieved through malicious programs designed to install backdoors into the enterprise. From the inside it might be as simple as loading several gigabytes worth of data onto an external device and taking it home.



These days most enterprises have full protection from the outside assaults. It is the threat from the inside that leaves them truly vulnerable. Most organizations have no methods in place to prevent trusted insiders from loading data onto external devices and walking away. And yet, this method of data leakage is perhaps the most dangerous risk among all types of data leaks. Not only does the trusted insider have access to the data, but they usually know the value of the data and what to do with it. If organizations are serious about prioritizing security based on the severity of risk, they must put insider threat protection on top of their list.

Additionally, organizations also need to be able to automatically audit this protection process. Without the visibility of auditing, businesses will be unable to quantify the risks posed by data leaks. They won't know whether data has moved between endpoints, what data it was or how much of it was potentially leaked. It is critical that auditing be baked into the data protection technology to fully realize its benefits.

Fiction:

Data leaks are the only aspect of data protection that enterprises must worry about.

The Facts:

Sure, data leaks have the potential to be devastating. Even if the data itself never makes its way into the hands of wrongdoers, the public relations nightmare that manifests itself after such an event can be harrowing. However, protecting the confidentiality of data is only one facet of safeguarding this information. There are two other huge components as well, namely protecting data integrity and availability.

A well-rounded data protection program should not only be able to mitigate the risk of data leaks, but also to minimize the threat of the data being tampered or destroyed. Failing to address the data integrity component of data protection leaves an organization highly vulnerable.

Auditing and content monitoring capabilities play an important role in this process of ensuring data integrity. Keeping tabs on where data is flowing and being changed can ensure greater control over malfeasance. Additionally, managing vulnerabilities and patches and securing endpoint configurations play a critical role in ensuring data integrity because unmanaged applications and machines can easily allow the propagation of malware and keyloggers, which could compromise the integrity and availability of data.



Fiction:

Email protection will plug all potential data leakage problems.

The Facts:

These days most enterprises have taken heed of the warnings of risk surrounding email data leaks. Security experts have long understood the hole that unmonitored e-mail can present an organization should an insider choose to transmit sensitive information outside the organization, which is why most organizations have endeavored to plug that gap with e-mail monitoring and filtering tools.

Unfortunately, though, some people are under the mistaken impression that e-mail is the only channel they need to guard from unwanted leaks. The truth is that there are plenty of other ways for data to make its way outside the security perimeter. Users can potentially click on malicious links on the Internet that can cause undetected backdoors to be installed on their system. Or more devastatingly, the users themselves can walk out the door with endpoints or devices under their arms, loaded with sensitive information. Clearly, the matter of shutting off data leaks expands much broader than just e-mail.

Fiction:

Enterprises can control data leakage through removable media by banning it.

The Facts:

When analysts first began warning of the enterprise risks posed by removable media, some IT executives reacted quickly with Draconian policies by banning the use of optical drives and USB devices. Once it became clear that users were ignoring these policies, IT departments responded by picking up technology that completely blocks access to these devices or even going so far as to glue shut USB ports.

Security staff that employ such tactics fail to understand why users rebelled in the first place. The outright ban of devices was bad policy because most of the banned devices are useful tools that enable users to more effectively do their jobs.



Banning removable media in order to battle the risks associated with its use really hampers daily business activities. Effective organizations should develop security policies that only ban the risky behavior that makes removable media a threat, then implement technology flexible enough to enforce these policies.

Fiction:

Encryption and content filtering are all you need to protect your data.

The Facts:

While content filtering has certainly improved the state of data protection today, it does have one glaring blind spot. The typical content filtering solution monitors network or e-mail activity, but once information is moved to the local machine it will usually lose oversight of what the user is doing with the data. A user with malicious intentions could easily move data to the local machine and copy it to a USB thumb drive without the content filtering system ever notifying security experts of the problem.

Similarly, encryption also has its own weaknesses. Most encryption solutions do a great job protecting information should a device or endpoint be lost or stolen. Encrypting these devices will prevent someone on the outside from accessing the data they contain. However, once an authorized user enters their password they have unimpeded access to this data. Encryption does not protect the data on the endpoint once that user has authenticated.

In order to achieve truly balanced protection, organizations must supplement encryption and content filtering with a sound endpoint solution that can monitor users and proactively enforce policies on the endpoint.

Lumension Security's Proactive Approach to Comprehensive Data Protection

Endpoints have become the new targets to get unfettered access to data as many organizations do not have enforceable policies and many cannot quantify their exposure to data leakage. While managing removable device usage and data flowing to and from these devices protects an organization from the greatest data leakage outlet, a complete data protection strategy must incorporate other technology to secure data-in-motion and data-at-rest.



Leveraging its proven Positive Security Model, Lumension Security delivers best-of-breed endpoint security solutions to help enterprises proactively enforce data protection policies. They do this by delivering platform, user and data security to protect against data theft and data loss. By securing endpoint configurations, enforcing patch management policies, and delivering granular controls around the use of external devices and policy enforcement of data access and transfer, Lumension Security effectively protects organizations from both the external and insider data threats. Lumension Security's Sanctuary Device Control puts management and control back in the hands of administrators who can not quantify the data leakage problem via the mass usage of external devices.