InformationWeek :: reports

Next

Reports.InformationWeek.com January 2012

How to Prevent an Illicit Data Dump

There are no silver bullets when it comes to protecting company and customer data from loss or theft, but there are technological and procedural systems that will go a long way toward preventing a WikiLeaks-like data dump.

By Michael Cobb

Presented in conjunction with

SECURITY dark READING
Protect The Business Enable Access

Report ID: S3850112

TABLE OF CONTENTS

Figures

ABOUT US

InformationWeek Reports' analysts arm business technology decision-makers with real-world perspective based on qualitative and quantitative research, business and technology assessment and planning tools, and adoption best practices gleaned from experience. To contact us, write to managing director **Art Wittmann** at *awittmann@techweb.com,* content director **Lorna Garey** at *lgarey@techweb.com,* editor-at-large **Andrew Conry-Murray** at *acmurray@techweb.com,* and research managing editor **Heather Vallis** at *hvallis@techweb.com.* Find all of our reports at *reports.informationweek.com*

Michael Cobb
InformationWeek Reports

Michael Cobb, CISSP-ISSAP, is a renowned security author with more than 15 years of experience in the IT industry. He is the founder and managing director of Cobweb Applications, a consultancy that helps companies secure their IT infrastructures and achieve ISO 27001 certification.

Michael co-authored the book *IIS Security* and has written numerous technical articles for leading IT publications.

EXECUTIVE SUMMARY

In today's business environment, there are many opportunities to increase productivity by sharing data and integrating network and business operations. However, network-based collaboration introduces corporate data into a broader environment that is more complex, vulnerable and difficult to safeguard. Also, the amount of data that needs protection has grown exponentially as data gathering and analysis capabilities improve. In addition to having more data at risk, businesses today suffer greater consequences if their data is lost or compromised. Although fines may not be financially crippling, damage to a company's reputation can be irreparable. While maintaining perimeter defenses to safeguard against outside threats is still an essential aspect of data protection, internal threats and data leaks are just as much of a problem and require technology as well as procedural and training systems. In this report, we examine how enterprises can better protect their data from leaks by an unauthorized or privileged user, ensure that large amounts of data aren't moved all at once, and recommend how to handle a data breach should one occur.

Previous Next
Table of Contents

Malicious or Not, Big Data Loss Happens

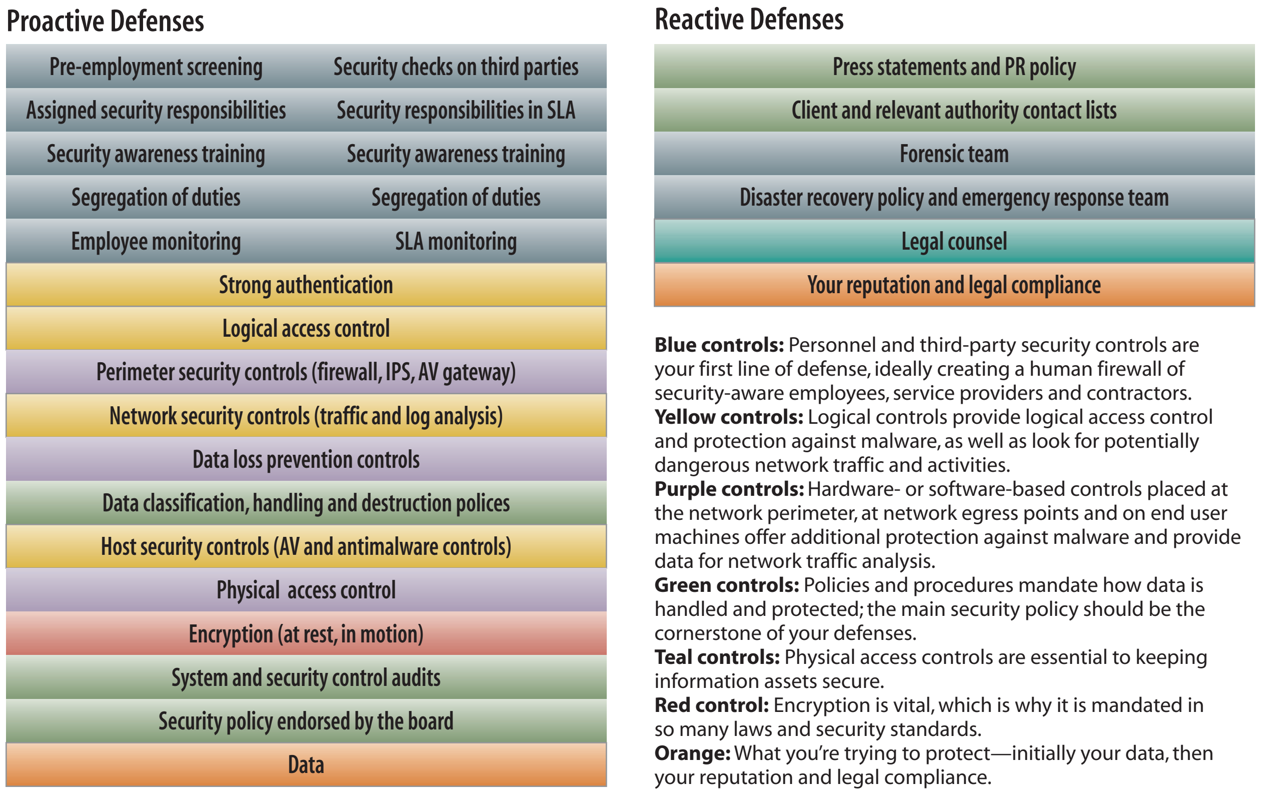
Laws have been passed and standards created, yet serious data breaches continue to occur—some on a colossal scale. In 2011 alone, 77 million Sony PlayStation users and more than 4 million clients of California's Sutter Health had their address and email records stolen or lost. And Private First Class Bradley E. Manning is awaiting trial for allegedly leaking the largest cache of secret data in U.S. history to an unauthorized source, WikiLeaks. A list of just some of the breaches that have been reported since 2003, when the first U.S. security breach notification law came into force, illustrates the myriad ways in which companies can lose control of their data (see Figure 1). It also seems to demonstrate that few companies are learning from the mistakes of others.

It's important to appreciate that nearly all data breaches are unintentional. A report just out in the United Kingdom shows that most of the data breaches suffered by local agencies in the past three years—more than

Figure 1

Layered Defenses Are Best Data Dump Offense

The systematic, layered defenses listed here will help protect your company's data—and reputation—from a data dump attack. These defenses appear in the order in which an attacker should confront them, so you can prevent an attack—or at least stop it in its tracks before it does any significant damage.


Proactive Defenses
Pre-employment screening
Security checks on third parties
Assigned security responsibilities
Security responsibilities in SLA
Security awareness training
Security awareness training
Segregation of duties
Segregation of duties
Employee monitoring
SLA monitoring
Strong authentication
Logical access control
Perimeter security controls (firewall, IPS, AV gateway)
Network security controls (traffic and log analysis)
Data loss prevention controls
Data classification, handling and destruction polices
Host security controls (AV and antimalware controls)
Physical access control
Encryption (at rest, in motion)
System and security control audits
Security policy endorsed by the board
Data
Reactive Defenses
Press statements and PR policy
Client and relevant authority contact lists
Forensic team
Disaster recovery policy and emergency response team
Legal counsel
Your reputation and legal compliance

Blue controls: Personnel and third-party security controls are your first line of defense, ideally creating a human firewall of security-aware employees, service providers and contractors.
Yellow controls: Logical controls provide logical access control and protection against malware, as well as look for potentially dangerous network traffic and activities.
Purple controls: Hardware- or software-based controls placed at the network perimeter, at network egress points and on end user machines offer additional protection against malware and provide data for network traffic analysis.
Green controls: Policies and procedures mandate how data is handled and protected; the main security policy should be the cornerstone of your defenses.
Teal controls: Physical access controls are essential to keeping information assets secure.
Red control: Encryption is vital, which is why it is mandated in so many laws and security standards.
Orange: What you're trying to protect—initially your data, then your reputation and legal compliance.

Data: *InformationWeek Reports/Dark Reading*

1,000—were accidental: USB sticks lost, emails sent to the wrong addresses, laptops stolen from parked cars, paper files gone astray and so on. However, some cases involved deliberate, malicious actions by insiders, such as terminated employees stealing data, people disclosing information to unauthorized third parties and people accessing information without proper cause. In one situation, scanned case notes from a social services agency relating to children were uploaded to Facebook.

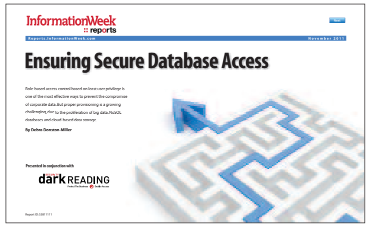
Employee actions and behavior, innocent or malicious, increase the risk of data loss and leakage; disclaimers about unintended recipients and confidentiality neither mitigate legal liability nor protect the data from misuse. Exacerbating the problem is the fact that data is more accessible—and portable—than ever. For example, a mobile device can easily hold tens of thousands of documents and emails, while removable media can store the data from an entire hard drive. These devices make it easier for employees, service providers and thieves to access, copy, lose or abuse your intellectual property and customer data.

Developing and enforcing rules around how data is handled within your company is the most effective way to reduce the likelihood of a major data loss.

The first step is to classify your company's data in terms of its value, legal storage and protection requirements, sensitivity and criticality. If you don't know what you need to protect and its value, you can't allocate the necessary and appropriate security controls to guard against data loss and theft. However, many companies don't bother with this fundamental exercise of identifying and prioritizing business information and systems, determining where data is located and completing a threat analysis.

With classifications in place, data should be labeled—either with metatags, in the case of digital data, or physical labels, in the case of printed material or physical storage devices. With policies and procedures covering how each class of data should be handled—from access to copying, printing, sharing and deleting—you can begin to educate your employees on the importance of safeguarding company and client data. Archived data requires a specific mention here because it represents a large amount of information in one spot, often stored on a backup system, such as a tape or CD. This makes it portable and an obvious target for thieves.

When employees break data-handling rules, they are typically not doing so with malicious intent—they just may not know the rules. For example, an employee may send a corporate document to a Gmail account so he or she can work on it at home, not realizing that by doing so the data is being sent outside the enterprise's defenses. It is important to be specific and explicit in your rules around data handling so users will not have to infer what is and isn't OK. This is especially key as the lines between work and home—and between corporate and personal smartphones, tablets and other devices, given the bring-your-own-device trend—continue to blur. Security pros at multinational companies must also be aware


InformationWeek :: reports
Next
Reports.InformationWeek.com November 2011
Ensuring Secure Database Access
Role-based access control based on least user privilege is one of the most effective ways to prevent the compromise of corporate data. But proper provisioning is a growing challenging, due to the proliferation of big data, NoSQL databases and cloud-based data storage.
By Debra Donston-Miller
Presented in conjunction with
dark READING
Report ID: S3811111

Related Report

Protect enterprise data integrity with role-based access control user provisioning, applying the concept of least user privilege. Get our report "Ensuring Secure Database Access."

Download

Previous Next

Table of Contents

of the different social and business cultures across their global offices. What is seen as an unacceptable abuse of IT in the United States may well be tolerated elsewhere.

Of course, that's not to say that all data policy breaches are inadvertent. Active breaches include altering security settings, accessing unauthorized parts of the network, and sharing work devices and sensitive information with nonemployees. Although these actions may be performed with good intentions—usually in the name of getting a job done more efficiently—they undermine IT security policies, open the door to potential threats and invite attackers inside the company. They occur mainly because employees don't know or appreciate the potential consequences.

Go Beyond Security Awareness Training

While it is important to build awareness around what is and isn't acceptable in terms of data handling, it isn't enough. It's essential to actively enforce your policies by monitoring employee access and activity with regard

Figure 2

Data Breach Timeline

This timeline of data breaches is long and well-populated, yet it does not include all the known data breaches suffered in the past decade—just some of the worst.

2010-2011	WikiLeaks	A variety of government files—including secret files relating to prisoners detained in Guantanamo Bay and U.S. State Department diplomatic cables—were obtained and published.
October 2011	Sutter Physicians Services and Sutter Medical Foundation	An unencrypted desktop computer containing personal data of more than 4 million patients was stolen.
April 2011	Sony	A data breach of Sony's Playstation Network resulted in the compromise of information of an estimated 100 million users.
May 2010	Cincinnati Children's Hospital Medical Center	A laptop containing more than 61,000 unencrypted patient records was stolen from an employee's car.
January 2001	Lincoln National Financial Securities	A security vulnerability may have leaked personal data of 1.2 million customers due to the sharing of a user name and password.
December 2009	RockYou	A database containing 32 million user names and plain-text passwords was breached using SQL injection.
June 2009	Baptist Medical Center	Hundreds of medical records containing sensitive patient information were found dumped in a landfill site.
January 2009	Heartland Payment Systems	In potentially the largest criminal breach of payment card data ever, estimates of up to 100 million cards from more than 650 financial services companies were compromised.
October 2008	Express Scripts	The company learned of a breach of its customer database upon receiving a letter demanding money and threatening to expose records of millions of patients. It notified about 700,000 consumers that their records may have been breached.
January 2008	GE Money	A magnetic tape containing 150,000 Social Security numbers and in-store credit card information from 650,000 retail customers went missing.
October 2007	U.K. Revenue and Customs	Two password-protected discs containing the entire database of personal details of about 25 million people in the United Kingdom were mailed unrecorded but never arrived.
September 2007	Gap	A laptop containing unencrypted personal information of 800,000 people who applied for jobs at retailer the Gap was stolen from a third-party vendor.
January 2007	T.J. Maxx	A computer security breach dating back to 2005 allowed hackers to access information on more than 45 million credit and debit card accounts.
August 2006	AOL	The release of data containing search keywords used by more than 650,000 people, intended for research purposes, became publicly accessible on the Internet.
May 2006	Department of Veterans Affairs	An external hard drive containing unencrypted information on 26.5 million people was stolen from the home of an employee.
December 2005	Ameriprise Financial	A laptop stolen from an employee's locked vehicle contained 158,000 client names and account identification numbers.
August 2004	University of California, Berkeley	A hacker gained access to sensitive personal data on 1.4 million Californians who participated in a state social program.

Data: *InformationWeek Reports/Dark Reading* to classified data. The objective is to deter and stop employees or contractors looking to exploit their legitimate access to your premises, assets or data. If employees know there's a chance that inappropriate activity will be picked up by network filters and log analyzers, they are far more likely to follow procedure, particularly if wrongdoing will incur strict disciplinary measures.

> "Part of your defense against a major data dump—intentional or otherwise—must be some form of DLP technology."

Given the ever-increasing array of devices and different types of users connecting to the corporate network, part of your defense against a major data dump—intentional or otherwise—must be some form of data loss prevention (DLP) technology. A software or hardware system installed at network egress points and end user machines, DLP technology uses advanced deep content filtering and controls over removable storage, optical media drives and wireless networking protocols to prevent unauthorized use and stop sensitive data from leaving the network in violation of information security policies. DLP options range in scope from simple email filters to deep packet analysis of network traffic, port blocking, data transfer monitoring and printer control.

Like network-based controls, DLP can address internal as well as external communications, and can therefore be used to control information flow between groups or types of users. It is important to determine how far a particular system goes in actually preventing unauthorized movements of data. To provide the ability to prevent and not just detect data leaks, a product must alert users in real time of a potential security threat resulting from their actions. This not only stops users from proceeding with the actions, but can also help them understand why such security controls are in place. It also reinforces the difference between good and bad work practices, and helps modify users' behavior.

Endpoint DLP systems have an advantage in that they can monitor and control access to physical devices, such as mobile devices with data storage capabilities. The disadvantage is that they must be installed on every workstation in the network. In addition, they won't work on users' cell phones and won't do anything to prevent breaches that occur when users access enterprise data from, say, an Internet cafe.

Know Your Network

Before you can make an informed choice as to which DLP system best suits your company's needs, you have to understand the traffic on your network. DLP systems use various methods for deep content analysis, ranging from keywords, dictionaries and regular expressions to partial document matching and fingerprinting. Testing for accuracy helps to ensure a system has an acceptable level of false positives and negatives. The most efficient way to do this testing is by conducting a network traffic analysis and adjusting alarm thresholds so regular permissible day-to-day activities don't trigger unnecessary alerts. For highly secure systems, it is better to err on the side of caution and live

FAST FACT

4M+

Number of patients whose personal data was stolen from Sutter Health in October 2011

with a higher number of false alarms to ensure you don't miss any suspicious activity.

Knowing what kind of traffic is normal and what is not will also go a long way toward preventing attacks from the outside. Outside attackers often test their attack tools to ensure the tools are working as expected before launching a full-scale smash and grab. It's vital that this testing phase is detected so the attack can be prevented, and acquiring and maintaining a sense of the traffic traversing your network will make identifying abnormal traffic easier.

Deploying open source tools such as darkstat and ntop on stand-alone passive sensors is a good way to gather traffic volume statistics, active IP addresses and observed services. Security pros should also consider using Layer 3 switches and routers to acquire granular information on hosts conversing on a per-connection basis. This will help suss out traffic from a company host to machines with which they have no business (literally) communicating. This involves collecting session data such as source IP, destination IP, source port, destination port, protocol and traffic sent by either side of a conversation. Flow-tools is an open source software package for collecting and processing NetFlow data from Cisco and Juniper routers, while Argus is a real-time flow monitor designed to track and report on the status and performance of all network transactions. If you spot a session of interest, a variety of tools—including tcpdump, Wireshark, Snort and daemonlogger—can reveal all content data.

DLP: Not a Silver Bullet

All that said, no DLP system is perfect. Many fail to protect all the possible channels on which data leakage can occur, and data synchronizations between employees' computers and their smartphones is not always controlled.

Further, Ponemon Institute research has shown that the document printing and imaging channel is the one most often used for stealing corporate data. Printers and photocopy machines can be controlled to some extent by DLP systems, but once output—even by an authorized person—a sensitive hard copy document becomes a security risk that no DLP system can protect.

Indeed, if a disgruntled employee or malevolent contractor wants to physically sneak confidential data out of the building, DLP products won't stop that. This makes pre-employment screening and service-level agreements with strong security clauses your first line of defense in reducing the chances of hiring anyone likely to present a security concern.

Most enterprises have greatly improved their perimeter defenses to protect their data from external threats, so the recruitment or placement of insiders is an attractive alternative for those looking to gain access to a company's information or physical assets. Once hired, they can exploit their legitimate access to the company's assets for a variety of purposes, unauthorized disclosure of information being the most common. By establishing that job applicants and contractors are who they claim to be and verifying their credentials, companies can go a long way toward weeding out potential problems.

However, just because employees are cleared upon hire does not mean they should be considered inscrutable for the term of their employment. Various factors—ranging from political or religious ideologies to revenge, disaffection, financial gain and coercion—can influence and change the behavior and actions of existing employees. Therefore, personnel monitoring must be an ongoing activity, especially at companies handling very sensitive or valuable data.

It is also important to segregate employee duties so the steps required to complete key processes are divided among two or more people. This way, no individual can act alone to subvert a process for his or her own purposes. Your physical security controls also must be robust. For example, guards and receptionists must be trained to identify suspicious behavior and perform spot checks.

> "No matter how many defenses are in place or how specific a security policy is, there's no such thing as a completely secure system."

And finally, database access controls and encryption are your last lines of defense. Set your databases not to allow queries that return complete data sets and to alert administrators if anyone tries to initiate a Select All query. In addition, put least user privilege and role-based access controls in place. And encrypt all data at rest or in transit around the network. Encryption will not prevent or even deter data loss or theft, but it will render the data unusable by data thieves or anyone who finds a lost device. Figure 2 on page 7 shows how all these different security controls create several layers of defenses to protect your data from accidental or malicious access.

Prepare for the Worst

No matter how many defenses are in place, how specific a security policy is or how well a company's employees are trained, there is no such thing as a completely secure system. You must have a plan in place to deal with a major loss of data should a breach occur.

Unfortunately, once data is in the hands of an attacker, you have little chance of preventing it from being published or sold. Many mobile device management systems allow administrators to remotely wipe devices, but you have to be quicker than the data thieves for the technology to be effective, and digital document expiry controls have not yet stood the test of time.

Still, if your company does suffer a data theft or loss, there are things you can—and must—do to mitigate any damage.

First and foremost, avoid releasing inaccurate or vague information. Your company will fare better in the court of public perception if it comes clean when a data breach occurs. When thieves stole confidential information about several hundred thousand job seekers from Monster.com in January 2009—in the company's second major breach in 18 months—Monster posted only a small security alert about the breach on its home page. Users who accessed the site via bookmarked links didn't even see the disclosure. Not surprisingly, this did not go down well with them.

Honesty plays far better than PR waffle, and it's important in terms of protecting any customers whose personal data has been compromised as a result of the breach. It's best to have a rehearsed incident response. You need to designate who can and who can't talk to the press, how information will be released and what support you'll offer those affected. The only caveat is that some information may have to be kept private because of ongoing police or legal investigations. Your company's legal team should be ready to advise you on this, while the forensic team should be drilled in how to secure potential criminal evidence and work in conjunction with law enforcement agencies.

Bottom line, the security best practices of layered security and continuous vigilance are more challenging to effect but more important than ever.

MORE LIKE THIS

Want More Like This?

InformationWeek creates more than 150 reports like this each year, and they're all free to registered users. We'll help you sort through vendor claims, justify IT projects and implement new systems by providing analysis and advice from IT professionals. Right now on our site you'll find:

Strategy: Email and Data Loss: Discover the pros and cons of email encryption, rights management, email gateways and full-on data loss prevention systems to safeguard data at risk through your enterprise email system.

Strategy: Best of Biometrics: As data volume and sensitivity grow, companies cannot rely on password- and token-based authentication. Biometrics can be used to provide strong access control, but you must weigh added complexity and costs against assurance that users are who they say they are.

Strategy: How to Choose Multifactor Authentication: Learn how to weigh the costs against the risks in selecting the best Web authentication method for your high-risk applications.

Strategy: Hardware-Based Authentication: Considering replacing your password systems with hardware authentication products? Factor in these six decision points.

PLUS: Find signature reports, such as the *InformationWeek* Salary Survey, *InformationWeek* 500 and the annual State of Security report; full issues; and much more.