M86 SECURITY

Data Loss Prevention Simplifying Compliance

Abstract: The aim of this white paper is to explain some of the key concepts of data loss prevention (DLP), the problems organizations find when implementing an effective DLP policy and what can be done to alleviate those problems. The focus of this paper is particularly on single-channel DLP at the email and Web gateway and uses PCI-DSS compliance as a case in point.

INTRODUCTION

Ris ng from a value of $50 million in 2006 to $215 million in 2008 and predicted to exceed $300 million in 2009[1] the growth of the Data Loss Prevention market is indicative of how important this area of security has become. After all, data is usually considered to be an organization's most important asset.

With increasing reliance on the electronic data transfer and storage as well as regulatory requirements, organizations continue to strive to find the best ways in which to control access to sensitive information - and it is not difficult to see why. The independent Web site, http://datalossdb.org/, is updated all-too-frequently with reports of data loss incidents around the world. The effects of not protecting data properly are apparent. Each breach or loss can cost an organization up to $86 per record[2] as well as a tarnished reputation and, increasingly, the wrath of a compliance officer or even the police.

Data Loss Prevention tends to be split up into three categories: network, host-based and information identification.

Network-based DLP solutions usually provide a "single-channeled" approach to identifying and controlling data at one point on the network, either the email or Internet gateways.

Host-based DLP solutions usually consist of an agent installed across all devices on a network and can be used to control access to hardware devices, such as memory sticks, as well as to the data itself.

Information identification usually refers to DLP products that utilize a number of technologies to identify and classify content across a network.

Data loss can occur at many different levels within an organization.

- Outbound or even internal emails may be sent to the wrong user by mistake. This is not uncommon given the "auto-completion of email addresses" feature present in many email clients – thus resulting in accidental but potentially costly security breach.
- Web 2.0 sites make it easy to share information without necessarily thinking about the implications of posting sensitive data.
- All the portable devices make it incredibly easy to remove data from a secure environment and then lose it on the way home or to a meeting.
- Unfortunately, you don't need to look very hard at all to find examples of data loss.

One of the biggest problems faced by an organization wishing to implement an effective DLP policy is the management of false-positives. False-positives occur when information is incorrectly identified as being in breach of policy. This may lead to an important email being blocked or access to essential information being denied. On the other hand, false-negatives can be equally as serious, if not more so. False-negatives can occur when sensitive information is not classified correctly and permitted to leave the secure environment. It is this quandary that has led to many organizations spending a small fortune on DLP products only to keep them in "Monitor only" mode due to the problems associated with misclassification and the problem with "Monitor only" mode is that by the time you close the gate, that horse has already bolted.

Another important problem, especially given the economic climate at the time of writing, is that DLP solutions can be extremely expensive, averaging out at approximately $61 per user in 2007[3]. So it is in an organization's interests to identify what they want to protect and perform a risk analysis against the cost of losing the data against the cost of protecting it. Indeed, many organizations may already be using a number of tools that provide sufficient DLP functionality as to obviate the need for further expenditure.

IMPLEMENTING DLP

For the majority of organizations, DLP does not need to be difficult to implement when using inexpensive, single-channel tools, but there are a few simple steps they need to follow.

First of all an organization must identify what information it is trying to control. For many, this will be dictated by industry regulations or local legislation. Other companies may merely wish to safeguard their own intellectual property. The ability to establish a core dictionary of key words, phrases or patterns is essential to an effective DLP policy. Whether it is credit card numbers, Social Security numbers, a list of medical complaints or financial terms this is the information that will be used to identify a potential data breach. Regular expressions, complex Boolean phrases, fingerprinting or even just simple lists of words can be combined to great effect here to identify content within traffic and permit remedial action.

This, however, is often seen as the most difficult aspect of establishing a DLP policy and will require some planning. Using gateway- or network-based tools to identify content within traffic can greatly diminish the size and scope of this task. Many organizations will only need to identify and control data when it is moving around or leaving the corporate network, so initial monitoring of data-in-motion is the perfect place to start a DLP project.

Once an organization has identified the content it wants to protect, it must look at ways of controlling it. Again, the simplest and most cost-effective manner of doing this is at the network or gateway level. Indeed some of the more advanced email and Web Gateway Security products already provide this functionality - it just needs configuring. Organizations should consider creating content-filtering rules and applying them as required to individuals and groups or even globally where necessary. Once content has been identified as being sensitive, a number of different actions can be taken depending upon the content, the user and in the case of email, the sender or the recipient.

Some examples of common DLP actions are:

Archive – the information is considered safe to access or to send, but it is archived for future analysis should it be required.

Block – access to the information is blocked, or in the case of emails, the email is not sent.

Quarantine – the identified data is held in a quarantine area for review. It can then be released, subject to inspection, or removed.

Monitor – information is identified and logged for reporting purposes. This is commonly used at the inception of a DLP project to identify trends in traffic or when the data is not particularly sensitive. It can also be used to generate reports of permitted access to sensitive data to satisfy auditing requirements.

Alert/Notify – often used in conjunction with one of the other actions, alerts and notifications can be used to inform an administrator or data security officer about an attempted security breach. These attempts are often accidental rather than malicious, so notifications can be used to help educate users about corporate policy regarding sensitive data.

Encrypt – in some cases, sharing the information may be permitted but only if the channel of communication or memory device is encrypted to avoid any problems arising from accidental loss or interception.

For a really effective approach to DLP, it needs to be included as part of a broader acceptable use policy (AUP). Users should be told what is acceptable and what is unacceptable. It is not safe to assume that users know what data is sensitive and that they understand the potential pitfalls associated with Information Technology. Like water, many people often take the path of least resistance, therefore this policy needs to be enforced by technology.

M86 Security recently published a step-by-step guide to approaching a DLP project which recommends the following:

Step 1: Do You Really Need a DLP Solution at the Moment?

The first question to ask, believe it or not, is actually whether you really need a DLP solution at the moment. The reason for this question is that the technology and capability of DLP solutions is improving all the time, so the longer you can delay the implementation, then the better the product – so the theory goes. I am not advocating putting your organization at risk, but DLP is a strategy that needs careful planning.

Step 2: What Type of Solution Do You Require?

There are many different types of products on the market that promise to solve DLP such as hard drive encryption products or endpoint port control solutions. While they may address one of the ways that data loss can occur they do not address the issue as a Content-aware DLP solution will. Content-aware DLP solutions focus on controlling the content or data itself.

There are two different types of Content Aware solutions:

a. Single Channel solutions – Focuses on just the data loss channel you want to address such as email or Web.

b. Enterprise DLP solutions – Involves lengthy implementations and big budgets. It can also be very disruptive to the organization but delivers much more coverage.

However, just because you are an enterprise don't assume you need an Enterprise DLP solution. Don't think automatically that you will need to go out and buy a new product. You might find that your incumbent vendors for email or Web might have a good enough range of products to meet your current needs and a solid roadmap to ensure they will continue to meet your needs in the future.

Step 3: Identify What You Want to Protect

If you know exactly where all the content is that needs to be protected, then you are well on your way. If you don't, then you will need to consider using a data discovery solution to answer this question first, and also make sure that you address this issue by ensuring you have control over where types of content are saved. This will pay dividends in the future.

Step 4: Establish Why the Content Needs to Be Protected

Is it for compliance reasons or for protection of Intellectual Property? This could change not only how the content is identified but also how it is reported on. For compliance, you will need to ensure that you meet not only the data coverage required, like credit card numbers and other personally identifying information (PII) as required for PCI DSS compliance, but also the reporting requirements for the auditing process. For IP control, perhaps the solution has to recognize source code, or perhaps CAD files? Ensure the solution you select has the coverage and is easy to teach for your required data types. Don't take the vendor's word for it. Try out the solutions against your data and compare different solutions. This is going to be a critical step in the success of your DLP solution, so you need to give it the time it deserves.

Step 5: Identify How Data is Currently Lost

This will help you determine the type of product to use. Is it through email? Is it being uploaded to Web sites such as Web email or blog sites? Is it the usage of USB flash drives on your endpoints? The most important advice here is not to try to solve all possibilities that you can think of for data loss. You have to remember that what you are trying to stop is the accidental loss of data. If you are trying to stop the deliberate loss of data, then that is significantly more difficult and will quite definitely have a serious impact on your business. If the user is resourceful and knowledgeable enough, they will find ways to do it. An audience that many companies forget about is the remote user and the devices they use off-site. People will be more bold and daring if they are not in the office of their organization.

Step 6: Policy Creation

This is where we get down to the implementation. Once the solution is installed, we now look at how we can create policy that recognizes the actual content we want to control and then how it will be controlled. The above steps that you have gone through will help you determine what should be in the policy and how you can prevent the information from leaking out of your organization.

Step 7: Testing

Like any other IT implementation, testing is a major factor for ensuring success. You need to do a significant amount of testing with this; always better to be run initially in monitoring only mode to gauge the impact while you are tuning the controls. The testing will help you to fine tune the policy and how it is enforced in the future.

Step 8: Policy Communication

A step many miss. Employees need to be brought into the project to guarantee success. It will impact their day-to-day functions, so you need to be certain they understand why these controls are in place and support its use. This can be as simple as explaining why you are implementing such a control and what could happen if you didn't. Obtain their feedback on the controls and how you might minimize the impact on their work.

Step 9: Policy Enforcement

Now that we have created the policy, tested it and communicated it, time has come to throw the big switch between just monitoring controls to actively implementing them. Don't turn them all on at once. Prioritize them and release the most important and critical ones first. Ensure you have plenty of coverage to rectify any issues not found in testing as they arise, as this will impact the employees who are trying to do their job. If you are not helpful or responsive, your employees' support will vanish!

Step 10: Future Proof Your Organization

You have taken the first steps here, but don't assume your job is done. Look for better ways of classifying content or where different types of content are saved. When new applications or systems are installed, consider how you can implement them to simplify the DLP controls required. Also continue to pay attention to the evolution of your DLP product. Keep it up to date as there will be newer and better ways of implementing the controls you have in place.

PCI-DSS AND M86 SECURITY: A DLP CASE STUDY

As mentioned earlier, for many organizations, DLP is being driven by ever-increasing regulatory requirements. HIPAA, Sarbanes-Oxley, GLBA, Basel II, PCI-DSS are amongst the many industry regulations organizations must comply with. All of them revolve around controlling data.

First established in 2004, PCI-DSS (Payment Card Industry Data Security Standards) is now one of the most widespread pieces of compliance regulations around, and any organization that handles credit card information is expected to be compliant or striving to attain it. While some suggest that PCI-DSS requires only a hardly-sufficient, simplistic approach to data security[4] it is nevertheless a good yardstick by which to measure an organization's data security.

As a case study for looking at DLP, PCI-DSS is ideal because its single aim is to ensure the protection of credit card information. The actual requirements for achieving PCI-DSS compliance are manifold. Although they are broken down into six distinct sections, each is addressed and used as examples, where appropriate, of how different single-channeled DLP tools can be used to help with compliance.

A. Build and Maintain a Secure Network

- Install and maintain a firewall configuration to protect cardholder data.
- Do not use vendor-supplied defaults for system passwords and other security parameters.

While not really relevant to a discussion of DLP, PCI-DSS's first requirement is to establish basic network security requiring the separation of the local network from the Internet and protecting the network from Internet-borne threats by using a firewall. It also requires organizations to secure this infrastructure by locking down access to integral systems – a good place to start.

B. Protect Cardholder Data

- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.

Security products like MailMarshal SMTP, MailMarshal Exchange and WebMarshal can be configured to detect content within data streams. MailMarshal (SMTP and Exchange) is configured to use regular expressions that can detect credit card numbers and data associated with credit cards. Rules can be created quickly and easily to ensure that any content that is considered to contain credit card information will be dealt with accordingly. WebMarshal can also identify phrases and expressions and block data being uploaded to Web sites, forums or blogs or prevent that data being sent via Web mail accounts such as Hotmail or Gmail. WebMarshal and MailMarshal SMTP can also utilize a number of other techniques to help protect against malicious code, phishing attacks, bad Web sites, dangerous file types and other threats that can arise at the Web or email gateway, thus helping further protect cardholder data.

MailMarshal Secure Email Server and MailMarshal SendSecure can be used in conjunction with MailMarshal SMTP to ensure that any emails containing credit card or personal information are only ever allowed to leave the email gateway in an encrypted fashion. WebMarshal has the ability to block sensitive content that is being uploaded to an unencrypted site, again ensuring that sensitive cardholder data is not being sent over the Internet in an insecure manner.

C. Maintain a Vulnerability Management Program

- Use and regularly update anti-virus software on all systems commonly affected by malware.
- Develop and maintain secure systems and applications.

MailMarshal (SMTP and Exchange) and WebMarshal can use multiple anti-virus engines and file detection techniques as well as zero-day protection tools to ensure malware is blocked. The M86 Web Filter is also able to identify attempts by malware to "call home" for updates and instructions.

All M86 products have been designed to secure unsecure protocols and methods of communication. From DoS and DHA attacks to blocking offensive language, M86 products allow administrator to protect their email and Web gateways from all kinds of threats and vulnerabilities.

D. Implement Strong Access Control Measures

- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.

MailMarshal (SMTP and Exchange) and WebMarshal can all be used to ensure confidential data is not transmitted beyond permitted users. MailMarshal for Exchange can enforce "ethical" walls within a company's internal email system; while MailMarshal SMTP Gateway can ensure that this data is not sent outside the organization (or if it is, then only to specific recipients – and even then you can choose to enforce encryption). WebMarshal can be used to prevent users from uploading confidential information to Web mail, blogs, forums or other sites.

E. Regularly Monitor and Test Networks

- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.

Alerts can be generated whenever MailMarshal or WebMarshal identifies credit card information in an email or HTTP traffic allowing for prompt action to be taken. Likewise, a range of reports can be created allowing for the identification of trends and in-depth forensic analysis.

F. Maintain an Information Security Policy

- Maintain a policy that addresses information security.

WebMarshal, MailMarshal and the M86 Web Filter are provided with a default security policy that can be adapted quickly and easily to suit the needs of any environment. An important part of maintaining an acceptable use policy is ensuring users now about it. M86's suite of security products uses email notifications and Web-based warning pages to ensure that users know that an acceptable use policy is in place and educate them when they have contravened that policy.

CONCLUSION

In summary, data and information has always been important and people have always tried to protect confidential information. The problem many organizations face today, however, is that it has never been easier to access or move data - and the costs have never been so high. Portable memory devices, email and Internet access provide easy means by which sensitive data can be transmitted, distributed or lost. Users can intentionally or accidentally share information with third-parties with just a few mouse clicks, and with regulators ready to pounce with large fines and, in some cases, prison sentences, data leakage is something that people can ill-afford to ignore.

As such, it is essential that organizations are able to identify their sensitive information and protect access to it. Whether it is intellectual property, personal information, data subject to regulatory requirements or even "Top Secret" military documents, organizations need to be aware of what it is, where it is going and how to protect it.

To this end, organizations need to deploy content-aware security products to help back up an Acceptable Use Policy combined with staff training that clearly states what information should be treated as confidential and any actions that should be taken when sharing it.

Currently, the easiest and most cost-effective method of achieving this is to use the single-channeled network and gateway tools that provide easy-to-use and extremely effective data loss prevention techniques that address the needs of most organizations. In many cases, this may well simply mean looking at gateway security products that are already in place and configuring them to meet new DLP requirements.

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry's leading Secure Web Gateway provider. The company's appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 24,000 customers and over 17 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advance threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

EMAIL SECURITY SOLUTIONS

M86 MailMarshal SMTP - provides software-based threat protection, unifying content security, policy enforcement, compliance and data leakage prevention. It acts as an email gateway, filtering all incoming and outgoing content at the perimeter and is highly scalable, flexible and easy to manage.

M86 MailMarshal Exchange - filters and manages internal, inbox-to-inbox email. It monitors and controls intra-organizational email content, facilitating a safe, productive working environment and compliance with acceptable use policies.

M86 MailMarshal Secure Email Server - a dedicated, policy-based, secure email solution that provides encryption, digital signature and deep content inspection of inbound and outbound email messages. It operates with any email gateway that can recognize S/MIME encrypted email and automatically updates contact details and secure certificate credentials for encryption contact via a centralized server.

M86 MailMarshal SendSecure - a hosted service that facilitates encrypted email messages to anyone in the world without requiring a pre-existing relationship or certificate and key exchanges. It doesn't require special software installed prior to reading secured messages.

M86 MailMarshal Service Provider Edition - a Software as a Service (SaaS) solution that enables managed and Internet Service Providers to offer complete end-to-end, hosted email security services. Includes email filtering, anti-spam, anti-virus, encryption, pornographic image detection, policy compliance, email archiving and reporting services delivered in a centrally managed, highly scalable architecture. It is complete with a customizable user interface and tiered service levels.

WEB SECURITY SOLUTIONS

M86 Secure Web Gateway - provides best-of-breed on-site and cloud-based real-time Web security. Patented, active Real-time Code Analysis and optional anti-virus modules inspect inbound and outbound communication. It keeps malware and crimeware out of networks and sensitive/confidential data in.

M86 WebMarshal - provides software-based, comprehensive Web access control and management, proxy caching, threat protection (URL, anti-virus and malware filtering) and data leakage prevention. It is policy-based, easy to manage and highly scalable.

M86 Web Filtering and Reporting Suite - provides high-performance, scalable, appliance-based Internet filtering, application control, detailed forensic reporting and real-time monitoring and mitigation of Web-based threats. It is interoperable and easy to deploy in any network infrastructure, and it utilizes "pass-by technology/span port deployment" for zero network impact and fail-safe operation. Also supports remote laptop filtering for PC and Mac.

ENDPOINT SOLUTIONS

Marshal EndPoint Security - a policy-based enforcement solution that allows only authorized removable media devices to connect to computers and servers, preventing data leakage and data theft. It enables organizations to monitor and control what information goes in and out of the network via removable media devices such as USB flash drives, iPods, PDAs and CDs.

REFERENCES:

1. Gartner Magic Quadrant for Content-Aware Data Loss Prevention, July 2009.
2. http://www.theregister.co.uk/2009/02/04/data_breach_cost_guesstimate/
3. Frost & Sullivan's 2008 World Data Leakage Prevention Market Report.
4. http://searchsoftwarequality.techtarget.com/news/column/0,294698,sid92_gci1335662,00.html#

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads

M86 SECURITY™

Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Millennium Centre, Bldg C, Level 1
600 Great South Road
Ellerslie, Auckland, 1051
New Zealand
Phone: +64 (0) 9 984 5700
Fax: +64 (0) 9 984 5720

Version 05.23.10